



SANS DFIR

SUMMIT & TRAINING



Summit: August 15 - 16 | Training: August 17 - 22

Hunting Windows U-boats with Cyber Depth Charges

Michael Haag

Senior Threat Researcher | Splunk

DFIR Summit & Training 2022



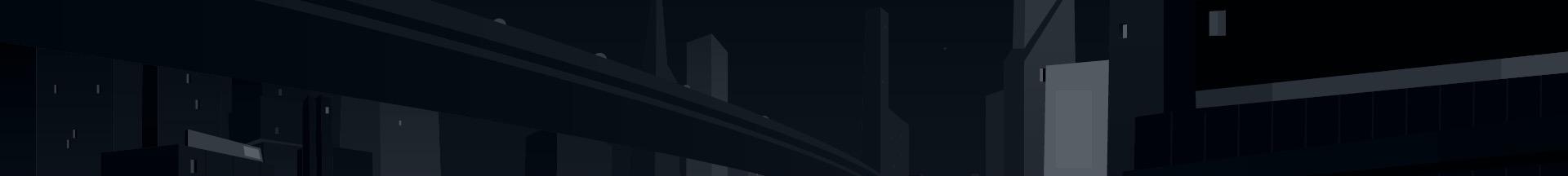
WHOAMI



@m_haggis

Git: mhaggis

- Splunk
 - Simulate/Emulate TAs
 - Research techniques
 - Generate content
- Red Canary
 - Co-Founded Atomic Red Team
 - Threat Research



NuggetPhantom

- Slashing through a binary store, came across an sys filename + digsig_status
- Turned out, we shipped a detection months ago, but some artifacts were missing

Tracking driver inventory to unearth rootkits

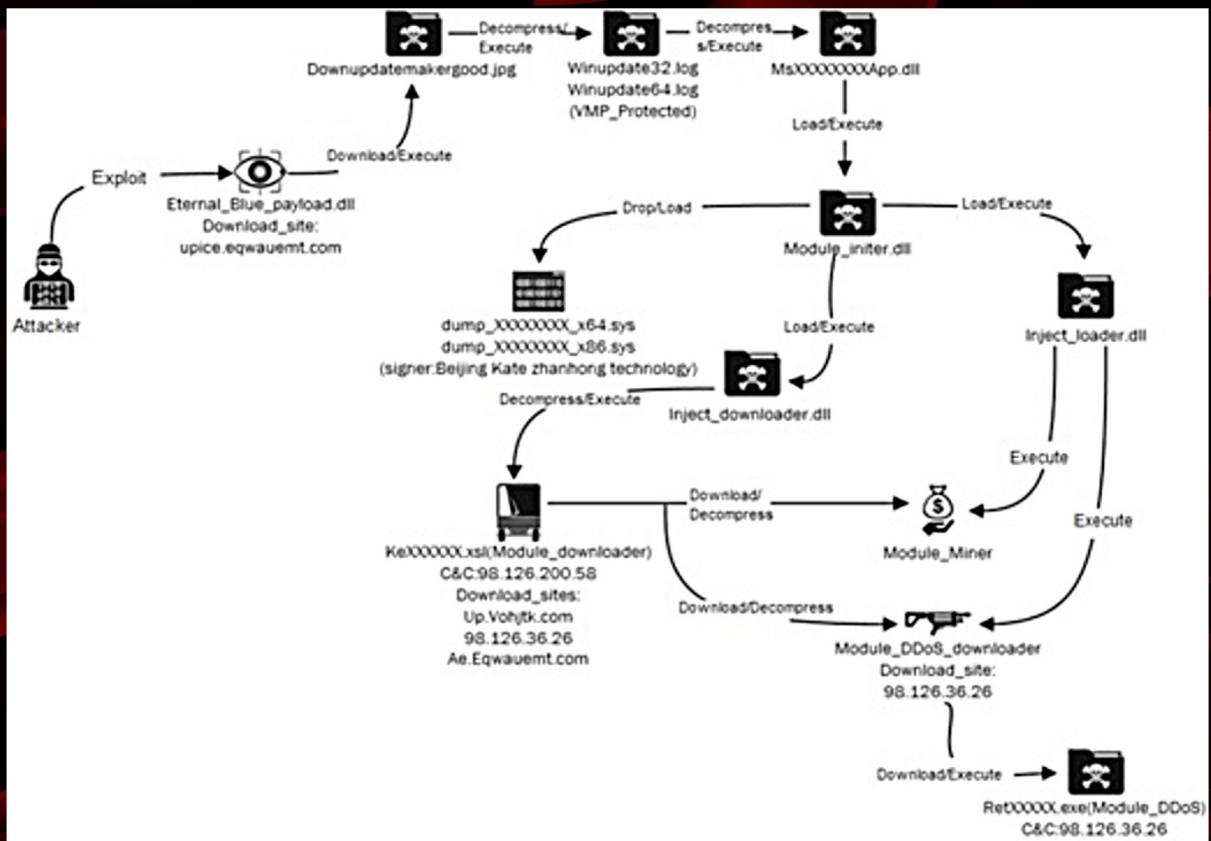
As defenders, we need to understand, enumerate, and evaluate the drivers in our environments.

