



**Cyber Security Threats, How to
Mitigate Them, and What to Ethically
Do Should You Be Compromised**

***Sam Chawkat
Chief Operations Officer***

Background



- ▶ Providing IT consulting to organizations of various sizes across several states and regions since 1996
- ▶ Our focus is in our slogan, *We Take I.T. Personally*
- ▶ We don't focus on just the tech, we focus on the customer experience and customer satisfaction
- ▶ Dynamic Network Solutions is your "one stop shop" helping organizations with IT, cabling, AV, security, cameras, and phone systems. If it plugs in or turns on we can take care of it

Cybersecurity is Safety

- ▶ Security: We must protect our computers and data in the same way that we secure the doors to our homes.
- ▶ Safety: We must behave in ways that protect us against risks and threats that come with technology.



Make Sure Door is Locked

Make Sure Door is Locked

Make Sure Door is Locked
When You Leave

Make Sure Door is Locked
When You Leave

Importance of Cybersecurity

- ◉ The internet allows an attacker to work from anywhere on the planet.

- ◉ Risks caused by poor security knowledge and practice:
 - Identity Theft
 - Monetary Theft
 - Legal Ramifications (for yourself and your organization)
 - Sanctions or termination if policies are not followed

- ◉ According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
 - Web Browser
 - Email
 - Web Applications
 - Excessive User Rights



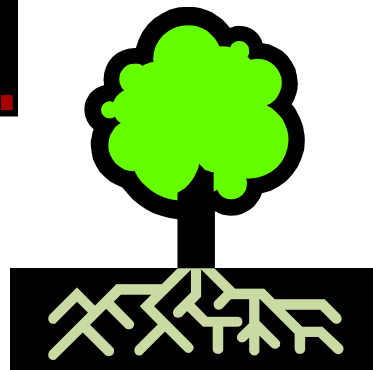
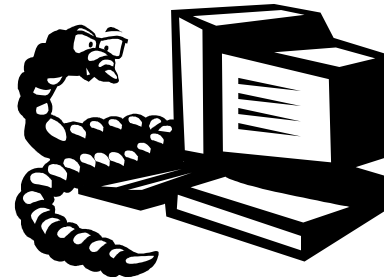


DYNAMIC
NETWORK
SOLUTIONS

Lets Discuss The Type Of Threats That Exist

Leading Threats

- ▶ Viruses
- ▶ Worms
- ▶ Social Engineering/Phishing
- ▶ Rootkits
- ▶ Botnets / Zombies
- ▶ Ransomware



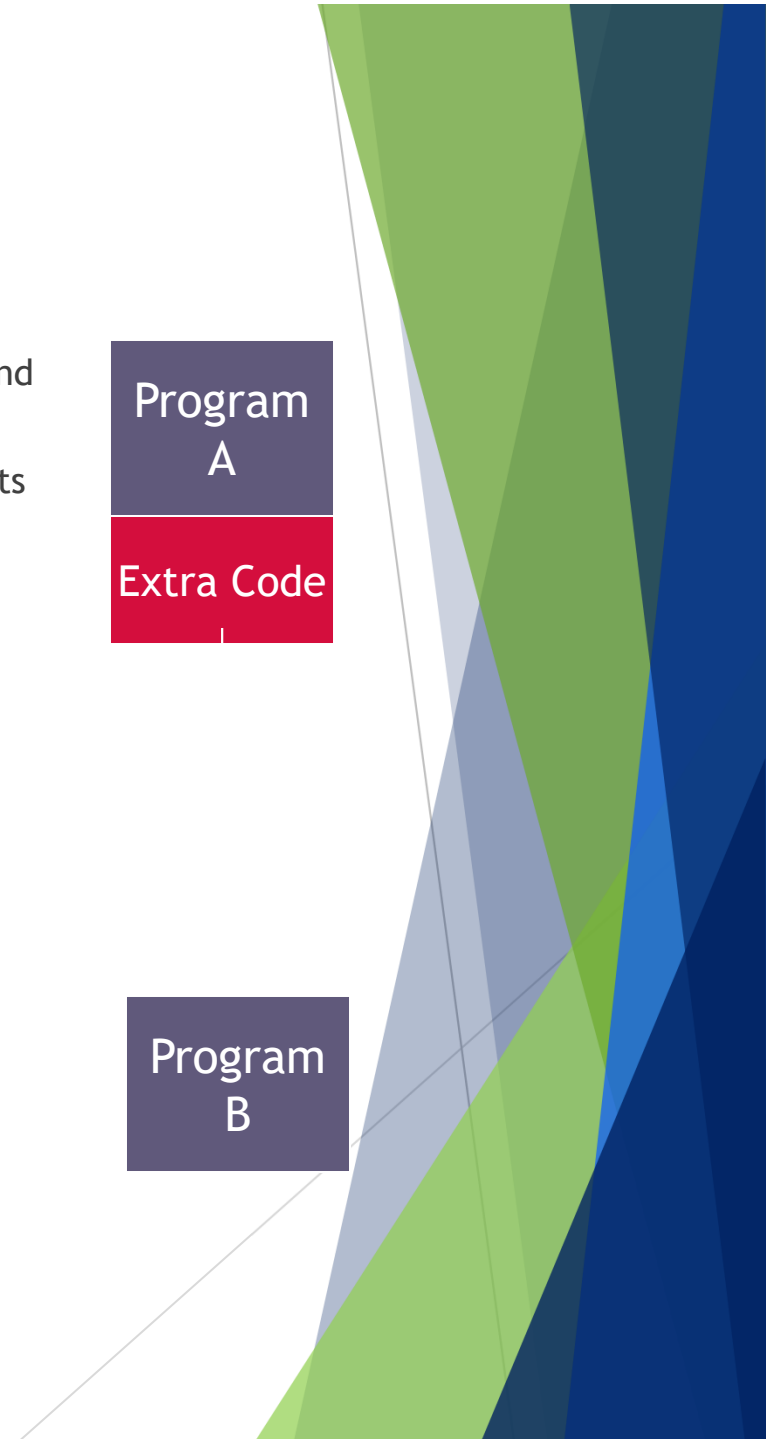
Viruses

- A virus attaches itself to a program, file, or disk.
- When the program is executed, the virus activates and replicates itself.
- The virus may be benign or malignant but executes its payload at some point (often upon contact).
 - Viruses can cause computer crashes and loss of data.
- In order to recover or prevent virus attacks:
 - Avoid potentially unreliable websites/emails.
 - System Restore.
 - Re-install operating system.
 - Use and maintain anti-virus software.

