SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

SUMMIT & TRAINING 2023

Austin, TX or Live Online for FREE

Summit: *August 3 - 4* | **Training:** *August 5 - 10*

0x10

DFIR

Breaching the Depths of the Abyss: Exposing Rootkits and Bootkits

Introduction

Michael Haag

Cyber Threat Connoisseur

Jose Hernandez

Distinguished Shield Builder

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

SUMMIT & TRAINING 2023

Agenda

- Problem
- What do drivers buy an adversary?
- LOLDrivers
- Bootloaders & Bootkits
- Key Takeaways

Problem

Problem:
Hunting drivers as Windows Rootkits is hard

- High volume
- Low reward
- Inability to determine good/bad
- Level 12 Threat Hunting

Problem

As the trend of adversaries exploiting drivers becomes increasingly prevalent, we find ourselves in the midst of a new era of "Bring Your Own Vulnerable Driver" attacks.

‘Bring your own vulnerable driver’ attack technique is becoming popular among threat actors

Updated on: 19 January 2023

Hackers backdoor Windows devices in Sliver and BYOVD attacks

By Bill Toulas February 6, 2023 04:00 PM

APTs adopt Vulnerable Drivers

Various different APTs and Threat actors have been adopting vulnerable drivers to bypass security controls

SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security

January 10, 2023 CrowdStrike Intelligence Team Research & Threat Intel

In part one on North Korea's UNC2970, we covered UNC2970's tactics, techniques and procedures (TTPs) and tooling that they used over the course of multiple intrusions. In this installment, we will focus on how UNC2970 utilized Bring Your Own Vulnerable Device (BYOVD) to further enable their operations.

Windows Drivers: What does it buy the adversary?

- Windows will load signed/unsigned, old and new
- Kernel level persistence, defense evasion
- Hard to prevent (AV)
- Hard to detect

Windows is getting “better” though

Defender/WDAC blocks *most* LOLDrivers

HVCI is there

LOLDrivers: Curated list of known evil

- Detection: Sigma, Sysmon, yara
- Prevention: WDAC, Sigma, ClamAV
- 1000+ drivers
- Full enrichment

loldrivers.io

Living Off The Land Drivers

Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

LOLDrivers: Curated list of known evil

API

via JSON or CSV

Sigma

via rule file

Sysmon

configuration file

Yara

.yara rules to hunt

LOLDrivers Scanner

https://t.ly/rY5oc

Suggested Folders:

```
C:\WINDOWS\inf
C:\WINDOWS\System32\drivers
C:\WINDOWS\System32\DriverStore\FileRepository
```

LOLDrivers: Walkthrough

MSqPq.sys

Description

BlackCat Ransomware Deploys New Signed Kernel Driver. BlackCat ransomware incident that occurred in February 2023.

- **UUID**: 8198f5af-4b40-4800-a22a-4a7cf957ef37
- **Created**: 2023-06-05
- **Author**: Guus Verbeek
- **Acknowledgement**: |

Download

This download link contains the malicious driver!

Commands

NOT SET

```
sc.exe create MSqPq.sys binPath=C:\windows\temp\MSqPq.sys type=kernel && sc.exe start MSqPq.sys
```

LOLDrivers: Walkthrough

Use Case	Privileges	Operating System
Elevate privileges	kernel	Windows 10

Detections

YARA	Sigma	Sysmon
▼ Expand	▼ Expand	▼ Expand
Exact Match	Names	Block
with header and size limitation	detects loading using name only	on hashes
Threat Hunting	Hashes	Alert
without header and size limitation	detects loading using hashes only	on hashes

LOLDrivers: Walkthrough

Known Vulnerable Samples

Property	Value
Filename	MSqPq.sys
MD5	97539c78d6e2b5356ce79e40bcd4d570
SHA1	f6793243ad20359d8be40d3accac168a15a327fb
SHA256	56066ed07bad3b5c1474e8fae5ee2543d17d7977369b34450bd0775517e3b25c
Authentihash MD5	e66ea646261c73baee310361524fbb7c
Authentihash SHA1	12d1ff0396dc1ffe15ad4fcb42319f6d4ee99393
Authentihash SHA256	0527451d72ba02db8479ea69689350cc563b939bb2cc685386719ab32b7e2772
RichPEHeaderHash MD5	b3c2084dcf3f40c0653c0d83ed93d1ec
RichPEHeaderHash SHA1	98192b19393d287eeaa3c6cb52aa97723a66d136
RichPEHeaderHash SHA256	783d7f55f46700737aafd36725d14b1c98049d9c0179f13143227d1e285d624b

Download

Certificates

▶ Expand

Imports

▶ Expand

Imports

▶ Expand

ImportedFunctions

▶ Expand

ExportedFunctions

▶ Expand

Signature

▶ Expand

Windows Drivers: Rapid Response

Terminator

Terminator antivirus killer is a vulnerable Windows driver in disguise

By Sergiu Gatlan May 31, 2023 03:25 PM 0

However, as a CrowdStrike engineer revealed in a Reddit post, Terminator just drops the legitimate, signed Zemana anti-malware kernel driver named zamguard64.sys or zam64.sys into the folder with a random name between 4 and 10 characters.

