U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Cyber Ghost Stories and Other cyber things that keep you awake at night

Ian Moore, CISSP

Supervisory Cybersecurity Advisor (SCSA) for Washington State

Cybersecurity Advisor (CSA) Program

Cybersecurity and Infrastructure Security Agency

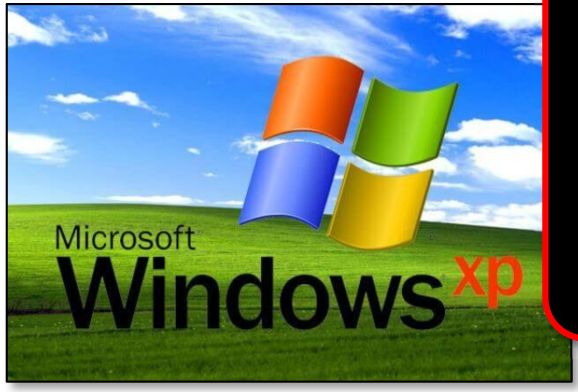
October 9th, 2024

Contents

- Story #1 – WA County and Ransomware
- Story #2 – WA Critical Infrastructure and Ransomware
- Story #3 – WA Org and Insider Threat
- Story #4 – WA Org and Business Email Compromise
- Top Current Cyber Threats
- Cyber Attack Sequence
- Biggest Vulnerabilities
- Top Cybersecurity Mitigation Measures
- CISA Assessments and Services
- Additional CISA Services

Story #1 – WA County and Ransomware

- Cybersecurity Service Provider firm notified county of encryption
- CISA called -> FBI called
- Partial encryption
    - Attacker used scheduled task to run encryption but used wrong time zone, probably
- Good backups, good team
    - Digital clock in contract 911 center - phishing
    - Win XP machine not on inventory
- ~140 hours down
- Elections admin affected slightly
- WA SoS creates new election solution



- IR plan
- Admin alerts
- Robust backups
- Shadow IT
- Network segmentation
- COOP, BCP, etc.

Story #2 – WA Critical Infrastructure and Ransomware

- Org notified of encryption by note on computers
  - Initial vector – phishing email likely
  - DB hack and rootkit installed
- Once encryption was confirmed, Internet disconnected
  - Closed the C&C connection
- Brought in MS DART
- Online systems unavailable
  - Services slowed
  - Hundreds of thousands of customers affected

- Rebuilt systems from backups
  - Didn't pay the ransom
  - CISA and FBI brought in from the beginning

Microsoft Detection and Response Team (DART)

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Phishing Guidance: Stopping the Attack Cycle at Phase One

CYBERSECURITY INFORMATION SHEET

- Email best practices
- IR plan
- Admin alerts
- Robust backups
- Network segmentation
- COOP, BCP, etc.

Story #3 – WA Org and Insider Threat

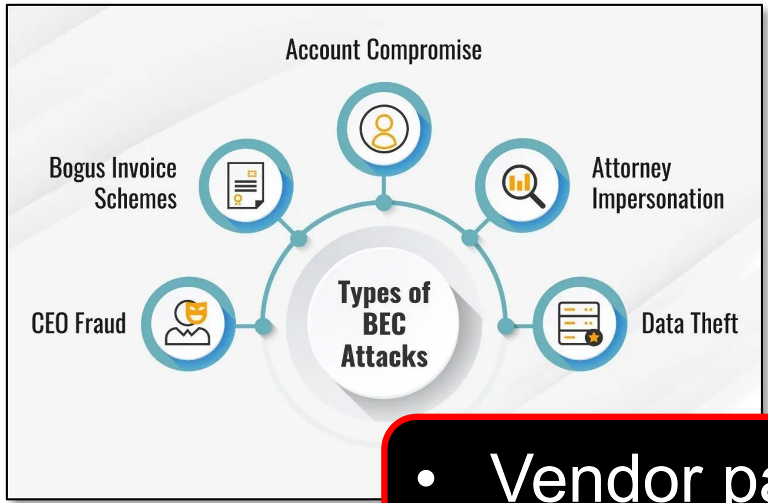
- Poor performing tech employee
- Low performance scores
- About to get let go
- Makes some scripts for backdoor
  - PowerShell, python, etc.
- Obscures remote account and tests access
- Employee gets released
- Managers escort him out and lock his on-prem accounts

