Threat Hunting with Microsoft Sentinel and Defender Unified Environment

---

By Grant Knoetze

What is Microsoft Sentinel

- It is a Security Incident and Event Management Tool.
- It allows an organization to collect data (logs), analyse, and perform security operations on its computer systems, that can be hardware applications, applications, or both.

Outcomes

- To understand APT attacks & targeted ransomware attacks' tactics & techniques and learn how to respond to them
- To learn how to perform in-depth investigation if needed to
- To learn how to perform threat hunting to detect attacks in early stages and creating new alerts for actively used techniques

Agenda For The Training

- Understanding the threat hunting process, including developing a hypothesis.
- Utilizing Cyber Threat Intelligence for threat hunting operations in Microsoft unified SIEM/XDR.
- Utilizing Kusto Query Language (KQL) at a later stage and performing hunts using it.

Intro to APT Attacks & MITRE ATT&CK

What's an APT Attack?

- APT stands for "Advanced Persistent Threats"
- It's Targeted attacks
- Stays for long time hidden in the organization
- Mostly carried by professional group of hackers (actors)
- These groups can be:
  - Nation state (intel agencies)
  - Professional hackers for hire
  - Financially targeted hackers
  - Activists

Why Companies Care about APT Attacks?

BRIEF

Boeing, Tesla manufacturer breached after ransomware attack

When the screens went black: How NotPetya taught Maersk to rely on resilience – not luck – to mitigate future cyber-attacks

Adam Bannister 09 December 2019 at 12:09 UTC
Updated: 09 December 2019 at 13:06 UTC

