

Killing me gently: Inside Gentlemen's EDR killer framework

By Jakub Souček

Archived: 2026-09-23 02:01:43 UTC

ESET researchers analyzed the robust EDR-killing toolset of the ransomware-as-a-service gang Gentlemen. Since the beginning of 2026, Gentlemen has emerged as one of the most active gangs in the ransomware ecosystem. The group distinguishes itself through a mature, operator-maintained set of endpoint detection and response (EDR) killers, i.e., tools for disrupting security software. Additionally, unlike most top-tier gangs, Gentlemen does not exhibit a strong US-centric victimology, instead targeting victims across Southeast Asia, South America, and Western Europe.

While there have been multiple reports covering Gentlemen in recent months, they have not focused on a detailed analysis of the group's EDR killers. Thanks to ESET's continued incident-level visibility, we can however provide a uniquely deep view into Gentlemen's EDR-killer development practices. The internal data leak that Gentlemen suffered in May 2026 then gave us even more insight into the inner workings of the group.

The leak also allowed us to confirm our hypothesis from February 2026 that Gentlemen operators actively develop and maintain a portfolio of EDR killers that they offer to affiliates, centered around their in-house framework we have named GentleKiller. They also incorporate third-party or leaked tools such as HexKiller, ThrottleBlood, and HavocKiller. These tools are standardized through a shared defense-evasion layer, impersonating predominantly security vendors using fake version information, and copied legitimate certificates and icons. Gentlemen also demonstrates an ability to unusually quickly operationalize newly disclosed Bring Your Own Vulnerable Driver (BYOVD) proofs-of-concept, often within days of public release.

In this blogpost, we share our findings on Gentlemen's suite of EDR killers gained through extensive research and corroborated by the recent leak. We aim to provide actionable insights by connecting the EDR killer packages to actual samples, and tying the leaked data to tactics, techniques, and procedures (TTPs). Our findings highlight Gentlemen as one of the most technically agile ransomware-as-a-service (RaaS) gangs active in 2026.

Key points of the blogpost:

- Gentlemen operators develop and maintain an EDR-killer suite provided directly to affiliates.
- GentleKiller is an in-house framework with at least eight variants abusing different vulnerable or malicious drivers.
- Gentlemen operators apply a unified evasion strategy across tools that standardizes impersonation and protection.
- Third-party EDR killers (HexKiller, ThrottleBlood, and HavocKiller) are operationally integrated.
- Gentlemen can rapidly adapt newly released EDR killer proofs-of-concept (PoCs).
- The gang's victimology is globally distributed and notably not US-focused.

- Gentlemen also uses OxideHarvest, a credential stealer maintained by one of the group's affiliates.

Throughout this blogpost, we refer to RaaS **operators** and **affiliates**.

Operators are responsible for developing the ransomware payload, managing decryption keys, maintaining the dedicated leak site, often negotiating the ransom payment with victims, and offering other tooling and services for a monthly fee or a percentage from the ransom payment (typically 5–20%).

Affiliates rent ransomware services from operators, deploy encryptors to victims' networks, and are also responsible for data exfiltration.

Gentlemen profile

Gentlemen emerged in late 2025 as a RaaS operation and quickly grew into one of the most active ransomware gangs observed in Q1 2026. The gang offers a generous 90% share to affiliates. Group-IB [disclosed](#) that Gentlemen was founded by hastalamuerte, a disgruntled former Qilin affiliate. PRODAFT [tweeted](#) on October 17th, 2025 that Gentlemen operators were previously affiliates of Qilin, Embargo, LockBit, Medusa, and BlackLock. On June 10th, 2026 Brian Krebs [shared evidence](#) of hastalamuerte's true identity.

Gentlemen utilizes double extortion – in addition to encrypting the victim data, the group also threatens to leak it if the ransom is not paid. For encryption, the operators offer a variant written in Go targeting Windows, Linux, and other platforms, and an ESXi variant written in C.

One of the things that sets Gentlemen apart is the gang's willingness to offer more than just encryptors to affiliates – in particular, the gang also provides EDR killers. [Recent ESET research](#) has shown that, in most ransomware intrusions, the responsibility for finding a reliable EDR killer typically falls on individual affiliates, not the RaaS operators themselves. Only a small number of exceptions to this model have been documented. One notable case is [RansomHub](#), which invested in developing its own EDR killer from scratch, EDRKillShifter, and then offered it to affiliates through the affiliate panel.

Gentlemen represents a different, and so far underreported, approach. Rather than relying on affiliates to source their own EDR killers, Gentlemen operators actively develop and maintain a portfolio of EDR killers for affiliates. This portfolio combines an in-house developed tool, which we named GentleKiller, along with externally sourced or leaked tooling, standardized through a shared evasion layer and staged in a consistent manner.

ESET researchers hypothesized that GentleKiller was an internal tool back in February 2026, and this was later supported by reports from [Group-IB](#) and [Check Point](#) – both mention that the gang provides EDR-killing capabilities to its (verified) affiliates. The [recently leaked internal data](#) of the gang provided the final piece of evidence: in the leaks, zeta88 (another alias used by hastalamuerte), the leader of the gang, openly talks about maintaining and providing EDR-killer packages.

Apart from confirming our suspicion about GentleKiller, the leaked data also allowed us to link a credential stealer we named OxideHarvest to Gentlemen; specifically, to one of its affiliates.

