Smarttech
YOUR 24/7 SECURITY PARTNER

Escalated Activity from "The Gentlemen" Ransomware Group

Contents

Overview

The emergence of The Gentlemen illustrates how quickly a modern ransomware-as-a-service operation can scale from a closed crew into one of the most productive extortion programs in the world. First observed in mid-2025, The Gentlemen combines a professionally engineered, Go-based encryptor with an aggressive self-propagation capability, a disciplined affiliate structure, and a relentless focus on internet-facing edge infrastructure as the primary route into victim networks.

What distinguishes the group is not a single novel technique but the maturity of the overall package. The operators pair strong per-file cryptography with a worm-like spreading module that attempts more than twenty distinct remote-execution methods against every host it can reach, maximising the blast radius of a single foothold. Around this locker sits a curated toolset for credential theft, Active Directory abuse, endpoint-protection evasion, and high-volume data exfiltration, supported by a structured affiliate program that pays its members an unusually generous ninety percent of every ransom.

The group operates a double-extortion model, encrypting data while simultaneously stealing it and threatening publication on a Tor-based data leak site. By early-to-mid 2026 the operation had claimed several hundred public victims across more than seventy countries and every populated continent, placing it among the two most active RaaS programs of the year. A rare leak of the group's own internal database in May 2026 exposed the people, tooling, and economics behind the brand, and confirmed that the same administrator who builds the platform also takes part directly in intrusions.

Threat Actor Profile & Campaign Overview

The Gentlemen is a ransomware-as-a-service operation that emerged around July to August 2025. The program began life as a closed group and started offering its locker to external affiliates in September 2025, later cementing an official partnership with the BreachForums marketplace to recruit penetration testers and initial access brokers.

The administrator and lead developer operates under the handles zeta88 and hastalamuerte, which the available evidence strongly indicates belong to the same individual. This operator builds and maintains the custom locker and the RaaS panel, runs the backend infrastructure, curates the shared toolset, assigns targets to teams, and manages negotiations and payouts. Before launching The Gentlemen, the same actor reportedly ran an affiliate crew called ArmCorp under the Qilin RaaS program; a public arbitration dispute on the RAMP forum in July 2025, over roughly 48,000 US dollars in allegedly withheld commission, marked the public split from Qilin. The earliest known Gentlemen sample was uploaded to public malware repositories on 17 July 2025, days before that dispute became public.
The operation is organised around a small, tightly coordinated core rather than a loose crowd. The May 2026 leak of the group's internal Rocket backend exposed nine actively communicating accounts (zeta88, qbit, quant, Kunder, JeLLy, Protagor, Bl0ck, Wick, and mAst3r).
Commercially, The Gentlemen distinguishes itself with an aggressive ninety-percent revenue share for affiliates, with the operator retaining ten percent; in collaborative intrusions that affiliate share is then split among the participants. By the first five months of 2026 the group had published in the order of 330 victims on its leak site, making it the second most productive public RaaS operation of the period, behind only Qilin. The true victim count is certainly higher, as organisations that pay are not listed. Separately, an

affiliate's SystemBC command-and-control server observed during an incident response engagement revealed a botnet of more than 1,570 likely corporate victims, underscoring a pipeline of compromised environments far larger than the public leak site suggests.

Targeting & Victimology

The Gentlemen is opportunistic in entry but broad in its appetite for victims, with a clear lean toward organisations that hold sensitive operational data and are likely to pay to restore service quickly. Manufacturing is consistently the hardest-hit sector, followed by technology, business services, healthcare, and consumer services. Notably, the group shows no restraint toward healthcare; where some ransomware operations avoid hospitals as a matter of informal policy or self-preservation, The Gentlemen has repeatedly targeted Healthcare, Manufacturing,Technology,Business Services, Consumer Services.

Geographically the campaign is global. Victims span North America, South America, Europe, Africa, and Asia, with public tracking recording organisations in more than seventy countries. The United States accounts for the largest single share of listed victims, followed by Thailand, France, Brazil, and the United Kingdom; Germany is also heavily represented. Earlier reporting noted a pronounced Asia-Pacific concentration in the group's first campaigns, which has since broadened into worldwide targeting as the affiliate base has grown.