Property	Value
Filename	zamguard64.sys
MD5	99c131567c10c25589e741e69a8f8aa3
SHA1	3b8ddf860861cc4040dea2d2d09f80582547d105
SHA256	45f42c5d874369d6be270ea27a5511efcca512aeac7977f83a51b7c4dee6b5ef
Authentihash MD5	38757cf8a65976f362f287c3e94f8c1b
Authentihash SHA1	87cdb7698822d92a070b83b732fffa0ea99e34a2
Authentihash SHA256	950b672d3300bcacefe568156fbc8b16fa09da13df2f6ecda31254faaaf041f9
RichPEHeaderHash MD5	c0210f91c028886456549a7aa78f8147
RichPEHeaderHash SHA1	ea5478898d988d1bfa1287940ad74e5445f80a8d
RichPEHeaderHash SHA256	820b53e3b20277040944a1286a3f401ca8fb24b4f93535dc570e2261632e2f26
Company	Zemana Ltd.
Description	ZAM
Product	ZAM

Download

Windows Drivers: Rapid Response

The rise of GMER

BlackOut

NimBlackOut

Pricing:
I'm selling the all in one version for $1.5k only for the first 5 people, then the price will be $3k.
$300 for one build for a specific AV/EDR/XDR. The following EDRs cannot be sold alone: SentinelOne, Sophos, CrowdStrike, Carbon Black, Cortex, Cylance.

gmer64.sys

Description

Driver used by the GMER application. Which is an application that detects and removes rootkits

- UUID: 7ce8fb06-46eb-4f4f-90d5-5518a6561f15
- Created: 2023-05-22
- Author: Michael Haag
- Acknowledgement: hfiref0x | hfiref0x

Download

Windows Drivers: Rapid Response

Undocumented driver-based browser hijacker RedDriver targets Chinese speakers and internet cafes

By Chris Neal

TUESDAY, JULY 11, 2023 13:07

834761775.sys

Description

Cisco Talos has identified multiple versions of an undocumented malicious driver named "RedDriver," a driver-based browser hijacker that uses the Windows Filtering Platform (WFP) to intercept browser traffic. RedDriver has been active since at least 2021. RedDriver utilizes HookSignTool to forge its signature timestamp to bypass Windows driver-signing policies. Code from multiple open-source tools has been used in the development of RedDriver's infection chain, including HP-Socket and a custom implementation of ReflectiveLoader. The authors of RedDriver appear to be skilled in driver development and have deep knowledge of the Windows operating system. This threat appears to target native Chinese speakers, as it searches for Chinese language browsers to hijack. Additionally, the authors are likely Chinese speakers themselves.

- **UUID**: 66813e1f-13c8-4884-931a-62b46350c345
- **Created**: 2023-07-12

Source and Prevalence

`sysmon` EventCode=6 | stats min(_time) as firstTime max(_time) as lastTime count by ImageLoaded Computer Signed Signature service_signature_verified service_signature_exists Hashes

ImageLoaded	Computer	Signed	Signature	service_signature_verified	service_signature_exists
C:\Temp\dell.sys	win-dc-mhaag-attack-range-270.attackrange.local	true	Dell Inc.	true	true
C:\Windows\System32\drivers\mmcss.sys	win-dc-mhaag-attack-range-270.attackrange.local	true	Microsoft Windows	true	true
C:\Windows\System32\drivers\mmcss.sys	win-host-mhaag-attack-range-803	true	Microsoft Windows	true	true
C:\ProgramData\combo12.sys	win-dc-mhaag-attack-range-270.attackrange.local	true	CAPCOM Co.,Ltd.	true	true
C:\Users\Administrator\Desktop\artifact_DriverInstallationPackage\builder\package 2\combo2.sys	win-dc-mhaag-attack-range-270.attackrange.local	true	CAPCOM Co.,Ltd.	true	true
C:\Windows\System32\DriverStore\FileRepository\compositebus.inf_amd64_a140581a8f8b58b7\CompositeBus.sys	win-dc-mhaag-attack-range-270.attackrange.local	true	Microsoft Windows	true	true

LOLDrivers Lookup

```
1 `sysmon` EventCode=6
2 | lookup loldrivers driver_name AS ImageLoaded OUTPUT is_driver driver_description
3 | search is_driver = TRUE
4 | stats  min(_time) as firstTime max(_time) as lastTime count by dest ImageLoaded driver_description
5 | `security_content_ctime(firstTime)`
6 | `security_content_ctime(lastTime)`
```

