MLTA Maryland Land Title Association

DYNAMIC NETWORK SOLUTIONS

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.

DYNAMIC NETWORK SOLUTIONS

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

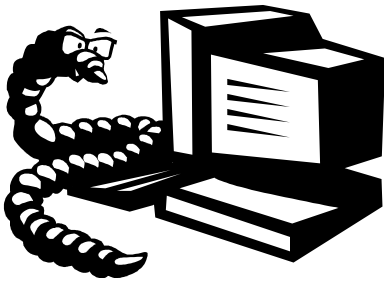
- According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
  - Web Browser
  - Email
  - Web Applications
  - Excessive User Rights

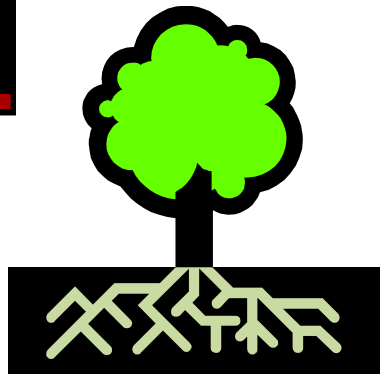
Lets Discuss The Type Of Threats That Exist

DYNAMIC NETWORK SOLUTIONS

Leading Threats

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





DYNAMIC NETWORK SOLUTIONS

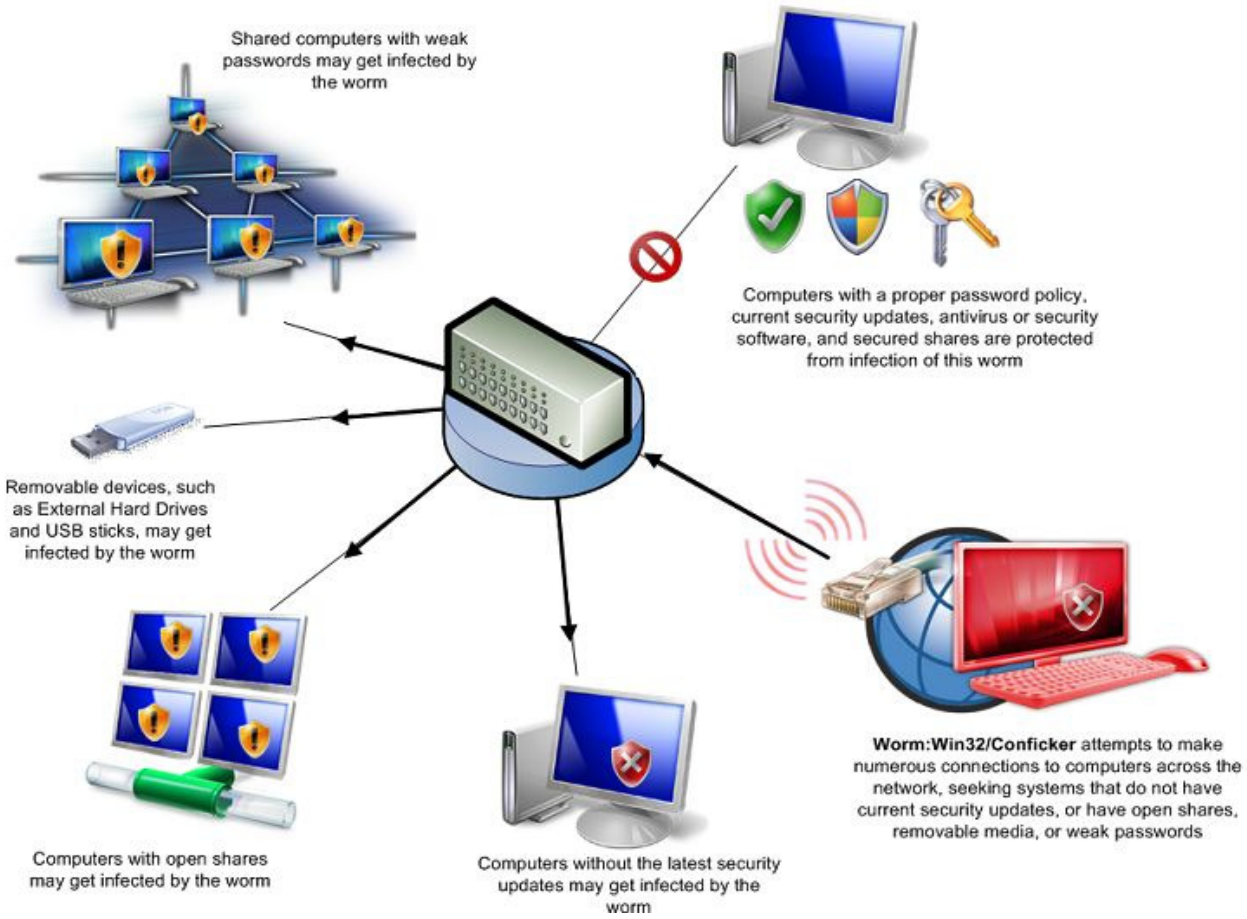
Viruses

- 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.

DYNAMIC NETWORK SOLUTIONS

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.



DYNAMIC NETWORK SOLUTIONS

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!

