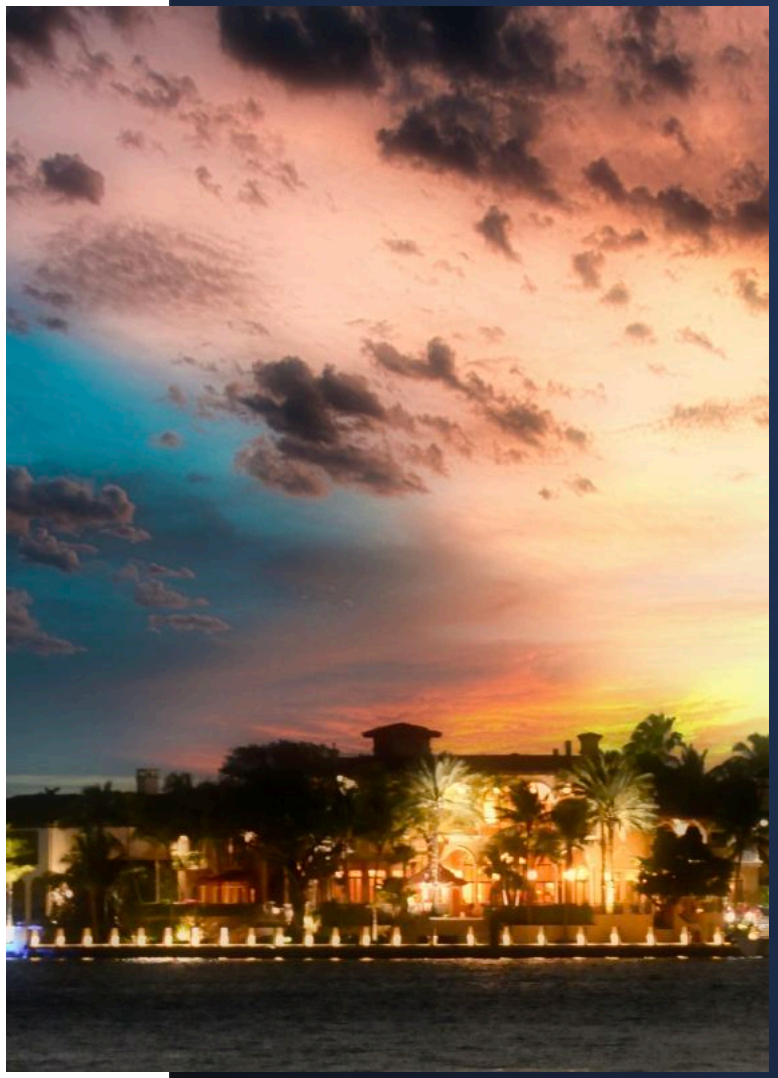
Defending against Ransomware

How to not get ransomware or you will have to learn how to recover from ransomware

The caveats: This is from a lengthy series of presentations (*Ransomware: identify, protect, detect, respond, recover*) cut down to a brief of about 20 minutes. All the guilty have been sentenced, and the bodies are buried. A moose once bit my sister. Any suggestion of events associated with the current living should be ignored. My boss doesn't know I'm here. External counsel is pretty sure I'm nuts. *Original presentation prepared June 2021.*

Dr. Samuel Liles

- Army National Guard, United States Marine Corps, Tribal Police Officer, Sheriffs Office (Corrections X2), Indiana Special Investigator
- Anything for a $ that was mostly legal, general information technology/security, since 1999 ran worldwide MCIWorldcom Y2K incident response, ran various programs for NCR (including worldwide 9/11 response for Sun).
- Purdue University Calumet (tenured associate professor, chair of faculty senate, lots and lots of stuff), National Defense University – IRMC/iCollege/CIC (associate professor) until sequestration, back to Purdue and ran cyber forensics laboratory and lots of gov consultation.
- CISO of US Army Corps of Engineers, lots of “stuff” with ARCYBER, NSA, others. Moved over to intelligence community, acting director of the DHS Intelligence and Analysis cyber team.
- Currently VP of Security at UKG, and Merchant Marine master/mate with tow, sail, and other creds