Victimology

While the victimology of large RaaS operations is often shaped more by affiliates' choices than by operator-led strategy, one particular pattern still tends to emerge. Most major ransomware gangs show a strong and persistent focus on the United States, which frequently accounts for roughly half of all announced victims. This US-centric bias is evident across several prominent groups, including Qilin, DragonForce, and Akira, and has effectively become the norm among top-tier ransomware operations.

Gentlemen stands out as a notable exception to this trend. Despite ranking among the five most active ransomware gangs in Q1 2026, its victimology does not exhibit a comparable US focus. Instead, Gentlemen affiliates consistently target victims across a broad and geographically diverse range of countries, with a significant number of victims coming from regions such as Southeast Asia, South America, and Western Europe. Indeed, the gang's targeting includes some otherwise unusual countries like Thailand, Brazil, and France.

The recently leaked data provides evidence that when it comes to choosing victims, Gentlemen utilizes a centralized approach of sorting through viable candidates and then distributing them to affiliates. Victims are chosen primarily based on their FortiGate (mis)configuration rather than their geographical location.

EDR Killers

In February 2026, we saw a previously undocumented EDR killer deployed by a Gentlemen affiliate and staged in a directory named GentlemenCollection. We named this tool GentleKiller. At the time, we hypothesized that it was not an affiliate-specific artifact but rather a tool provided to affiliates by the Gentlemen operators. Since then, we have observed the same staging pattern (dropping GentleKiller and other EDR killers to the GentlemenCollection directory) multiple times across unrelated intrusions that we investigated, consistently involving Gentlemen affiliates. In parallel, two independently published reports by [Group-IB](#) and [Check Point](#) assessed that the Gentlemen operators explicitly offer EDR-disabling capabilities as part of their RaaS program.

Taken together, these observations allowed us to conclude that GentleKiller is a component of an EDR-killer suite maintained by the Gentlemen operators. This was later confirmed in the group's leaked data.

Besides GentleKiller, the suite also contains HexKiller, HavocKiller, and ThrottleBlood; all ESET names for EDR killers used by affiliates of rival gangs too and obtained by Gentlemen via unknown means. We also saw DemoKiller in several intrusions, but this EDR killer did not exhibit any ties to Gentlemen and therefore we exclude it from the gang's suite and instead consider it affiliate-specific. The following part of the blogpost covers these tools in more detail and places them into the broader EDR-killer ecosystem. While these tools are operationally integrated into Gentlemen intrusions, we assess with high confidence that only GentleKiller is developed in-house by the Gentlemen operators, whereas the remaining EDR killers were likely sourced externally and subsequently modified and standardized to fit the operators' toolset. Our assessment is based on:

- GentleKiller appearing mainly in Gentlemen-related intrusions, often deployed to the GentlemenCollection directory,
- continuous development with clear access to the source code that allows creating new variants and supporting newly emerged PoCs, and
- third-party reporting mentioning Gentlemen offering EDR-killing capabilities to trusted affiliates.

Defense evasion strategy

Gentlemen operators apply a specific set of defense evasion techniques to the gang's various EDR killers. These techniques are applied to compiled samples rather than source code. This gives Gentlemen the option to protect even the EDR killers whose source code the gang does not possess.

All the EDR killers that are part of Gentlemen's portfolio follow these defense-evasion patterns, which points to a standardized strategy, namely:

- Advanced binary protection (Enigma or Themida) is applied to a significant portion of the samples we detected. The filename suffix often identifies the method used (Enigma, Themida, or none).
- Filenames are chosen to closely resemble those of well-known software vendors, particularly companies operating in the cybersecurity domain.
- Executables impersonate the vendors by having the following attributes, all matching the same vendor or product:
 - fabricated version information,
 - invalid digital signatures copied from legitimate executables, and
 - icons matching those of the impersonated vendors.

Although a small number of samples deviate from this approach, likely due to inconsistent development practices, the vast majority of observed EDR killers adhere to this pattern. In Table 1, we show how the suffixes work. Later in the blogpost, we explain how the suffixes are appended to filenames.

Table 1. Naming pattern of the EDR killers maintained by Gentlemen

Suffix	Protection	Fake signature	Fake version information
1	Enigma	Yes	Yes
2	Themida	Yes	Yes
Light	None	Yes	Yes
Clear	None	No	No

