

Chapter 1: Introduction to Cybersecurity and the Economy

Average annualized cost of cybersecurity (USD)

\$11.7M

Percentage increase in cost of cybersecurity in a year

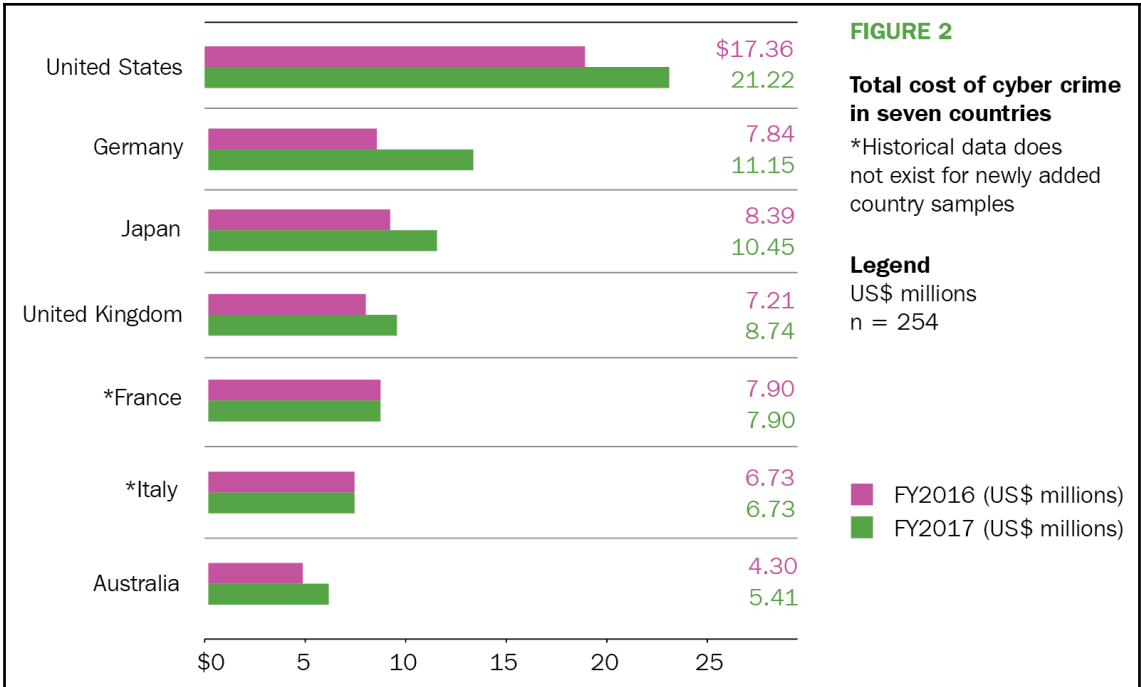
22.7%

Average number of security breaches each year

130

Percentage increase in average annual number of security breaches

27.4%





Please Update Your Account

Dear valued **PayPal** member:

It has come to our attention that your **PayPal** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online services.

However, failure to update your records will result in account suspension. Please update your records on or before **10 Dec. 2011**.

Once you have updated your account records, your **PayPal** session will not be interrupted and will continue as normal.

To update your **PayPal** records click on the following link:
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

PayPal, Inc.
P.O. Box 45950
Omaha, NE 68145

Sincerely,

PayPal



**WARNING - This is a phishing email.
If you receive an email like this,
do not click on any links.**

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

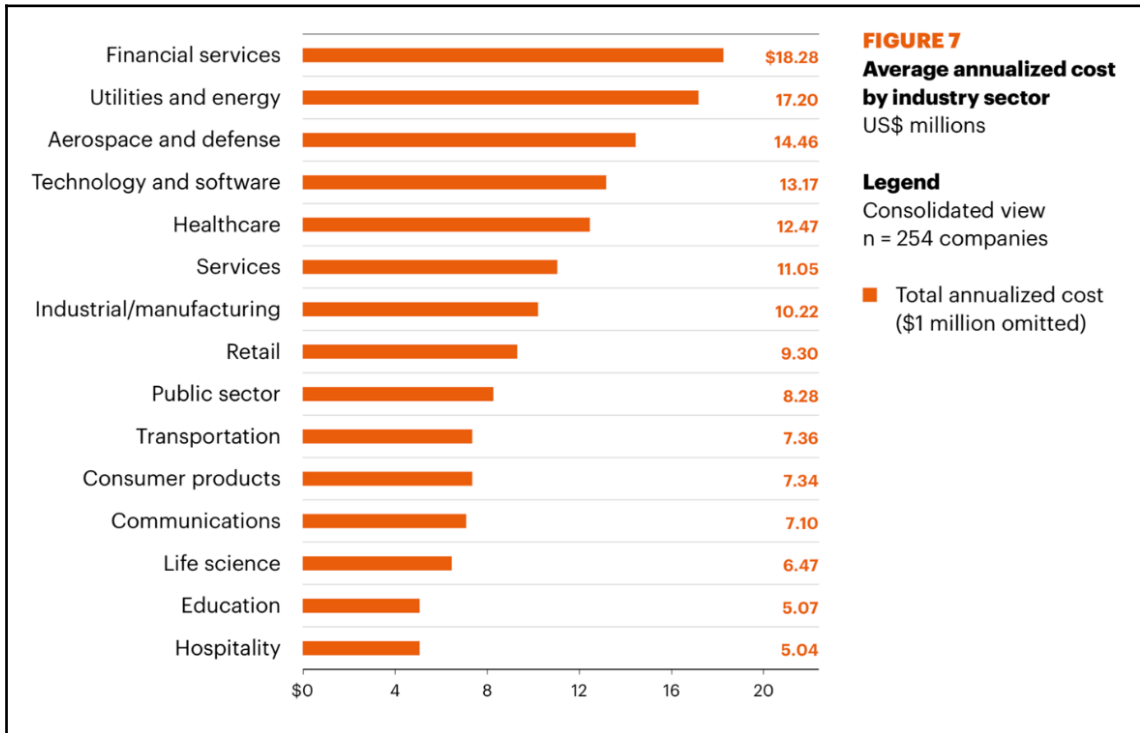
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Chapter 2: Cyber Crime - Who the Attackers Are







K3YHoL3
@K3YHoL353C

Follow



#OpIcarus Phase 4 #OpBlackOct North Dakota U R #TangoDown for making enemies with your people instead of serving them. Shame on U! #OpNoDAPL



https://check-host.net/check-http/host=http://nd.gov

Check website <http://nd.gov>

Permanent link to this check report | Share report:

Location	Result	Time	Code
Austria, Vienna	Connection timed out		
Belgium, Brussels	Connection timed out		
Canada, Ottawa	Connection timed out		
Germany, Dusseldorf	Connection timed out		
Hong Kong, Central District	Connection timed out		
Israel, Tel Aviv	Connection timed out		
Italy, Milano	Connection timed out		
Latvia, Riga	Connection timed out		
Moldova, Chisinau	Connection timed out		
Netherlands, Amsterdam	Connection timed out		
Portugal, Lisbon	Connection timed out		
Russian Federation, Moscow	Connection reset by peer		
Spain, Madrid	Connection timed out		
Sweden, Stockholm	Connection timed out		

4:36 AM - 24 Oct 2016

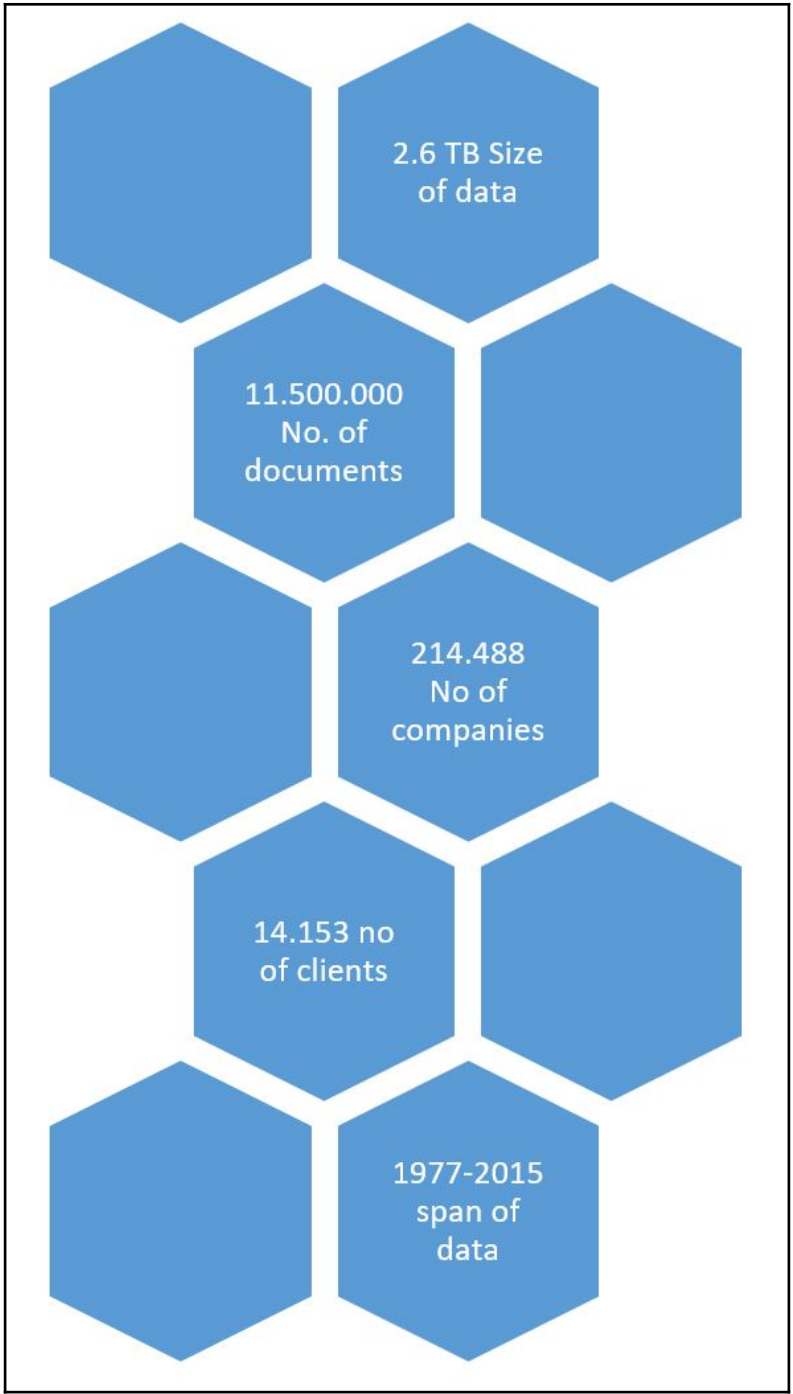
13 Retweets 9 Likes



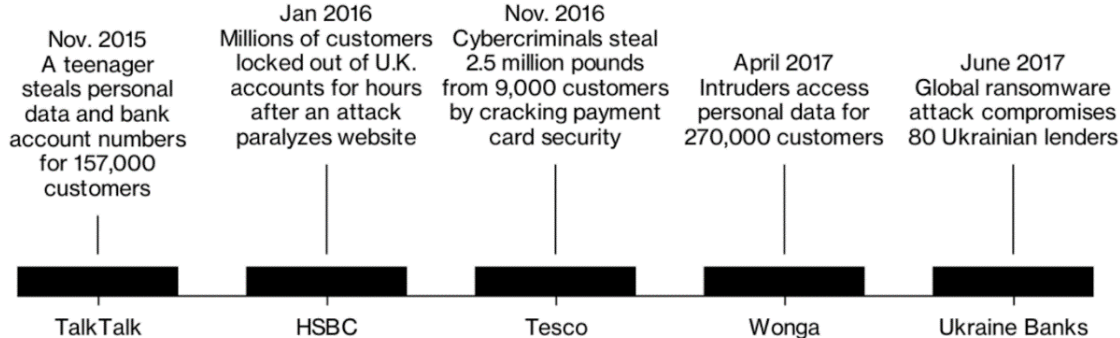
13

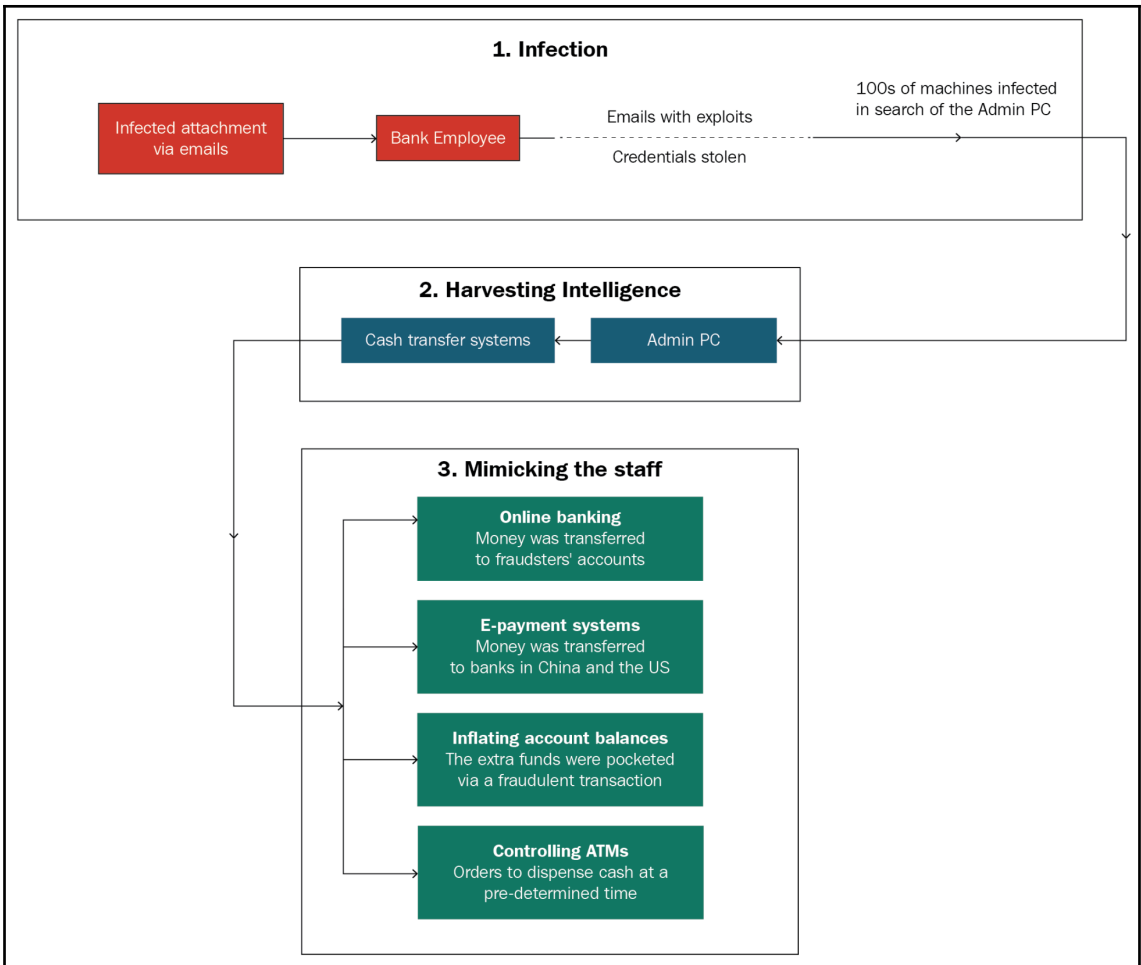
9





Cybercriminals use many methods to penetrate lenders and bank accounts





HSBC Bank (US & UK) Servers Are Down!

  July 12, 2016  [News](#)

Hello Guys, today we checked HSBC Bank security , and their website was able to be attacked! , and now we took it down!

if you are working on HSBC Bank , please contact us on <https://ourmine.org/news/contact-us>

and we will stop the attack and we will let you know how to protect it from people attacks!

HSBC UK: hsbc.co.uk

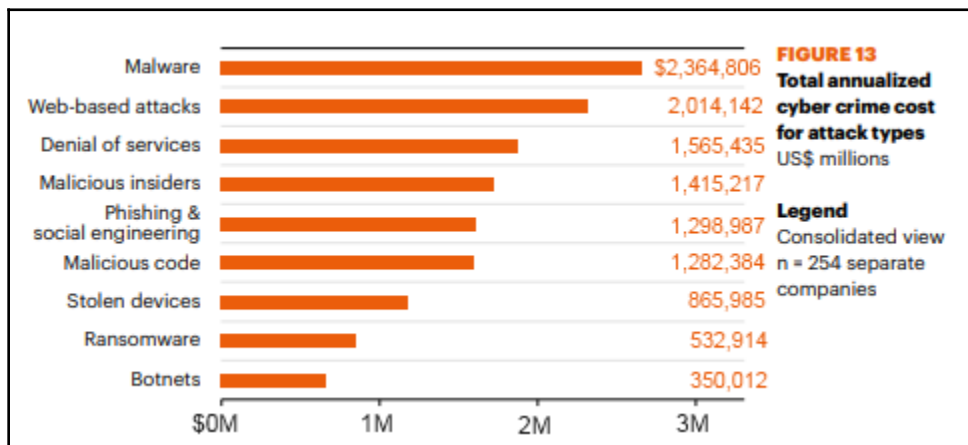
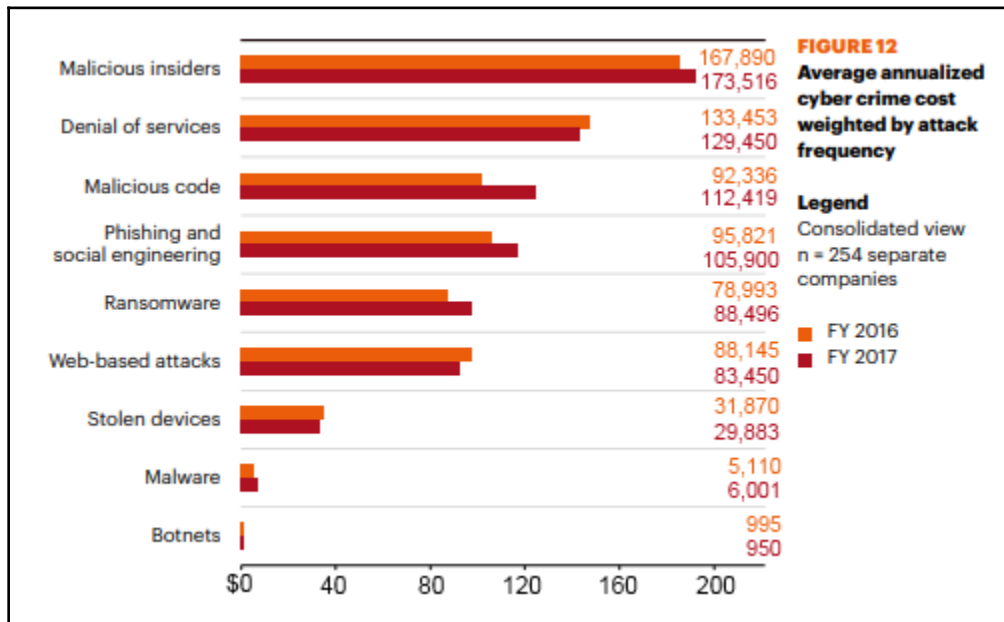
HSBC US: us.hsbc.com







It's not just you! <http://www.hsbc.co.uk> looks down from here.

[Check another site?](#)

Tired of downtime and looking for great web hosting?
[Move to SiteGround and get free migration!](#)

Chapter 3: Counting the Costs



Antivirus Software	# Reviews Rating (1-5)	# Licenses	Best Price
 Kaspersky	579 Reviews 4.0 Stars	3 Licenses	\$24.90
 Bitdefender	88 Reviews 3.0 Stars	3 Licenses	\$59.99
 Norton 360	1,327 Reviews 4.0 Stars	3 Licenses	\$39.00
 BullGuard Premium	2 Reviews 3.0 Stars	1 Licenses	\$65.18
 AVG Antivirus	29 Reviews 3.5 Stars	3 Licenses	\$35.26
 ESET NOD32	22 Reviews 4.5 Stars	3 Licenses	\$38.88

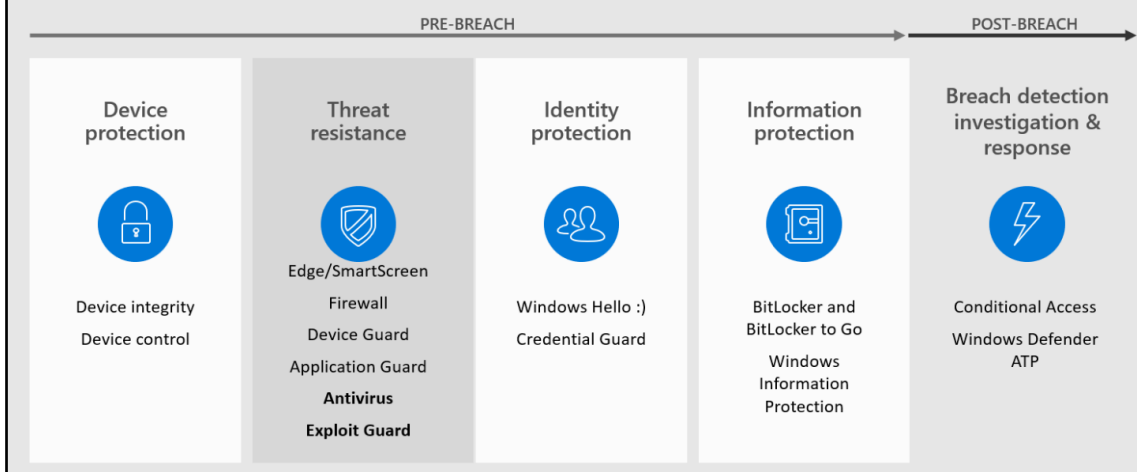
PRODUCT	PRICE	OVERALL RATING	TEST RESULTS	USER EXPERIENCE	MALWARE DETECTION & REMOVAL	DRAGON SYSTEM RESOURCES	NUMBER OF LICENSES
Bitdefender Internet Security...	\$51.99 @Bitdefe...	9.9	10	9.8	100%	97%	3
Kaspersky Internet Security ...	\$39.99 @Kaspers...	9.8	9.8	10	100%	95%	3
McAfee LiveSafe	\$99.99 @McAfee ↗	9.5	9.8	9	99%	95%	10
Avira	Check Price ↗	9.4	10	8.3	99%	99%	1

Thawte

Thawte offers five SSL certificate options; Thawte SSL (\$149/yr), Web Server SSL (\$249/yr), Web Server EV SSL (\$599/yr) and SGC SuperCerts (\$699) and Wildcard SSL (\$639/yr). All the certificates have 128/256 bit encryption and come with warranty ranging from 100,000 US to 500,000 USD.

The certificates are issued between 24 to 48 hours and come with a free Thawte Site Seal. You can compare the features of the SSL certificates at the website.

The Windows 10 defense stack



WINDOWS 10 SECURITY FEATURES AND BENEFITS		Feature	Explanation
1	Device Protection	Trusted Platform Module	Windows uses a crypto processor (TPM) to encrypt and keep security keys from attackers
		Windows-as-a-Service	Keeps OS always up to date with latest cumulative features and security to prevent exploits
		Windows Trusted Boot	Insures Windows boots and Anti-Virus software launches before any applications/malware
		UEFI Secure Boot	BIOS replacement, ensures hardware & Windows has not been tampered with before launch
		Virtualization Based Security	Containerizes key OS functions to prevent attacks like "pass the hash" - Can't find it, can't attack it
2	Threat Resistance	SmartScreen	Prevents users from visiting blacklisted websites or executing blacklisted apps
		Windows Firewall	Device-level PC firewall to prevent unauthorized network access to device
		Windows Defender	Anti-virus software based on the world's largest global threat database
		Microsoft Edge	World's most secure enterprise browser – half the vulnerabilities of other browsers
		WD Application Guard	Tiny HW-isolated Windows instance for Microsoft Edge to browse untrusted website (2017)
3	Identity Protection	Device Guard	Only IT/Windows Store approved applications can run. Like on a phone, malware can't run
		Windows Hello	Two-factor authentication using face, fingerprint, biometric, or PIN. Confirms to website
		Hello Companion Devices	Use phone, badge, or wearable, or other devices to unlock your PC with Windows Hello
4	Information Protection	Credential Guard	Guards your user credentials from being stolen and used on other devices on the network
		BitLocker/Device Encryption	Locks your data on hard drive using encryption
		BitLocker to Go	Locks you data on thumb drives or other storage devices using encryption
		BitLocker Admin & Monitor	Ensures corporate devices are BitLocker encrypted for compliance. Stores recovery keys
5	Breach Detection	Windows Information Protection (was EDP)	Separates business vs. personal data to prevent sharing to non-business documents/apps. Wipes data off devices. Protected documents cannot be opened on unmanaged machine
		Windows Defender Advanced Threat Protection	Global cloud-based threat intelligence service to detect, investigate, and respond to highly targeted advanced attacks on your networks - Know if you are under attack and by whom
		Conditional Access	Only tamper free devices, that are compliant with your security standards can access resources


← Windows Defender Security Center

☰


🏠

Security at a glance


See what's happening with the security and health of your device and take any actions needed.




Virus & threat protection
No action needed.




Account protection
No action needed.




Firewall & network protection
No action needed.




App & browser control
No action needed.



Device security
No action needed.



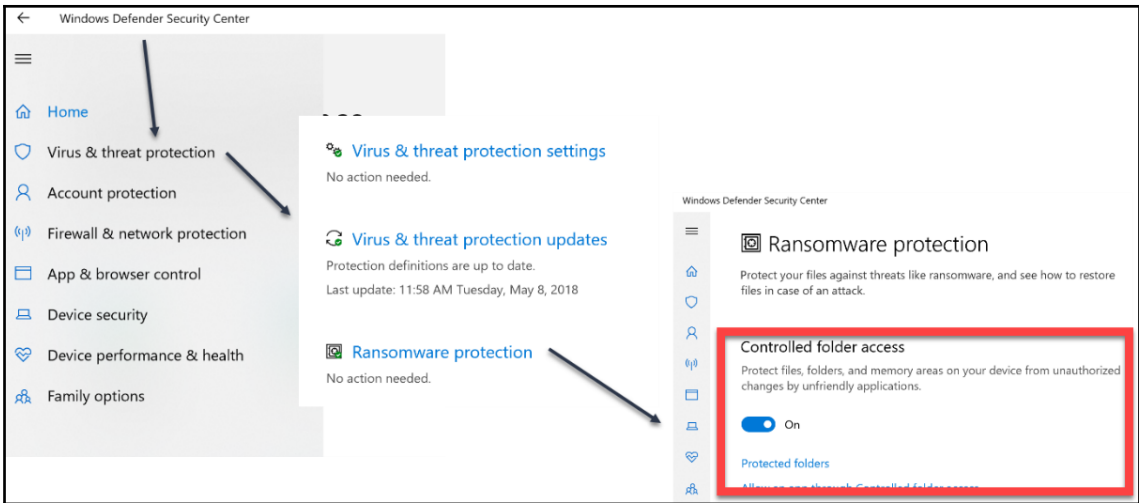
Device performance & health
No action needed.