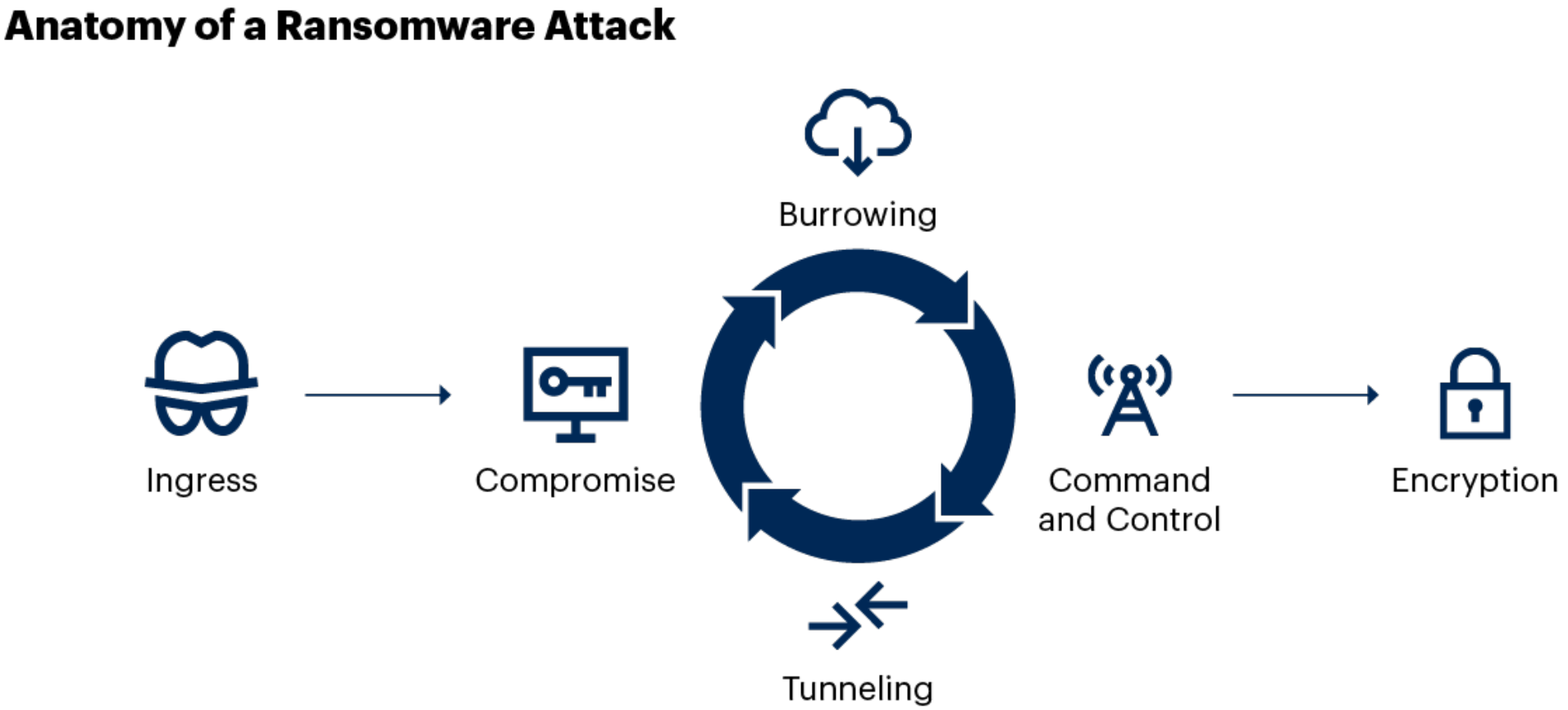


Fair warning: I am an iconoclast. If you only think about doctrine, you'll never be prepared for the future. Innovation is found in questioning the common and facilitating the uncommon.

Iconoclast: A person who attacks cherished beliefs or institutions. – Merriam Webster

Iconoclast: The lonely guy mumbling in the corner. - Former Boss

Traditional explanation of ransomware



Source: Gartner

724116_C

Players in a ransomware attack

Other Conti departments with their own distinct budgets, staff schedules, and senior leadership include:

–**Coders:** Programmers hired to write malicious code, integrate disparate technologies
–**Testers:** Workers in charge of testing Conti malware against security tools and obfuscating it
–**Administrators:** Workers tasked with setting up, tearing down servers, other attack infrastructure
–**Reverse Engineers:** Those who can disassemble computer code, study it, find vulnerabilities or weaknesses
–**Penetration Testers/Hackers:** Those on the front lines battling against corporate security teams to steal data, and plant ransomware.

