

hid01.ir

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.

hid01.ir

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



Two years after WannaCry, a million computers remain at risk

The threat posed by the leaked NSA tools remains a

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)."

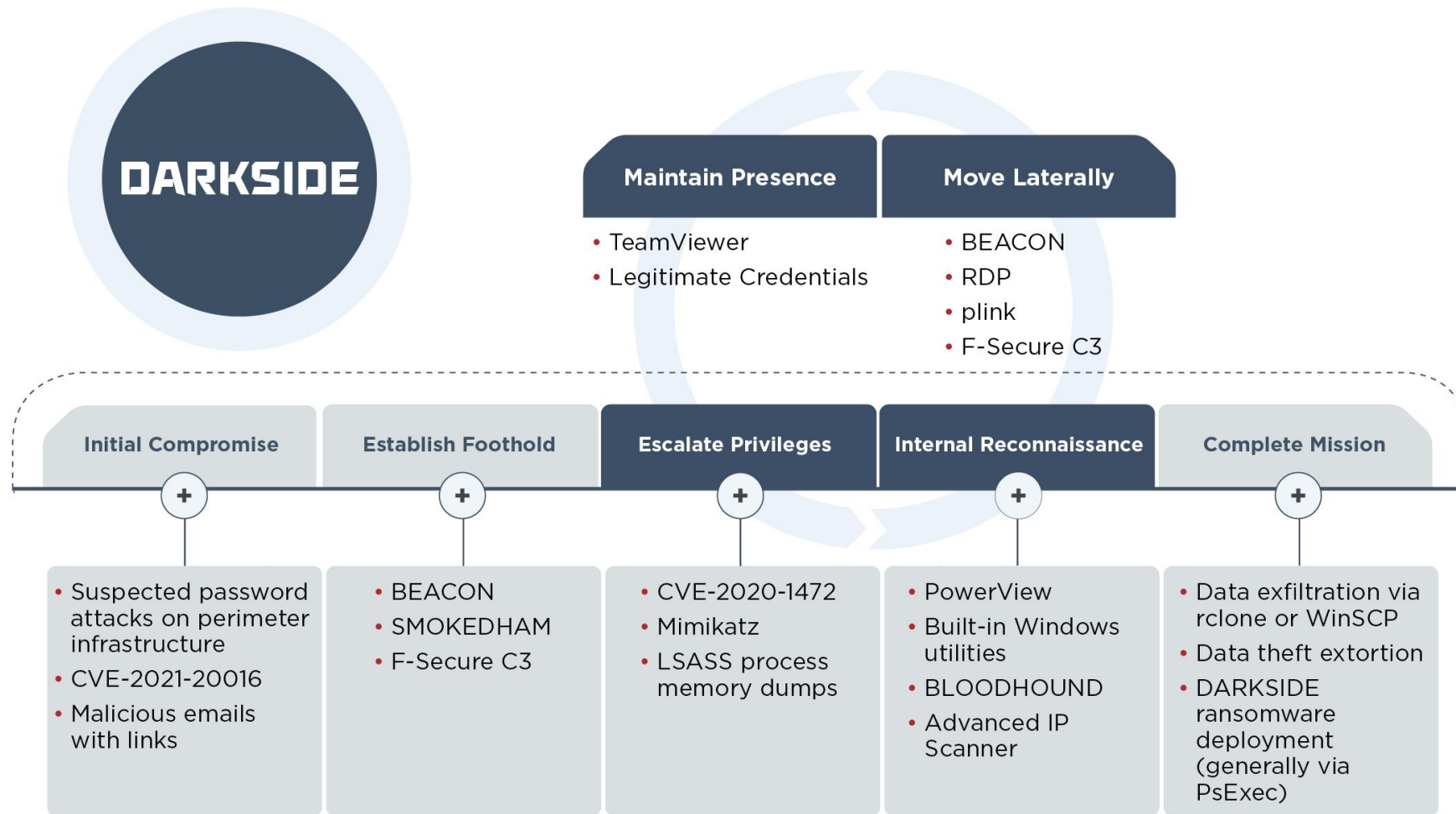
MITTRE ATT&CK

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Data from Cloud Storage Object	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Configuration Repository (0/2)	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (0/2)	Inhibit System Recovery	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	Group Policy Modification	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Network Denial of Service (0/2)	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Windows Management Instrumentation	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Resource Hijacking
Search Victim-Owned Websites				External Remote Services	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Service Stop
				Hijack Execution Flow (0/11)	Process Injection (0/11)	Impair Defenses (0/7)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Application Layer Protocol		System Shutdown/Reboot
				Implant Container Image	Scheduled Task/Job (0/6)	Indicator Removal on Host (0/6)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Non-Standard Port		
				Office Application Startup (0/6)	Valid Accounts (0/4)	Indirect Command Execution	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Protocol Tunneling		
				Pre-OS Boot (0/5)		Masquerading (0/6)	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Proxy (0/4)		
				Scheduled Task/Job (0/6)		Modify Authentication Process (0/4)		Process Discovery		Man-in-the-Middle (0/2)	Remote Access Software		
				Server Software Component (0/3)		Modify Cloud Compute Infrastructure (0/4)		Query Registry		Screen Capture	Traffic Signaling (0/1)		
