ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

The Gentlemen Ransomware: A Rapidly Scaling RaaS Threat Targeting Bangladesh

TLP: CLEAR
Distribution: Public
Advisory on: The Gentlemen Ransomware: A Rapidly Scaling RaaS Threat Targeting Bangladesh
Severity: High
Threat Type: Ransomware-as-a-Service (RaaS) / Double Extortion
Affected Sectors: Banking and NBFIs, RMG and manufacturing, telecommunications, healthcare, education, government-linked service providers, NGO
Date: 09 August 2026

Executive Summary

BGD e-GOV CIRT is issuing this advisory to raise awareness of **The Gentlemen, a Ransomware-as-a-Service (RaaS)** operation that has scaled rapidly since it surfaced in mid-2025 and has since become one of the most active ransomware programs globally by claimed victim count.

This threat has direct relevance to Bangladesh; public reporting indicates that a large, Bangladesh-headquartered non-governmental development organization was listed on the group's extortion site in **July 2026**, with the operators threatening to publish exfiltrated data unless a ransom is paid.

The group operates a cross-platform, self-propagating encryptor that can independently spread across **Windows, Linux, NAS, BSD, and VMware ESXi systems** within a compromised network, and it is capable of encrypting an entire domain-joined environment within minutes once a Domain Controller is compromised. Affiliates are offered an unusually generous 90 percent share of ransom proceeds, which has attracted a large pool of experienced operators and fuelled a sharp rise in the group's attack volume through 2026.

Given the group's reliance on exploitable edge devices (firewalls, VPN gateways, backup software, and hypervisor management interfaces), weak or reused credentials, and Active Directory misconfigurations, organizations in Bangladesh across the NGO/development, banking and financial services, ready-made garment (RMG) and manufacturing, telecommunications, healthcare, and education sectors should treat this as an immediate risk requiring urgent review of internet-facing infrastructure and backup resilience.

Threat Overview

The Gentlemen is a financially motivated, double-extortion ransomware operation believed to be run by a small, disciplined core team of roughly **20 individuals operating out of a Russian-speaking region**. The group's targeting rules explicitly exclude organizations located in Russia and other Commonwealth of Independent States (CIS) countries, a pattern consistent with many Russian-speaking cybercriminal operations.

The operation formally began offering its ransomware platform to external affiliates in September 2025, though development activity and early intrusions have been traced back to at least mid-2025. Unlike traditional RaaS programs that offer affiliates 70-80 percent of ransom proceeds, The Gentlemen offers a 90 percent share, together with full control over victim negotiations. This unusually generous split has attracted experienced operators away from competing ransomware brands and has been a key driver of the group's explosive growth.

Victim counts tracked from the group's dark-web leak site have grown from roughly **30 claimed victims in autumn 2025** to several hundred by mid-2026, spanning more than 70 countries and over 20 industry verticals, including manufacturing, technology, healthcare, financial services, education, transportation, retail, energy, and non-governmental organizations. Independent telemetry recovered from a compromised command-and-control server tied to the group's proxy infrastructure suggests the true number of affected organizations, including those never listed publicly, may be substantially higher than the leak-site count alone.

The group supplies affiliates with a **Go-based encryptor** (obfuscated with the Garble toolchain) capable of targeting Windows, Linux, NAS, and BSD systems, along with a dedicated C-based variant built specifically for VMware ESXi hypervisors. This multi-OS capability allows a single affiliate to encrypt an organization's workstations, servers, network-attached storage, and virtualization layer in a single coordinated operation.