✓ **3 events** (before 7/24/23 6:34:10.000 PM) No Event Sampling ▾ Job ▾

Events (3) Patterns **Statistics (3)** Visualization

20 Per Page ▾ Format Preview ▾

dest	ImageLoaded	driver_description
mswin-ADFS.attackrange.local	C:\Windows\System32\drivers\monitor.sys	https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules
mswin-dc01.attackrange.local	C:\Windows\System32\drivers\monitor.sys	https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules
mswin-server.attackrange.local	C:\Windows\System32\drivers\monitor.sys	https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules

Driver Inventory

With a PowerShell Scripted input on a Splunk Universal Forwarder, we can inventory at scale drivers from all endpoints.

```
[powershell://DriverInventory]
script = driverquery /FO csv /v
schedule = 0 0 * * *
sourcetype = PwSh:DriverInventory
index=win
```

```
1 `driverinventory`
2 | stats values(Path) min(_time) as firstTime max(_time) as lastTime count by host DriverType
3 | rename host as dest
4 | `security_content_ctime(firstTime)`
5 | `security_content_ctime(lastTime)`
```

✓ **464,945 events** (7/23/23 6:00:00.000 PM to 7/24/23 6:54:19.000 PM) No Event Sampling

Events (464,945) Patterns **Statistics (3)** Visualization

20 Per Page Format Preview

dest	DriverType	values(Path)
mswin-server	Kernel	C:\Windows\system32\DRIVERS\NDProxy.sys C:\Windows\system32\DRIVERS\ahcache.sys C:\Windows\system32\DRIVERS\cnghwassist.sys C:\Windows\system32\DRIVERS\ipfltdrv.sys C:\Windows\system32\DRIVERS\ndistapi.sys C:\Windows\system32\DRIVERS\ndiswan.sys C:\Windows\system32\DRIVERS\netbt.sys C:\Windows\system32\DRIVERS\npcap.sys C:\Windows\system32\DRIVERS\rasacd.sys C:\Windows\system32\DRIVERS\sacdrv.sys C:\Windows\system32\DRIVERS\scfilter.sys C:\Windows\system32\DRIVERS\splknetdrv.sys C:\Windows\system32\DRIVERS\splunkdrv.sys C:\Windows\system32\DRIVERS\tdx.sys C:\Windows\system32\DRIVERS\vxn65x64.sys C:\Windows\system32\DRIVERS\wanarp.sys C:\Windows\system32\DRIVERS\xenbus.sys C:\Windows\system32\DRIVERS\xenfilt.sys C:\Windows\system32\DRIVERS\xennet.sys C:\Windows\system32\DRIVERS\xenvbd.sys C:\Windows\system32\DriverStore\FileRepository\compositebus.inf_amd64_a140581a8f8b58b7\CompositeBus.sys C:\Windows\system32\Drivers\UcmCx.sys C:\Windows\system32\Drivers\UcmTcpciCx.sys C:\Windows\system32\Drivers\acpiex.sys C:\Windows\system32\Drivers\cng.sys C:\Windows\system32\Drivers\ksecdd.sys C:\Windows\system32\Drivers\ksecpkg.sys C:\Windows\system32\Drivers\msgpioclx.sys C:\Windows\system32\drivers\1394ohci.sys C:\Windows\system32\drivers\3ware.sys C:\Windows\system32\drivers\ACPI.sys C:\Windows\system32\drivers\ADP80XX.SYS C:\Windows\system32\drivers\AWSNVMe.sys C:\Windows\system32\drivers\AcpiDev.sys C:\Windows\system32\drivers\AgileVpn.sys C:\Windows\system32\drivers\BasicDisplay.sys

Driver Dashboard

New Sys Files

dest	file_create_time	file_name	file_path	count	firstTime	lastTime
win-dc-mhaag-attack-range-270.attackrange.local	2022-05-12T19:55:12-06:00	combroker.sys	C:\Users\Administrator\Desktop\U-Program\seewolf\combroker.sys	1	2022-05-12T19:55:12-06:00	2022-0 12T19:5
win-dc-mhaag-attack-range-270.attackrange.local	2022-05-12T19:55:46-06:00	$IOVYWD9.sys	C:\$Recycle.Bin\S-1-5-21-2059343465-2300599999-2417073716-500\$IOVYWD9.sys	1	2022-05-12T19:55:46-06:00	2022-0 12T19:5 06:00
win-dc-mhaag-attack-range-270.attackrange.local	2022-05-12T19:56:42-06:00	Capcom.sys	C:\Users\Administrator\Desktop\U-Program\seewolf\Capcom.sys	1	2022-05-12T19:56:42-	2022-0 12T19:5