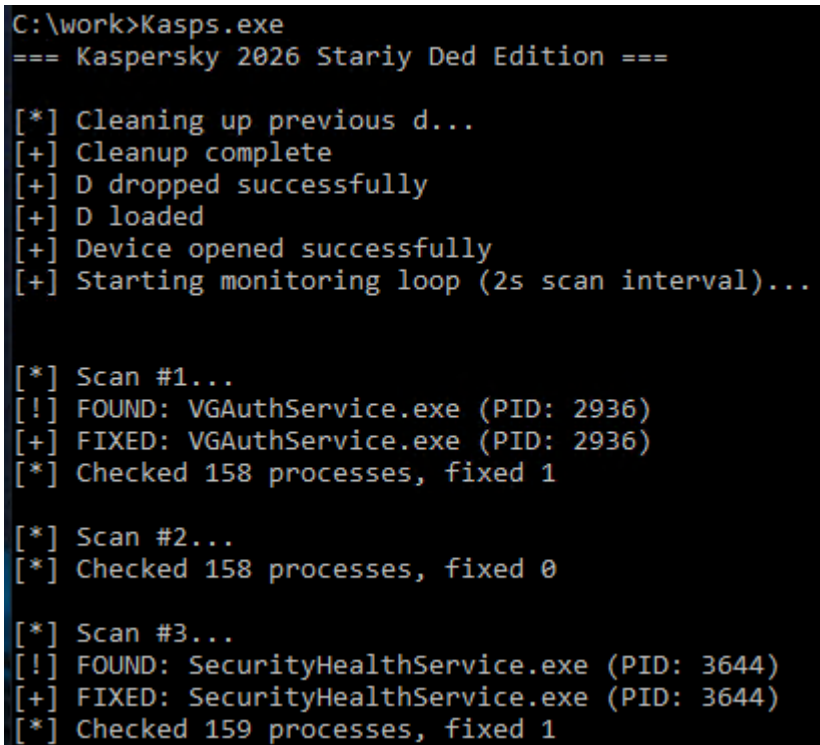
GentleKiller

GentleKiller is by far the most prevalent EDR killer observed in the Gentlemen ecosystem. At the time of writing, we are aware of at least eight distinct variants, each impersonating a different legitimate product and abusing a different vulnerable or malicious driver. Despite these surface-level differences, we classify all of these samples under the GentleKiller umbrella due to a high degree of shared internal characteristics.

When abstracting away the impersonation layer and the specific drivers used, the underlying code reveals numerous structural and behavioral commonalities that strongly suggest the use of a shared development template. This template is reused across variants, with only minimal modifications. The defining characteristics of the template include:

- consistent strings across variants,
- terminating processes periodically in a loop,
- targeting a broad set of security solutions, and
- employing identical code obfuscation.

An example of GentleKiller's output is illustrated in Figure 1, and a code snippet showing the code obfuscation is depicted in Figure 2.



```
C:\work>Kasps.exe
=== Kaspersky 2026 Stariy Ded Edition ===

[*] Cleaning up previous d...
[+] Cleanup complete
[+] D dropped successfully
[+] D loaded
[+] Device opened successfully
[+] Starting monitoring loop (2s scan interval)...

[*] Scan #1...
[!] FOUND: VGAuthService.exe (PID: 2936)
[+] FIXED: VGAuthService.exe (PID: 2936)
[*] Checked 158 processes, fixed 1

[*] Scan #2...
[*] Checked 158 processes, fixed 0

[*] Scan #3...
[!] FOUND: SecurityHealthService.exe (PID: 3644)
[+] FIXED: SecurityHealthService.exe (PID: 3644)
[*] Checked 159 processes, fixed 1
```

Figure 1. Output window spawned by GentleKiller

```

.text:000000000411B10      lea     rcx, aKaspersky20265 ; "=== Kaspersky 2026 Stariy Ded Edition ="...
.text:000000000411B17      call   _text_80
.text:000000000411B1C      movzx  edx, cs:_ZL2_9
.text:000000000411B23      call   _ZL3_7v ; __7(void)
.text:000000000411B28      movsx  ebx, al
.text:000000000411B2B      call   _ZL3_2v ; __2(void)
.text:000000000411B30      movsx  ecx, al
.text:000000000411B33      call   _ZL3_0v ; __0(void)
.text:000000000411B38      movsx  r9d, cs:_ZL2_8
.text:000000000411B40      movsx  eax, al
.text:000000000411B43      mov     edi, ecx
.text:000000000411B45      movsx  r10d, cs:_ZL2_1
.text:000000000411B4D      imul   edi, eax
.text:000000000411B50      lea     esi, ds:0[rdi*4]
.text:000000000411B57      mov     [rsp+518h+var_4C4], edi
.text:000000000411B5B      mov     [rsp+518h+var_498], esi
.text:000000000411B62      xor     rax, rax
.text:000000000411B65      jz      short near ptr loc_411B67+1
.text:000000000411B67      loc_411B67: ; CODE XREF: main+E5↑j
.text:000000000411B67      add     [rdi], cl
.text:000000000411B69      mov     esi, 66D231C2h
.text:000000000411B6E      pxor    mm0, mm0
.text:000000000411B71      pxor    xmm2, xmm2
.text:000000000411B75      add     eax, ebx
.text:000000000411B77      movzx   r8d, cs:_ZL2_7
.text:000000000411B7F      pxor    xmm1, xmm1
.text:000000000411B83      movzx   ecx, cs:_ZL2_3
.text:000000000411B8A      lea     r13d, [rdi+rdi*2]
.text:000000000411B8E      add     eax, esi
.text:000000000411B90      div     r9d
.text:000000000411B93      xor     edx, edx
.text:000000000411B95      sub     eax, r10d
.text:000000000411B98      cvtsi2sd xmm0, rax
.text:000000000411B9D      movsx   eax, r8b
.text:000000000411BA1      cvtsi2sd xmm2, eax
.text:000000000411BA5      movsx   eax, cl

```

Figure 2. Code obfuscation implemented by GentleKiller

This design prioritizes ease of deployment and operational flexibility for affiliates, while minimizing development effort for the operators. It allows the Gentlemen operators to integrate abused drivers into their toolset very soon after an EDR killer PoC is disclosed. This was the case with [UnknownKiller](#) and [PoisonKiller](#), which were adopted within a matter of days.

