Prepare Now for a Ransomware Attack

October 14, 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623**.

- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Box at any time during the presentation.**

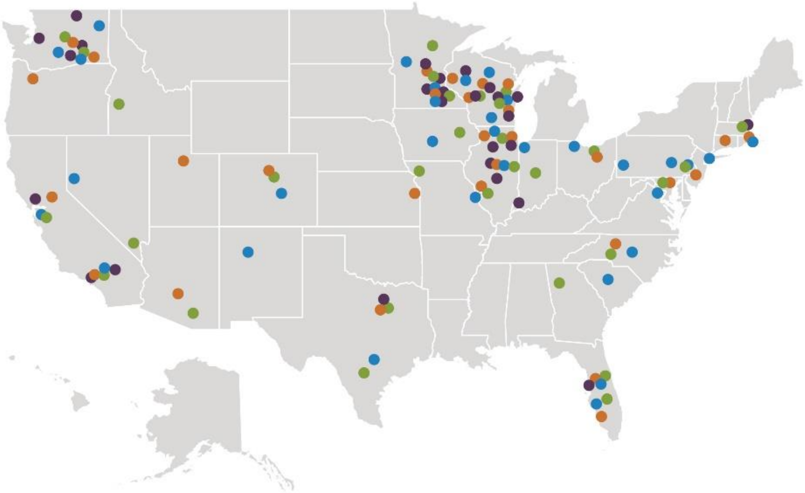
- The **PowerPoint presentation**, as well as the **webinar recording**, will be sent to you within the next 10 business days.

- For future webinar invitations, subscribe at CLAconnect.com/subscribe.

- Please complete our online survey.

About CliftonLarsonAllen

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- More than 6,100 employees
- Offices coast to coast



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

Ransomware Attacks

Are You Prepared?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

C:\whoami

- "Professional Student"
- Science Teacher / Self Taught Computer Guy
- IT Consultant - Project Manager → IT Staff/Help Desk → Hacker
- Assistant Scout Master (Boy Scouts)

Goals

Ransomware and Cybercrime

- Understanding the attackers
- How it’s done and what to look out for

Ransomware Kill Chain

- Attack vectors and defensive controls

Ransomware Recovery Strategies

Ransomware and Cybercrime

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Current State of Cybercrime

- Hackers have monetized their activity
  - Theft of personally identifiable information (PII)
  - Payment fraud
  - **Ransomware**

- Most attacks are carried out by organized crime

Organized Crime

- Hacking is run like a business where people specialize in different areas
  - Writing malware
  - Renting botnets
  - Social Engineering
  - Stealing data
  - Selling data (collect data from various sources/BIG DATA)
  - Etc.
- Most attacks are completely automated

Think like an attacker

Ransomware attacks can be automated

Can require little effort by attacker once attack has been launched

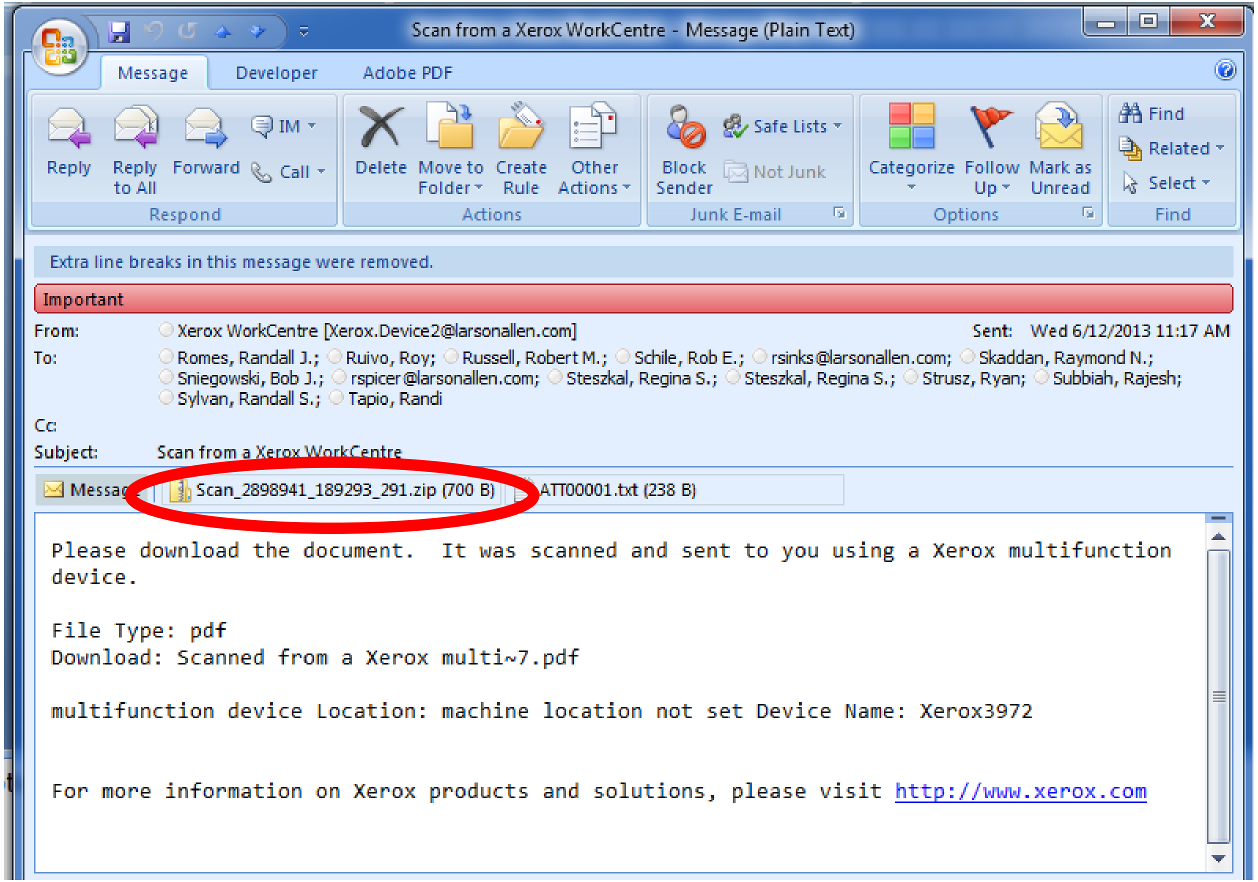
Monetization comes in the form of cryptocurrency which is largely unregulated

ANY **type of organization can be targeted regardless of the type of data they maintain**

Ransomware

- Attack on the **availability** of network data
- Easier to do than exfiltration of the data
- Uses strong encryption to render victim's files unreadable
- Payments are often in Bitcoin
- Cyber criminals attempt to delete host and network backups
- User credentials are used for network access
- Many variants and constant evolution

Ransomware



Extra line breaks in this message were removed.