Sc Create New Kernel Driver

dest	user	parent_process_name	process_name	process
win-dc-mhaag-attack-range-270.attackrange.local	Administrator	cmd.exe	sc.exe	sc.exe create Atomi322 binpath= "C:\Users\Administrator\Desktop\artifact_DriverInstallationPackage\builder\package2\combo.sys" type= kernel start= auto displayname= "Atomi322"
win-dc-mhaag-attack-range-270.attackrange.local	Administrator	cmd.exe	sc.exe	sc.exe create Atomi3222 binpath= "C:\Users\Administrator\Desktop\artifact_DriverInstallationPackage\builder\package2\combo2.sys" type= kernel start= auto displayname= "Atomi3222"

Audit & Prevent

Inventory Drivers

Enable Windows Attack Surface Reduction rules (can’t prevent? Audit!)

Use SecureBoot

Driver Signing Enforcement

Implement Application Control

Windows Defender Application Control or AppLocker

Ensure HVCI is enable

Bootloaders & Bootkits

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING 2023

What is a Bootloader or BootKit?

	Bootloader	Bootkit
Purpose	Loads the operating system into memory after startup	Infects the system to gain control before the OS boots up
Location	Stored in non-volatile memory	Infects low-level system areas like MBR or VBR
Effect on system	Essential for system operation	Causes harm, evades detection, and maintains unauthorized access
Interacts with OS	Loads the OS kernel	Manipulates or bypasses the OS

What is a Bootloader?

A bootloader is a software or set of instructions that loads the operating system into the computer's memory upon startup. It initializes the hardware components and creates an environment for the operating system to run.

Key points:

- It prepares the system for operation after the power-on self-test (POST).
- Its main task is to load the kernel of the OS into memory.
- It's stored in non-volatile memory like ROM or EPROM.

What is a BootKit?

A bootkit is a type of malicious software that infects the computer at a level deep enough to gain control before the operating system has fully booted up. It targets the bootloader and can therefore bypass security measures like antivirus software and OS security features.

Key points:

- It infects the system at a lower level (e.g., Master Boot Record or Volume Boot Record).
- It's designed to evade detection and removal.
- It can be used to create persistent and stealthy access to a compromised system.

Why does this matter?

01	System Integrity and Security	Bootkits are a serious security threat as they operate at a lower level than most security measures.
02	Optimizing System Performance	Understanding bootloaders can be useful for operating system developers and IT professionals
03	Troubleshooting and Repair	Knowledge about bootloaders and bootkits can aid in troubleshooting various system issues, including boot failures and malware infections.
04	Understanding the Tech Stack	Bootloaders and bootkits are integral parts of the larger technological ecosystem.

What about UEFI and SecureBoot?

UEFI (Unified Extensible Firmware Interface) and **Secure Boot** are modern technologies designed to enhance the security and functionality of the system boot process.

UEFI: This is a specification that defines a software interface between an operating system and platform firmware. It is designed to replace the Basic Input/Output System (BIOS) firmware interface. UEFI provides several enhancements over BIOS, including:

- Better compatibility with modern hardware.
- Faster boot times.
- Support for booting from larger (>2TB) disks.
- CPU-independent architecture and drivers.

Secure Boot: This is a security standard developed by members of the PC industry to help ensure that a device boots using only software that is **trusted** by the Original Equipment Manufacturer (OEM). When the PC starts, the firmware checks the signature of each piece of boot software, including firmware drivers (Option ROMs) and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system.