Tactics, Techniques & Procedures

The Gentlemen is a ransomware-as-a-service threat whose tooling is highly adaptable, allowing affiliates to tailor operations to the target environment, including operating systems, enterprise services, remote-access infrastructure, and virtualization platforms.

A representation of the tactics and techniques utilized by The Gentlemen group, can be found below:

Tactic	Techniques
Initial Access	Valid Accounts, Valid Accounts: Domain Accounts, External Remote Services, Exploit Public-Facing Application, Phishing
Execution	Windows Management Instrumentation, Command and Scripting Interpreter, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Software Deployment Tools
Persistence	Create Account, Create or Modify System Process, Boot or Logon Autostart Execution
Privilege Escalation	Exploitation for Privilege Escalation, Forced Authentication, Adversary-in-the-Middle
Defense Evasion	Obfuscated Files or Information, Indicator Removal, Proxy, Modify Registry, Domain Policy Modification: Group Policy Modification, Impair Defenses, Impair Defenses: Disable or Modify Tools
Credential Access	OS Credential Dumping, Brute Force, Unsecured Credentials, Credentials from Password Stores
Discovery	Remote System Discovery, Network Service Discovery, Permission

	Groups Discovery, Account Discovery, Account Discovery: Domain Account, Domain Trust Discovery, Cloud Service Discovery
Lateral Movement	Remote Services, Remote Services: Remote Desktop Protocol, Remote Services: SMB/Windows Admin Shares, Remote Services: SSH, Remote Service Session Hijacking
Collection	Data from Local System, Data from Network Shared Drive, Data Staged, Data Staged: Local Data Staging, Email Collection
Exfiltration	Exfiltration Over Alternative Protocol, Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol, Transfer Data to Cloud Account
Command and Control	Application Layer Protocol, Application Layer Protocol: Web Protocols, Remote Access Software, Protocol Tunneling, Encrypted Channel
Impact	Data Encrypted for Impact, Service Stop, Inhibit System Recovery, Defacement

The group systematically combines initial access through valid accounts and exposed services with broad discovery, privilege escalation, and rapid lateral movement to establish and expand footholds within enterprise environments.
Initial access is primarily achieved through valid accounts, frequently domain accounts sourced from infostealer credential logs or recovered through brute force, and through exploitation of public-facing applications such as exposed Fortinet and Cisco edge appliances. External remote services, particularly VPN gateways, provide an additional entry path, while phishing remains a supplementary delivery vector.
Execution relies on built-in Windows mechanisms, including Windows Management Instrumentation and the command and scripting interpreter, with both PowerShell and the Windows command shell used to run commands and stage payloads. Software deployment tooling, most notably Group Policy, is abused to push the locker across the domain.
Persistence is established by creating new accounts, creating or modifying system processes such as Windows services, and configuring boot or logon autostart execution through scheduled tasks and registry run keys. Privilege escalation is pursued through exploitation for privilege escalation, alongside forced authentication and adversary-in-the-middle techniques such as NTLM relay, which the group uses to coerce and capture authentication and escalate toward domain-level privileges.
Defense evasion is extensive. The Go-based locker is obfuscated to frustrate analysis, and the operators perform aggressive indicator removal, clearing Windows event logs and deleting shadow copies, prefetch files, RDP logs, and PowerShell history. They modify the registry, abuse Group Policy modification, route activity through proxies, and impair defenses by disabling or modifying security tools, including dedicated EDR-killer kits and bring-your-own-vulnerable-driver techniques.
Credential access combines OS credential dumping, including extraction of LSASS memory, brute forcing of exposed panels, harvesting of unsecured credentials, and theft of credentials from password stores such as browser secret stores, enabling reuse of corporate sessions.
Discovery operations are broad and largely automated, covering remote system discovery, network service discovery, permission groups discovery, local and domain account discovery, domain trust discovery, and cloud service discovery, giving operators a detailed picture of the environment and its trust relationships.
Lateral movement is conducted through legitimate remote services, Remote Desktop Protocol, SMB and Windows admin shares, and SSH, and through remote service session