While some builds don't target all the processes known to GentleKiller, the general set, provided in Table 2, is consistent. We leveraged AI to map the process names to their corresponding vendors, and acknowledge that there might be minor inconsistencies. Overall, GentleKiller targets more than 400 processes that the AI mapped to 48 products.

Table 2. A complete list of process names targeted by GentleKiller, mapped to their corresponding vendors

Vendor	Targeted processes
Acronis	acronis_agent.exe, BackupAndRecoveryAgent.exe, managementagenthost.exe, mms.exe
AlienVault	alienvault-agent.exe, osqueryd.exe
Avast	afwServ.exe, aswEngSrv.exe, aswidsagent.exe, aswToolsSvc.exe, AvastSvc.exe, AvastUI.exe, avastsvc.exe, avastui.exe, bccavsvc.exe, wsc_proxy.exe
AVG	AVGUI.exe, AVGSvc.exe, avgnt.exe, avgsvca.exe, avgToolsSvc.exe
Binary Defense	BinaryDefenseAgent.exe

Vendor	Targeted processes
Bitdefender	Arrakis3.exe, BDAvScanner.exe, BDFsTray.exe, BDFileServer.exe, BDLived2.exe, BDLogger.exe, BDScheduler.exe, BDStatistics.exe, bdagent.exe, bdemsrv.exe, bdntwrk.exe, bdredline.exe, bdregsvr2.exe, bdservicehost.exe
Blumira	BlumiraAgent.exe
Bromium	BromiumDaemon.exe, BrDifxapi.exe
Carbon Black	cb.exe, cbcomms.exe, cbdefense.exe, carbonsensor.exe, RepMgr.exe
Cisco Talos	cfrutil.exe, CiscoAMPCEFWDriver.exe, cisco_amp_connector.exe, immunet.exe
CrowdStrike	ARWSRVC.EXE, ARCUpdate.exe, CSFalconContainer.exe, CSFalconService.exe, CSFalconUI.exe, csfalcondataprotect.exe, csfalcondaterepair.exe, REPRVC.EXE
Cynet	CynetEPS.exe, CynetMS.exe, CynetSvc.exe
Cybereason	ActiveConsole.exe, cybereason.exe, CybereasonActiveProbe.exe, CybereasonCR.exe
Cyvera	CyveraConsole.exe, CyveraService.exe, CyvrAgentSvc.exe, CyvrFsFlt.exe, cyvrfsflt.exe
Cylance/BlackBerry	CylanceSvc.exe
Darktrace	DarktraceTSA.exe
Deep Instinct	DeepInstinct.exe, DeepInstinctService.exe, DIAgentService.exe
Elastic	a2guard.exe, a2service.exe
ESET	eamonm.exe, eamsi.exe, ecl.exe, efwd.exe, egui.exe, eguiProxy.exe, ekrm.exe, ekrmEpfw.exe, ERAAgent.exe, EraAgentSvc.exe
Fortinet	firesvc.exe, firetray.exe, FortiTray.exe, fortiedr.exe, fw.exe
G DATA	GDDServer.exe, QHPISVR.EXE, QUHLPSVC.EXE, SAPISSVC.EXE
Heimdall	HeimdalsecurityAgent.exe
Huntress	HuntressAgent.exe, HuntressRMM.exe
Kaspersky	avp.exe, avpsus.exe, avpui.exe, kavfs.exe, kavfsscs.exe, kavfswd.exe, kavfswp.exe, kavtray.exe, klactprx.exe, klcsldcl.exe, klcsweb.exe, klnagent.exe, klnagchk.exe, klscctl.exe, klserver.exe, klwtblfs.exe, kpf4ss.exe, ksde.exe, ksdeui.exe, vapm.exe
LogRhythm	LogProcessorService.exe