- Weeks later the manager checks activity from the remote accounts
  - After investigation they noticed the ex-employee was still doing stuff and likely sabotaging the org or stealing data

- Access Management
- Admin alerts
- Network segmentation
- Background Investigations
- Remote Access Policies
- HR Termination Policies

Story #4 – WA Org and Business Email Compromise

- Private industry org working with many customers and suppliers
- New salesperson calls to introduce himself
  - He is one of the new contacts for some company
- Over the months they establish repour
- Then requests to change account and routing number because of conflict with their old bank
- After a few months, they get a call that they haven’t paid in a few months.
- The company is out that money
- They can work with the FBI and US Secret Service, but it is likely gone



- Vendor payment policies
- Finance alerts
- Employee Training
- 2 Person approval

Top Current Cyber Threats

Top Ransomware Groups

- ~~Lockbit – Drive by, Public-facing Apps, Ext. remote services~~
- Blackcat/Alphv – Phishing/SE, Compromised Accounts
- Cl0p – MOVEit Vuln, GoAnywhere, Public-facing Apps
- Royal – Phishing, RDP, Public-facing Apps
- Black Basta – Phishing, LotL
- Volt Typhoon – LotL, SOHO, Impacket

#StopRansomware

$1.1 billion reported in 2023

Dad Jokes
@Dadsaysjokes

How did the hacker escape the police?

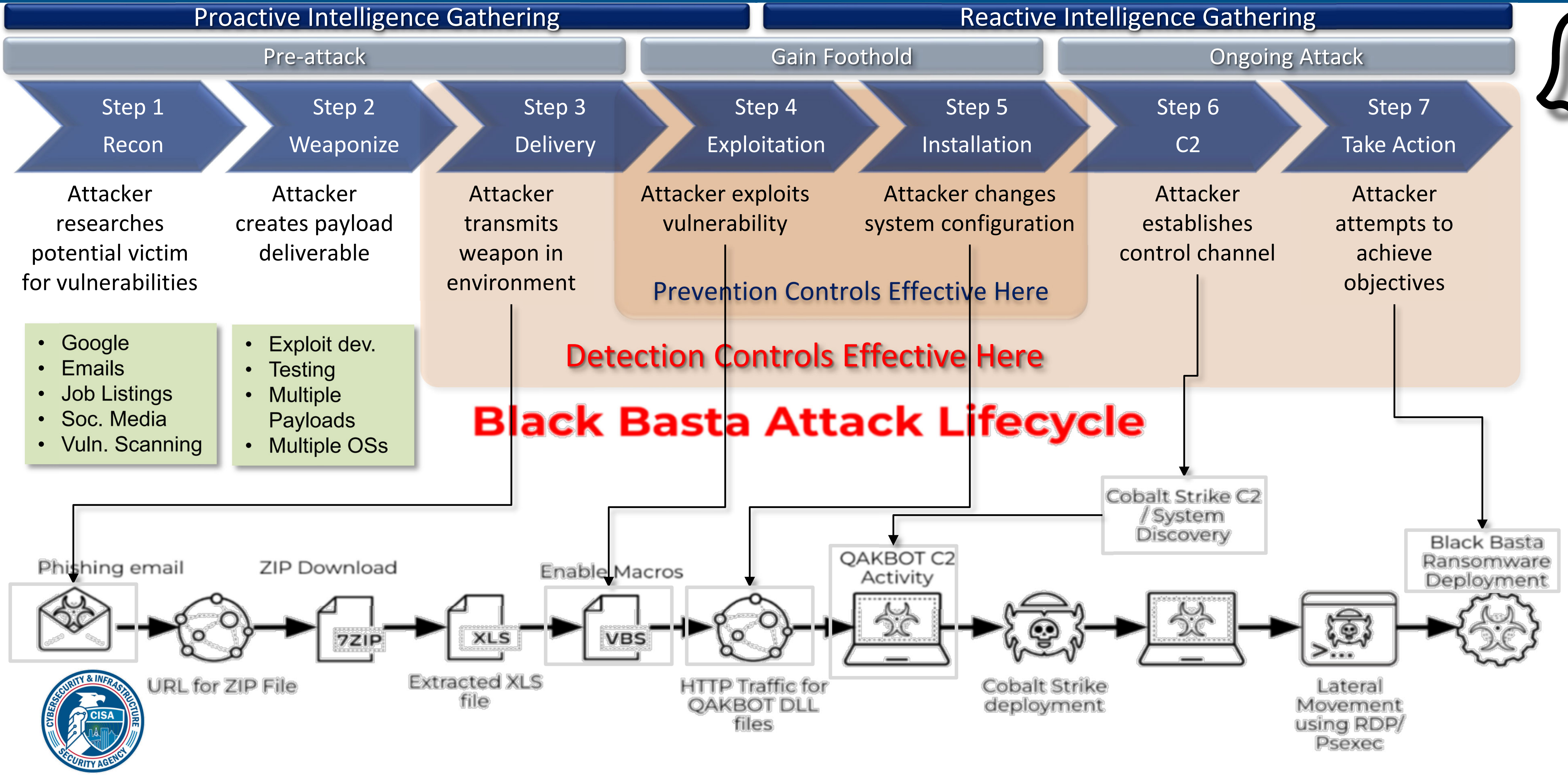
He just ransomware!