Program
A

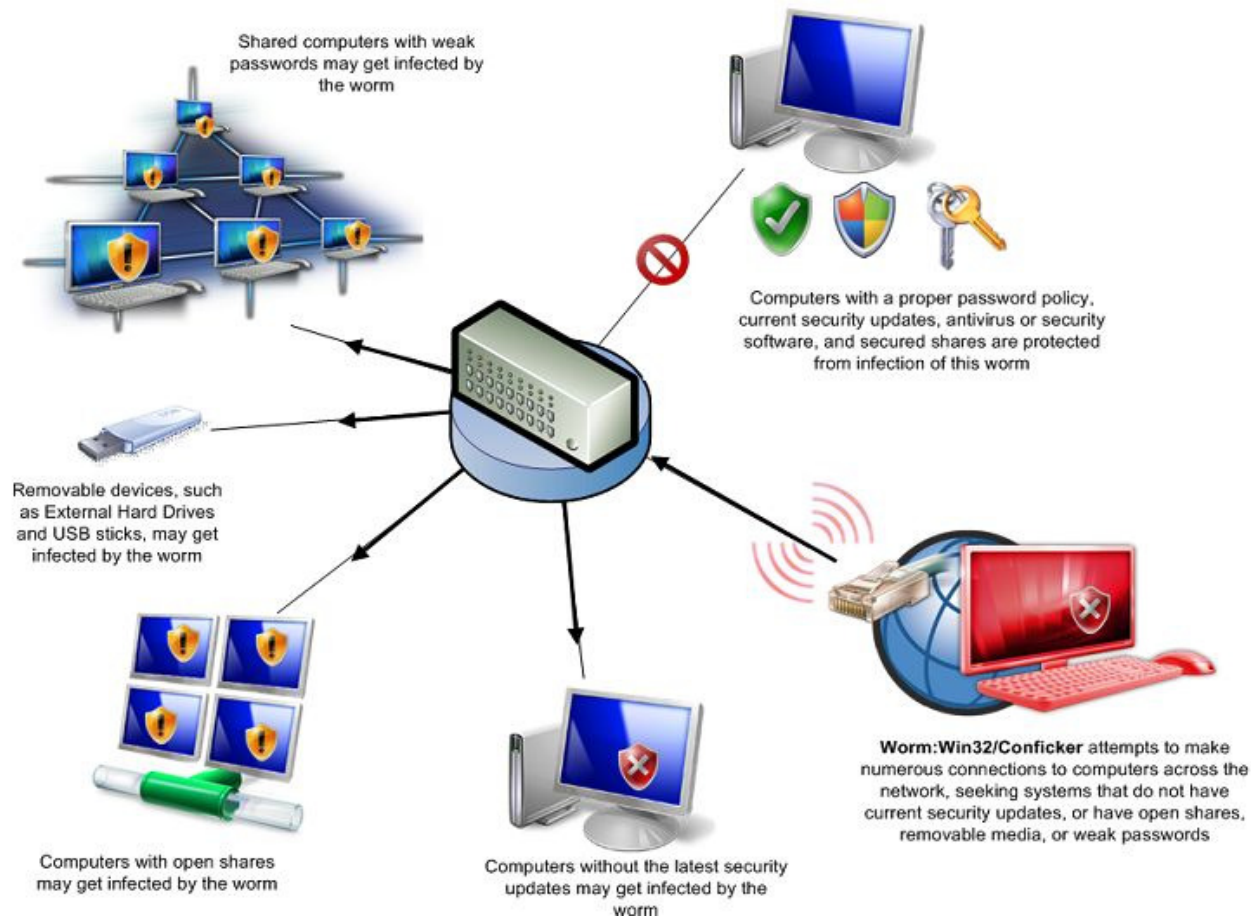
Extra Code

Program
B



Worms

- ▶ Independent program that replicates itself and sends copies from computer to computer across network connections.
- ▶ Upon arrival, the worm may be activated to replicate.



Social Engineering

- ▶ Manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.
- ▶ Tip - Removal of staff members email addresses from your website

Phone Call:
This is John,
the System
Administrator.
What is your
password?



In Person:
What ethnicity
are you? Your
mother's
maiden name?



Email:
ABC Bank has
noticed a
problem with
your account...

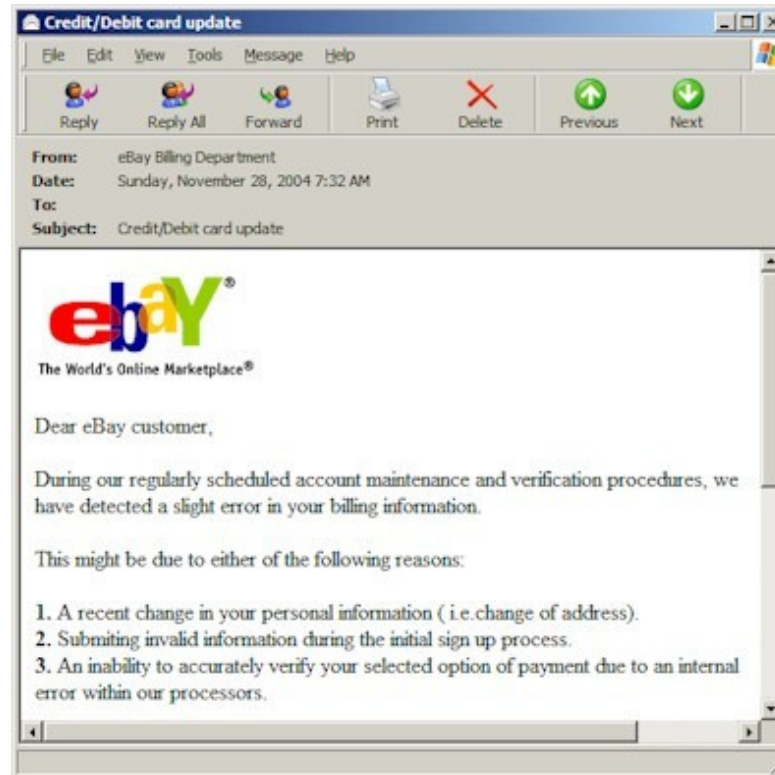
and have
some
lovely
software
patches!

I have come
to repair
your
machine...



Phishing: Counterfeit Email & Documents

- ▶ A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.
- ▶ Now legitimate resources like Office365 documents are being used to perform this and evade detection



Phishing: Counterfeit Email

Re: [EXTERNAL:] Re: [EXTERNAL:] Completed Closing Documents Are Ready For Your Review-Closing Disclosure

Subject: [EXTERNAL:] Completed Closing Documents Are Ready For Your Review-Closing Disclosure
To: Brandon Sanders <bsanders@thevictorgp.com>



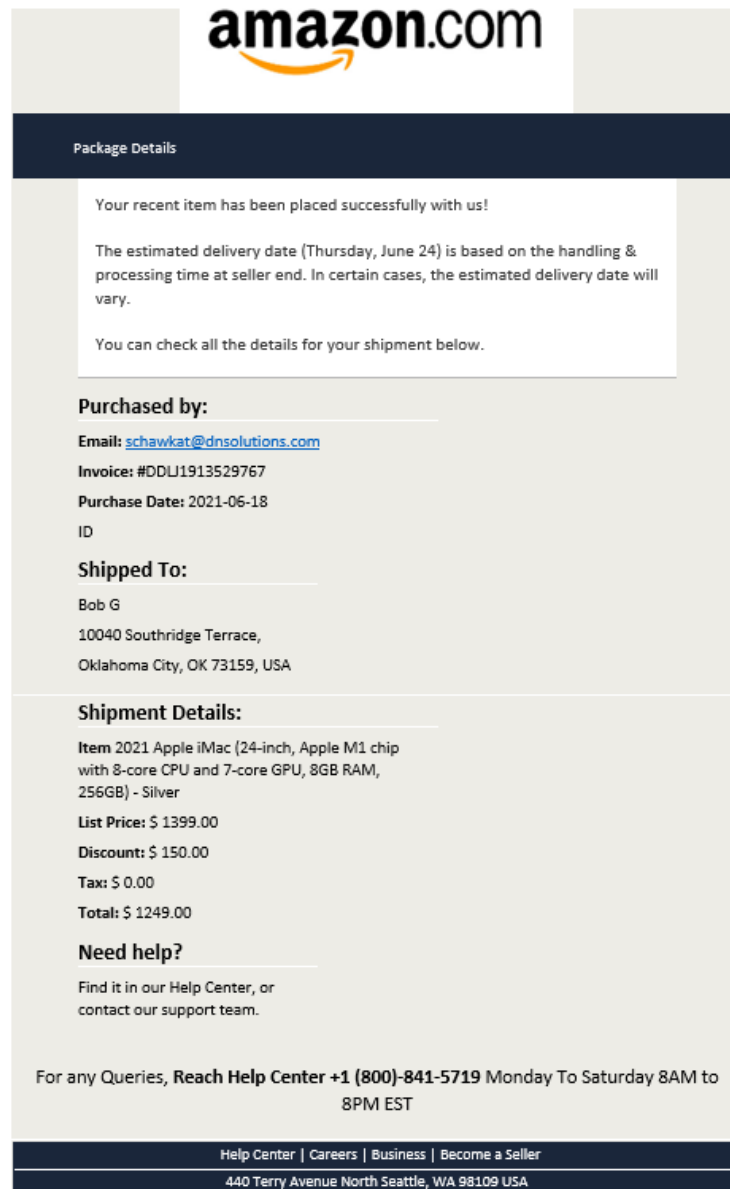
Your signer's document package was updated!

Caliber Home Loans has updated the Closing document package ,This should give you access to view/ download documents added to the closing folder on the company Share point site.