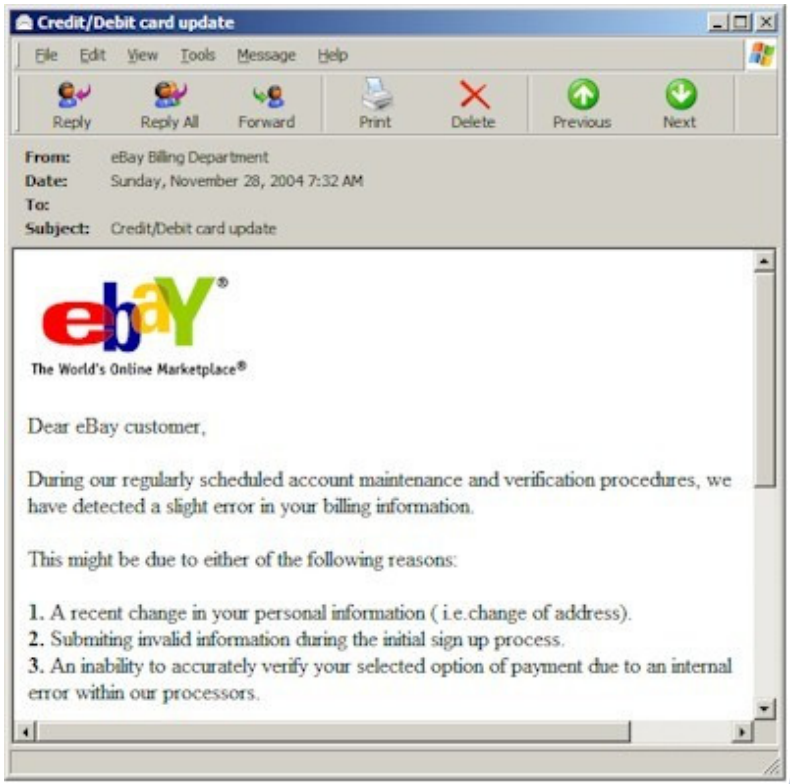
I have come to repair your machine…

DYNAMIC NETWORK SOLUTIONS

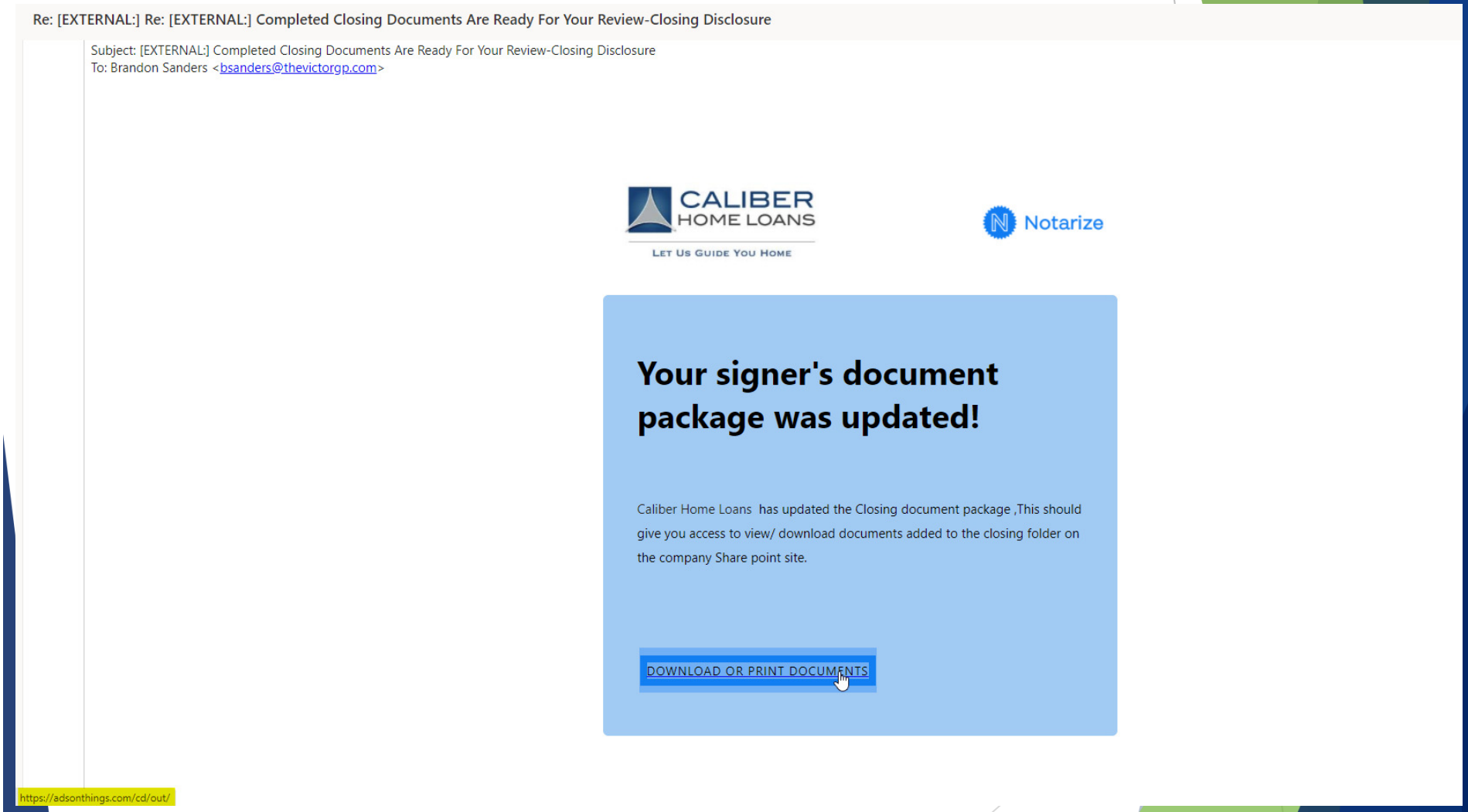
Phishing: Counterfeit Email & Documents

- A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.

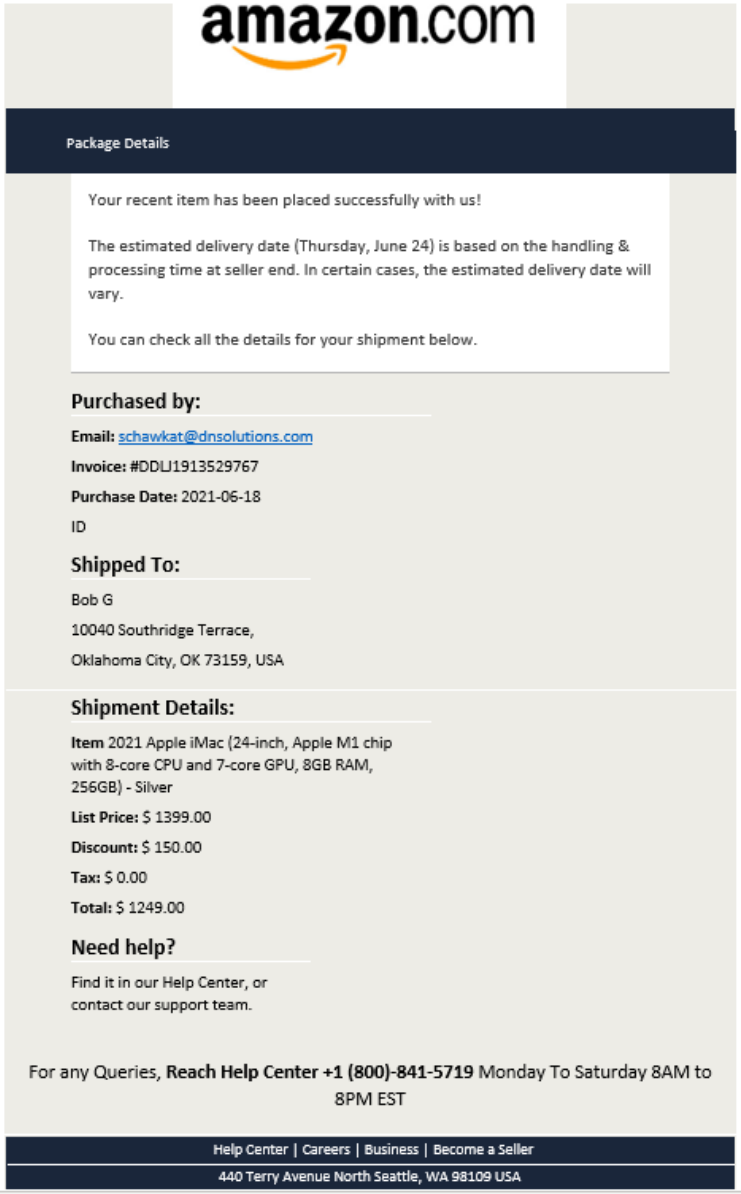
- Now legitimate resources like Office365 documents are being used to perform this and evade detection



Phishing: Counterfeit Email



Phishing: Counterfeit Email



amazon.com

Package Details

Your recent item has been placed successfully with us!

The estimated delivery date (Thursday, June 24) is based on the handling & processing time at seller end. In certain cases, the estimated delivery date will vary.

You can check all the details for your shipment below.

Purchased by:

Email: schawkat@dnsolutions.com

Invoice: #DDLJ1913529767

Purchase Date: 2021-06-18

ID

Shipped To:

Bob G

10040 Southridge Terrace,

Oklahoma City, OK 73159, USA

Shipment Details:

Item 2021 Apple iMac (24-inch, Apple M1 chip with 8-core CPU and 7-core GPU, 8GB RAM, 256GB) - Silver

List Price: $ 1399.00

Discount: $ 150.00

Tax: $ 0.00

Total: $ 1249.00

Need help?

Find it in our Help Center, or contact our support team.