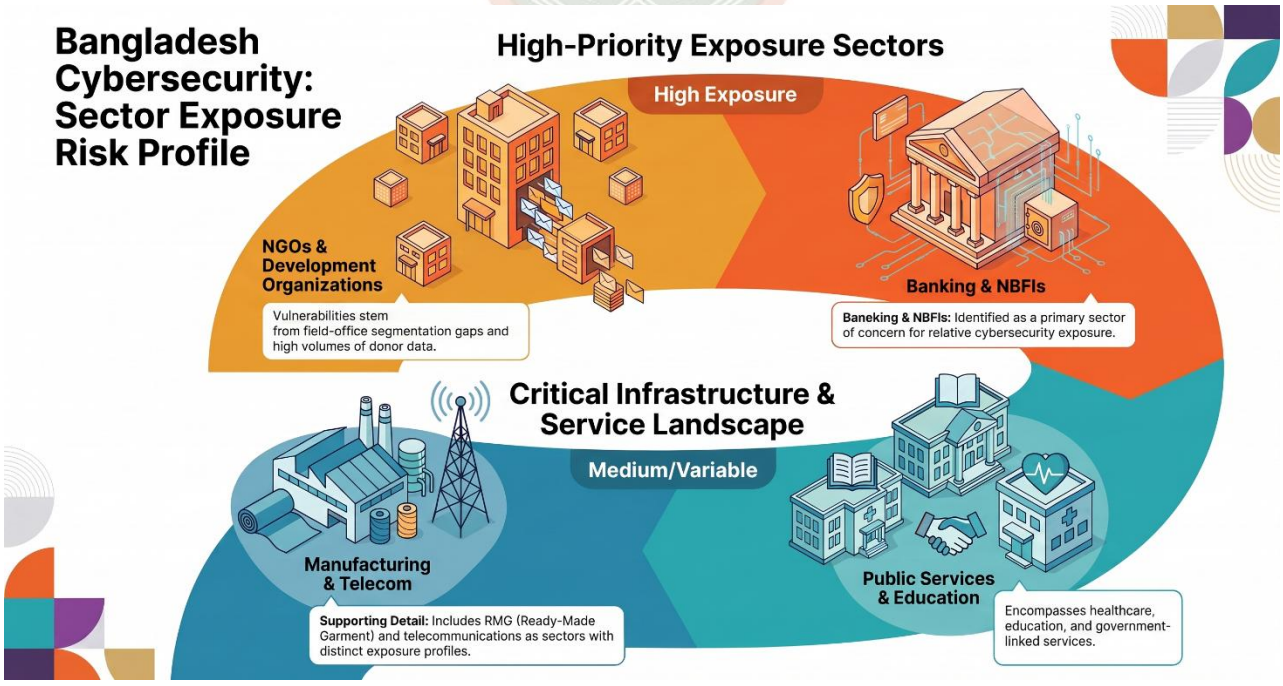

Figure: Bangladesh Sector Exposure

Relevance and Impact to Bangladesh

- **Confirmed regional targeting**: Public reporting has already linked this threat group to at least one large non-governmental development organization headquartered in Bangladesh, listed on the group's extortion site with a threat to leak internal data.
- **Sector exposure**: The group's established victim profile (NGOs and development organizations, financial services, manufacturing, healthcare, education, and telecommunications) closely mirrors sectors that BGD e-GOV CIRT has repeatedly flagged as high-value targets within Bangladesh.
- **Infrastructure exposure**: Bangladeshi organizations that operate internet-facing firewalls, VPN concentrators, backup servers, or VMware ESXi hosts without current patching are directly exposed to the group's primary initial access method.
- **Regional targeting bias**: Independent industry analysis has noted that this group has disproportionately targeted victims in Asia compared to many other ransomware operations, increasing the relative likelihood of further activity in Bangladesh and the wider region.
- **Operational risk to development and donor-funded organizations**: NGOs and development organizations in Bangladesh often manage large volumes of beneficiary, financial, and donor data across distributed field offices, and are frequently under-resourced for enterprise-grade security controls, making them attractive and comparatively soft targets for double-extortion operators.

BGD e-GOV CIRT strongly recommends that government agencies, financial institutions, NGOs and development organizations, telecommunications operators, and large enterprises in Bangladesh review the technical indicators and mitigation guidance in this advisory and act on the priority recommendations without delay.

Technical Analysis: Attack Lifecycle

The encryptor is written in Go and obfuscated with the **Garble toolchain**, targeting Windows, Linux, NAS, and BSD hosts from a single codebase; a separate, purpose-built C variant targets VMware ESXi hypervisors. Execution is fully operator-controlled through command-line flags, and the binary requires a build-specific password to run, a straightforward but effective anti-sandbox control; automated detonation environments that invoke the sample without the correct password receive a "**bad args**" error and no further execution.

```
:: Representative operator invocation:
:: authenticate, run local + share encryption, self-propagate using
the current
:: session token, then wipe free space to hinder recovery
gentlemen.exe --password <buildPassword> --full --spread "" --wipe
```

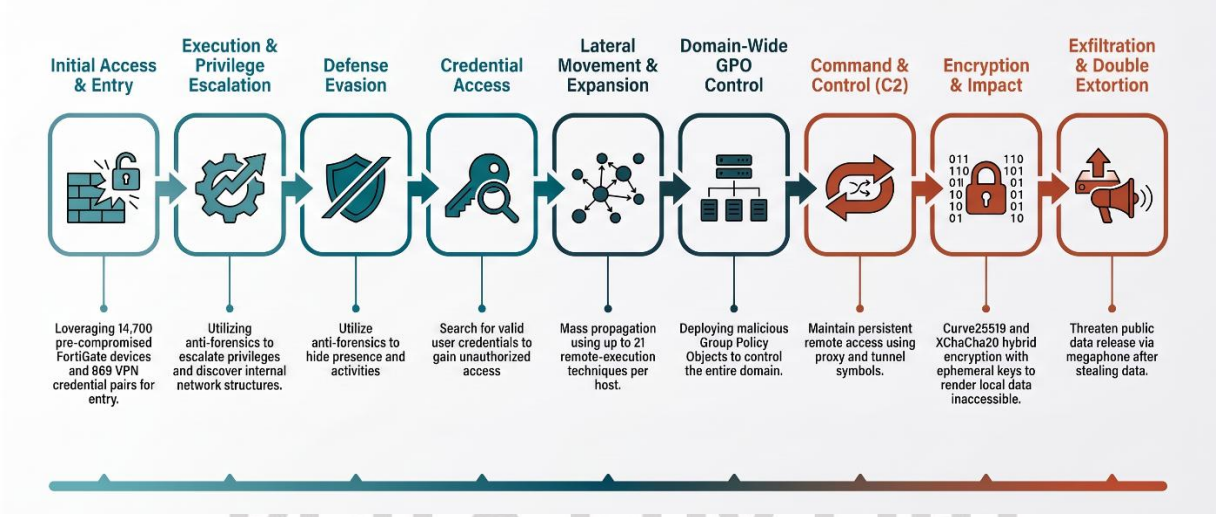

Figure: End-to-End Attack Lifecycle

Initial Access

Initial access is predominantly achieved through exploitation of internet-facing edge devices and abuse of valid credentials, rather than through sophisticated custom exploits:

- **Edge device exploitation**: Authentication-bypass and remote code execution vulnerabilities in firewalls, VPN gateways, backup software, and hypervisor management interfaces are exploited for unauthenticated or low-privilege network entry (see the CVE table below).
- **Pre-compromised access inventory**: Affiliates draw on an operator-maintained database reported to contain roughly 14,700 already-compromised FortiGate devices and 969 validated, brute-forced VPN credential pairs, allowing reconnaissance to be skipped entirely in favor of immediate network access.

- **Access brokerage**: Initial access is also purchased from independent initial access brokers (IABs), and credentials are sourced from infostealer malware logs and exposed administrative panels.
- **Conventional vectors**: Phishing, exposed Remote Desktop Protocol (RDP) endpoints, and weak or reused administrative credentials remain secondary but consistently observed entry points.

The following vulnerabilities have been associated with this threat group's initial access and privilege escalation activity and should be prioritized for patching and exposure review:

CVE	Affected Product	Role in Attack Chain
CVE-2024-55591	Fortinet FortiOS / FortiProxy	Authentication bypass used for initial access to edge devices
CVE-2025-32433	Erlang/OTP SSH server	Remote code execution used for initial access
CVE-2025-33073	Windows SMB client	Privilege escalation / lateral movement
CVE-2025-55182	Edge/remote-access gateway software	Exploited for initial access
CVE-2023-27532	Veeam Backup & Replication	Missing authentication abused for credential and backup access
CVE-2024-37085	VMware ESXi	Authentication bypass enabling hypervisor-level compromise
CVE-2025-7771	ThrottleStop.sys driver (BYOVD)	Kernel-level code execution to disable endpoint defenses

Execution, Persistence, and Privilege Escalation

Privilege escalation to SYSTEM is invoked via the **--system flag** (implied by --full). When set, the malware does not attempt in-process token manipulation; instead it schedules a one-time task that re-executes the binary under the SYSTEM account, optionally delayed using the --T flag:

```
:: Create a one-time task that re-executes the binary as SYSTEM,
one minute from now
schtasks /Create /RU SYSTEM /SC ONCE /TN gentlemen_system /TR
"C:\path\to\malware.exe" /ST <current_time+T>
schtasks /Run /TN gentlemen_system
```

When re-launched inside this scheduled-task context, the process sets the environment variable LOCKER_BACKGROUND=1 to signal that it is the elevated, background encryption worker rather than the operator-invoked parent process — a useful process-lineage artifact for EDR detection logic.

- **Kernel-level defense impairment**: Bring-Your-Own-Vulnerable-Driver (**BYOVD**) technique loads the legitimately signed **ThrottleStop.sys** driver, renamed **ThrottleBlood.sys**, and exploits **CVE-2025-7771** to obtain arbitrary kernel-level code execution, bypassing driver-signature enforcement and EDR self-protection.
- **Custom EDR-killer utilities**: Operator-supplied binaries (observed as All.exe and Allpatch2.exe, associated with a framework referred to as "**GentleKiller**") are executed to terminate endpoint protection and antivirus processes at the kernel level ahead of encryption.
- **Persistence (Windows)**: The encryptor removes any pre-existing scheduled task of the same name and recreates it to run at every system startup, and separately writes a Run-key value under the current user hive:

```
schtasks /Delete /TN UpdateUser /F
schtasks /Create /SC ONSTART /TN UpdateUser /TR
"C:\path\to\malware.exe"
reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
GupdateU /t REG_SZ /d "C:\path\to\malware.exe" /f
```

- **Persistence (Linux/ESXi):** Equivalent persistence on non-Windows hosts is achieved by modifying `/etc/rc.local.d/local.sh` and dropping a disguised binary at `/bin/.vmware-authd`.

Defense Evasion and Anti-Forensics

Before encryption begins, the malware systematically dismantles defensive and forensic capabilities on the local host through a scripted sequence of native commands rather than custom tooling, which makes the sequence highly amenable to behavioral detection:

```
# Disable real-time protection and whitelist the malware's own
process
Set-MpPreference -DisableRealtimeMonitoring $true -Force
Add-MpPreference -ExclusionProcess <malware_name> -Force
Add-MpPreference -ExclusionPath C:\ -Force

:: Destroy Volume Shadow Copy backups (two redundant methods)
vssadmin delete shadows /all /quiet
wmic shadowcopy delete

:: Remove forensic artifacts
del /f /q C:\Windows\Prefetch\*.*
```

```
del /f /q "C:\ProgramData\Microsoft\Windows Defender\Support\*.*"
del /f /q %SystemRoot%\System32\LogFiles\RDP*\*.*
```

The malware additionally deletes PowerShell command history from every local user profile (`C:\Users\*\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt`) and clears the Windows Security and System event logs using native log-management calls, directly impairing timeline reconstruction during incident response.