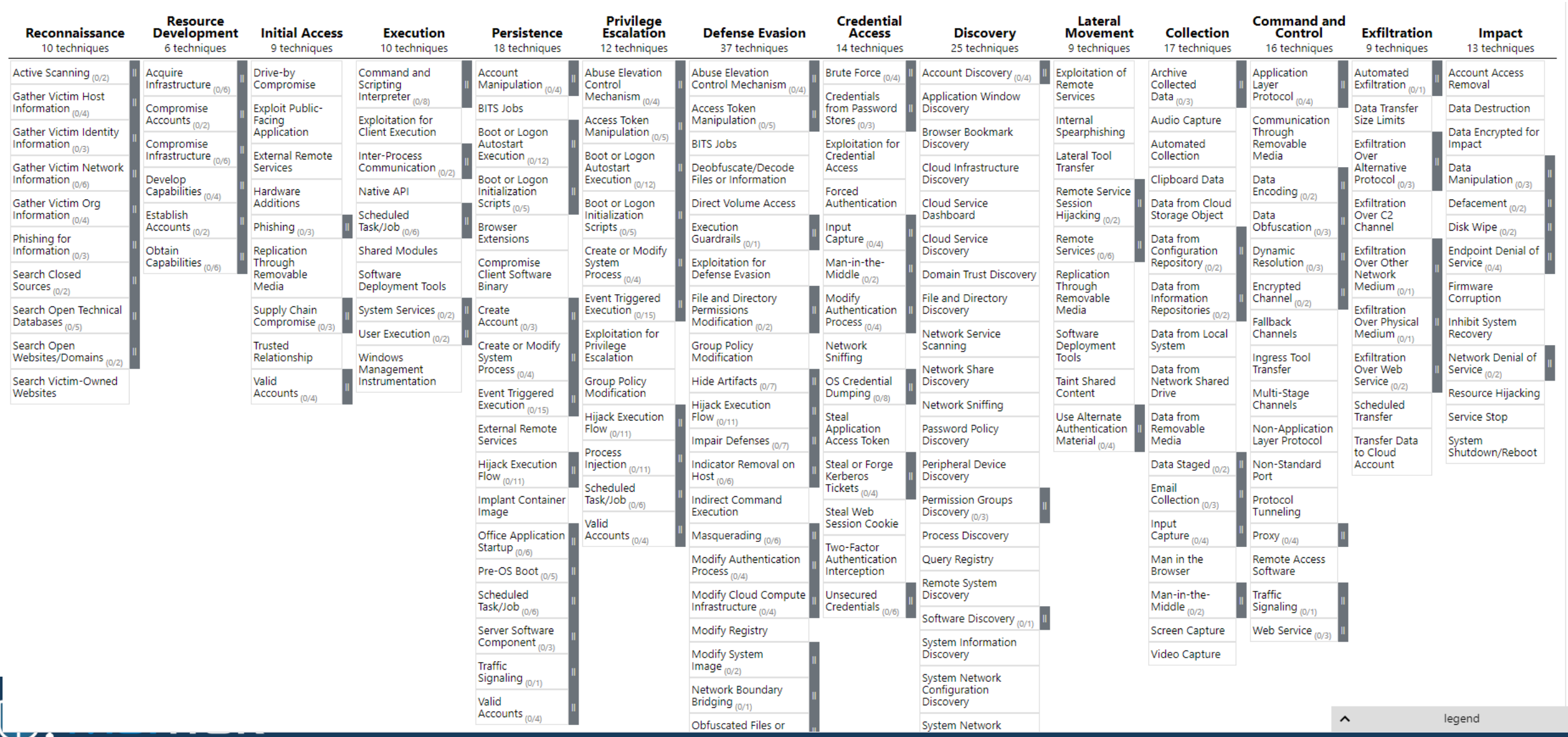
Ransomware | Cyber-attacks | Maritime

The APT Attack