For any Queries, **Reach Help Center +1 (800)-841-5719** Monday To Saturday 8AM to 8PM EST

Help Center | Careers | Business | Become a Seller

440 Terry Avenue North Seattle, WA 98109 USA

DYNAMIC NETWORK SOLUTIONS

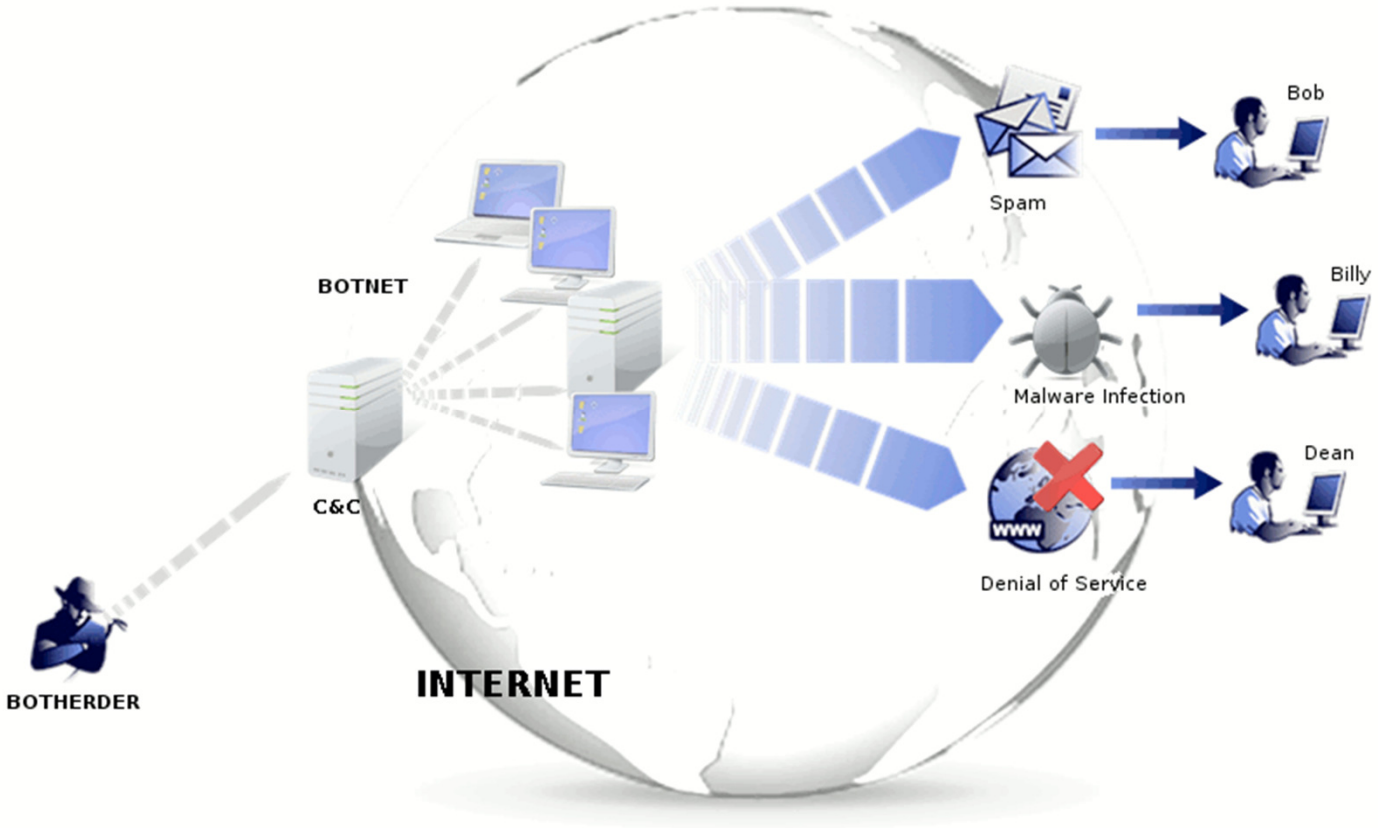
Rootkit

- 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.

DYNAMIC NETWORK SOLUTIONS

Botnet

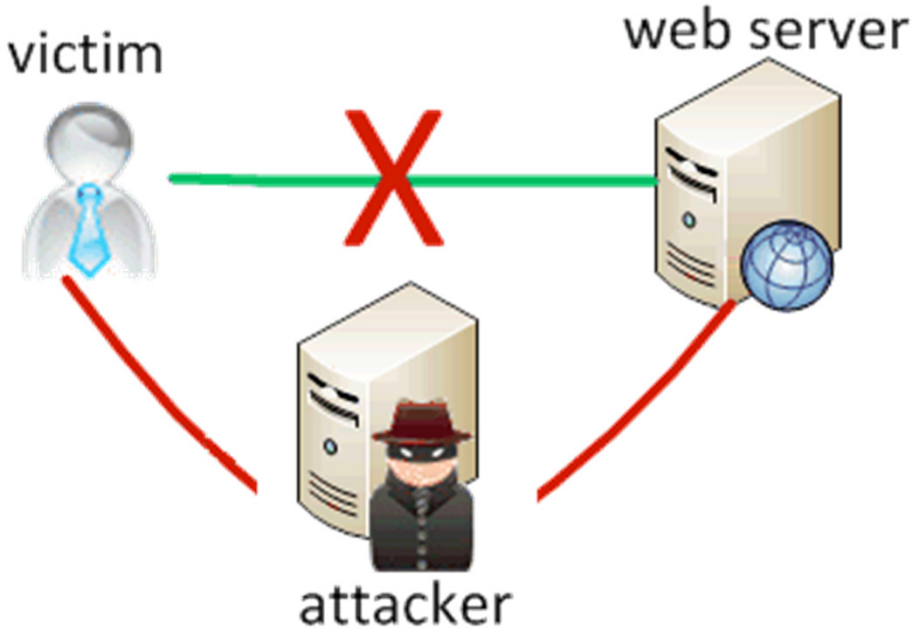
- A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called zombies.



DYNAMIC NETWORK SOLUTIONS

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.