Important

From: Xerox WorkCentre [Xerox.Device2@larsonallen.com]

Sent: Wed 6/12/2013 11:17 AM

To: Romes, Randall J.; Ruivo, Roy; Russell, Robert M.; Schile, Rob E.; rsinks@larsonallen.com; Skaddan, Raymond N.; Sniegowski, Bob J.; rspicer@larsonallen.com; Steszkal, Regina S.; Steszkal, Regina S.; Strusz, Ryan; Subbiah, Rajesh; Sylvan, Randall S.; Tapio, Randi

Cc:

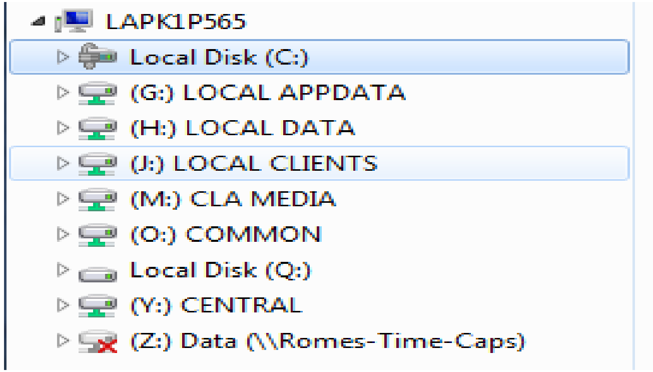
Subject: Scan from a Xerox WorkCentre

Messag Scan_2898941_189293_291.zip (700 B) ATT00001.txt (238 B)

```
Please download the document.  It was scanned and sent to you using a Xerox multifunction
device.

File Type: pdf
Download: Scanned from a Xerox multi~7.pdf

multifunction device Location: machine location not set Device Name: Xerox3972


For more information on Xerox products and solutions, please visit http://www.xerox.com
```

Ransomware

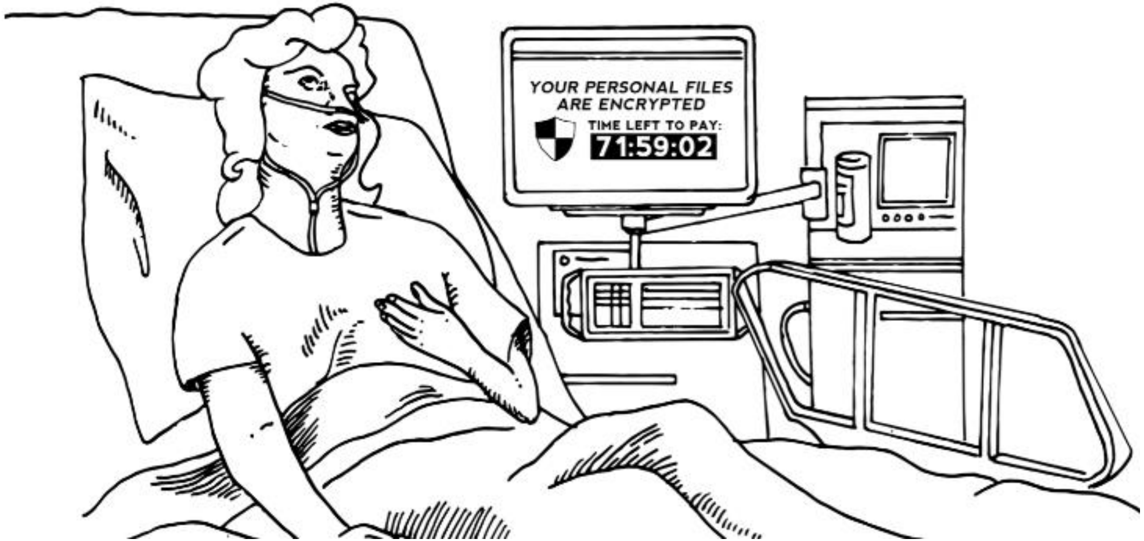
- Malware encrypts everything it can interact with



```
LAPK1P565
  Local Disk (C:)
  (G:) LOCAL APPDATA
  (H:) LOCAL DATA
  (J:) LOCAL CLIENTS
  (M:) CLA MEDIA
  (O:) COMMON
  Local Disk (Q:)
  (Y:) CENTRAL
  (Z:) Data (\\Romes-Time-Caps)
```

Hospital ransomware: A chilling wake-up call

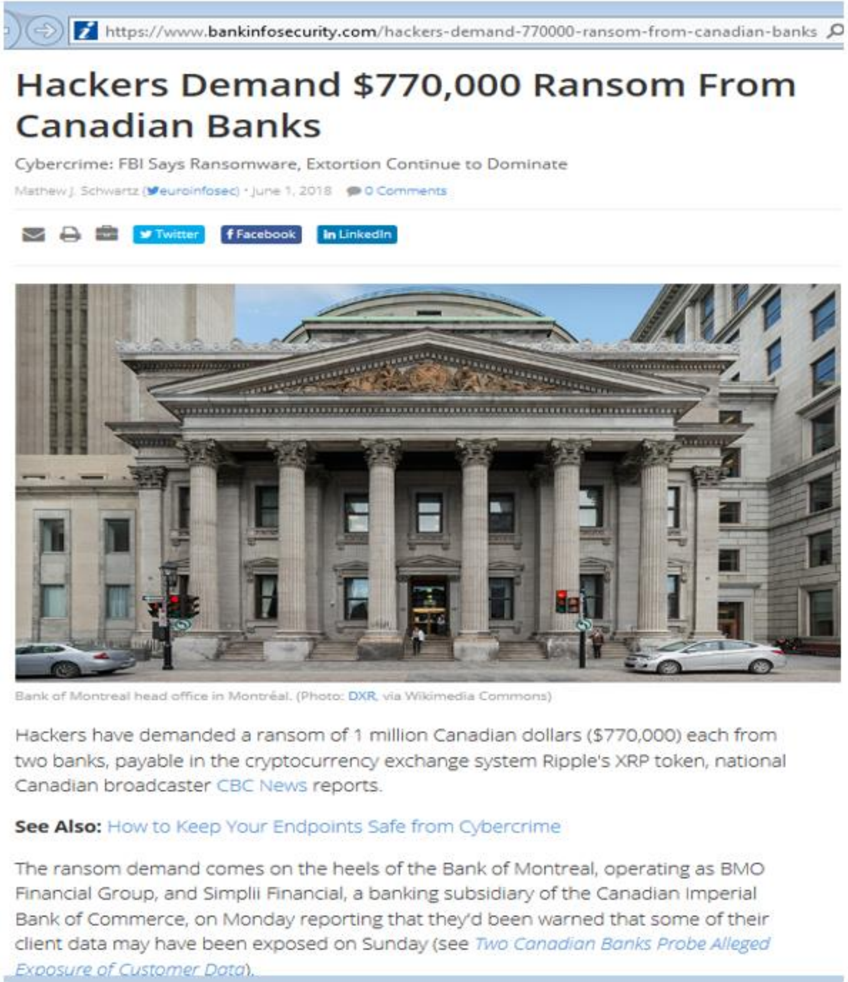
Hollywood Presbyterian was forced to pay up, just like everyone else.