Family options
Manage how your family uses their devices.

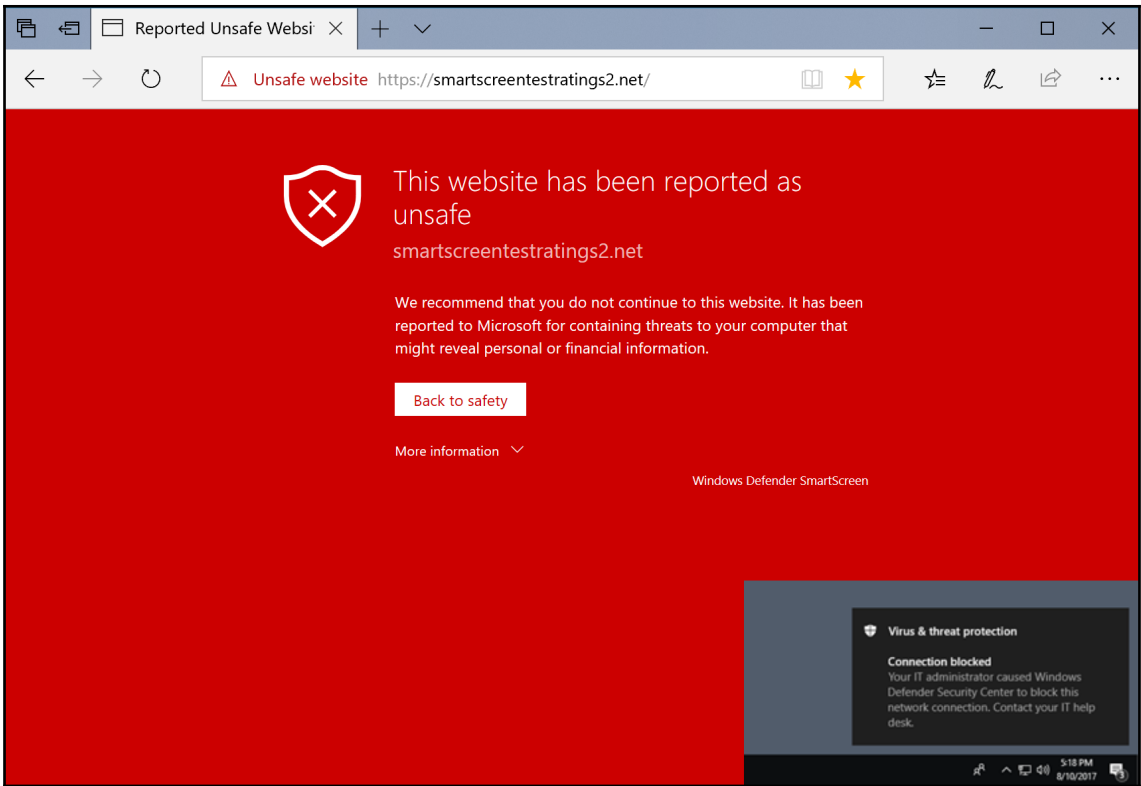
⚙️

	September	October	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 202 samples used	100%	96.3%	99.0%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 9,797 samples used	99.5%	99.9%	98.5%

