MALICIOUS

Classifications: Backdoor | Miner | PUA

Threat Names: XMRig | App/Generic-GD | XMRig.A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**OKLA.exe**
ID	#7914161
MD5	4379963b0db3cf12eb6d98cf99309530
SHA1	63c16beb848298bee79917d07acef355ab201eab
SHA256	edc3533b754041cd2d716a3f353342264b1075e68074c010b20bee3c73cb7452
File Size	2466.74 KB
Report Created	2024-10-01 23:36 (UTC+2)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 20 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Miner, PUA
	• YARA detected "XMRig_Miner" from ruleset "PUAs" in memory dump data from (process #6) xmrig.exe. • YARA detected "XMRig_Miner" from ruleset "PUAs" in process image data from (process #1) okla.exe.			
5/5	Extracted Configuration	XMRig configuration was extracted	1	Miner
	• A configuration for XMRig was extracted from artifacts of the dynamic analysis.			
3/5	Execution	Executes code with kernel privileges	1	-
	• (Process #6) xmrig.exe executes code with kernel privileges to perform system level actions.			
3/5	Reputation	Suspicious file detected via reputation	2	-
	• Reputation analysis labels the sample itself as App/Generic-GD. • File "xmrig.exe" is a known suspicious file.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #6) xmrig.exe reads the network adapters' addresses by API.			
2/5	Execution	Sends control codes to a driver	1	-
	• (Process #6) xmrig.exe controls driver "\\.\WinRing0_1_2_0" through API DeviceIOControl.			
2/5	Anti Analysis	Creates an unusually large number of processes	1	-
	• Above average number of processes were monitored.			
2/5	Network Connection	Sets up server that accepts incoming connections	4	Backdoor
	• (Process #6) xmrig.exe starts a TCP server listening on port 49807. • (Process #6) xmrig.exe starts a TCP server listening on port 49797. • (Process #6) xmrig.exe starts a TCP server listening on port 49793. • (Process #6) xmrig.exe starts a TCP server listening on port 49802.			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task to be triggered by CALENDAR.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #6) xmrig.exe enables process privilege "SeLockMemoryPrivilege".			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #6) xmrig.exe resolves hostname "pool.hashvault.pro" to IP "95.179.241.203".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #6) xmrig.exe opens an outgoing TCP connection to host "45.76.89.70:80".			
1/5	Obfuscation	Resolves API functions dynamically	2	-

Score	Category	Operation	Count	Classification
	• (Process #1) okla.exe resolves 50 API functions by name. • (Process #6) xmrig.exe resolves 75 API functions by name.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "xmrig.exe".			
-	Trusted	Known clean file	4	-
	• Embedded file "" is a known clean file. • File "C:\windows\inf\wmiaprpl\wmiaprpl.h" is a known clean file. • File "WinRing0x64.sys" is a known clean file. • File "C:\windows\system32\wbem\performance\wmiaprpl_new.ini" is a known clean file.			

Malware Configuration: XMRig

Metadata	Key	Extracted Value
Version	Value	6.22.0
Socket	Tags Address Port Network Protocol C2	Mining Pool #0 pool.hashvault.pro 80 tcp ✔
Credential	Tags Username Password	Mining Pool #0 44nkuDevyMkUnE7Lc4kJThfZqW3zyQ62nZxB9Ca6ikxTK7SMYdLmb9eSdp3PcYDwziHMN1xyq3Yq7BNcbGXDCBhWMzEVE… TOP4