Process: Cyber kill chain

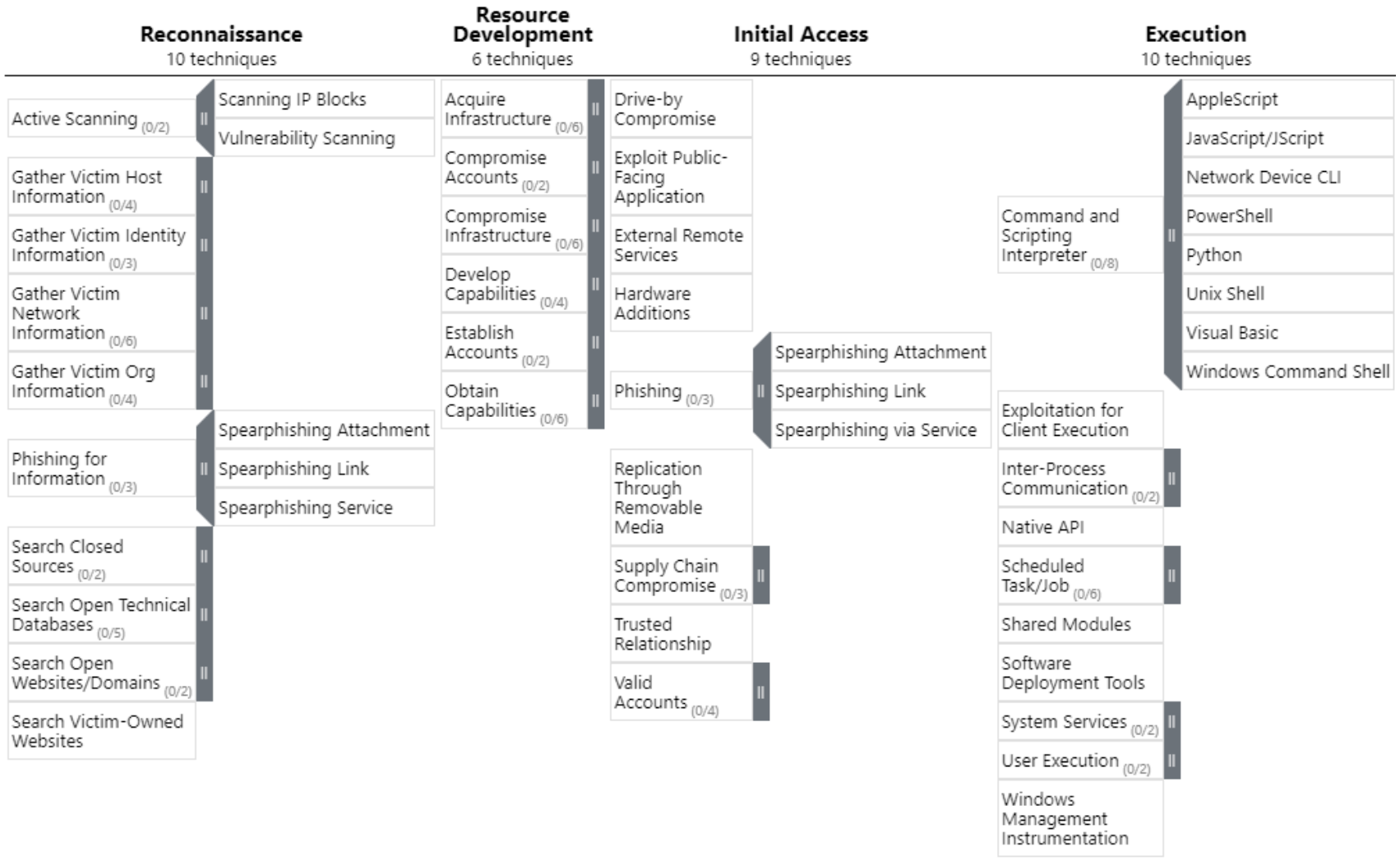
So, What's Cyber Kill Chain?

