THREAT HUNTING

LAB

GentleKiller: Inside The Gentlemen RaaS EDR-Killer Framework and Its BYOVD Driver Arsenal

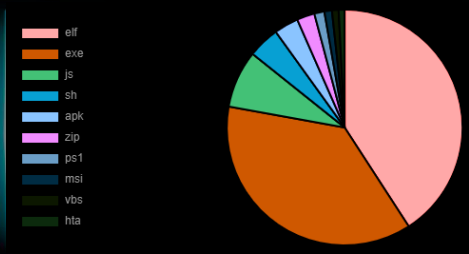
PUBLIC

Index

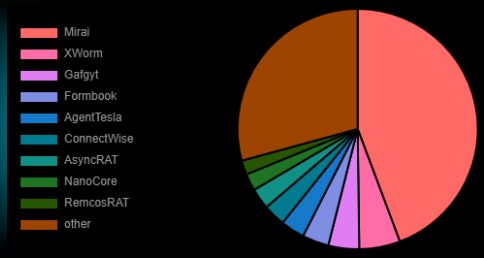
Global Weekly Threat Overview

Salesforce has revealed that it disabled the Klue Battlecards app integration within its platform in response to a security incident impacting the competitive intelligence company on June 11, 2026. Organizations will be unable to connect to Salesforce via the app until further notice. Salesforce took this action because the security teams recently detected unusual activity involving the app that may have resulted in unauthorized access to a subset of customer data via the app's connection to Salesforce. This issue is limited to Klue's app connection and does not arise from a vulnerability within the Salesforce platform.

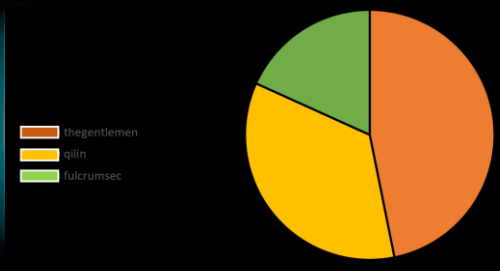
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Microsoft researchers have detailed an exploit chain, named AutoJack, that turns an AI browsing agent into a delivery vehicle for remote code execution. Steer the agent to load an attacker's web page, and that page's JavaScript can reach a privileged local service on the same machine and spawn a process on the host. The flaw sits in AutoGen Studio, the open-source prototyping interface for Microsoft Research's AutoGen multi-agent framework.

Global Weekly Notable One

Defense Evasion: Impair Defenses

The Gentlemen operation is a ransomware-as-a-service program that emerged in mid-2025 and rapidly positioned itself among the most active RaaS crews, with hundreds of published victims by early 2026. Instead of leaving defense evasion entirely to affiliates, operators provide a curated toolkit that couples a Go-based locker with a mature, operator-maintained suite of EDR killers, lowering the barrier for less technical partners.

Gentlemen affiliates deploy EDR killers shortly before encryption to systematically terminate security processes and services, often via Bring Your Own Vulnerable Driver (BYOVD) that grants kernel-level capabilities to kill protected EDR/AV components. These binaries are heavily packed, masquerade as legitimate security products, and install vulnerable or malicious drivers as services, combining user-mode orchestration with kernel-mode process termination.