Vendor	Targeted processes
McAfee/Trellix	AGMService.exe, AGSService.exe, masvc.exe, macmnsvc.exe, McAfeeAgent.exe, mcshield.exe, mfeann.exe, mfevtps.exe, mftfp.exe, mfeepghost.exe, mfevfire.exe, mfemactl.exe, mfemacsvc.exe, mfemgr.exe, mfemms.exe, MgntSvc.exe, ModuleCoreService.exe, tepfsvc.exe
Microsoft Defender	MSASCui.exe, MSASCuiL.exe, MpDefenderCoreService.exe, MsMpEng.exe, MsMpSvc.exe, MsSense.exe, msascuil.exe, msseces.exe, NisSrv.exe, nissrv.exe, SecurityHealthService.exe, SecurityHealthSystray.exe, SenseCncProxy.exe, SenseIR.exe, SenseNdr.exe, SenseSampleUploader.exe, smartscreen.exe, windefend.exe
Morphisec	MorphisecService.exe
Norton/Symantec	ccApp.exe, ccSvcHst.exe, ccsvchst.exe, ns.exe, nsservice.exe, nortonsecurity.exe, rtvscan.exe, SepMasterService.exe, sepWscSvc64.exe, smc.exe, SmcGui.exe, snac.exe, SymCorpUI.exe, SymWSC.exe
OSSEC/Wazuh	ossec-agent.exe, wazuh-agent.exe
Palo Alto Networks (Traps/Cortex)	cortexService.exe, trapsagent.exe, trapsd.exe, Traps.exe
Panda Security	panda_url_filtering.exe, pavfnsrv.exe, pavsrv.exe, psanhost.exe, PSANHost.EXE, pselamsvc.EXE, PSUAMain.EXE, PSUAService.EXE, pangps.exe
Qualys	qualys-cloud-agent.exe, QualysAgent.exe
Rapid7	ir_agent.exe, rapid7_endpoint.exe
Red Canary	RedCanaryAgent.exe
Sangfor	CSAAgent.exe, CSAService.exe, SangforAgent.exe, SangforCSA.exe, SangforEDR.exe, SangforInterface.exe, SangforMonitor.exe, SangforProtect.exe, SangforService.exe, SangforTray.exe, SangforUD.exe
SentinelOne	Sentinel.exe, SentinelAgent.exe, SentinelAgentWorker.exe, SentinelCtl.exe, SentinelHelperService.exe, SentinelMemoryScanner.exe, SentinelPowerShellExtension.exe, SentinelRanger.exe, SentinelServiceHost.exe, SentinelStaticEngine.exe, SentinelStaticEngineScanner.exe, SentinelUI.exe
SonicWall	SonicWallClientProtectionService.exe, swc_service.exe
Sophos	hmpalert.exe, McsAgent.exe, McsClient.exe, SavApi.exe, SAVAdminService.exe, SAVService.exe, SEDService.exe, SophosADSyncService.exe, SophosClean.exe, SophosCleanM64.exe, SophosFIMService.exe, SophosFS.exe, SophosHealth.exe, SophosLiveQueryService.exe, SophosMTR.exe, SophosMTRExtension.exe,

Vendor	Targeted processes
	SophosNetFilter.exe, SophosNtpService.exe, SophosOsquery.exe, SophosOsqueryExtension.exe, Sophos.PolicyEvaluation.Service.exe, SophosSafestore64.exe, SophosUI.exe, SophosUpdateMgr.exe, sophosav.exe, sophossps.exe, SSPService.exe
Tanium	TaniumClient.exe, TaniumCX.exe, tanclient.exe
ThreatLocker	ThreatLockerConsent.exe, threatlockerservice.exe, threatlockertray.exe
TrendAI	coreFrameworkHost.exe, coreServiceShell.exe, NTRTScan.exe, ntrtscan.exe, Ntrtscan.exe, OfcService.exe, ofcDdaSvr.exe, PccNTMon.exe, PccNt.exe, TISafe.exe, TISafeSvc.exe, TmCCSF.exe, tmicAgentSetting.exe, TMBMSRV.exe, Tmbmsrv.exe, tm_netsrv.exe, TmListen.exe, tmntsrv.exe, TmPfw.exe, tmproxy.exe, TmProxy.exe, TmPreFilter.exe, TmSSClient.exe, TmsaInstance64.exe, TmWscSvc.exe, VOneAgentConsole.exe, VOneAgentConsoleTray.exe
Uptycs	VectorAgent.exe, UptycsAgent.exe
Varonis	DatAdvantage.exe, VaronisAgent.exe
WatchGuard	wlcsservice.exe
Webroot	WRSa.exe, WRSkyClient.exe, WRSVC.exe, wrsa.exe
Windows Sysinternals	Sysmon.exe, Sysmon64.exe
Zscaler	zlclient.exe

GentleKiller variants

Each GentleKiller variant impersonates a different product and abuses a different malicious or vulnerable driver. Table 3 provides a list of the eight GentleKiller variants we have observed so far. The <suffix> refers to the naming pattern explained in Table 1. Drivers' filenames refer to how GentleKiller drops them to disk.

Table 3. List of GentleKiller variants

Variant name	Filenames	Abused driver
Kaspersky	Kasp<suffix>.exe	eb.sys, a rootkit (PoC)
FACEIT Anti-Cheat	FaceIT<suffix>.exe	nseckrnl.sys, NSecsoft NSecKrnL driver (PoC)
Valorant	Valorant<suffix>.exe	GameDriverX64.sys, an anti-cheat driver (PoC)

Variant name	Filenames	Abused driver
Javelin	EAAntiCheat<suffix>.exe EASolo<suffix>.exe	stpm_(old new).sys, two vulnerable ProcessMonitor Driver samples by Safetica (PoC)
WatchDog	BitD<suffix>.exe	dmx.sys, Zemana's WatchDog Antimalware Driver (PoC)
Network Blocker	MB<suffix>.exe	360netmon_wfp.sys, a vulnerable driver by Qihoo 360 Technology (PoC)
Cleaner	Deletor.exe	IMFForceDelete, IObit's IMF ForceDelete filter driver (PoC); the driver is dropped without the trailing .sys extension
G11	G11<suffix>.exe Symantec<suffix>.exe	PoisonX, a rootkit (PoC)

Third-party EDR killers

Apart from the internally developed GentleKiller, Gentlemen has incorporated multiple third-party solutions into its suite, summarized in Table 4 and described in the following sections. The <suffix> refers to the naming pattern explained in Table 1. Driver filenames refer to how the associated EDR killers drop them to disk.