- **Process and service termination**: The malware iterates a hardcoded list of process and service names spanning database engines (e.g., sqlservr), backup/recovery agents (e.g., VeeamNFSSvc), virtualization services (e.g., vmms), office productivity software, and security agents, using taskkill /IM <name>.exe /F for processes and sc config <name> start=disabled followed by net stop <name> for services — releasing file locks and disabling recovery paths simultaneously.
- **Anti-forensic disk wipe**: When invoked with --wipe, free disk space is overwritten after encryption completes, defeating file-carving and undelete-based recovery attempts against deleted originals.

Credential Access and Internal Discovery

- **Credential dumping**: In-memory credential material is harvested using Mimikatz, targeting LSASS process memory for cached domain and local credentials.
- **Network and AD reconnaissance**: Internal mapping is performed using Advanced IP Scanner and Nmap for host/service discovery, combined with Active Directory enumeration (domain trusts, organizational units, group memberships, and privileged accounts) to identify high-value targets and plan the self-propagation and GPO-deployment phases.
- **Persistent fallback access**: AnyDesk is installed with a hardcoded, operator-known password, providing a remote-access channel that survives credential rotation and is independent of the original intrusion vector — this should be treated as a durable indicator of compromise in its own right.

Lateral Movement and Self-Propagation

The self-propagation module, enabled via the --spread flag, is the most distinctive and operationally dangerous component of this threat: it converts a single-host encryptor into a worm that autonomously deploys itself across every reachable system on the network. The flag accepts either explicit **domain/user:password** credentials for authenticated lateral movement, or an empty string to reuse the current session's authentication token.

Once triggered, the infected host is converted into a distribution point:

1. The binary is copied into `C:\Temp` on the local host.

2. A hidden SMB share is published (`\\<self>\share$`) configured for anonymous access, exposing the payload to any host that can reach the infected system.
3. A copy of PsExec is dropped locally or downloaded, and the malware enumerates all reachable workstations, servers, and domain controllers as targets.

Against every enumerated target, the malware first runs a single scripted "**defense evasion blob**" over the network to strip the remote host's protections before attempting deployment:

```
# Disable Defender, disable the host firewall on all profiles, add
broad exclusions
Set-MpPreference -DisableRealtimeMonitoring $true;
Add-MpPreference -ExclusionPath 'C:\';
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled
False;

# Re-enable legacy SMBv1 on the target to widen available
propagation methods
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -
NoRestart;

# Loosen anonymous-access restrictions on the target
reg     add     'HKLM\SYSTEM\CurrentControlSet\Control\Lsa'     /v
EveryoneIncludesAnonymous /t REG_DWORD /d 1 /f
```

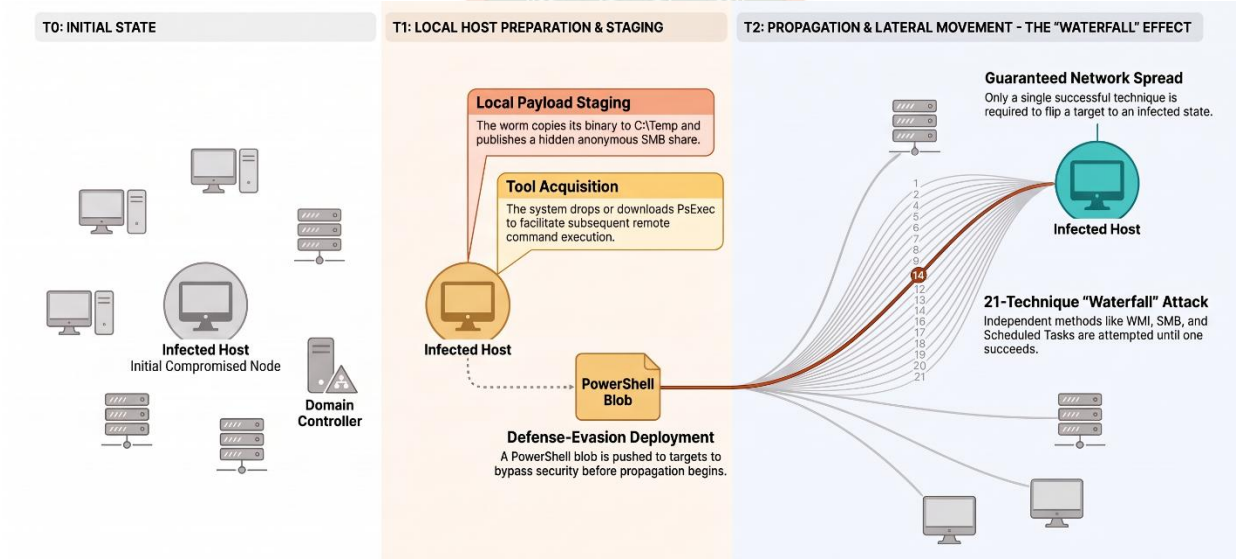

Figure: Self-Propagation Worm Mechanism

The malware then attempts payload execution through as many as **21 independent remote-execution techniques** per target host, including remote file copy over the C$ administrative share, PsExec, WMIC, remote scheduled task creation, remote Windows service creation, PowerShell remoting, and direct WMI process creation. Each method is attempted independently, so a single successful execution on any one host is sufficient to keep the worm

spreading even in partially hardened environments — this redundancy, rather than any single technique, is the core of its propagation strategy.