CASEY SMITH • MICHAEL HAAG

June 27, 2019

<https://redcanary.com/blog/tracking-driver-inventory-to-expose-rootkits/>

NuggetPhantom



<https://nsfocusglobal.com/nuggetphantom-analysis-report/>

Problem: Hunting drivers as Windows Rootkits is hard.

- High volume
- Low reward
- May take years
- A special level of Threat Hunting
- A real challenge

Agenda

- What do drivers buy an adversary?
- Driver Signing
- Hunting
- LOLDrivers
- Prevent

What do drivers buy an adversary?

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



Drivers and Signatures

32-Bit drivers typically unsigned

Windows Vista and up - new enforcement

- But require backwards compatibility

Which introduced -

LOLDrivers / ScrewedDrivers / BYOVD

- Vulnerable signed drivers

Certificate theft

- Steal cert, sign malware.



What to Hunt Where to Hunt How to Hunt

Driver Signing - Subvert Trust Controls: Code Signing

POSTED: 28 FEB, 2022 | 9 MIN READ | THREAT INTELLIGENCE

 SUBSCRIBE

FOLLOW 



Dixin: Stealthy Backdoor Designed for Attacks Against Hardened Networks

Espionage tool is the most advanced piece of malware Symantec researchers have seen from China-linked actors.

