# Qilin Ransomware-as-a-Service: Threat Analysis and Strategic Outlook

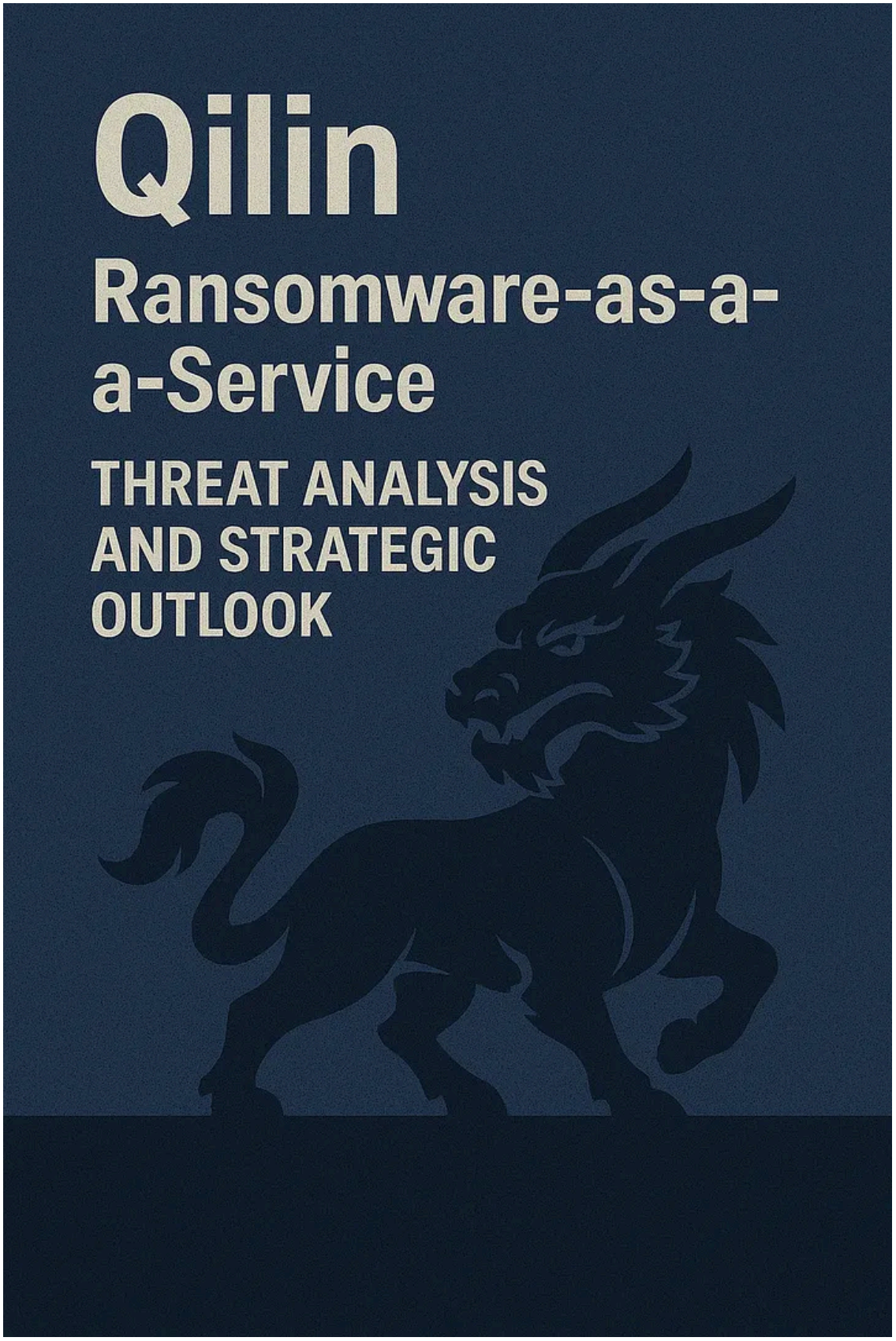
By BeGoodToAll

Published: 2025-08-18 · Archived: 2026-04-10 03:08:01 UTC

11 min read

Aug 18, 2025

Press enter or click to view image in full size




**Executive Summary**

Qilin ransomware, also known as Agenda, has emerged as one of the most significant and evolving cyber threats globally, rapidly ascending to become a top-tier ransomware-as-a-service (RaaS) operation. Since its initial

