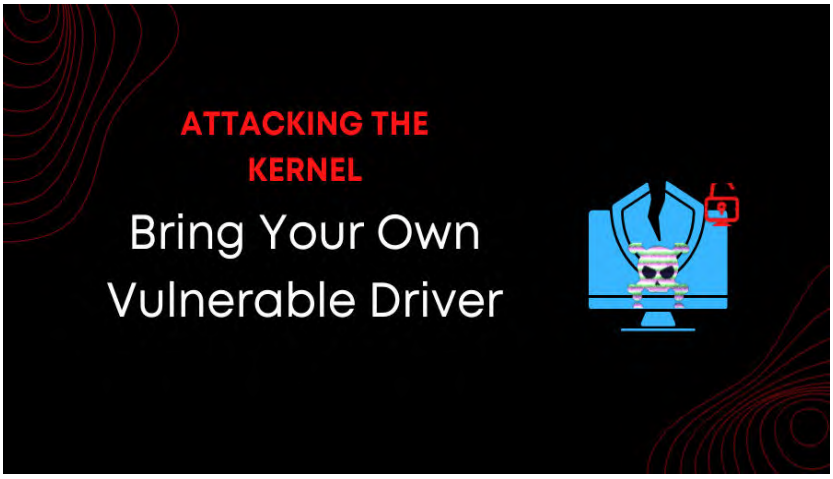
SEQURETEK

BYOVD Attacks: Abusing Legitimate Drivers to Bypass Security



Doc Ref No.: SQTK/ADV/2024/0019 - BYOVD Attack-IoC

10 YEARS | SEQURETEK SIMPLIFY SECURITY

TRUSTED BY

Global Customers | Global Investors, Analysts & Institutions | Global Alliances, Partners & Service Providers

IP

Indicator	Type
175[.]118[.]126[.]65	Server hosting malicious PowerShell script
175[.]118[.]126[.]65:8002	Server hosting malicious PowerShell script

URL

Indicator	Type
hxxp://175[.]118[.]126[.]65:8002/js/wi.txt	Server hosting malicious PowerShell script

Command Line

Data	Type
wmic service where \"PathName like '%sophos%'\" call delete /nointeractive	Attempt to delete Sophos services
wmic service where \"PathName like '%sophos%'\" call stopservice /nointeractive	Attempt to stop Sophos services

File Path

File_Path	Description
%sysdir%\drivers\updatedrv.sys	updatedrv.sys (ZAL)
\programdata\usoshared\updatedrv.sys	updatedrv.sys (ZAL)

MD5 Hashes

MD5	Description
d81c6549b9de83cd0d41910e1e7de32d	ter.exe
eb525d99a31eb4fff09814e83593a494	Anti-Logger driver used by ter.exe (ZAM.exe)
175ae9855ce9011e2825a7c05b453021	Cryptominer installer
2a0d26b8b02bb2d17994d2a9a38d61db	XMRig Miner
2a3ce41bb2a7894d939fbd1b20dae5a0	zam64.sys

SHA1 Hashes

SHA1	Description
e335715b84faedd9daccca7bee34fd3355f9c05e	ter.exe
290d6376658cf0f8182de0fae40b503098fa09fd	Anti-Logger driver used by ter.exe (ZAM.exe)
d3176d2e45abf5934a9acee53336e1547a42f371	Cryptominer installer
889a9cb0a044c1f675e63ea6ea065a8cf914e2ab	XMRig Miner
cd248648eafca6ef77c1b76237a6482f449f13be	zam64.sys

SHA256 Hashes

SHA256	Description
397eb84bfebb366c2719c02bbadfdf9de8ef608808d680c9f127f9a62ccca083	ter.exe
6f55c148bb27c14408cf0f16f344abcd63539174ac855e510a42d78cfaec451c	Anti-Logger driver used by ter.exe (ZAM.exe)
c3e6034ee65a1131068998399f110d0c944686683197b607c5598e9c09af1c39	Cryptominer installer
3c54646213638e7bd8d0538c28e414824f5eaf31faf19a40eec608179b1074f1	XMRig Miner
2bbc6b9dd5e6d0327250b32305be20c89b19b56d33a096522ee33f22d8c82ff1	zam64.sys

MITRE ATT&CK TACTICS AND TECHNIQUES

Technique Title	ID	Use
Reconnaissance		
Identify Target Systems or Networks	T1595	Threat actors research and identify potential targets, focusing on systems with vulnerable Zemana drivers and known BYOVD attack vectors.
Resource Development		
Acquire Infrastructure	T1583	Adversaries obtain the Terminator tool or its variants, Zemana drivers, and other resources from criminal forums or sources like the RAMP forum.
Initial Access		
Exploit Public-Facing Application	T1190	Threat actors exploit vulnerabilities in Zemana drivers (e.g., insufficient verification of IOCTL codes) to gain initial access to target systems.

Technique Title	ID	Use
Execution		
Scripting	T1064	BYOVD attacks involve the execution of scripts (e.g., PowerShell) to deploy tools like Terminator and exploit Zemana driver vulnerabilities.
Persistence		
Boot or Logon Autostart Execution	T1547.001	Adversaries establish persistence by configuring Terminator or other tools to execute on system boot or user logon.
Privilege Escalation		
Bypass User Account Control (UAC)	T1548.002	Threat actors may attempt to escalate privileges by bypassing UAC to install or execute the Terminator tool or manipulate Zemana drivers.
Defense Evasion		
Obfuscated Files or Information	T1027	Adversaries may use techniques to obfuscate the Terminator tool, making it harder for security solutions to detect and analyze.
Credential Access		
Credential Dumping	T1003	BYOVD attacks may involve the dumping of credentials from compromised systems for lateral movement or further privilege escalation.
Discovery		
System Information Discovery	T1082	Adversaries gather information about the target system, including details about the Zemana drivers, system architecture, and security products.
Lateral Movement		
Exploitation for Lateral Movement	T1210	Threat actors exploit vulnerabilities in Zemana drivers to move laterally within the network, compromising additional systems.
Collection		
Data from Local System	T1005	Adversaries collect data from compromised systems, potentially including information about the Zemana drivers, security configurations, and sensitive files.
Command and Control		
Remote Access Tools	T1219	The Terminator tool or its variants may be used as a remote access tool for command and control purposes, enabling threat actors to control compromised systems.
Exfiltration		
Exfiltration Over Alternative Protocol	T1048	Threat actors may exfiltrate stolen data using alternative protocols to avoid detection, potentially including information obtained through BYOVD attacks.
Impact		
Disable Security Tools	T1562.001	BYOVD attacks aim to disable security tools, leveraging Terminator or similar tools to manipulate Zemana

Technique Title	ID	Use
		drivers, compromising Endpoint Detection and Response (EDR) solutions.