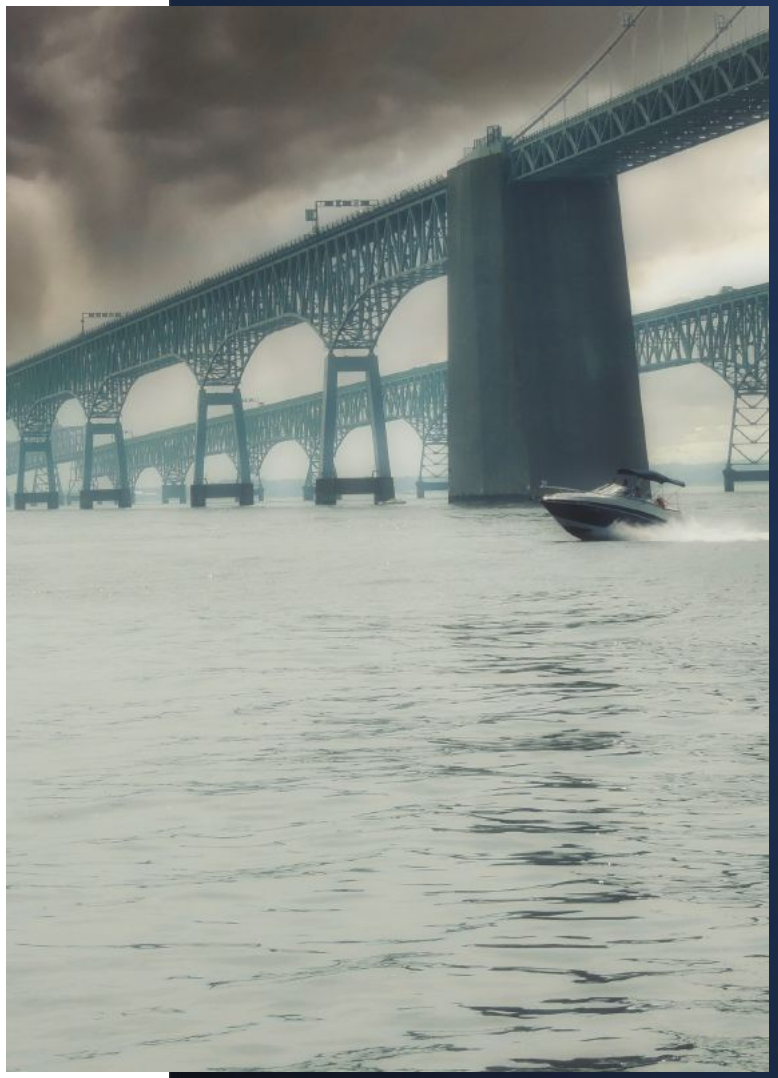
Source: Krebs on Security, 2022, "Conti Ransomware Group Diaries, Part II: The Office", https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

- Stage 1 (Software development)
  - Exploitation development
  - Access creation/discovery
  - Persistence mechanism created
- Stage 2 (Script deployment and writing)
  - Inventory of assets
  - Technical research of company structure
- Stage 3 (Systems administrator)
  - Deployment of ransomware
  - Enabling target package
- Stage 4 (Lawyer)
  - Research of insurance and company worth
  - Negotiation of ransomware payment terms
  - Analysis of payment
  - Name and shame or turning over the keys