appearance in July 2022, Qilin has demonstrated remarkable adaptability and sophistication, consistently refining its tactics, techniques, and procedures (TTPs) to maximize impact and financial gain. This report provides a comprehensive analysis of Qilin's evolution, operational model, attack methodologies, victimology, and recent activities, along with strategic recommendations for defense and future trend forecasts. Its professionalized approach, including offerings like "legal support" to affiliates, highlights a concerning new phase in the cybercrime economy.

**Introduction to Qilin Ransomware (Agenda Ransomware)**

Qilin ransomware, initially observed in July 2022 under the name "Agenda," operates on a **Ransomware-as-a-Service (RaaS) model**. This model allows core developers to provide their malicious software and infrastructure to affiliates in exchange for a percentage of the profits generated from attacks. The name "Qilin" references a Chinese mythological creature symbolizing power and prosperity, a fitting metaphor for the group's perceived influence and financial objectives. Despite the Chinese name, the group is **linked to Russian-speaking cybercriminals**, often recruiting affiliates on Russian-language forums and notably excluding Commonwealth of Independent States (CIS) countries from its targets.

**Evolution of Qilin Ransomware**

Qilin has undergone significant technical and operational evolution since its inception.

- **July 2022:** First sighted as "Agenda" with code written in **Go (Golang)**.
- **September-December 2022:** Rebranded to "Qilin" and saw a complete redesign in **Rust language**, significantly improving its portability, efficiency, stealth, and evasion capabilities across Windows, Linux, and VMware ESXi servers.
- **Late 2023:** Gained popularity through targeted attacks on **VMware ESXi infrastructure**.
- **2024:** Expanded capabilities to include **Chrome Stealer functionality** and robust encryption/evasion tactics. A new, more advanced variant, **Qilin.B**, emerged, offering enhanced encryption (AES-256-CTR and ChaCha20) and sophisticated operational tactics.

**Early 2025:** Attacks intensified, with **over 310 victims claimed** by March 2025. By May 2025, public sources identified Qilin as the leading ransomware threat overall.

**Tactics, Techniques, and Procedures (TTPs)**

Qilin employs **sophisticated and adaptive TTPs** that follow a structured attack kill chain.

**1. Initial Infection Vectors**

- **Phishing and Spear-Phishing:** The most common method, involving malicious attachments or links in convincing emails.
- **Exploitation of Exposed Applications and Interfaces:** This includes **Citrix, Remote Desktop Protocol (RDP)**, and unpatched vulnerabilities in critical software.
- **Compromised Credentials:** Gaining initial access through leaked or purchased valid credentials.
- **Vulnerability Exploitation:** Actively exploiting specific CVEs in widely used products (detailed in **Vulnerabilities Exploited and Products/Technologies** section).

**2. Execution Flow:** Once initial access is gained, Qilin follows a detailed execution sequence to maximize damage and evade detection.

- **Payload Deployment:** The ransomware payload (often named w.exe or a .dll variant like stevedore) is typically deployed to a temporary directory (e.g., C:\temp). Execution requires a specific password provided as a command-line argument, which is then hashed (SHA-256) and compared against a pre-defined hash in the ransomware's configuration.
- **Privilege Escalation:** Qilin seeks to elevate privileges to **SYSTEM-level access**, often through an embedded **Mimikatz module** to steal user tokens from processes like lsass.exe, winlogon.exe, or wininit.exe. It can also use PowerShell and PsExec for lateral movement.
- **Lateral Movement:** Qilin exhibits **worm-like propagation capabilities** across local networks when the -spread command-line argument is used. It embeds **Sysinternals PsExec** (version 2.43) to establish connections and move to other domain computers. Domain reconnaissance is performed to identify targets. Evidence also shows use of **VMware vCenter for self-distribution** (-spread-vcenter).

