WHITE PAPER

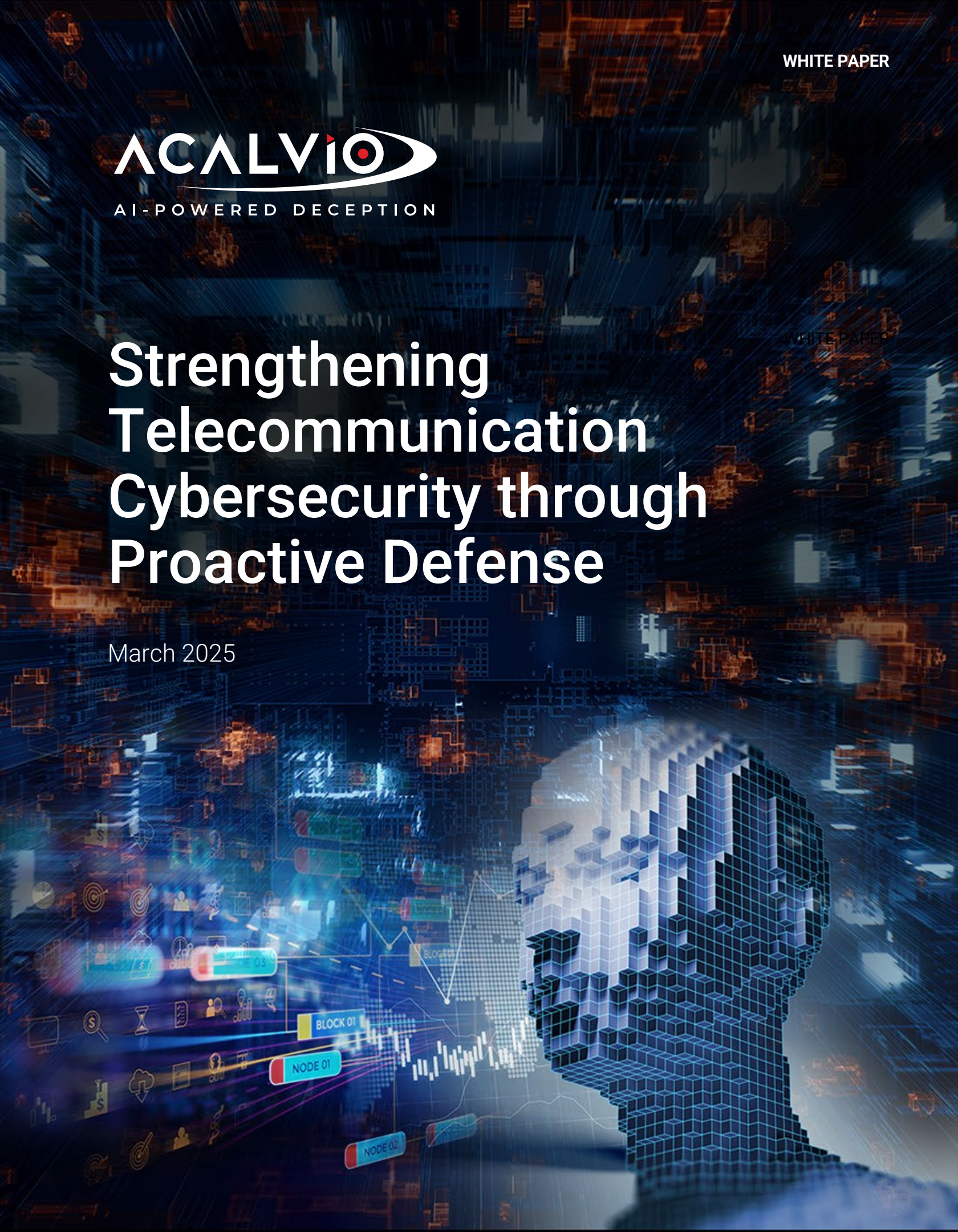
ACALVIO

AI-POWERED DECEPTION

WHITE PAPER

Strengthening Telecommunication Cybersecurity through Proactive Defense

March 2025



Strengthening telecommunication cybersecurity through proactive defense

The telecommunications industry faces a growing onslaught of sophisticated cyber threats, highlighted by the "Salt Typhoon" campaign that compromised over eight major telcos. This attack demonstrated not only the vulnerabilities inherent in existing defenses but also the extraordinary persistence and reach of advanced threat actors. With extended access to critical environments and exfiltration of sensitive data, including high-value communications, Salt Typhoon underscores the urgent need for elevated cybersecurity measures tailored to counter evolving and persistent threats.