Mitre ATT&CK Matrix

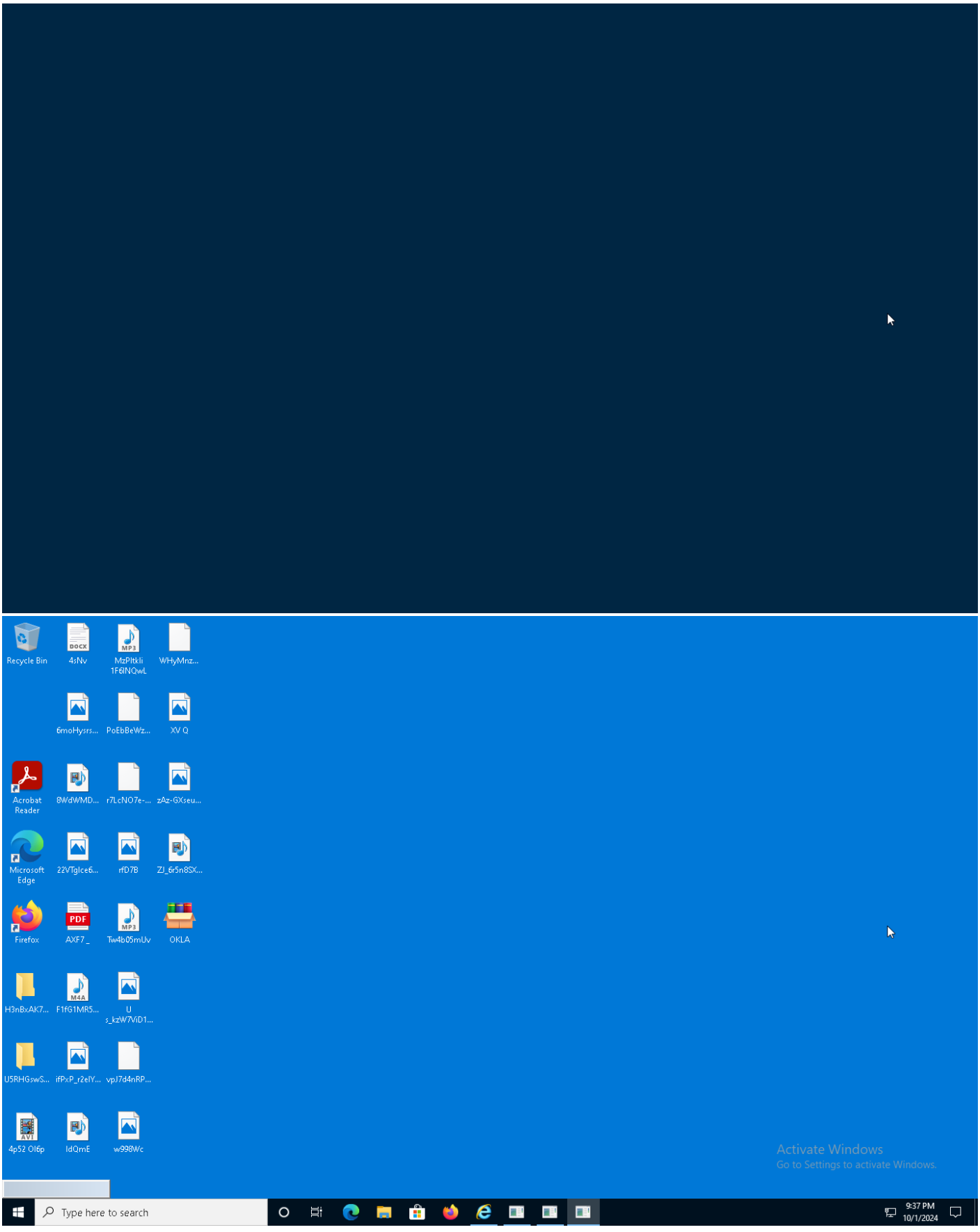
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1016 System Network Configuration Discovery			#T1071.004 DNS		
	#T1053 Scheduled Task/Job	#T1053 Scheduled Task/Job	#T1053 Scheduled Task/Job	#T1497 Virtualization/ Sandbox Evasion		#T1016 System Network Configuration Discovery			#T1095 Non-Application Layer Protocol		
				#T1027.002 Software Packing		#T1497 Virtualization/ Sandbox Evasion					

