Smarttech
YOUR 24/7 SECURITY PARTNER

THREAT ACTOR SPOTLIGHT

Published 4 September 2026
Threat Intelligence Team

THE GENTLEMEN

Fast-scaling ransomware-as-a-service group that split from Qilin in July 2025 over an unpaid commission dispute. Pairs a Go and C-based multi-platform locker with an in-house EDR-killer suite, and is now growing faster than any ransomware operation on record.

Storm-2697 | ArmCorp | Stinkbug | Qilin RaaS

RISK RATING	ACTIVE SINCE	MOTIVATION	PRIMARY VECTOR	RANSOMWARE TIES
Critical	2025	Financial extortion	Fortinet/Cisco edge exploits, stolen credentials	90/10 affiliate split, RaaS

ATTACK CHAIN

1 Initial Access
Exploits exposed FortiOS/FortiProxy and Cisco/Erlang SSH devices, or uses stolen and brute-forced domain credentials.

2 Credential Harvesting
Dumps credentials and abuses NTLM relay and reflection to escalate privileges across the domain.

3 Defense Evasion
Deploys GentleKiller, an in-house EDR-killer suite built on eight-plus BYOVD variants, to blind security tooling.

4 Mass Propagation
Spreads via RDP, SMB, SSH, PsExec, and WMI, using NETLOGON group policy to encrypt domain-joined systems at once.

5 Double Extortion
Encrypts Windows, Linux, and ESXi hosts, staging exfiltrated data for release on a Tor-based leak site if unpaid.

MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1190	Exploit public-facing application (FortiOS, Cisco/Erlang SSH)
T1078	Valid accounts (stolen or brute-forced credentials)
T1557	NTLM relay/reflection for privilege escalation
T1567	Exfiltration over web service (Snowflake & cloud)
T1562.001	Impair defenses (GentleKiller EDR-killer, BYOVD)
T1021	Lateral movement via RDP/SMB/PsExec/WMI
T1490	Inhibit system recovery (shadow copy deletion, backup tampering)

SECTOR BY SECTOR Summary

Manufacturing
Hit hardest of any sector, using exposed Fortinet and Cisco edge devices as a foothold onto production networks.

Technology
Targeted for high-value credentials, letting the group pivot into downstream customers and partner networks.

Healthcare
Struck despite the operational risk, reinforcing that this group draws no line around patient-critical systems.

Smarttech
YOUR 24/7 SECURITY PARTNER

THE GENTLEMEN

ORIGIN & EVOLUTION

Split from Qilin on 22 July 2025 after a dispute over a $48,000 commission payment, taking its own affiliate program with it. Microsoft tracks the group as Storm-2697; it previously operated under the name ArmCorp while still a Qilin affiliate. In May 2026 its own backend was breached, leaking chat logs, affiliate details, and negotiation transcripts, exposing the operation it built to disrupt others.

THREAT LANDSCAPE CONTEXT

A direct offshoot of Qilin, run by an administrator (hastalamuerte) who learned the trade as a Qilin affiliate before building a rival operation. Its 90/10 affiliate split, the highest in the market, is actively pulling talent away from competitors rather than just growing organically.

SIGNATURE TRADECRAFT

Gains access through exposed FortiOS/FortiProxy and Cisco/Erlang SSH devices, or stolen and brute-forced domain credentials, then abuses NTLM relay and reflection to escalate privileges. Its signature tool is GentleKiller, an in-house EDR-killer suite built on eight-plus BYOVD variants, paired with NETLOGON group policy abuse to encrypt every domain-joined system at once rather than machine by machine.

ANALYST OUTLOOK

The 90/10 split briefly made it the #1 ransomware group globally in June 2026, ahead of Qilin. The May 2026 backend leak is a real setback, but the group's fast scaling suggests it will rebuild quickly rather than fold.

NOTABLE INCIDENTS

UK software consultancy

April 2026

Stole data from a UK-based consultancy, then reused the same Fortinet VPN credentials to compromise one of that consultancy's clients in Turkey, a documented case of chain-victimization.

Soniva Dental Care

May 2026

Breached the practice's remote desktop web services infrastructure, potentially affecting up to 30,000 Texas residents.

Gator Cases, LLC

April 2026

Hit the US manufacturer, prompting data breach notification letters to nearly 1,200 affected individuals.