DYNAMIC NETWORK SOLUTIONS

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

DYNAMIC NETWORK SOLUTIONS

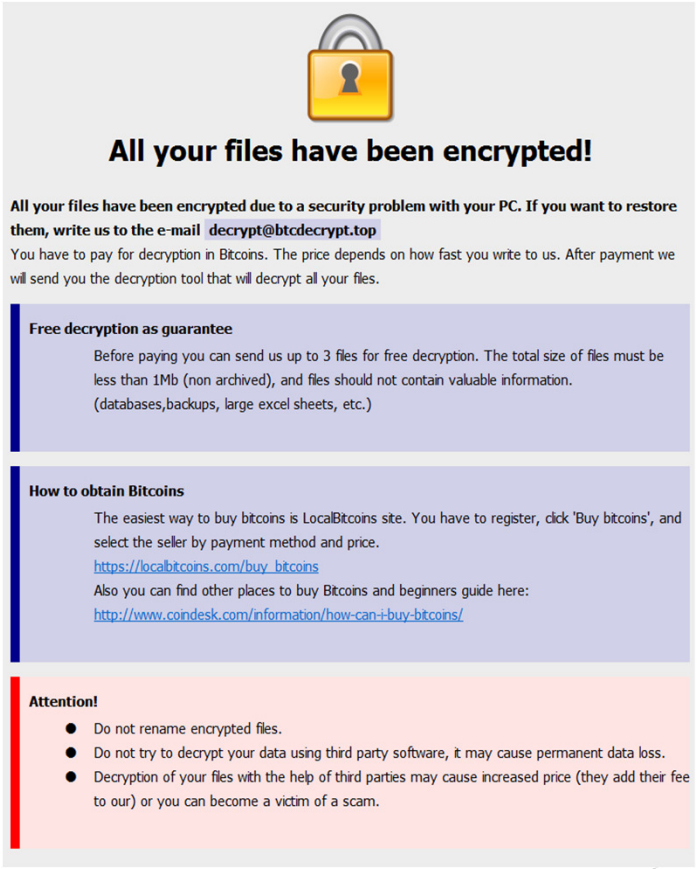
Threats From Password Cracking

- 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

DYNAMIC NETWORK SOLUTIONS

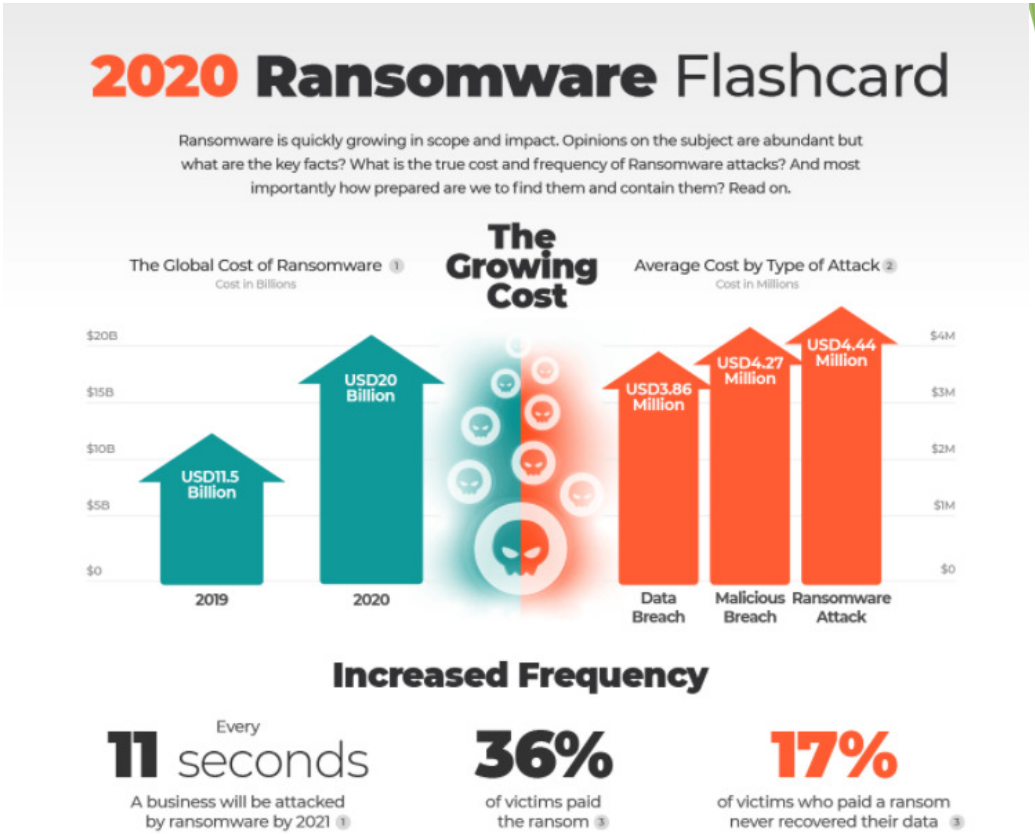
What is Ransomware?

- 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?



DYNAMIC NETWORK SOLUTIONS

Very Bad!

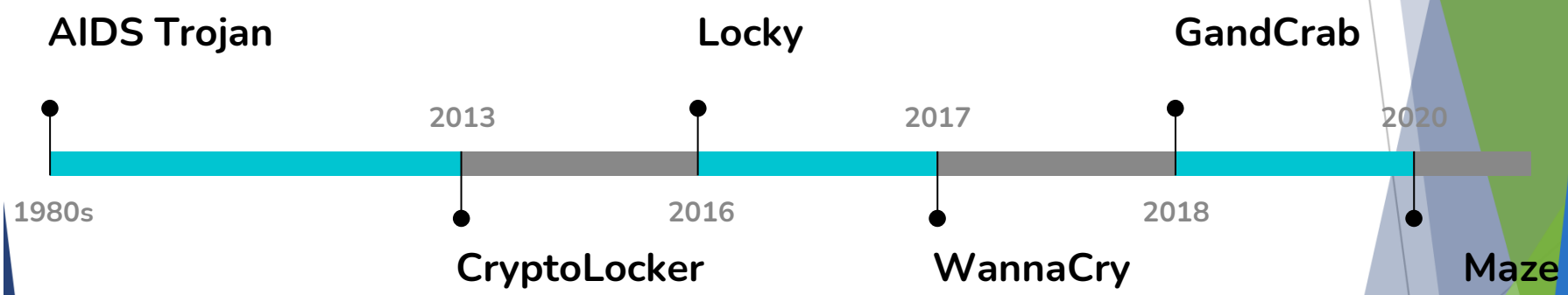


DYNAMIC NETWORK SOLUTIONS

How Does Ransomware Work?