http://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/

Ransomware

(One year ago)



https://www.bankinfosecurity.com/hackers-demand-770000-ransom-from-canadian-banks

Hackers Demand $770,000 Ransom From Canadian Banks

Cybercrime: FBI Says Ransomware, Extortion Continue to Dominate

Mathew J. Schwartz (@euroinfosec) • June 1, 2018 • 0 Comments

Twitter
Facebook
LinkedIn

Bank of Montreal head office in Montréal. (Photo: DXR, via Wikimedia Commons)

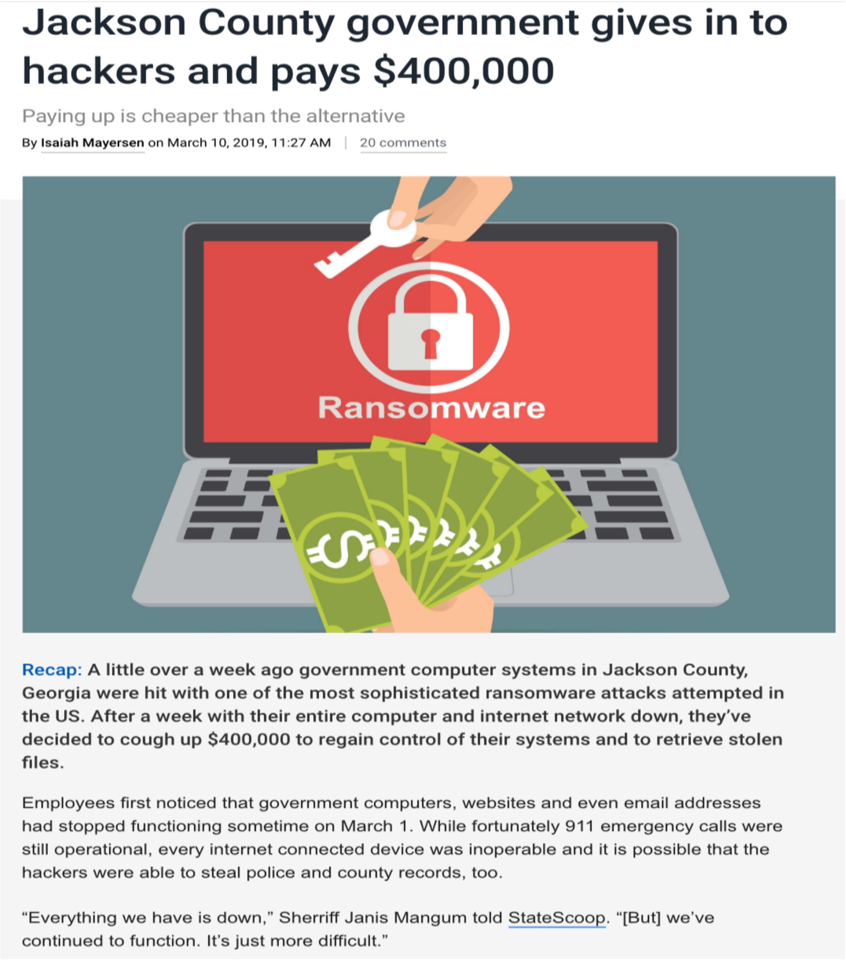
Hackers have demanded a ransom of 1 million Canadian dollars ($770,000) each from two banks, payable in the cryptocurrency exchange system Ripple's XRP token, national Canadian broadcaster CBC News reports.

See Also: How to Keep Your Endpoints Safe from Cybercrime

The ransom demand comes on the heels of the Bank of Montreal, operating as BMO Financial Group, and Simplii Financial, a banking subsidiary of the Canadian Imperial Bank of Commerce, on Monday reporting that they'd been warned that some of their client data may have been exposed on Sunday (see *Two Canadian Banks Probe Alleged Exposure of Customer Data*).

Ransomware

(Six months ago)



Jackson County government gives in to hackers and pays $400,000

Paying up is cheaper than the alternative

By Isaiah Mayersen on March 10, 2019, 11:27 AM | 20 comments

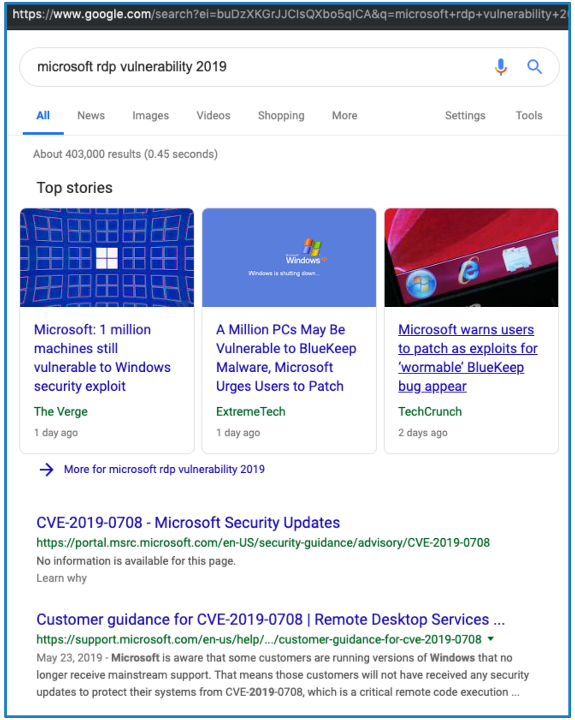
Recap: A little over a week ago government computer systems in Jackson County, Georgia were hit with one of the most sophisticated ransomware attacks attempted in the US. After a week with their entire computer and internet network down, they've decided to cough up $400,000 to regain control of their systems and to retrieve stolen files.

Employees first noticed that government computers, websites and even email addresses had stopped functioning sometime on March 1. While fortunately 911 emergency calls were still operational, every internet connected device was inoperable and it is possible that the hackers were able to steal police and county records, too.

"Everything we have is down," Sherriff Janis Mangum told StateScoop. "[But] we've continued to function. It's just more difficult."