Table 4. List of third-party EDR killers offered by Gentlemen

ESET name for the EDR killer	Filenames	Abused driver
HexKiller	Avast<suffix>.exe	googleApiUtil64.sys, Baidu Antivirus BdApi driver
ThrottleBlood	Sent<suffix>.exe	ThrottleBlood.sys, driver by TechPowerUp LLC
HavocKiller	HwAudKiller.exe Sophos<suffix>.exe	havoc.sys, Huawei Audio driver

HexKiller

HexKiller is an EDR killer that we previously assessed as being exclusive to the Warlock gang. Therefore, its appearance within Gentlemen intrusions is unexpected and noteworthy.

We found HexKiller staged alongside GentleKiller binaries within the GentlemenCollection directory. Nevertheless, its presence in Gentlemen intrusions does not, by itself, imply direct collaboration or operational overlap between the Gentlemen and Warlock gangs. It is plausible that Gentlemen operators obtained HexKiller through indirect means, such as private exchanges, secondary distribution channels, or sample leaks, without any

need for direct interaction with Warlock. We therefore don't consider this to be evidence of a deeper relationship between the two groups.

ThrottleBlood

This EDR killer has been repeatedly observed in intrusions carried out by MedusaLocker affiliates, and, less frequently, by DragonForce affiliates. Additionally, it was [linked](#) to Gentlemen by Trend Micro in September 2025.

At present, we do not have sufficient evidence to conclusively determine the origin of ThrottleBlood. In our telemetry, it appears prominently deployed across multiple MedusaLocker intrusions and sporadically in DragonForce-related activity. These incidents show little operational overlap beyond the use of ThrottleBlood itself. One possible explanation is that ThrottleBlood is commercially distributed on underground markets, or alternatively a tool developed by MedusaLocker operators and shared with their affiliates, some of whom may also have ties to DragonForce.

Neither hypothesis, however, fully explains how a ThrottleBlood sample appeared in Gentlemen's possession. As a result, we cannot rule out the possibility of Gentlemen acquiring the tool through it leaking beyond the originally intended context. What we state with high confidence, however, is that Gentlemen did not develop this EDR killer in-house.

HavocKiller

HavocKiller is the final addition to Gentlemen's EDR-killer arsenal. While the tool was publicly [disclosed](#) by Huntress on March 19th, 2026, ESET telemetry confirms its use in real-world intrusions dating back to at least January 23rd, 2026, indicating that it had been operational for weeks prior to public reporting. We can also corroborate Huntress's assessment regarding its purpose: in all cases observed by ESET, the deployment of HavocKiller was part of ransomware-related activity.

Based on its technical characteristics, we assess that HavocKiller is not developed by the Gentlemen operators themselves, but instead was obtained through external means. Although the samples were staged within the GentlemenCollection directory and Gentlemen's standard set of defense evasion techniques was applied to them, the underlying implementation differs substantially from GentleKiller. This strongly suggests that HavocKiller represents a third-party EDR killer that was adapted operationally, but its architecture does not fit into Gentlemen's framework.

OxideHarvest

We also detected several deployments of a tool we named OxideHarvest, a credential stealer written in Rust. Since Rust is not the programming language of choice for Gentlemen, we do not attribute the tool to the group. However, as Check Point [noted](#), a Gentlemen affiliate named quant maintains a tool referred to as buildx641, whose naming and functionality immediately reminded us of OxideHarvest. Indeed, after further investigation, we found an OxideHarvest sample named buildx641.exe [uploaded to VirusTotal](#); we conclude that buildx641 and OxideHarvest are the same tool.

OxideHarvest comes wrapped inside different packers, often mimicking legitimate software in version information and icon (similar, but not identical, to what Gentlemen does with GentleKiller). The protected payload is a simple, straightforward credential stealer. To function, OxideHarvest requires the user to specify the list of hosts (-i), username (-u), password (-p), number of threads (-t), and an output file (-o) as command line options. The tool then uses the supplied credentials to log into the specified hosts (passed as a newline-delimited text file), employs multithreading, and exfiltrates credentials into the supplied output file. Figure 9 shows the result of the --help command of OxideHarvest, and Table 5 shows its configuration dictating which credentials are targeted.

```
build.exe --help
Usage: build.exe [OPTIONS] --ip-list <IP_LIST> --threads <THREADS> --output <OUTPUT>

Options:
-i, --ip-list <IP_LIST>
-u, --username <USERNAME>
-p, --password <PASSWORD>
-t, --threads <THREADS>
-o, --output <OUTPUT>
-h, --help                Print help
```