hijacking. The locker's self-propagation module weaponises these channels, using PsExec, WMI, scheduled tasks, services, and PowerShell remoting to deploy itself to every reachable host.
Collection focuses on data from local systems and network shared drives, with data staged locally before theft and email collected where relevant. Exfiltration is carried out over alternative protocols, including symmetric-encrypted, non-C2 channels, and through transfer to cloud accounts, typically using automated tooling directed at NAS, backup, and virtualization targets.
Command and control is maintained over application-layer and web protocols, remote access software, protocol tunnelling such as Cloudflare tunnels, and encrypted channels, with Tor-based onion infrastructure used for victim communications.
Impact is delivered through data encrypted for impact, using per-file Curve25519 key exchange paired with the XChaCha20 stream cipher so that recovery without the attacker-held key is effectively impossible. Before and during encryption the group performs service-stop actions against database, backup, and security services, and inhibits system recovery by deleting shadow copies and wiping free disk space. Defacement is achieved by replacing the victim's desktop wallpaper with a branded ransom image.

Known Exploited Vulnerabilities

Rather than relying on a single flaw, The Gentlemen and its affiliates track and weaponise a focused set of vulnerabilities spanning edge access, backup and virtualization infrastructure, privilege escalation, and lateral movement.

2025

CVE	Impacted Product	CVSS Score
CVE-2025-32433	Erlang/OTP SSH (Cisco products)	10.0
CVE-2025-33073	Microsoft Windows NTLM / SMB Client (reflection / relay)	8.8
CVE-2025-7771	TechPowerUp ThrottleStop.sys driver (BYOVD)	8.7

2024

CVE	Impacted Product	CVSS Score
CVE-2024-55591	Fortinet FortiOS / FortiProxy (authentication bypass)	9.8
CVE-2024-37085	VMware ESXi (Active Directory integration authentication bypass)	6.8

2023

CVE	Impacted Product	CVSS Score
CVE-2023-27532	Veeam Backup & Replication (missing authentication)	7.5

CVE-2024-55591 is the group's primary initial-access vector against exposed FortiGate appliances and underpins its curated database of pre-compromised devices. CVE-2025-

7771 is abused as a bring-your-own-vulnerable-driver technique, the ThrottleStop.sys driver, renamed ThrottleBlood.sys, is used to obtain kernel-level execution and terminate endpoint protection. CVE-2023-27532 and CVE-2024-37085 support the group's focus on backup and virtualization infrastructure, while CVE-2025-32433 and CVE-2025-33073 are tracked and evaluated for exposed SSH services and NTLM relay workflows respectively.

Indicators of Compromise

SHA-256

f483faa2b9c9815a0efb08023fe5d243b1b9f7e04b95127c506b6aae824c9d09
c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73
efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f
1af419b36a5edefef387409e2b3248c9223f7dc49a4f7b15ea095d371c3a70b2
36946eb02e95a1b61f2cbd8cc762d9c7a4001c3bfde4fa839b389ebb946a646e
3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235
24ac3588fb8cfbff63b7fdfcbc7dec1f3c60e54e6f949dd69d68e89e0c89d966
860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923
87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c
b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6
1334f0189a8e6dbc48456fa4b482c5726ab7609f7fa652fcc4c1a96f2334436f
dfe696ff713318c53fb17731bd4a6585a02c085b590149b19847990b324a0be6
fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958
48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd
91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1
4a175eed927c0a477eafb8aa35a93c191748acaa78ac7aecd8ea3c4cd868887c
f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12
4de88220ff6a6dcb137b17d8d3f77ab4bacc39ea4e4d1147f687b021b7a82b8c
dce2e5cc00eff2493f8ced546dc51f9d5ef78c5ee56805906ec642dfa77a1c70
22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67
5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca

Recommendations

1. Strengthen Preventive Controls
    - Enforce phishing-resistant MFA for VPN, VDI, RDP gateways, privileged accounts, backup consoles, and VMware vCenter.
    - Disable or tightly restrict internet-facing RDP; route administrative access through hardened jump servers.
    - Keep operating systems, VPN appliances, firewalls, hypervisors, backup platforms, and remote access tools fully patched.
    - Enable antivirus and EDR protections at all times and ensure tamper protection is enforced.