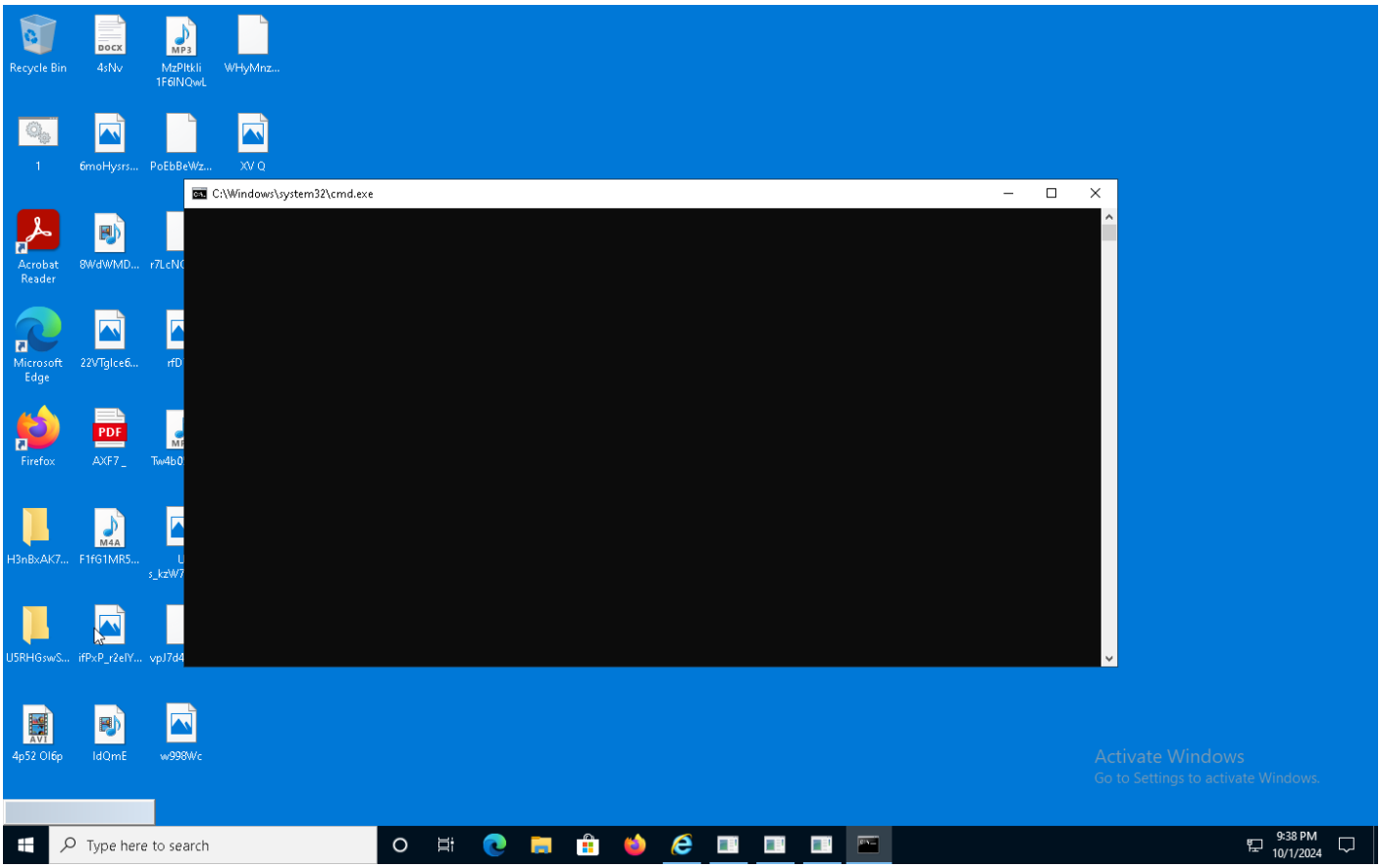
Sample Information

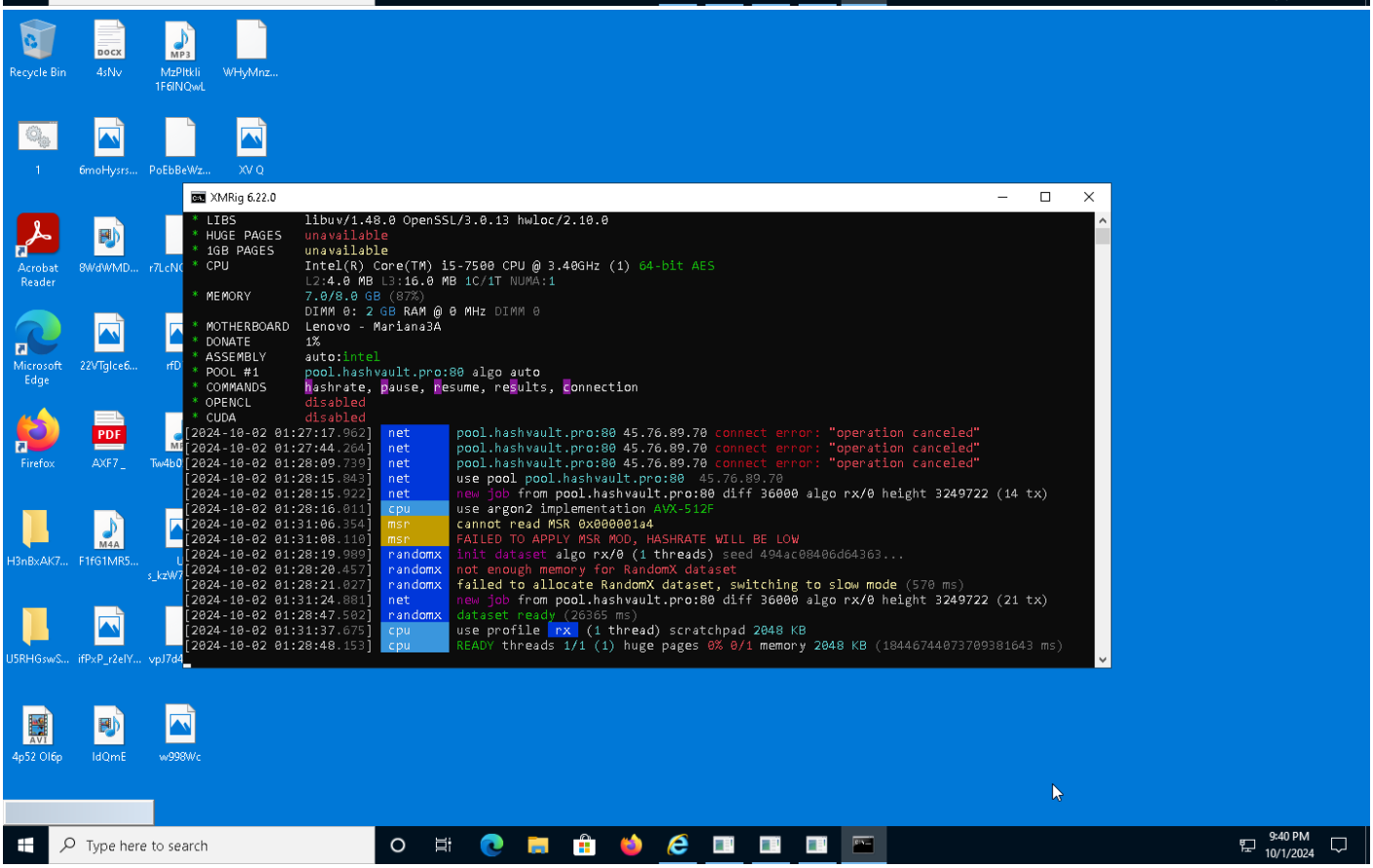
ID	#7914161
MD5	4379963b0db3cf12eb6d98cf99309530
SHA1	63c16beb848298bee79917d07acef355ab201eab
SHA256	edc3533b754041cd2d716a3f353342264b1075e68074c010b20bee3c73cb7452
SSDeep	49152:nILLyvOacuT9fbDxw6++uxp+NqiurJoP6rZ0B1qxtVujoiJ67XoifXUGOOnx:nxzfaJ+uxp+8rZ9t8JQfEQx
ImpHash	0ae9e38912ff6bd742a1b9e5c003576a
File Name	OKLA.exe
File Size	2466.74 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-10-01 23:36 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	54
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✖
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	4