UEFI Revocation List

UEFI Revocation List files contain the, now-revoked, signatures of previously approved and signed firmware and software used in booting systems with UEFI Secure Boot enabled.

```
SHA 256 FLAT,PE256 Authenticode,Filename,Architecture,Partner,CVEs,Revocation List Date
2DF05C41ACC56D0F4C9371DA62EC6CB311C9AFB84B4A4D8C3738583CCC874D38,C805603C4FA038776E42F263C604B49D96840322E1922D5606A9B0BBB5BFFE6F,BOOTX64.EFI,64-bit, Ciscso Systems Inc.,CVE-2020-10713;
AA6F27B8B2CA5826F497362042C003B5E1D7CA22383D82730FBC5C45E048D839,56FB79AAB26EE9D0E0CA372FB86A8BB459ACBC505D0AB35E6A632A3D5F88DCB3,bootia32.efi,32-bit,Neverware,CVE-2020-10713; CVE-2020-
3F8F266488F3B888EB77B8DF43582FA8124366B7D0670ED78926410F9C9F411F,D8D4E6DDF6E42D74A6A536EA62FD1217E4290B145C9E5C3695A31B42EFB5F5A4,bootx64.efi,64-bit,Neverware,CVE-2020-10713; CVE-2020-1
4E371DD0448F1DE869EE087B59FF88D11865463715272BCC6C29B0D5E21DBD82,F277AF4F9BDC918AE89FA35CC1B34E34984C04AE9765322C3CB049574D36509C,bootx64.efi,64-bit,Miray Software AG,CVE-2020-10713; CV
A9F6C38C2608D6F36F246E74A9FD17E915C89E54EAFA2281B8ACE86133DF22B3,ADCC0B6FD6DC5911BF42F036C033FC3E43F07A8312E91D0D8D32793B62940C7E,BOOTia32.efi,32-bit,whitecanyon,CVE-2020-10713; CVE-202
0E5EB8D0BEBF089A974BC0CA85D33D73F9A0BF72ED2A5E3A62A0387B51D509CE,68EE4632C7BE1C66C83E89DD93EAEE1294159ABF45B4C2C72D7DC7499AA2A043,bootx64.efi,64-bit,Miray Software AG,CVE-2020-10713; CV
F88E92940985413ACD440DAA20C08DF99C54613636826D9D95B898D39C44B19B,148FE18F715A9FCFE1A444CE0FFF7F85869EB422330DC04B314C0F295D6DA79E,bootmgfw.efi,64-bit,Microsoft,CVE-2020-10713; CVE-2020-
50484376441815F7F85AA294290A9B6072A6A9E8FEAE79447C5C4DE855C5A3D3,AD3BE589C0474E97DE5BB2BF33534948B76BB80376DFDC58B1FED767B5A15BFC,BOOTx64.efi,64-bit,whitecanyon,CVE-2020-10713; CVE-2020
7B5DFE4F9E4EE68E3CDD9C91BCAE26DB334D49AE4C1F9525CECD834DE48DF110,E051B788ECBAEDA53046C70E6AF6058F95222C046157B8C4C1B9C2CFC65F46E5,bootx64.efi,64-bit,NTI Corporation,CVE-2020-10713; CVE-
0DD832075D552DA3D29B1EF471FC23B47C0D54B9FD1541935B23F1C5813DA08C,C452AB846073DF5ACE25CCA64D6B7A09D906308A1A65EB5240E3C4EBCAA9CC0C,BOOTX64.EFI,64-bit,Alt Linux LTD,CVE-2020-10713; CVE-20
2F871712447DDE7C3552F5AA90A2292821C6F32D92788E00DEE8566F8D4DE209,98CC8B91FEC5252F62E81843D9D5D8AC2A2F253AA38152B3236A5092200ED290,bootia32.efi,32-bit,Alt Linux LTD,CVE-2020-10713; CVE-2
5156A8AE596C06692AEF13AC6524C7F1E20D52E4EA0F5A5AD43A6874EDCC5E1F,3A91F0F9E5287FA2994C7D930B2C1A5EE14CE8E1C8304AE495ADC58CC4453C0C,bootx64.efi,64-bit,Alt Linux LTD,CVE-2020-10713; CVE-20
CEF9A1B433C4ED851EC0C373F7E1F19A2B8C306A821D114F177B14E8C070276F,1B909115A8D473E51328A87823BD621CE655DFAE54FA2BFA72FDC0298611D6B8,,64-bit,Alt Linux LTD,CVE-2020-10713; CVE-2020-14308; C
C4B5797189521611B809720ED9C4734F1DEC8A2EE2597781FFE438F652A58CE5,8C0349D708571AE5AA21C1136348233207329 7D868F29058916529EFC520EF70,bootx64.efi,64-bit,Alt Linux LTD,CVE-2020-10713; CVE-20
5C39F0E5E0E7FA3BE05090813B13D161ACAF48494FDE6233B452C416D29CDDBE,C452AB846073DF5ACE25CCA64D6B7A09D906308A1A65EB5240E3C4EBCAA9CC0C,,64-bit,Alt Linux LTD,CVE-2020-10713; CVE-2020-14308; C
9EA346FCFE6DB7F3140DA8FFD5738F6CF97D6014DA61033B32049CB17696B372,EED7E0EFF2ED559E2A79EE361F0962AF3B1E999131E30BB7FD07546FAE0A7267,,64-bit,Alt Linux LTD,CVE-2020-10713; CVE-2020-14308; C
E352109145416E3B61DCF5E09492D24410828121E7D74C08CE0D3157B45A0831,BADFF5E4F0FEA711701CA8FB22E4C43821E31E210CF52D1D4F74DD50F1D039BC,BOOTx64.EFI,64-bit,BITDEFENDER,CVE-2020-10713; CVE-2020
A95666BFAF48FD9C4CAF2F3ED4EB593145C48BD3C93E4B00638088CE7EE962CF,D89A11D16C488DD4FBBC541D4B07FAF8670D660994488FE54B1FBFF2704E4288,,64-bit,BITDEFENDER,CVE-2020-10713; CVE-2020-14308; CVE
AECD34387179AFF5CE02103679312CDEB1DA835015A8548FCE93765E7219612E,F2A16D35B554694187A70D40CA682959F4F35C2CE0EAB8FD64F7AC2AB9F5C24A,,64-bit,BITDEFENDER,CVE-2020-10713; CVE-2020-14308; CVE
24D6B301A1268BA8B3732759815388552 05EB0115609800F2B5B95377483B108,5B248E913D71853D3DA5AEDD8D9A4BC57A917126573817FB5FCB2D86A2F1C886,bootx64.efi,64-bit,Blancco Technology Group,CVE-2020-10
3D23947C39680B9FCF22B092B97C9D38EDCC02F7AD13D3A925D1EE0B62797E73,7EAC80A915C84CD4AFEC638904D94EB168A8557951A4D539B0713028552B6B8C,grubx64.efi,64-bit,Canonical,CVE-2020-10713; CVE-2020-1
```