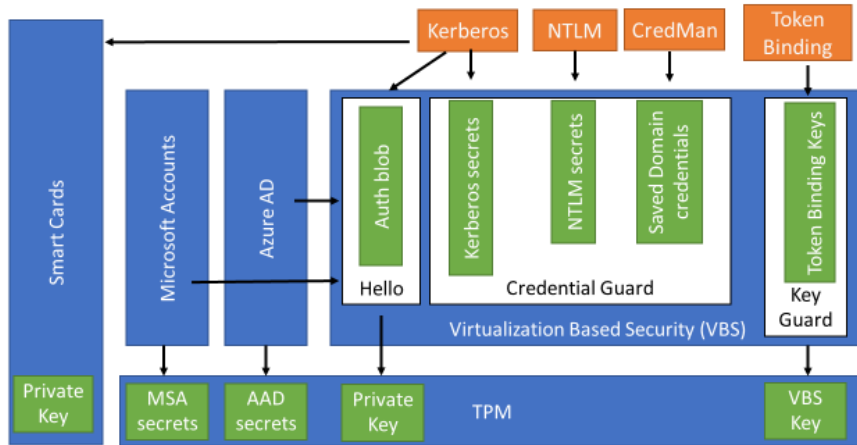


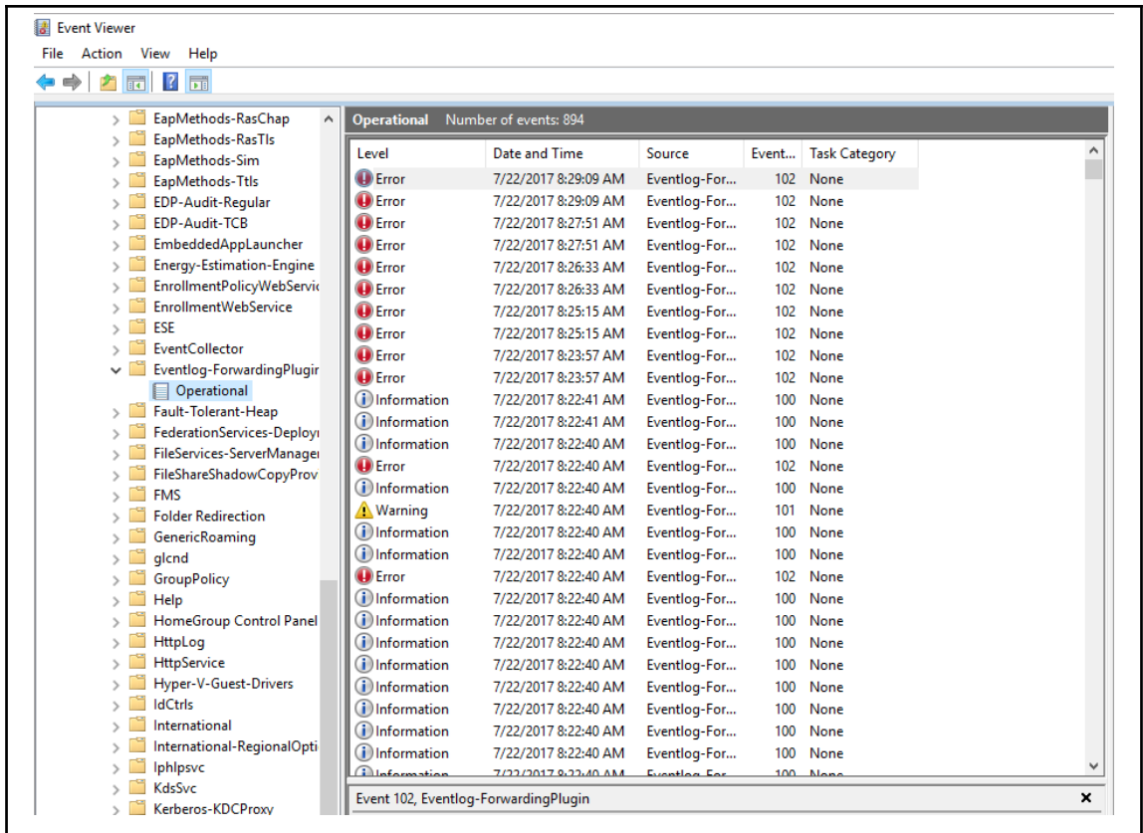
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-MpPreference -EnableNetworkProtection Enabled
PS C:\Windows\system32> _
```



The "Guards"



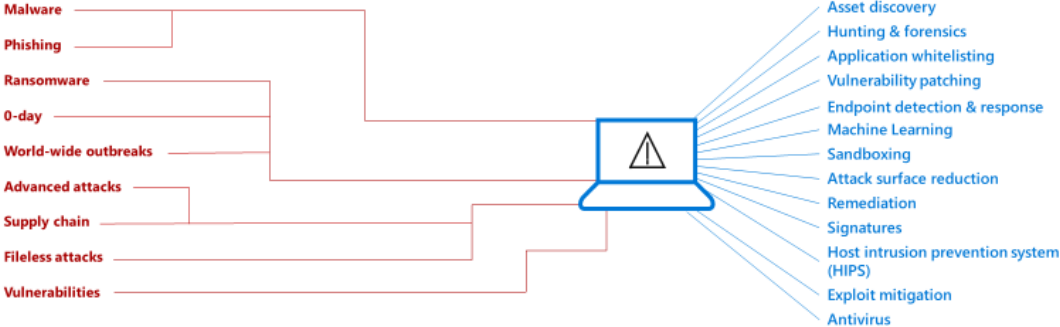


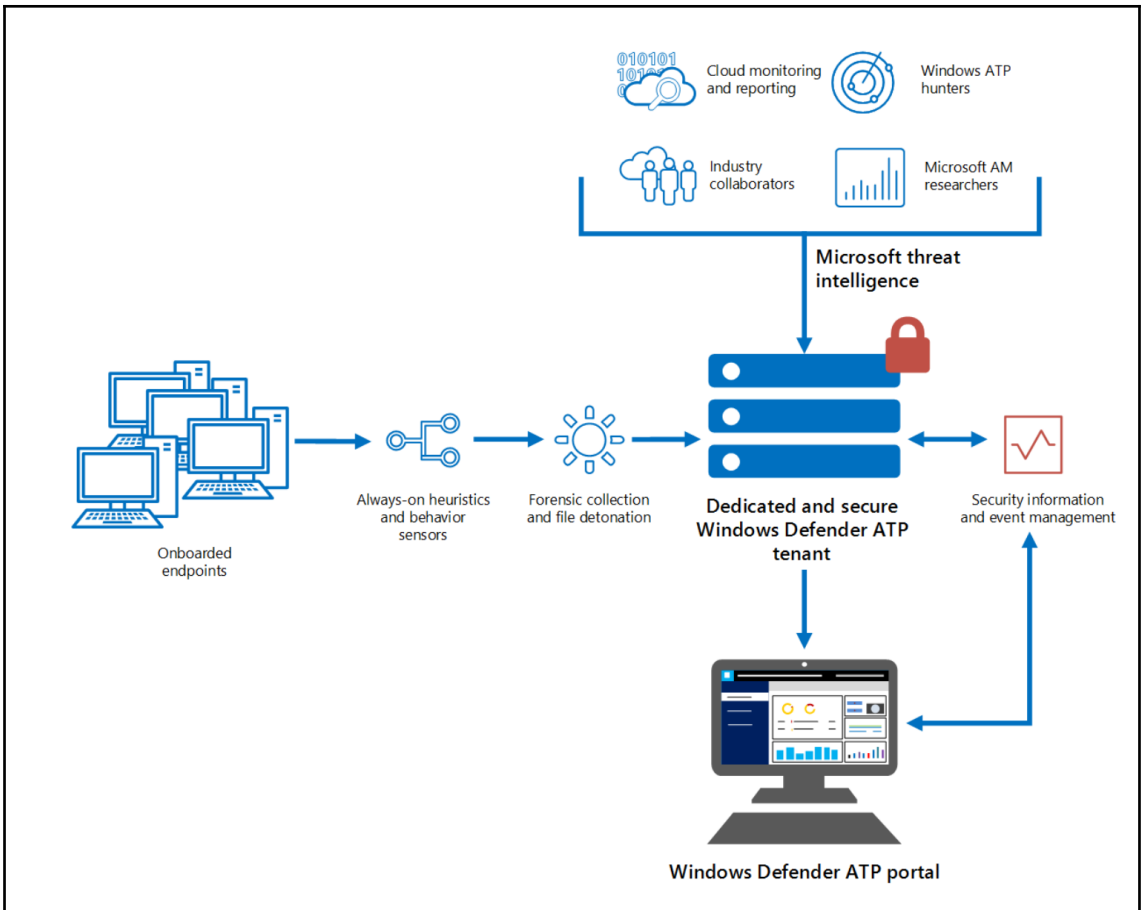
Protecting an endpoint is hard

PERFORMANCE
Hit on your endpoints

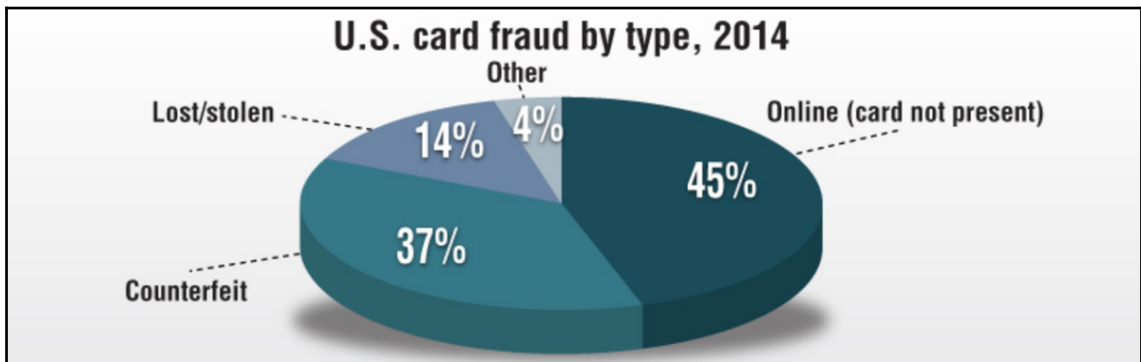
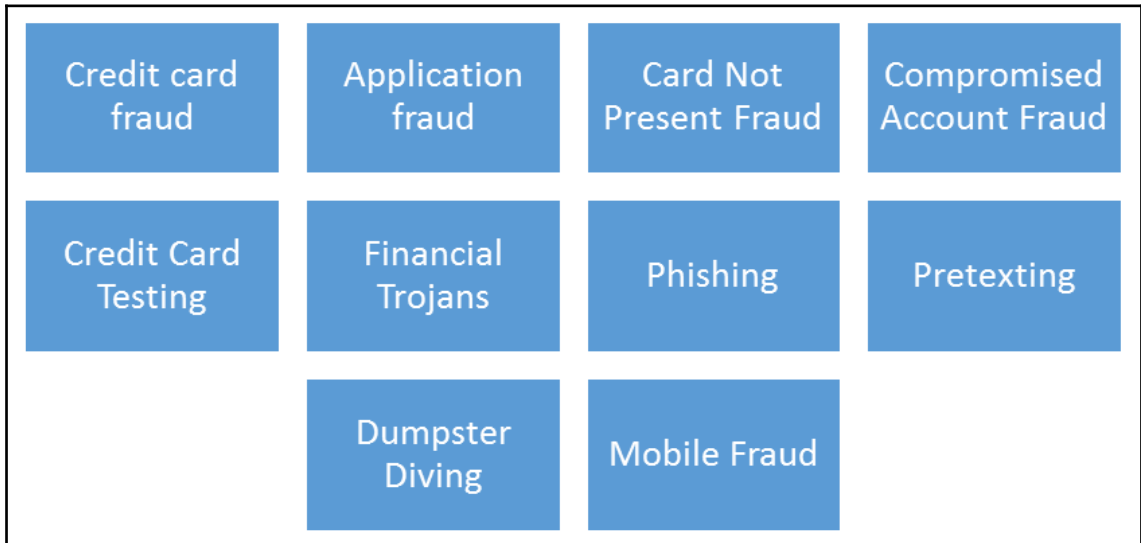
SECURITY TEAM
Time and skills

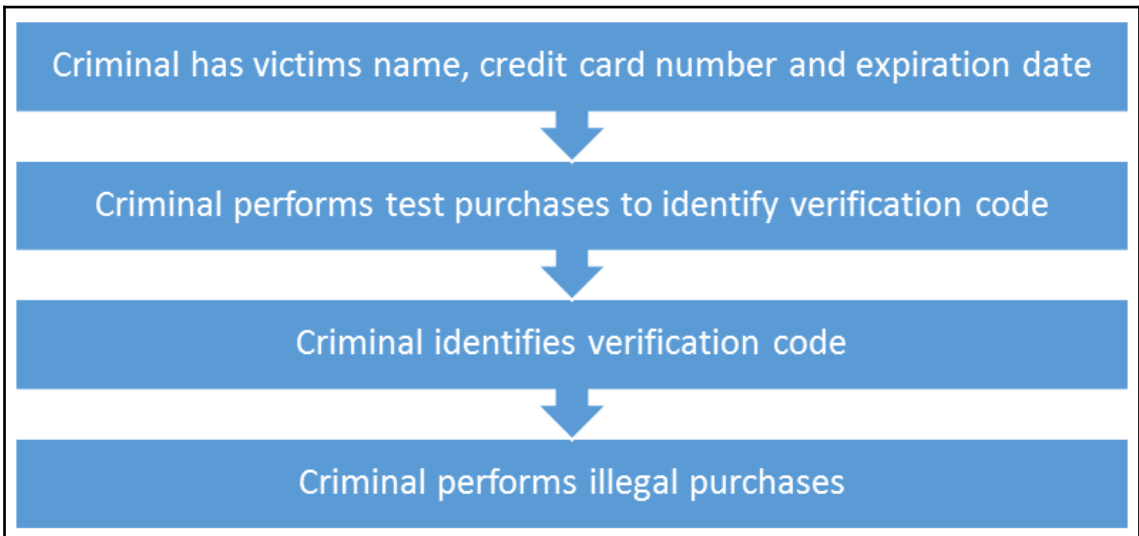
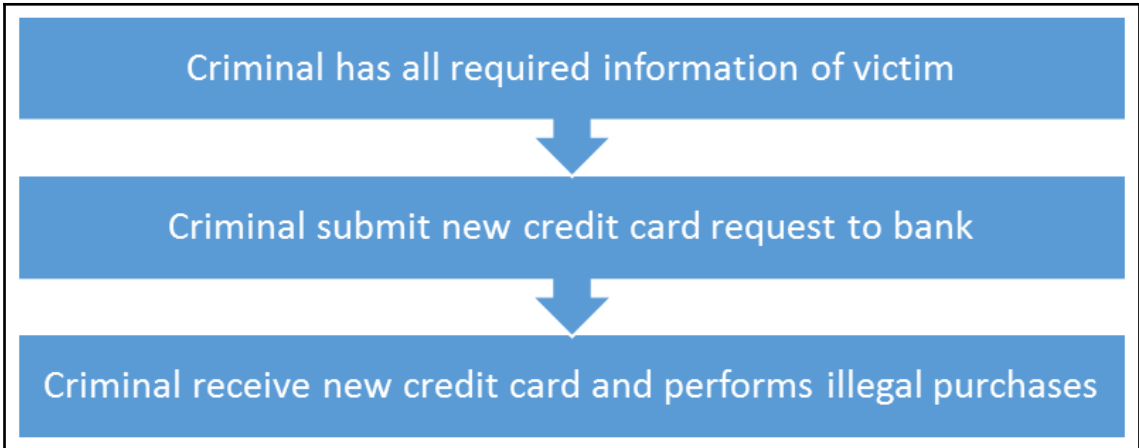
COST
Multiple solutions and on-prem infrastructure

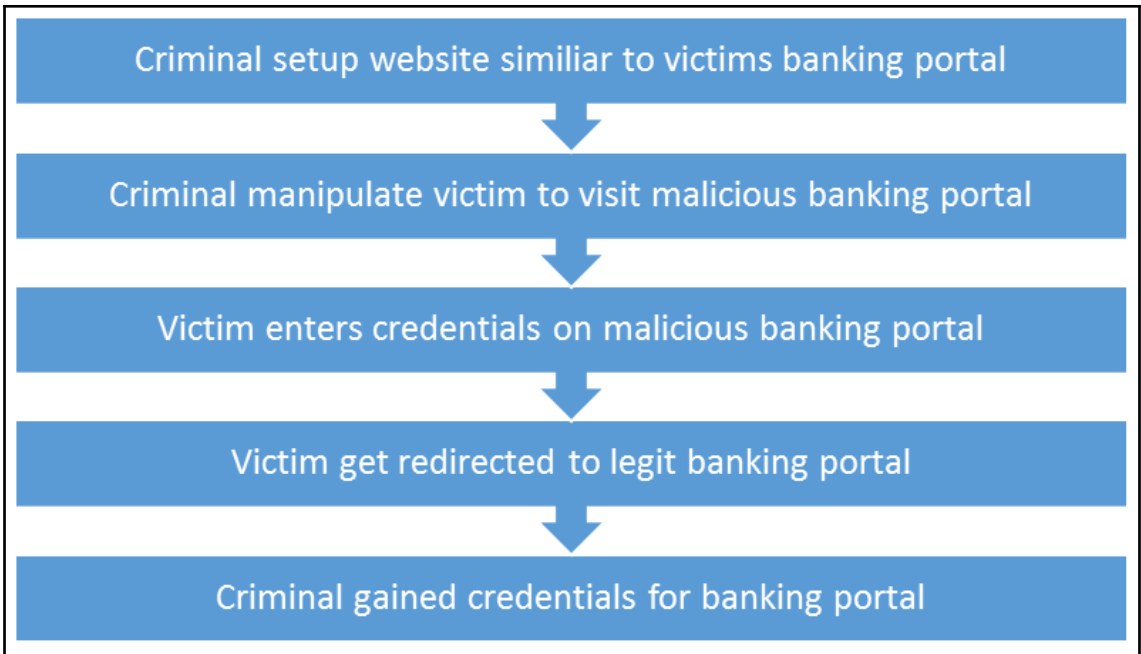


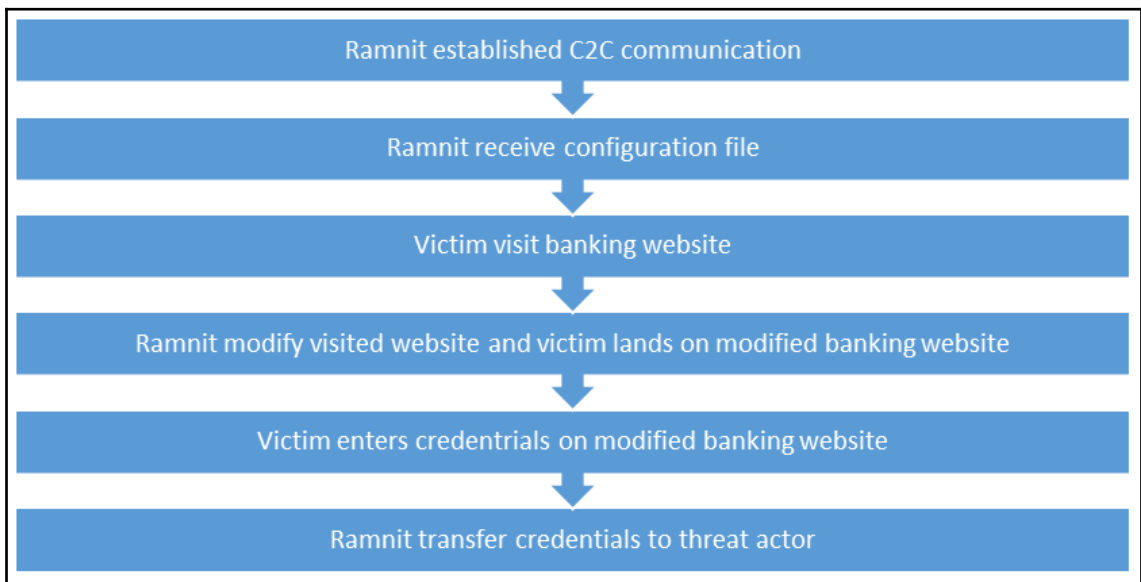
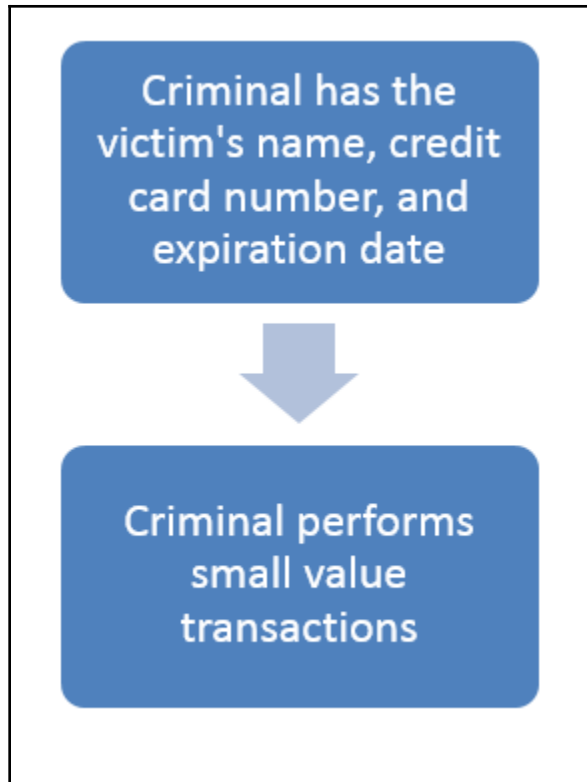


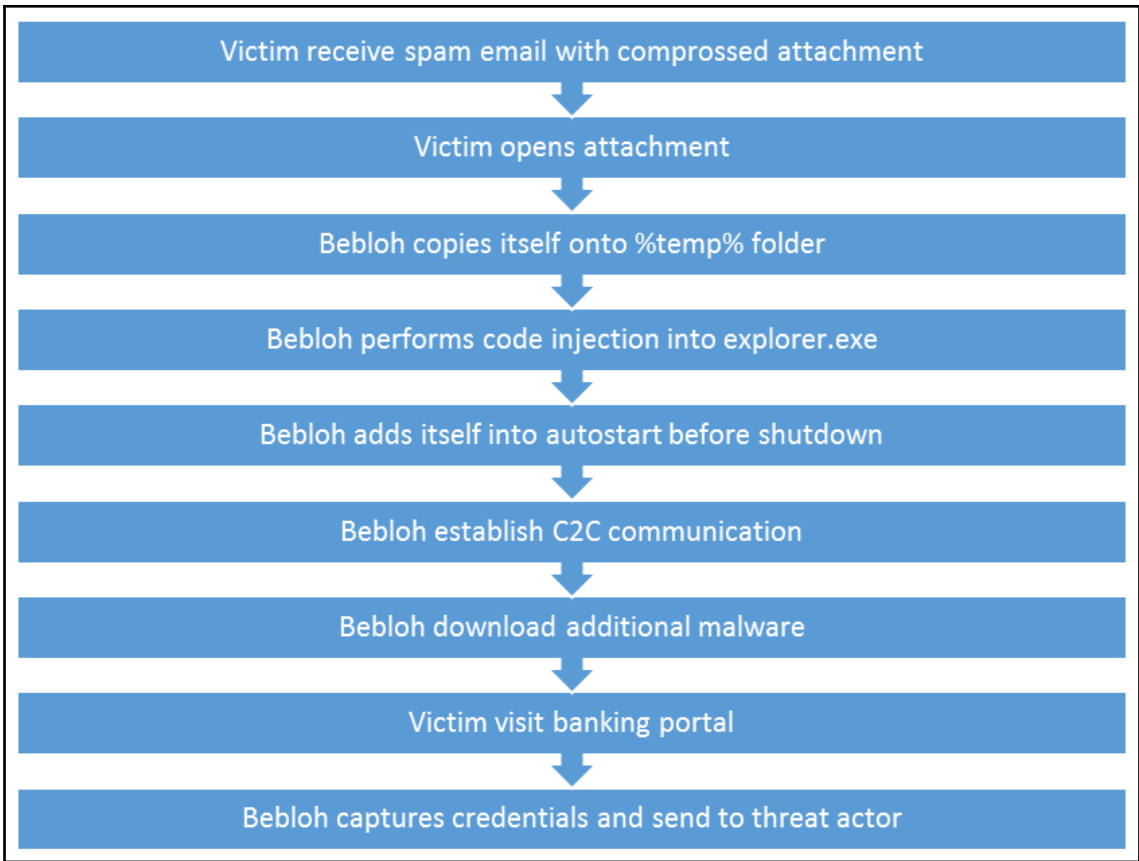
Chapter 4: The Threat Landscape











Dear [REDACTED]

It has come our attention that our online banking portal might have been compromised. Protecting our customers identity and assets is very important to us. We therefore are reaching out to you asking you to reset your credentials immediately.

The government is supporting us during the crisis. They have helped build a secure approach to reset customer records without the need of visiting a local branch. Please therefore use the below URL to perform the data reset. Since keeping your records secure is a top priority for us you will be asked to enter the following information's:

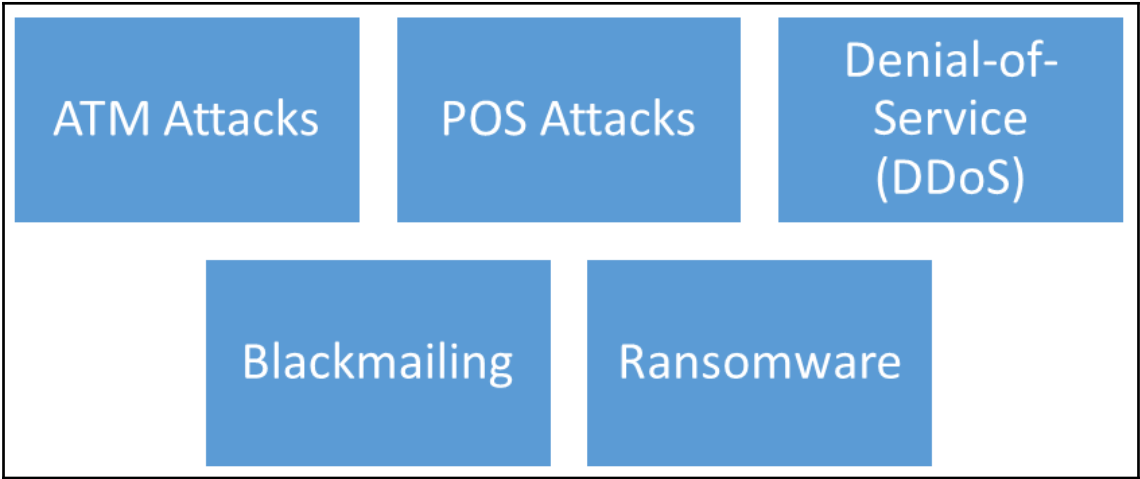
- Government ID number
- First and Last Name as it appears on Government ID
- Home address
- Phone number
- Amount and merchant of last 3 purchases
- Expected balance
- Username
- Password

Your security is important to us. We therefore ask to complete this within he next 5 business days. In case you need assistance please contact us over the secure phone line: [REDACTED].

Secure URL: [REDACTED]

Thank You,

[REDACTED]
Fraud Detection & Investigation
[REDACTED]



Chapter 5: Phishing, Spamming, and Scamming to Steal Data and Money

Subject: Record Update.
From: "Dept. Of Labor" <records@dol.gov>
Date: 1/18/2016 1:57 PM
To: undisclosed-recipients;



This is an urgent request to update your employment record at the U.S Department of Labor.

[Update](#)

Thank you

U.S Dept. of Labor
Frances Perkins Building,
200 Constitution Ave., NW,
Washington, DC 20210



Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: [0p2uYq5RIho](#)

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.



[Get the UPS My Choice app for Facebook](#)



[Download the UPS mobile app](#)



We need your help

Your account has been suspended, as an error was detected in your informations.
The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

[Update your information](#)

You are currently made disabled of :



Adding a payment method
Adding a billing address

Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright © 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.



We couldn't verify your recent transaction

Dear Client,

We just wanted to confirm that you've changed your password. If you didn't make this change, please check information in here. It's important that you let us know because it helps us prevent unauthorised persons from accessing the [PayPal](#) network and your account information.



We've noticed some changes to your unusual selling activities and will need some more information about your recent sales.

[Verify Information Now](#)


Thank you for your understanding and cooperation. If you need further assistance, please click [Contact](#) at the bottom of any [PayPal](#) page.

Sincerely,
[PayPal](#)

irs Identity Verification Service — Inbox

irs gov  Today at 5:02 AM 

To: @kaspersky.com
irs Identity Verification Service



Dear Tax Payer,

This is an automated email, please do not reply.

We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow [this link](#) to verify your information.

Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.

Scott

To:
Reply-To:
Urgent

Hello Stuart,

Have you got a minute? I am currently tied up in a meeting. We need to faciliate a wire transfer to Indonesia for payment of an invoice Peter needs us to pay for today.

Let me know so I can pass across further information to you. Thanks.

Regards,
Scott

Sent from my iPhone

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

From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice **04/16000331799** (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne, Albuquerque, New Mexico, 87110
T: [866-905-9901](tel:866-905-9901) | Copyright © 2016

Urgent Request