Ransomware

(More Recently…)



https://www.google.com/search?ei=buDzXKGrJJClsQXbo5qlCA&q=microsoft+rdp+vulnerability+2

microsoft rdp vulnerability 2019

About 403,000 results (0.45 seconds)

Top stories

Microsoft: 1 million machines still vulnerable to Windows security exploit
The Verge
1 day ago

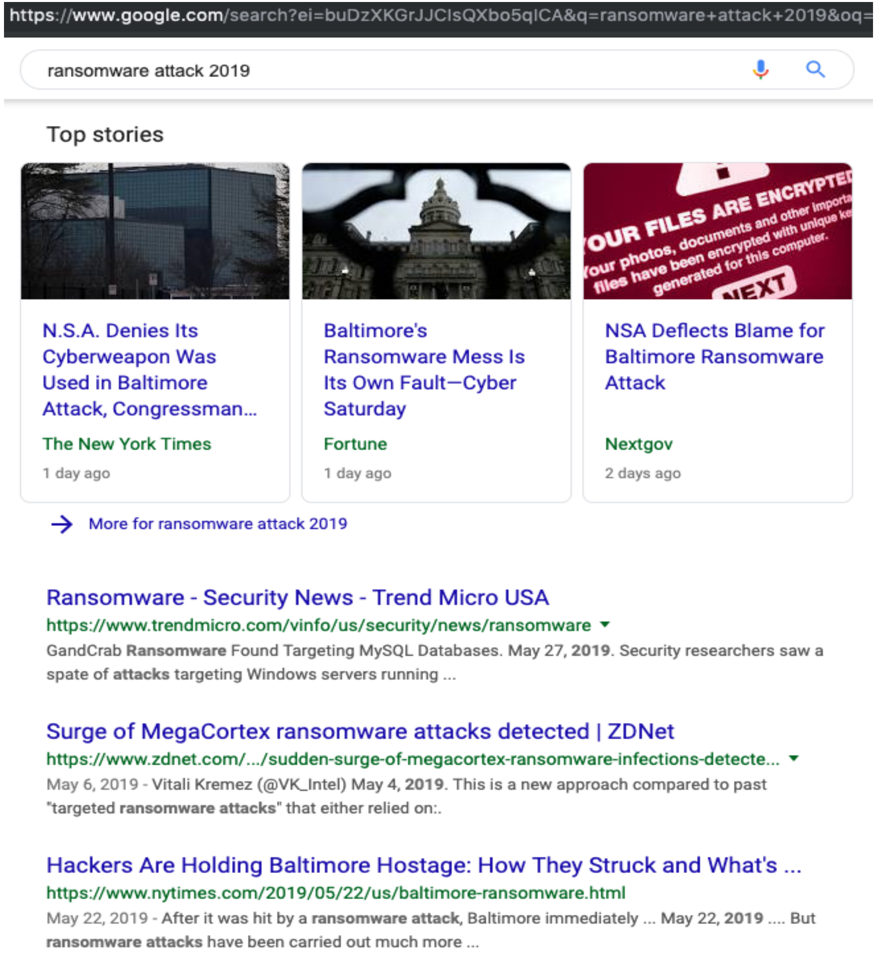
A Million PCs May Be Vulnerable to BlueKeep Malware, Microsoft Urges Users to Patch
ExtremeTech
1 day ago

Microsoft warns users to patch as exploits for 'wormable' BlueKeep bug appear
TechCrunch
2 days ago

More for microsoft rdp vulnerability 2019

CVE-2019-0708 - Microsoft Security Updates
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
No information is available for this page.
Learn why

Customer guidance for CVE-2019-0708 | Remote Desktop Services ...
https://support.microsoft.com/en-us/help/.../customer-guidance-for-cve-2019-0708
May 23, 2019 - **Microsoft** is aware that some customers are running versions of **Windows** that no longer receive mainstream support. That means those customers will not have received any security updates to protect their systems from CVE-**2019**-0708, which is a critical remote code execution ...



https://www.google.com/search?ei=buDzXKGrJJClsQXbo5qlCA&q=ransomware+attack+2019&oq=

ransomware attack 2019

Top stories

N.S.A. Denies Its Cyberweapon Was Used in Baltimore Attack, Congressman...
The New York Times
1 day ago

Baltimore's Ransomware Mess Is Its Own Fault—Cyber Saturday
Fortune
1 day ago

NSA Deflects Blame for Baltimore Ransomware Attack
Nextgov
2 days ago

More for ransomware attack 2019

Ransomware - Security News - Trend Micro USA
https://www.trendmicro.com/vinfo/us/security/news/ransomware
GandCrab **Ransomware** Found Targeting MySQL Databases. May 27, **2019**. Security researchers saw a spate of **attacks** targeting Windows servers running ...

Surge of MegaCortex ransomware attacks detected | ZDNet
https://www.zdnet.com/.../sudden-surge-of-megacortex-ransomware-infections-detecte...
May 6, 2019 - Vitali Kremez (@VK_Intel) May 4, **2019**. This is a new approach compared to past "targeted **ransomware attacks**" that either relied on:.

Hackers Are Holding Baltimore Hostage: How They Struck and What's ...
https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html
May 22, 2019 - After it was hit by a **ransomware attack**, Baltimore immediately ... May 22, **2019** .... But **ransomware attacks** have been carried out much more ...

Ransomware variants

- Since 2015 over 215 different variants have been discovered, of which only 97 have known remediation tools

Bad Rabbit

Wannacry

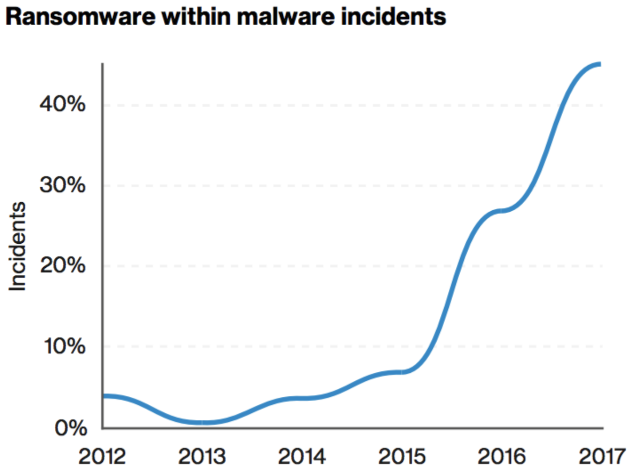
Petya

Ryuk

Next?

