Technical

EDR Bypass Technique Trend

Index

CISA Reveals How 12 Ransomware Gangs are Bypassing EDRs

Endpoint Detection and Response (EDR) has a critical role in most companies' security setup, but cybercriminals are mastering EDR bypass tactics. How can we defend against them?

One trend this year has changed the cybersecurity environment irreversibly: the growth in EDR bypass techniques and the range of methods that are evading traditional security systems.

The greatest impact comes from new abilities to bypass network perimeter defenses, endpoint protection, and email security. Cybercriminals have focused much of their efforts on bypassing Endpoint Detection and Response (EDR) solutions, given the critical role that most companies give to EDRs in their security frameworks.

Are organizations underestimating the severity of EDR evasion when creating their cybersecurity stack? Let's explore how ransomware gangs have mastered EDR bypass tactics in their attack chains and how we can defend against them.

#StopRansomware

The Cybersecurity and Infrastructure Security Agency (CISA) is the US agency responsible for cybersecurity and infrastructure protection against both private and nation-state attacks. One important role of CISA is keeping the cybersecurity community up-to-date on the latest intelligence on cybercrime attack methods.

Through their advisories, CISA provides valuable insights into well-known ransomware groups in the cybersecurity landscape, intending to help users prevent potential disruptions or damage to their systems. In particular, this report makes reference to intelligence from #StopRansomware, a CISA initiative that pulls together information on the most prevalent ransomware actors, and has highlighted several EDR evasion tactics that have come to the fore in recent months.

The Variety of EDR Bypass Methods & TTPs

Over the past year, CISA has released information on twelve ransomware gangs, bringing attention to their prevalence and impact in the world of cybersecurity.

CISA uses the MITRE ATT&CK Matrix to map the techniques, tactics, and procedures (TTPs) used by these gangs to evade defenses, particularly EDRs — most of which can be found in MITRE's Defense Evasion Tactic section.

It is important to be aware of how cyberattackers are bypassing traditional defenses so we can build a more cohesive defense strategy. Let's find out more about the twelve gangs and their principal EDR evasion techniques used to deliver ransomware.

RansomHub

RansomHub offers Ransomware as a Service (RaaS), allowing threat actors easy access to a range of ransomware tools.

RansomHub Ransomware gives affiliates the ability to clear system logs on both Windows and Linux to hinder potential incident response efforts [T1070]. They use Windows Management Instrumentation (WMI) [T1047] to disable antivirus software.

In some cases, RansomHub-specific tools were deployed to disable EDR systems [T1562.001], such as EDRKillShifter, using the Living off the Land (LotL) technique known as Bring Your Own Vulnerable Driver (BYOVD) where attackers implant a

legitimate driver, with in-built vulnerabilities, onto a targeted system. This driver can then be exploited because legitimately-signed drivers are trusted by the OS, allowing attackers to evade detection.

Blacksuit (Royal)

Blacksuit actors exploit a legitimate admin account [T1078] to log into the domain controller remotely using Server Message Block (SMB). SMB is a communication protocol used to share files, printers, serial ports, and miscellaneous communications between nodes on a network.

Once inside, they deactivate antivirus software [T1562.001] by modifying Group Policy Objects [T1484.001], a tool for managing and configuring applications, software operations, and user settings throughout an entire organization.

Additionally, Blacksuit used PowerTool64.exe and GMER to remove EDR software. GMER and PowerTool64 are primarily designed to remove rootkits, however, they can also be maliciously leveraged to uninstall applications at the kernel level.

Black Basta

Affiliates of Black Basta, who offer RaaS, have affected organizations and critical infrastructure across the world, particularly North America, Europe, and Australia. Affiliates use a Black Basta tool called Backstab to disable EDR systems [T1562.001]. Additionally, they have used PowerShell scripts to disable antivirus products, further enhancing their ability to evade detection and carry out attacks undetected [T1059].

Akira

Akira has struck organizations across North America, Europe and Australia. As threat actors Akira prepare for lateral movement, they often disable security software to evade detection.

Cybersecurity researchers have observed Akira actors weaponizing virtual machines [T1562] and using PowerTool to exploit the Zemana AntiMalware driver, terminating antivirus-related processes [T1562.001].

Phobos

This gang works on a RaaS model and CISA has recorded them as targeting county governments, emergency services, education, public healthcare, and other critical infrastructure.

Phobos ransomware modifies system firewall configurations using terminal commands through LotL techniques [T1562.004]. Additionally, Phobos actors evade EDR detection using tools such as Universal Virus Sniffer (UVS), Process Hacker, and PowerTool [T1562.001].

ALPHV Black

This threat actor is known to specifically target the healthcare sector. ALPHV has adopted customized EDR killers, specifically ibmModule.dll and 363.sys [T1562.001], and virtual machines for malware deployment, exemplifying the ongoing evolution of tactics designed to bypass and evade defensive measures.

Play

The Play Ransomware group has impacted businesses and critical infrastructure in North America, South America, and Europe.

This gang initially uses infostealers to gather network information [T1016] and scan for antivirus software [T1518.001]. They also deploy tools such as ProcessHacker, GMER, IOBit, and PowerTool to disable EDR software [T1562.001] and remove log files [T1070.001]. In certain cases, cybersecurity researchers have observed Play ransomware actors using PowerShell scripts to target and disable Microsoft Defender, specifically.

Rhysida

Rhysida Ransomware has been deployed against several sectors, including education, healthcare, manufacturing, information technology, and government.