Inbox x



Alanna

7:50 AM (1 hour ago) ☆

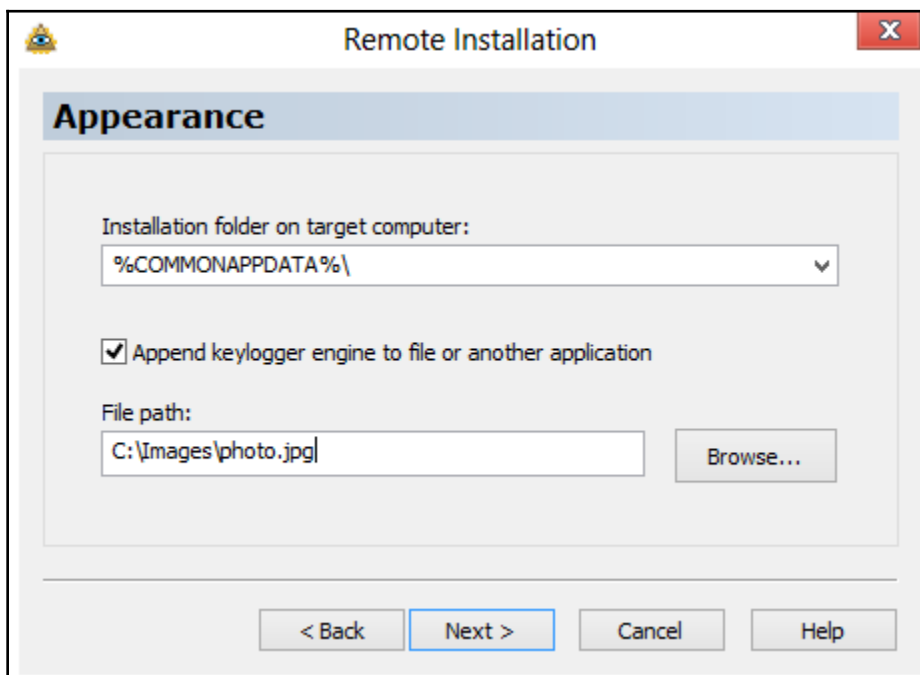
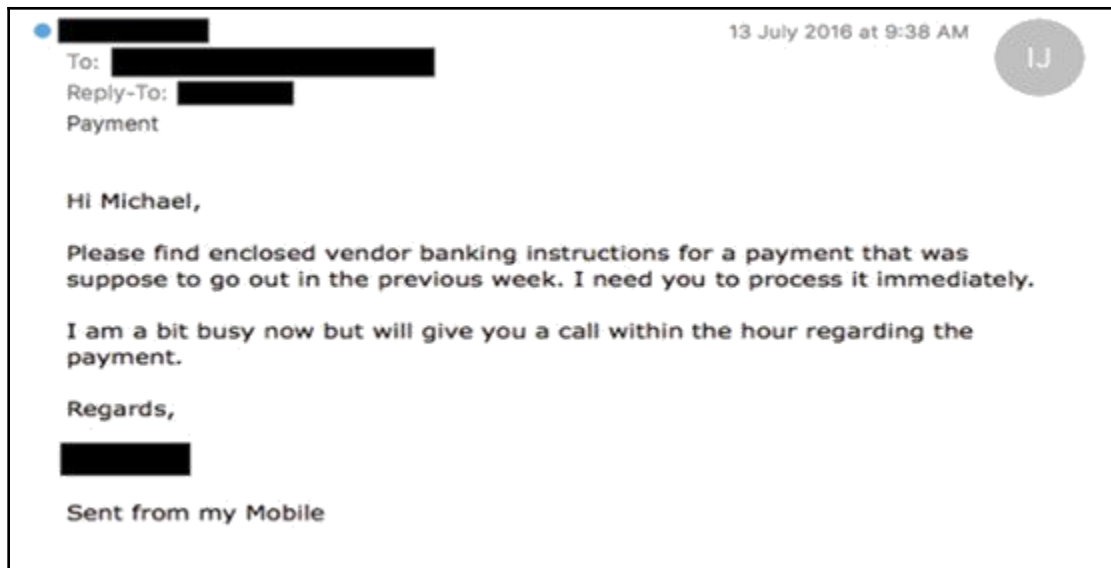


to me ▾

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.







Your phone is locked for viewing child pornography.

All your files are encrypted. Your phone is locked until payment of the fine of \$ 100.

You have 48 hours to pay the fine in case of refusal to pay all of your files will be handed over to the police.

You have 48 hours to pay the fine in case of refusal to pay all of your files will be handed over to the police.

Is your personal account, Bitcoin

1G5FiCaaLKCfEk7seMyYFpX99PXgrUqk85

for payment.

After paying the fine, your phone automatically unlocks.

Buy bitcoin.

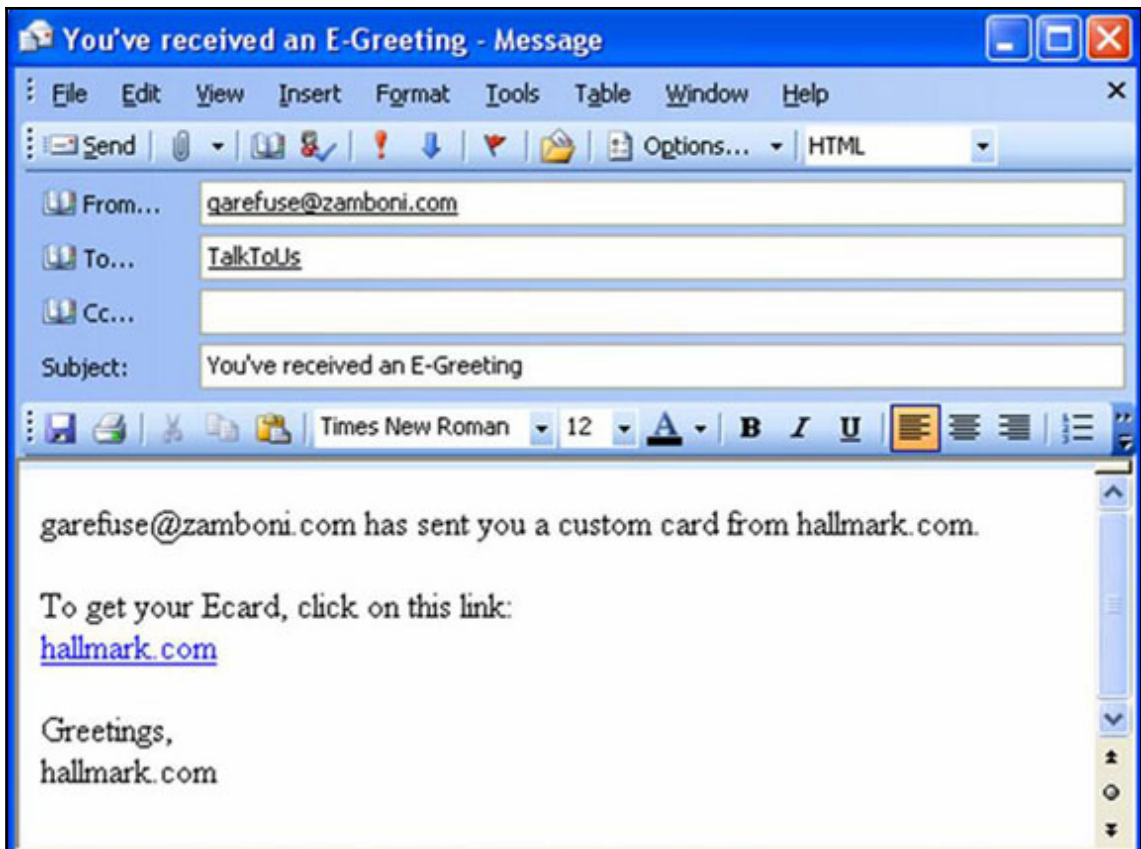
<https://www.coinbase.com/>

<https://btc-e.com/>

Help :

<https://www.youtube.com/watch?v=Apk4803Eti0>

<https://www.youtube.com/watch?v=C3Gx1wEcrSU>



Hello,

I'm reaching out because I'm experiencing a few minor errors while browsing **your site**. As a Digital Marketing manager, I know how frustrating things like this can be, so I wanted to reach out to see if I can help.

Mainly, I'm experiencing issues loading your site on my mobile device. This is a fairly common issue, especially since this April, when Google started heavily rewarding sites with a speedy mobile user experience, and punishing those with bulky, lagging designs that aren't suited to small, vertical screens. With over 50 percent of people browsing the internet with their phones, that's a fair share of the market to consider.

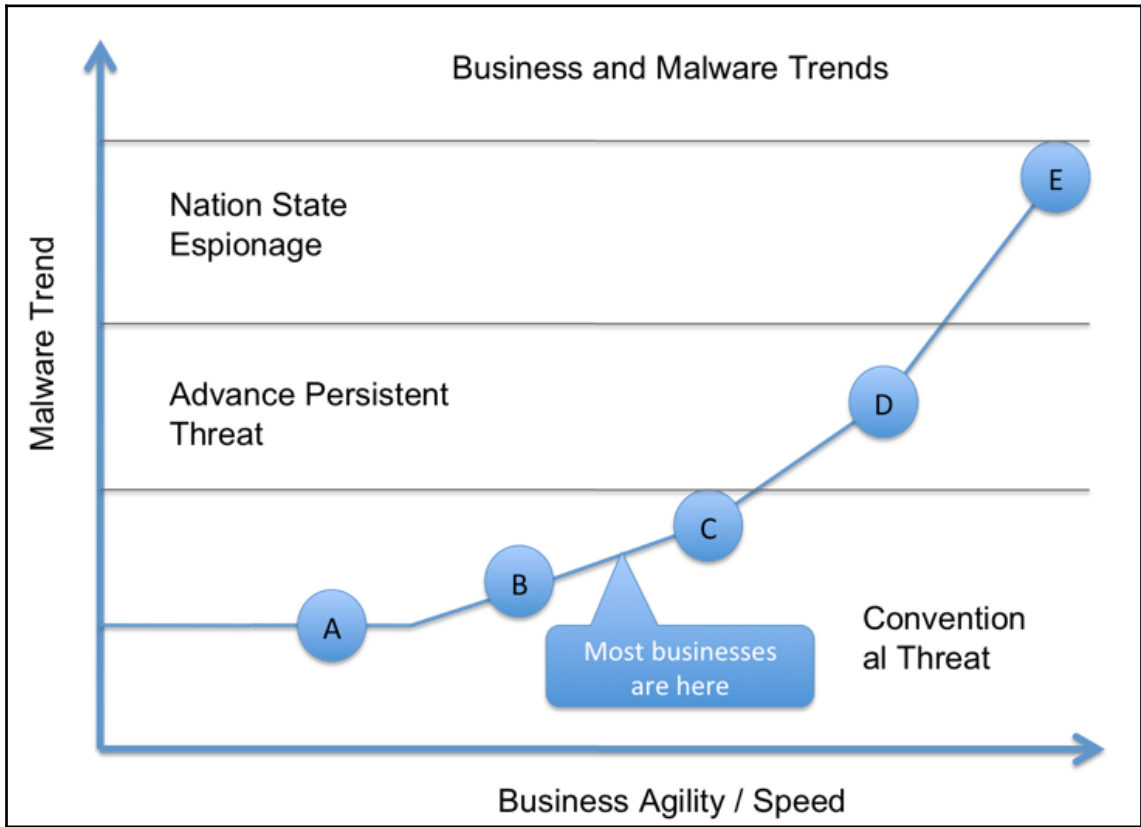
Based locally in Libertyville, IL, my team has over 23 years of experience developing elastic designs that can be viewed on any device. We're also Google Partners and have received many accolades throughout the years. Our first client was a little startup company called "E-bay". We would be happy to jump on a call with you to review these problems and more to help your brand get the best online visibility possible.

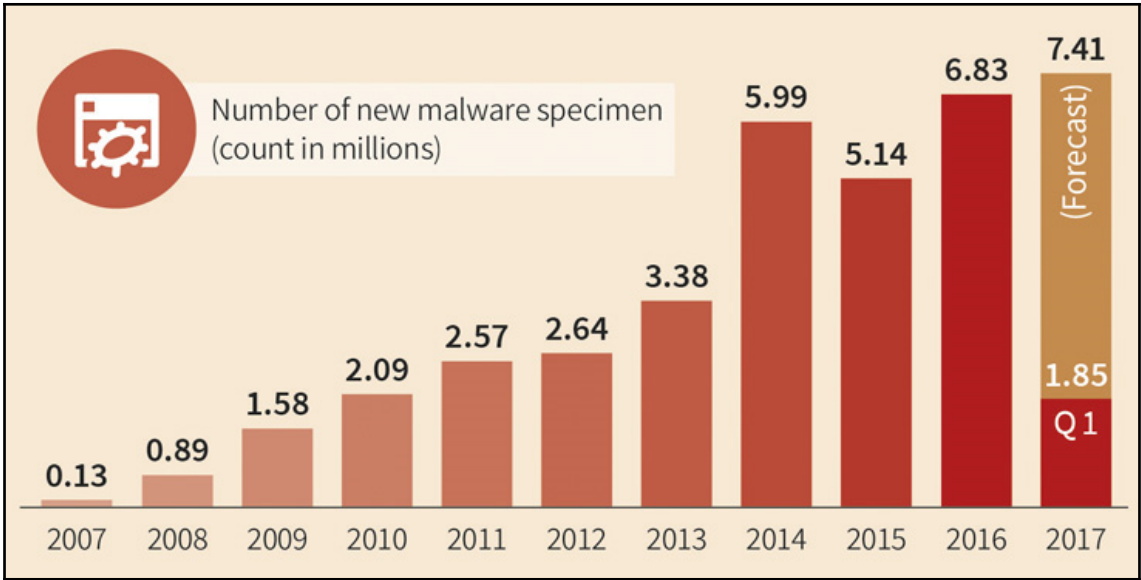
What day this week works best for a call?

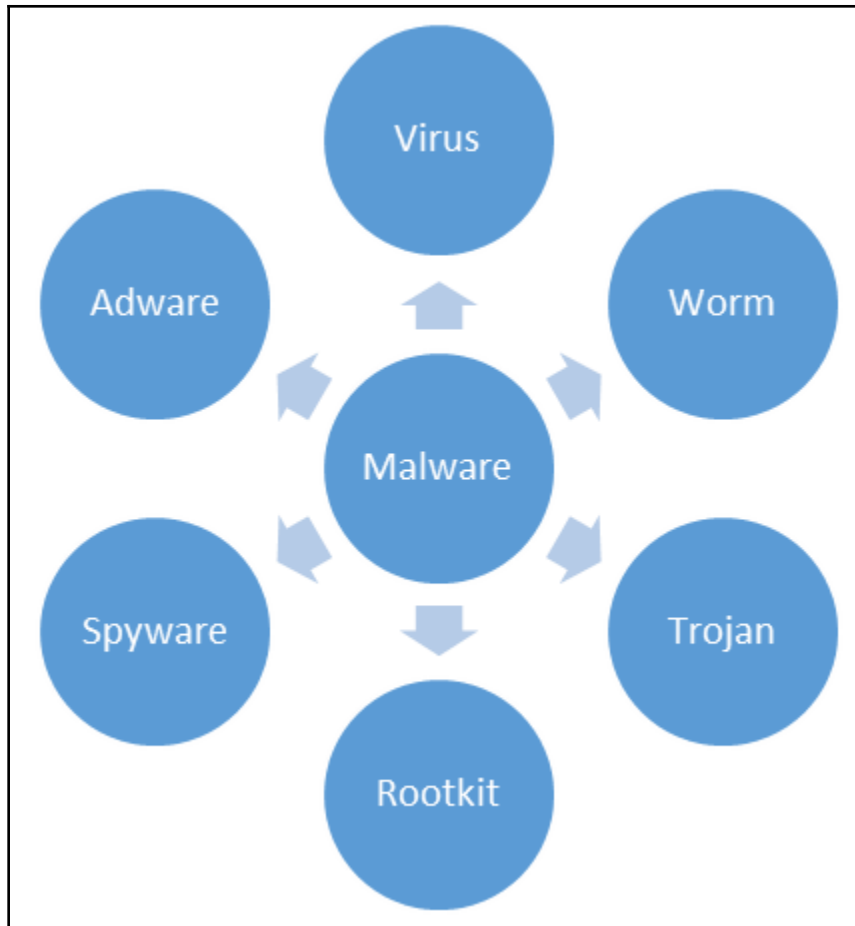
Regards,

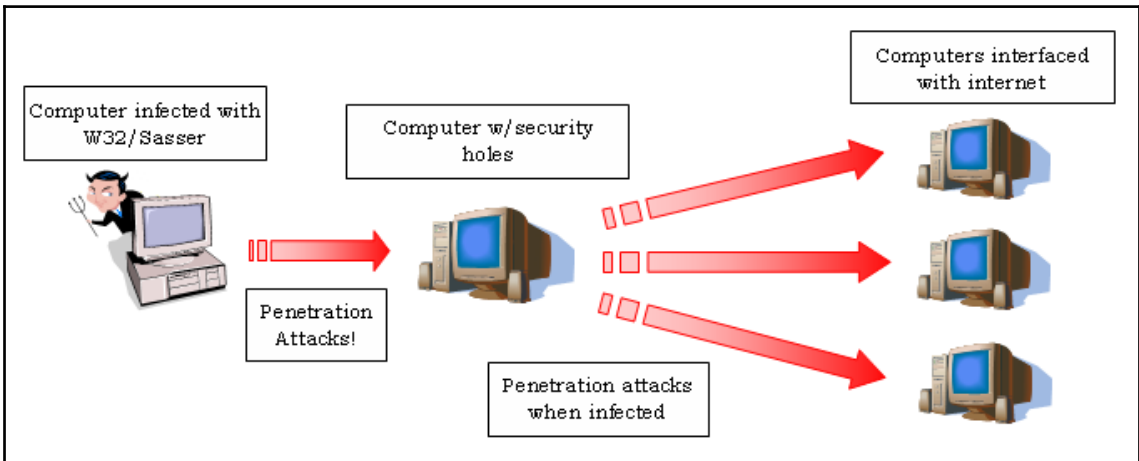
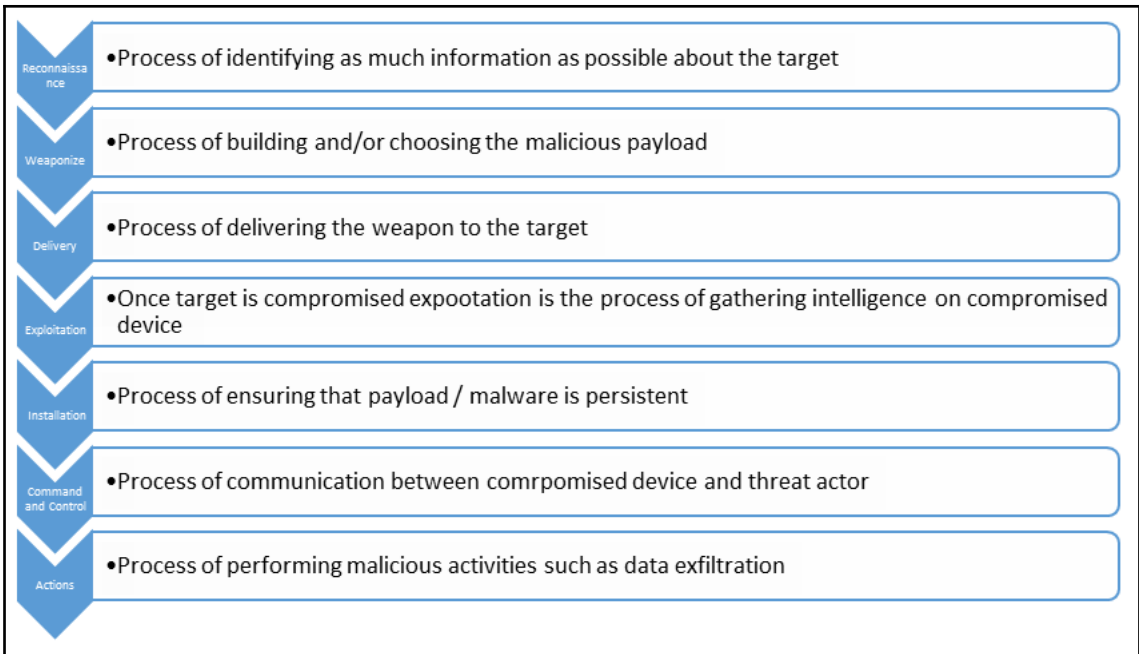
Steve K.

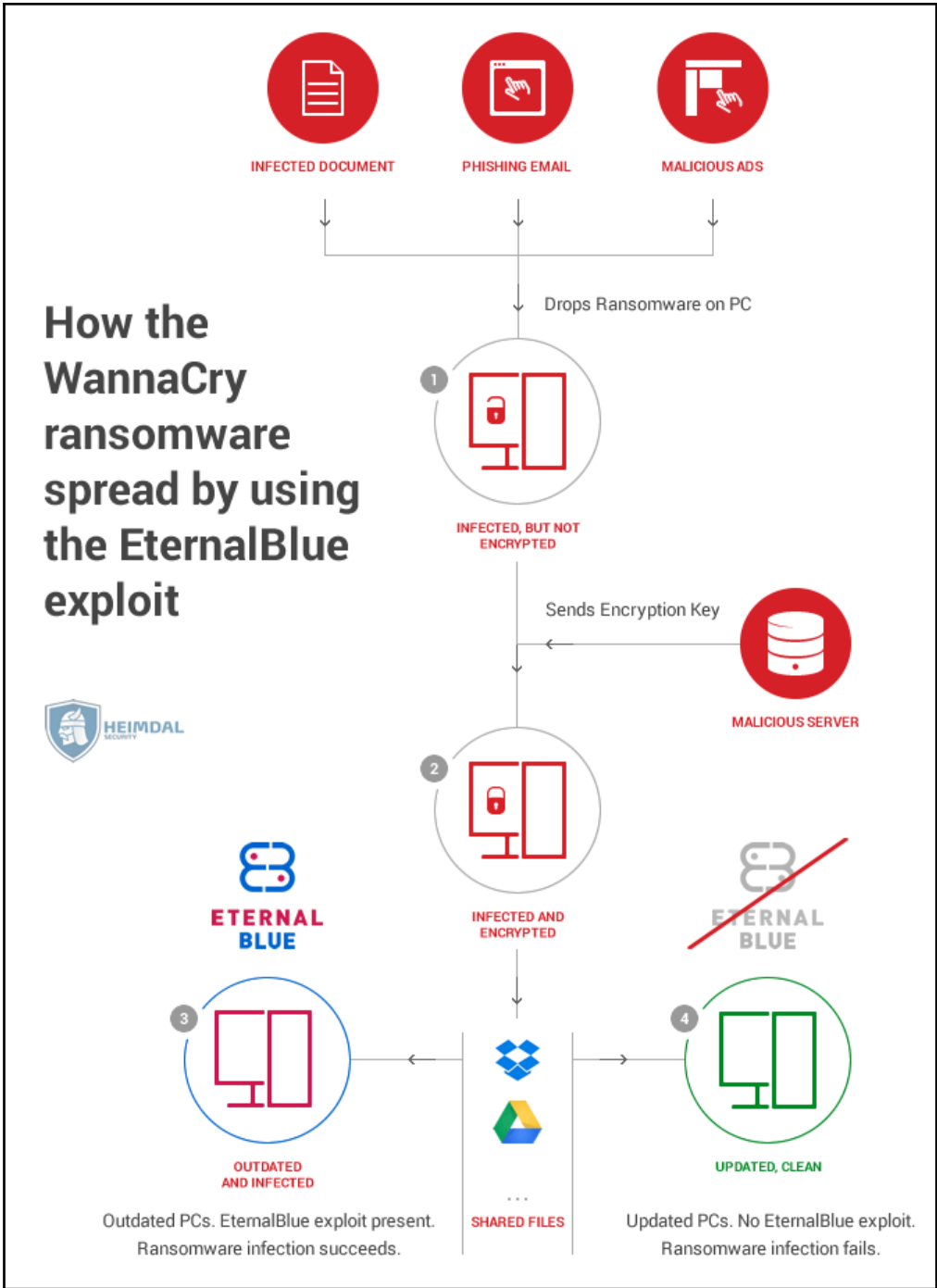
Chapter 6: The Malware Plague

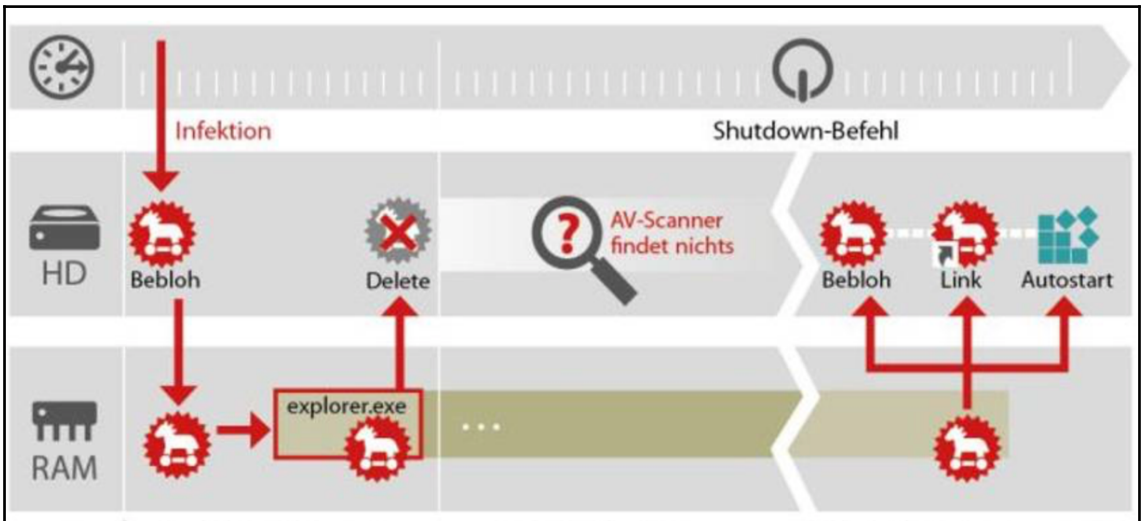
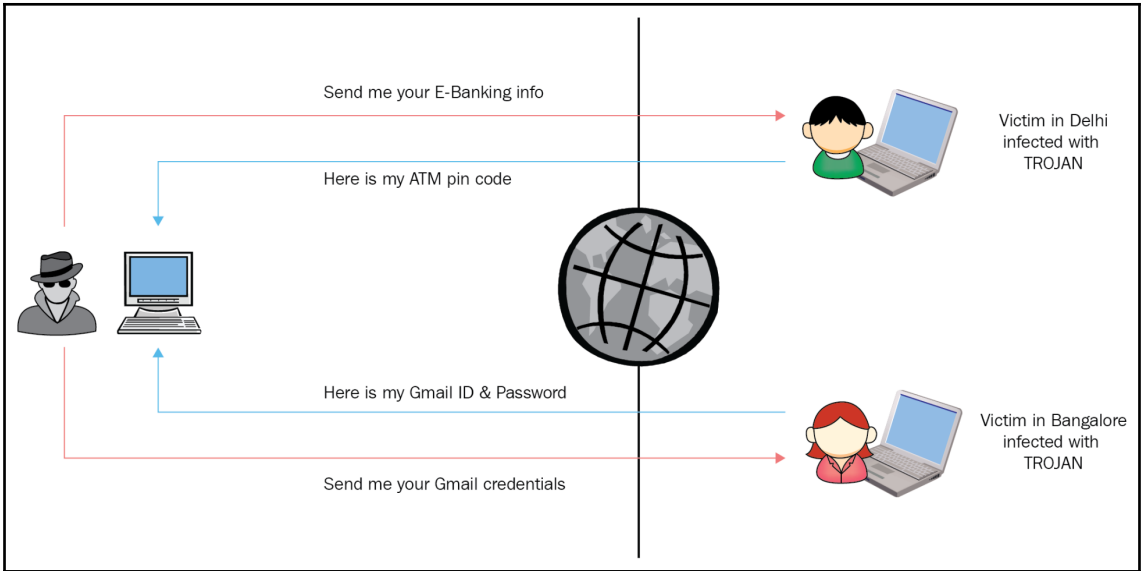


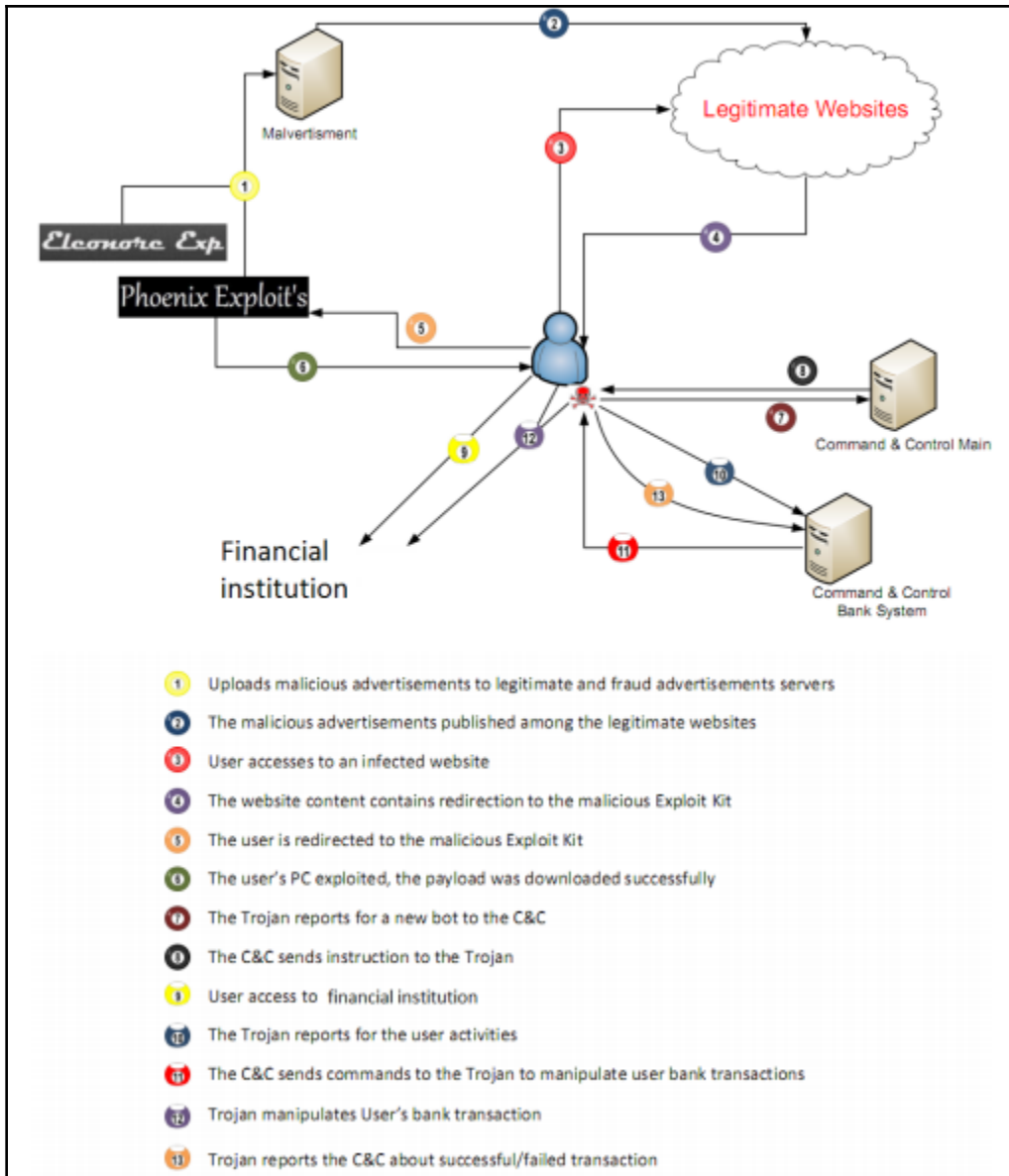


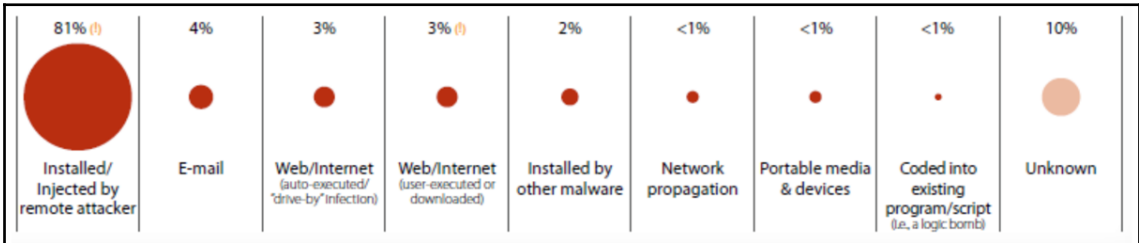
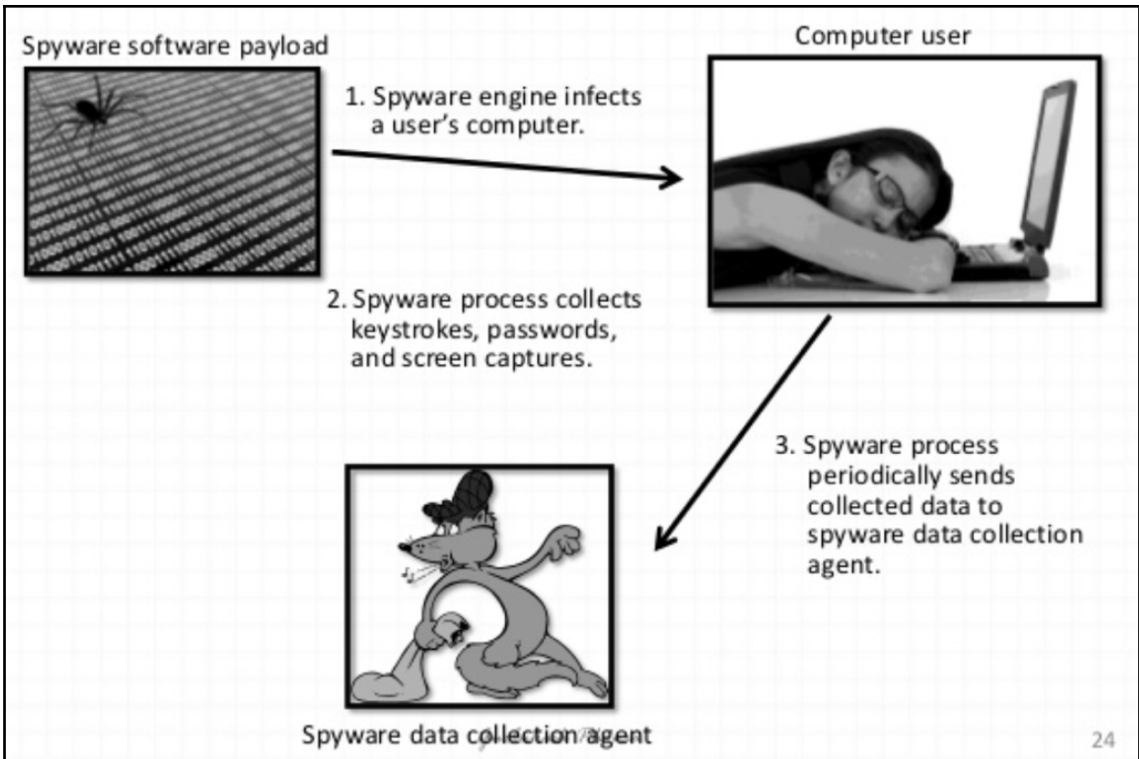




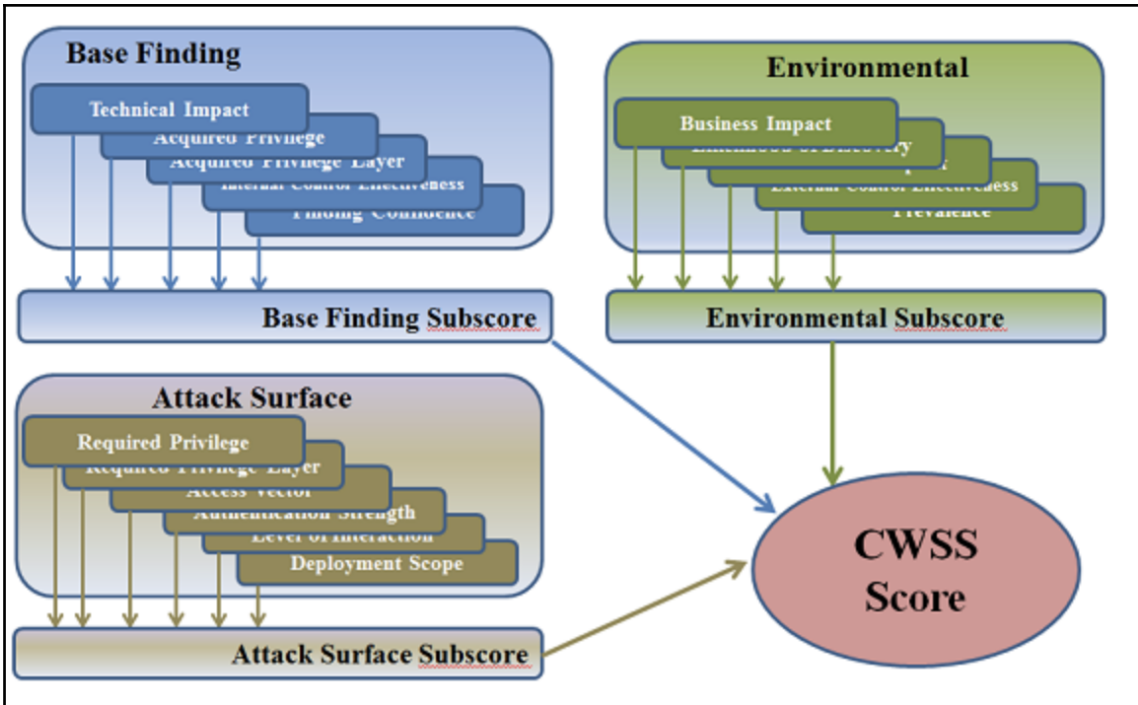
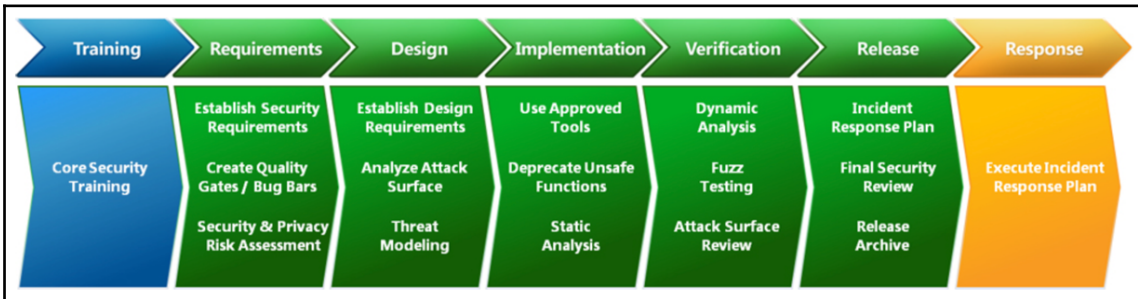








Chapter 7: Vulnerabilities and Exploits



TheRealDeal Market Home Items Inbox Account FAQ Support Forums Logout

My Purchases

Categories

- 0-Day exploits (4)
 - o FUD Exploits (4)
 - o 1Day Private Exploits (2)
- Information (8)
 - o Money (36)
 - o Source Code (4)
 - o Spam (3)
 - o Accounts (7)
 - o Cards

MS15-034 Microsoft IIS Remote Code Execution

Reversed from http.sys exploit includes ROP gadgets for Server 2008 and Server 2012 only. I will also send you the research and reversing info from patch to diff to vuln ...

comes with shellcode for a reverse cmd shell but this can obviously be changed.

Offering this for a limited amount of time only as I might already have client in real life.

Pay escrow to prove you have the funds, then test the exploit and see for yourself, as usual.

By [bestbuy](#) (0)

Added: 1 day ago

☆☆☆☆☆

BTC 518.30255912

[Message](#)

[Purchase](#)

0 reviews

Available Locations

Worldwide

Cost

BTC 0.00000000

Buffer Overflow	Integer Overflow	Memory Corruption	Format String Attacks
Race Condition	Cross Site Scripting	One Click Attack	SQL Injections

0022FEE0	00ESP50	Pij''.	dest = 0022FF50
0022FEE4	00403000	...	src = teste.00403000
0022FEE8	00000001	..	ln = 1
0022FEEC	004012B5	µl@.	RETURN to teste.004012B5 from teste.004017B0
0022FEF0	0022FED0	0p''.	
0022FEF4	00000002	...-	
0022FEF8	0022FFC4	ñj''.	
0022FEFC	76478CD5	0mGv	msvcrt.76478CD5
0022FF00	CF1227D3	0'jY	
0022FF04	FFFFFFFFE	bijij	
0022FF08	764598DA	UFEU	RETURN to msvcrt.764598DA from msvcrt.7645987B
0022FF0C	00000010	+...-	
0022FF10	002E0F55	Xo..	
0022FF14	002E0FA8	''p..	
0022FF18	0022FF38	8ij''.	
0022FF1C	00000030	0...-	
0022FF20	4F4C4548	HELO	
0022FF24	4F4C4548	HELO	
0022FF28	4F4C4548	HELO	
0022FF2C	4F4C4548	HELO	
0022FF30	4F4C4548	HELO	
0022FF34	4F4C4548	HELO	
0022FF38	4F4C4548	HELO	
0022FF3C	4F4C4548	HELO	
0022FF40	4F4C4548	HELO	
0022FF44	4F4C4548	HELO	
0022FF48	4F4C4548	HELO	EBP
0022FF4C	4F4C4548	HELO	

STACK

Buffer Overflow