<https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck>

<https://gist.github.com/MHaggis/9ab3bb795a6018d70fb11fa7c31f8f48>

Driver Signing - Subvert Trust Controls: Code Signing

	B	C	D	E	F	G	H	I	J
	Date	Publisher	Company	Description	Product		Product Version	File Version	Machine Type
Verified	11:59 PM 11/27/2013	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System		6.1.7600.1172	6.1.7600.1172	64-bit
A required certificate is not within its validity period.	1:03 AM 9/3/2019	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	MS LAN Driver	Microsoft® Windows® Operating System		6.1.7600.16385	6.1.7600.16385	64-bit
The digital signature of the object did not verify.	8:23 PM 2/28/2022	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	MS LAN Driver	Microsoft® Windows® Operating System		6.1.7600.16385	6.1.7600.16385	64-bit
Signed	7:07 AM 1/23/2013	Anhua Xinda (Beijing) Technology Co., Ltd.	n/a	n/a	n/a		n/a	n/a	64-bit
A certificate was explicitly revoked by its issuer.	4:05 AM 2/6/2021	Fuqing Yuntan Network Tech Co.,Ltd.	n/a	n/a	n/a		n/a	n/a	64-bit
A certificate was explicitly revoked by its issuer.	4:05 AM 2/6/2021	Fuqing Yuntan Network Tech Co.,Ltd.	n/a	n/a	n/a		n/a	n/a	64-bit
Signed	7:52 AM 4/30/2014	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System		6.1.7600.938	6.1.7600.938	64-bit
Unsigned	12:54 AM 11/18/2009	n/a	n/a	n/a	n/a		n/a	n/a	32-bit
Unsigned	7:52 AM 4/30/2014	n/a	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System		5.2.3790.938	5.2.3790.938	32-bit
The digital signature of the object did not verify.	8:23 PM 2/28/2022	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System		6.1.7600.1172	6.1.7600.1172	64-bit
Unsigned	8:42 AM 4/20/2010	n/a	n/a	n/a	n/a		n/a	n/a	32-bit
Unsigned	10:26 AM 11/19/2009	n/a	Microsoft Corporation	ntbios driver	Microsoft(R) Windows (R) NT Operating System	5, 0, 2, 1	5, 0, 2, 1	5, 0, 2, 1	32-bit
Unsigned	1:29 AM 7/18/2008	n/a	n/a	n/a	n/a		n/a	n/a	32-bit
A required certificate is not within its validity period.	4:49 PM 10/12/2012	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	MS LAN Driver	Microsoft® Windows® Operating System		6.1.7600.1421	6.1.7600.1421	64-bit
The digital signature of the object did not verify.	8:23 PM 2/28/2022	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System		6.1.7600.1172	6.1.7600.1172	64-bit
Unsigned	3:04 AM 5/18/2009	n/a	Microsoft Corporation	ntbios driver	Microsoft(R) Windows (R) NT Operating System	5, 0, 2, 1	5, 0, 2, 1	5, 0, 2, 1	32-bit
Unsigned	2:44 AM 3/26/2009	n/a	n/a	n/a	n/a		n/a	n/a	32-bit
The digital signature of the object did not verify.	8:23 PM 2/28/2022	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System		6.1.7600.1172	6.1.7600.1172	64-bit

<https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck>

<https://gist.github.com/MHaggis/9ab3bb795a6018d70fb11fa7c31f8f48>

Driver Signing - Subvert Trust Controls: Code Signing

```
VersionInfo : File: \96bf3ee7c6673b69c6aa173bb44e21fa636b1c2c73f4356a7599c121284a51cc
              InternalName: ntbio.sys
              OriginalFilename: ntbios.sys
             FileVersion: 5, 0, 2, 1
              FileDescription: nt bios driver
              Product: Microsoft(R) Windows (R) NT Operating System
              ProductVersion: 5, 0, 2, 1
              Debug: False
              Patched: False
              PreRelease: False
              PrivateBuild: False
              SpecialBuild: False
              Language: English (United States)
```

```
File: \8d9a2363b757d3f127b9c6ed8f7b8b018e65
      InternalName: wantd.sys
      OriginalFilename: wantd.sys
     FileVersion: 6.1.7600.1172
      FileDescription: WAN Transport Driver
      Product: Microsoft Windows Operating System
      ProductVersion: 6.1.7600.1172
      Debug: False
```

```
Get-ItemProperty -Path <path>| Format-list -Property VersionInfo
https://gist.github.com/MHaggis/9ab3bb795a6018d70fb11fa7c31f8f48
```

Digital Signature Results

- Digsig_result
 - Signed, Unsigned, Expired, Bad Signature, Invalid Signature, Invalid Chain, Untrusted Root, Explicit Distrust

- Digsig_publisher

- Digsig_issuer
 - Signers gone bad

- Digsig_subject

- Digsig_sign_time
 - First time seen, old sign time

- company_name

Verified	Date	Publisher	Company	Description	Product	Product Version	File Version	Machine Type
Signed	7:52 AM 4/30/2014	Anhua Xinda (Beijing) Technology Co., Ltd.	Microsoft Corporation	WAN Transport Driver	Microsoft Windows Operating System	6.1.7600.938	6.1.7600.938	64-bit