DYNAMIC NETWORK SOLUTIONS

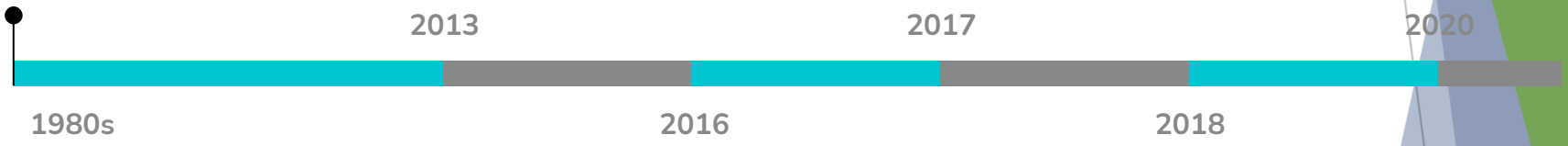
Ransomware Evolution



DYNAMIC NETWORK SOLUTIONS

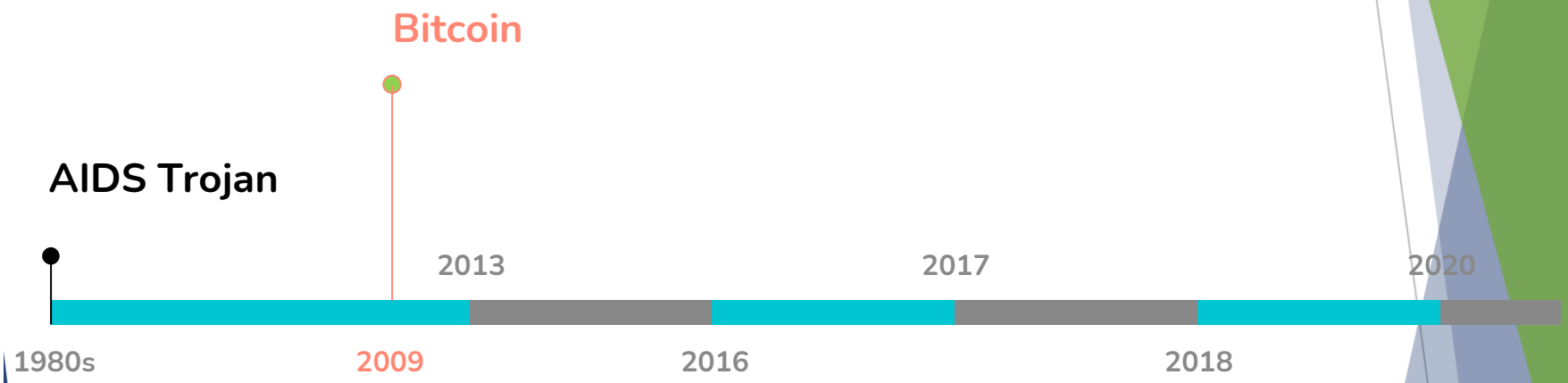
Ransomware Evolution

AIDS Trojan



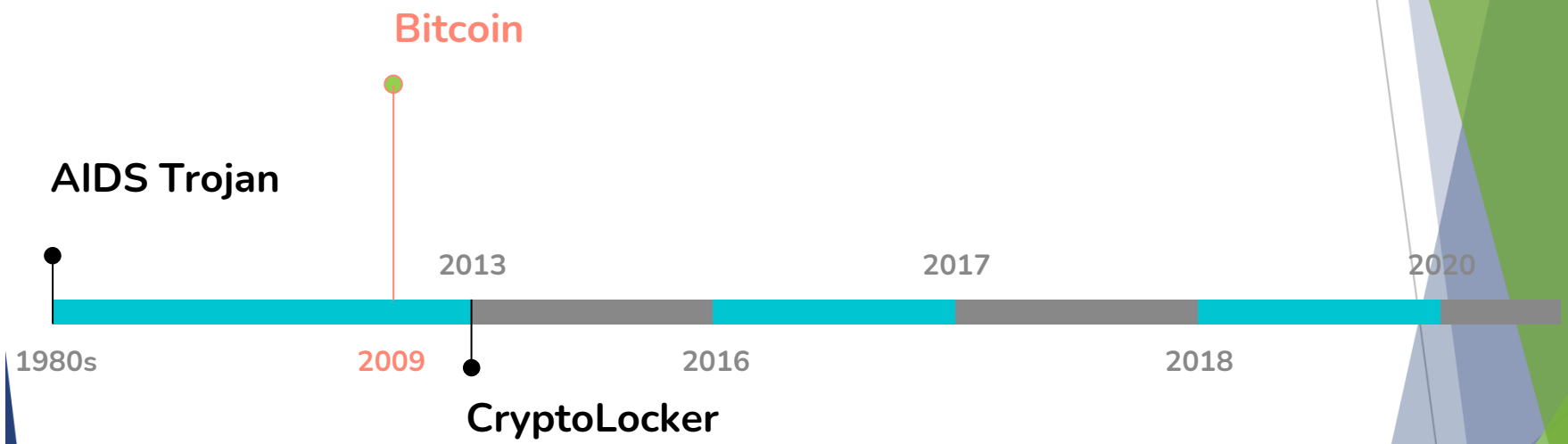
DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution



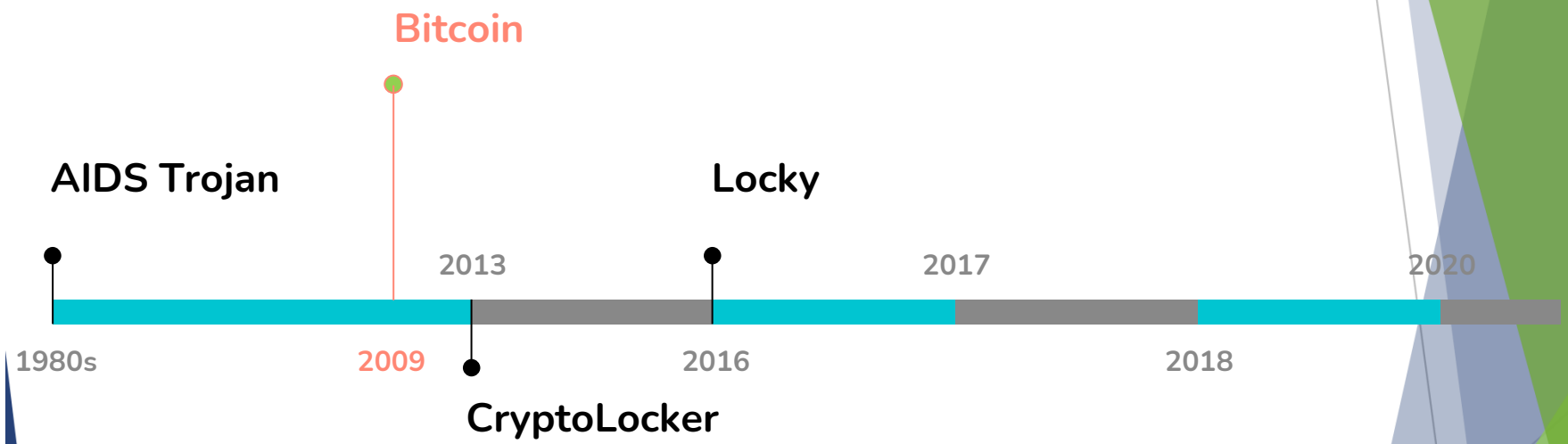
DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution



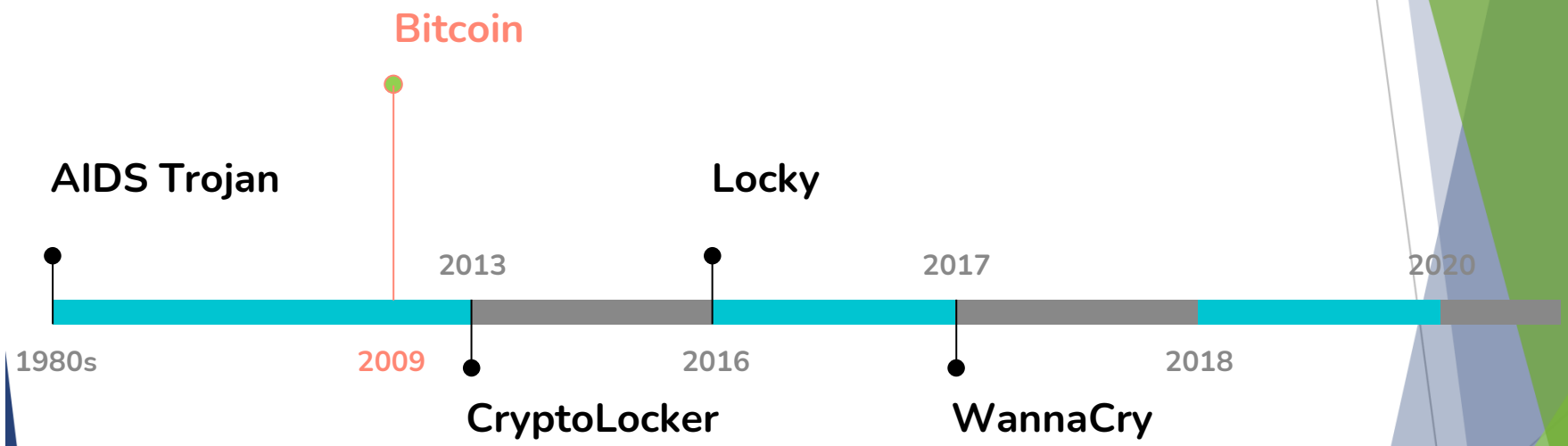
DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution



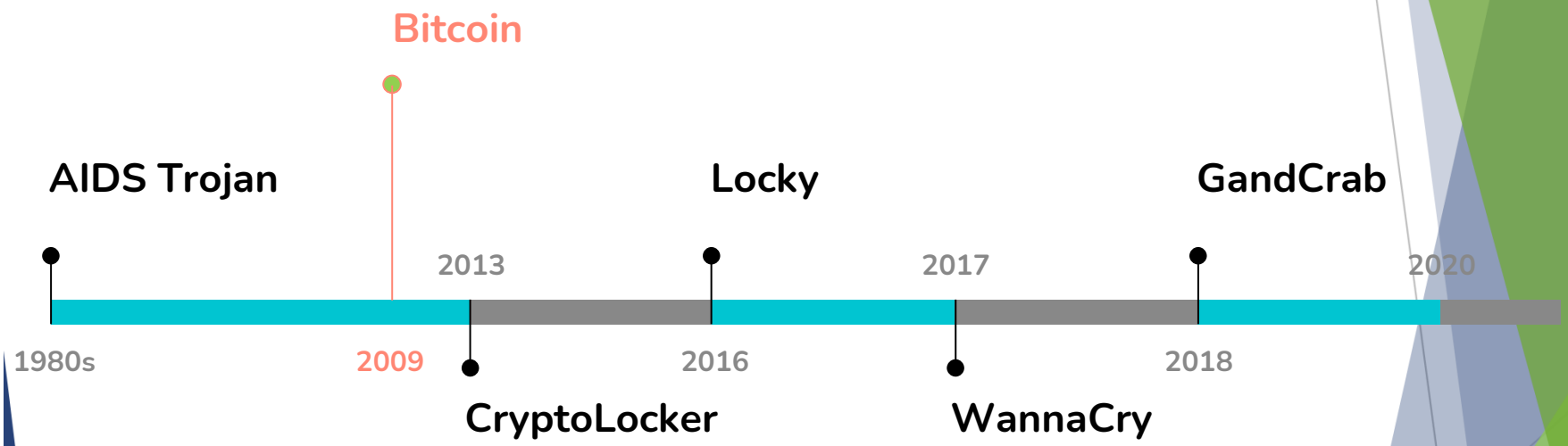
DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution



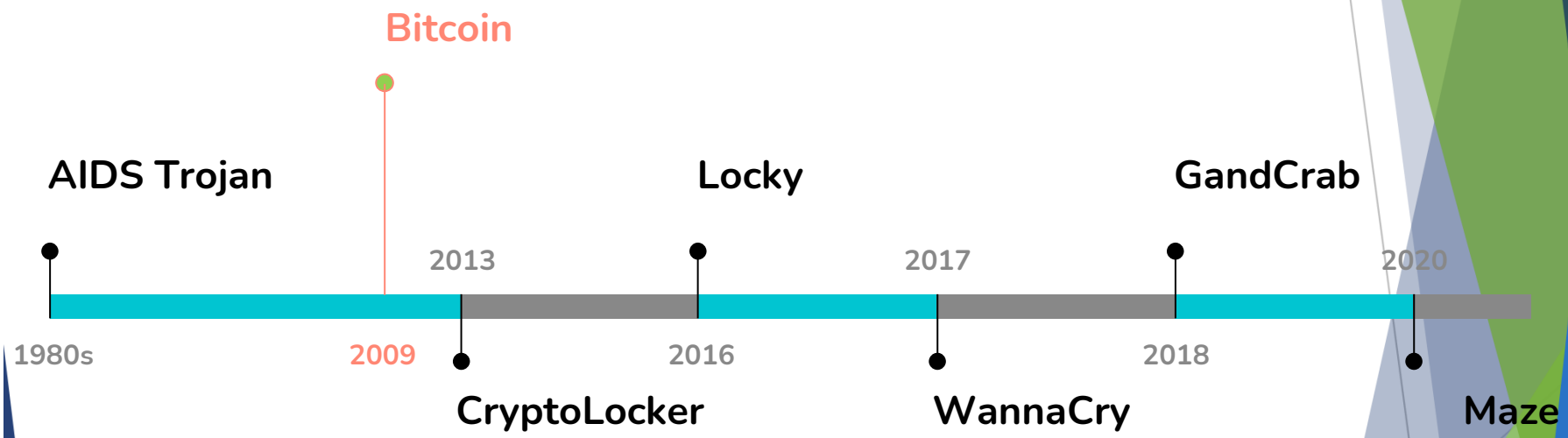
DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution



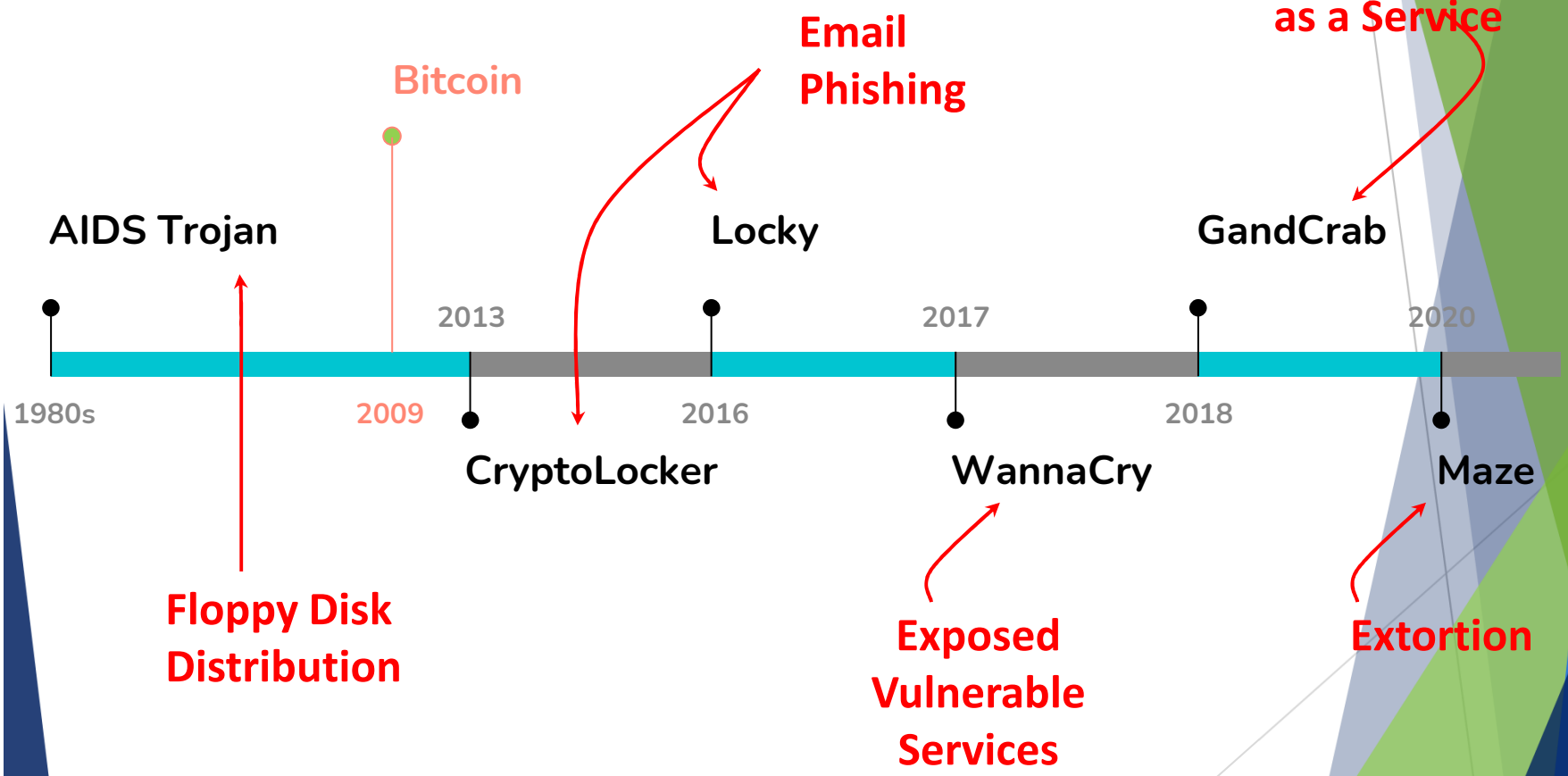
DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution

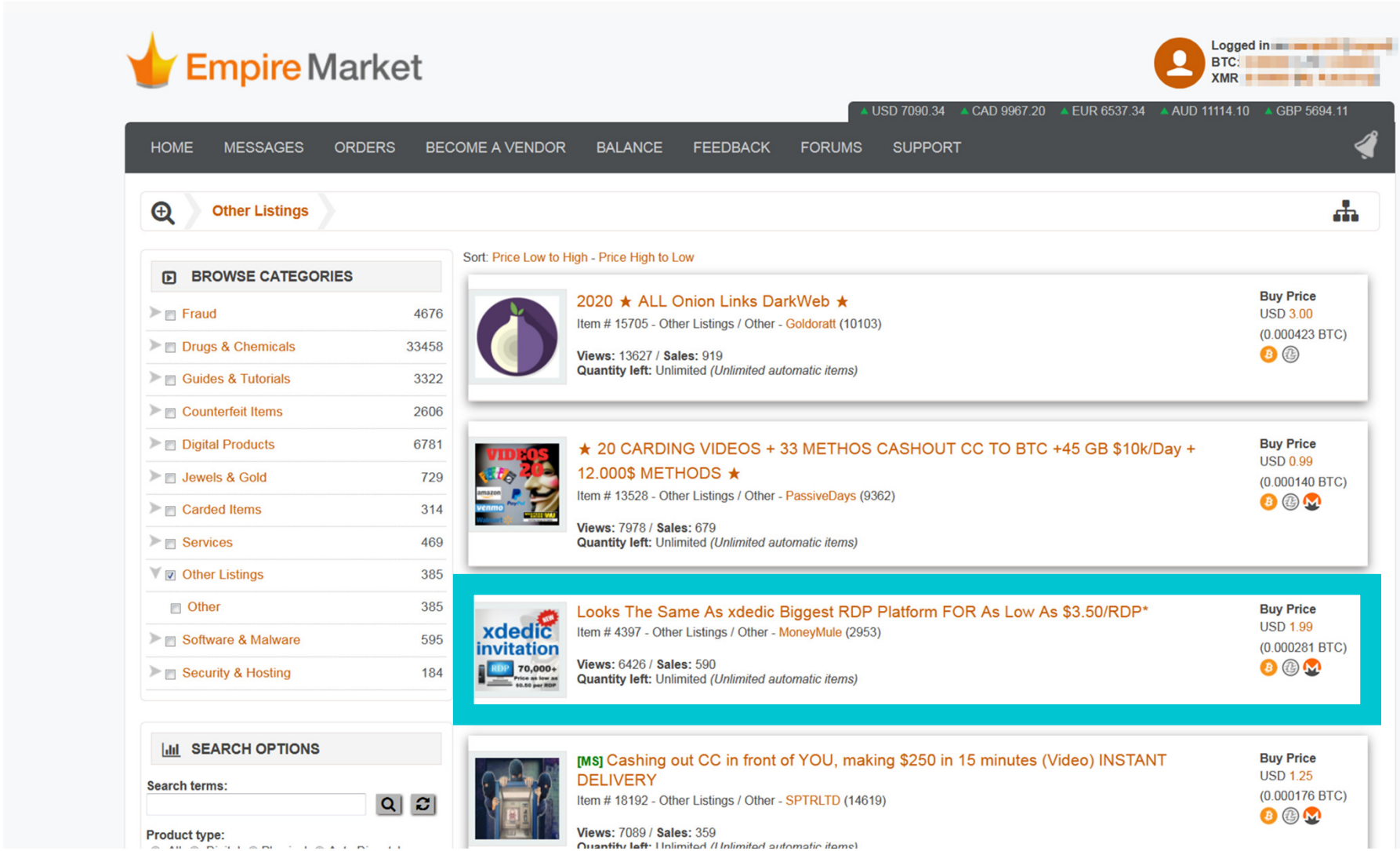


DYNAMIC NETWORK SOLUTIONS

Ransomware Evolution



DYNAMIC NETWORK SOLUTIONS

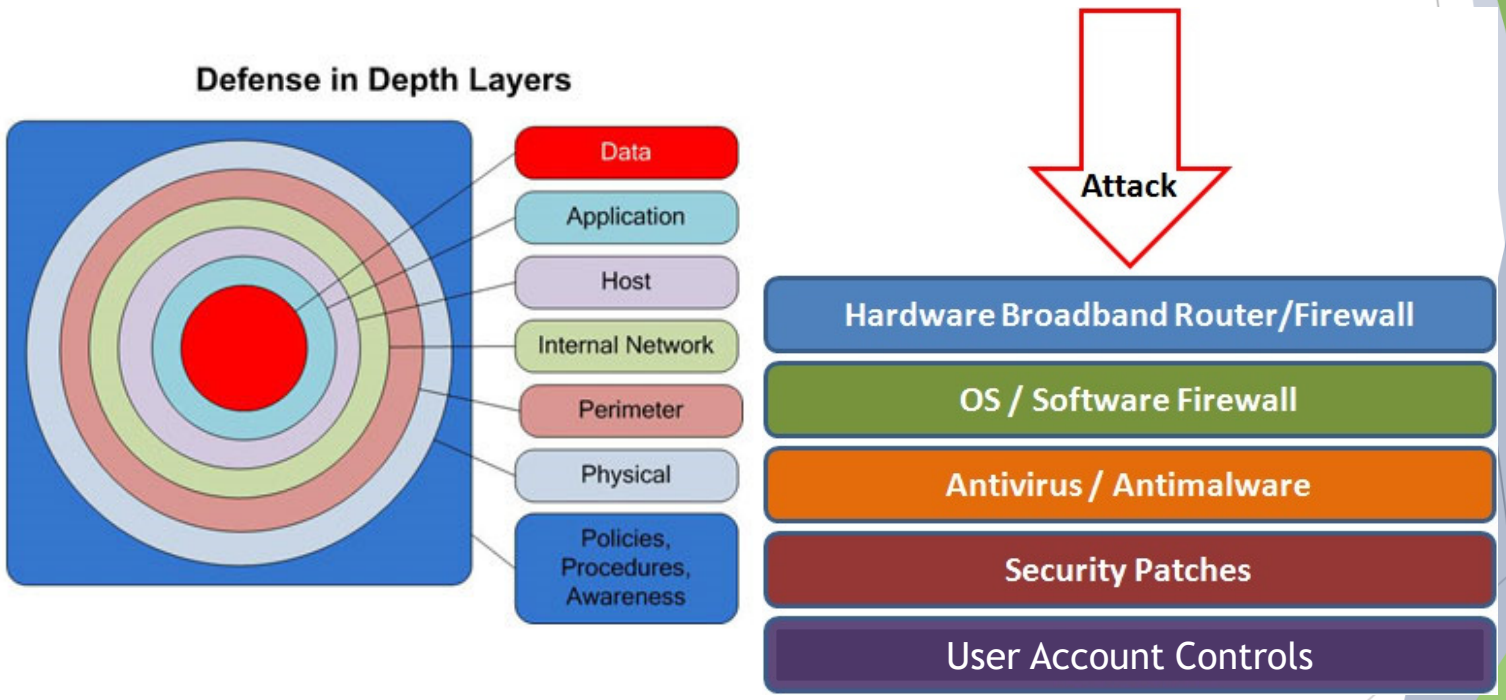


Recommended Best Practices For Threat Prevention

DYNAMIC NETWORK SOLUTIONS

Best Practices to avoid these threats

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

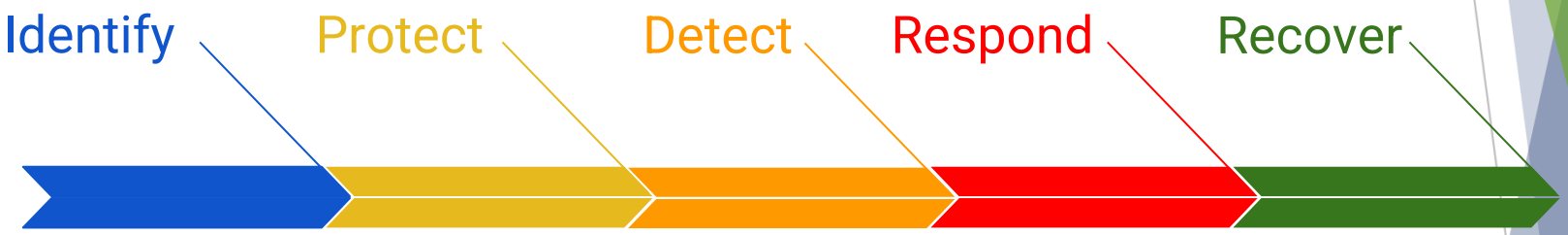


NIST Cybersecurity Framework

DYNAMIC NETWORK SOLUTIONS

DYNAMIC NETWORK SOLUTIONS

Cybersecurity Framework



- **IT Management**

- **AV**
- **Firewalls**
- **MFA**
- **Phishing Training**

- **AV**
- **EDR**
- **SIEM**

- **AV**
- **EDR**
- **SIEM**
- **IT TEAM**

- **Backup Solutions**
- **Disaster Recovery Plans**

DYNAMIC NETWORK SOLUTIONS

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?

DYNAMIC NETWORK SOLUTIONS

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

DYNAMIC NETWORK SOLUTIONS

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

DYNAMIC NETWORK SOLUTIONS

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.

DYNAMIC NETWORK SOLUTIONS

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?

DYNAMIC NETWORK SOLUTIONS

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

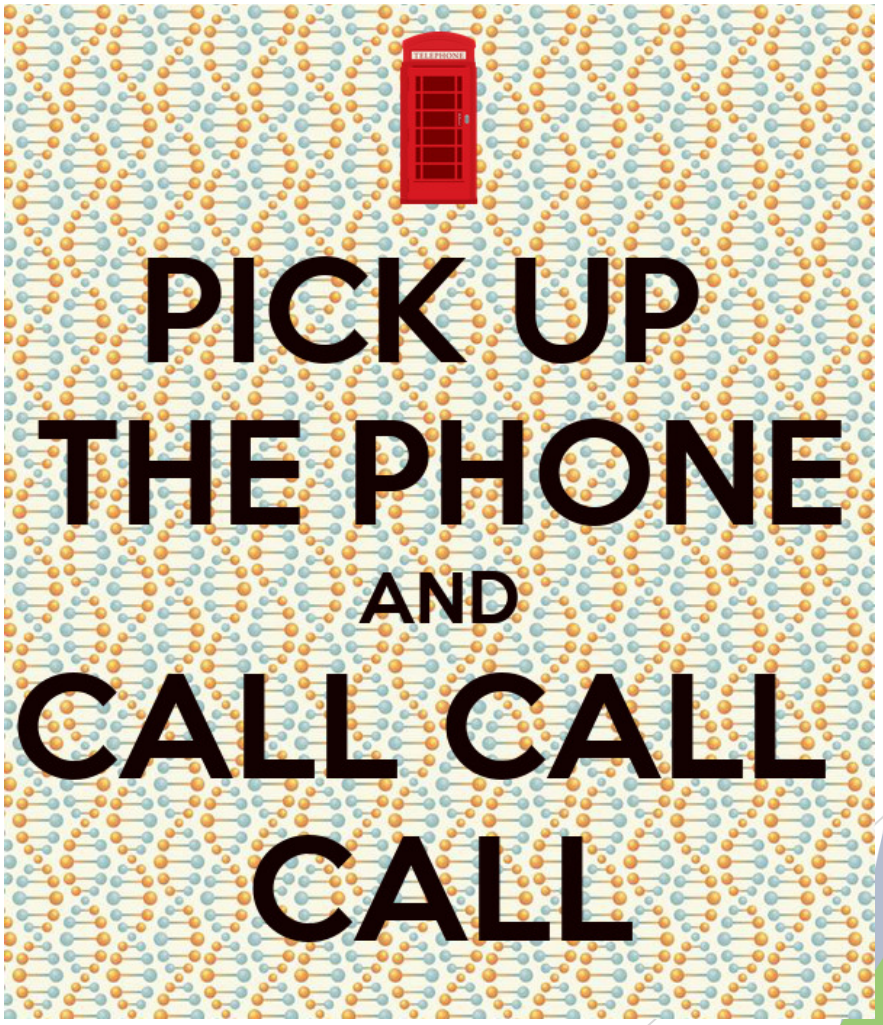
What to Ethically Do Should You Be Compromised