				Traffic Signaling (0/1)		Modify Registry		Remote System Discovery		Video Capture	Web Service (0/3)		
				Valid Accounts (0/4)		Modify System Image (0/2)		Software Discovery (0/1)					
						Network Boundary Bridging (0/1)		System Information Discovery					
						Obfuscated Files or		System Network Configuration Discovery					
								System Network					

MITTRE ATT&CK: Sub-Techniques

Reconnaissance 10 techniques		Resource Development 6 techniques		Initial Access 9 techniques		Execution 10 techniques	
Active Scanning (0/2)	Scanning IP Blocks	Acquire Infrastructure (0/6)	Drive-by Compromise			AppleScript	
	Vulnerability Scanning	Compromise Accounts (0/2)	Exploit Public-Facing Application			JavaScript/JScript	
Gather Victim Host Information (0/4)		Compromise Infrastructure (0/6)	External Remote Services			Network Device CLI	
Gather Victim Identity Information (0/3)		Develop Capabilities (0/4)	Hardware Additions			PowerShell	
Gather Victim Network Information (0/6)		Establish Accounts (0/2)				Python	
Gather Victim Org Information (0/4)		Obtain Capabilities (0/6)	Phishing (0/3)			Unix Shell	
	Spearphishing Attachment			Spearphishing Attachment		Visual Basic	
Phishing for Information (0/3)	Spearphishing Link			Spearphishing Link		Windows Command Shell	
	Spearphishing Service			Spearphishing via Service			
Search Closed Sources (0/2)		Replication Through Removable Media				Exploitation for Client Execution	
Search Open Technical Databases (0/5)		Supply Chain Compromise (0/3)				Inter-Process Communication (0/2)	
Search Open Websites/Domains (0/2)		Trusted Relationship				Native API	
Search Victim-Owned Websites		Valid Accounts (0/4)				Scheduled Task/Job (0/6)	
						Shared Modules	
						Software Deployment Tools	
						System Services (0/2)	
						User Execution (0/2)	
						Windows Management Instrumentation	