11:16 AM · Aug 10, 2021

158 Reposts 20 Quotes 1,073 Likes 14 Bookmarks

https://www.cisa.gov/stopransomware/ransomware-guide

Cyber Attack Sequence: How the adversary attacks



Proactive Intelligence Gathering

Reactive Intelligence Gathering

Pre-attack

Gain Foothold

Ongoing Attack

Step 1 Recon: Attacker researches potential victim for vulnerabilities

- Google
- Emails
- Job Listings
- Soc. Media
- Vuln. Scanning

Step 2 Weaponize: Attacker creates payload deliverable

- Exploit dev.
- Testing
- Multiple Payloads
- Multiple OSs

Step 3 Delivery: Attacker transmits weapon in environment

Step 4 Exploitation: Attacker exploits vulnerability

Step 5 Installation: Attacker changes system configuration

Step 6 C2: Attacker establishes control channel

Step 7 Take Action: Attacker attempts to achieve objectives

Prevention Controls Effective Here

Detection Controls Effective Here

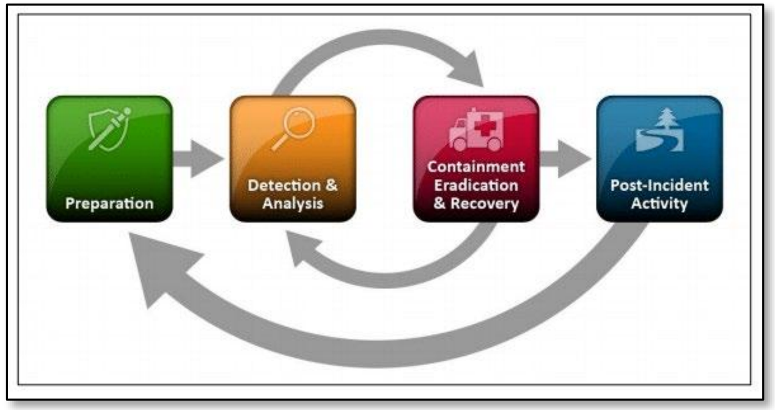
Black Basta Attack Lifecycle

Phishing email
URL for ZIP File
ZIP Download
7ZIP
Extracted XLS file
XLS
Enable Macros
VBS
HTTP Traffic for QAKBOT DLL files
QAKBOT C2 Activity
Cobalt Strike deployment
Cobalt Strike C2 / System Discovery
Lateral Movement using RDP/ Psexec
Black Basta Ransomware Deployment

Biggest Vulnerabilities

- Flat (Unsegmented) Network
- Outdate Technology – No longer vendor supported (XP)
- Shadow IT group in another part of the network
- Lack of dedicated cybersecurity staff
- Fragmented IT Governance at local level
- No endpoint detection installed or misconfigured
- Incident Response plan not exercised before the big “Event”

MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-4-07
To complete the log-in procedure, stare directly at the sun.