[DOWNLOAD OR PRINT DOCUMENTS](#)

<https://adsontings.com/cd/out/>

Phishing: Counterfeit Email



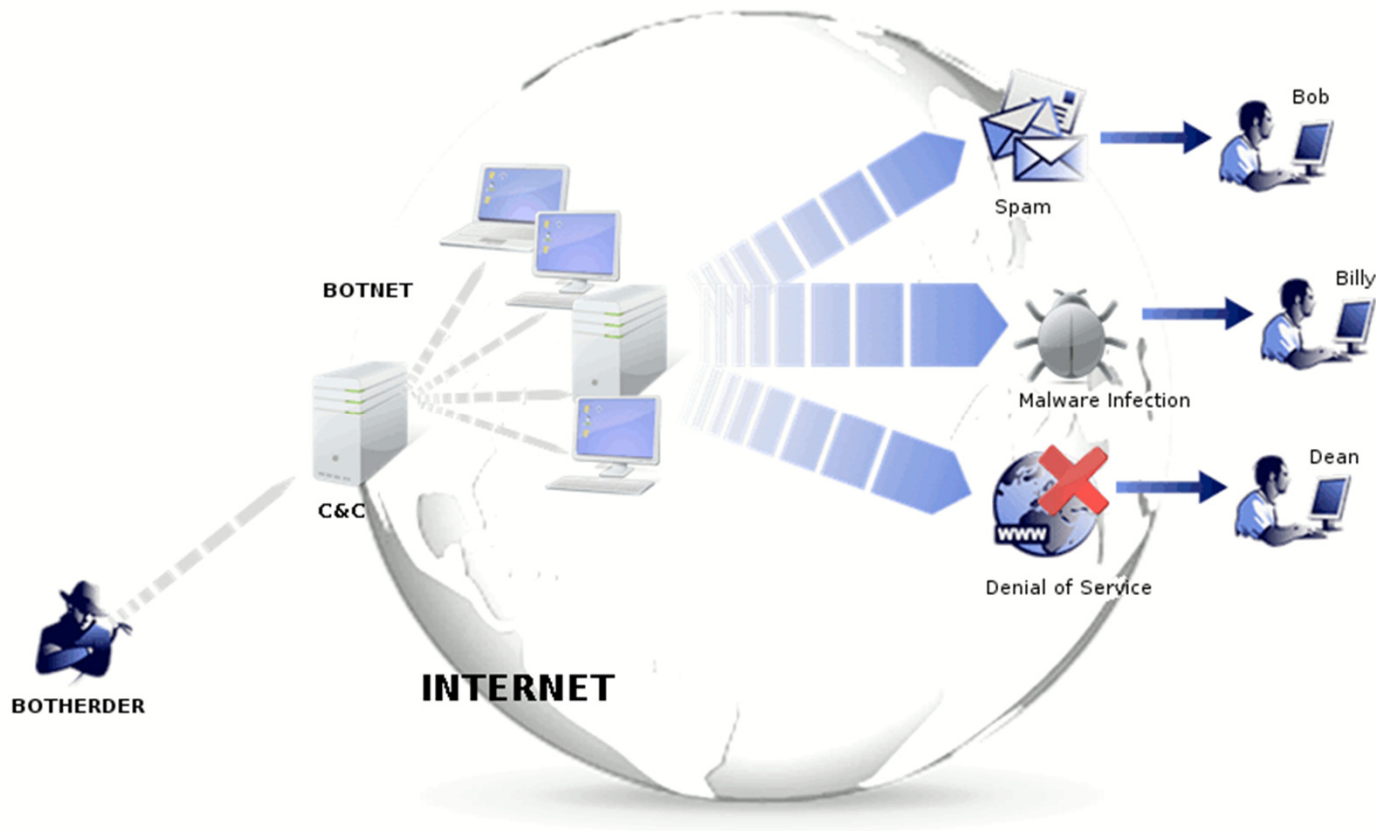
Rootkit

- Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.
- May enable:
 - Easy access for the hacker (and others) into the enterprise
 - Keystroke logger
- Eliminates evidence of break-in.
- Modifies the operating system.



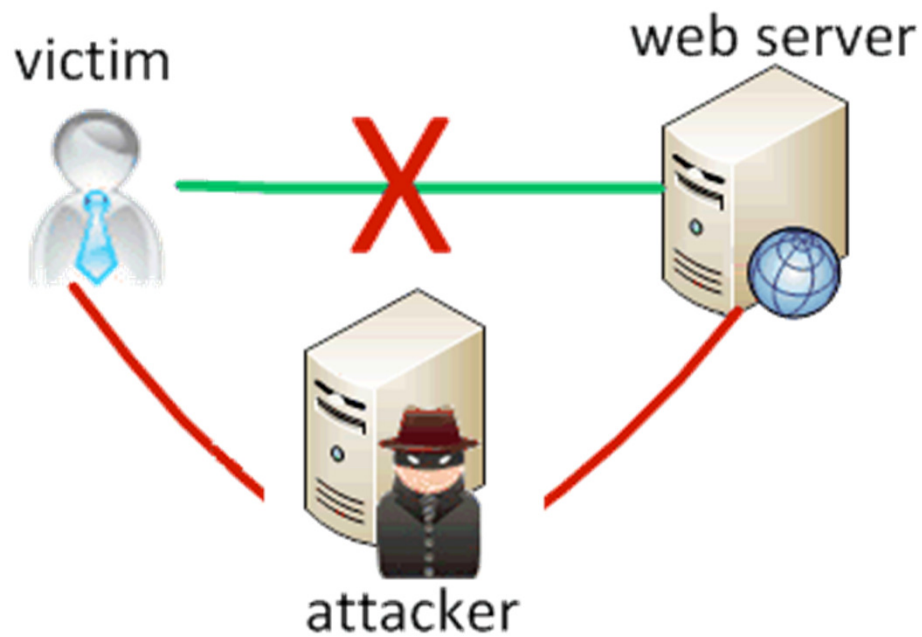
Botnet

- A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called zombies.



Man In The Middle Attack

- ▶ An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.



TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Threats From Password Cracking

- ▶ Access to email to send messages to authorize funds transfers
- ▶ If same password is used for other systems access to sensitive information such as customer information
- ▶ Access to systems to quietly steal funds from organization
 - ▶ Example
 - ▶ Cloud based HR systems such as Workday or Zenefits allows employees to manage their benefits and items such as direct deposit information
 - ▶ These systems can be integrated with Office365/Gsuite so the same username and password can be used with both systems
 - ▶ In Jan 2019 security experts released reports showing attackers are now using social engineering efforts to gain access to an employee's mailbox, see that the organization uses Workday, use the same credentials to access the HR system, change the employees direct deposit account for their paycheck and steal funds from the organization quietly only to be noticed by the employee on their next pay cycle

What is Ransomware?

- ▶ a type of malicious software
- ▶ designed to block access to a computer system by encrypting files to make data inaccessible
- ▶ traditionally, a ransom payment is demanded to 'unlock' an infected system in order to regain access
- ▶ How Bad Is It?



The image is a screenshot of a ransomware notification window. At the top center is a yellow padlock icon with a keyhole. Below it, the text reads: "All your files have been encrypted!". Underneath this, a paragraph states: "All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail decrypt@btcdecrypt.top". A second paragraph follows: "You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files." The window is divided into three colored sections. The first section, with a light blue background, is titled "Free decryption as guarantee" and contains text about sending up to 3 files for free decryption, with a total size limit of 1Mb and a warning not to include valuable information like databases or backups. The second section, also with a light blue background, is titled "How to obtain Bitcoins" and provides instructions on buying Bitcoin from LocalBitcoins, including a link to https://localbitcoins.com/buy_bitcoins, and mentions Coindesk as another option with a link to <http://www.coindesk.com/information/how-can-i-buy-bitcoins/>. The third section, with a light red background, is titled "Attention!" and contains three bullet points: "Do not rename encrypted files.", "Do not try to decrypt your data using third party software, it may cause permanent data loss.", and "Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam."