- Enable vulnerable-driver protection such as Microsoft vulnerable driver blocklist, WDAC, or equivalent controls to reduce BYOVD risk.

- Block unauthorized remote management tools such as AnyDesk, Atera, ScreenConnect, Splashtop, TeamViewer, MeshAgent, and Remotely unless explicitly approved.
- Restrict application execution using allowlisting or application control to prevent execution from temporary folders, user profiles, downloads, and SMB shares.
- Limit administrative privileges and ensure employees operate with standard user accounts wherever possible.
- Remove standing domain administrator access and use just-in-time privileged access for administrative tasks.
- Restrict PsExec, remote service creation, and administrative share abuse to reduce ransomware propagation.
- Segment critical environments including Active Directory, backup infrastructure, VMware ESXi/vCenter, file servers, production systems, and user networks.
- Restrict use of personal or unmanaged devices on corporate networks unless strong device posture, EDR, encryption, and access controls are enforced.
- Monitor and restrict high-risk file-transfer tools such as Cyberduck, WinSCP, Rclone, MEGAsync, FileZilla, and s5cmd.

2. Build a Resilient Recovery Strategy

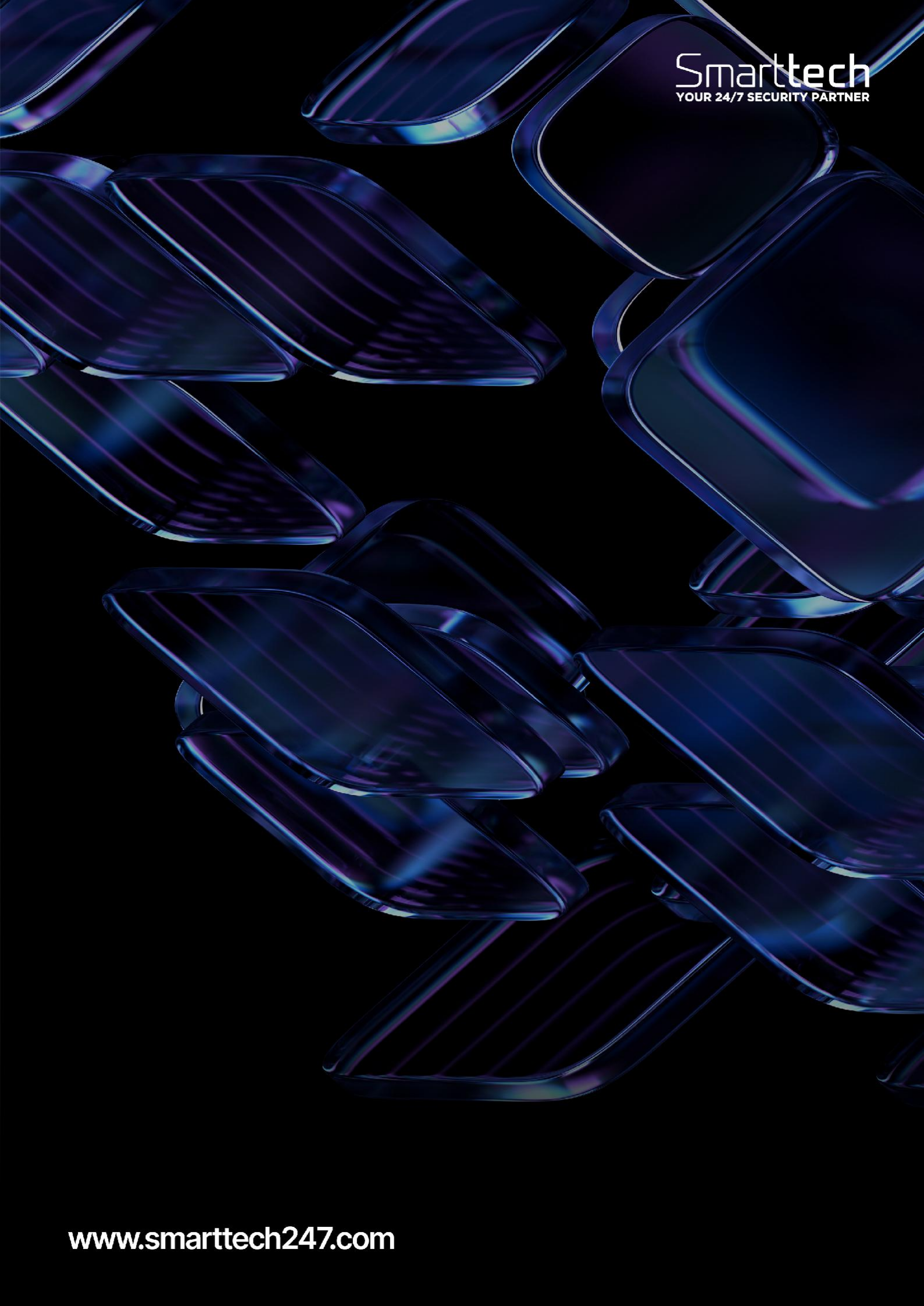
- Develop and regularly update the ransomware response plan covering credential compromise, RMM abuse, data exfiltration, ESXi targeting, backup disruption, and encryption.
- Maintain offline, encrypted, and immutable backups for critical systems and data.
- Test restoration procedures frequently to confirm that backups are usable and clean
- Keep backup infrastructure isolated from standard domain credentials and user networks.
- Maintain clean golden images for critical servers, endpoints, domain controllers, and recovery systems.
- Define clear recovery priorities for crown-jewel assets such as identity systems, backup platforms, ERP, EHR, file shares, VMware infrastructure, and production systems.
- Ensure backup administrators, domain administrators, and virtualization administrators use separate accounts and separate access paths.
- Monitor for backup deletion, failed backup jobs, VSS deletion, disabled backup agents, and suspicious backup-console logins.
- Preserve critical logs outside the compromised domain, including EDR, VPN, DNS, proxy, firewall, Active Directory, backup, and vCenter logs.
- Maintain an up-to-date emergency contact directory for executives, IT, security, legal, communications, cyber insurance, external incident response vendors, law enforcement, regulators, and key suppliers.
- Pre-approve crisis communication templates for employees, customers, regulators, partners, and media.