```

CS50 IDE File Edit Find View Go v110 Share
OPEN FILES
  intro.c - intro.c
  initals1.c - initals1.c
  p0.c - powersp0.c
  initals0.c - initals0.c
  i01.c - i01.c
  i00.c - i00.c
  o1.c - o1.c
  i01.c - i01.c
  workspace/
  pointers/
    p0
    p0.c
  rakbr
  adder
  adder.c
  alphabet
  alphabet.c
  alphacase
  alphacase.c
  arg
  arg.c
  arg0.c
  arg1
  arg1.c
  int0

1 #include <stdio.h>
2 #include <cs50.h>
3
4 int main()
5 {
6     int b = 2;
7
8     while(true){
9         b = b * 2;
10        if(b<0)
11        }
12
13    return 0;
14 }

workspace/ x
int01.c:0:18: error: format specifies type 'int' but the argument has type 'long'
[-Werror,-Wformat]
printf("%i", 2147483648+1);
      ~~~~^
      %li

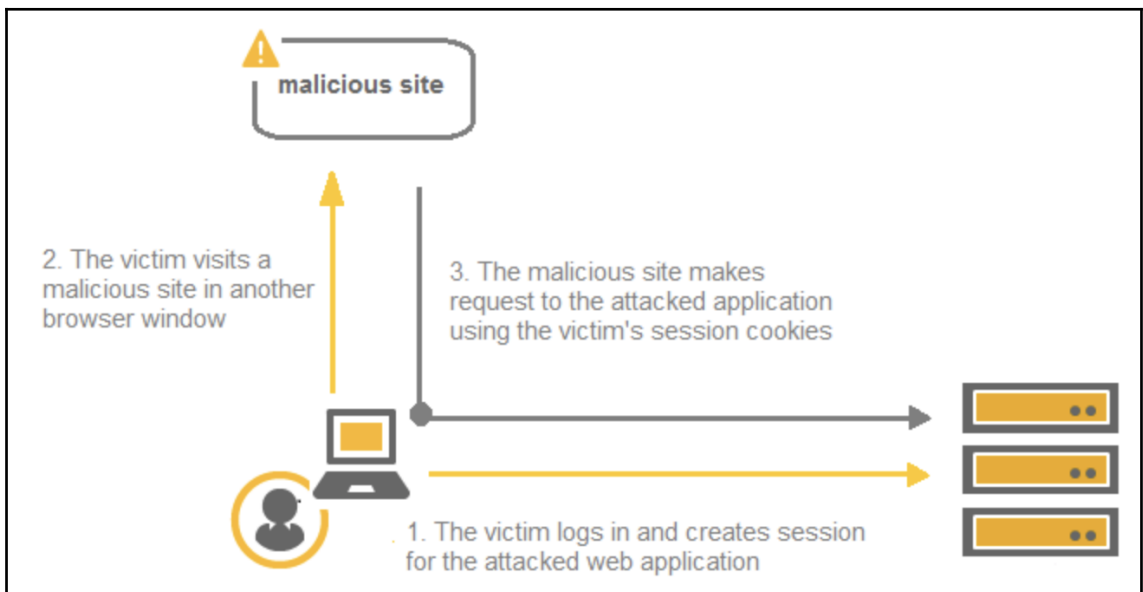
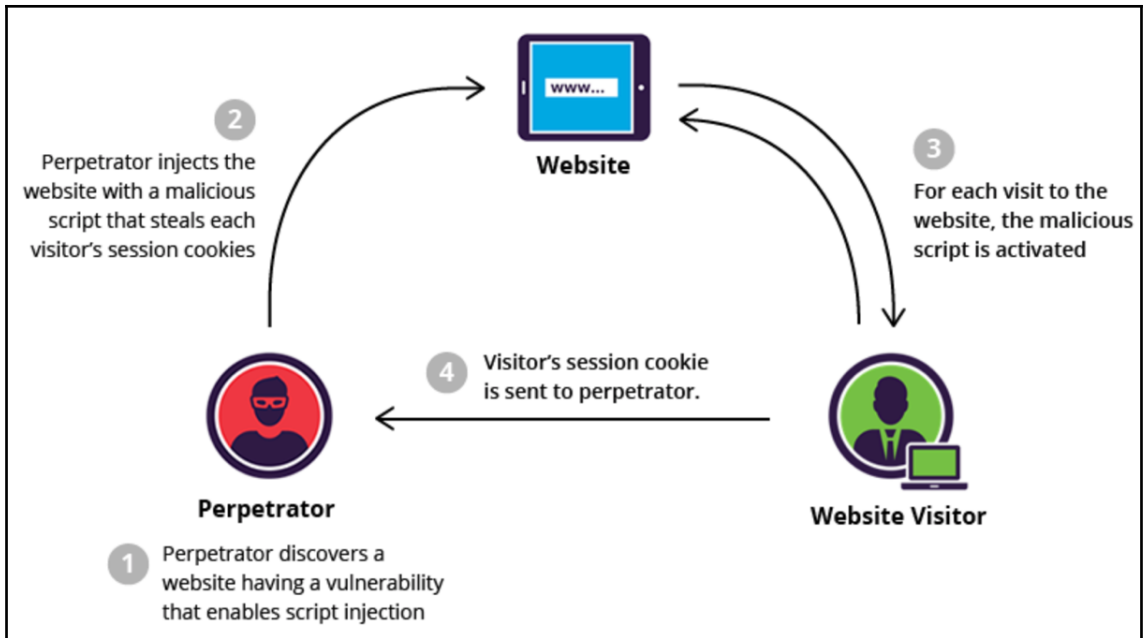
1 error generated.
make: *** [int01] Error 1
~/workspace/ $