What path to take

Drivers may be loaded from anywhere

Most likely always find in

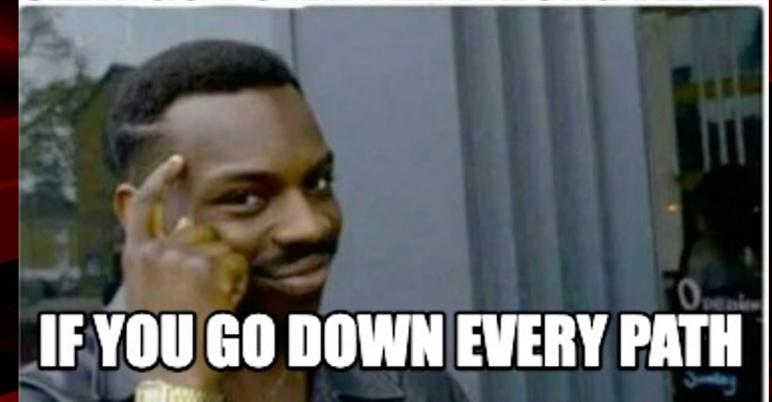
- \system32\drivers\
- \spool\drivers\
- \programdata\

Combine paths with digsig_result

Note the name -

Will not be "evildriver.sys"

CANT GO DOWN THE WRONG PATH



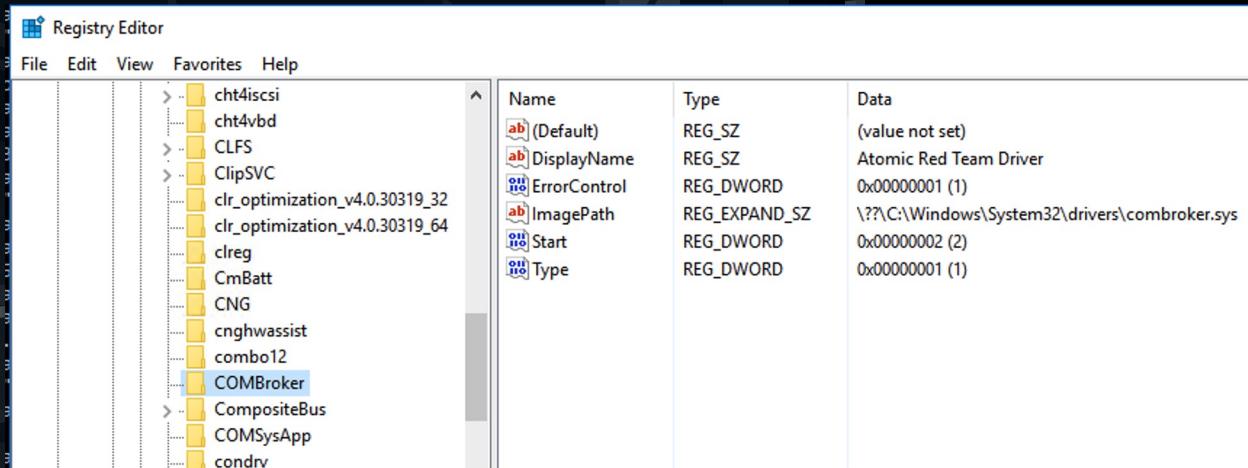
observed_filename:c:\windows\system32\drivers\ digsig_result:"Explicit Distrust"

DFIR Summit & Training 2022

Check the registry

New driver - who dis?

\Machine\System\CurrentControlSet\Services



The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes File, Edit, View, Favorites, and Help. The left pane displays a tree view of registry keys under "Services". The right pane shows a table with columns for Name, Type, and Data. One entry, "COMBroker", is selected in the tree view and highlighted in the table.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	Atomic Red Team Driver
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	\??\C:\Windows\System32\drivers\combroker.sys
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000001 (1)

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\MySafeModeService, Default = Service

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\MySafeModeService, Default = Service

DFIR Summit & Training 2022

Windows EventCode 7045

`wineventlog_system` EventCode=7045 Service_Type="kernel mode driver"