- Establish clear ransom decision-making authority, including legal, sanctions, insurance, executive, and board-level escalation.

3. Empower with Risk Awareness & Preparedness
    - Conduct routine tabletop exercises simulating Qilin-style ransomware scenarios, including VPN compromise, unauthorized RMM deployment, data theft, ESXi encryption, and backup disruption.
    - Train employees to recognize phishing attempts, suspicious links, fake CAPTCHA pages, malicious installers, MFA fatigue attempts, and unusual system behavior.
    - Train helpdesk teams to detect social engineering attempts related to password resets, MFA resets, remote access enrollment, and account recovery.
    - Maintain an accurate asset inventory covering endpoints, servers, cloud assets,
    VMware infrastructure, backup systems, privileged accounts, remote access tools, and critical applications.
    - Maintain network flow inventories to understand how critical systems communicate and where segmentation is required.
    - Identify and document crown-jewel data locations, including HR, finance, legal, customer data, patient data, source code, intellectual property, and regulated information.
    - Review third-party and MSP access regularly, ensuring vendors use MFA, named accounts, least privilege, session logging, and time-bound access.
    - Review ransomware readiness metrics with executive leadership, including MFA coverage, EDR health, backup restore success, privileged account count, patching SLA compliance, and RMM exceptions.

References

- https://www.ransomware.live/group/thegentlemen
- https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/
- https://www.microsoft.com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/
- https://research.checkpoint.com/2026/dfir-report-the-gentlemen/
- https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
- https://www.cybereason.com/blog/the-gentlemen-ransomware
- https://www.cisa.gov/stopransomware/ransomware-guide
- https://www.nist.gov/cyberframework
- https://attack.mitre.org/



Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com