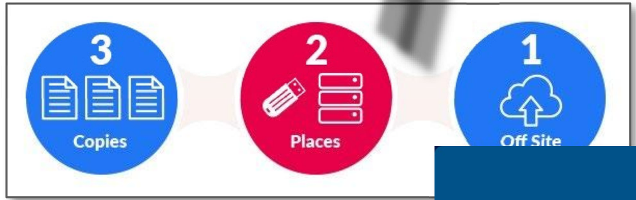
Top Cybersecurity Mitigation Measures

- Remove Internet Exposed Services
- Vulnerability Scanning and Patching
- Remove Legacy Systems
- Segment Network
- Intrusion Detection Systems (IDS)
- End Point Protection
- Phishing Resistant Multi-Factor Authentication (MFA)
- Secure/Robust Backups
- Annual Security Awareness
- Incident Response Plan

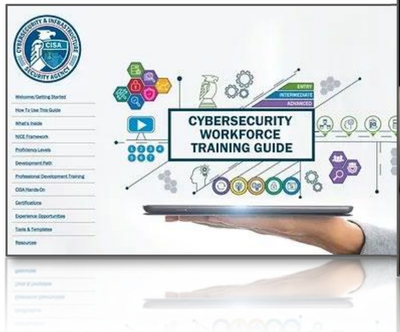
Best Bang for your Buck!

MFA

SLCGP



.gov



User name: john_smith

Password: ••••••••••

PASSCODE:

CISA Assessments and Services

Steps to enhance your cybersecurity

1. Vulnerability Scanning (Cyber Hygiene)
   - Web Application Scanning (WAS)

2. Assessments
   - Cyber Resilience Review (CRR)
     - Cyber Resiliency Essential (CRE)
   - Cyber Infrastructure Survey (CIS)
   - External Dependencies Management (EDM)
   - Ransomware Readiness Assessment (RRA)
   - Incident Management Review (IMR)

3. Technical Services
   - Remote Penetration Test (RPT)
   - Risk and Vulnerability Assessment (RVA)
   - Validated Architecture Design Review (VADR)

4. Exercises

Cybersecurity Evaluations Tool (CSET)

All our services are NO-COST!

Additional CISA Services

Protective Security Advisors (PSA)

- Various levels of physical security assessments
- Active Shooter Training

Emergency Communications

- Support to 9-1-1 centers and other communications

Exercise Support

- National support (Multi-state)
- Table-top Exercises (Whole Organization)
- Table-top In a Box (Department)

Conclusion

- Story #1 – WA County and Ransomware
- Story #2 – WA Critical Infrastructure and Ransomware
- Story #3 – WA Org and Insider Threat
- Story #4 – WA Org and Business Email Compromise
- Top Current Cyber Threats
- Cyber Attack Sequence
- Biggest Vulnerabilities
- Top Cybersecurity Mitigation Measures
- CISA Assessments and Services
- Additional CISA Services

Contacts

Ron Watters, CISSP, GSLC
Region 10 (Western WA, OR, ID, AK)
Cybersecurity Advisor (CIRCIA)
(206) 348-4071
Ronald.Watters@cisa.dhs.gov

Christopher Callahan, CISSP, GICSP
Region 10 (Western WA, OR, ID, AK)
Chief of Cybersecurity
(206) 601-4575
Christopher.Callahan@cisa.dhs.gov

Ian Moore, CISSP
Region 10 (WA)
Supervisory Cybersecurity Advisor (SCSA)
for Washington State
(360) 594-1832
Ian.Moore@cisa.dhs.gov

Daniel Brown, CISSP, CISM
Region 10 (Inland NW)
Cybersecurity Advisor
(509) 981-9920
Daniel.Brown@cisa.dhs.gov

For inquiries or further information,
contact cyberadvisor@cisa.dhs.gov

Alexander Salazar, CISSP
Region 10 (WA, King County Area)
Cybersecurity Advisor
(206) 225-5546
Alexander.Salazar@cisa.dhs.gov

https://www.cisa.gov/cyber-resource-hub

Questions!

https://www.cisa.gov/cyber-resource-hub