TIR-20260805 The Gentlemen Ransomware Operation

8/5/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

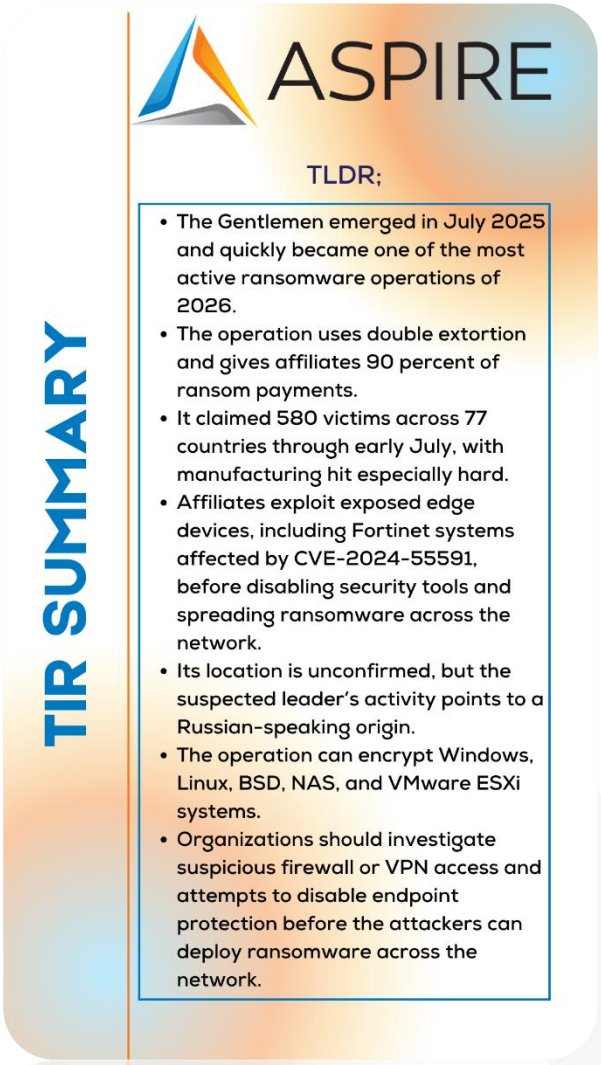
Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Gentlemen is a financially motivated ransomware group that has become one of the most active ransomware-as-a-service operations in 2026. The group appeared in mid-2025, initially operating as a closed team before opening its ransomware platform to affiliates. Its growth has been driven by a 90 percent affiliate payout and a toolset designed to compromise Windows, Linux, network-attached storage, BSD, and VMware ESXi environments.

The operation uses double extortion by stealing data before encrypting systems and threatening to publish it if the victim does not pay. The ransomware can spread across a network using several remote-execution methods at once, leaving defenders less time to contain the attack.



The Gentlemen has targeted organizations across manufacturing, technology, healthcare, financial services, education, transportation, construction, and logistics. Although U.S. organizations are among its victims, the operation is not focused on one country. Through July 7, 2026, 580 victims across 77 countries had been listed on its data leak site. These numbers come from the group's leak site and have not all been independently verified. The total could be higher because victims that pay may never be publicly named.

THE GENTLEMEN RANSOMWARE OPERATION

The Gentlemen emerged around July 2025 and began openly recruiting affiliates in September. The operation grew out of ArmCorp, an affiliate group that operated within the Qilin ransomware group.

The split followed a July 2025 payment dispute on the RAMP cybercrime forum, where a user called hastalamuerte accused Qilin of withholding about $48,000 in commission. The name zeta88 later appeared in the threat actor recruitment posts on underground forums and in internal group chats leaked in May 2026. Check Point Research compared those messages with earlier posts by hastalamuerte and concluded that the two aliases were very likely used by the same person.

The Gentlemen follows a ransomware-as-a-service model. The core group develops the ransomware, runs the leak site, maintains the infrastructure, and controls the decryption keys. Affiliates gain access to victim networks, steal data, and deploy the ransomware. They keep 90 percent of ransom payments, compared with the 70 to 80 percent commonly offered by other ransomware operations. In May 2026, the threat actor also partnered with a BreachForums operator to recruit penetration testers and initial access brokers.