Active Defense offers a transformative approach to address these challenges, empowering organizations to move beyond reactive strategies and adopt proactive methods to detect and disrupt attackers. At the heart of Active Defense is cyber deception, a strategy that employs realistic traps such as honeytokens and network decoys to anticipate attacker behavior, lure them into controlled environments, and gather actionable intelligence. By integrating deception into their defenses, telecommunications organizations can gain critical early-warning capabilities and reduce the risk of significant breaches while adapting to the ever-changing threat landscape.

"As attackers leverage advanced tactics and persistence mechanisms, organizations must rethink their approach to cybersecurity," says Ed Amoroso, CEO of Tag Infosphere. "Deception technologies are proving to be a game-changer, enabling early detection and offering insights into adversary behaviors that were previously unattainable."

Ed Amoroso
CEO, Tag Infosphere

Telco Environments: A Prime Target for Cyber Attacks

The telecommunications sector continues to experience relentless and sophisticated cyber threats. In 2024, the “Salt Typhoon” campaign executed the largest attack against U.S. telcos, exfiltrating sensitive data, including call records and communications involving high-ranking officials. Despite extensive investigations, it remains uncertain whether the threat actors have been fully evicted, underscoring the challenge of countering advanced persistence mechanisms.

While Salt Typhoon brought renewed attention to these risks, similar attack variants have targeted telecommunications firms for years. Groups like “Volt Typhoon” exemplify the sustained and evolving nature of these exploits. The strategic importance of telecommunications ensures it will remain a priority target, with adversaries adapting their tactics and leveraging the latest advancements to achieve their objectives.

Attacker Objectives: Long-Term Espionage and Data Exfiltration

Telecommunications organizations and ISPs are critical targets for advanced threat actors due to the strategic value of their data. Call records, movement logs of high-profile individuals, and corporate communications represent key assets for long-term espionage and sustained data exfiltration operations.

Attackers prioritize critical services, such as database servers and cloud infrastructures, leveraging these environments to establish deep persistence. With extended access, they intercept sensitive communications, extract high-value data, and maintain operational stealth to evade detection for months, if not longer.

The reliance of telcos on vast vendor ecosystems presents another critical vulnerability. Threat actors exploit these trusted relationships to propagate laterally across supply chains, magnifying their operational impact and creating cascading risks across interconnected organizations.

Persistence and Stealth: Threat Actors' Operational Edge

The Salt Typhoon attacks against leading telecommunications organizations exposed the alarming sophistication of modern threat actors, who remained undetected for months. Their ability to establish deep persistence highlights the maturity and effectiveness of their methods.

Initial access often exploits vulnerable edge devices—such as routers and gateways—with privileged access to core environments. Many of these devices are legacy systems riddled with unpatched vulnerabilities. Security teams face compounded challenges due to incompatibility with endpoint detection and response (EDR) solutions and limited log visibility. Even when logs are accessible, proprietary formats complicate forensic analysis, further delaying detection.

Once inside, attackers employ living-off-the-land (LotL) techniques, utilizing legitimate OS tools like WMIC, PSExec, and ProcDump for reconnaissance, credential harvesting, and lateral movement. Additional utilities, such as CertUtil and BITSAdmin, facilitate the stealthy download of malicious payloads from command-and-control (C2) servers.

To maintain persistence and evade detection, Salt Typhoon leverages modular, custom malware like SparrowDoor, Demodex, SnappyBee, and Ghostspider. These tools employ advanced techniques such as DLL search order hijacking, obfuscated payloads, and in-memory rootkits. The modular design and advanced obfuscation make these malware families highly adaptable, enabling attackers to evolve their tactics dynamically and remain undetected in even well-monitored environments.

Modular Malware and Advanced Persistence Mechanisms

Ghostspider exemplifies the sophistication of modern modular malware, leveraging reflective loading to evade detection. Its architecture, controlled via specific command codes from the C&C server, enables dynamic evolution and adaptability. Individual components can be deployed or updated independently, allowing attackers to adjust functionality based on the phase of the attack or shifting operational goals. This modularity complicates detection and analysis, as offensive patterns continuously adapt. Key commands supported by Ghostspider include:

- **Upload:** Load malicious modules into memory for attacker-controlled task execution.
- **Create:** Initialize resources to activate loaded modules.
- **Normal:** Execute core functions, such as data exfiltration or system manipulation.
- **Close:** Remove active modules to minimize traces and free resources.
- **Update:** Modify behavior to adjust timing and communication intervals for enhanced stealth.
- **Heartbeat:** Maintain periodic contact with the C&C server to confirm accessibility.