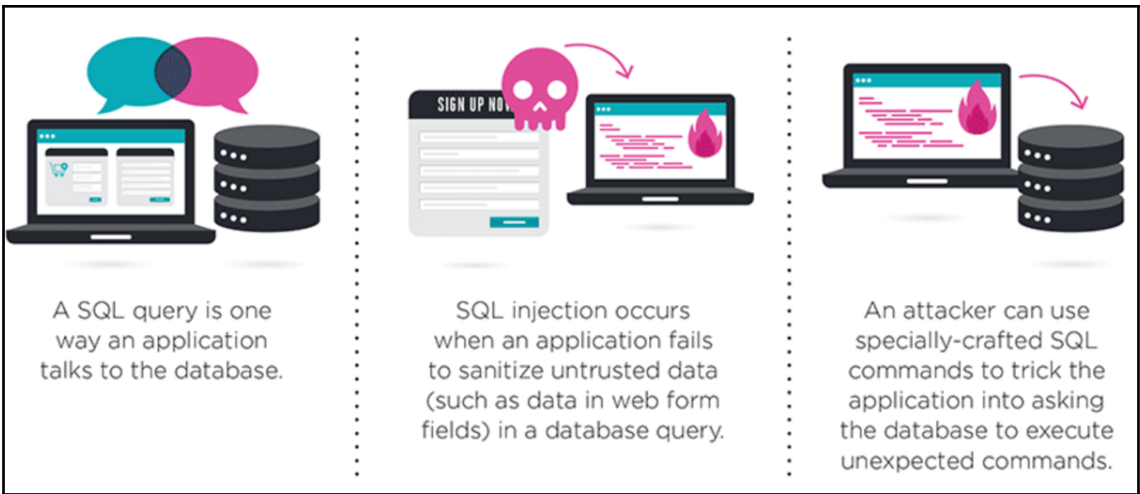
```

integer overflow

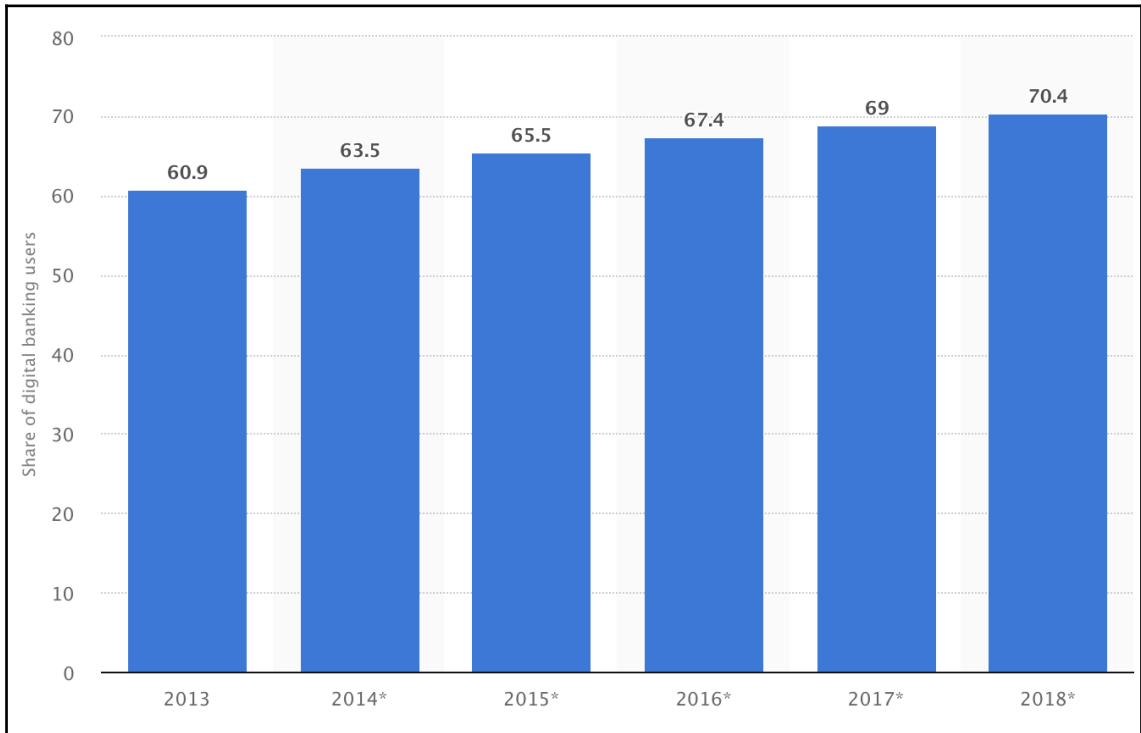
```
Terminal
File Edit View Search Terminal Help
ilroy@dallas ~/vulnerable $ vi format.c
ilroy@dallas ~/vulnerable $ vi formatstr.c
ilroy@dallas ~/vulnerable $ ./formatstr %x
1064b2e
ilroy@dallas ~/vulnerable $ cat formatstr.c
include <stdio.h>
include <string.h>
include <stdlib.h>

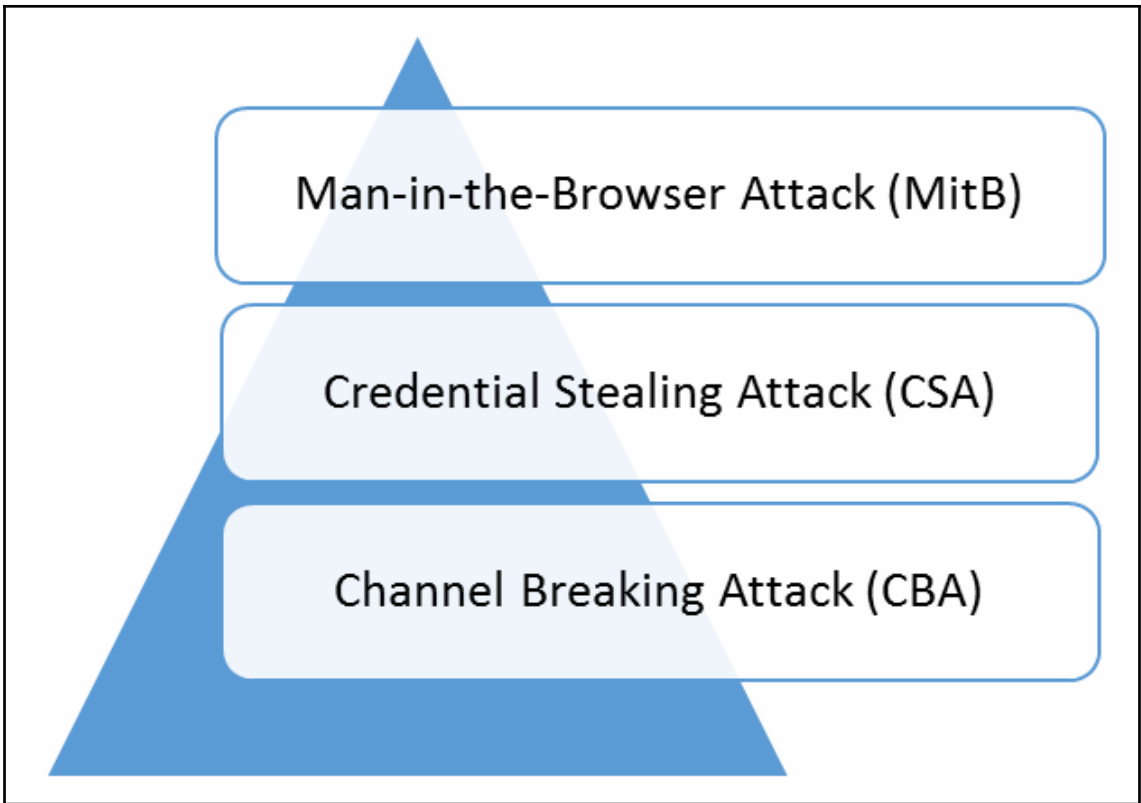
int main(int argc, char *argv[])
{
    char *x=(char *)malloc(40);
    strncpy(x,argv[1],40);
    printf(x);
    printf("\n");
    return(0);
}
ilroy@dallas ~/vulnerable $
```



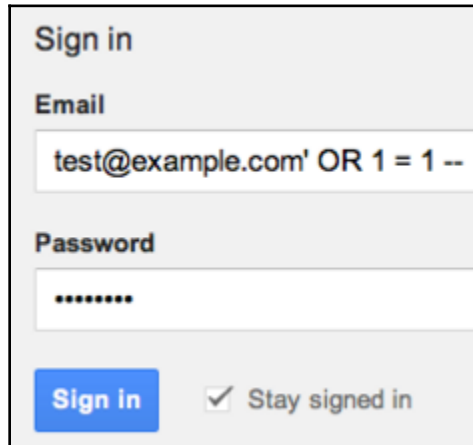


Chapter 8: Attacking Online Banking Systems





Chapter 9: Vulnerable Networks and Services - a Gateway for Intrusion



Sign in

Email

test@example.com' OR 1 = 1 --

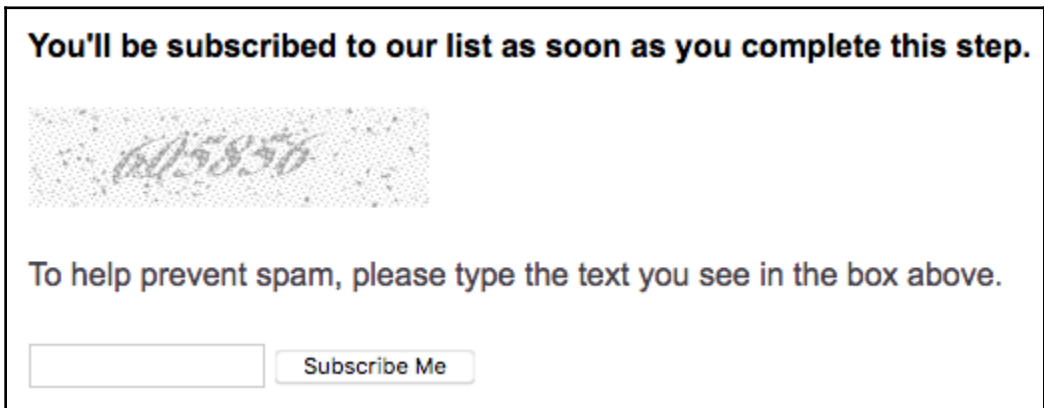
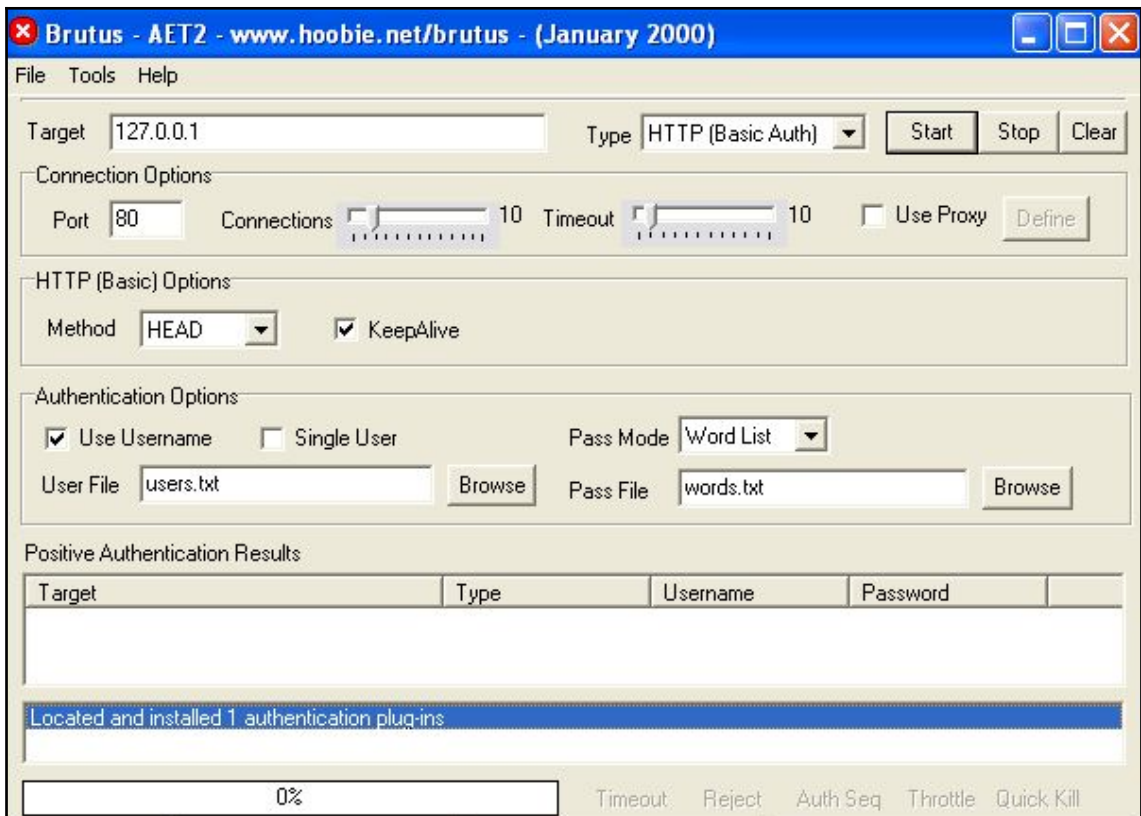
Password

Sign in Stay signed in

MEDUSA

Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

```
Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]     : File containing target hostnames or IP addresses
-u [TEXT]     : Username to test
-U [FILE]     : File containing usernames to test
-p [TEXT]     : Password to test
-P [FILE]     : File containing passwords to test
-C [FILE]     : File containing combo entries. See README for more information.
-O [FILE]     : File to append log information to
-e [n/s/ns]   : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]     : Name of the module to execute (without the .mod extension)
-m [TEXT]     : Parameter to pass to the module. This can be passed multiple times with a
                different parameter each time and they will all be sent to the module (i.e.
                -m Param1 -m Param2, etc.)
-d            : Dump all known modules
-n [NUM]     : Use for non-default TCP port number
-s           : Enable SSL
-g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
-r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
-R [NUM]     : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
-t [NUM]     : Total number of logins to be tested concurrently
-T [NUM]     : Total number of hosts to be tested concurrently
-L           : Parallelize logins using one username per thread. The default is to process
```



```
MacBook-Pro-de-akita:scripts ak1t4$ dcipher 09573e52f752f3f5e6250b62aa34b8a8c08a4d22
✓ 605856
MacBook-Pro-de-akita:scripts ak1t4$
```

```

root@kali:~# aircrack-ng -a2 -b [REDACTED] w /root/Desktop/Everything2016.txt /root/Desktop/-02.cap
Opening /root/Desktop/-02.cap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[08:30:03] 76108192/310022794 keys tested (2546.07 k/s)

Time left: 1 day, 1 hour, 31 minutes, 15 seconds      24.55%

KEY FOUND! [ [REDACTED] ]

Master Key      : 20 2A 17 18 00 1D EF 3A 29 3F 9B A7 84 5E 2A AA
                  FE B2 E1 29 9A 9F 75 CF 73 31 24 74 31 2B B8 FC

Transient Key   : 4D 76 38 A8 0F EB A7 52 4D 01 BF 87 7E DA 20 19
                  CB 0B 2C D4 3F 66 76 79 FE 8F FD C9 6A D5 AE FB
                  20 E6 AE F8 A3 61 90 BA 9D 48 93 B5 F0 29 1F EE
                  24 96 75 35 D6 03 68 DA 68 9D 11 FC 03 12 33 15

EAPOL HMAC     : F1 99 FA E3 55 94 25 53 3B F7 33 6A 4D B8 2B 0C
root@kali:~# █

```

```

Kismet Sort View Windows
Name      BSSID      I C  Ch  Freq  Pkts  Size  Bcn%  Sig  Clnt  Manuf      Cty  Seen By
TRENDnet  00:14:01:5F:97:12 A 0  1  2417  1  0B  ---  ---  1  TrendwareI --- wlan0  DRD1812
QQF93     00:1F:90:F2:CD:C2 A W  1  2412  1  0B  ---  ---  1  ActiontecE US wlan0  Networks
landscapers 00:14:BF:07:2F:84 A N  6  2437  2  0B  10% -86 1  Cisco-Link --- wlan0  17
linksys_SES_45997 00:16:B6:1B:E4:FF A 0  6  2447  2  0B  ---  ---  1  Cisco-Link --- wlan0  Packets
linksys   00:1A:70:D9:BC:13 A N  6  2437  2  0B  ---  ---  1  Cisco-Link --- wlan0  787
MPA41    00:1F:90:E6:E0:84 A W  11 2462  3  0B  ---  ---  1  ActiontecE --- wlan0
TFS      00:09:5B:D7:9D:B2 A N  --- 2462  4  0B  ---  ---  1  Netgear    --- wlan0
Autogroup Probe 00:13:E8:92:3F:CB P N  ---  ---  5  0B  ---  ---  1  IntelCorpo --- wlan0  Pkt/Sec
meskas   00:18:01:F5:65:E1 A 0  11 2462  7  0B  10% -87 1  ActiontecE US wlan0  10
6SI03    00:1F:90:FA:F4:C8 A W  --- 2412  8  0B  ---  ---  1  ActiontecE --- wlan0
Xu Chen  00:18:01:F9:70:F0 A N  6  2442  9  0B  0%  -75 1  ActiontecE US wlan0  Elapsed
7J4R0    00:1F:90:E6:04:F1 A W  11 2462  14  0B  ---  -70 1  ActiontecE --- wlan0  00:01.05
TK421    00:18:01:FE:68:77 A 0  6  2437  14  0B  ---  -82 1  ActiontecE --- wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0  11 2462  14  0B  0%  -31 1  Netgear    --- wlan0
Pickles  00:1F:33:F3:C5:4A A 0  2  2422  17  0B  ---  ---  1  Netgear    --- wlan0
38c8     00:16:CE:07:60:77 A W  6  2447  38  0B  ---  -76 1  HonHaiPrec --- wlan0

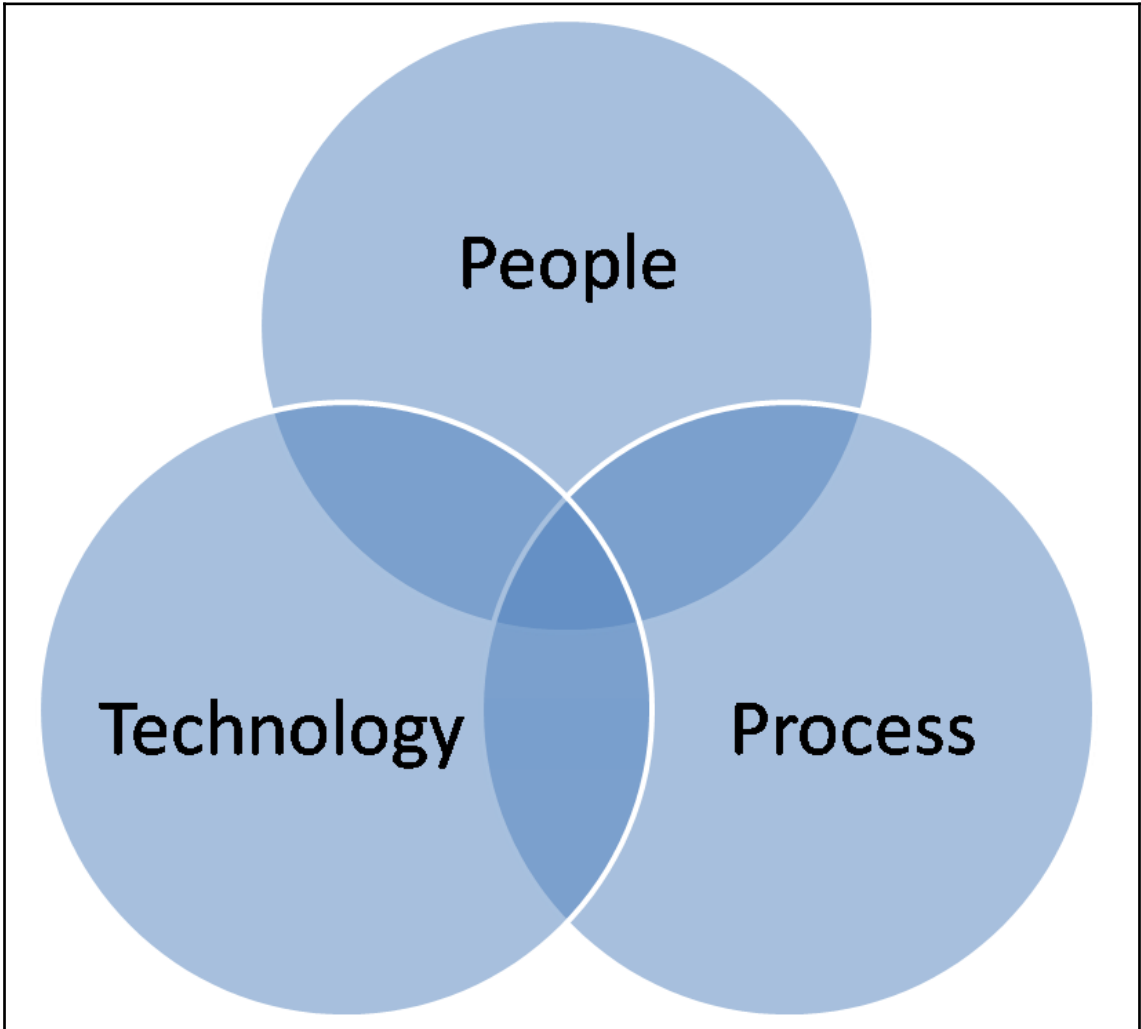
MAC      Crypt Freq  Pkts  Size  Manuf      DHCP Host  DHCP OS
00:13:10:35:59:CB  0 2462  624  0B Cisco-Link  ---  ---
00:11:24:A4:6F:B3  6 2452  6  708B AppleCompu ---  ---
00:13:10:35:59:C9  5 2452  5  1K Cisco-Link  ---  ---
00:17:AB:3D:25:98  4 2452  4  626B Nintendo  ---  ---
00:13:E8:92:3F:CB  8 ---  8  1K IntelCorpo  ---  ---

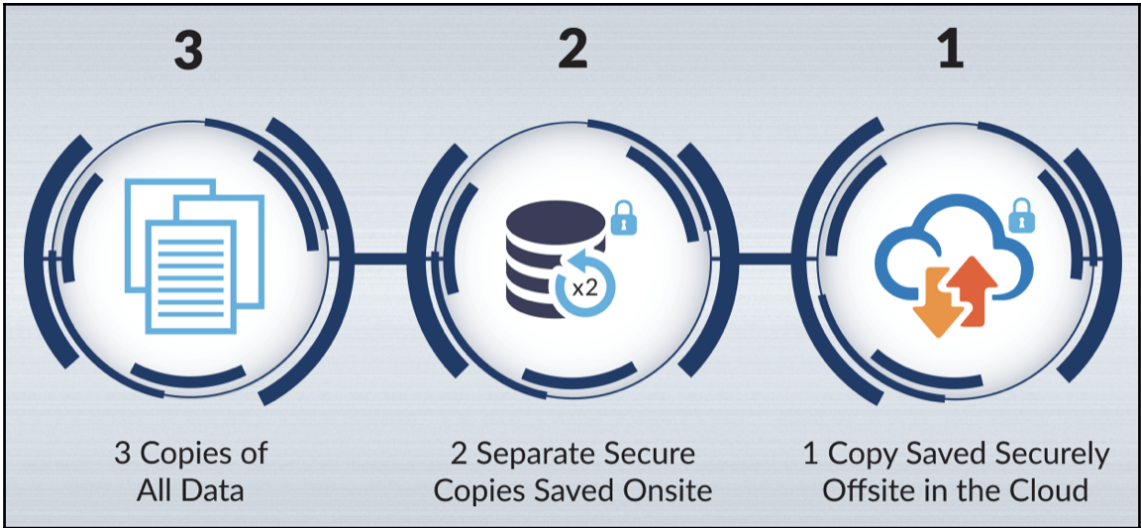
No GPS info (GPS not connected)