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

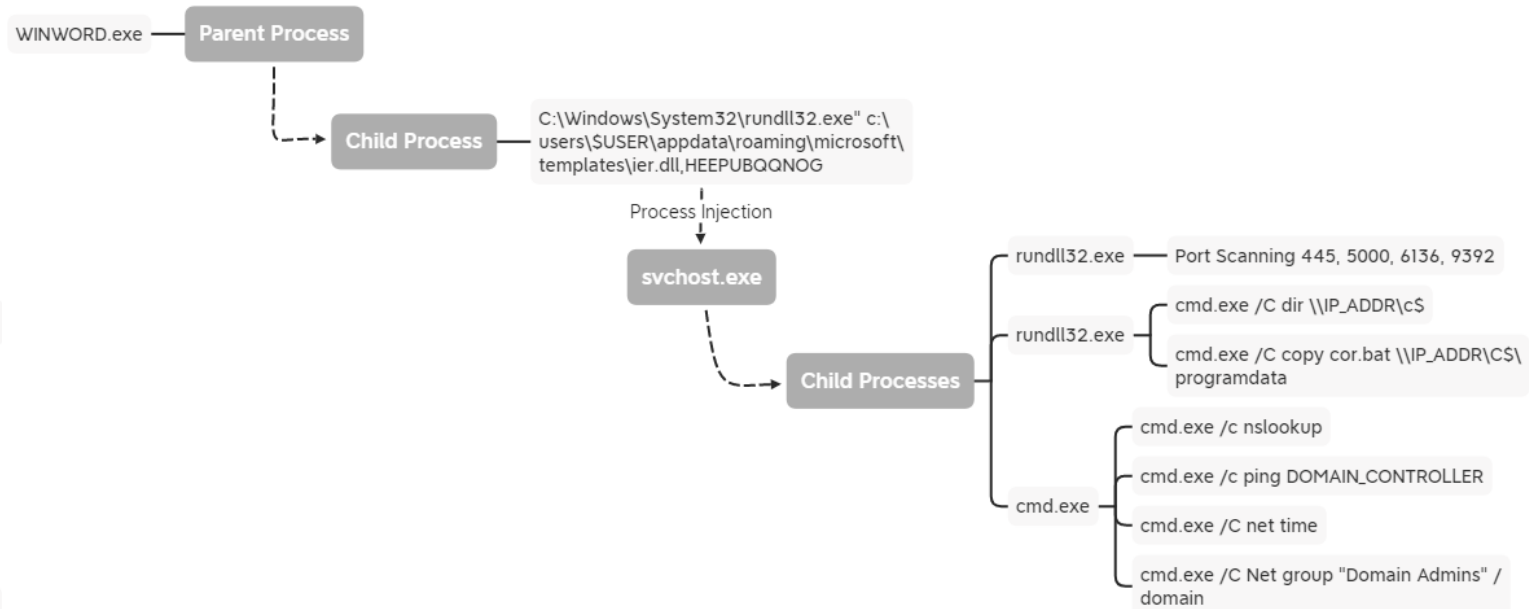
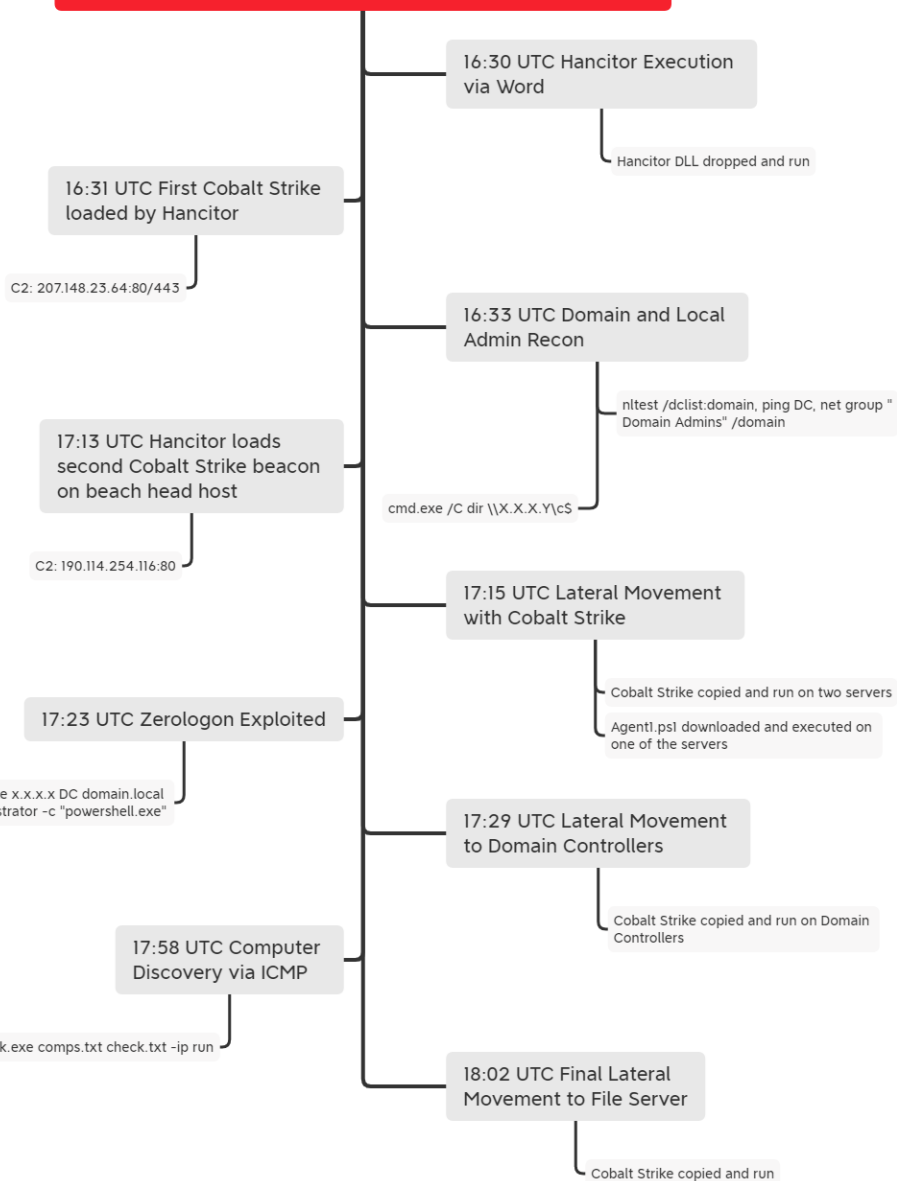
- **DARKSIDE Functionality:**