"The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs)."

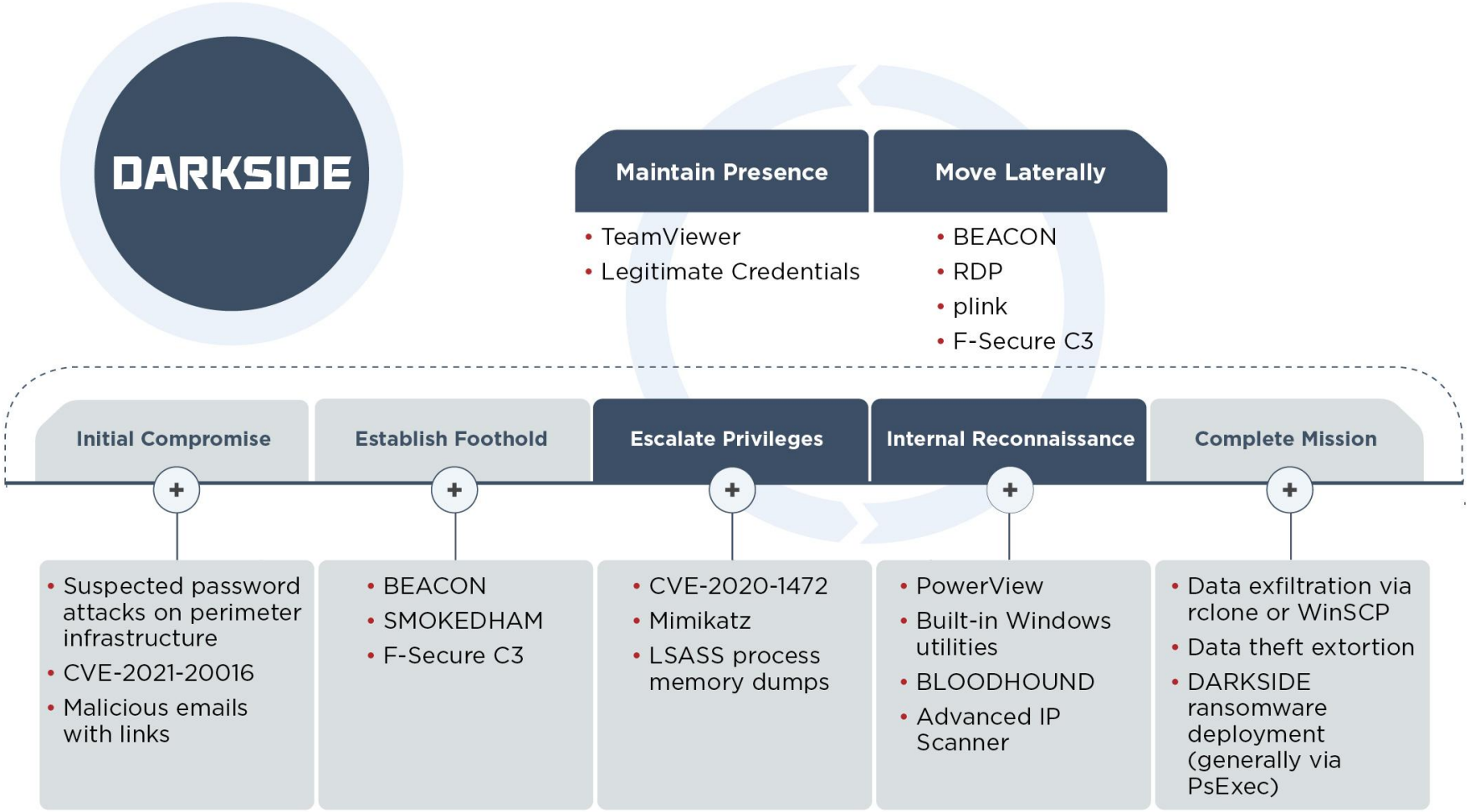
MITTRE ATT&CK



MITTRE ATT&CK: Sub-Techniques



Case Study: DARKSIDE Ransomware



Case Study: DARKSIDE Ransomware

- Ransomware-as-a-Service (RaaS)
- Used by different groups
- **UNC2465 Actor Attack Lifecycle:**
  - **Initial Access:** Used Spearphishing with Dropbox Link
  - **1st Stage:** a zip file with .LNK downloads a .Net Backdoor
  - **2nd Stage:** SMOKEDHAM .Net backdoor included keylogging functionality
  - **Privilege Escalation:** Through Mimikatz
  - **Reconnaissance:** Blookhound (for mapping the targets to the AD), Advanced IP Scanner
  - **Lateral Movement:** Stolen Credentials, NGROK tunneling for RDP ports, PsExec & cron jobs (like scheduled tasks but for linux)
  - Deployed **DARKSIDE** ransomware for encryption & exfiltration

Case Study: DARKSIDE Ransomware

- **UNC2659 Actor Attack Lifecycle:**
  - **Initial Access:** Used a SonicWall VPN Vulnerability
  - **Persistence:** Using TeamViewer
  - **Exfiltration**: rclone (legitimate application) to the cloud)

Case Study: DARKSIDE Ransomware

- **UNC2628 Actor Attack Lifecycle:**
  - **Initial Access:** Password Spraying Attack on the Corporate VPN
  - **Persistence:** Cobalt Strike BEACON & Malicious Domain Account **“spservice”**
  - **Privilege Escalation:** Through Mimikatz
  - **Reconnaissance:** BEACON & basic OS commands
  - **Lateral Movement:** Stolen Credentials, RDP and used BEACON communications to interact with the infected machines
  - **Exfiltration:** SFTP & RClone

Case Study: DARKSIDE Ransomware

- **DARKSIDE Functionality:**
  - Encrypt local disks and network shares
  - Delete volume shadow copies
  - Empty Recycle Bins
  - Perform UAC bypass
  - Terminate processes & stopping services
  - And much more
- **More Info:** https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

Case Study: From Zero To Domain Admin

From Zero to Domain Admin

- 16:30 UTC Hancitor Execution via Word
  - Hancitor DLL dropped and run
- 16:31 UTC First Cobalt Strike loaded by Hancitor
  - C2: 207.148.23.64:80/443
- 16:33 UTC Domain and Local Admin Recon
  - nltest /dclist:domain, ping DC, net group "Domain Admins" /domain
  - cmd.exe /C dir \\X.X.X.Y\c$
- 17:13 UTC Hancitor loads second Cobalt Strike beacon on beach head host
  - C2: 190.114.254.116:80
- 17:15 UTC Lateral Movement with Cobalt Strike
  - Cobalt Strike copied and run on two servers
  - Agent1.ps1 downloaded and executed on one of the servers
- 17:23 UTC Zerologon Exploited
  - zero.exe x.x.x.x DC domain.local administrator -c "powershell.exe"
- 17:29 UTC Lateral Movement to Domain Controllers
  - Cobalt Strike copied and run on Domain Controllers
- 17:58 UTC Computer Discovery via ICMP
  - check.exe comps.txt check.txt -ip run
- 18:02 UTC Final Lateral Movement to File Server
  - Cobalt Strike copied and run