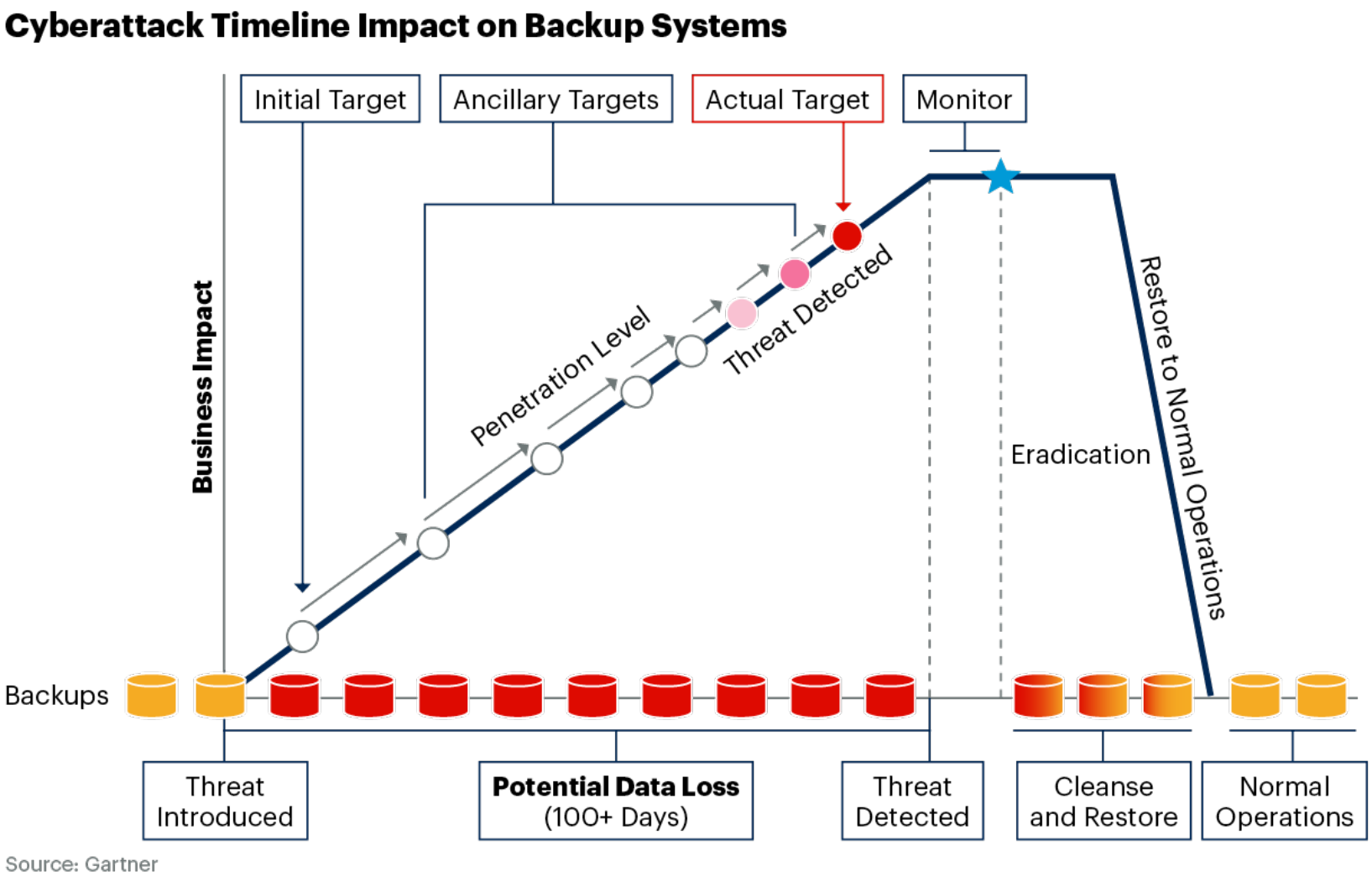
Ransomware is nothing but malware on a mission

The conundrum of a technical defense against ransomware

- Signature based systems (virus protection, intrusion detections systems, intrusion prevention systems, firewalls)
  - Slow to update
  - Never understands the known unknowns
- User Entity Behavior Analysis (UEBA)
  - Misses the first few things
  - Can be difficult to manage