**3. Defense Evasion:** Qilin meticulously neutralizes defensive and recovery mechanisms.

- **Log Deletion:** System logs (including Windows PowerShell and System logs) are systematically deleted to eliminate traces of intrusion and hamper forensic analysis.
- **Security Tool Disabling:** It attempts to disable security services like antivirus and intrusion detection solutions by terminating specific processes and services (configurable via process_black_list and win_services_black_list).
- **Backup Corruption/Deletion:** It corrupts backups by deleting **Volume Shadow Copies (VSS)**, disabling scheduled backup jobs, removing backup jobs within management consoles, and overwriting free disk space with cipher utilities (e.g., cipher /w: "X:\").
- **Obfuscation and Anti-Analysis:** Qilin uses packed code, control flow modifications, string encryption, and anti-analysis checks to evade static detection, sandbox, and VM environments.

**4. Custom Encryption & Double Extortion:** Qilin is known for its **double extortion tactics**, encrypting files and exfiltrating victim data, then threatening to release the stolen data if the ransom is not paid.

- **Encryption Methods:** It employs multiple encryption algorithms, including **ChaCha20, AES-256, and RSA-4096**. Encryption keys, nonces, and parameters are RSA-4096 encrypted and appended to the encrypted file.
- **Customization:** Affiliates can customize filename extensions of encrypted files and configure encryption modes (skip-step, percent, fast, normal). It encrypts a wide range of file types, focusing on critical data.

**5. System Shutdown/Reboot:** As a final disruptive measure, Qilin often initiates a reboot of compromised systems, including backup servers and VPN servers, after encryption to hinder recovery efforts and disrupt operations. It can also boot systems into Safe Mode to bypass security tools.

**Ransomware Demand Value**

Ransom demands typically **range from $25,000 to several million**, depending on the size of the victim. More specific ranges noted are **$50,000 to $800,000**. The attack on Synnovis, for example, involved a staggering **$50**

**million ransom demand**. In 2024 alone, Qilin amassed **over $50 million in ransom payments**.

**Target Profiles and Geography**

Qilin ransomware stands out for its **opportunistic and indiscriminate approach to target selection**, focusing on vulnerability rather than a specific industry.

**Targeted Sectors:** Qilin targets large enterprises and high-value organizations. It has particularly focused on **healthcare and education sectors**, but also impacts manufacturing, legal & professional services, financial services, government, critical infrastructure, automotive, publishing, IT, and retail. Critical infrastructure entities are considered lucrative due to the high cost of downtime.

**Geographical Focus:** While initially known to focus on Africa and Asia, Qilin's reach is global. Victims have been identified across **25 countries**, including the **United States (the most targeted country)**, United Kingdom, France, Canada, Germany, Japan, Australia, UAE, Brazil, Colombia, Indonesia, Netherlands, Serbia, Saudi Arabia, South Africa, Taiwan, and Thailand. Recent campaigns have shown a focus on **Spanish-speaking regions**.

**Affiliate Recruitment and Operations**

Qilin operates a **highly structured RaaS model** with attractive incentives for its affiliates.