Defensive Strategies

- Defense in Depth / Layered Security:
  - Email spam filters
  - Removal of ads from the network
    - ◊ Webproxy
  - Staff awareness
  - Minimized user permissions
  - Patching
  - Disaster recovery - Working backup and Restore

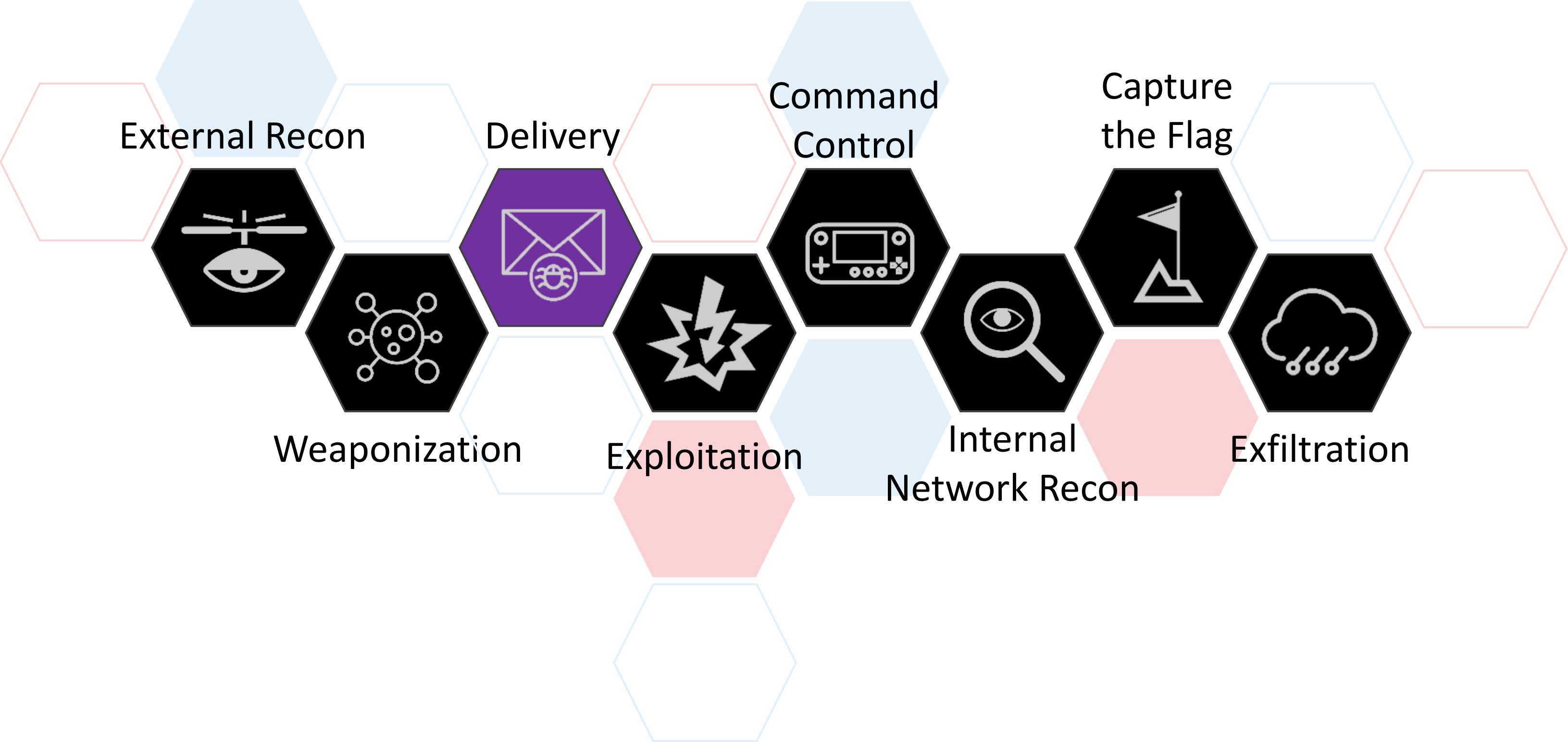


Ransomware Kill Chain

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

CyberKill Chain



External Recon

Weaponization

Delivery

Exploitation

Command Control

Internal Network Recon

Capture the Flag

Exfiltration

Delivery - Attacker

Direct exploit of publicly available service

Phishing

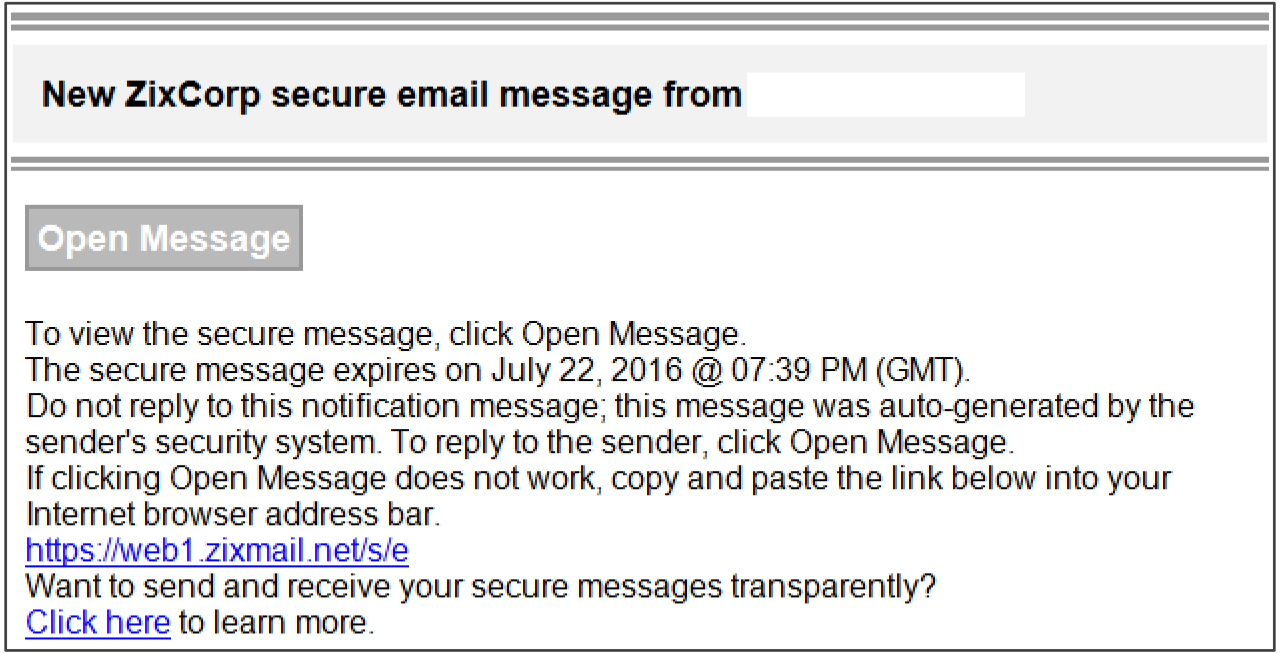
Social Engineering

- Email spoofing
- Call spoofing

Malicious hardware

- ”Free” USB drive from vendors

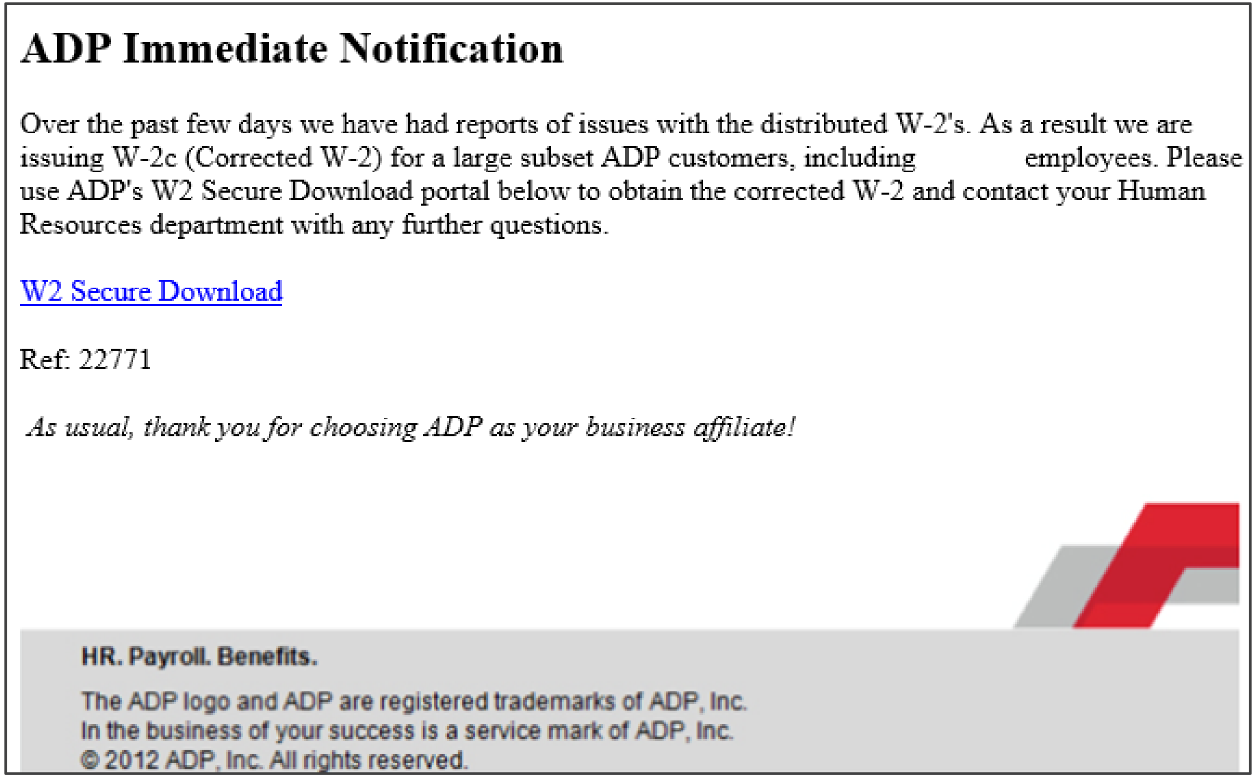
Phishing Email



New ZixCorp secure email message from

To view the secure message, click Open Message.
The secure message expires on July 22, 2016 @ 07:39 PM (GMT).
Do not reply to this notification message; this message was auto-generated by the sender's security system. To reply to the sender, click Open Message.