ComputerName	EventCode	Service_File_Name	Service_Name	Service_Start_Type	Service_Type
win-dc-mhaag-attack-range-270.attackrange.local	7045	C:\Users\Administrator\Desktop\artifact_DriverInstallationPackage\builder\package2\combo.sys	Atomi322	auto start	kernel mode driver
win-dc-mhaag-attack-range-270.attackrange.local	7045	C:\Users\Administrator\Desktop\artifact_DriverInstallationPackage\builder\package2\combo2.sys	Atomi3222	auto start	kernel mode driver
win-dc-mhaag-attack-range-270.attackrange.local	7045	C:\Windows\System32\drivers\combroker.sys	Atomic Red Team Driver	auto start	kernel mode driver
win-dc-mhaag-attack-range-270	7045	system32\drivers\dfs.sys	DFS Namespace Server Filter Driver	system start	kernel mode driver
win-dc-mhaag-attack-range-270	7045	system32\drivers\dfsrro.sys	DFS Replication ReadOnly Driver	boot start	kernel mode driver
win-dc-mhaag-attack-range-270.attackrange.local	7045	\SystemRoot\system32\DRIVERS\npcap.sys	Npcap Packet Driver (NPCAP)	demand start	kernel mode driver

Known Vulnerable Drivers

LOLDrivers / ScrewedDrivers

- CapCom Driver
- Dell Drivers
- Asrock Drivers

<https://github.com/eclypsium/Screwed-Drivers/blob/master/DRIVERS.md>

<https://www.rapid7.com/blog/post/2021/12/13/developer-based-attacks-past-and-present/>

<https://attackerkb.com/topics/zAHZGAFaQX/cve-2021-21551>

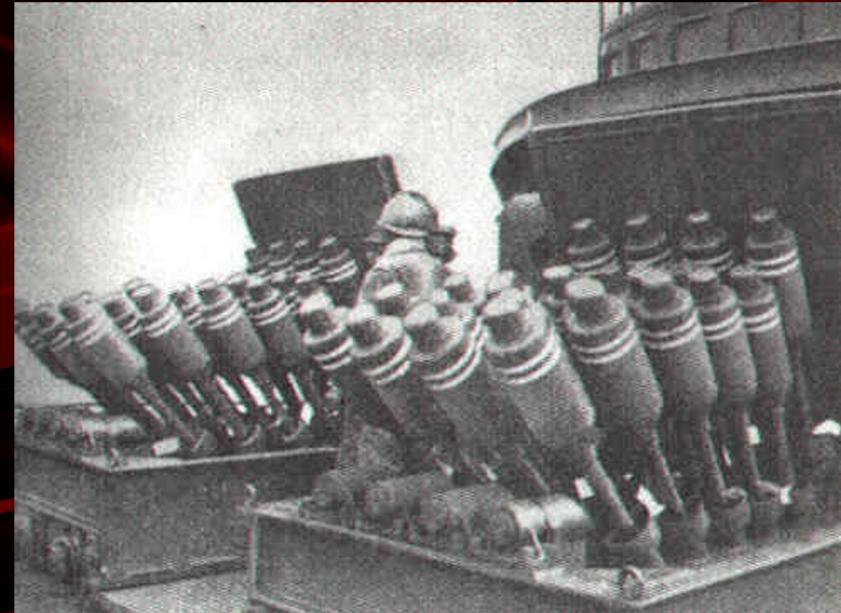
MSFT Block list - <https://bit.ly/3laHK73>



Windows will load them all.



Stack and rank



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

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	2022-05-12T19:55:12-06:00
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	2022-05-12T19:55:46-06:00
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	2022-05-12T19:56:42-06:00	2022-05-12T19:56:42-06:00

Sc Create New Kernel Driver

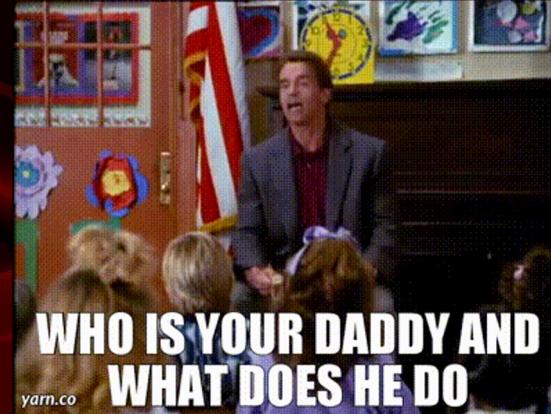
dest	user	parent_process_name	process_name	process
win-dc-mhaag-attack-range-270.attackrange.local	Administrator	cmd.exe	sc.exe	sc.exe create Atomi322 binpath= "C:\Users\Administrator\Desktop\artifact_DriverInstallationPackage\builder\package2\combo.sys" type= kernel start= auto displayname= "Atomi322"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