- **Profit-Sharing Structure:** Affiliates typically receive between **80% to 85% of ransom payments**. Specifically, 80% for payments under $3 million and 85% for payments over $3 million. This lucrative split makes it a very appealing option in the RaaS ecosystem.
- **Customizable Affiliate Panel:** Qilin provides affiliates with a proprietary panel (or builder) divided into sections for managing and coordinating attacks. Affiliates can configure ransom notes, file extensions, directories to skip or encrypt, processes and services to terminate, and encryption modes.
- **Exclusion of CIS Countries:** A common trait among Russian-speaking cybercriminal groups, Qilin's rules prohibit attacks on entities in Russia or other CIS countries.
- **Enhanced Affiliate Services:** Qilin is positioned not just as a ransomware group, but as a **full-service cybercrime platform**. This includes unique offerings to lure and support affiliates:
- **Legal Support ("Call Lawyer" feature):** Introduced in 2025, this feature within the affiliate panel simulates legal engagement to psychologically pressure victims during negotiations, signaling to affiliates that Qilin is organized and invested in their success.
- **Spam Services and In-House Journalists:** Qilin offers spam distribution and employs "in-house journalists".
- **PB-scale Data Storage:** Provides large-scale data storage for exfiltrated data.

**DDoS Option:** A DDoS attack capability was introduced in April 2025 to increase pressure on victims.

**Vulnerabilities Exploited and Products/Technologies**

Qilin leverages a variety of vulnerabilities, particularly those in public-facing applications and remote access solutions.

**Specific CVEs Exploited:**

- **CVE-2023–27532:** A critical vulnerability in **Veeam Backup & Replication software**. Exploiting this allows attackers to retrieve encrypted credentials from the configuration database, bypassing authentication and facilitating broader network compromise.
- **CVE-2024–21762** and **CVE-2024–55591:** Critical vulnerabilities in **Fortinet's FortiGate and FortiProxy devices**, enabling authentication bypass and remote code execution. CVE-2024–21762, patched in February 2025, remains a major concern with tens of thousands of exposed systems.
- **CVE-2025–29824:** An unpatched Windows CLFS vulnerability exploited by Play ransomware, which is sometimes associated with broader ransomware ecosystem activities. While not directly attributed to Qilin, it highlights a pattern of exploiting critical OS vulnerabilities.
- **CVE-2024–27198:** A vulnerability in **JetBrains software** leveraged by BianLian for data extortion operations. While not directly Qilin, it shows the types of software vulnerabilities targeted by sophisticated RaaS groups.

**Types of Products/Technologies Exploited:**

- **Firewall/VPN Solutions:** Fortinet devices (FortiGate, FortiProxy), SonicWall SSL VPN.
- **Backup Solutions:** Veeam Backup & Replication.
- **Remote Access:** RDP and Citrix.
- **Virtualization Platforms:** VMware ESXi, vCenter servers.
- **File Transfer Applications:** Cleo file transfer (CVE-2024–50623), which are increasingly attractive targets.

**Interesting Patterns in Vulnerability Exploitation:**

- **Re-use of Vulnerabilities:** Qilin, and the broader cybercriminal ecosystem, demonstrate a pattern of **sharing and reusing successful exploitation narratives and vulnerabilities**. This is seen with CVE-2024–55591, which was also incorporated by LockBit and SuperBlack ransomware operations.
- **Focus on Public-Facing Applications and Remote Services:** A consistent target for initial access, as these offer direct entry points into corporate networks.
- **Exploitation of Older/Unpatched Vulnerabilities:** Many vulnerabilities exploited by ransomware are old, discovered between 2010 and 2019. Qilin's exploitation of CVE-2024–21762, even after it was patched, indicates a reliance on organizations failing to apply timely updates.

**Targeting of Critical Infrastructure Software:** The focus on products like Fortinet, Veeam, and VMware underscores a strategy to impact critical services that have low tolerance for downtime.



**Recent Activities and Developments (2024–2025)**

Qilin has been highly active and prominent in 2024 and 2025:

- **Leading Ransomware Group:** Ranked as the **most prevalent ransomware in public threat intelligence reports by 2025**. In June 2025, Qilin emerged as a significant threat, leading with **81 victims**. It also led in claimed victims for the third time in four months by August 2025, accounting for 17% of total victims in July 2025 with **73 reported incidents**.