Figure 3. The help of OxideHarvest

Table 5. Embedded configuration of OxideHarvest

```
{
  "chromium_browsers": [
    [
      "Google Chrome",
      "\\Google\\Chrome\\User Data",
      true
    ],
    [
      "Google Chrome Beta",
      "\\Google\\Chrome Beta\\User Data",
      true
    ],
    [
      "ChromeBeta",
      "\\Google\\Chrome SxS\\User Data",
      true
    ],
    [
      "Chromium",
      "\\Chromium\\User Data",
      true
    ],
    [
      "Microsoft Edge",
      "\\Microsoft\\Edge\\User Data",
      true
    ],
  ],
}
```

```
[
  "Torch",
  "\\Torch\\User Data",
  true
],
[
  "Comodo",
  "\\Comodo\\Dragon\\User Data",
  true
],
[
  "Nichrome",
  "\\Nichrome\\User Data",
  true
],
[
  "Maxthon5",
  "\\Maxthon5\\Users",
  true
],
[
  "Epic Privacy Browser",
  "\\Epic Privacy Browser\\User Data",
  true
],
[
  "Vivaldi",
  "\\Vivaldi\\User Data",
  true
],
[
  "QIP",
  "\\QIP Surf\\User Data",
  true
],
[
  "Cent",
  "\\CentBrowser\\User Data",
  true
],
[
  "Elements",
  "\\Elements Browser\\User Data",
  true
],
[
  "TorBro",
```

```
        "\\TorBro\\Profile",
        true
    ],
    [
        "CryptoTab",
        "\\CryptoTab Browser\\User Data",
        true
    ],
    [
        "Brave",
        "\\BraveSoftware\\Brave-Browser\\User Data",
        true
    ],
    [
        "Opera",
        "\\Opera Software\\Opera Stable\\",
        false
    ],
    [
        "OperaGX",
        "\\Opera Software\\Opera GX Stable\\",
        false
    ],
    [
        "Opera Neon",
        "\\Opera Software\\Opera Neon\\User Data",
        false
    ]
],
"gecko_browsers": [
    [
        "Mozilla Firefox",
        "\\Mozilla\\Firefox\\Profiles\\",
        false
    ],
    [
        "Slim",
        "\\FlashPeak\\SlimBrowser\\Profiles\\",
        false
    ],
    [
        "PaleMoon",
        "\\Moonchild Productions\\Pale Moon\\Profiles\\",
        false
    ],
    [
        "Waterfox",
```

```
        "\\Waterfox\\Profiles\\",
        false
    ],
    [
        "Cyberfox",
        "\\8pecxstudios\\Cyberfox\\Profiles\\",
        false
    ],
    [
        "BlackHawk",
        "\\NETGATE Technologies\\BlackHawk\\Profiles\\",
        false
    ],
    [
        "IceCat",
        "\\Mozilla\\icecat\\Profiles\\",
        false
    ],
    [
        "KMeleon",
        "\\K-Meleon\\",
        false
    ]
]
}
```

Conclusion

Gentlemen demonstrates an interesting approach: operator-managed EDR killers, ready to use by affiliates. While most ransomware gangs continue to delegate EDR killing to affiliates, Gentlemen has chosen to centralize this function by offering affiliates a ready-to-use, standardized EDR-killer suite. This decision makes Gentlemen an attractive operator for affiliates as it materially lowers the entry barrier for them, making their job consequently easier.

This model differs even from the few known exceptions in the ecosystem. In the case of RansomHub, the operators invested in a single EDR killer, EDRKillShifter, developed entirely in-house. Gentlemen, by contrast, maintains a diverse portfolio of EDR killers, blending original development (GentleKiller) with rapidly adapted third-party or publicly disclosed tooling (HexKiller, ThrottleBlood, and HavocKiller). The consistent application of defense evasion techniques across these tools further obscures and complicates straightforward attribution when samples are observed in isolation.

Because EDR-killer techniques continue to commoditize and circulate across underground communities, this blogpost underscores the necessity of incident-level investigation and analysis. Without such context, Gentlemen's EDR killers are likely to be misattributed, or not attributed at all, masking the true extent of this operator's involvement. Thanks to our continuous insight into Gentlemen intrusions, we were able to provide protection

against the group's attacks months before the recently leaked data confirmed our high-confidence hypotheses on the gang's EDR-killer suite.

The GentleKiller framework illustrates a deliberate balance between in-house development and pragmatic reuse of external research. While some components show signs of rushed implementation or inconsistent polish, the overall toolset demonstrates high operational effectiveness and tight integration into Gentlemen's ransomware workflow. The group's ability to adapt newly published BYOVD PoCs within days further underscores its agility.

From a defense perspective, understanding how GentleKiller works allows defenders to better design their defensive strategies and defend even against yet-to-be-developed, new additions to Gentlemen's EDR-killing arsenal.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

IoCs

Files

SHA-1	Filename	Detection	Description
8AE6BD18B129061F6364 2531F1B684CF0383C75D	Kasps.exe	Win64/KillAV.EA	GentleKiller (Kaspersky variant).
BA914FE77B177B457994 03B16DD14765C510A074	eb.sys	Win64/Agent.ITG	A custom rootkit used by the Kaspersky variant of GentleKiller.
D605994FC72A2BB59B5C FB1624A1B9170ECA73A2	FaceIT1.exe	Win64/KillAV.EA	GentleKiller (FACEIT Anti-Cheat variant, Enigma-protected).
B0B912A3FD1C05D72080 848EC4C92880004021A1	nseckrnl.sys	Win64/VulnDriver .NSecsoft.A	NSecsoft NSecKrl driver abused by the FACEIT Anti-Cheat variant of GentleKiller.
5AA3124E5C4921E5EDFC 60133B5D71DA21B07DA3	Valorant2.exe	Win64/KillAV.EA	GentleKiller (Valorant variant, Themida-protected).