Threat Hunting Activity

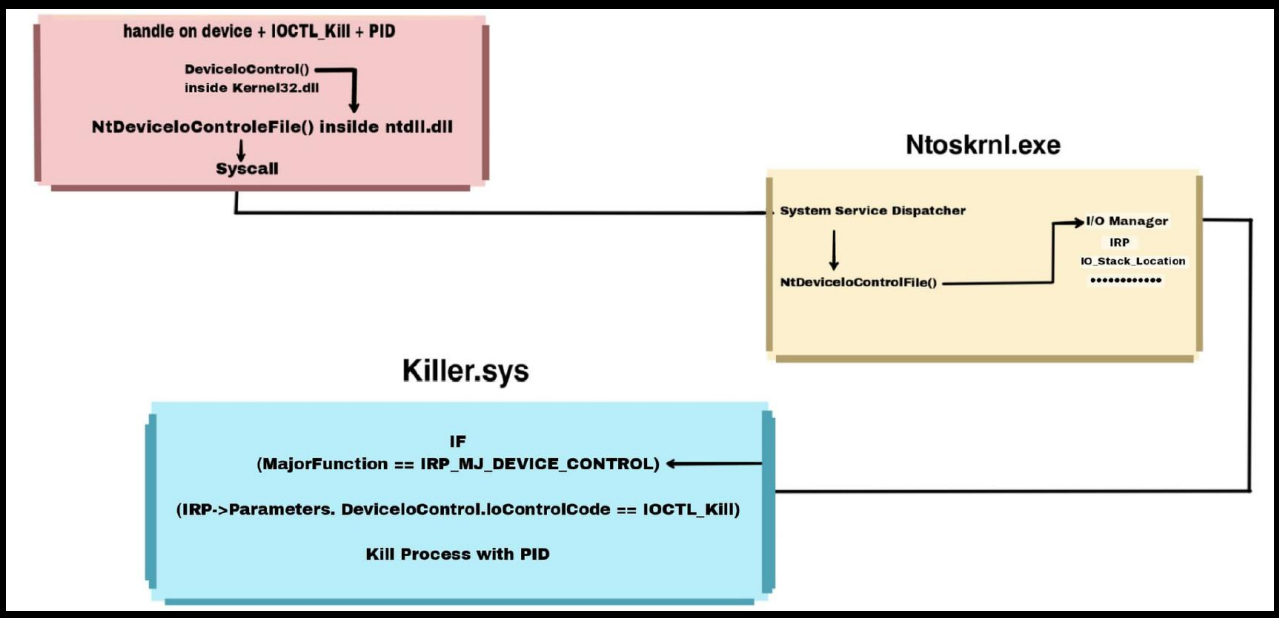
TACTIC Defense Evasion

TECHNIQUES T1629 – Impair Defenses

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may span both native defenses as well as supplemental capabilities installed by users or mobile endpoint administrators.

Threat Hunting Activity

The EDR killer framework dubbed GentleKiller is provided directly by operators to affiliates and staged in a dedicated “GentlemenCollection” directory during intrusions.
The same package integrates several external EDR killers (HexKiller, ThrottleBlood and HavocKiller) which are re-wrapped with Gentlemen’s protection, further diversifying the BYOVD surface defenders have to handle.



The diagram show how a process can abuse a vulnerable driver to kill arbitrary processes. The malicious process opens a handle to the device and sends a custom IOCTL_Kill with a target PID via DeviceIoControl/NtDeviceIoControlFile; the request is dispatched by ntoskrnl.exe’s I/O manager as an IRP to Killer.sys, which checks for IRP_MJ_DEVICE_CONTROL with that IOCTL code and then terminates the process identified by the PID.

Threat Hunting Activity

An example of execution is provided where the framework is working with Kaspersky solutions

```
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
```

Threat Hunting Activity

During analysis and research a list of vulnerable but not already-blocked drivers was disclosure. These drivers are used by GentleKiller to terminate EDR services. Hunting for those drivers can reveal first steps execution.

ActionType	AdditionalFields	File...	FileSize	FolderPath
FileCreated	{"FileType":"PortableExecutable"}	vgk.sys	53793336	C:\Users\[redacted]\AppData\Local\Temp\7zF1BEB108\vgk.sys
FileCreated	{"FileType":"Unknown"}	vgk.sys	53793336	C:\Program Files\Riot Vanguard\vgk.sys
FileCreated	{"FileType":"PortableExecutable"}	vgk.sys	53793336	C:\Program Files\Riot Vanguard\vgk.sys
FileCreated	{"FileType":"PortableExecutable"}	vgk.sys	53793336	C:\Users\[redacted]\AppData\Local\Temp\7zE200B020\vgk.sys
FileCreated	{"FileType":"Unknown"}	vgk.sys	53793336	C:\Program Files\Riot Vanguard\vgk.sys


CRITICAL PROCESS:
ACCESS CONTROL -
- OFFLINE (FAILED)
WARNING:
PROCESS REMOVAL
INITIATED
PROCESS:
ENCRYPTION PROTOCOL
- CORRUPTED
(0% INTEGRITY)
THREAT
HUNTING
SORINT.SEC

PUBLIC