Domain-Wide Deployment via Group Policy

The most severe impact scenario occurs when a Domain Controller is compromised. The malware includes a built-in Group Policy deployment mode (invoked via a dedicated --gpo path) that:

1. Copies the encryptor binary to the NETLOGON share on the compromised Domain Controller, making it accessible to every domain-joined system.
2. Creates a malicious Group Policy Object (GPO) containing an immediate scheduled task pointed at the staged binary.
3. Forces a policy refresh across the domain (equivalent to bulk gpupdate /force / Invoke-GPUpdate activity), triggering near-simultaneous execution of the scheduled task on every domain-joined endpoint.

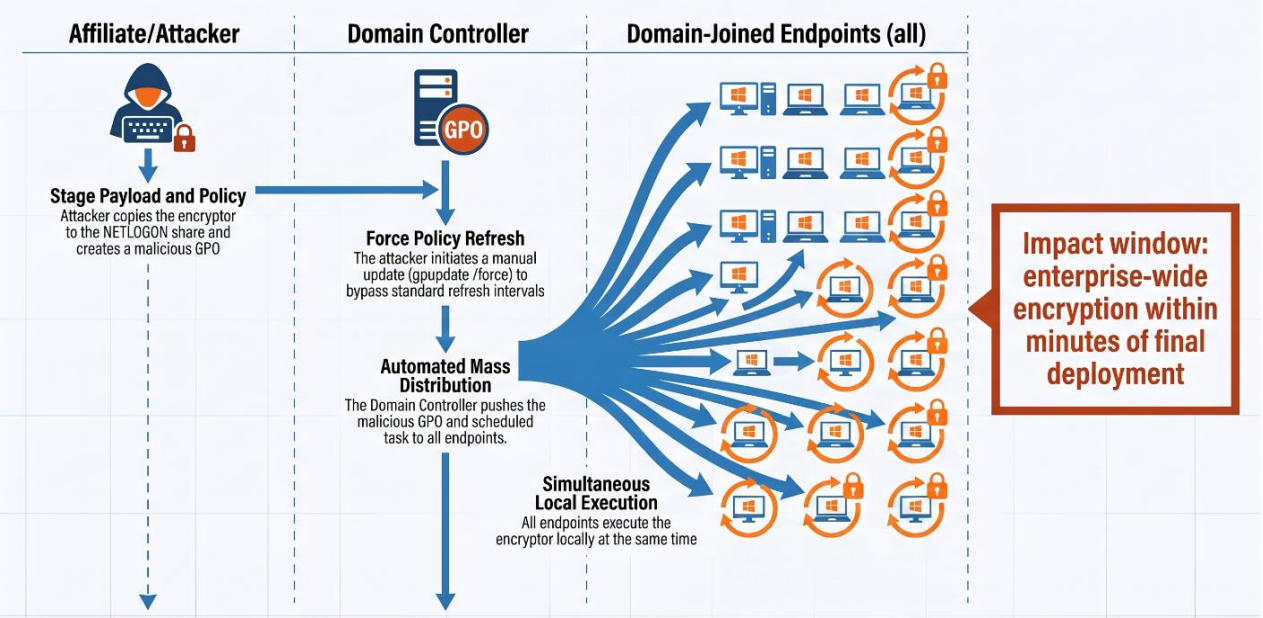

Figure: Domain-Wide GPO Deployment Sequence

This mechanism can achieve enterprise-wide encryption within minutes of final deployment and does not depend on the 21-technique self-propagation module succeeding host-by-host, making Domain Controller hardening and GPO change monitoring among the single most important defensive controls against this threat.

Command and Control

- **Framework-based C2:** Affiliates commonly deploy Cobalt Strike beacons for interactive command-and-control alongside the ransomware payload.
- **Proxy tunnelling:** SystemBC is used to establish SOCKS5 proxy tunnels using an RC4-encrypted communication protocol, allowing the operator to route traffic through the victim network and stage additional tooling without generating conventional outbound connections that would be flagged by simple network-layer monitoring.
- **Negotiation channel:** Ransom negotiation is conducted out-of-band via the Tox and Session messaging protocols rather than through the leak site itself, complicating law-enforcement and takedown efforts.