Recycle Bin
4sNv
MzPltkli 1F6lNQwL
WHyMnz...
6moHysrs...
PoEbBeWz...
XV Q
Acrobat Reader
8WdWMD...
r7LcNO7e-...
zAz-GXseu...
Microsoft Edge
22VTglce6...
rfD7B
ZJ_6r5n8SX...
Firefox
AXF7 _
Tw4b05mUv
OKLA
H3nBxAK7...
F1fG1MR5...
U s_kzW7ViD1...
U5RHGswS...
ifPxP_r2elY...
vpJ7d4nRP...
4p52 Ol6p
ldQmE
w998Wc
Activate Windows
Go to Settings to activate Windows.
Type here to search
9:37 PM
10/1/2024





Screenshots truncated

NETWORK

General

1.99 KB total sent

4.58 KB total received

2 ports 80, 53

2 contacted IP addresses

1 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

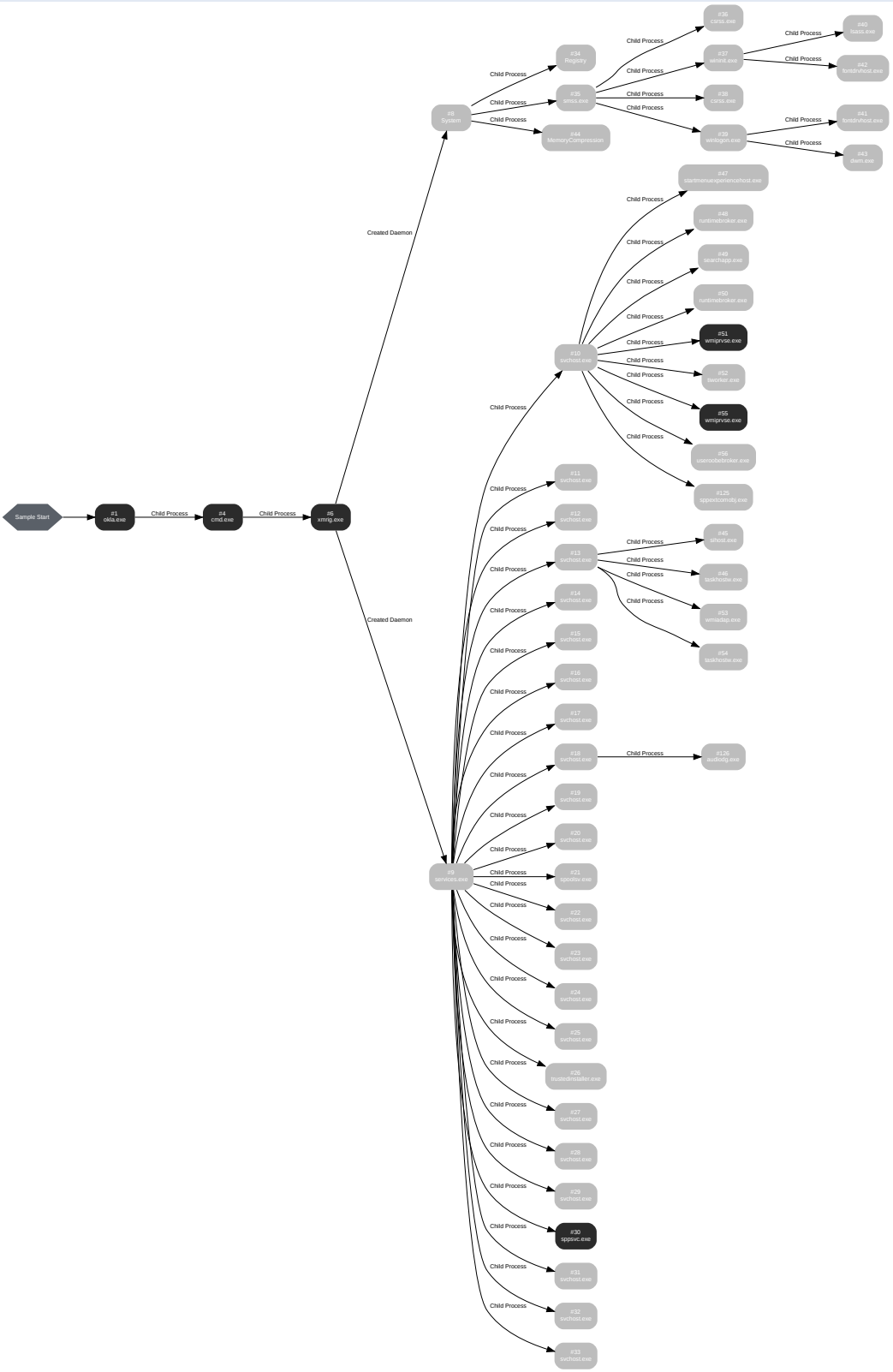
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	pool[.]hashvault[.]pro	NO_ERROR	95.179.241.203, 45.76.89.70	-	CLEAN

BEHAVIOR

Process Graph



Process #1: okla.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\okla.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\OKLA.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 110668, Reason: Analysis Target
Unmonitor End Time	End Time: 139825, Reason: Terminated
Monitor duration	29.16s
Return Code	0
PID	4548
Parent PID	-
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
	14.20 KB	11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5	✖
1.cmd	183 bytes	c0b8774d6bdb8fe949a1e03352f43f7725399171adbd12bd6d8557a9bfb2c9ad	✖
xmrig.exe	6215.00 KB	ca28f4aeaa5e16d216cd828b67454a56f3c7feeb242412d26ed914fadff20d40	✔
__tmp_rar_sfx_access_check_13795656	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	86
File	232
Environment	5
System	14
Window	2
Process	2
-	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\Users\OqXZRaykm\Desktop\1.cmd" "
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 136821, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	217.56s
Return Code	Unknown
PID	4324
Parent PID	4548
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	46
Environment	9
Process	2

Process #6: xmrig.exe

ID	6
File Name	c:\users\oqxzraykm\desktop\xmrig.exe
Command Line	xmrig --url pool.hashvault.pro:80 --user 44nkuDevyMkUnE7Lc4kJThfZqW3zyQ62nZxB9Ca6ikxTK7SMYdLmb9eSdp3PcYDwziHMN1xyq3Yq7BNcbGXDCBhWMzEVEBX --pass TOP4
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 149058, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	205.32s
Return Code	Unknown
PID	3092
Parent PID	4324
Bitness	64 Bit

Host Behavior

Type	Count
Module	131
File	88
Environment	3
System	1117
-	4
Process	1
User	2
-	2
-	6
-	1

Network Behavior

Type	Count
DNS	1
TCP	4

Process #8: System

ID	8
File Name	System
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 248034, Reason: Created Daemon
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	4
Parent PID	-
Bitness	64 Bit

Process #9: services.exe

ID	9
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Created Daemon
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	612
Parent PID	3092
Bitness	64 Bit

Process #10: svchost.exe

ID	10
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	780
Parent PID	612
Bitness	64 Bit

Process #11: svchost.exe

ID	11
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	828
Parent PID	612
Bitness	64 Bit