SHA-1	Filename	Detection	Description
7556AE58C215B8245A43 F764F0676C7A8F0FDD1A	vgk.sys	Win64/VulnDriver .PerfectWorld.A	Tower of Fantasy AntiCheat driver abused by the Valorant variant of GentleKiller.
331879F5EEC8892BBD89 6F90BDBB1BAD0BF63BD6	EASolo2Light.exe	Win64/KillAV.EA	GentleKiller (Javelin variant abusing Safetica's newer driver).
F11AEBCCB9A86A7E2E65 3F90BAEC697F233C255F	EASOLO1clear.exe	Win64/KillAV.EA	GentleKiller (Javelin variant abusing Safetica's older driver).
EF9CD06683159397F099 CAA244E94E6EAD96EBA	EAAntiCheatLight .exe	Win64/KillAV.EA	GentleKiller (Javelin variant abusing both drivers).
711EF221526997039E80 4A18DB9647C91680BBE2	stpm_old.sys	Win64/VulnDrive r.Safetica.A	Safetica's Process Monitor Driver (older) abused by the Javelin variant of GentleKiller.
68FEC379F2AE76C3D2CE 913F7BE650CEA1D06990	stpm_new.sys	Win64/VulnDrive r.Safetica.H	Safetica's Process Monitor Driver (newer) abused by the Javelin variant of GentleKiller.
A11EE9CDC59E5CAA59AE FD27B30D104F3AD68E62	BitD1.exe	Win64/KillAV.EA	GentleKiller (WatchDog variant, Themida-protected).
96F0DBF52AED0AFD43E4 4500116B04B674F7358E	dmx.sys	Win64/VulnDrive r.WatchDogDev.C	Zemana's WatchDog Antimalware Driver abused by the WatchDog variant of GentleKiller.

SHA-1	Filename	Detection	Description
2F86898528C6CAB3540C 486A9BFAA0C029B73950	MB2.exe	Win64/KillAV.EA	GentleKiller (Network Blocker variant, Themida-protected).
9AD51AD97C01E97AB592 14116740785E0F6320A8	360netmon_wfp.sys	Win64/VulnDriver.Qihoo360.A	360netmon.sys driver abused by the Network Blocker variant of GentleKiller.
A19117175DBC9BA4D23B 5DCE8415E299A2E32192	Deletor.exe	Win64/KillAV.EA	GentleKiller (Cleaner variant).
12500F6C87CE62712A0E D6652C57468D15C14223	IMFForceDelete	Win64/VulnDriver.IObit.D.gen	IMF ForceDelete filter driver abused by the Cleaner variant of GentleKiller.
D29670E684E40DDC89B4 7010C37CBC96737035B6	Symantec.exe	Win64/KillAV.EA	GentleKiller (G11 variant).
56BEE9DF5833A637F5C5 4D5911DF98B0812FE643	G11.sys	Win64/Agent.IYQ	PoisonX rootkit used by the G11 variant of GentleKiller.
CF4D74DF17A91B4A36A2 911B22AFEC5D8FA93A01	Avast.exe	Win32/KillAV.NVL	HexKiller incorporated into Gentlemen modus operandi by adding the evasion layer.
EC296F9501AD71E43081 0CB5CDC38D954D4BA536	googleApiUtil64.sys	Win64/VulnDriver.Baidu.B	Baidu Antivirus BdApi driver abused by HexKiller.
7131B377E96016DC1911 020C9F95B1B4D042D7B4	Sent.exe	Win64/KillAV.AT	ThrottleBlood incorporated into Gentlemen modus operandi by adding the evasion layer.

SHA-1	Filename	Detection	Description
82ED942A52CDCF120A89 19730E00BA37619661A3	ThrottleBlood.sys	Win64/VulnDriver.GPUZ.B	ThrottleStop.sys driver abused by ThrottleBlood.
F0537CBB773AE12100B3 6731E7C39F5A9D852B14	Sophos.exe	Win64/KillAV.DE	HavocKiller incorporated into Gentlemen modus operandi by adding the evasion layer.
1FA071303FB846308571 E64727501FB98B1C2BE6	havoc.sys	Win64/VulnDriver.Huawei.D	Vulnerable driver abused by HavocKiller.
A5CF917EC4A7DFBDFA43 621398604805D860C718	buildx641.exe	Win64/Spy.Agent.AGC	OxideHarvest.
D4B19141102015D43632 1E6F26976E98183CFD27	buildx64.exe	Win64/Spy.Agent.AGC	OxideHarvest.

MITRE ATT&CK techniques

This table was built using [version 19](#) of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	GentleKiller and related tools are console-based executables that run visibly and emit debug strings during execution.
	T1106	Native API	User-mode components interact directly with kernel drivers via DeviceIoControl and other native Windows APIs to perform privileged actions.
Persistence	T1543.003	Create or Modify System Process: Windows Service	The EDR killers install and start vulnerable or malicious drivers as services prior to exploitation.
Stealth	T1036	Masquerading	Gentlemen's EDR killers are protected by impersonating legitimate vendors through filenames, version information, icons, and copied digital certificates.

Tactic	ID	Name	Description
	T1036.001	Masquerading: Invalid Code Signature	The protection applied to Gentlemen's EDR killers adds an invalid code signature as part of the impersonation strategy.
	T1027	Obfuscated Files or Information	Some executables are protected with packers (e.g., Enigma, Themida) and custom control-flow obfuscation.
Defense Impairment	T1685	Disable or Modify Tools	GentleKiller and other EDR killers that Gentlemen is in possession of aim to bypass security products such as EDRs.



Source: <https://www.welivesecurity.com/en/eset-research/killing-me-gently-inside-gentlemens-edr-killer-framework/>