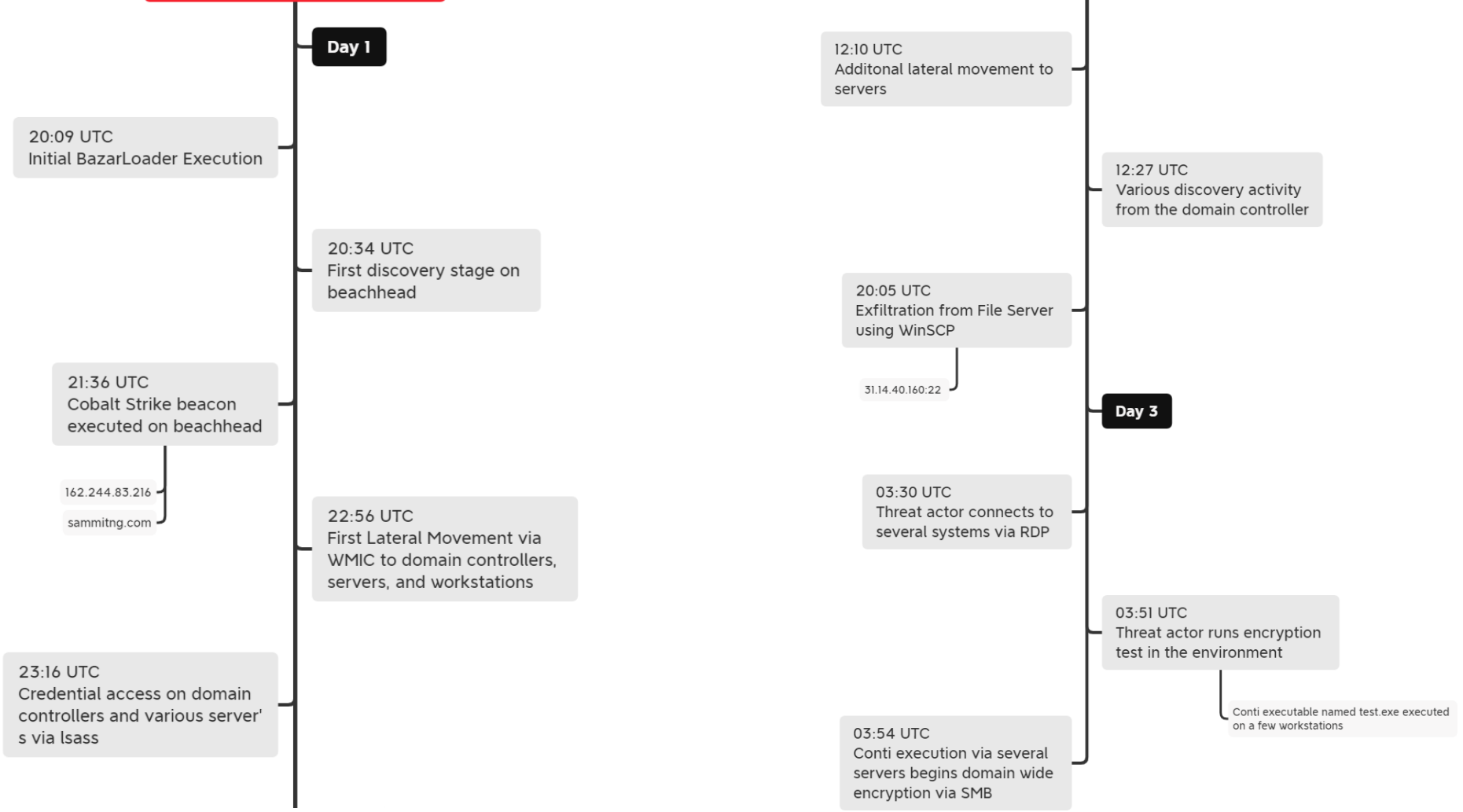
Hancitor Process Tree

- WINWORD.exe — **Parent Process**
  - **Child Process** — C:\Windows\System32\rundll32.exe" c:\users\$USER\appdata\roaming\microsoft\templates\ier.dll,HEEPUBQQNOG
    - Process Injection
      - **svchost.exe**
        - **Child Processes**
          - rundll32.exe — Port Scanning 445, 5000, 6136, 9392
          - rundll32.exe
            - cmd.exe /C dir \\IP_ADDR\c$
            - cmd.exe /C copy cor.bat \\IP_ADDR\C$\programdata