Process #12: svchost.exe

ID	12
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1012
Parent PID	612
Bitness	64 Bit

Process #13: svchost.exe

ID	13
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	324
Parent PID	612
Bitness	64 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	3005.56 KB	4d1dd315b78b6d3ab1a6bbd64acd522231215c4cf7e6e9356fe23672f267b4c4	✖
-	1280.00 KB	b27b2a975ad467a735c2680270c10afbbaaf04a8b38a2a5c7e369eedf457160e	✖
-	16.00 KB	cef3995a37b8c6bee82e7948fd548135b08dec35ba71e8fb40b1668df27fcecc	✖
-	768.00 KB	368434202c8c3e41feced015f7e55c16694a204689a08695684451ee98d9db74	✖

Process #14: svchost.exe

ID	14
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	52
Parent PID	612
Bitness	64 Bit

Dropped Files (11)

File Name	File Size	SHA256	YARA Match
-	68.00 KB	bf43158c8a3bfeebb7bf1066e1e6cd5ff315feb45021fa88a9e91c268930c037	✖
-	1092.00 KB	e44b9feeddca3d2ea3c08f0e39822f448226b96069a953d0d82bb73ae9ccdd22	✖
-	1028.00 KB	eb6662b420b9913a884263376b0cddac1ad9a60c8502d959235d2176241c1e0d	✖
-	1092.00 KB	b405130193b5c3e21954b931fc9c38f4d8d4cfc49a0ea0a5ed282599297f2b09	✖
-	1028.00 KB	52a36e9b8b80b0051e87dcb935a274d4d03e19df86e57b605364a58ee6b58130	✖
-	68.00 KB	79937c02c94cb6162edb647a1f29d3c6617d292f4ced22b263f93396b742a1ae	✖
-	68.00 KB	ba1b2f4cbbb9edd38138d1c183143652cac8e1bee29e7517470f7c35c5b5c316	✖
-	1092.00 KB	3d0f0e88e804ea98635b235aa732601dc2ebbf2c20738d2c1407cd5a00170d40	✖
-	1092.00 KB	700e87284bf8d632e151f8010248b1b0e4c7d75f2184504f15dd463c83798a6e	✖
-	68.00 KB	a32073074e7c98a97ad5e73cf3a923f114ab66993e9a1732ca4d40faca55d0ee	✖
-	68.00 KB	8534891ff8f28d1628a922310641fcaf6d77bcfb976bdda9fe6774eaef5e91af	✖

Process #15: svchost.exe

ID	15
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	444
Parent PID	612
Bitness	64 Bit

Process #16: svchost.exe

ID	16
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	420
Parent PID	612
Bitness	64 Bit

Process #17: svchost.exe

ID	17
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k NetworkService -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1248
Parent PID	612
Bitness	64 Bit

Process #18: svchost.exe

ID	18
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1504
Parent PID	612
Bitness	64 Bit

Process #19: svchost.exe

ID	19
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1624
Parent PID	612
Bitness	64 Bit

Process #20: svchost.exe

ID	20
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1644
Parent PID	612
Bitness	64 Bit

Process #21: spoolsv.exe

ID	21
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1776
Parent PID	612
Bitness	64 Bit

Process #22: svchost.exe

ID	22
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	1796
Parent PID	612
Bitness	64 Bit

Process #23: svchost.exe

ID	23
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	2068
Parent PID	612
Bitness	64 Bit

Process #24: svchost.exe

ID	24
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	2304
Parent PID	612
Bitness	64 Bit

Process #25: svchost.exe

ID	25
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	2816
Parent PID	612
Bitness	64 Bit

Process #26: trustedinstaller.exe

ID	26
File Name	c:\windows\servicing\trustedinstaller.exe
Command Line	C:\Windows\servicing\TrustedInstaller.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	4012
Parent PID	612
Bitness	64 Bit

Process #27: svchost.exe

ID	27
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	2536
Parent PID	612
Bitness	64 Bit

Process #28: svchost.exe

ID	28
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k NetworkService -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 326796, Reason: Terminated
Monitor duration	78.76s
Return Code	0
PID	2156
Parent PID	612
Bitness	64 Bit

Process #29: svchost.exe

ID	29
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k wsappx -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	3584
Parent PID	612
Bitness	64 Bit

Process #30: sppsvc.exe

ID	30
File Name	c:\windows\system32\sppsvc.exe
Command Line	C:\Windows\system32\sppsvc.exe
Initial Working Directory	C:\Windows
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 265336, Reason: Terminated
Monitor duration	17.30s
Return Code	0
PID	2128
Parent PID	612
Bitness	64 Bit