**Major Campaigns:**

- **Synnovis Attack (June 2024):** A high-profile attack on a UK-based pathology services provider, causing "critical incident" at several London NHS hospitals and disrupting blood transfusions, test processing, and operations. Qilin demanded $50 million and later leaked approximately 400GB of purported Synnovis data. The group unusually claimed it was politically motivated.
- **Yanfeng Automotive Interiors (November 2023):** Qilin claimed responsibility for an attack on one of the world's largest automotive parts suppliers.
- **Lee Enterprises (February 2024):** Targeted a major U.S. publishing network, disrupting services and exfiltrating sensitive personal and corporate data (350 GB, 120,000 documents) impacting nearly 40,000 individuals.
- **City of Abilene, Texas (April 2025):** Encrypted systems and exfiltrated 477 GB of data, disrupting bus services and other operations for roughly a month.
- **U.S. Financial Advisory Firm (July 2025):** Exfiltrated approximately 340 GB of sensitive data.
- **Cobb County, GA (2025):** Attacked by Qilin, with over 400,000 files threatened for leak.
- **Moonstone Sleet Connection:** In March 2025, Microsoft revealed that **North Korean hacker group Moonstone Sleet is now using Qilin ransomware** in some of their attacks.
- **Qilin.B Variant:** Documented in October 2024, this new variant boasts enhanced encryption capabilities and more sophisticated operational tactics.
- **Influx of Affiliates:** Qilin's recent spike in activity may be attributed to an influx of affiliates from rival groups that have faced disruptions, such as **RansomHub, LockBit, ALPHV/BlackCat, Everest, and BlackLock**. Group-IB observed Qilin's DLS disclosures doubling since February, suggesting migration from RansomHub.
- **Shift in Data Exfiltration Tactics:** By August 2024, Qilin was observed to be changing tactics to include **credential harvesting (specifically Chrome browser credentials)** rather than exfiltrating massive amounts of victim-specific data.

**Role of Qilin Ransomware in the Ransomware Landscape and its Evaluation**

Qilin represents the **professionalization and evolution of the RaaS model**. It's not merely a ransomware group but a **full-service cybercrime platform**, offering affiliates advanced payloads, customizable features, and extensive support beyond just encryption. Its adaptability (Rust/Golang variants, multiple encryption modes), aggressive negotiation tactics, and ability to evade detection position it as a **formidable and persistent threat**.

Qilin's strategic move to offer "legal assistance" and DDoS options marks a **new frontier in psychological extortion**, aiming to further gamify and automate negotiation dynamics by exploiting organizational panic. This strategic shift suggests Qilin's ambition to dominate the ransomware landscape by mimicking legitimate enterprise service models. Its consistent ranking as a top threat and its ability to absorb affiliates from dismantled groups signify its robust operational maturity and significant impact on the overall cyber threat landscape.

**Qilin Ransomware Detection Rules (Sigma)**

These rules would aim to detect Qilin's behaviors and artifacts at various stages of the attack chain.

**Sigma Rules (Behavioral Detection based on Logs)** Sigma rules are generic signatures for SIEM systems, correlating various log sources to detect malicious behaviors.

**Process Creation & Command-Line Arguments:**

- Detection of anomalous usage of built-in Windows tools commonly misused by ransomware to inhibit system recovery: bcdedit.exe, fsutil.exe (deletejournal), vssadmin.exe (Delete Shadows /all /quiet), wbadmin.exe, and wmic.exe (shadowcopy or shadowstorage).
- Execution of PowerShell scripts (IPScanner.ps1, ShareFinder.ps1, Get-ADComputer) for reconnaissance, credential harvesting, or log clearance (Get-WinEvent -ListLog * | Where-Object {$_.RecordCount} … ClearLog($l)).
- Execution of PsExec or cmd.exe with –spread argument for lateral movement, or net stop/start <service> to disable security services.
- Installation or unexpected usage of Remote Monitoring and Management (RMM) software (e.g., ScreenConnect/ConnectWise, AnyDesk, SimpleHelp) or other remote access tools.