https://uefi.org/revocationlistfile

The Boots

As defenders, how can we learn more about Boot Kits and Loaders?

```
 TTTTT H   H EEEEE      BBBBB  0000  0000 TTTTT SSSSS
   T   H   H E          B   BB 0   00   0   T   S
   T   HHHHH EEEE       BBBBB  0   00   0   T   SSSSS
   T   H   H E          B   BB 0   00   0   T       S
   T   H   H EEEEE      BBBBB  0000  0000   T   SSSSS
1. Set BootExecute value to ""autocheck autoche *""
2. Revert BootExecute value to its default ""autocheck autochk *""
3. Display the current BootExecute value
4. Set BootExecute value to a custom value
5. Exit
Enter your choice (1-5): _
```

https://github.com/MHaggis/notes/blob/master/utilities/theBoots.ps1

The Boots

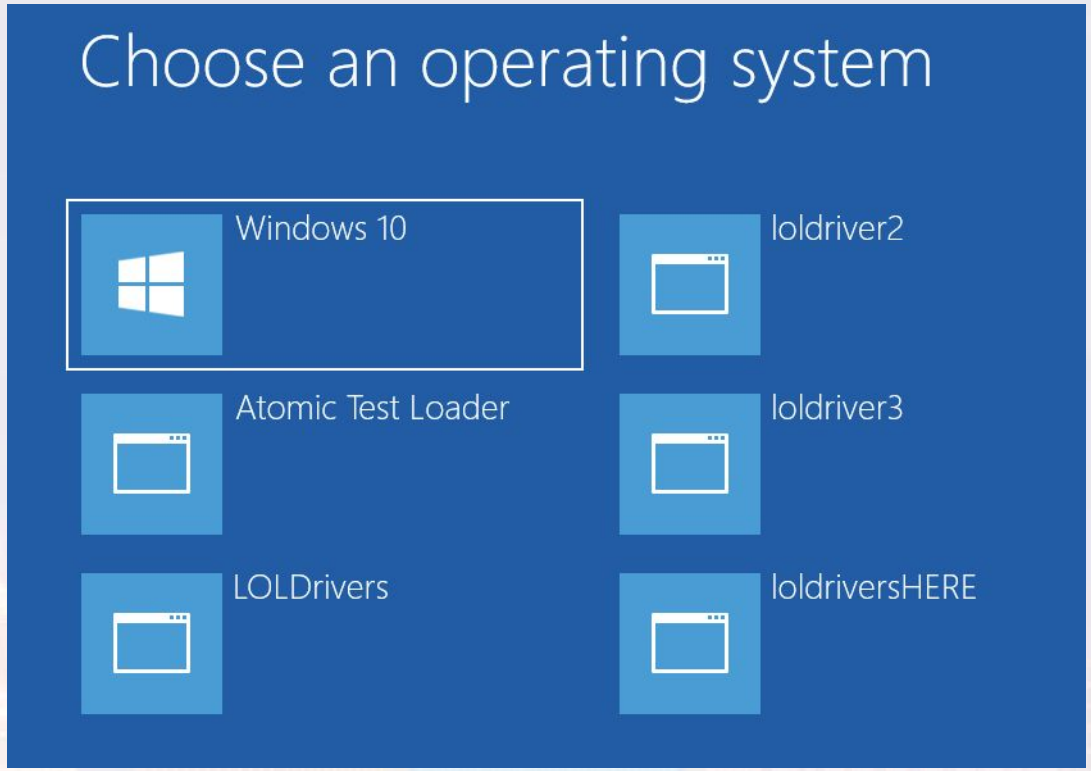
```
Clear-Host
Write-Host @"
 TTTTT H   H EEEEE      BBBBB  0000  0000 TTTTT SSSSS
   T   H   H E          B   BB 0   00   0   T   S
   T   HHHHH EEEE       BBBBB  0   00   0   T   SSSSS
   T   H   H E          B   BB 0   00   0   T       S
   T   H   H EEEEE      BBBBB  0000  0000   T   SSSSS
"@

function Show-Menu {
    Write-Host "1. Set BootExecute value to `"`"autocheck autoche *`"`""
    Write-Host "2. Revert BootExecute value to its default `"`"autocheck autochk *`"`""
    Write-Host "3. Display the current BootExecute value"
    Write-Host "4. Set BootExecute value to a custom value"
    Write-Host "5. Exit"
}

$exit = $false

while (-not $exit) {
    Show-Menu
    $choice = Read-Host "Enter your choice (1-5)"

    switch ($choice) {
        "1" {
            reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager" /v BootExecute /t REG_MULTI_SZ /d "autocheck autoche *" /f
            Write-Host "BootExecute value updated to `"`"autocheck autoche *`"`""
        }
        "2" {
            reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager" /v BootExecute /t REG_MULTI_SZ /d "autocheck autochk *" /f
            Write-Host "BootExecute value reverted to its default `"`"autocheck autochk *`"`""
        }
        "3" {
            $value = (Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager" -Name "BootExecute").BootExecute
            Write-Host "Current BootExecute value: `"$value`""
        }
        "4" {
            $custom_value = Read-Host "Enter the custom value for BootExecute"
            reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager" /v BootExecute /t REG_MULTI_SZ /d "$custom_value" /f
            Write-Host "BootExecute value updated to `"`"$custom_value`"`""
        }
        "5" { $exit = $true }
        default {
            Write-Host "Invalid choice. Please enter a number between 1 and 5."
        }
    }
    Write-Host ""
}
```