          - cmd.exe
            - cmd.exe /c nslookup
            - cmd.exe /c ping DOMAIN_CONTROLLER
            - cmd.exe /C net time
            - cmd.exe /C Net group "Domain Admins" /domain

Source: thedfirreport.com

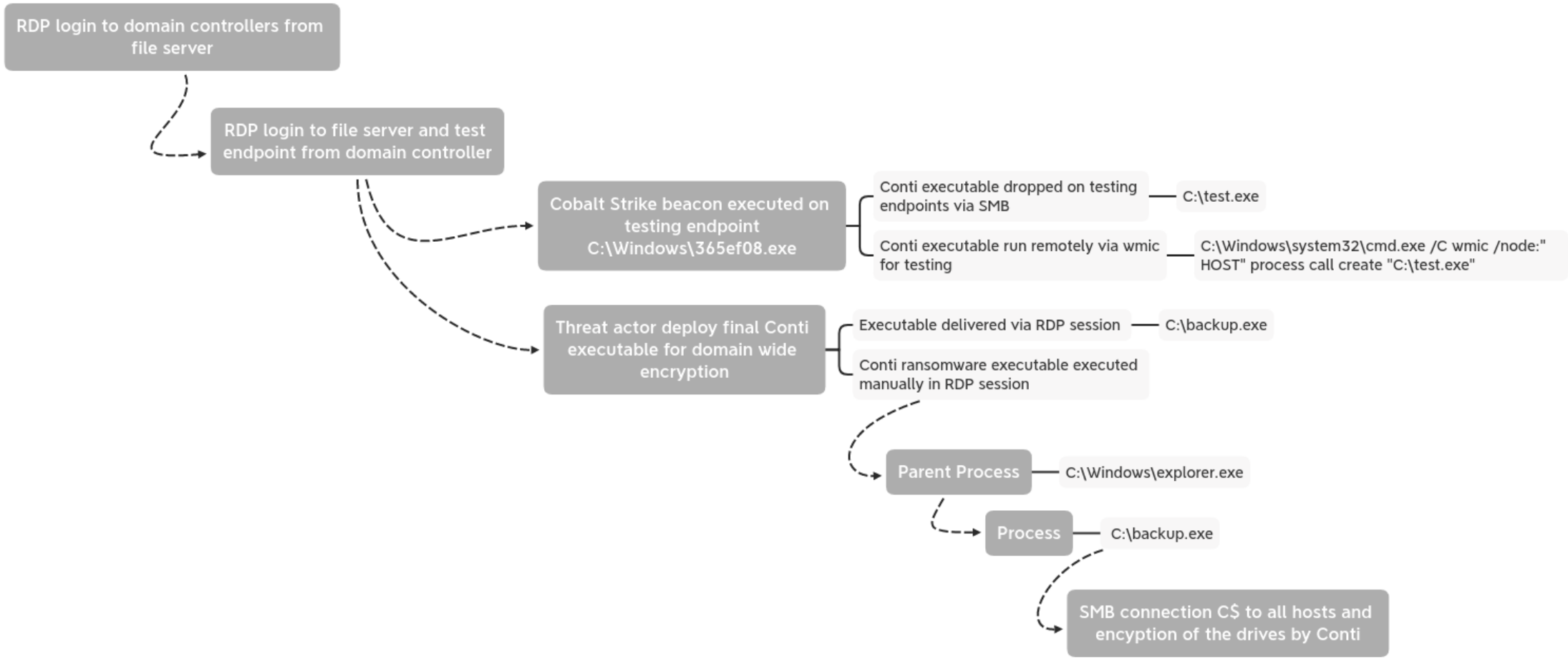
Case Study: Conti Ransomware

BazarLoader to Conti Ransomware in 32 Hours



Source: thedfirreport.com

Conti Ransomware Deployment



Source: thedfirreport.com

What’s common between these attacks?