Modular Malware and Advanced Persistence Mechanisms (cont.)

Demodex, a rootkit designed for persistence, employs advanced anti-analysis techniques to evade detection. By removing PE headers from memory and implementing obfuscation strategies such as string encoding and API call masking, Demodex renders static analysis exceptionally difficult. Furthermore, these techniques bypass in-memory forensic tools like WinDbg and Volatility, presenting significant challenges for security teams attempting to analyze or disrupt its operation.

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration
T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1543 Create or Modify System Process	T1134 Access Token Manipulation	T1134 Access Token Manipulation	T1056 Input Capturer	T1482 Domain Trust Discovery	T1021 Remote Services	T1113 Screen Capture	T1071 Application Layer Protocol	T1567 Exfiltration Over Web Service
	T1047 Windows Management Instrumentation	T1547 Boot or Logon Autostart Execution	T1543 Create or Modify System Process	T1036 Masquerading		T1087 Account Discovery				
		T1574 Hijack Execution Flow	T1547 Boot or Logon Autostart Execution	T1027 Obfuscated Files or Information						
		T1078 Valid Accounts	T1574 Hijack Execution Flow	T1070 Indicator Removal						
		T1053 Scheduled Task/Job	T1078 Valid Accounts	T1574 Hijack Execution Flow						
			T1053 Scheduled Task/Job	T1562 Impair Defenses						
				T1078 Valid Accounts						

Figure 1: TTPs used by Salt Typhoon

Diverse and Evasive Exploit Techniques

Modern threat actor groups operate with a level of organization rivaling professional software development teams. Dedicated "infrastructure teams" design modular and highly evasive malware, while Malware-as-a-Service (MaaS) offerings provide baseline variants that attackers customize for each campaign. This streamlined approach enables rapid generation of unique malware variants tailored to specific operational goals, complicating detection and analysis.

The involvement of Advanced Persistent Threat (APT) groups like Volt Typhoon and Flax Typhoon in the telecommunications sector further amplifies the complexity. These actors share common tools and techniques, resulting in overlapping tactics, techniques, and procedures (TTPs). This convergence not only obfuscates attribution efforts but also introduces significant variation in offensive sequences, making defensive preparations more challenging.

Implications for Cyber Defense

The unprecedented access achieved by recent exploits like Salt Typhoon underscores the urgent need to reevaluate and strengthen telecommunications cybersecurity. The Federal Communications Commission (FCC) has responded with proposed measures to safeguard critical communications infrastructure, detailed in its directive, *"Fact Sheet: Implications of Salt Typhoon Attack and FCC Response."*

Key initiatives include:

Broader Action:

- Expanding cybersecurity requirements across a range of communication providers.
- Identifying additional ways to enhance cybersecurity defenses for communications systems.

Effective defense strategies must adopt a multi-layered, defense-in-depth approach. This involves reinforcing individual defense mechanisms while integrating complementary and interdependent layers to eliminate gaps and improve overall visibility. A critical component of this strategy is Active Defense, which empowers organizations to move beyond reactive measures and proactively engage with attackers. By incorporating techniques like cyber deception—such as honeytokens and decoys—Active Defense enables defenders to detect threats early, disrupt adversary operations, and gain actionable intelligence.

Such an approach provides greater resilience against sophisticated, evolving threats targeting the telecommunications sector while positioning defenders to anticipate and neutralize adversarial tactics.

Strengthening Prevention Controls

Recent campaigns have exploited vulnerabilities in edge devices, including Cisco routers and Ivanti firewalls, using “N-day” exploits—vulnerabilities targeted before organizations can apply patches. These attacks highlight the critical need to fortify prevention mechanisms.

The FCC’s directive outlines specific recommendations to strengthen prevention controls, including:

- **Decommissioning Legacy Systems:** Phasing out outdated equipment that poses significant security risks.
- **Accelerating Patch Cycles:** Increasing the speed and frequency of patch management to address known vulnerabilities promptly.
- **Hardening Configurations:** Reducing attack surfaces by enforcing secure configurations and eliminating weak defaults.