Host Behavior

Type	Count
System	385

Process #31: svchost.exe

ID	31
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k wusvcs -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 282914, Reason: Terminated
Monitor duration	34.88s
Return Code	0
PID	1032
Parent PID	612
Bitness	64 Bit

Process #32: svchost.exe

ID	32
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	3388
Parent PID	612
Bitness	64 Bit

Process #33: svchost.exe

ID	33
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248034, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.34s
Return Code	Unknown
PID	5504
Parent PID	612
Bitness	64 Bit

Process #34: Registry

ID	34
File Name	-
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	72
Parent PID	-
Bitness	64 Bit

Process #35: smss.exe

ID	35
File Name	c:\windows\system32\smss.exe
Command Line	\SystemRoot\System32\smss.exe
Initial Working Directory	C:\Windows
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	356
Parent PID	4
Bitness	64 Bit

Process #36: csrss.exe

ID	36
File Name	c:\windows\system32\csrss.exe
Command Line	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	452
Parent PID	-
Bitness	64 Bit

Process #37: wininit.exe

ID	37
File Name	c:\windows\system32\wininit.exe
Command Line	wininit.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	520
Parent PID	-
Bitness	64 Bit

Process #38: csrss.exe

ID	38
File Name	c:\windows\system32\csrss.exe
Command Line	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	528
Parent PID	-
Bitness	64 Bit

Process #39: winlogon.exe

ID	39
File Name	c:\windows\system32\winlogon.exe
Command Line	winlogon.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	588
Parent PID	-
Bitness	64 Bit

Process #40: lsass.exe

ID	40
File Name	c:\windows\system32\lsass.exe
Command Line	C:\Windows\system32\lsass.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248293, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.09s
Return Code	Unknown
PID	620
Parent PID	520
Bitness	64 Bit

Process #41: fontdrvhost.exe

ID	41
File Name	c:\windows\system32\fontdrvhost.exe
Command Line	"fontdrvhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	712
Parent PID	588
Bitness	64 Bit

Process #42: fontdrvhost.exe

ID	42
File Name	c:\windows\system32\fontdrvhost.exe
Command Line	"fontdrvhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	720
Parent PID	520
Bitness	64 Bit

Process #43: dwm.exe

ID	43
File Name	c:\windows\system32\dwm.exe
Command Line	"dwm.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	916
Parent PID	588
Bitness	64 Bit

Process #44: Memory Compression

ID	44
File Name	-
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	1360
Parent PID	4
Bitness	64 Bit

Process #45: sihost.exe

ID	45
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	2288
Parent PID	324
Bitness	64 Bit

Process #46: taskhostw.exe

ID	46
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	2376
Parent PID	324
Bitness	64 Bit

Process #47: startmenuexperiencehost.exe

ID	47
File Name	c:\windows\systemapps\microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy\startmenuexperiencehost.exe
Command Line	"C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
Initial Working Directory	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	2628
Parent PID	780
Bitness	64 Bit

Process #48: runtimebroker.exe

ID	48
File Name	c:\windows\system32\runtimebroker.exe
Command Line	C:\Windows\System32\RuntimeBroker.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	2256
Parent PID	780
Bitness	64 Bit

Process #49: searchapp.exe

ID	49
File Name	c:\windows\systemapps\microsoft.windows.search_cw5n1h2txyewy\searchapp.exe
Command Line	"C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca
Initial Working Directory	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	3156
Parent PID	780
Bitness	64 Bit

Process #50: runtimebroker.exe

ID	50
File Name	c:\windows\system32\runtimebroker.exe
Command Line	C:\Windows\System32\RuntimeBroker.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	3252
Parent PID	780
Bitness	64 Bit

Process #51: wmiprvse.exe

ID	51
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	3756
Parent PID	780
Bitness	64 Bit

Process #52: tiworker.exe

ID	52
File Name	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.153_none_e74acfe72624a02b\tiworker.exe
Command Line	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.153_none_e74acfe72624a02b\TiWorker.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	4048
Parent PID	780
Bitness	64 Bit

Process #53: wmiadap.exe

ID	53
File Name	c:\windows\system32\wbem\wmiadap.exe
Command Line	wmiadap.exe /F /T /R
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 321707, Reason: Terminated
Monitor duration	73.41s
Return Code	0
PID	628
Parent PID	324
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	3.36 KB	ae2b6236d3eeb4822835714ae9444e5dcd21bc60f7a909f2962c43bc743c7b15	✖
-	29.04 KB	c20b11dff802aa472265f4e9f330244ec4aca81b0009f6efcb2cf8a36086f390	✖
-	777.09 KB	34d047689cb731eead66c75e1daf1f2e0c6fd68155dd53dfd4fc352c39a4aa81	✖