**Network Activity:**

- Anomalous VPN device logins or other suspicious logins.
- Abnormal amount of data outgoing over any port, or use of common data exfiltration tools (e.g., Rclone, Rsync, WinSCP, FileZilla, MegaSync, FreeFileSync, Chisel, Cloudflared, sftp, ftp).
- Connections to known C2 servers, suspicious domains, or TOR traffic.
- Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz, NTDSutil.exe).

**System Modifications:**

- Newly created AD accounts or accounts with escalated privileges and recent activity related to privileged accounts (e.g., Domain Admins).
- Unexpected scheduled tasks or services created for persistence.
- Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations.
- Changes to ESXi root passwords or SSH enablement.

**Log Integrity:** Monitoring for deletion of system logs (Windows Security logs, PowerShell logs, etc.).

**Strategic Cyber Foresight: Qilin's 2025 Ransomware Outlook**

Here's what to expect:

**Sustained Dominance and Aggressive Growth**

◦ Qilin is expected to remain a leading and pervasive ransomware threat globally, having recently ranked as one of the most active groups with a significant increase in claimed victims.

◦ It will likely continue to capitalize on the disruption of other major ransomware groups, attracting experienced affiliates and expanding its network.

**Enhanced Technical Sophistication and Adaptability**

◦ Qilin will continue to evolve its Rust-based malware variants, such as Qilin.B, featuring enhanced encryption capabilities (AES-256-CTR, ChaCha20, RSA-4096), improved evasion tactics, and more robust defense evasion techniques like clearing Windows Event Logs and self-deletion.

◦ Its highly customizable and modular design will ensure its continued adaptability to specific victim environments and attack scenarios.

◦ Expect continued exploitation of both newly disclosed and persistently unpatched vulnerabilities in widely used enterprise software, including Fortinet devices and Veeam Backup & Replication. It may also increasingly automate exploitation chains.

**Professionalization and Innovative Extortion Tactics**

◦ Qilin is redefining the Ransomware-as-a-Service (RaaS) model by expanding its ecosystem of “premium” services for affiliates.

◦ This includes unique offerings like “legal assistance” through a “Call Lawyer” feature during ransom negotiations, DDoS attack capabilities, automated negotiation tools, PB-scale data storage, and support from “in-house journalists” to create public leak blogs. These services aim to maximize pressure on victims and may increasingly leverage AI for more sophisticated psychological extortion.

◦ The group’s primary motivation remains financial profit, and all its innovations are geared towards maximizing ransom collection.

**Evolving Victimology and Attack Vectors**

◦ While remaining opportunistic across all verticals, Qilin is expected to intensify its strategic targeting of high-value organizations and critical sectors, including healthcare, manufacturing, legal and professional services, financial services, and virtual machine infrastructure.

◦ A significant trend is the shift towards targeting Managed Service Providers (MSPs) through sophisticated phishing campaigns and credential harvesting (e.g., from Google Chrome), which grants access to multiple downstream victims.

◦ The observed use of Qilin by North Korean state-sponsored threat actors (Moonstone Sleet) suggests a continued dual motivation for both financial gain and espionage, potentially involving sophisticated identity falsification.

**Conclusion**

Qilin ransomware is unequivocally establishing itself as a **dominant and evolving global threat** in the cybercriminal landscape, indicating its continued prominence in the near future.

In the near future, organizations must recognize that Qilin's sustained activity, driven by its sophisticated operational model and aggressive recruitment following the disruption of other major groups, necessitates a **proactive, layered, and intelligence-driven defense strategy**. This includes robust incident response planning, immutable backups, vigilant patching, and advanced detection capabilities to counter its evolving TTPs.

---