- 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>

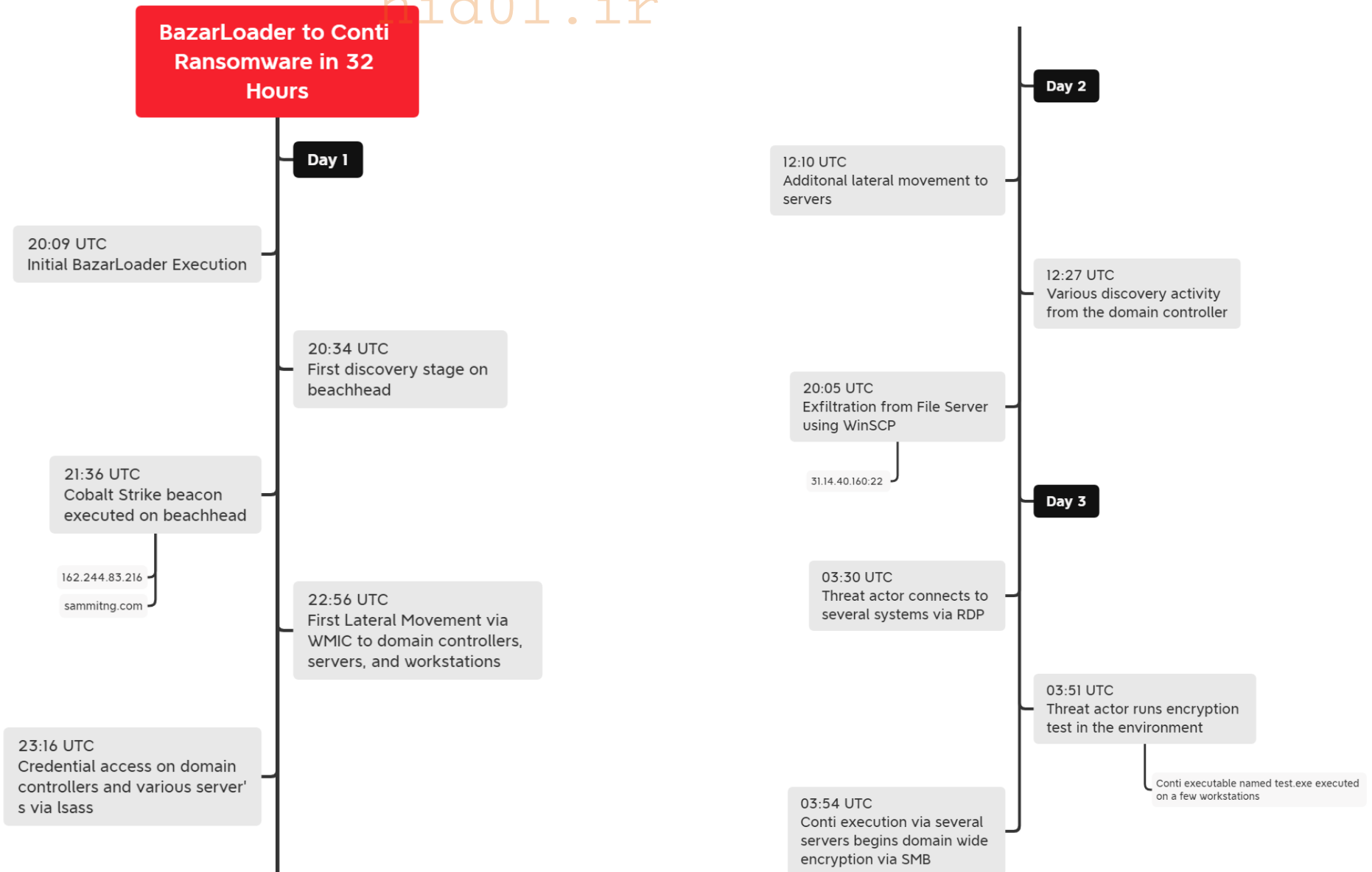
Case Study: From Zero To Domain Admin

From Zero to Domain Admin