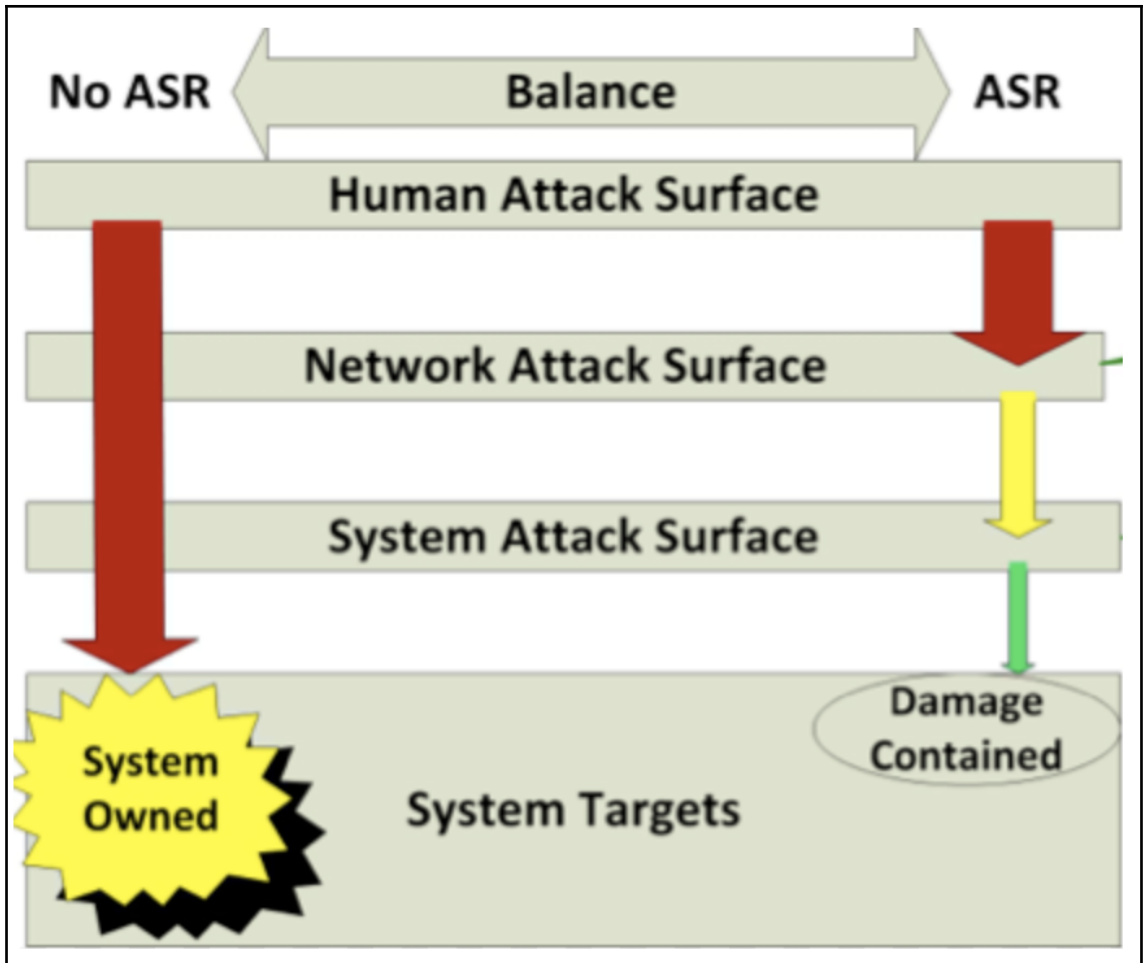
INFO: Detected new managed network "landscapers", BSSID 00:14:BF:07:2F:84, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "QQF93", BSSID 00:1F:90:F2:CD:C2, encryption yes, channel 1, 54.00 mbit wlan0
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect 9

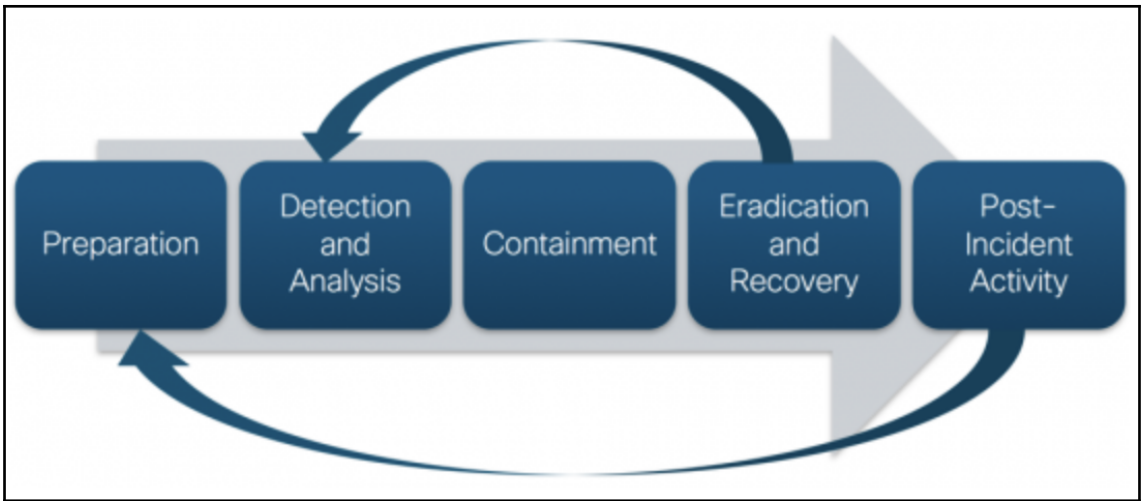
```

Chapter 10: Responding to Service Disruption









Chapter 11: The Human Problem - Governance Fail

The screenshot shows a web browser window displaying an email from the IRS. The email subject is "Final reminder: Notice of Tax Return" and is dated April 10, 2013. The email body contains the IRS logo, the text "Department of the Treasury Internal Revenue Service", and a message about claiming a tax refund online. A link labeled "Get Started" is highlighted, and a mouse cursor is hovering over it. The actual link in the footer is "careybaptist.org.uk/inc./s/".

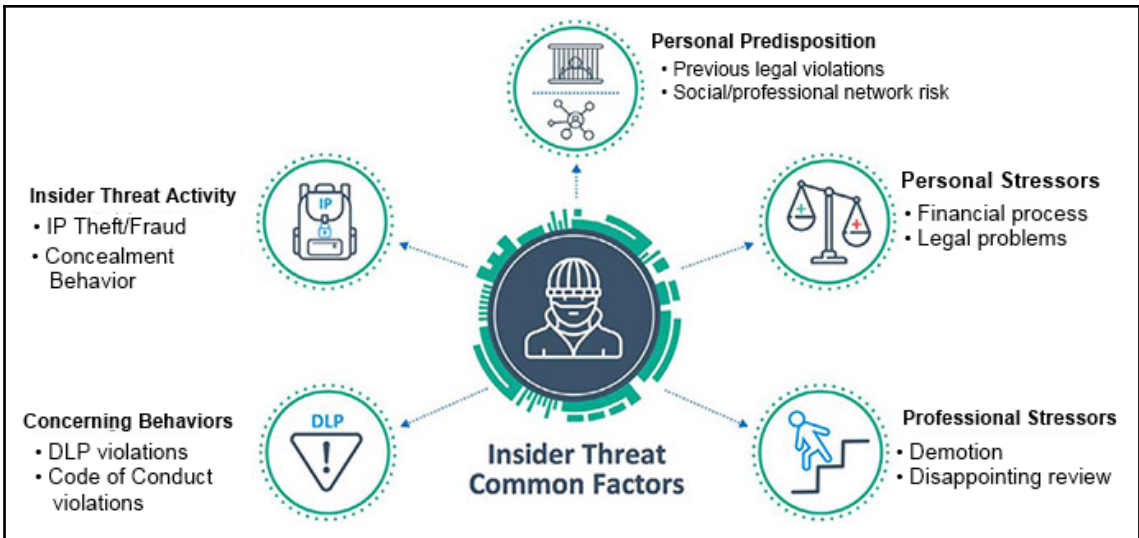
Annotations with red arrows point to the IRS logo, the "Get Started" link, and the actual link in the footer.

Wow! Looks official, right? It says IRS, it has the logo... etc.

If it sounds too good to be true, then it probably is too good to be

Hover the mouse over the link, but DO NOT click the link!

Now observe the actual link you would be taken to!



From: John Doe <jdoe@companydomain.us>
Date: July 30, 2015 at 10:27 AM EDT
To: Jane Smith jsmith@companydomain.com

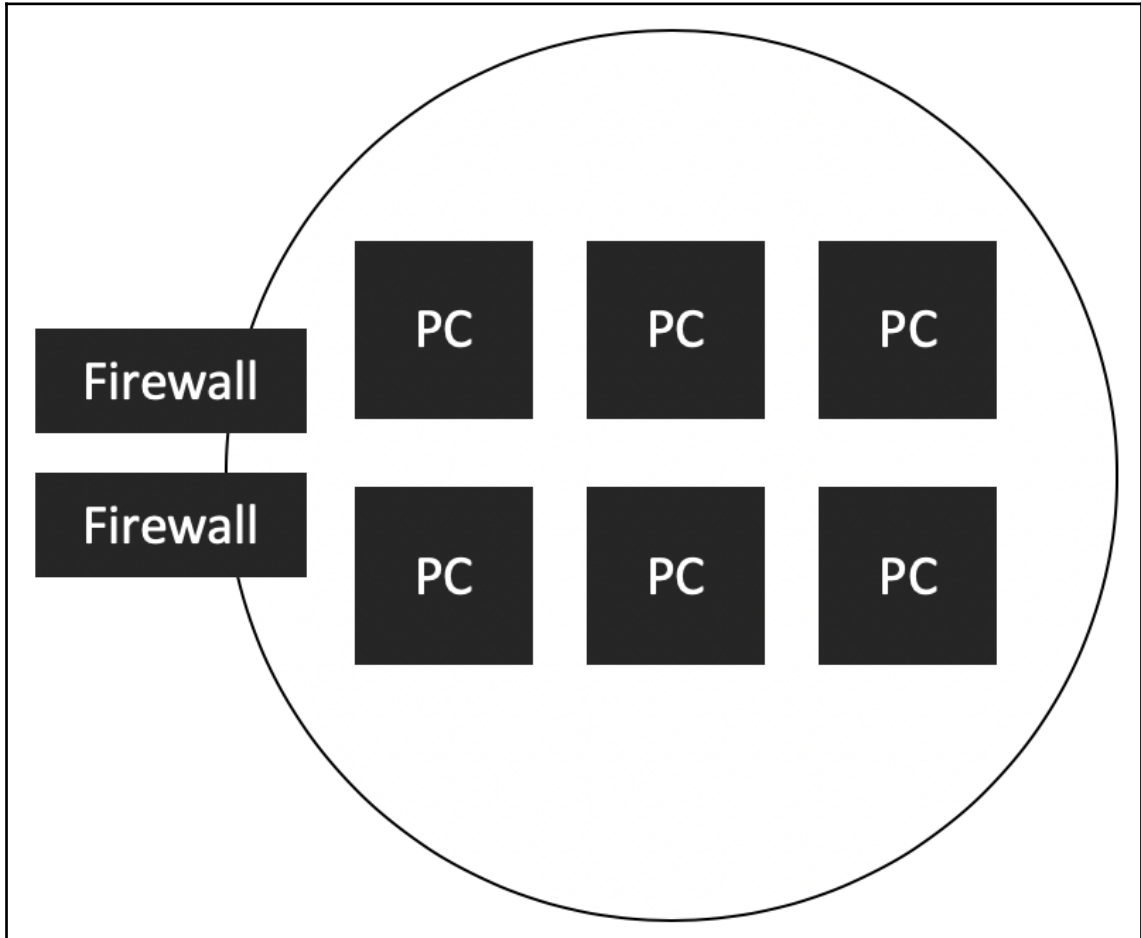
Jane,

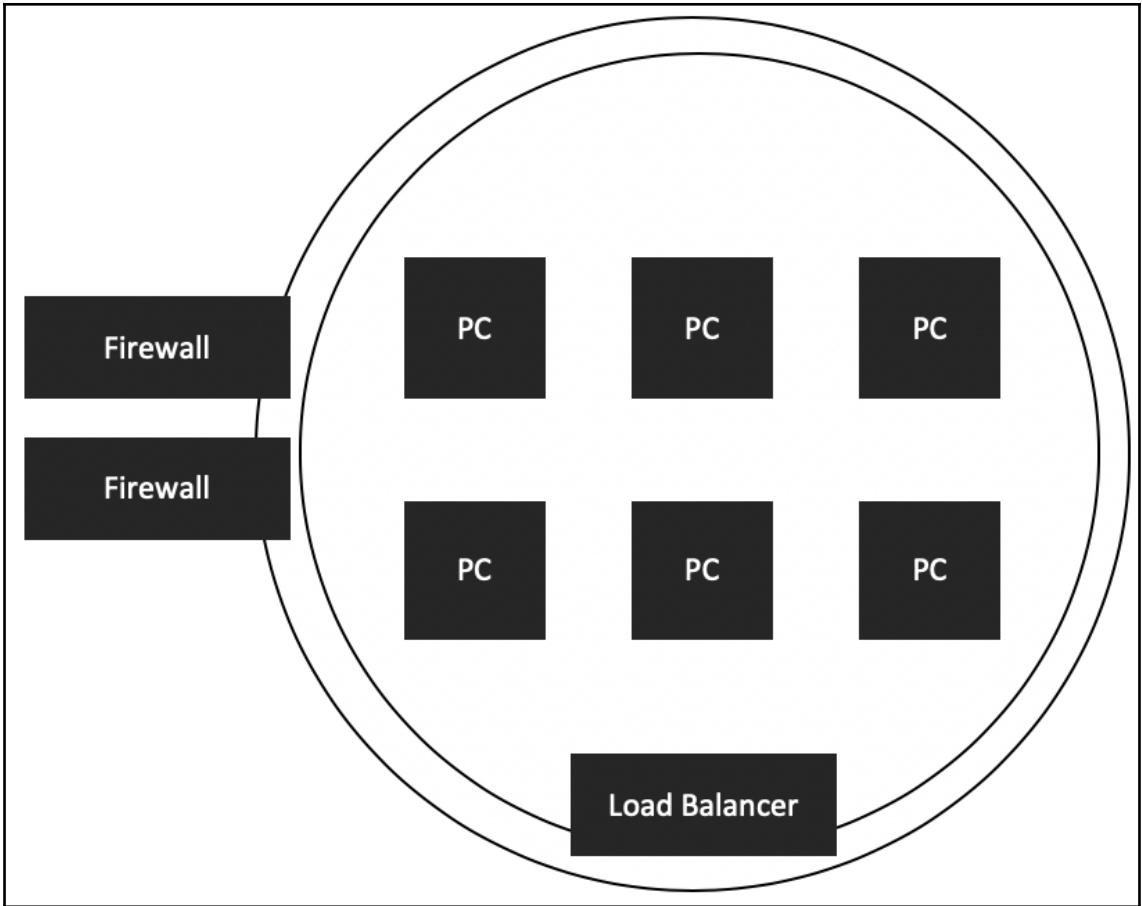
Process a wire of \$98,500 USD to the attached wiring instructions. This should be coded to Admin Expenses. Let me know when it is completed.

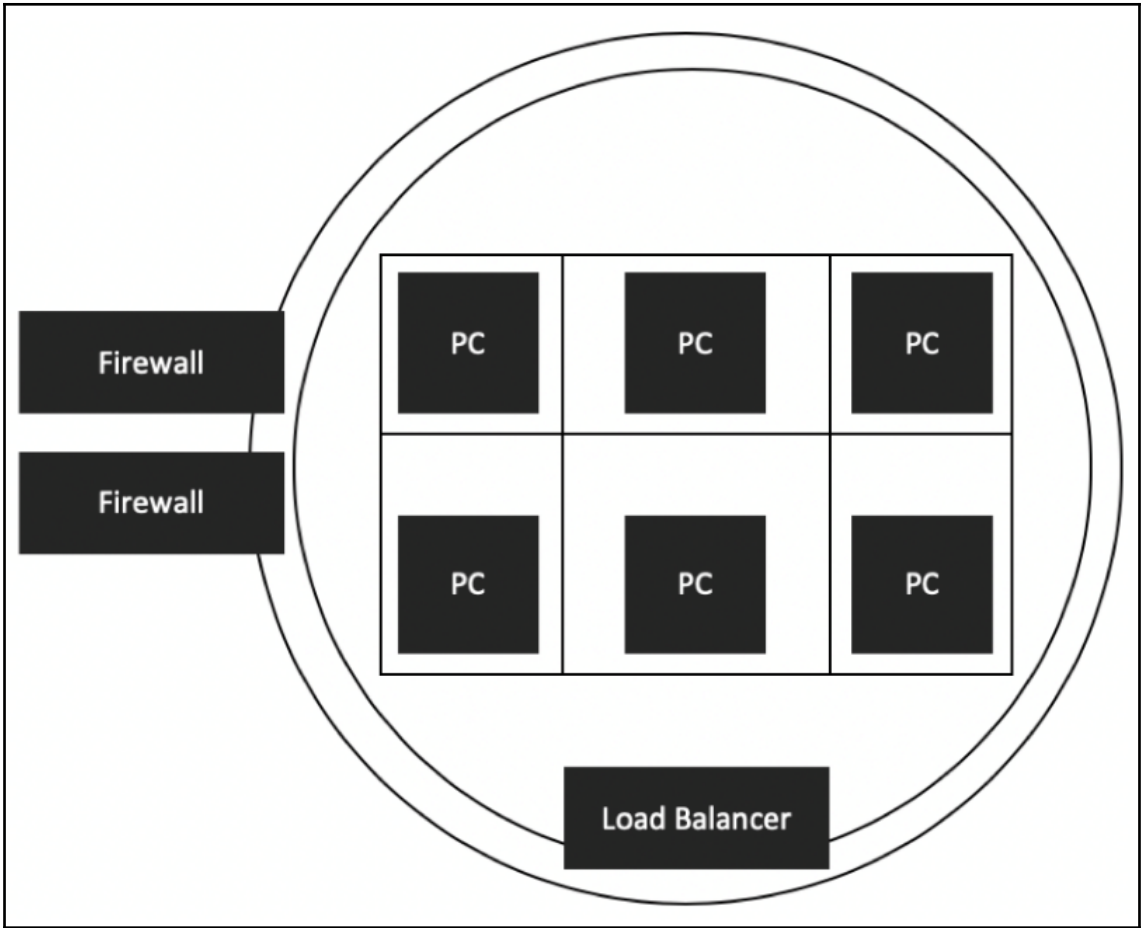
Thanks,

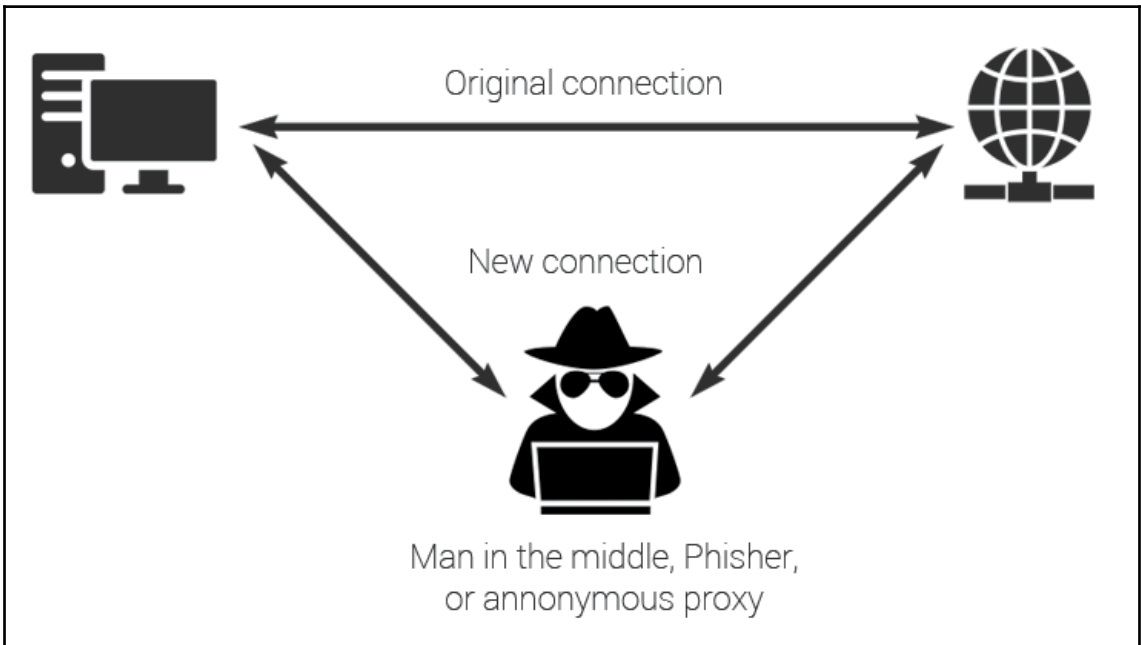
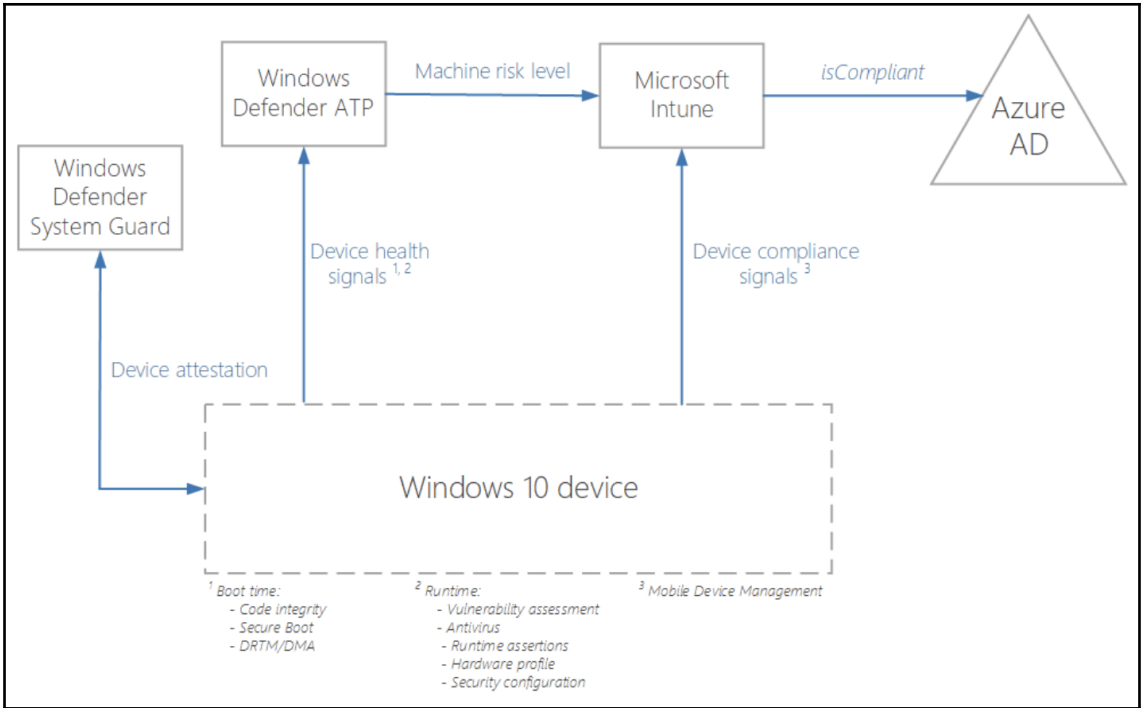
John Doe
 CEO, Company Domain

Chapter 12: Securing the Perimeter and Protecting the Assets



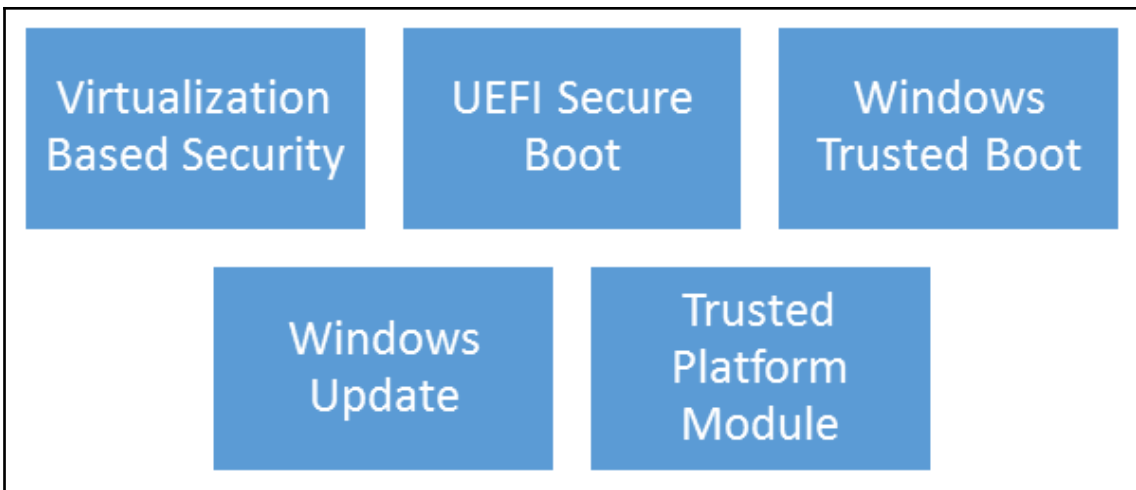
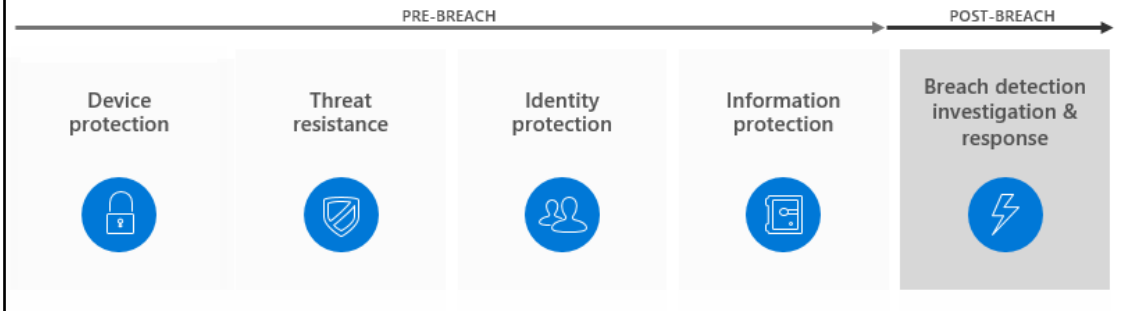


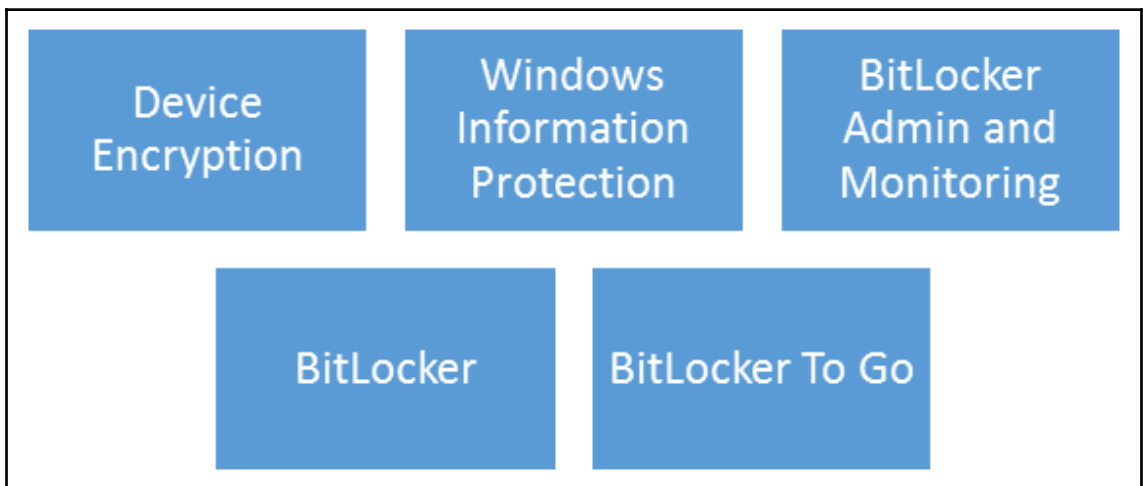
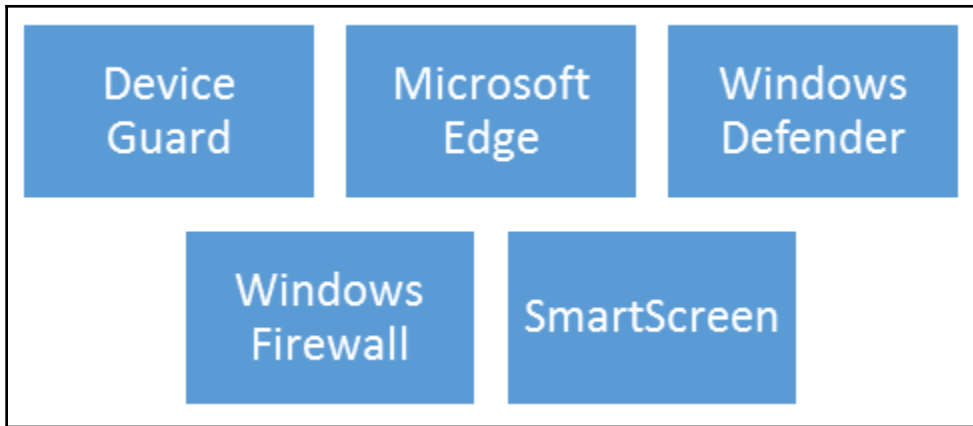




THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND





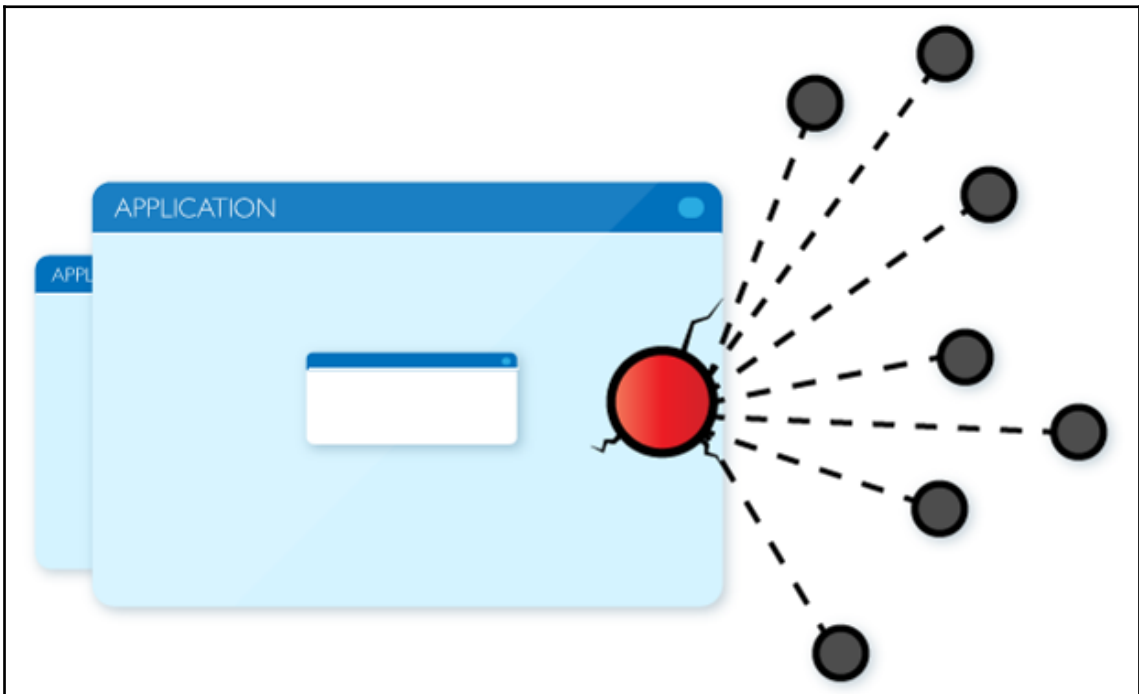
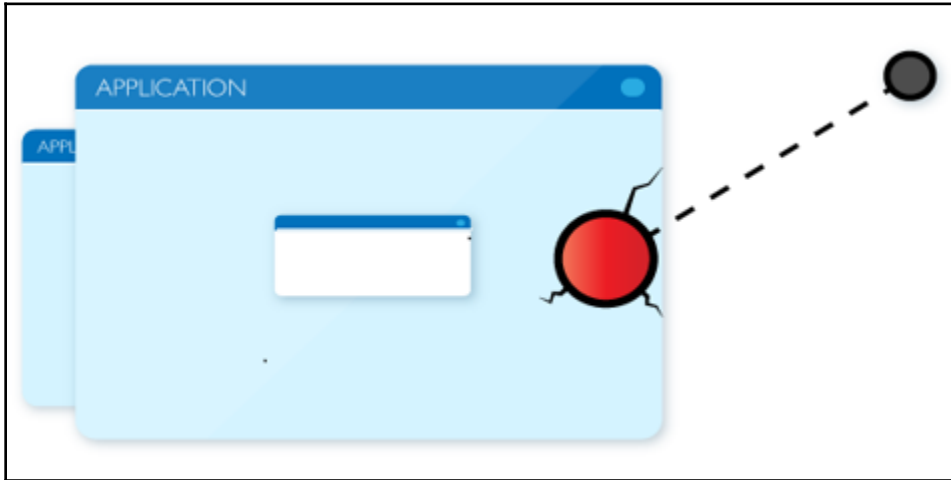


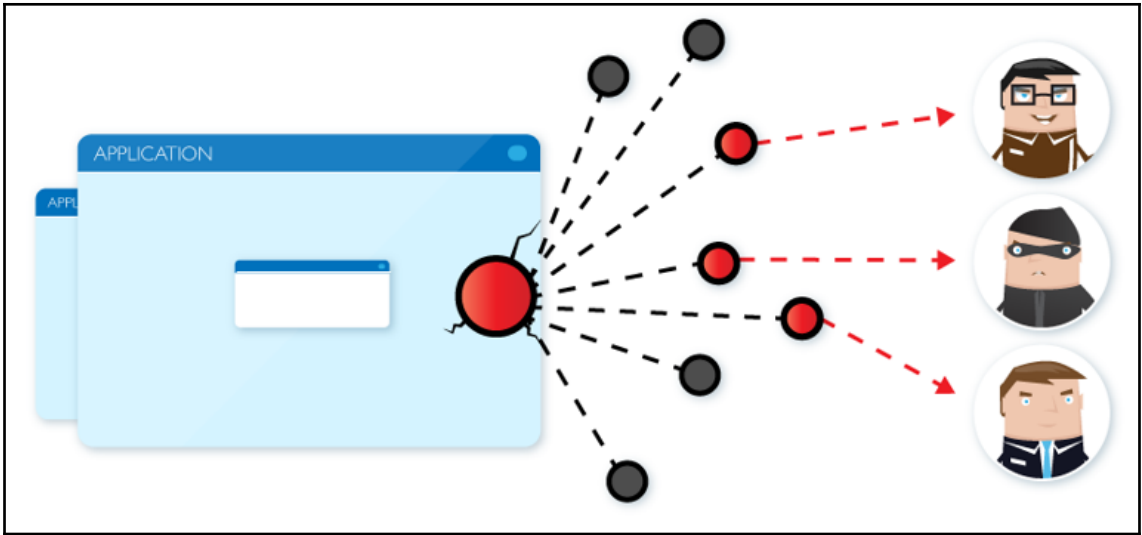
Security
Management

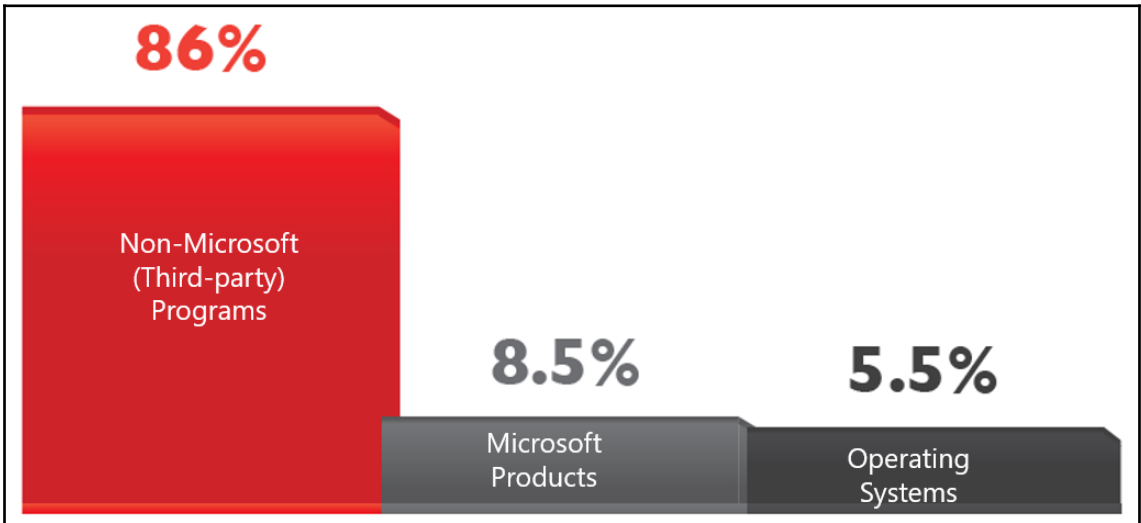
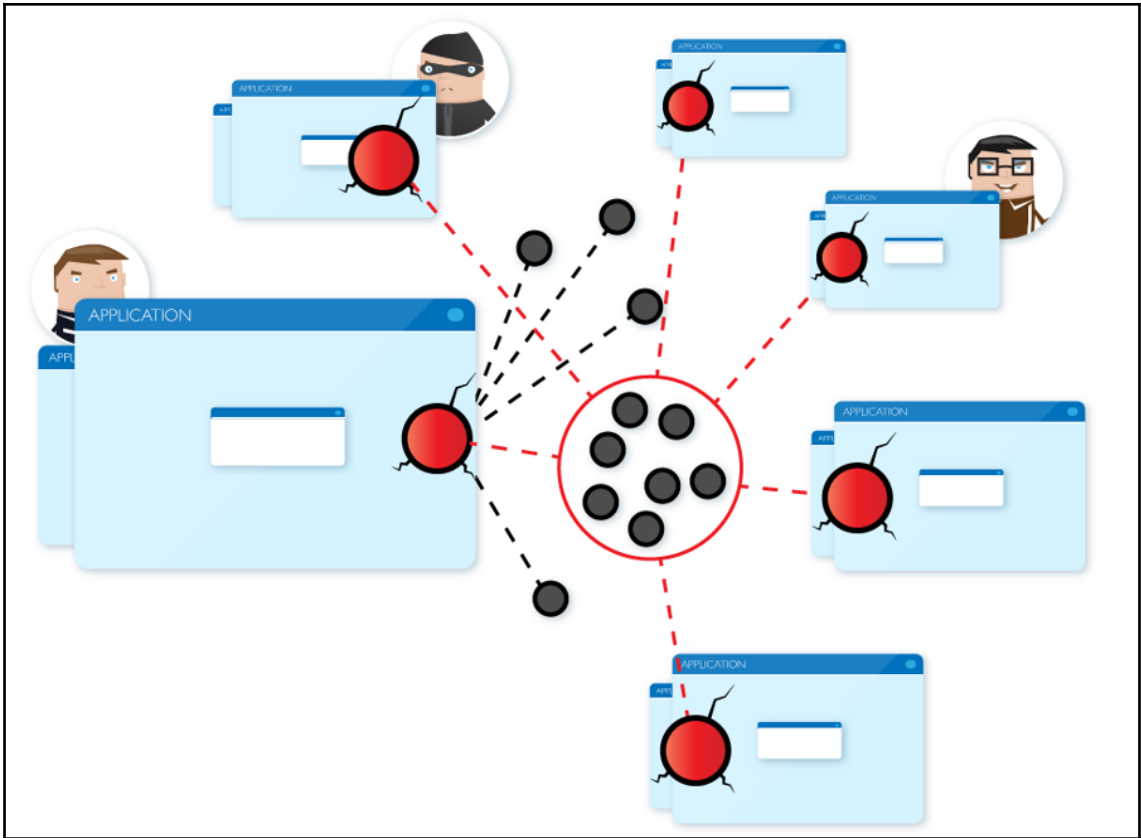
Conditional Access

Windows Defender
Advanced Threat
Protection (ATP)

Chapter 13: Threat and Vulnerability Management





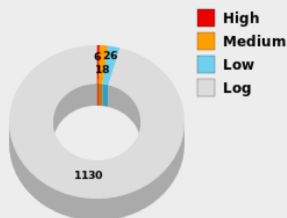




Results (1180 of 1280)



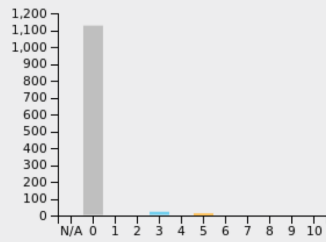
Results by Severity Class (Total: 1180)



Results vulnerability word cloud



Results by CVSS (Total: 1180)



1 - 10 of 1180

Vulnerability	Severity	QoD	Host	Location	Created
Microsoft Remote Desktop Protocol Detection	0.0 (Log)	80%	192.168.86.61	3389/tcp	Tue Oct 24 15:22:06 2017
DNS Server Detection (UDP)	0.0 (Log)	80%	192.168.86.7	53/udp	Tue Oct 24 15:14:47 2017

9,955 Assets

2,908 Discovered Assets

License Usage: 9955 / 5000000 (0.20%)

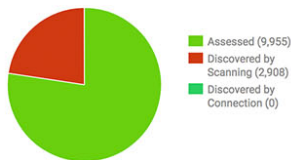
17 Sites

39 Asset Groups

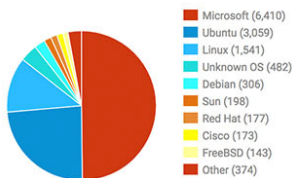
7,862 Tagged Assets

ASSET CHARTS

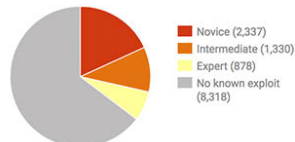
Assessment Status



Assets by Operating System



Exploitable Assets by Skill Level



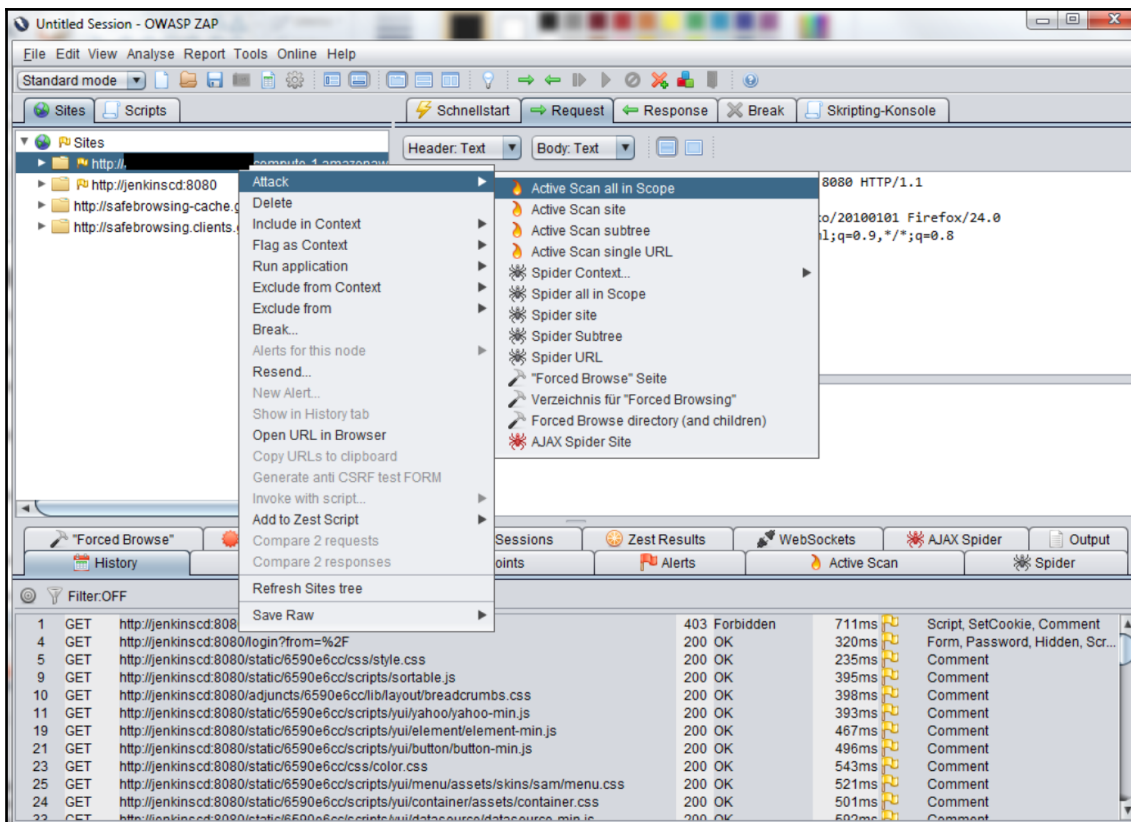
SCANNED

Address	Name	Site	Operating System	Vulnerabilities	Risk	Assessed	Last Scan	Delete	
10.1.10.101	server001	Los Angeles - Full Audit	Microsoft Windows Server 2003 R2, Enterprise Edition SP2	89	339	1429	1,690,272	Yes	Sun Oct 11 2015