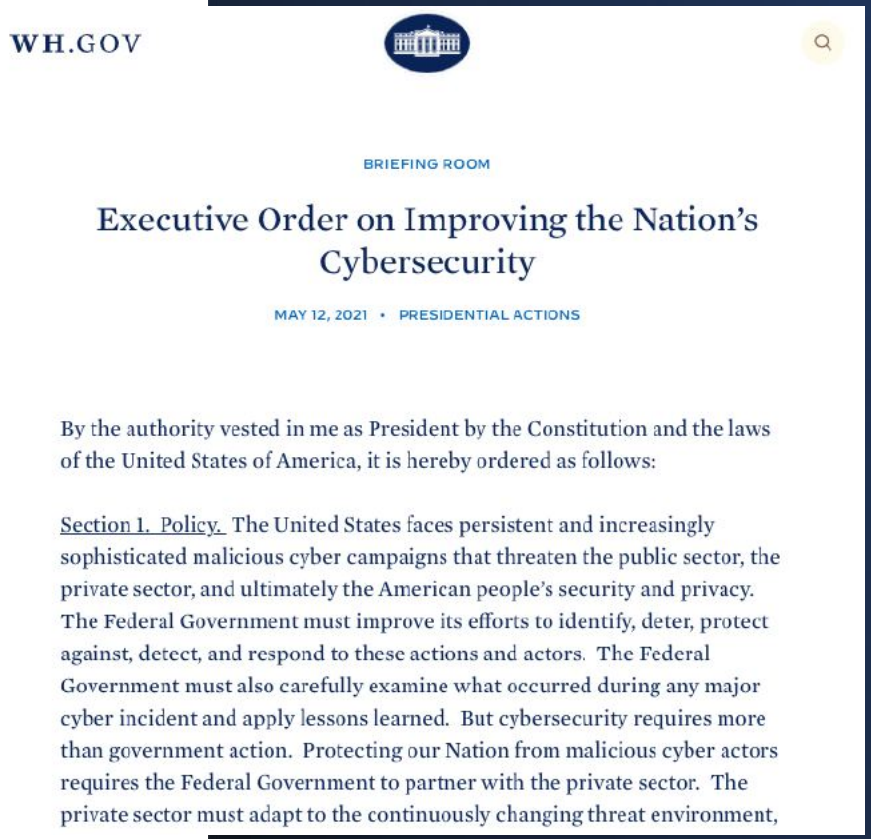


Exploitation timeline of ransomware



Whitehouse: Improving the nations cybersecurity executive order

- Multifactor Authentication on every system
- Endpoint Detection and Response deployed to every interactive system, operating system, server, end point, etc.
- Encrypt all devices and backups with a robust solution
- Empower the security team to succeed with executive level representation to corporate and investors leadership
- Share and incorporate threat models understanding that a security incident is an existential risk



WH.GOV

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment,

White House Memo on Ransomware

- Implement the five best practices from the Presidents Executive Order
- Backup your data, system images, and configuration, regularly test them, and keep the backups offline
- Update and patch systems promptly
- Test your incident response plan
- Check your security team's work
- Segment your networks

THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

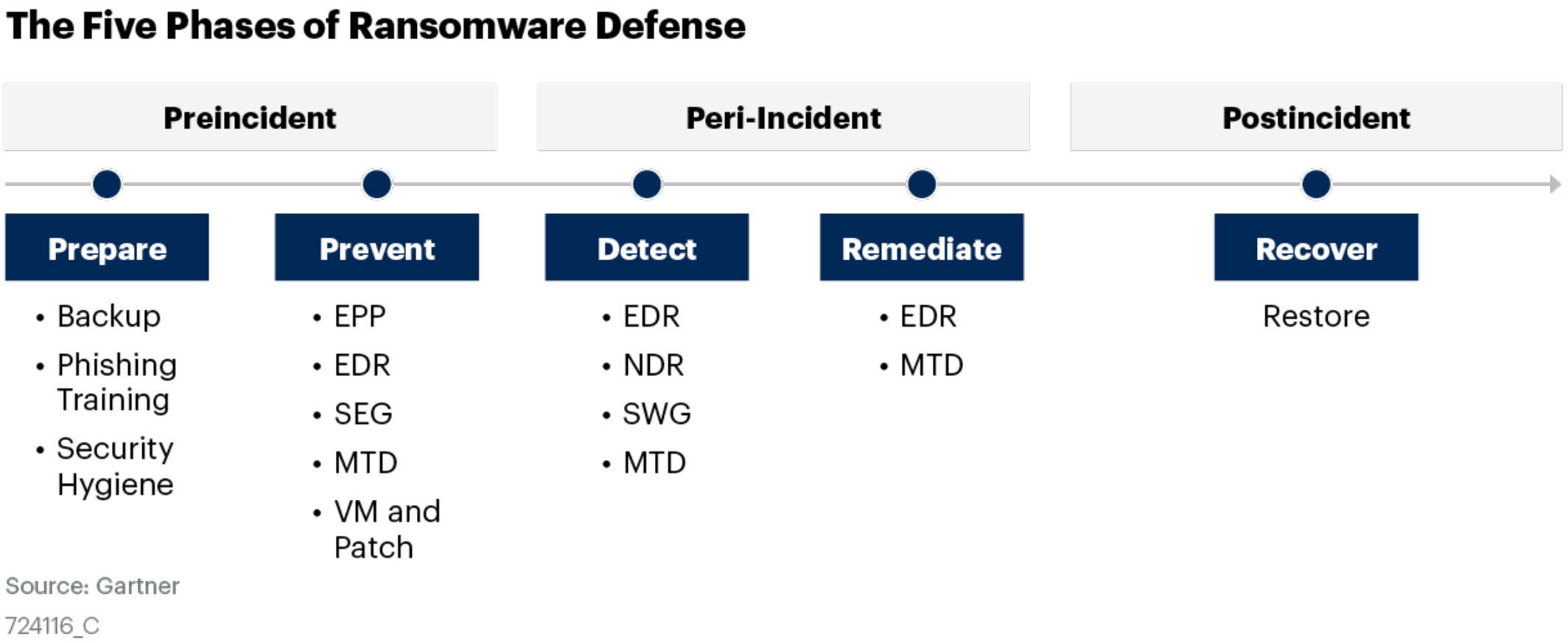
The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively. To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations.

