مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

EDRSilencer Disrupting Endpoint Security Solutions

Tracking #:432316409

Date:18-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a significant threat posed by EDRSilencer, a red team tool that malicious actors are repurposing to evade detection from endpoint detection and response (EDR) solutions.

TECHNICAL DETAILS:

Recently Trend Micro's Threat Hunting Team has identified EDRSilencer, a red team tool designed to disrupt endpoint detection and response (EDR) solutions by leveraging the Windows Filtering Platform (WFP). This tool is being repurposed by threat actors to evade detection, complicating the identification and removal of malware.
Originally crafted for red team assessments, EDRSilencer is utilized to block network communication from various EDR products, preventing them from sending telemetry to their management consoles. This capability enables malware to remain hidden, as EDR solutions become less effective at identifying threats.

1. **Process Discovery**: EDRSilencer scans the system for running EDR processes.
2. **Execution**: It can block all detected EDR traffic or target specific processes by path.
3. **Privilege Escalation**: The tool sets persistent WFP filters to block both IPv4 and IPv6 communications.
4. **Impact**: EDR tools fail to send alerts or telemetry, allowing malicious activities to go undetected.

Technical Details:
EDRSilencer creates filters using WFP that are capable of blocking communications from a hardcoded list of EDR processes (see **Table** for details). The filters are persistent, ensuring they remain active across system reboots.
Key Features

- **Command-Line Interface**:
  - blockedr: Blocks traffic from all detected EDR processes.
  - block <path>: Blocks traffic from a specific process.
  - unblockall: Removes all filters.
  - unblock <filter id>: Removes a specific filter.

Testing and Effectiveness:
In testing scenarios, EDRSilencer was found to effectively silence EDR products after adjusting the filters to include additional processes not initially hardcoded. This capability can lead to significant gaps in security monitoring.

List of executable names associated with common EDR products terminated by EDRSilencer:

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

Indicators of Compromise (IOCs):

SHA256	Description
721af117726af1385c08cc6f49a801f3cf3f057d9fd26fcec2749455567888e7	HackTool.Win64.EDRSilencer.REDT

RECOMMENDATIONS:

- **Multi-layered Security Controls**:
  - Network Segmentation: Isolate critical systems and sensitive data to limit lateral movement.
  - Defense-in-Depth: Utilize multiple layers of security controls, including firewalls, intrusion detection systems, antivirus, and EDR solutions.
- **Enhanced Endpoint Security**:
  - Behavioral Analysis: Deploy solutions that leverage behavioral analysis and anomaly detection to identify unusual activities that may bypass traditional EDR.
  - Application Whitelisting: Restrict execution to approved applications only, minimizing the risk of malicious software.
- **Continuous Monitoring and Threat Hunting**:
  - Proactive Threat Hunting: Regularly search for indicators of compromise (IoCs) and advanced persistent threats (APTs) within your network.
- **Strong Access Controls**:
  - Principle of Least Privilege: Ensure users and applications operate with the minimum level of access necessary for their functions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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