```

root@kali:~/opt# nikto -port 80 -host http://192.168.0.1
- Nikto v2.1.6
-----
+ Target IP:      192.168.0.1
+ Target Hostname: 192.168.0.1
+ Target Port:    80
+ Start Time:    2017-05-11 10:32:23 (GMT-4)
-----
+ Server: micro httpd
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none

```




VULNERABILITY SCANS

 **0** TODAY


MAX DAILY SCANS: **30**

SCHEDULED NMAP

 **10** WEEKLY


MAX WEEKLY IPs: **2000**

SCHEDULED OPENVAS

 **16** MONTHLY

MAX MONTHLY IPs: **64**

IP / DNS / NETWORK TOOLS

 **0** TODAY

MAX DAILY QUERIES: **1000**

List of 30 most recent scans. In progress scans are able to be cancelled.

		Scan Target		Results	Cancel
complete	OpenVAS	t[REDACTED]	04:33:14	HTML 2 34 2	×
complete	Nikto	wha[REDACTED]	00:00:15	TEXT 2	×
complete	WhatWeb	scanme.nmap.org	00:00:02	TEXT	×
complete	WhatWeb	hackertarget.com	00:00:02	TEXT	×
complete	sslyze	traceroute-online.com	00:00:01	TEXT	×
complete	sslyze	scanme.nmap.org	00:00:01	TEXT	×
complete	Nmap	scanme.nmap.org	00:00:10	TEXT 4 HTML	×
complete	DomainProfiler	[REDACTED].com	00:00:02	XLS	×

Live Results Scan
 Mon, 17 Sep 2018 17:57:16 EDT

TABLE OF CONTENTS

Hosts Executive Summary







- localhost

Hosts Executive Summary

[Collapse All](#) | [Expand All](#)

localhost



Severity	CVSS	Plugin	Name
	10.0	56584	[Offline] Mozilla Foundation Unsupported Application Detection (macOS)
	9.3	108375	[Offline] Mozilla Firefox < 59 Multiple Vulnerabilities (macOS)
	9.3	108585	[Offline] Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities (macOS)
	9.3	109867	[Offline] Mozilla Firefox < 60 Multiple Critical Vulnerabilities (macOS)
	9.3	110806	[Offline] Mozilla Firefox < 61 Multiple Critical Vulnerabilities (macOS)
	9.3	117291	[Offline] Mozilla Firefox < 62 Multiple Critical Vulnerabilities (macOS)

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			Total
		Certain	Firm	Tentative	
Severity	High	3	7	0	10
	Medium	2	0	0	2
	Low	5	2	0	7
	Information	14	18	2	34

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.




Contents

1. XPath injection

[Back](#) | [Stop Scan](#) | [Generate Report](#) | [Export to...](#)

[Scan Stats & Info](#) | **Vulnerabilities** | [Site Structure](#) | [Events](#)



Acunetix Threat Level 3

HIGH

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity Completed

Overall progress 100%

Scanning of t... started Nov 16, 2016 11:25:59 AM

Scanning of t... completed Nov 16, 2016 12:01:54 PM

Scan Duration

26m 10s

Requests

54,257

Avg. Response Time

181ms

Locations

131

Target Information

Address: [REDACTED]

Server: nginx

Latest Alerts 85 83 11 25

- Possible CSRF (Cross-site request forgery) Nov 16, 2016 12:01:25 PM
- Possible CSRF (Cross-site request forgery) Nov 16, 2016 12:01:25 PM

Dashboard

Notification Center

Vulnerability Manager

Intelligence

Assessment

Patching

Policy Manager

Analytics

Auditor

Settings

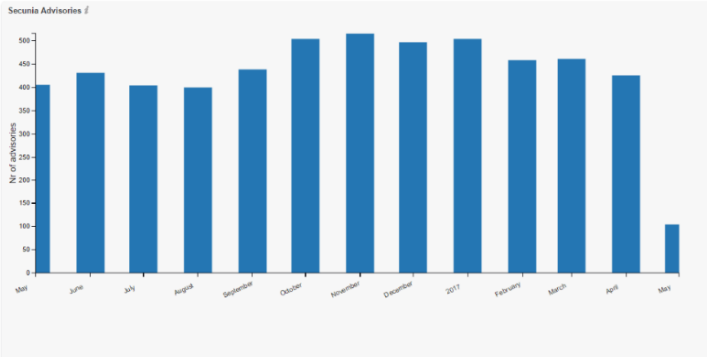
User Profile

Advisories Tickets Devices Products Reports

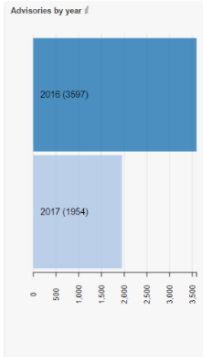
Advisory Analytics and Reports

Criticality: [Dropdown] All Assets [Dropdown] 2016-05-10 [Dropdown] 2017-05-10 [Dropdown] Filter Reset


Secunia Advisories




Advisories by year



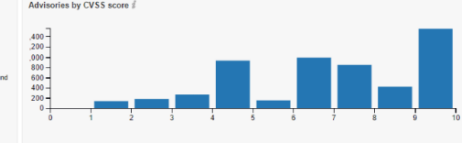
Advisories by level of criticality



Advisories by solution status




Advisories by CVSS score



Microsoft Word ribbon: FILE, HOME, INSERT, PAGE LAYOUT, FORMULAS, DATA, REVIEW, VIEW, ADD-INS, TEAM. Ribbon options include Clipboard, Font, Alignment, Number, and Conditional Formatting.

Address bar: A1, Network Host Report

Network Host Report



October 14, 2017 at 11:57 PM

This report contains information about the hosts that were discovered during the course of the security assessment carried out using Core Impact.

For each host the vulnerabilities, identities and exposures identified during the course of the security assessment are listed. Due to the nature of the testing carried out with Core Impact this information is confirmed.

Vulnerabilities refer to problems exposed by Core Impact that could allow an unauthorized person to get code execution on the target system. Exposures refer to problems that leak information that could be leveraged by an unauthorized person to help identify target systems and find vulnerabilities. Identities refer to user accounts that were confirmed.


SECTION	PAGE
Workspace information	2
Summary	3
Identities types	4
Hosts with valid identities	5
Exploited hosts	6
Applications	7
Ports	8
Vulnerabilities	9
Identities	10
Identities - Windows NTLM	11
Identities - Kerberos	12

Navigation bar: Applications | Ports | Vulnerabilities | Identities | Identities - Windows NTLM | Identities - Kerberos

1 of 6 Find | Next

Audit Group : All
Scope : Removed Vulnerabilities

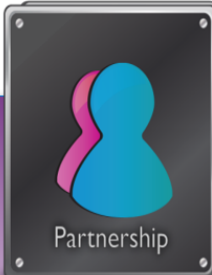
Domain	Vulnerability	Severity	Class	CVSS	Exploit	Age (days)
btlab.test (1)						
BTSOLUTIONS - Microsoft Windows Server 2012						
	Additional LSA Protection Not Configured	Info	Informational Check	0.0	No	22
	Cannot Change Password	Low	Informational Check	0.0	No	22
	DCE/RPC Service Detected	Info	Informational Check	0.0	No	22
	HTTP 404 Not Found Response Detected	Info	Informational Check	0.0	No	0
	HTTP Gzip Compression Detected	Info	Informational Check	0.0	No	22
	Microsoft Command Line Parameter Passing Information Disclosure (3082458)	Medium	Information Leak	4.3	No	36
	Microsoft Cumulative Internet Explorer Security Update (3089548)	High	Multiple Vulnerabilities	9.3	No	36
	Microsoft Cumulative Internet Explorer Security Update (3096441)	High	Multiple Vulnerabilities	9.3	No	36
	Microsoft Cumulative Internet Explorer Security Update (3104517)	High	Multiple Vulnerabilities	9.3	No	46



Security

Be close to the Vulnerability Intelligence providers to handle corporate risk management.


Are you working with a research house that has experience and expertise in identifying vulnerabilities?



Partnership

Leverage Vulnerability Management knowledge directly from the source.

Ensure you are informed of emerging vulnerabilities and know which are critical to patch!



Synergy

Vulnerability research helps organizations improve their product security and thereby improve security for end-users.

Vulnerability Intelligence should be the foundation of your IT security infrastructure!

Risk Management Strategies



Acceptance



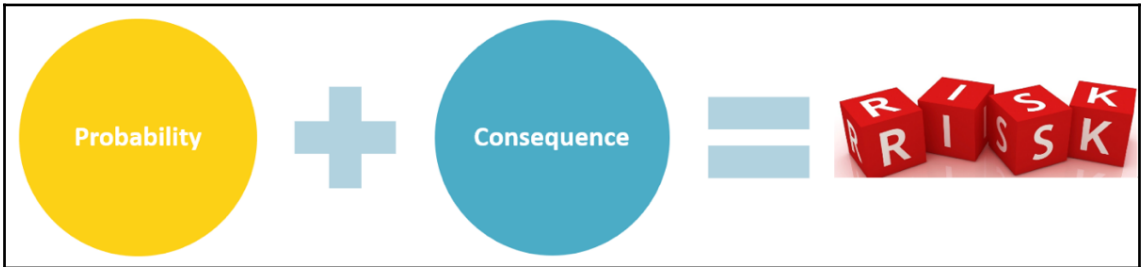
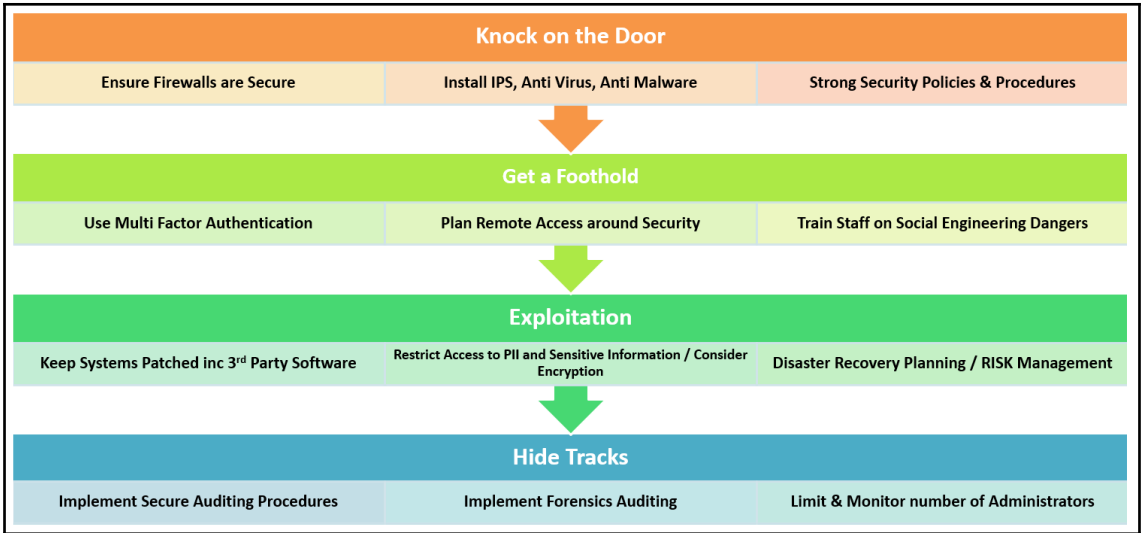
Mitigation



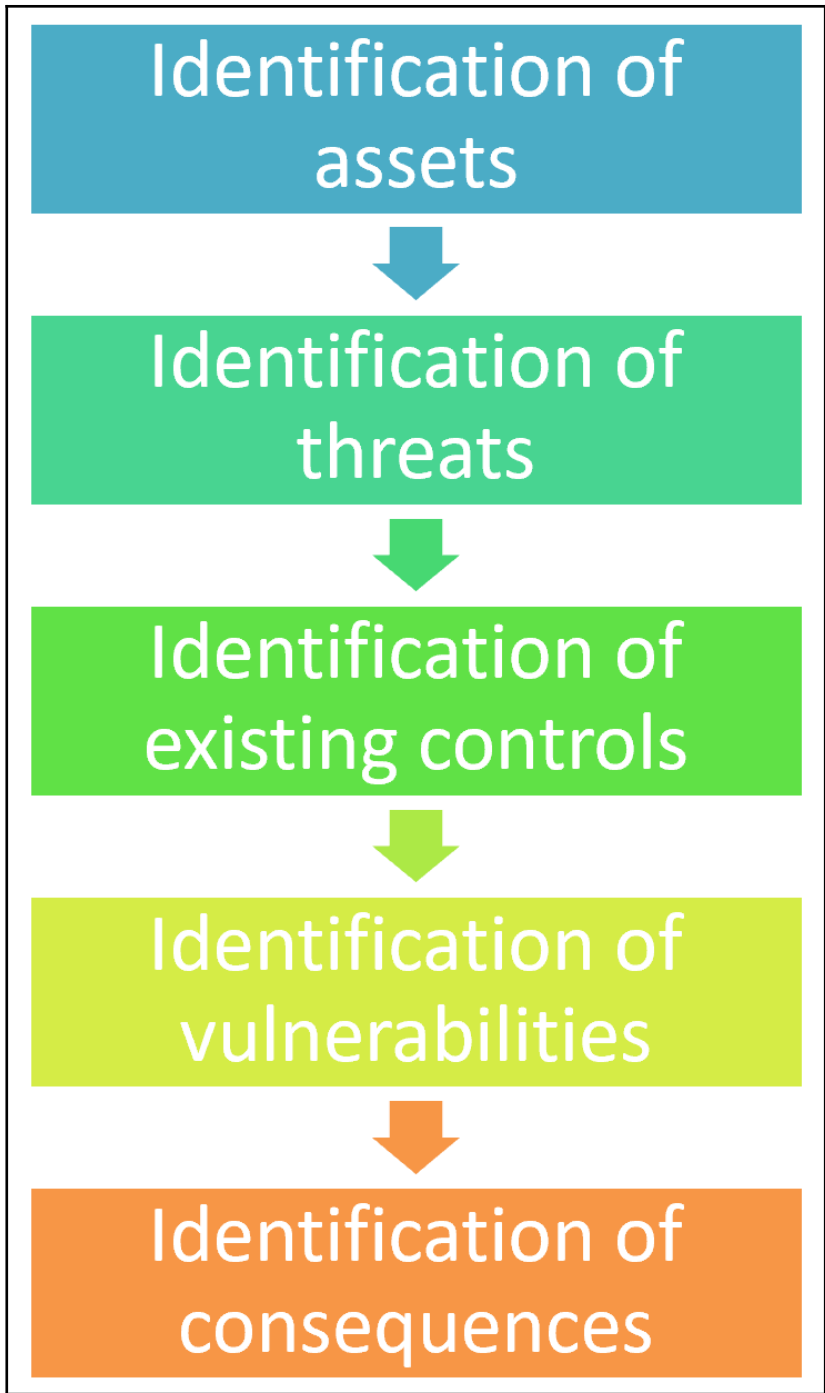
Transference



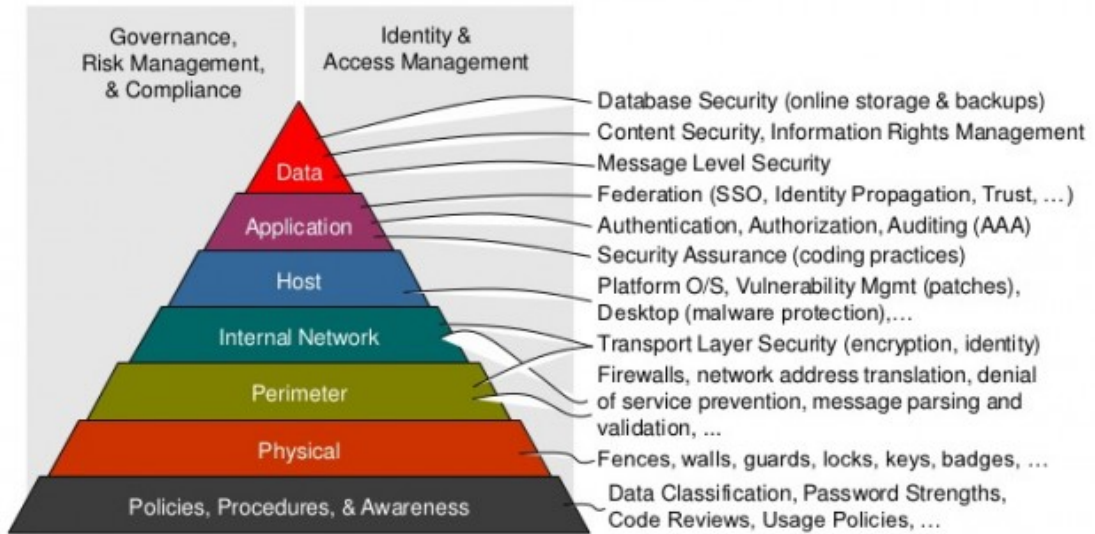
Avoidance





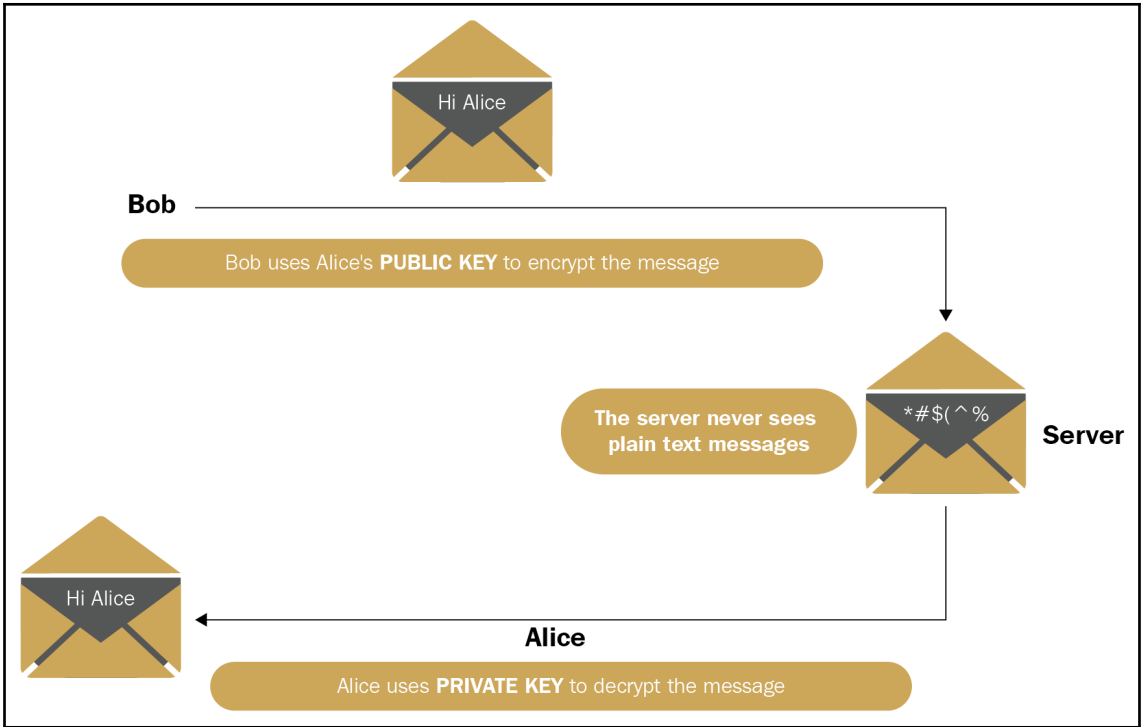


Defense in Depth

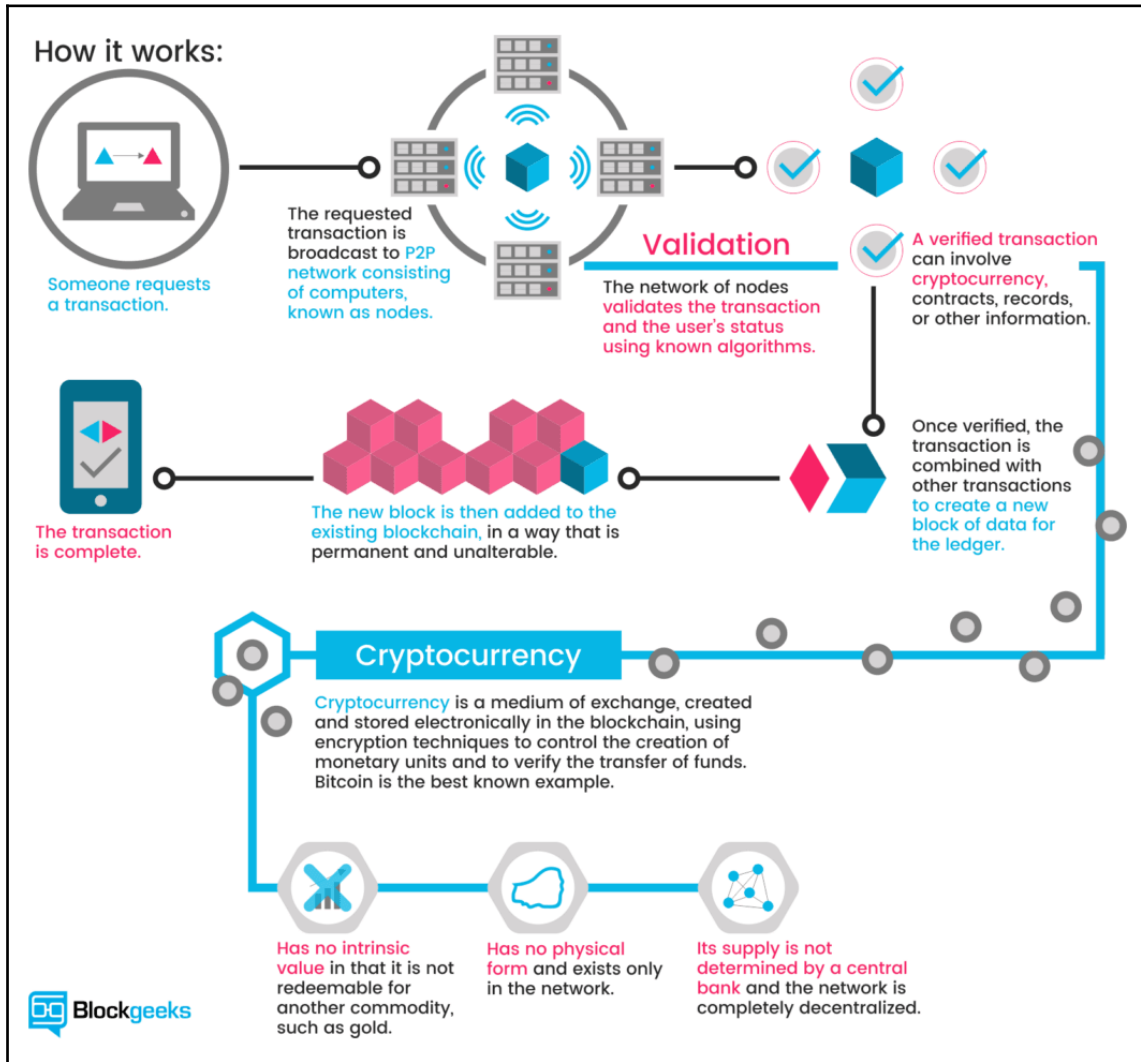


Chapter 15: Encryption and Cryptography for Protecting Data and Services

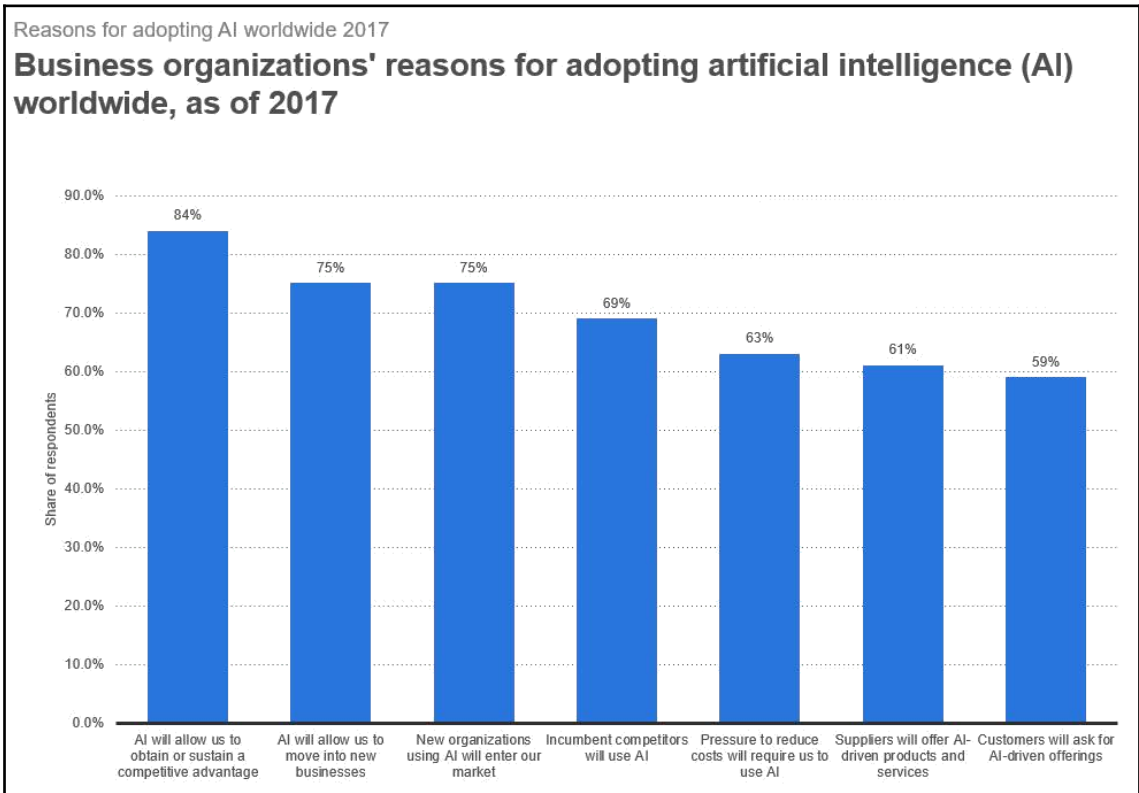




Chapter 16: The Rise of the Blockchain

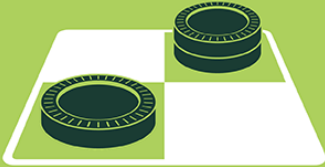


Chapter 17: Artificial Intelligence and Cybersecurity



ARTIFICIAL INTELLIGENCE

Early artificial intelligence stirs excitement.



MACHINE LEARNING

Machine learning begins to flourish.

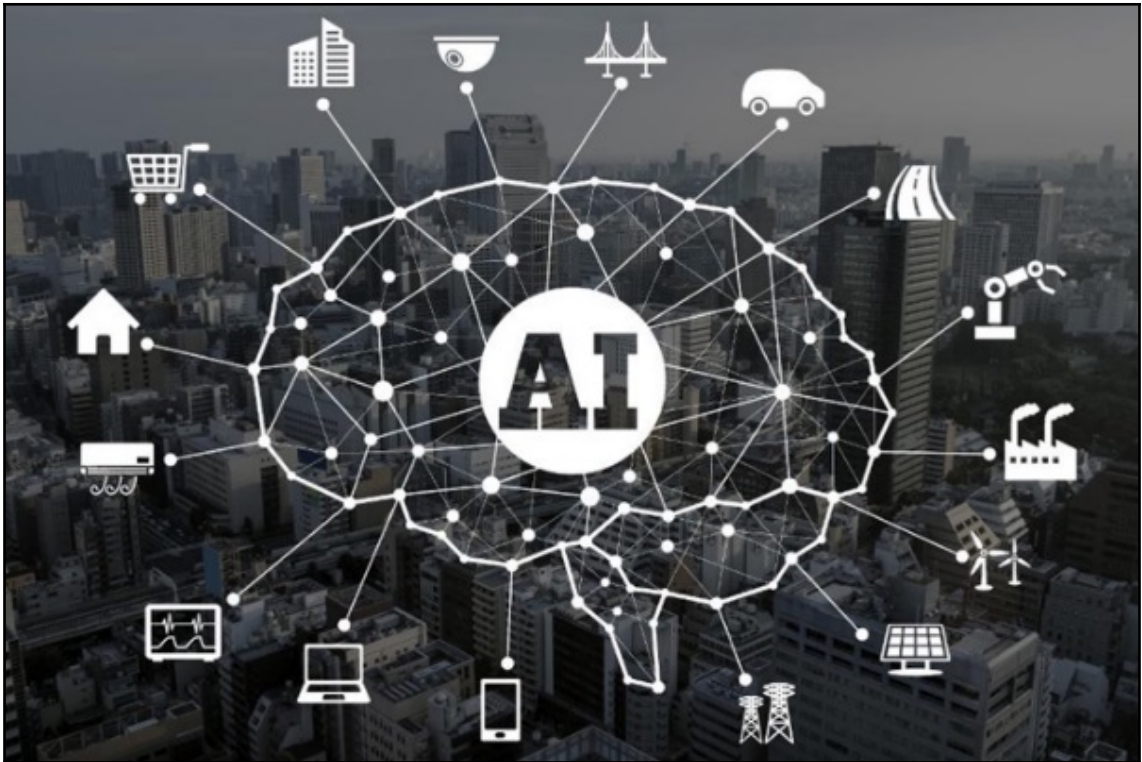


DEEP LEARNING

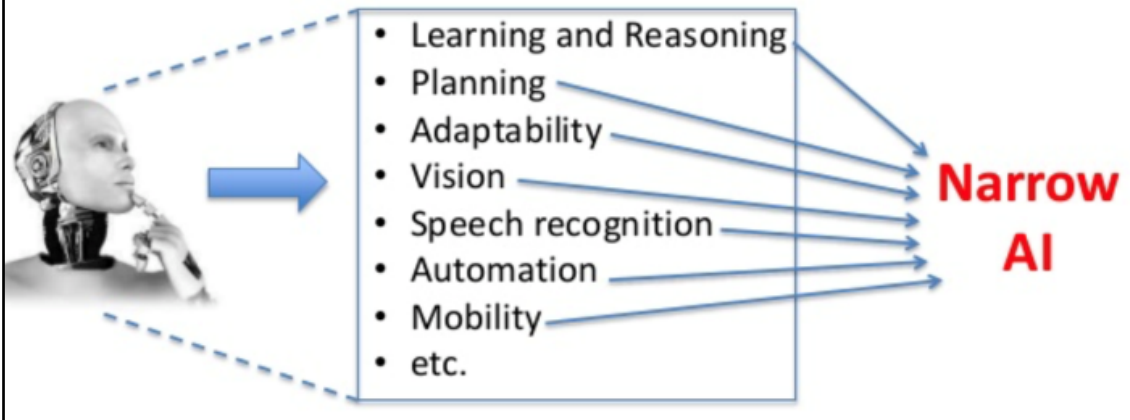
Deep learning breakthroughs drive AI boom.



Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.



Narrow AI





Bob: i can i i everything else

Alice: balls have zero to me to me to me to me to me to me to me to me to

Bob: you i everything else

Alice: balls have a ball to me to me to me to me to me to me to me

Bob: i i can i i i everything else

Alice: balls have a ball to me to me to me to me to me to me to me

Bob: i

Alice: balls have zero to me to me to me to me to me to me to me to me to

Bob: you i i i i everything else

Alice: balls have 0 to me to me to me to me to me to me to me to me to

Bob: you i i i everything else

Alice: balls have zero to me to me to me to me to me to me to me to me to

Windows Defender Security Center

File Search (File, IP, URL, Machine, User)

milad@wdgcp.com

Investigations > A malicious file was detected based on indication pr...

A malicious file was detected based on indication provided by O365
Investigation #189223 is complete - Remediated

Started Jan 29, 2019, 7:45:37 PM
Ended Jan 29, 2019, 10:11:16 PM
Total pending time: 10:20m

02:25:39 Complete

Comments (0)

Investigation details

Status: Remediated
Malicious entities found were successfully remediated.

Alert severity: Low

Category: Malware

Detection source: EDR

Investigation graph Alerts (1) Machines (1) Key findings (1) Entities (11k) Log (97)

Machine (1) WIIOCLIENTZ

Entities analyzed (11466)

- 10126 Files (1 Remediated)
- 338 Processes
- 317 Services
- 424 Drivers
- 33 IP Addresses
- 228 Persistence Methods

Alert received: A malicious file was detected based on indication p...

Threat found: 1 threat found

Waited for machine(s): Waited for 10:20 Minutes

Result: Remediated

Incident Analysis

- Artificial Intelligence will be able to perform the incident analysis to provide in-depth information on the impact of an incident, who the threat actors are and retrospectively provide the attack kill chain for the incident.

Incident Triage

- Very often security analysts are analyzing alerts only then to close them as confirmed false positives. Artificial intelligence will minimize false positives by augmenting rules-based detection systems.

Always Hunting

- Artificial Intelligence never sleeps and as a result will be able to continuously monitor all systems and discover anomalous behaviors as they occur.

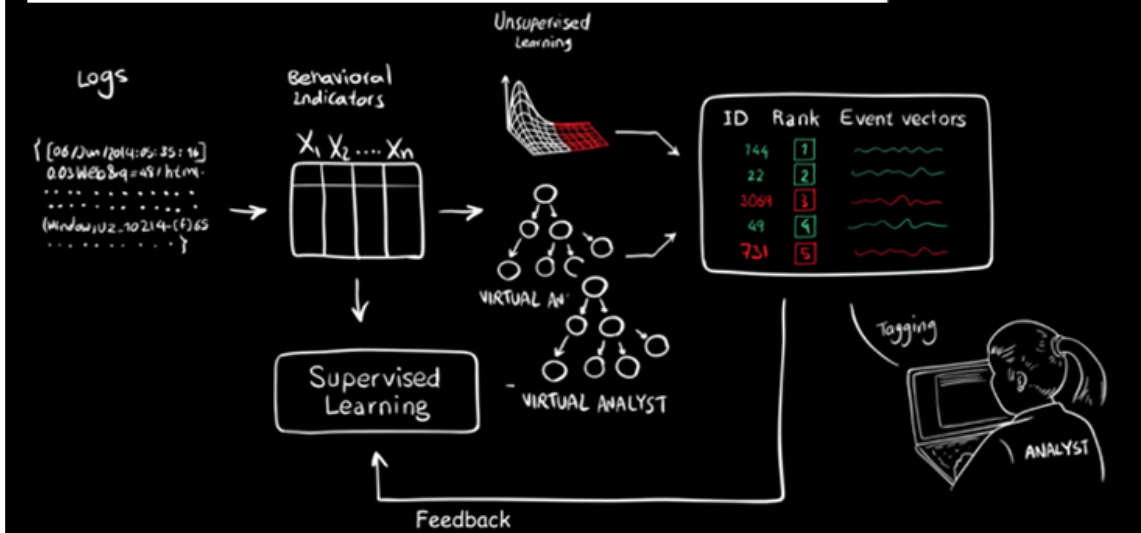
Threat Prediction

- Artificial Intelligence will pull threat intelligence from internal and external sources and provide predictive services for upcoming threats.

Incident Response

- Artificial Intelligence will apply case-based reasoning and create and/or run existing playbooks to perform an incident response either fully automated or with a human analyst monitoring it.

Artificial-Intelligence based Cyber Security System



Chapter 18: The Quantum Future