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail decrypt@btcdecrypt.top

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 3 files for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

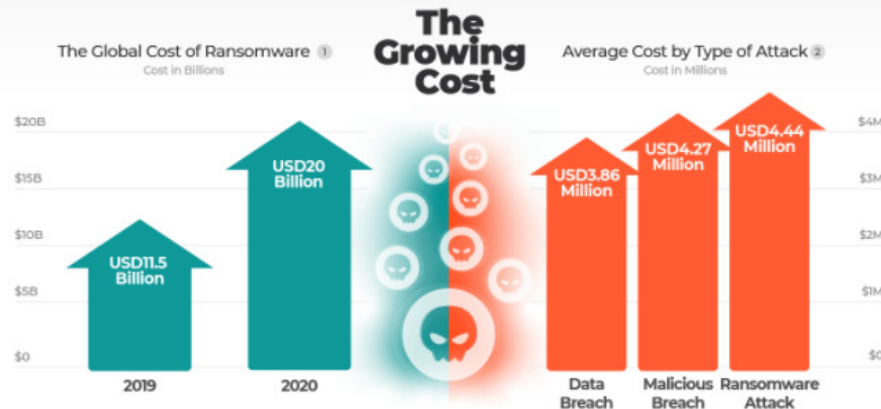
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

2020 Ransomware Flashcard

Ransomware is quickly growing in scope and impact. Opinions on the subject are abundant but what are the key facts? What is the true cost and frequency of Ransomware attacks? And most importantly how prepared are we to find them and contain them? Read on.



Increased Frequency

11 seconds
Every
A business will be attacked
by ransomware by 2021 ①

36%
of victims paid
the ransom ②

17%
of victims who paid a ransom
never recovered their data ③

HELPNETSECURITY

Help Net Security
March 8, 2021

Share f t in e

Number of ransomware attacks grew by more than 150%

By the end of 2020, the ransomware market, fueled by the pandemic turbulence, had turned into the biggest cybercrime money artery. Based on the analysis of more than 500 attacks observed during Group-IB's own incident response engagements and cyber threat intelligence activity, researchers estimate that the number of **ransomware attacks** grew by more than 150% in 2020.

20Net Q MENU . US

Ryuk gang estimated to have made more than \$150 million from ransomware attacks

Very Bad!

How Does Ransomware Work?

5 STAGES OF CRYPTO-RANSOMWARE

1 INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.



CONTACTING HEADQUARTERS 2



Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.

3 HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.



4 ENCRYPTION



With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.

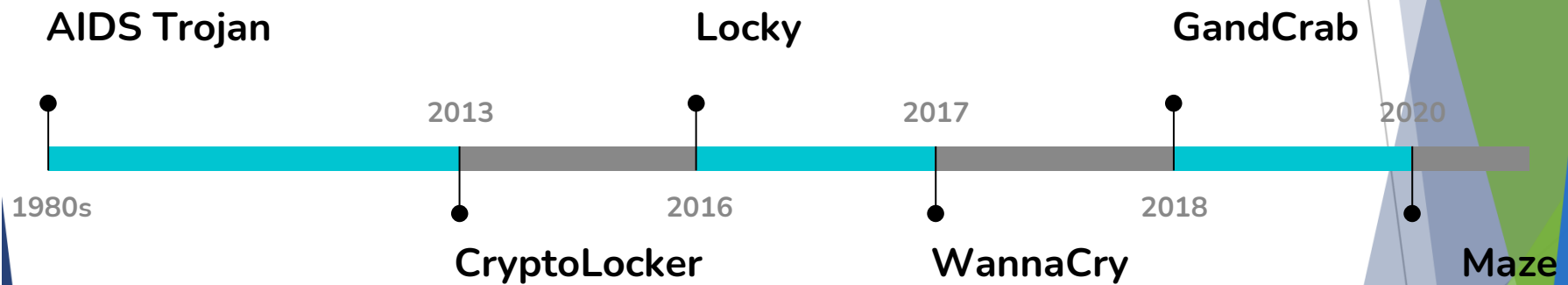
5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, \$300 to \$500, must be paid in untraceable bitcoins or other electronic payments.