While these measures raise the bar for adversaries, no prevention strategy can fully eliminate risk. Advanced threat actors exploit gaps such as zero-day vulnerabilities, stolen credentials, and insider threats. To address these challenges, organizations must adopt an "assume breach" mindset, pairing robust prevention controls with advanced detection strategies to enhance visibility and coverage across the threat landscape.

Evolving Threat Detection Beyond TTP-Centric Approaches

Traditional threat detection relies heavily on TTP-centric methodologies, using rules, signatures, and behavioral patterns to identify “known bad” activity. Detection engineering teams focus on creating these rules based on the tactics, techniques, and procedures (TTPs) of specific threat actors, aiming to identify repeatable patterns in malicious behavior.

However, the evolving threat landscape has exposed the limitations of this approach. The Salt Typhoon campaign illustrates how advanced adversaries evade detection for extended periods by employing living-off-the-land techniques and dynamically loading modular malware in memory. These tactics render traditional detection mechanisms ineffective, as attacker behavior no longer adheres to predefined or a priori patterns. Consequently, TTP-centric tooling often observes suspicious activity but lacks the capability to classify it as malicious, leaving critical gaps in defense.

Layered Defense: Integrating Complementary Detection Layers

The sophistication of modern threat actors, as evidenced by the success of the Salt Typhoon campaign, underscores the inadequacy of relying on a single detection approach. A layered defense strategy is essential to counter these advanced threats effectively.

Strategically integrating complementary detection layers enhances overall defense capabilities. Combining traditional mechanisms that identify "known bad" activity with advanced techniques capable of detecting unknown or evolving threats minimizes blind spots. This multi-faceted approach improves coverage, strengthens detection efficacy, and creates a more resilient cybersecurity posture against sophisticated adversaries.

Cyber Deception: A Proactive Approach to Detection

Cyber deception offers a forward-thinking method for detecting threats by anticipating attacker objectives, deploying tailored traps, and monitoring adversarial interactions. This proactive strategy shifts the defensive paradigm by engaging attackers directly, uncovering stealthy activities that evade traditional detection mechanisms.

Unlike traditional TTP-centric approaches, deception-based detection is agnostic to specific attacker tactics. When integrated with existing detection layers, it enhances visibility, identifying sophisticated threats earlier in their lifecycle. By complementing traditional measures, deception provides a robust framework to detect, contain, and neutralize adversarial efforts.

For the telecommunications sector, an effective deception strategy demands precise decisions about the type, volume, and placement of deceptive assets. A tailored approach aligned with critical assets and common threat vectors maximizes its impact, offering unparalleled insights into attacker behavior while safeguarding high-value systems.

Deception Strategies for Telecommunications

Deception technology provides tailored cybersecurity strategies to protect telecommunications organizations from advanced threats. These strategies focus on safeguarding critical assets, detecting stealthy threats, and diverting attackers away from high-value targets.

Critical Asset Protection

Telecommunications networks house sensitive data and communications critical to both business operations and national security. High-value targets include database servers, billing systems, Active Directory environments, and Call Detail Records (CDRs), which contain information such as call duration, cell tower usage, and sender/recipient details.

An effective deception strategy identifies critical assets and deploys deceptive elements—such as honeytokens and decoys—around them and along common attack pathways. These assets are designed to engage and divert attackers, luring them away from legitimate systems into controlled environments. For example, honeytoken accounts mimicking service accounts for CDR data can be strategically placed in Active Directory. Any interaction with these assets triggers immediate alerts, enabling defenders to detect, track, and neutralize threats, regardless of the attacker's tactics, techniques, or tools.

Deception Strategies for Telecommunications

Deception technology offers tailored cybersecurity strategies to address critical threats in telecommunications. A prime example involves using honeytoken accounts strategically within Active Directory. These accounts mimic service accounts for commercial or open-source Call Detail Record (CDR) data stores, enticing attackers during reconnaissance.

When attackers query for targets, such as service accounts related to CDR providers, they encounter the planted honeytoken accounts. Any interaction with these accounts triggers an immediate alert, allowing the defense team to swiftly identify and disrupt the threat. This approach is independent of the attacker's tools or techniques, making it effective against a broad spectrum of adversary tactics.

For instance, an attacker performing reconnaissance with the command: setspn -Q */*CUCM* might identify honeytoken accounts associated with Cisco Unified Communications Manager (CUCM), a widely-used CDR repository. Such interactions not only alert defenders but also create opportunities to engage and analyze the attacker's behavior.