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, consectetuer adipiscing elit. Praesent mattis eros a tellus. Quisque leo tortor, commodo id, dapibus et, lacinia et, justo. Ut urna sapien, dictum eu, cursus vel, consectetuer tincidunt, eros. Etiam in libero. Etiam tempor. Maecenas ligula felis, commodo eget, scelerisque id, suscipit nec, odio. Vivamus commodo, magna in mollis feugiat, felis nisl dapibus dolor, eu blandit orci nulla in orci. Cras felis ipsum, mollis at, semper et, tincidunt id, ipsum. Ut consectetuer elit nec elit. Cras luctus molestie ligula. In gravida tempor nunc.

Curabitur nisl ligula, pulvinar et, volutpat non, porta a, ipsum. Donec tristique ante at 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 nisl. Ut quam. Pellentesque lobortis vehicula risus.

Etiam massa erat, tempor et, elementum fringilla, pellentesque ac, odio. Cras sed felis. Aliquam erat volutpat. Etiam tristique. Donec pellentesque, nulla semper adipiscing faucibus, nibh augue semper sapien, eget feugiat 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 lacinia. 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 iaculis ipsum. Morbi neque. Quisque augue. Etiam eleifend rhoncus 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 lacinia tortor arcu eget magna. Mauris eget enim at ante luctus ultricies. Integer eu nunc eget tellus iaculis vestibulum. Suspendisse potenti. Aenean aliquam mauris id turpis.

Your Sincerely,
Daniel Brady.

DYNAMIC NETWORK SOLUTIONS

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