The technical security controls



Requirement for backups of all systems ($$$$$)

- Backups must be kept offline/encrypted when not actively receiving back up information.
- Backups must be segmented from other networks so that an attack against production systems can not impact the back ups.
- Backups must be encrypted using a certificate store dedicated to the backup infrastructure which creates a dependency on services for restoration.
- Backing up a personal computer or server is easy compared to backing up a cloud instance. Consider built in cloud tools for sharing/replication.

Stop phishing and similar ($$)

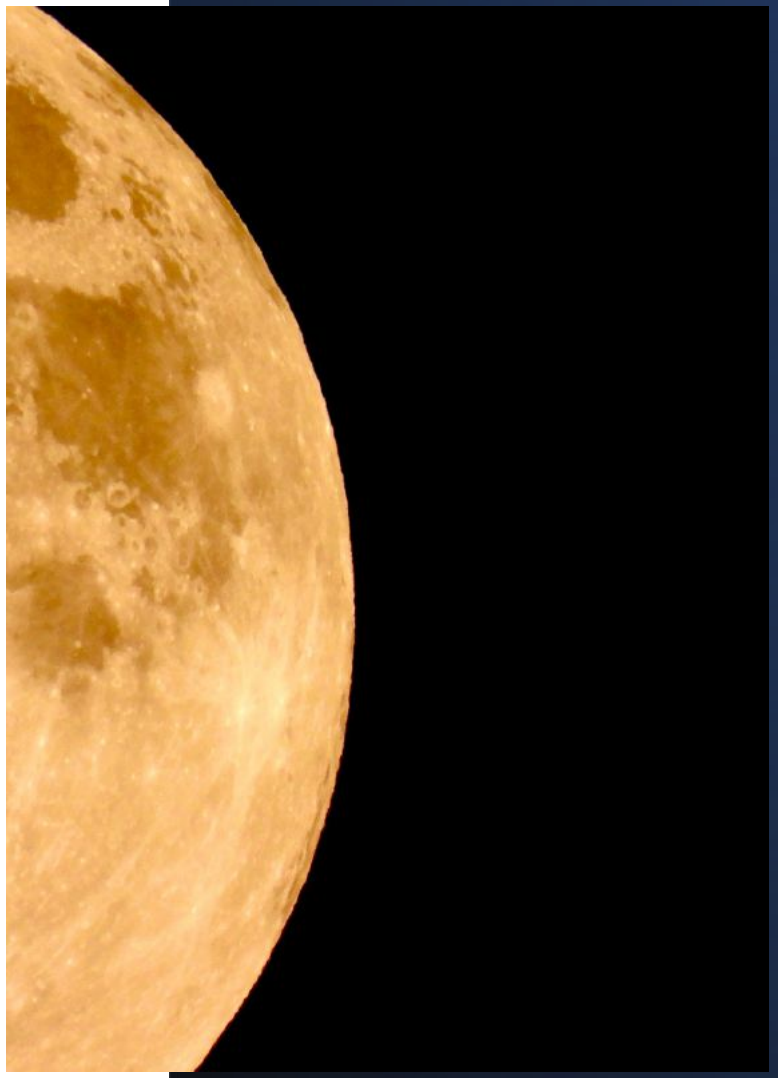
- Require email security to robustly block and cleanse emails with a default denial to use of email as a file transfer mechanism.
- Require vendor review of security settings
  - Microsoft Security team review of O365
  - Google Security team review Gsuite
- Stop using communication tools that ask users to “click a link” to find out more.
- Suggest that external emails be marked with a header at top and bottom as “External Email Be Careful With Links”
- Suggest all links in emails be overwritten with HXXPS:// (you can’t drop malware you can’t get to).
- Use vendor security tools like the deployment of Microsoft Defender on all servers and Domain Controllers.

Internet facing systems zero vuln ($$$)

- Remediate all vulnerabilities within 24 hours for external facing systems (requires a dedicated patching team empowered to take action) and a software bill of materials for dependency walks
- End of life or extended service licensed systems should have a steep glide slope to retirement.
- Require all external facing system segmentation at the physical layer from internal assets (virtualized servers sharing a backplane breaking the barrier are an issue)
- Make sure logical controls like domain controllers are segmented and can not update each other. Why do you have active directory?
- No RDP, SMB 1 or 2, or similar services on external systems.