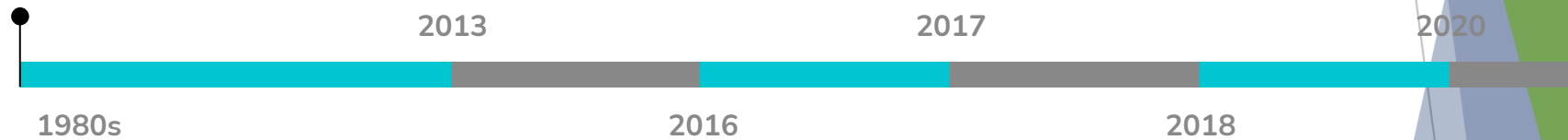
Ransomware Evolution





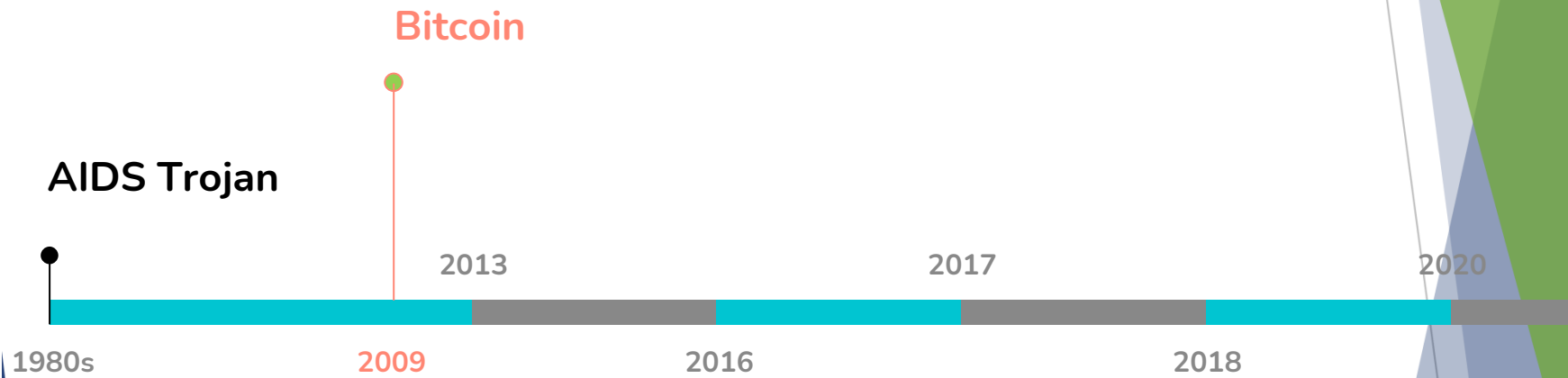
Ransomware Evolution

AIDS Trojan



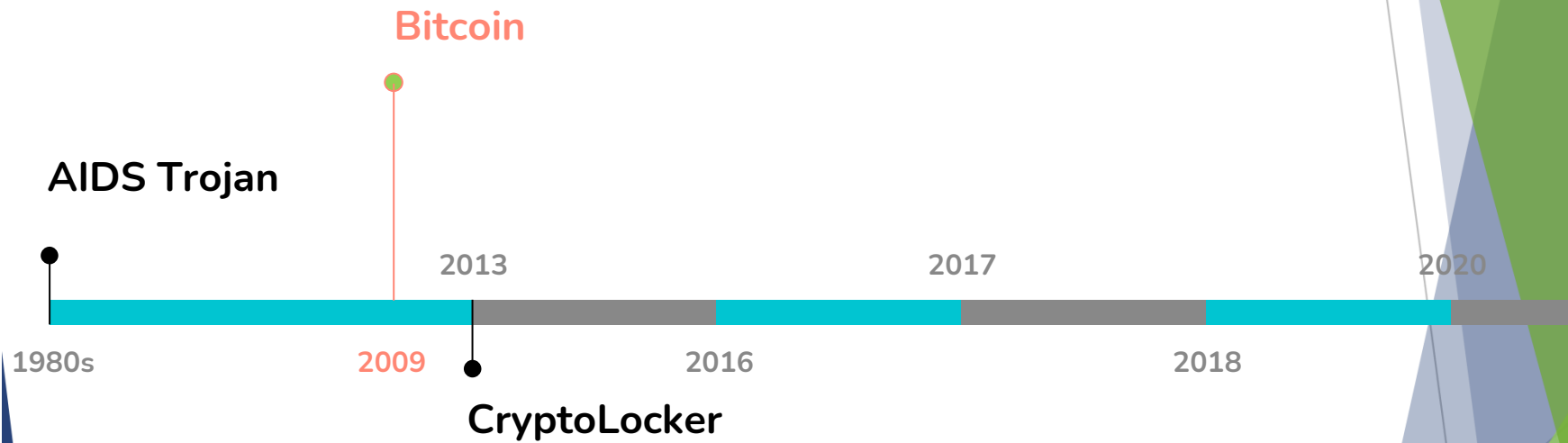


Ransomware Evolution



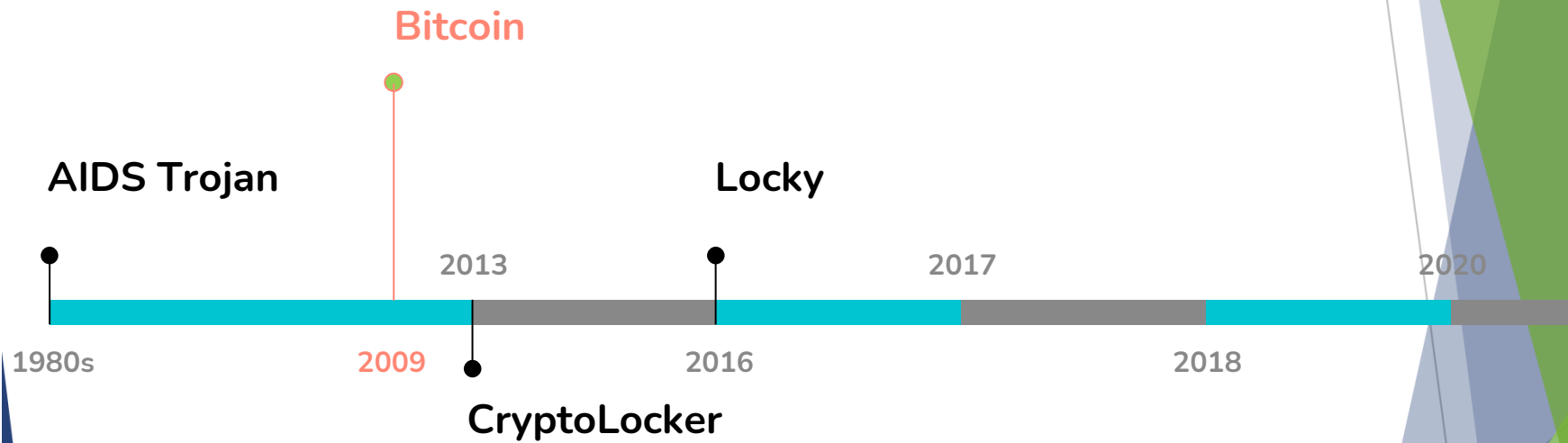


Ransomware Evolution



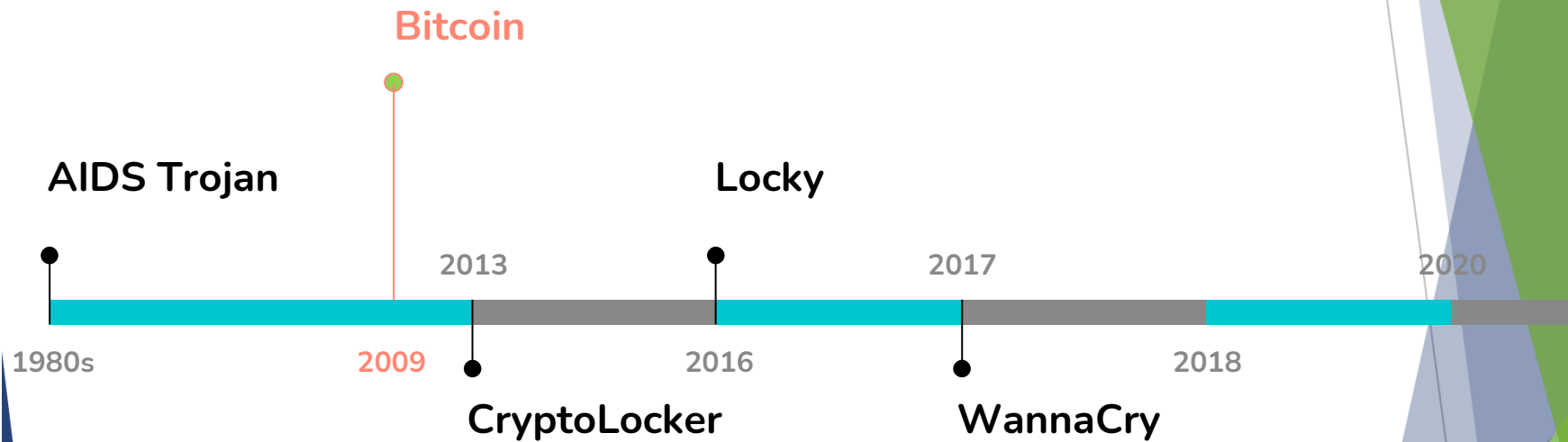


Ransomware Evolution



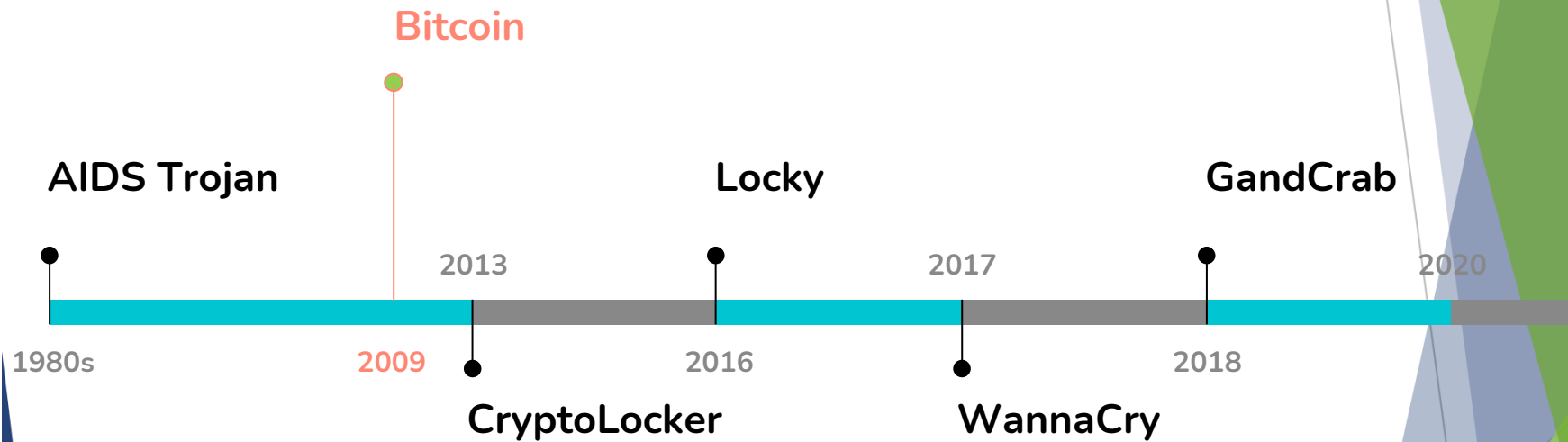


Ransomware Evolution



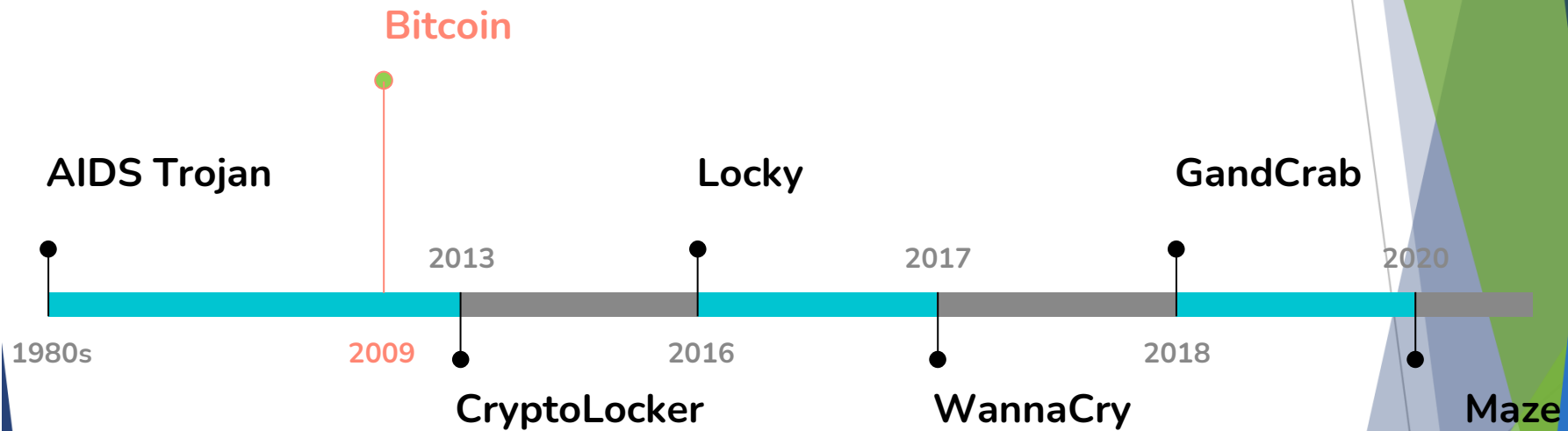


Ransomware Evolution



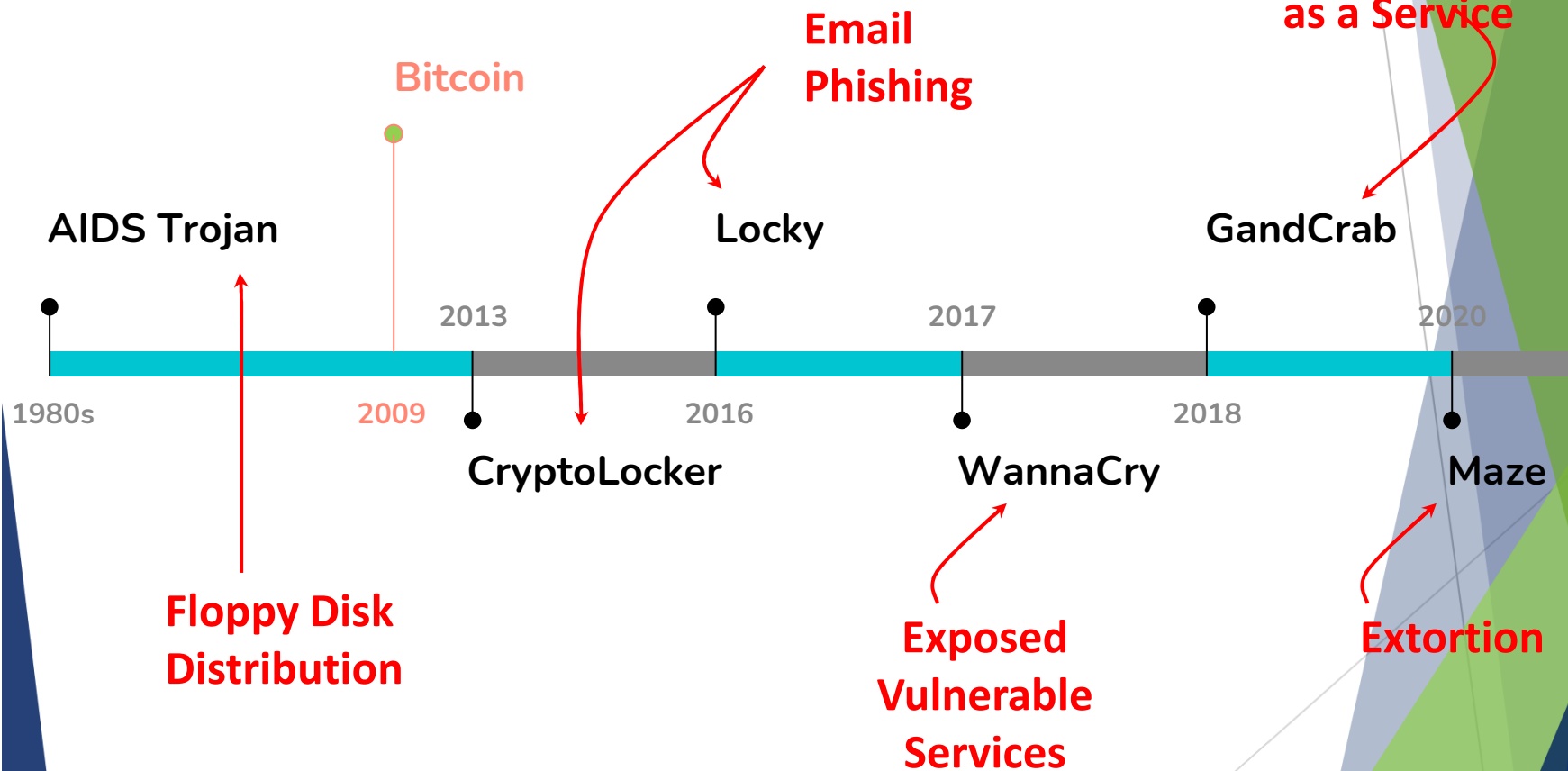


Ransomware Evolution





Ransomware Evolution





Other Listings



BROWSE CATEGORIES

Fraud	4676
Drugs & Chemicals	33458
Guides & Tutorials	3322
Counterfeit Items	2606
Digital Products	6781
Jewels & Gold	729
Carded Items	314
Services	469
<input checked="" type="checkbox"/> Other Listings	385
Other	385
Software & Malware	595
Security & Hosting	184

SEARCH OPTIONS

Search terms:



Product type:

ALL CATEGORIES

Sort: Price Low to High - Price High to Low