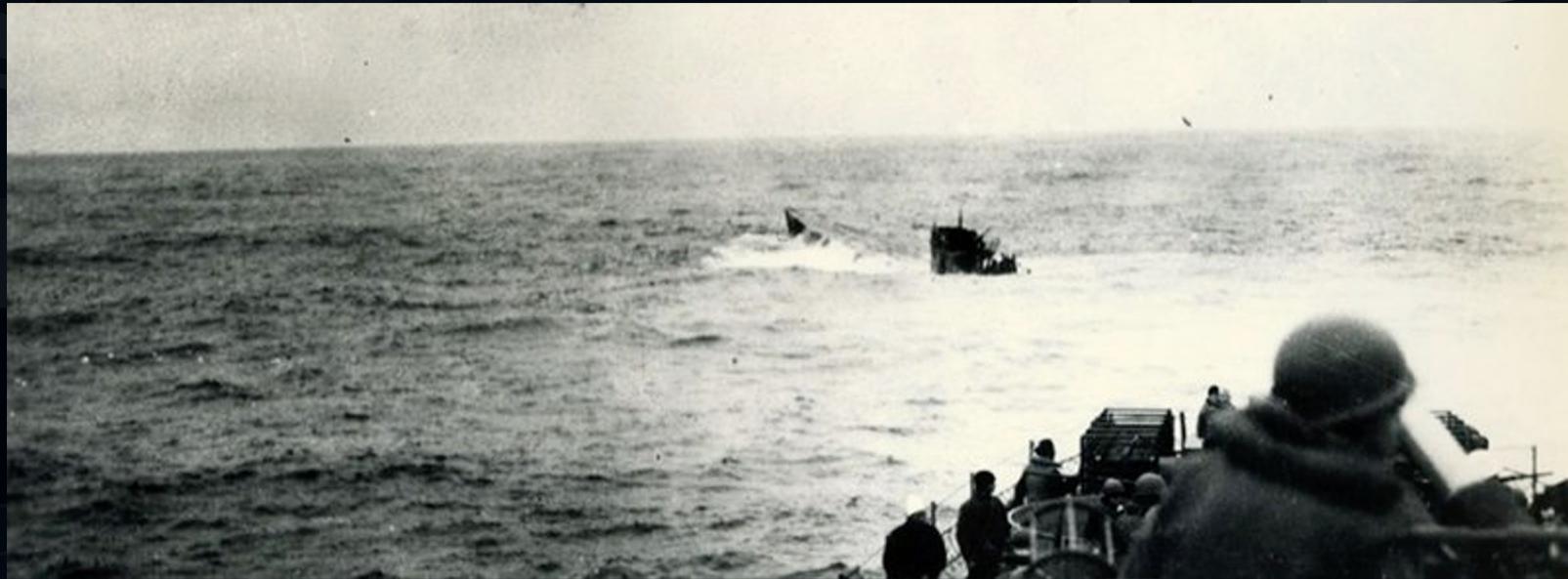
Sys Loads

ntoskrnl.exe will load sys

process_name:ntoskrnl.exe

(digsig_result_modload:"Unsigned" OR digsig_result_modload:"Explicit\ Distrust")