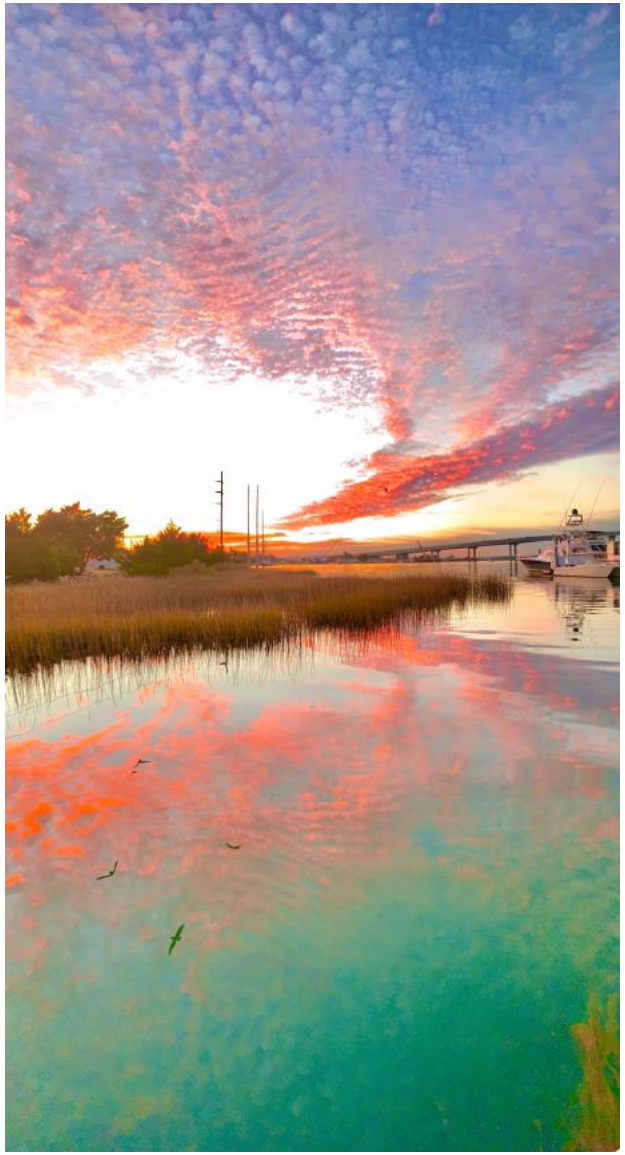
Stop ransomware ($)

- Segment networks working towards a zero-trust network/architecture strategy.
  - Step 1, segment by campus
  - Step 2, segment by building
  - Step 3, segment by floor or workspace
  - Step 4 segment by user
- Consider an architectural requirement of “recovery by organization” as a guiding principle.
- All network segments shall pass through a firewall/IDS as an inspection point.



Third parties and third-party processors ($$$)

- All data transactions need to go through a firewall and intrusion detection system (IDS) before entering the enclave of the organization
  - The traditional evolving organizational architecture is an organic logical mesh
  - Deploy actionable, resilient, blocking and detection across the enterprise
  - This will be a BIG issue within some product environments
- All data transactions need to go through a firewall and IDS before moving between product and corporate either direction
  - Need to reduce the bastion hosts or jump point servers to one with backup
  - Need to deploy a data loss prevention (DLP) solution in line with the firewall and intrusion detection system (IDS)