Early threat detection

Attackers in telecommunications environments increasingly rely on stealth techniques like living-off-the-land (LotL) and adaptive malware to evade traditional detection mechanisms. For example, consider an attacker who gains initial access to an endpoint and uses built-in OS tools, such as wmic.exe and PSExec, for reconnaissance, credential harvesting, and lateral movement. To bypass detection tailored to these tools, the attacker can switch to alternatives like Invoke-WMIExec (a PowerShell-based variant of wmic.exe) or use SMB propagation tools such as Impacket, CrackMapExec, or Invoke-SMBExec. This flexibility complicates traditional detection engineering, as attackers evolve their techniques to avoid predefined rules.

In this attack scenario, an adversary uses PSExec and WMIC to escalate privileges and move laterally within the environment. As shown in the example diagram, attackers targeting endpoints or infrastructure assets often execute reconnaissance commands like: setspn -Q */*CUCM* to locate service accounts for critical systems, such as Cisco Unified Communications Manager (CUCM), which manages Call Detail Records (CDRs).

Strategically embedding realistic and enticing deception assets, such as honeytokens on endpoints and decoys in the network, provides an effective countermeasure for early threat detection. These traps are crafted to align with attacker objectives and mimic as high-value targets. Regardless of the specific tools or tactics employed, attackers consistently aim to elevate privileges, evade defenses, establish persistence, gain access to credentials, and move laterally across the environment.

Strategically placed deceptions expose malicious activity by creating traps aligned with these attacker goals. Well-designed and carefully positioned traps trigger immediate alerts when accessed or interacted with, providing security teams with critical early-warning signals to respond swiftly and mitigate threats before significant damage occurs.

Early threat detection (cont.)

For example, a honeytoken mimicking a CUCM service account can generate an alert upon interaction, enabling defenders to detect threats early in the attack lifecycle. This proactive approach disrupts adversary operations, regardless of their tools or tactics, while generating actionable intelligence for further analysis.