Unit 42 reported that The Gentlemen claimed 117 victims in June 2026, just under four times its January total. Its review of leak-site data counted 580 claimed victims through July 7, including 103 manufacturers. Check Point's June 2026 threat report ranked The Gentlemen as the month's most prevalent ransomware group, accounting for 17 percent of published attacks. Victims have also included organizations in manufacturing, IT services, healthcare, financial services, construction, and logistics. Its telemetry showed the most activity in Brazil, China, Indonesia, Taiwan, and Thailand.

No country has been confirmed as the threat actor's base of operations. The operation's suspected leader communicates in Russian and has been active on Russian-language cybercrime forums. This points to a Russian-speaking origin, although its affiliates could be located in other countries.

Connections to Other Groups

The Gentlemen is best understood as a breakaway operation rather than a completely new ransomware group. Its suspected founder previously worked as a Qilin affiliate and had experience with other ransomware ecosystems.

A May 2026 leak of the group's internal database exposed nine accounts and conversations about its infrastructure, ransomware builder, payouts, affiliates, victims, vulnerabilities, EDR-killing tools, and ransom negotiations. Despite the leak, The Gentlemen continued adding victims and updating its malware.

Tactics, Techniques, and Procedures (TTPs)

The Gentlemen does not follow one fixed attack path because affiliates bring their own access and tools. Most incidents begin with an exposed edge device or a compromised account, followed by network discovery and credential theft. Once the attackers have administrative access, they disable security controls and deploy the ransomware across as many systems as possible.

Initial Access

The threat actor often gains access through internet-facing firewalls, virtual private network appliances, and other remote access services. Observed access methods include:

- Affiliates exploit vulnerabilities in exposed firewalls, VPN appliances, and other online services.
- Fortinet devices are a frequent target. CVE-2024-55591, an authentication bypass vulnerability in FortiOS and FortiProxy, has been associated with the threat actor's Fortinet activity.
- Stolen, leaked, weak, and default credentials are used to access remote services.
- Internal conversations leaked in May 2026 showed interest in Cisco edge appliances, NTLM relay attacks, and stolen Outlook Web Access and Microsoft 365 credentials.

- Affiliates also purchase access from initial access brokers.

In some incidents, access was established long before the ransomware was deployed, suggesting it may have been purchased from another threat actor or access broker. In others, encryption began within hours of the initial compromise. The timing depends on the affiliate and how the access was obtained.

Discovery and Lateral Movement

After gaining access, affiliates scan the internal network and gather information about Active Directory, connected systems, open ports, and available services. Tools observed during this stage include:

- SharpADWS for collecting information about Active Directory objects and the domain environment.
- NetScan and Advanced IP Scanner for locating systems, ports, and services across the network.
- Native Windows commands for identifying domain administrators, domain controllers, active sessions, and trusted domains.

Observed tools include Mimikatz for credential theft, Cobalt Strike for controlling compromised systems, and SystemBC for routing traffic through a SOCKS proxy. Their use depends on the affiliate handling the attack.

The Go-based encryptor also contains its own propagation feature. When enabled, it enumerates reachable systems, copies the ransomware to remote hosts, and attempts several execution methods against each target. The malware can:

- Copy the encryptor through administrative shares such as C$ or retrieve it from a hidden Server Message Block share.
- Execute the ransomware remotely with PsExec or Windows Management Instrumentation.
- Create and run remote scheduled tasks and Windows services.
- Use Windows Remote Management and PowerShell Invoke-Command to run commands on other systems.
- Authenticate with supplied domain credentials or reuse the current session token.

The ransomware can also be deployed through Group Policy from a compromised domain controller, causing it to run across domain-joined systems when policies refresh. In some attacks, a custom Go backdoor was installed before the ransomware. It collects host and network details, connects to a command-and-control server, runs commands through the Windows command shell, and creates a SOCKS proxy for moving through the network.