If clicking Open Message does not work, copy and paste the link below into your Internet browser address bar.
https://web1.zixmail.net/s/e
Want to send and receive your secure messages transparently?
Click here to learn more.

Phishing Email



ADP Immediate Notification

Over the past few days we have had reports of issues with the distributed W-2's. As a result we are issuing W-2c (Corrected W-2) for a large subset ADP customers, including employees. Please use ADP's W2 Secure Download portal below to obtain the corrected W-2 and contact your Human Resources department with any further questions.

W2 Secure Download

Ref: 22771

As usual, thank you for choosing ADP as your business affiliate!

HR. Payroll. Benefits.

The ADP logo and ADP are registered trademarks of ADP, Inc.
In the business of your success is a service mark of ADP, Inc.
© 2012 ADP, Inc. All rights reserved.

Poor Email Filtering

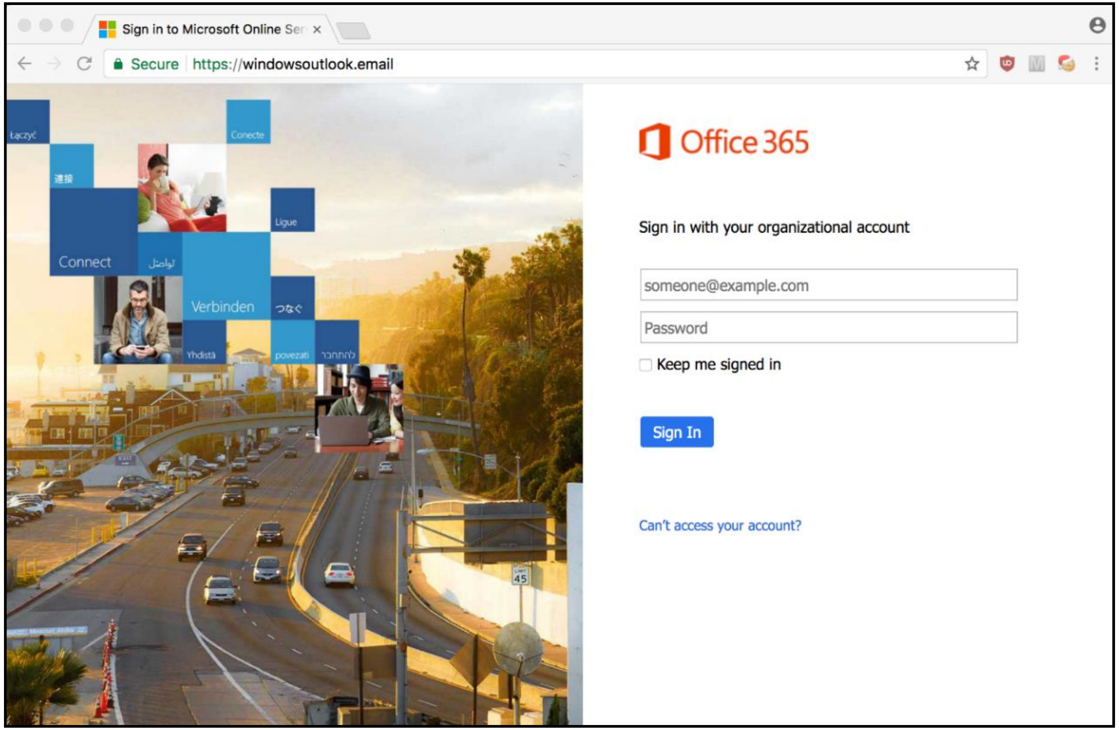
```
Connected to mail.cogentco.com (38.9.X.X).
MAIL FROM: <hacker@contoso.com>
250 OK
RCPT TO: <david.anderson@claconnect.com>
250 Accepted
```