The group uses valid stolen SSH, VPN, and RDP credentials to gain access to NAS devices and VMware hypervisors [T1078]. Once inside the system, attackers employ LotL techniques to execute a PowerShell script known as SilentKill to terminate antivirus-related processes and services, bypassing Endpoint Protection's real-time defense layer [T1562.001].

AvosLocker

Affiliates of AvosLocker's RaaS model use their ransomware to disable EDR software using the LotL technique of BYOVD. They exploit a legitimate Avast Anti-Rootkit driver file (asWarPot.sys) to disable EDR defense solutions [T1562.001]. After this, they use custom PowerShell scripts [T1059.001] and batch (.bat) scripts [T1059.003] for lateral movement and privilege escalation.

Snatch

Snatch threat actors have targeted a range of critical infrastructure sectors including defense, agriculture, and information technology.

The Snatch ransomware family reboots the system into Windows Safe Mode to bypass EDR tools [T1562.001], performing an executable file named "safe.exe" or a similar variation. The ransomware executable's name is typically a string of hexadecimal characters matching the SHA-256 hash of the file to evade rule-based detection [T1036]. Upon initiation, the Snatch ransomware payload:

- Queries and modifies registry keys [T1012][T1112]
- Uses various native Windows tools to enumerate the system [T1569.002]
- Finds processes [T1057] and creates benign processes to execute Windows batch files

LockBit 3.0

The LockBit gang employs perhaps the largest variety of tools to bypass EDR and defense systems in the world of cybercrime. The tools they use to disable EDR processes include Backstab, Defender Control, Terminator GMER, PCHunter, PowerTool, ProcessHacker, and TDSSKiller [T1562.001].

Additionally, LockBit 3.0 affiliates use Bat Armor to bypass PowerShell's execution policy [T1059.001], allowing them to deploy a batch script, "123.bat" and variations, to disable and uninstall anti-malware software.

BianLian

BianLian is a ransomware developer, deployer, and data extortion cybercriminal group. BianLian group actors use several LotL techniques, leveraging PowerShell [T1059.001] and Windows Command Shell [T1059.003] to disable antivirus tools [T1562.001], specifically Windows Defender and Anti-Malware Scan Interface (AMSI). To do this, they often use a Deployment Image Servicing and Management (DISM) executable — a Windows tool designed to install, uninstall, configure, and update features, packages, and drivers.

They also modify the Windows Registry [T1112] to disable tamper protection for Sophos services, such as SAVEnabled, SEDEEnabled, and SAVService, allowing them to uninstall them.

EDR Bypass Methods — At-A-Glance

We have compiled an at-a-glance table to allow us to compare how the twelve different ransomware gangs have approached **EDR evasion**. Each column represents an attack method that can successfully **bypass endpoint defenses such as EDRs**.

EDR BYPASS METHODS USED → / GROUP NAME	GMER Anti-Rootkit	Powertool	EDRKill Shifter	Windows Management Instrumentation	Backstab Tool	LotL - PowerShell	LotL BYOVD	Universal Virus Sniffer	Process Hacker	IOBit Hacking	PCHunter	TDSSKiller	Own Access Point
RansomHub			●	●		●	●						
Blacksuit (Royal)	●	●											
Black Basta					●	●							●
Akira		●											
Phobos		●				●		●	●				
ALPHV Black						●							●
Play	●	●				●			●	●			
Rhysida						●							●
AvosLocker						●	●						●
Snatch						●							●
LockBit 3.0	●	●		●	●		●		●		●	●	●
BianLian				●		●	●						●

This image shows that there is no EDR defense that is impenetrable. Each of the cybercriminal groups highlighted here have several methods available to evade EDR detection.

> **Read our annual Lumu Compromise Report 2024 to find out our latest statistics on the threat actors and analysis of their behaviors.**

While these are the techniques currently known about, and highlighted by CISA, these cybercriminal gangs (and others) are constantly developing new and original methods to bypass our endpoint defenses. While these defenses are important, we have to assume that ransomware gangs will be able to bypass defenses, no matter how they evolve, and plan for catching them on the other side.

What Happens When the EDR Is Bypassed?

Each ransomware gang discussed here has found at least two methods to evade, bypass, or disable EDR protections to carry out their attack chain successfully.

This trend exposes the fallacy of the cybersecurity mindset that says we can rely on a single pillar to secure an entire enterprise — and highlights the need to reevaluate the traditional triad of Firewall, EDR, and email security, operating in silos.

Furthermore, the evolution of cybersecurity has led many organizations to lean more heavily on EDR through either Extended Detection and Response (XDR) and Managed Detection and Response (MDR). These are often sold as the ultimate solution, but in reality have similar issues to the traditional stack.

- XDRs rely heavily on endpoints to gather information centrally, however, the same weaknesses remain when EDR or other traditional security measures are bypassed.
- The MDR approach integrates human threat hunting, monitoring, and response, but security analysts could be left blind to the threats, and ineffective, as they tend to rely, primarily, on EDRs.

While EDRs are a vital pillar of any cybersecurity strategy, they are not infallible. A robust architecture should also include full network visibility to fill the gaps in other layers of defense.

All movement, whether legitimate or criminal in nature, has to be done through the networks, making them the ultimate source of truth and the best way to detect when an attacker has breached the outer defenses. This makes it essential for SecOps teams to use the network as their base for operations.

Good network visibility allows SecOps teams to observe the network traffic caused by threat actors, allowing them to take action before it is too late. Great network visibility integrates with existing tools to automate real-time actions.

If you would like to learn more about how to do this in practice, open a Lumu Free account today to get immediate visibility across your network.