Defense Evasion and Encryption

Disabling security software is a major part of the Gentlemen's activity. The core group maintains GentleKiller, an EDR-killing framework with at least eight variants. These tools load vulnerable or malicious drivers that can terminate endpoint security processes.

Affiliates also have access to third-party EDR-killing tools, including HexKiller, ThrottleBlood, and HavocKiller. Providing these tools gives affiliates ready-made options for disabling security products before ransomware deployment.

The ransomware takes several additional steps before encryption:

- It disables Microsoft Defender real-time monitoring and adds the ransomware executable, staging folders, and the C:\ drive to the Defender exclusion list.
- It can disable Windows Firewall across all profiles and enable Server Message Block version 1 to support lateral movement.
- It stops processes and services associated with databases, backup products, virtual machines, email servers, and business applications so their files can be encrypted.
- It deletes Volume Shadow Copies with vssadmin and Windows Management Instrumentation to prevent recovery.
- It clears the System, Application, and Security event logs and deletes PowerShell command history, prefetch data, Defender logs, and Remote Desktop Protocol records.
- Its optional wipe function overwrites free disk space after encryption, while another setting allows the executable to delete itself.

The primary Windows encryptor is written in Go and protected with Garble obfuscation. It generates a unique Curve25519 key pair for each file and uses the resulting shared

secret as the XChaCha20 encryption key. Files of 1 MB or less are encrypted in full, while larger files are damaged by encrypting three separate sections to reduce the time needed.

The encryptor handles local drives and mapped network shares in separate processes. The Gentlemen also has versions for Linux, BSD, NAS devices, and VMware ESXi. Encrypted files are given the extension assigned to that build, and a README-GENTLEMEN.txt ransom note is placed in affected directories.

Recent Attacks

Oltenia Energy Complex

On December 26, 2025, The Gentlemen encrypted files on the business network of Oltenia Energy Complex, Romania's largest coal-based electricity producer. The company did not disclose how the attackers gained access. The attack took its enterprise resource planning system, document management applications, email, and website offline, partially disrupting business operations.

Electricity production continued without interruption. The company isolated the affected systems and began restoring them from backups while investigating whether any data had been stolen.

The Adaptavist Group

In March 2026, an unauthorized party used stolen credentials to access systems belonging to U.K.-based technology consultancy The Adaptavist Group. The company confirmed that business contact information, contracts, and nondisclosure agreements were present on affected systems.

The Gentlemen claimed a much broader compromise, but Adaptavist said it had not found evidence supporting claims that customer production systems or additional sensitive client data had been accessed. This incident is why threat actor statements should not be treated as confirmed facts without evidence from the victim or investigators.

Soniva Dental Care

In May 2026, suspicious remote-access sessions were detected on systems belonging to Soniva Dental Care, a dental services provider with locations in Texas and Massachusetts. The activity targeted the company's Remote Desktop Web Services infrastructure.

Soniva blocked external connections, disabled remote-access accounts, and reset company passwords. Its patient record system was restored quickly, but files containing names, addresses, dates of birth, identification numbers, and medical information may have been accessed. At least 30,000 Texas residents were affected. The Gentlemen later claimed responsibility and posted samples of the data on its leak site.

The Gentlemen has claimed attacks against the following U.S.-based organizations, although most have not independently confirmed the group's attribution:

- Soniva Dental Care
- South Texas Spinal Clinic
- TDS Telecommunications
- Gator Cases
- FMS, Inc.
- Clark Fixture Technologies
- Manhattan Fire & Security
- E-Control Systems
- Internal Medicine of Southwest Florida
- Trigon America
- Executive Coach
- Lopes Law
- Tangram Interiors
- Conecsus
- MatTek Corporation
- Advantage Home Health Care

Conclusion

The Gentlemen became one of the most active ransomware operations of 2026 less than a year after it emerged. Its affiliate model helped it expand quickly by bringing more attackers into the operation and giving them tools to disable security controls before deploying ransomware across a domain. Unexpected access through an edge device or attempts to shut down endpoint protection may be early signs of an incoming ransomware attack.

Aspire's Recommendations

These recommendations address activity documented in Gentlemen attacks. The priority is to stop affiliates before they obtain the administrative access needed to deploy ransomware across the domain.