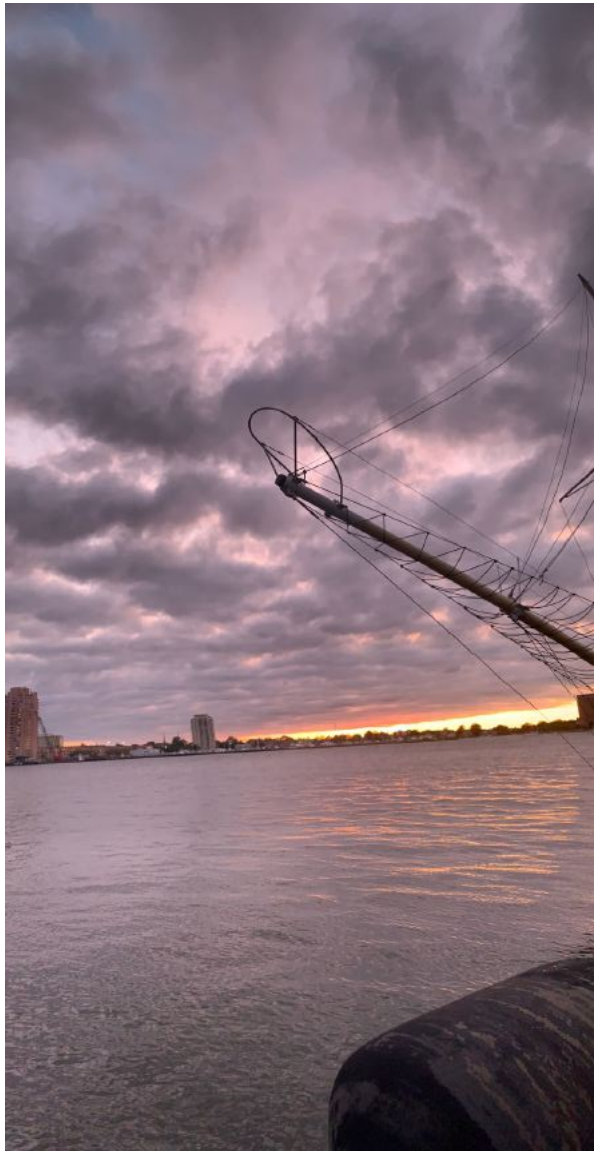


Minimum host/server/system security controls

- Antivirus
- Endpoint Detection Response (EDR) (HX, CrowdStrike or similar)
- Identity protections (Defender, ForgeRock, or similar)
- Multiple Factor Authentication (MFA) to access
- Encrypted file system
- Rotating administrator passwords
- Hardened Domain Controller GPOs
- Constant back ups of data and configuration

Harden all systems against malware and ransomware

- Utilize the best practices of STIGs for operating systems documenting the current build practice with security review
- Privileged, executive, root accounts shall not be used for commodity applications and shall be banned from using email, collaboration, etc. utilities. Test accounts must be reset after every use.
- MFA should be deployed to all systems, accounts, and any exceptions shall be hardened and use restricted
- The MFA broker (other factor) and agent (system) must not reside on the same logical or physical infrastructure.
- PowerShell specifically shall be restricted, and the zones of use shall be determined and logged.
- Harden domain controller (Microsoft Defender)

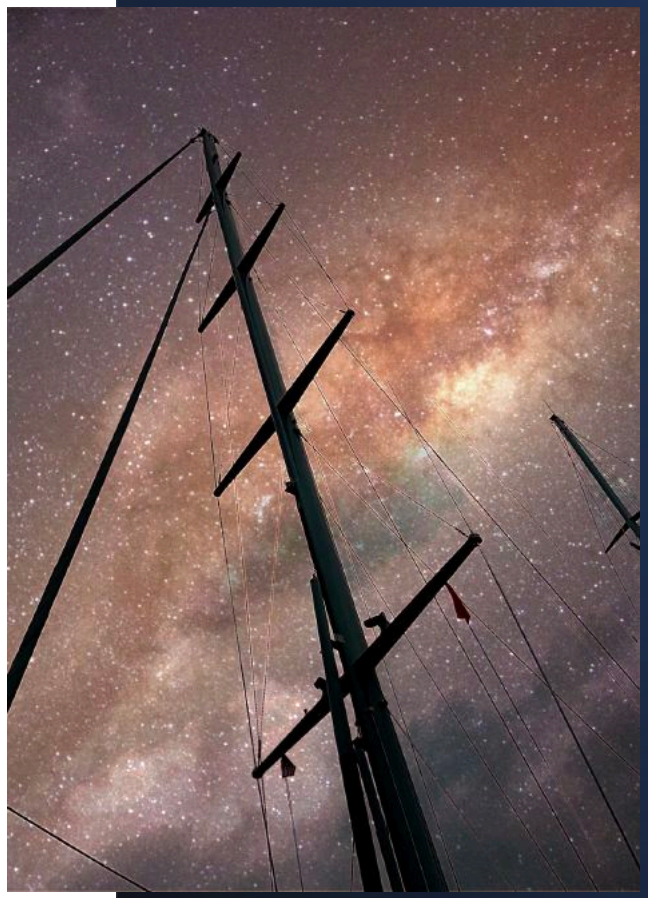


Know what you have

- All software, hardware, virtual assets need to be in an asset management tool and tracked in REAL time
- Inventory systems should be accessible from outside the environment
- Network access shall be controlled through the deployment of a network access control technology
- Scanning of all corporate, engineering, product, VPN environments will be accelerated, and systems not tagged as scanned will through network access control be scanned before connecting

Knowledge, Skills, Abilities

- You should understand the concept of ransomware groups as a business and contractor to the nation state
- You should understand the alignment of actionable ransomware defense toward a national strategy
- You should be able to explain the concepts of segmentation, offline back ups, and a general idea of prioritization
- You should be able to express how the security controls work together to interrupt the ransomware attack chains




Any questions before I leave?