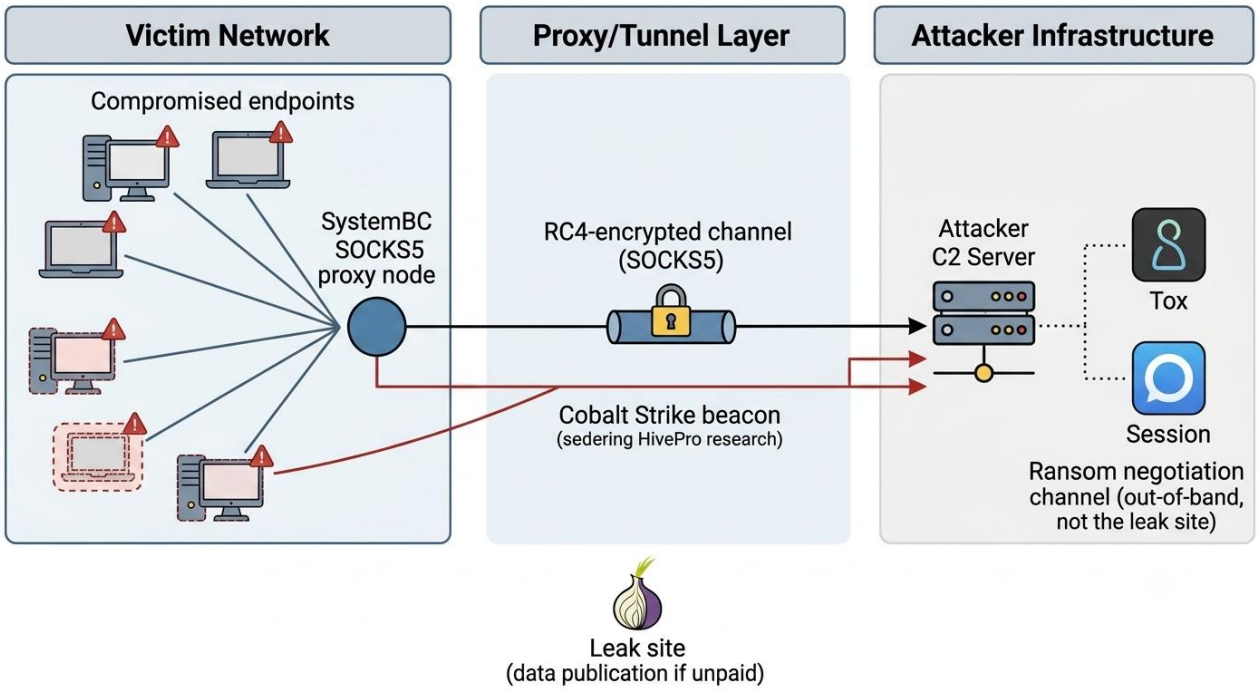

Figure: Command-and-Control Architecture

Encryption Mechanism

Encryption uses a hybrid cryptographic design combining **Curve25519** elliptic-curve key exchange with the **XChaCha20** stream cipher, applied independently on a per-file basis:

1. For each file, the malware generates a unique, ephemeral Curve25519 key pair (a random private key and its corresponding public key).
2. It computes an Elliptic-Curve Diffie-Hellman (ECDH) shared secret between the ephemeral private key and the operator's embedded public key.
3. The shared secret becomes the XChaCha20 encryption key; the nonce is derived from the first 24 bytes of the ephemeral public key.

4. File contents are encrypted with XChaCha20 using this key and nonce. Small files are encrypted in full; large files instead have three distributed chunks encrypted in 64 KB XChaCha20 blocks, each with an independently mutated nonce to prevent keystream reuse across chunks.
5. The Base64-encoded ephemeral public key is appended to the file footer, allowing decryption only by whoever holds the operator's corresponding private key — third-party or brute-force decryption is not mathematically feasible.

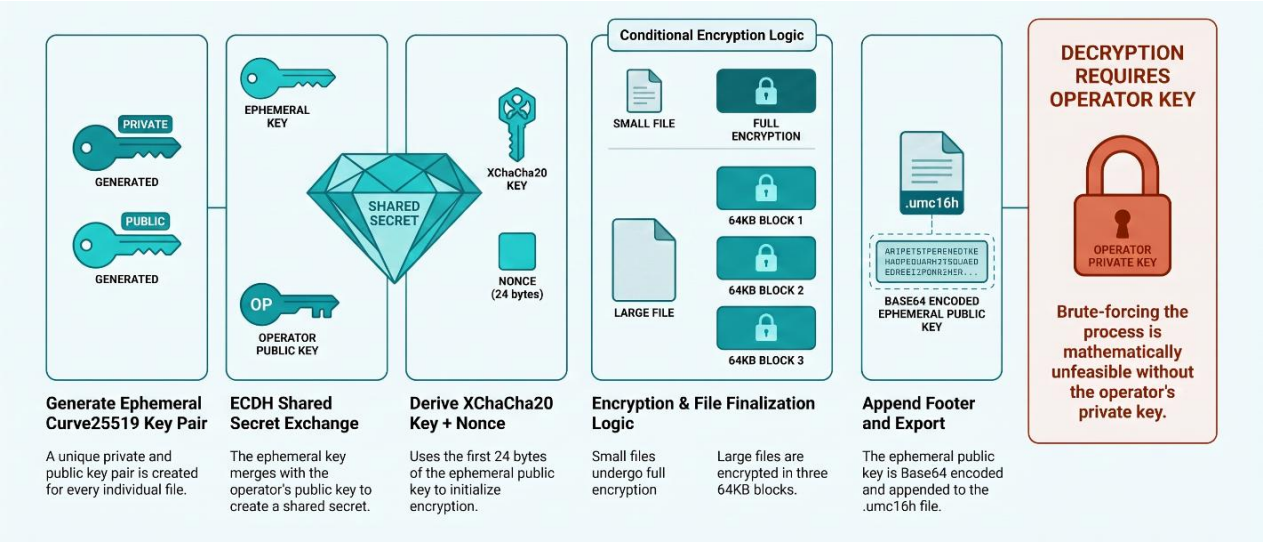

Figure: Hybrid Encryption Process

Immediately before encrypting each file, the malware forces file access to succeed regardless of existing permissions:

```
takeown /f <file_path> /r /d y
icacls <file_path> /grant *S-1-1-0:(OI)(CI)F /T
attrib -R <file_path>
```