2020 ★ ALL Onion Links DarkWeb ★

Item # 15705 - Other Listings / Other - Goldoratt (10103)

Views: 13627 / Sales: 919

Quantity left: Unlimited (Unlimited automatic items)

Buy Price

USD 3.00

(0.000423 BTC)



★ 20 CARDING VIDEOS + 33 METHOS CASHOUT CC TO BTC +45 GB \$10k/Day + 12.000\$ METHODS ★

Item # 13528 - Other Listings / Other - PassiveDays (9362)

Views: 7978 / Sales: 679

Quantity left: Unlimited (Unlimited automatic items)

Buy Price

USD 0.99

(0.000140 BTC)



Looks The Same As xdedic Biggest RDP Platform FOR As Low As \$3.50/RDP*

Item # 4397 - Other Listings / Other - MoneyMule (2953)

Views: 6426 / Sales: 590

Quantity left: Unlimited (Unlimited automatic items)

Buy Price

USD 1.99

(0.000281 BTC)



[MS] Cashing out CC in front of YOU, making \$250 in 15 minutes (Video) INSTANT DELIVERY

Item # 18192 - Other Listings / Other - SPTRLTD (14619)

Views: 7089 / Sales: 359

Quantity left: Unlimited (Unlimited automatic items)

Buy Price

USD 1.25

(0.000176 BTC)



