K logix
Be confident.

MAY 2025 | THREAT INTEL NEWSLETTER

Killing the Frontline: The Rise of EDR Killers in Ransomware Attacks

C-Suite level threat review by applicable business area addressing active threats.

Endpoint Detection and Response (EDR) platforms are a frontline cybersecurity defense for many organizations. These tools monitor devices, flag suspicious behavior, and stop threats like malware before they spread. EDRs use behavioral analytics and system callbacks to track what is happening on a system in real time. However, as EDR capabilities have become more effective at stopping threats, threat actors have adapted. Attackers are now deploying specialized tools called EDR killers to disable these defenses early in an attack. These techniques align with the MITRE ATT&CK tactic of Impairing Defenses, specifically disabling security tools to pave the way for destructive attacks (MITRE T1562.001).

EDRKillShifter:

EDRKillShifter is one of the most effective EDR killers used today. It was first linked to the RansomHub group in 2024. Since then, other major ransomware operations like Medusa, Play, and BianLian have reused it. With multiple groups using the tool, it poses a cross-industry threat affecting various countries and sectors.

ABYSSWORKER:

ABYSSWORKER is an EDR killer linked to the Medusa ransomware group. Medusa operates as a Ransomware-as-a-Service (RaaS), targeting industries like healthcare, education, legal, and manufacturing. So far, in 2025, Medusa has claimed over 60 attacks. Medusa's use of multiple EDR killers highlights how critical these tools are to carrying out successful attacks.

EDRKillShifter

Threat Level: High

Attack:

EDRKillShifter starts with a Bring Your Own Vulnerable Device (BYOVD) attack, installing a legitimate Windows driver with a known vulnerability. These vulnerabilities often go unnoticed because they exist in signed and trusted software. To launch EDRKillShifter, the attacker must enter a specific 64-character password to unlock a hidden file and load the final stage of the attack directly into memory. Running in memory allows it to avoid leaving traces on a disk and makes it tougher for traditional antivirus tools to detect. Once active, EDRKillShifter disables the EDR and antivirus processes. It also removes callbacks, which are security tools that monitor system activity, such as file access and process creation. With security defenses out of the way, the attacker is free to execute ransomware or other harmful payloads without interference.

Remediation:

- Patch drivers and software to limit vulnerabilities that could be used during BYOVD attacks.
- Limit admin privileges across the organization to make it harder for attackers to gain elevated access if they gain access to the environment.
- Turn on tamper protections in EDR tools to block unauthorized changes.

ABYSSWORKER

Threat Level: Medium

Attack:

ABYSSWORKER uses a BYOVD approach, but instead of relying on a vulnerable third-party driver, it installs a custom-built driver called smuol.sys. This driver pretends to be a legitimate CrowdStrike Falcon driver and is signed with stolen certificates, allowing it to slip past security checks and gain high-level access. Once installed, ABYSSWORKER disables EDR security tools by killing processes, removing callbacks, and even rebooting the system if needed. It goes even further by actively protecting the ransomware during execution. The custom-made driver monitors what programs are launched and blocks any that try to interfere with its end goal. It also prevents other applications from accessing the ransomware by stripping away their permissions.

Remediation:

- Run simulated EDR killer attacks to test how your organizations defenses react.
- Monitor for revoked or stolen driver certificates with tools like Windows Defender Application Control. Check certificate issue and expiration dates to help identify outdated or suspicious certificates.
- Configure systems to only allow pre-approved drivers to run.

EDRKillShifter:

- **EDRKillShifter Capabilities and Details:** https://www.welivesecurity.com/en/eset-research/shifting-sands-ransomhub-edrkillshifter/
- **EDRKillShifter Shifting Gangs:** https://thehackernews.com/2025/03/hackers-repurpose-ransomhubs.html

ABYSSWORKER:

- **Technical dive into ABYSSWORKER:** https://www.elastic.co/security-labs/abyssworker
- **Medusa's work with ABYSSWORKER:** https://www.cybersecuritydive.com/news/medusa-ransomware-malicious-driver-edr-killer/743181/

How K logix Can Help

Technology Advisory

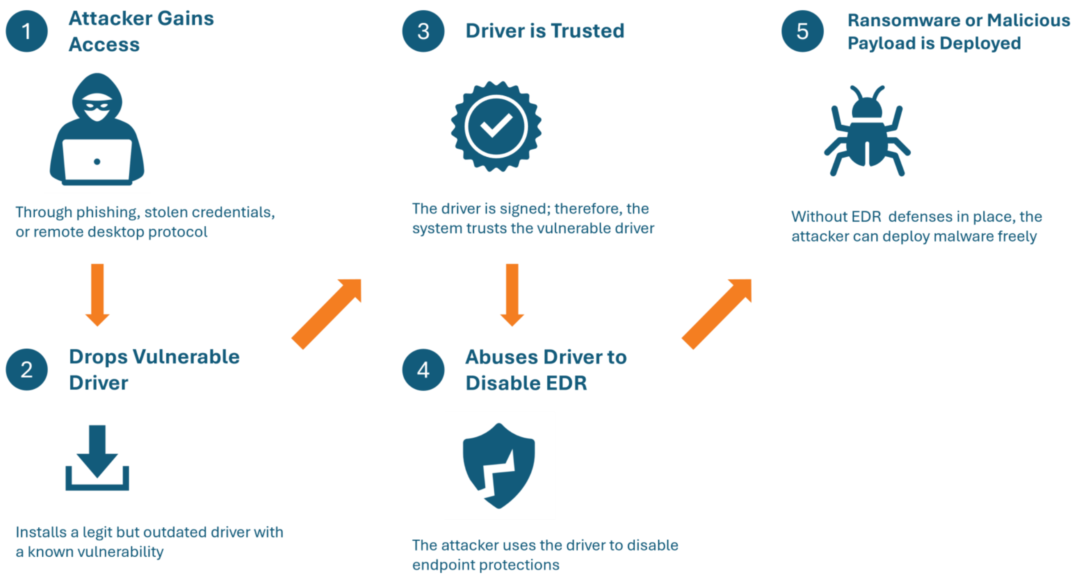
- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports



1 Attacker Gains Access

Through phishing, stolen credentials, or remote desktop protocol

2 Drops Vulnerable Driver

Installs a legit but outdated driver with a known vulnerability

3 Driver is Trusted

The driver is signed; therefore, the system trusts the vulnerable driver

4 Abuses Driver to Disable EDR

The attacker uses the driver to disable endpoint protections

5 Ransomware or Malicious Payload is Deployed

Without EDR defenses in place, the attacker can deploy malware freely

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.