A configurable speed flag sets the proportion of each large-file chunk that is actually encrypted, ranging from roughly 0.3 percent to 9 percent — sacrificing completeness for throughput while still rendering the file unusable. Encrypted files are renamed with the *.umc16h* extension, and a *README-GENTLEMEN.txt* ransom note is dropped in affected directories. Because decryption requires the operator's private key, and Volume Shadow Copies and backup infrastructure are deliberately targeted for destruction earlier in the chain, recovery without paying the ransom depends entirely on the availability of offline, immutable, or otherwise inaccessible backups.

Data Exfiltration and Double Extortion

Consistent with the double-extortion model used by most modern RaaS operations, affiliates exfiltrate sensitive data — commonly ranging from hundreds of gigabytes to multiple

terabytes per victim — before encryption begins, typically staging and transferring data over encrypted channels via WinSCP. If a victim does not pay, stolen data is published on a Tor-based leak site, and additional public pressure is applied through negotiation over the Tox and Session messengers and, in some cases, a branded social media presence. The group has demonstrated consistent follow-through on data-leak threats, which should factor into any organizational risk and incident-response decision-making.

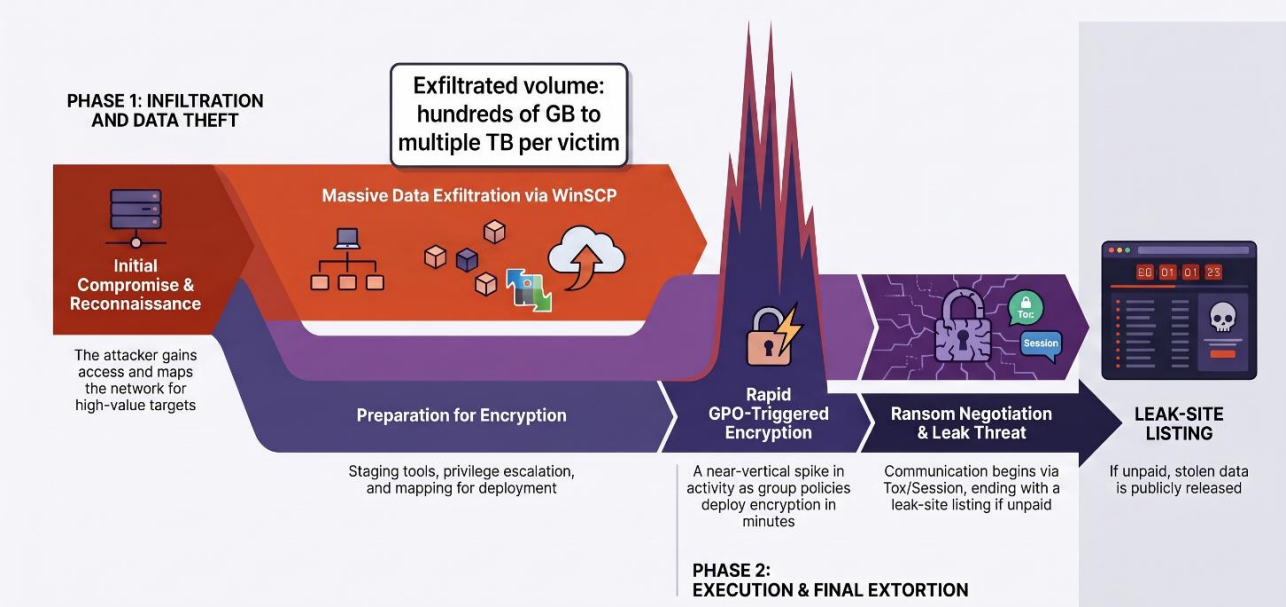

Figure: Double Extortion Timeline

MITRE ATT&CK Mapping

Tactic	Representative Techniques
Initial Access	T1078 Valid Accounts; T1133 External Remote Services; T1190 Exploit Public-Facing Application
Execution	T1059.001/.003 PowerShell & Windows Command Shell; T1047 WMI; T1053.005 Scheduled Task
Persistence	T1053.005 Scheduled Task; T1547.001 Registry Run Keys; T1543.003 Windows Service
Privilege Escalation	T1078 Valid Accounts; kernel driver abuse (BYOVD)
Defense Evasion	T1562.001/.004 Impair Defenses; T1070.001/.004 Indicator Removal; T1036 Masquerading; T1027 Obfuscation
Credential Access	T1003 OS Credential Dumping; T1555 Credentials from Password Stores
Discovery	T1018 Remote System Discovery; T1135 Network Share Discovery; T1482 Domain Trust Discovery; T1518.001 Security Software Discovery

Lateral Movement	T1021.001/.002/.006 RDP, SMB Admin Shares, WinRM; T1570 Lateral Tool Transfer
Command and Control	T1090.003 Multi-hop Proxy; T1071.001 Web Protocols; T1573.002 Asymmetric Cryptography; T1105 Ingress Tool Transfer
Exfiltration	T1041 Exfiltration Over C2 Channel
Impact	T1486 Data Encrypted for Impact; T1490 Inhibit System Recovery; T1489 Service Stop; T1657 Financial Theft

Indicators of Compromise (IoC)

The following indicators, drawn from published threat research as of July 2026, should be used for retrospective log review, threat hunting, and detection rule creation. Note that ransomware infrastructure changes frequently; these indicators should be treated as a starting point rather than an exhaustive list.