SMTP Envelope

```
DATA
354 Enter message, ending with "." on a line by itself
FROM: <ElonMusk@tesla.com>
TO: <david.anderson@claconnect.com>
Subject: Free Tesla Car
```

SMTP Message

Phishing Website



Sign in to Microsoft Online Ser ×

Secure https://windowsoutlook.email

Office 365

Sign in with your organizational account

someone@example.com

Password

□ Keep me signed in

Sign In

Can't access your account?

Delivery - Attacker

- In Person
  - RFID clone
  - Media drops
  - Tailgating
  - Attacking weak wireless implementations

Phone Calls

- Call someone and have them download a remote access tool- spoofing phone numbers is extremely easy
- *“Hi, this is Randy from Comcast Business users support. I am working with Dave, and I need your help…”*
  - Name dropping → Establish a rapport
  - Ask for help
  - Inject some techno-babble
- *“I need you to visit the Microsoft Update site to download and install a security patch. Do you have 3 minutes to help me out?”*

Password Guessing

- Internet accessible services that do not require multi-factor authentication
  - RDP, OWA, VPN, etc.
- Employees choosing weak passwords
- Employees reusing passwords found in known data breaches

Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584

Delivery - Defense

Mail Security Controls

Security Assessments of email system

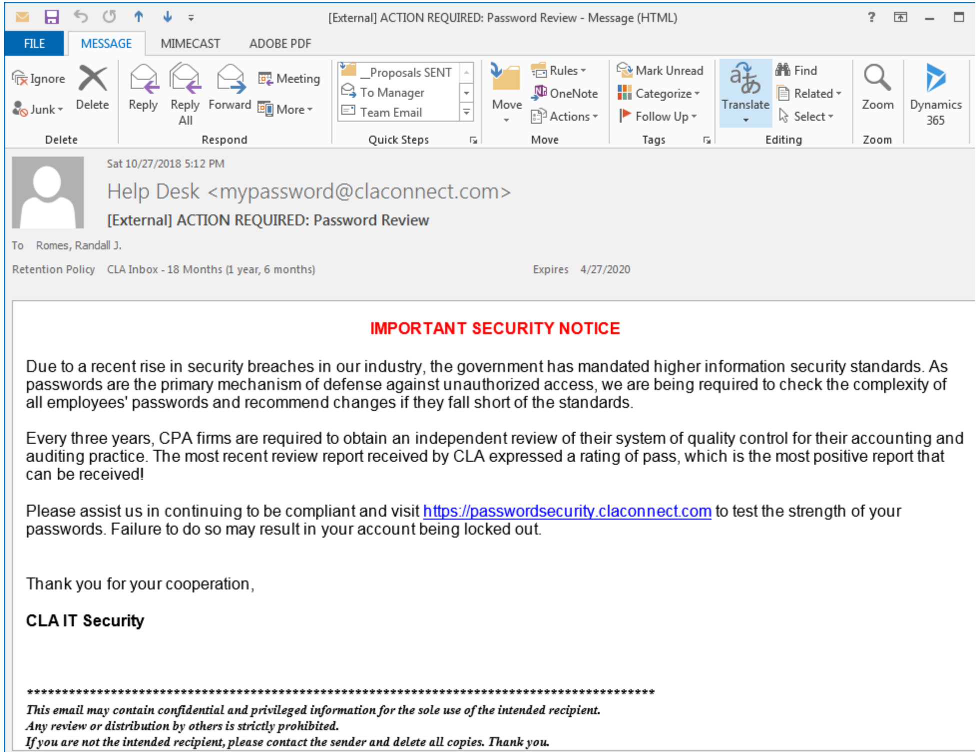
- Cloud - offsite
- OWA - onsite
- Endpoint

Spam Filters

Monitoring

Delivery - Defense

- All Staff - Security Awareness Training
  - Analyze email “FROM” field
  - Hover over links
  - Is the email expected
  - Who ya gonna call?



Sat 10/27/2018 5:12 PM

Help Desk <mypassword@claconnect.com>

[External] ACTION REQUIRED: Password Review

To Romes, Randall J.

Retention Policy CLA Inbox - 18 Months (1 year, 6 months) Expires 4/27/2020

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, the government has mandated higher information security standards. As passwords are the primary mechanism of defense against unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standards.

Every three years, CPA firms are required to obtain an independent review of their system of quality control for their accounting and auditing practice. The most recent review report received by CLA expressed a rating of pass, which is the most positive report that can be received!

Please assist us in continuing to be compliant and visit https://passwordsecurity.claconnect.com to test the strength of your passwords. Failure to do so may result in your account being locked out.