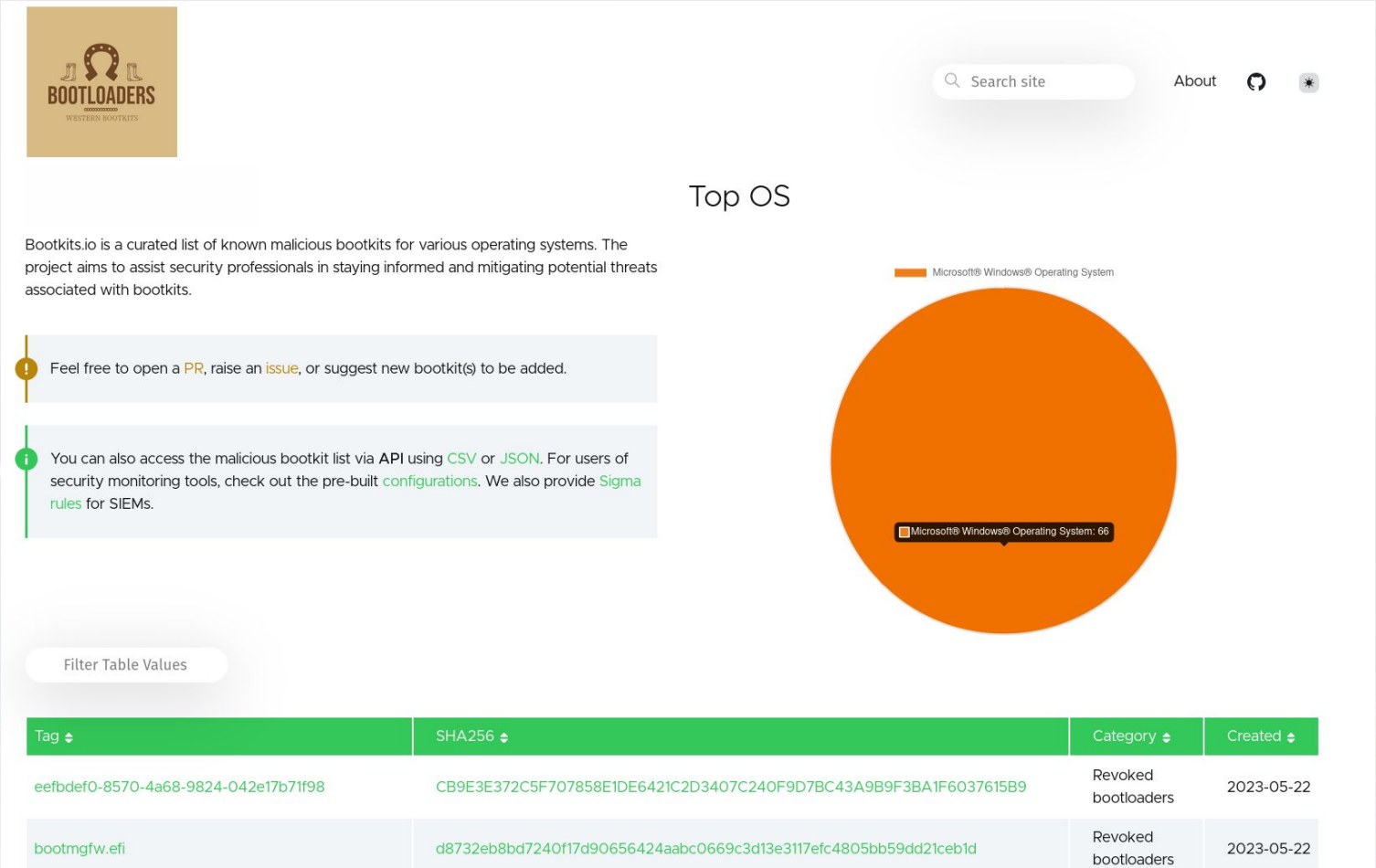


https://blogs.vmware.com/security/2021/06/detecting-uefi-bootkits-in-the-wild-part-1.html

Releasing Today: Bootloaders Project

bootloaders.io

theboots.io



Bootloaders Project

Enhanced Security Awareness and Response

Resource for Research and Education

Improved Threat Mitigation Strategies

Find Bootloaders at Scale

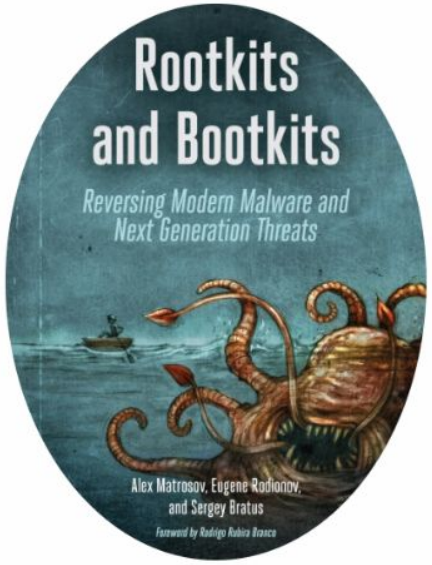
```
PS C:\Users\Administrator> bcdedit /enum /v

Windows Boot Manager
--------------------
identifier              {9dea862c-5cdd-4e70-acc1-f32b344d4795}
device                  partition=C:
description             Windows Boot Manager
locale                  en-US
inherit                 {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
bootshutdowndisabled    Yes
default                 {0daf9bba-94c8-11e6-b1fd-0e5bdc9ce43b}
resumeobject            {0daf9bb9-94c8-11e6-b1fd-0e5bdc9ce43b}
displayorder            {c33d32c6-ede4-11ed-ac06-029797d01917}
                        {0daf9bba-94c8-11e6-b1fd-0e5bdc9ce43b}
toolsdisplayorder       {b2721d73-1db4-4c62-bf78-c548a880142d}
timeout                 30

Windows Boot Manager
--------------------
identifier              {c33d32c6-ede4-11ed-ac06-029797d01917}
device                  partition=C:
description             Atomic Boots
locale                  en-US
inherit                 {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
bootshutdowndisabled    Yes
default                 {0daf9bba-94c8-11e6-b1fd-0e5bdc9ce43b}
resumeobject            {0daf9bb9-94c8-11e6-b1fd-0e5bdc9ce43b}
displayorder            {0daf9bba-94c8-11e6-b1fd-0e5bdc9ce43b}
toolsdisplayorder       {b2721d73-1db4-4c62-bf78-c548a880142d}
timeout                 30
```

```
[powershell://bootloader]
script = (bcdedit /enum /v) -split "-------------------" | % { if ($_ -match "path\s+(.+)") { Write-Output
"Path: $($matches[1])" }; if ($_ -match "identifier\s+(.+)") { Write-Output "Identifier: $($matches[1])" }; if
($_ -match "description\s+(.+)") { Write-Output "Description: $($matches[1])" } }
schedule = 0 0 * * *
sourcetype = PwSh:bootloader
  index=win
```

Shout out to:
bootkits.io



[REVERSING MODERN MALWARE AND NEXT GENERATION THREATS]

BY ALEX MATROSOV, EUGENE RODIONOV, AND SERGEY BRATUS

GITHUB TWITTER PUBLISHER AMAZON

Key Takeaways

LOLDrivers & Bootloaders is here to enhance and help you get ahead

Utilize Detection and Prevention from the projects

Detection can be tricky, think outside the box for inventory

Begin investigating how to integrate with your security stack

Thank you 🙏