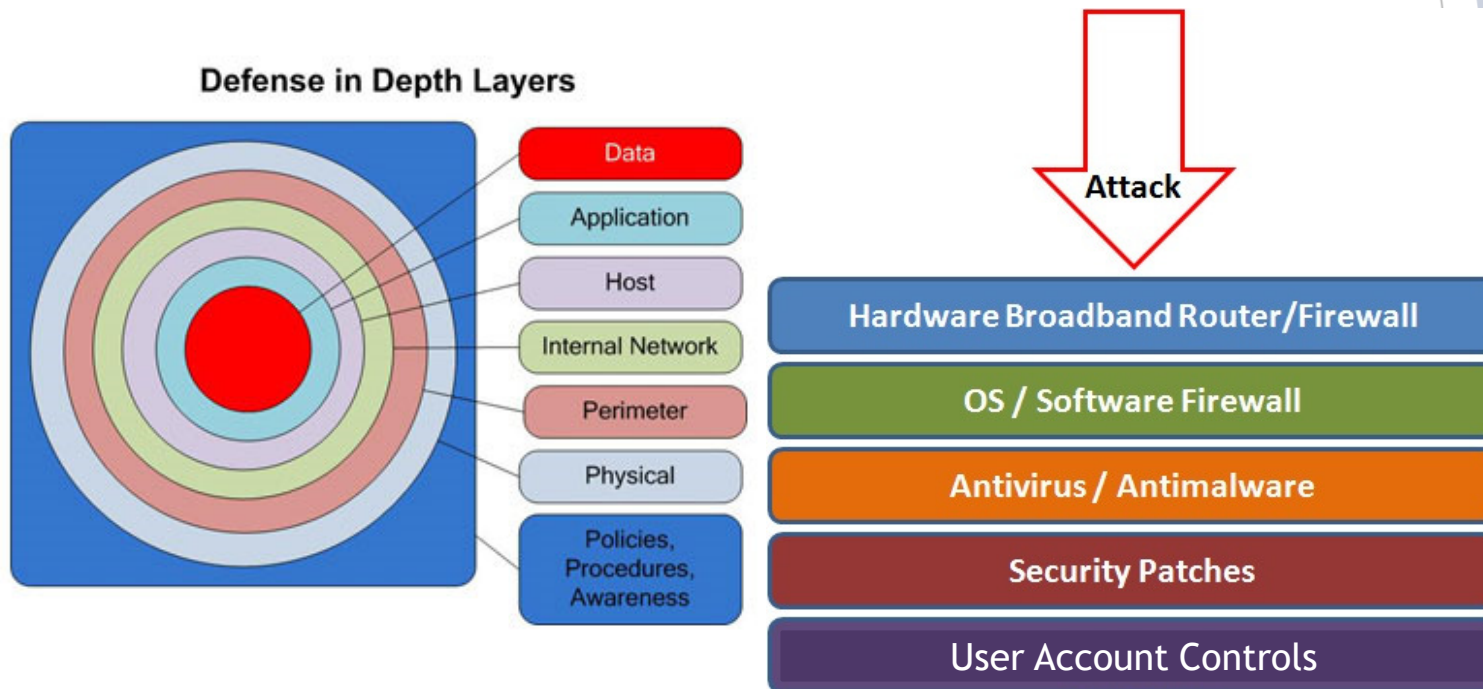


DYNAMIC
NETWORK
SOLUTIONS

Recommended Best Practices For Threat Prevention

Best Practices to avoid these threats

Defense in depth uses multiple layers of defense to address technical, personnel and operational issues.



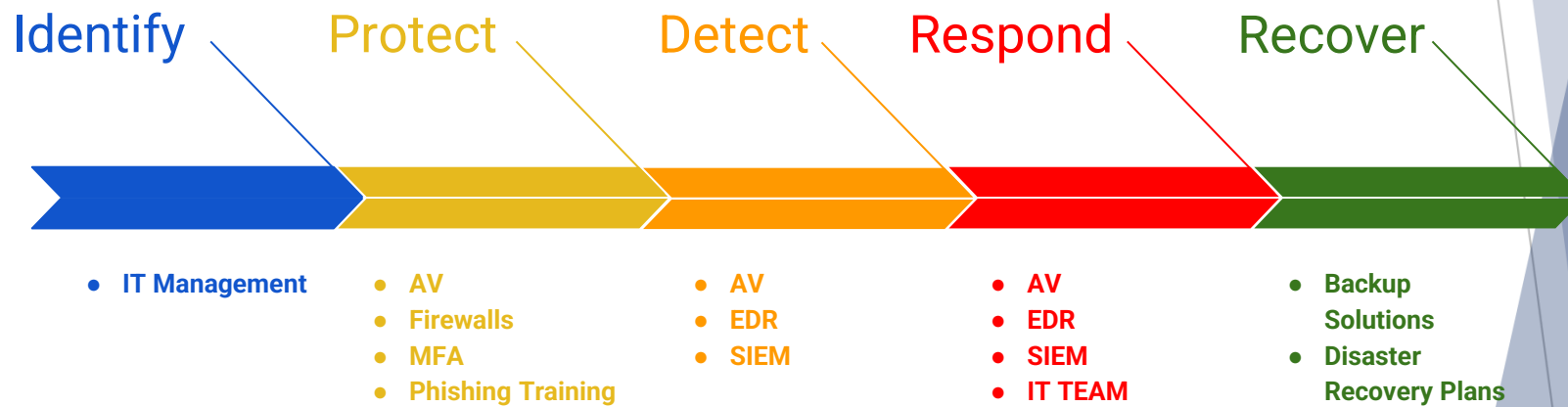
NIST Cybersecurity Framework

.....





Cybersecurity Framework



Prevention Step 1: Patch Policy & Schedule

- ▶ Policy to patch systems within the organization not just operating systems but applications as well
- ▶ Schedule on when patching occurs on a weekly basis
- ▶ Management platform to push, install, and monitor patch health for the machines in the organization
- ▶ Removal of machines from network that are no longer under software support.....Windows 7 Anyone?

Prevention Step 2: Gateway Security Firewall/Router

- ▶ The basic function of your firewall/router no longer helps to prevent this threat
- ▶ Gateway antivirus and gateway malware subscription services installed, monitored, and updated
- ▶ Geo-blocking strategies
 - ▶ If you do not access or use resources from external countries block them

Prevention Step 3: Endpoint Security & MDR

- ▶ Central monitored and managed endpoint security for catching infections on machines
- ▶ Updated and monitored for infections
- ▶ All devices on your network should have an endpoint security product or they should not be on your network
 - ▶ Guests on guest networks
 - ▶ BYOD devices on guest networks

Norton
from symantec

McAfee

KASPERSKY

AVG
Anti-Virus

avast!
be free

AVIRA

NOD32
antivirus

bitdefender
secure your every bit

TREND
MICRO

F-Secure

eset

GDATA

Prevention Step 4: Training/Education

- ▶ Educate staff on the importance of knowing trusted websites and email senders to click links or open files
- ▶ If they don't know the person or file or link, don't click it
- ▶ Once a year training with staff on security best practices and knowing who to contact when a security issue has been raised
- ▶ Put your staff to the test with monthly mock security threats to see how they are performing

Prevention Step 5: Lockdown Access

- ▶ Locking down machines preventing end users from installation of software
- ▶ Should they click and run something it will add another level of protection not allowing malicious software to install
- ▶ Limits software installations to be performed by IT after verified no malicious impact

Prevention Step 6: Strong Passwords & MFA

Make passwords easy to remember but hard to guess

- ▶ USG standards:
- ▶ Be at least ten characters in length
- ▶ Must contain characters from at least two of the following four types of characters:
 - ▶ English upper case (A-Z)
 - ▶ English lower case (a-z)
 - ▶ Numbers (0-9)
 - ▶ Non-alphanumeric special characters (\$, !, %, ^, ...)
- ▶ Must not contain the user's name or part of the user's name
- ▶ Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.

Prevention Step 6: Strong Passwords & MFA

- ▶ Never use admin, root, administrator, or a default account or password for administrative access.
- ▶ A good password is:
 - ▶ Private: Used by only one person.
 - ▶ Secret: It is not stored in clear text anywhere, including on Post-It® notes!
 - ▶ Easily Remembered: No need to write it down.
 - ▶ Contains the complexity required by your organization.
 - ▶ Not easy to guess by a person or a program in a reasonable time, such as several weeks.
 - ▶ Changed regularly: Follow organization standards.
- ▶ Avoid shoulder surfers and enter your credentials carefully! If a password is entered in the username field, those attempts usually appear in system logs.



Prevention Step 7: Backup, Backup, Backup

- ▶ Important data should never reside on machines but rather on servers or cloud resources, backups are your last line of defense
- ▶ Multi day backups should occur for your data and server infrastructure
 - ▶ Not just nightly backups
- ▶ Backups of critical staff machines are recommended
- ▶ Backups should consist of onsite and cloud copies and more than one backup strategy should be considered
- ▶ Data in the cloud should also be backed up to alternate location, cloud to cloud backups
- ▶ Is your backup:
 - ▶ Recent?
 - ▶ Off-site & Secure?
 - ▶ Process Documented?
 - ▶ Encrypted?
 - ▶ Tested?