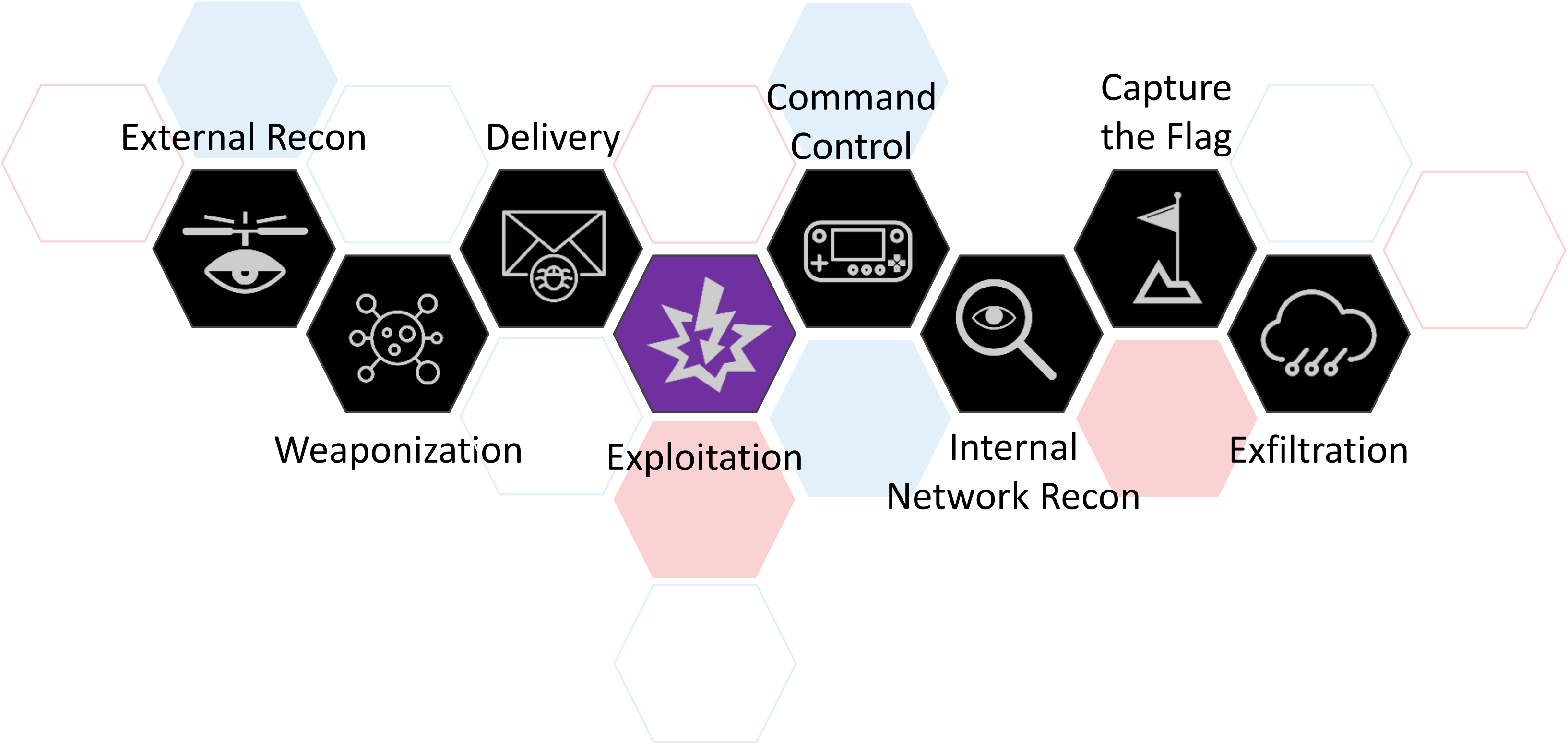
Thank you for your cooperation,

CLA IT Security

****

This email may contain confidential and privileged information for the sole use of the intended recipient.
Any review or distribution by others is strictly prohibited.
If you are not the intended recipient, please contact the sender and delete all copies. Thank you.

CyberKill Chain



External Recon

Weaponization

Delivery

Exploitation

Command Control

Internal Network Recon

Capture the Flag

Exfiltration

Exploitation

Missing patches

- MS17-010 (WannaCry / ETERNALBLUE)
- Bluekeep

System Configuration

- Malicious Office documents (Macros, OLE, etc.)
- HTML Applications (.HTA)
- PowerShell is often utilized to run/deliver the code

Exploitation - Defense

- Security Policy
  - Least Privilege
  - Layered Defense
  - Secure by Design
  - Assume Breach
- Patch management
- Practice Restore Capabilities

Exploitation - Defense

Security Baseline

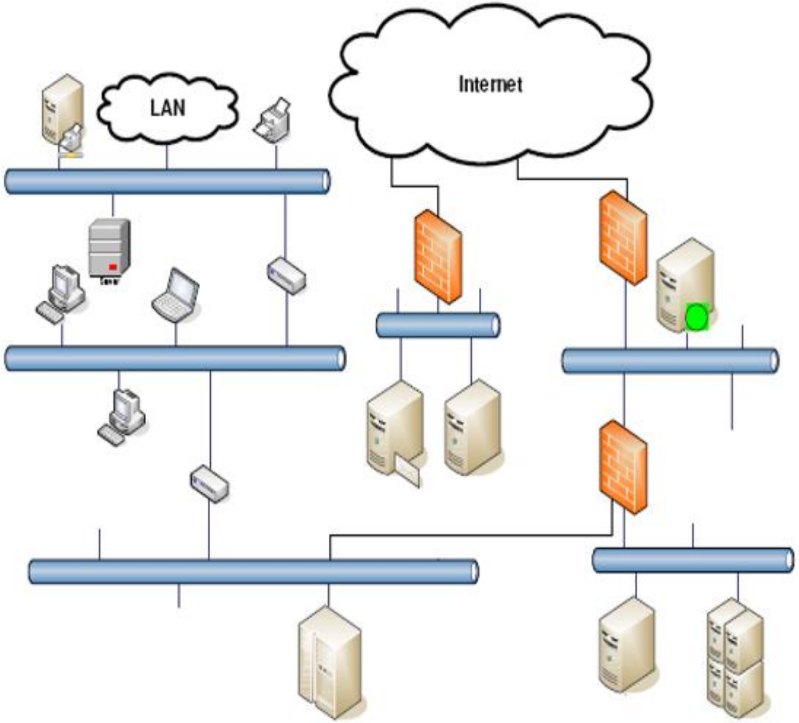
- “Golden Image”
- Desired State Configuration
- GPO
  - User
  - machine
- Benchmarks
  - CIS
  - NIST

Exploitation - Defense

- Application whitelisting
  - AppLocker
  - Windows Device Guard
- Protect Office Applications
  - Block Macros
  - Windows Defender Exploit Guard
- Log Management

Exploitation - Defense

- Network Monitoring
  - User level
  - Temporal
  - Attempts
  - Behavior
- Segmentation
  - Block endpoint SMB
  - Guest Wi-Fi
  - IoT
  - Secure transactions



Ransomware Recovery Strategies

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Data Backup

- Ensure ALL critical systems and data are being backed up
- Practice a full system and data restore to verify your confidence in full system and data restore capabilities
  - Understand how long it will take to recover various backup types
- Segment critical backups to prevent deletion
  - Attackers will attempt to delete or encrypt all accessible backups

Incident Response

- Playbooks for common incident types
- Ensure employees understand their responsibilities and procedures to follow in the event of an incident

TEST!

Cyber Insurance

- Helping or hurting organizations?
- Should you pay?
  - You won’t need to if appropriate measures are taken
- Average cyber insurance payout is ???

?????????????????????????????????????

Summary

Increased sophistication and adoption by attackers

Preventative measures are essential

- Requires technical and procedural controls

Data backup and incident response are critical to mitigate the impact of a Ransomware attack

CLAconnect.com

Randy Romes, CISSP, CRISC, CISA, MPC, PCI-QSA
Managing Principal - Cybersecurity
612.397.3114
Randy.Romes@claconnect.com