- Targeting endpoints first and then move laterally in the organization
- Use of legitimate applications such as:
  - ADFind
  - WinSCP
  - Teamviewer
- Use of legitimate accounts to move laterally inside the organization.

  Mostly stolen through spear-phishing or lsass memory dumps

Threat Hunting Process

- Understanding the Threat Hunting Process
- Including Developing a Hypothesis

Agenda

- Introduction to Threat Hunting
- Key Concepts and Importance
- Threat Hunting Process Overview
- Developing a Hypothesis
- Tools and Techniques
- Real-World Examples
- Conclusion

What is Threat Hunting?

- Definition: Proactive cybersecurity methodology to identify threats missed by automated tools.
- Focus: Human-driven, hypothesis-based process.

Why is Threat Hunting Important?

- Identifying unknown or advanced threats.
- Reducing dwell time of attackers.
- Enhancing overall security posture.

Key Principles of Threat Hunting

- Proactive vs. Reactive
- Hypothesis-Driven
- Iterative Process

Common Threats Identified During Hunting

- Insider threats
- Advanced Persistent Threats (APTs)
- Malware and ransomware
- Lateral movement within networks

Threat Hunting Process Overview

- Phase 1: Hypothesis Development
- Phase 2: Data Collection
- Phase 3: Investigation and Analysis
- Phase 4: Mitigation and Reporting

Phase 1: Developing a Hypothesis

- Definition: An educated guess about potential threats in the environment.
- Purpose: Guide the hunting process and focus efforts.

Sources for Hypothesis Development

- Threat Intelligence Feeds
- Known Attack Patterns (e.g., MITRE ATT&CK)
- Behavioral Anomalies
- Historical Data
- Suspicious Indicators

Examples of Hypotheses

- “Threat actors are using compromised credentials to access sensitive systems.”
- “Lateral movement is occurring using pass-the-hash techniques.”
- “A phishing campaign is targeting specific employees.”

Key Questions to Guide Hypotheses

- What assets are attackers likely targeting?
- What TTPs (tactics, techniques, procedures) might they use?
- What gaps exist in current defenses?

Phase 2: Data Collection

- Collect logs, network traffic, endpoint data, etc.
- Focused on data relevant to the hypothesis.

Data Sources for Threat Hunting

- SIEM (Security Information and Event Management) tools
- EDR (Endpoint Detection and Response) solutions
- Network Traffic Analysis tools
- Threat intelligence platforms

Phase 3: Investigation and Analysis

- Techniques: Pattern recognition, anomaly detection, and behavioral analysis.
- Identify indicators of compromise (IOCs)

Key Analysis Techniques

- Timeline reconstruction
- Correlation of events
- Behavioral profiling

Phase 4: Mitigation and Reporting

- Document findings and evidence.
- Collaborate with incident response teams.
- Recommend security improvements.

Tools for Threat Hunting

- Example tools: Splunk, ELK Stack, Wireshark, and Sysmon.
- Importance of automation and analytics in augmenting manual efforts.
- We will be focusing on using the Microsoft unified environment which is Azure Sentinel for SIEM/SOAR and Defender XDR.

Challenges in Threat Hunting

- Data overload
- Sophistication of attackers
- Skill and resource gaps

Benefits of Threat Hunting

- Improved detection capabilities
- Reduced risk of breaches
- Enhanced understanding of adversaries

Metrics for Success

- Threats identified
- Mean time to detection (MTTD)
- False positive rate

Developing a Threat Hunting Program

- Training for analysts.
- Investing in appropriate tools.
- Continuous process improvement.

The Role of Hypothesis in Threat Hunting

- Central to focusing effort.
- Links strategic goals to actionable steps.

Recap of the Threat Hunting Process

- Hypothesis → Data Collection → Investigation → Mitigation.

Final Thoughts

- Continuous improvement is key.
- Collaboration with other security teams is essential.