DFIR Summit & Training 2022



#PenTestReportTips

- 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

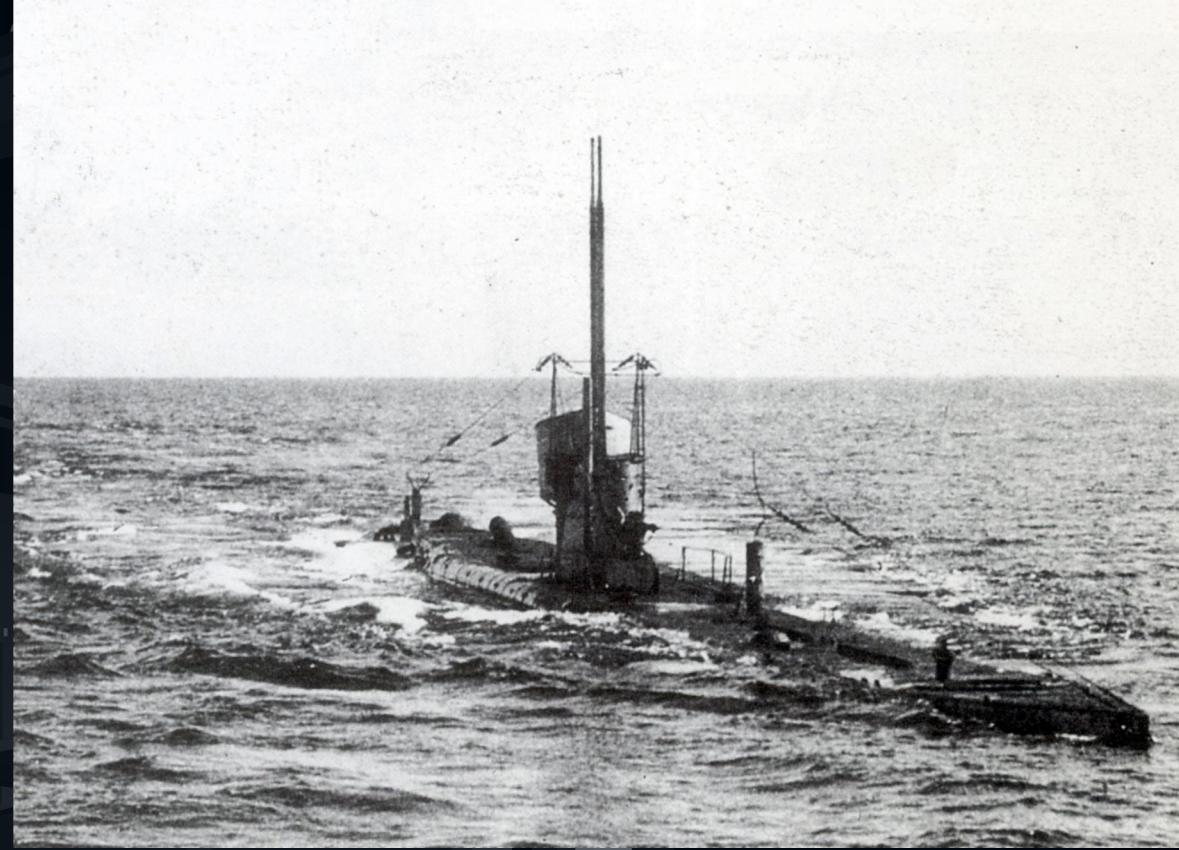
	Target(s)	Rating	Description	Rec	Reference	Notes
1	[IP Address 1]	Critical	MS14-066 Vulnerability	Apply Patch	https://support.microsoft.com/en-us/kb/2992611	Exploited – DOS Achieved
2	[IP Address 2]	Critical	MS15-034 Vulnerability	Apply Patch	https://support.microsoft.com/en-us/kb/3042553	Exploited – DOS Achieved
3	[IP Address 3] [IP Address 4]	Medium	XSS (Reflected)	Fix Apache Server / Code	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet	Instances in numerous URIs
4	[IP Address 5]	Medium	SSL Certificate Not Valid for Hostname	Register SSL Certificates for Hostname	https://wiki.mozilla.org/Security/Server_Side_TLS	None
5	[IP Address 6]	Medium	Sensitive Data Leakage (POODLE)	Disable SSL 3.0	https://technet.microsoft.com/en-us/library/security/3009008.aspx	None

Summary

- Investigate preventative measures today
- Inventory drivers and check prevalence
(compare with the knowns)
- Monitor for new registered kernel mode drivers
- Test with Atomic Red Team

Conclusion:
Hard. However,
obtainable.

<https://github.com/MHaggis/notes>



Thank you for listening