- Patch internet-facing firewall and VPN appliances, giving priority to Fortinet devices affected by CVE-2024-55591. Aspire's CTI team previously issued an Emergency Flash Notice regarding this vulnerability.
    - Review management logs for unfamiliar source addresses, unexpected administrator logins, and newly created accounts.
- Require phishing-resistant multi-factor authentication for firewall management, VPN access, Microsoft 365, and privileged accounts.
    - Revoke active sessions and rotate credentials if an edge device may have been compromised.
- Limit remote use of PsExec, Windows Management Instrumentation, and Windows Remote Management to approved administrative systems. Restrict Server Message Block traffic between network segments and alert on unauthorized Group Policy changes.
- Enable EDR tamper protection and the Microsoft vulnerable driver blocklist. Use application control to prevent GentleKiller and other unauthorized tools from loading kernel drivers or stopping security services.
- Monitor for scheduled tasks named gentlemen_system, DefU, UpdateGU, and UpdateGU2. Investigate unexpected use of vssadmin, wmic, wevtutil, or

schtasks, particularly when followed by security-service failures or encryption activity.

- Keep immutable or offline backups that cannot be accessed with domain administrator credentials. Test recovery procedures for domain controllers, VMware ESXi hosts, NAS devices, and other systems the ransomware can encrypt.

MITRE MAP

Initial Access	T1190 – Exploit Public-Facing Application T1078 – Valid Accounts T1133 – External Remote Services
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell T1059.003 – Command and Scripting Interpreter: Windows Command Shell T1047 – Windows Management Instrumentation
Persistence	T1053.005 – Scheduled Task/Job: Scheduled Task T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1543.003 – Create or Modify System Process: Windows Service
Stealth	T1036 – Masquerading T1036.001 – Masquerading: Invalid Code Signature T1027 – Obfuscated Files or Information T1070.003 – Indicator Removal: Clear Command History
Defense Impairment	T1685 – Disable or Modify Tools T1685.005 – Disable or Modify Tools: Clear Windows Event Logs T1686.003 – Windows Host Firewall
Credential Access	T1110 – Brute Force T1003 – OS Credential Dumping
Lateral Movement	T1021.002 – Remote Services: SMB/Windows Admin Shares T1021.006 – Remote Services: Windows Remote Management
Command and Control	T1090 – Proxy T1105 – Ingress Tool Transfer
Impact	T1486 – Data Encrypted for Impact T1490 – Inhibit System Recovery T1489 – Service Stop

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

IP Address

- 81[.]177[.]215[.]15:9443 – Go backdoor command-and-control server

SHA-256 Hashes

- 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67 – Go ransomware encryptor
- fe1033335a045c696c900d435119d210361966e2fb5cd1ba3382608cfa2c8e68 – Gentlemen wallpaper file

Files and Artifacts

- README-GENTLEMEN.txt
- %TEMP%\gentlemen.bmp
- Scheduled tasks: gentlemen_system, DefU, UpdateGU, and UpdateGU2
- Environment variable: LOCKER_BACKGROUND=1

SUPPORTING DOCUMENTATION

Romanian energy provider hit by Gentlemen ransomware attack

Australian sugar producer works to restore operations as ransomware group claims attack | The Record from Recorded Future News

Security incident March 2026

Killing me gently: Inside Gentlemen's EDR killer framework

The Gentlemen ransomware: Dissecting a self-propagating Go encryptor | Microsoft Security Blog

The Gentlemen RaaS: rapid growth and a new ransomware variant | Securelist

Thus Spoke…The Gentlemen - Check Point Research

A New Ransomware Leader Emerges as June 2026 Attack Volumes Climb Worldwide - Check Point Blog

The Gentlemen Ransomware Group Is Scaling Faster Than Any Other Group on Record

No Manners Here: The Ruthless Rise of The Gentlemen Ransomware

The Gentlemen Ransomware Attack on The Clinic in North Dakota - DeXpose

Soniva Dental Care Data Breach Affects At Least 30,000 Patients

APPENDIX: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.