Indicator Type	Value
Encrypted file extension	`.umc16h`
Ransom note filename	`README-GENTLEMEN.txt`
Registry persistence key	`HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GupdateU`
Linux/ESXi persistence path	`/bin/.vmware-authd and /etc/rc.local.d/local.sh`
IPv4 (C2 / infrastructure)	`194.87.31.69`
IPv4 (C2 / infrastructure)	`91.107.247.163`
IPv4 (SystemBC proxy)	`45.86.230.112`

SHA256 (sample)	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5
SHA256 (sample)	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a
SHA256 (sample)	22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67
SHA256 (sample)	2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d
SHA256 (sample)	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235
Tor leak site	tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion

Mitigation and Recommended Actions

Priority actions

- Identify and patch all internet-facing firewalls, VPN concentrators, backup software, and hypervisor management interfaces against the vulnerabilities listed in the CVE table, prioritizing FortiOS/FortiProxy, Veeam Backup & Replication, and VMware ESXi.
- Audit internet-facing systems for indicators of prior exploitation, and rotate credentials for any accounts or devices that may have been exposed to brute-force attempts.
- Enforce phishing-resistant multi-factor authentication (MFA) on all remote access, VPN, and administrative accounts, and eliminate legacy authentication protocols where feasible.

Harden Active Directory and internal segmentation

- Treat Domain Controllers as tier-0 assets: restrict interactive and network logons, and monitor for unusual administrative share writes, abnormal remotely launched binaries, and PowerShell sessions spawned under scheduled-task contexts.
- Alert on the creation of new Group Policy Objects, changes to NETLOGON/SYSVOL scheduled-task files, and bulk policy-refresh activity across domain-joined systems — this is the group's single most impactful deployment mechanism and must be detectable in near real time.
- Enforce strict SMB signing, fully disable SMBv1, and restrict lateral network movement between internal segments to contain any self-propagation attempt.
- Treat virtualization management interfaces (e.g., ESXi) as tier-0 infrastructure: disable SSH by default, enable only for defined maintenance windows, and isolate management interfaces on a dedicated VLAN.

Strengthen endpoint and defense controls

- Enable EDR/antivirus tamper protection, restrict who can modify security-agent configuration, and alert on commands that disable real-time protection or add broad scanning exclusions.
- Monitor for unsigned or known-vulnerable driver loading events (BYOVD activity) and for tools used to terminate security processes at the kernel level.
- Implement behavioral alerts for the deletion of Volume Shadow Copies, clearing of Windows Security/System event logs, and mass deletion of Prefetch or RDP log artifacts.

Detect reconnaissance, credential theft, and C2 activity

- Monitor for internal use of network scanning and enumeration tools not sanctioned for routine administrative use.
- Deploy detection for credential-dumping activity from memory and for access to locally stored credential stores.
- Monitor for anomalous outbound connections over non-standard ports, unexpected SOCKS5 proxy traffic from endpoints that should never act as proxies, and traffic patterns consistent with known offensive-security C2 frameworks.

Ensure recovery capability

- Maintain and regularly test offline, immutable, or air-gapped backups for all critical systems, including domain controllers, file servers, databases, and virtualization hosts.
- Implement behavioral alerts for use of shadow-copy deletion and disk-wiping utilities, which are consistently used by this threat group immediately before and after encryption.
- Develop and rehearse an incident response and business continuity plan specific to enterprise-wide ransomware encryption scenarios, including domain-wide GPO-based deployment.

Organizational and third-party risk management

- Establish minimum security requirements for third-party vendors, managed service providers, and donor/partner platforms with network access, and monitor for breach disclosures affecting them.
- For NGOs and development organizations in particular, ensure that field offices and remote sites are covered by the same patching, MFA, and backup standards as head-office infrastructure.
- Engage a qualified incident response provider and legal counsel before any communication with the threat actor if a compromise is suspected or confirmed, and avoid unilateral ransom negotiation.

References

- https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/
- https://www.hivepro.com/threat-advisory/the-gentlemen-ransomware-a-rapidly-scaling-raas-threat
- https://www.picussecurity.com/resource/blog/how-the-gentlemen-ransomware-spreads-and-encrypts-entire-networks
- https://www.fortiguard.com/threat-actor/6387/the-gentlemen-ransomware
- https://www.dexpose.io/the-gentlemen-ransomware-attack-on-brac/
- https://www.cisa.gov/stopransomware/ransomware-guide