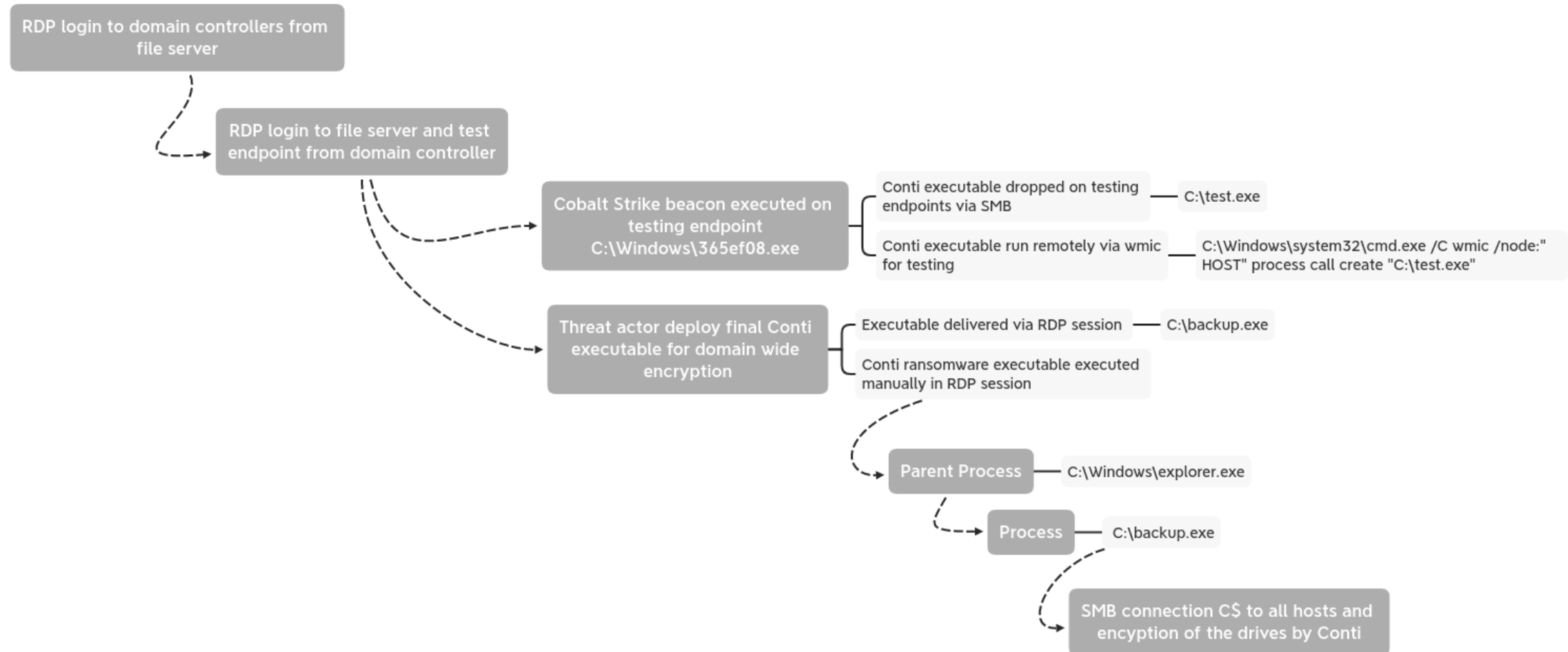
Source: thedfirreport.com

Case Study: Conti Ransomware



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.