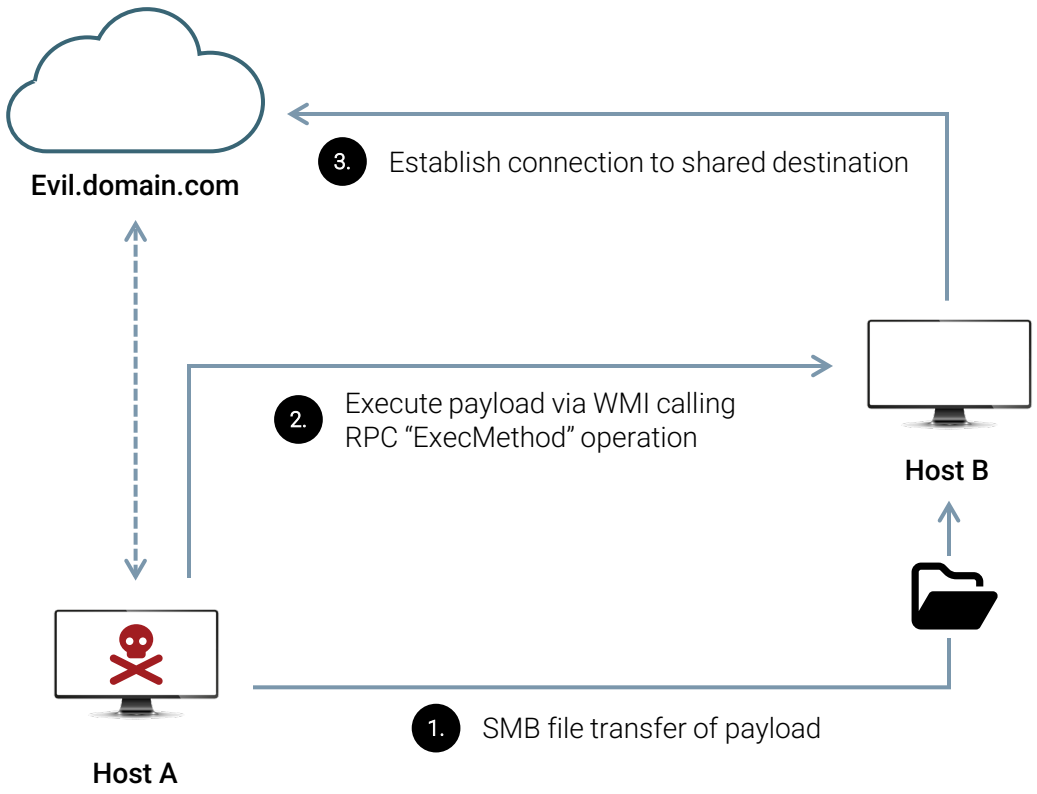


Figure 2: WMI lateral movement procedural steps

Generate Threat Intel Through Adversary Engagement

As threat actors continue to evolve and employ novel attack techniques, defense teams must achieve deeper visibility into emerging attacker TTPs. A core principle of Active Defense, deploying high-interaction decoys that simulate critical assets in telecommunications environments—such as billing servers and database servers—enables defenders to engage attackers directly and gain valuable insights into their methods.

Telco threats increasingly leverage custom, modular malware enhanced with anti-analysis techniques, making it challenging to capture malware artifacts for forensic investigation. High-interaction decoys provide an effective means to monitor attacker behavior in a controlled, instrumented environment and collect malware artifacts for subsequent analysis, significantly improving defenders' ability to counter advanced threats.

Threat Hunting

As advanced threats evolve to maintain long-term persistence, defense teams are relying more heavily on proactive threat hunting to identify and confirm the presence of adversaries. Recent telecommunications attacks highlight this challenge, with defense teams often uncertain whether attackers have been fully evicted from compromised environments. Such uncertainty arises from the sophisticated persistence mechanisms employed by threat actors.

An integral component of Active Defense, traditional threat hunting methods—centered on Indicator of Compromise (IoC) sweeps and log searches—are effective against disk-based malware but fall short when confronting modern threats that exploit in-memory techniques. To counter these stealthy attacks, threat hunting teams must enhance their tooling and methodologies. Incorporating deception assets into hunting activities provides a controlled opportunity to identify latent threats that are persistent and awaiting activation.

For example, deploying baits designed to mimic deceptive Call Detail Record (CDR) data can expose adversaries attempting to target such assets. By initiating these baits as part of hypothesis testing and validation, defense teams can uncover and confirm hidden threats, improving their ability to detect and neutralize stealthy, persistent attackers before they execute their objectives.

Summary

The telecommunications industry is under siege from increasingly sophisticated cyber threats that exploit advanced malware, stealth tactics, and persistent vulnerabilities to evade detection. Traditional defenses, often anchored in rule-based approaches, struggle to counter the evolving strategies of attackers. To address these challenges, organizations must adopt Active Defense strategies that go beyond passive detection, enabling proactive engagement with adversaries.

At the heart of Active Defense lies cyber deception—a transformative technology that empowers defenders to anticipate, detect, and disrupt threats before significant damage occurs. By deploying realistic traps such as honeytokens and network decoys, defenders can lure attackers into controlled environments, gain critical insights into their tactics, and neutralize threats with precision. As the threat landscape grows more complex, Active Defense represents a vital shift toward proactive, dynamic security, with deception playing a central role in this evolution.

ACALVIO

AI-POWERED DECEPTION

Acalvio is the leader in autonomous cyber deception technologies, arming enterprises against sophisticated cyber threats including APTs, insider threats and ransomware. Its AI-powered Active Defense Platform, backed by 25 patents, enables advanced threat defense across IT, OT, and Cloud environments. Additionally, the Identity Threat Detection and Response (ITDR) solutions with Honeytokens enable Zero Trust security models. Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from Cloud, on-premises, or through managed service providers.

For more information, please visit www.acalvio.com

© 2025 Acalvio Technologies, Inc. All rights reserved.

Copyright Notice

Copyright © 2025 Acalvio Technologies. All Rights Reserved. This document may have been furnished under a license for use only within the terms of that license and may have confidential information on Acalvio Technologies. If you do not have a valid nondisclosure agreement with Acalvio or a valid contract for use of this document, then you received this document without authorization and are not legally entitled to own, read or use it. Usage, duplication, and disclosure of this document is subject to limitations by the US Government as Restricted Rights Software under the applicable contract, federal laws and regulations. The information and the illustrations provided in the document are subject to change without notice. Acalvio Technologies disclaims all warranties and liability for any inaccuracies or errors herein.

Written and designed at Acalvio Technologies, 2520 Mission College Boulevard, Suite 110, Santa Clara, CA 95054, USA. Printed in the USA.