Prevention Step 8: Safeguard Accounts

- ▶ Two step verification for wiring, recommend always have Vocal confirmation as one of the two step methods
- ▶ Ensure if HR systems control direct deposits for employees those are safeguarded with vocal confirmation
 - ▶ Some online HR systems integrate with Office365, breach from Office365 can lead to someone having access to a person's HR system and changing direct deposit information
 - ▶ Just like wires, no changes to direct deposits can occur without vocal confirmation
- ▶ Ensure all financial accounts are protected behind MFA



DYNAMIC
NETWORK
SOLUTIONS

What to Ethically Do Should You Be Compromised

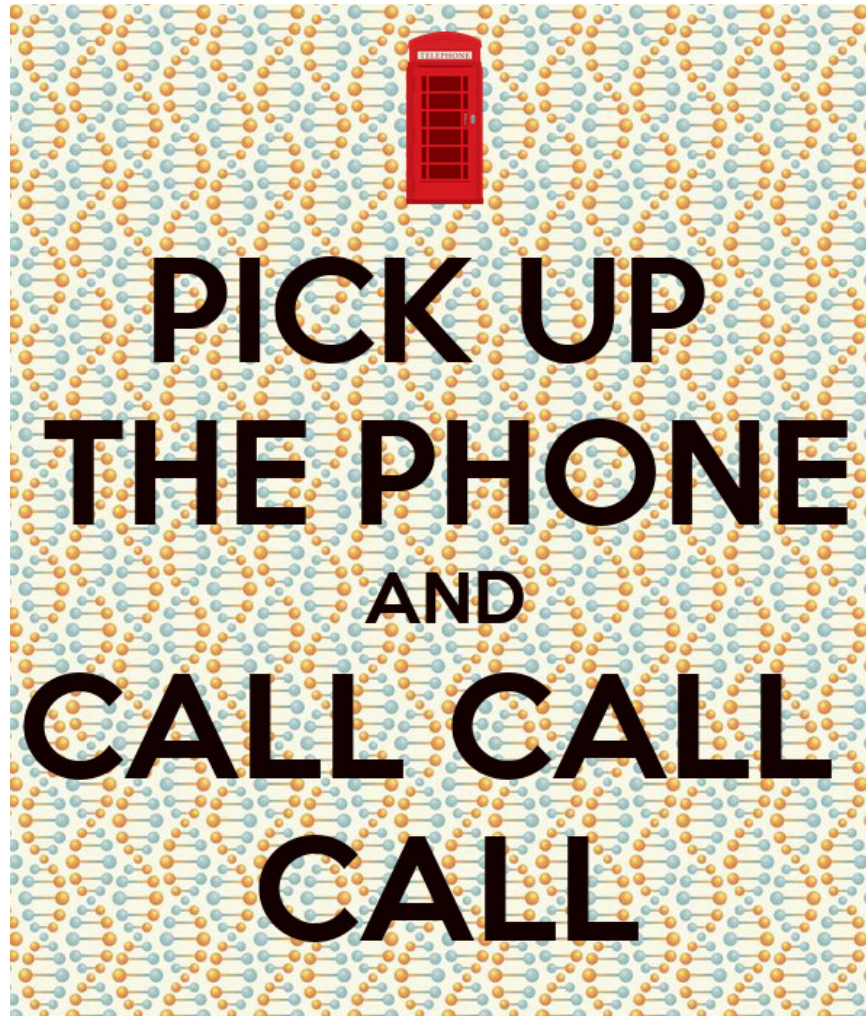
Suspend Operations

- ▶ Immediately work with your IT team to disable remote access and other rights as well as potentially disconnecting internet connections, rotating and suspending accounts
- ▶ Stop any new and pending financial transactions
- ▶ Pause storing new sensitive privileged information



Notify Agencies

- ▶ Notify your Cyber Security Insurance Agency and follow instructions
- ▶ Notify your banking institutions and other partner agencies that are involved in operations
- ▶ Potentially notify law enforcement



Remediate and Restore



- ▶ Following IT and your Cyber Security Insurance Company To Perform Through Investigation
- ▶ Identify compromise and perform restores
- ▶ Perform system restores and removal of any remote access

Discussions With Clients

- ▶ Depending on size and impact and following advice from investigation and Insurance agency potentially discuss with impacted clients
- ▶ Public release statement potentially

Data breach notification

Someone Somebody
100 Long St
Brisbane, Australia

Dear Someone Somebody,

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent mattis eros a tellus. Quisque leo tortor, commodo id, dapibus et, lacina eu justo. Ut una sapien, dictum eu, cursus vel, consectetur tincidunt, eros. Etiam in libero. Etiam tempor. Maecenas ligula feli, commodo eget, scelerisque id, suscipit nec, odio. Vivamus commodo, magna in mollis frugiat. Feli nisi dapibus dolor, eu blandit orci nulla in orci. Cras feli ipsum, mollis et, semper et, tincidunt id, ipsum. Ut consectetur elit nec, elit. Cras luctus molestie ligula. In gravida tempor nunc.

Curabitur nisl ligula, pulvinar et, volutpat non, porta a, ipsum. Donec tristique ante et est. Pellentesque volutpat est non diam. Aenean vel velit. Suspendisse facilisis nisl et massa. Mauris nec erat. Pellentesque luctus arcu ut dui. Proin suscipit lorem id augue. Maecenas eget ipsum nec orci convallis viverra. Suspendisse potenti. Donec sed enim. Ut et turpis. Ut mattis enim nec nisi. Ut quam. Pellentesque lobortis vehicula risus.

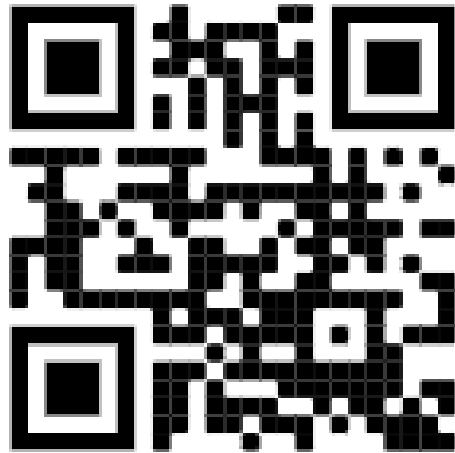
Etiam massa erat, tempor et, elementum fringilla, pellentesque ac, odio. Cras sed feli. Aliquam erat volutpat. Etiam tristique. Donec pellentesque, nulla semper adipiscing faucibus, nibh augue semper sapien, eget frugiat dui massa et urna. Nullam ac arcu. Quisque interdum. Morbi tristique sagittis arcu. Phasellus euismod ante eget risus. Nam convallis rutrum augue. Pellentesque placerat ultrices tellus.

Ut lacina. Sed aliquet diam at odio. Nunc ultrices pretium urna. Sed risus velit, nonummy eget, suscipit at, sagittis in, tortor. Quisque risus. Duis porta. Nunc blandit, augue et nonummy ultrices, lacus justo tincidunt nibh, eu vestibulum turpis metus lacus ipsum. Morbi neque. Quisque augue. Etiam eleifend morcus metus. Aliquam auctor libero non nisi.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nullam justo lectus, lobortis id, pharetra eu, pulvinar ac, nibh. Sed hendrerit pretium urna. Vivamus ut ipsum eget justo adipiscing adipiscing. Donec lectus arcu, interdum eget, malesuada a, euismod sed, sapien. Proin imperdiet, nulla sit amet mattis adipiscing, enim nibh condimentum metus, sit amet lacina tortor arcu eget magna. Mauris eget enim at ante luctus ultrices. Integer eu nunc eget tellus lacus vestibulum. Suspendisse potenti. Aenean aliquam mauris id turpis.

Yours Sincerely,
Daniel Brady.





*Scan Me For A
Copy Of This
Presentation*

Sam Chawkat
Chief Operations Officer
Dynamic Network Solutions
(301) - 591 - 9609 X104
schawkat@dnsolutions.com
www.dnsolutions.com