Process #54: taskhostw.exe

ID	54
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe None
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	3064
Parent PID	324
Bitness	64 Bit

Process #55: wmiprvse.exe

ID	55
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	3696
Parent PID	780
Bitness	64 Bit

Host Behavior

Type	Count
Module	31
Registry	2

Process #56: useroobebroker.exe

ID	56
File Name	c:\windows\system32\oobe\useroobebroker.exe
Command Line	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	2748
Parent PID	780
Bitness	64 Bit

Process #125: sppextcomobj.exe

ID	125
File Name	c:\windows\system32\sppextcomobj.exe
Command Line	C:\Windows\system32\SppExtComObj.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 265250, Reason: Terminated
Monitor duration	16.96s
Return Code	0
PID	5536
Parent PID	780
Bitness	64 Bit

Process #126: audiodg.exe

ID	126
File Name	c:\windows\system32\audiodg.exe
Command Line	C:\Windows\system32\AUDIODG.EXE 0x374 0x378
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 248294, Reason: Child Process
Unmonitor End Time	End Time: 354379, Reason: Terminated by timeout
Monitor duration	106.08s
Return Code	Unknown
PID	5816
Parent PID	1504
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
edc3533b754041cd2d716a3f353342264b1075e68074c010b20bee3c73cb7452	C:\Users\OqXZRaykm\Desktop\OKLA.exe	Sample File	2466.74 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
ca28f4aeaa5e16d216cd828b67454a56f3c7feeb242412d26ed914fadff20d40	xmrig.exe, C:\Users\OqXZRaykm\Desktop\xmrig.exe, \\?\C:\Users\OqXZRaykm\Desktop\xmrig.exe	Dropped File	6215.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
3f3c4ecbfab6fb2f0db4325aa408f34548402c403d85ec7074c06093df9ae516	-	Memory Dump	8924.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
fc9dedc2c6e64d9a2d075e05ca18677819b88965582e37bfe11dc39aab961a00	-	Memory Dump	8924.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
fce99ad24b5391ff61e7b9b89b78a25f7a012afd733d95493121eb6741e70888	-	Memory Dump	8924.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a91f4373ceebadfc70b3bd0758848918f928c3c76562e3d9d531574796fd9e9c	-	Extracted File	2.82 KB	image/png	-	CLEAN
27d3a1a2da49dc535cc10806abaae9dfa49e4f5f44a40540ead50e065b99ca68	-	Extracted File	5.42 KB	image/png	-	CLEAN
6f86849b026f0c45c0c8a1145048960bbdefdaea3beac030f114b1ff16057994	-	Extracted File	15.36 KB	image/png	-	CLEAN
c0b8774d6bdb8fe949a1e03352f43f7725399171adbd12bd6d8557a9bfb2c9ad	1.cmd, C:\Users\OqXZRaykm\Desktop\1.cmd, \\?\C:\Users\OqXZRaykm\Desktop\1.cmd	Dropped File	183 bytes	text/x-msdos-batch	Access, Create, Read, Write	CLEAN
11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5	, WinRing0x64.sys, \\?\C:\Users\OqXZRaykm\Desktop\WinRing0x64.sys	Dropped File	14.20 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
1027b3001f02a641e63f0f8890d8c241a96ad9f9b6f51ac18f1708e0b9b153e2	-	Extracted File	6.25 KB	image/png	-	CLEAN
1c3bb1a35e8514323bd820b6e04969b5e4b5a593e977ef626b1da3eb6a672a31	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask	Modified File	4.57 KB	text/xml	-	CLEAN
f55911caf9f7fcebaef124d63942a6753027370ec04f8842485505c71761af71	c:\programdata\microsoft\network\downloader\edb.chk	Modified File	8.00 KB	application/octet-stream	-	CLEAN
f4ccb76f8aa67b88212ad905153cfd4f7432c326a453eadf6f458c8ba6dbb913	c:\programdata\microsoft\network\downloader\edb.chk	Modified File	8.00 KB	application/octet-stream	-	CLEAN
368434202c8c3e41feced015f7e55c16694a204689a08695684451ee98d9db74	c:\programdata\microsoft\network\downloader\qmgr.db	Dropped File	768.00 KB	application/x-ms-ese	-	CLEAN
cef3995a37b8c6bee82e7948fd548135b08dec35ba71e8fb40b1668df27fcecc	c:\programdata\microsoft\network\downloader\qmgr.jfm	Dropped File	16.00 KB	application/octet-stream	-	CLEAN
278a78e763bf40bf51eea886688c19e71959b93205a42721fd1efc18a0117394	c:\programdata\microsoft\network\downloader\edb.chk	Modified File	8.00 KB	application/octet-stream	-	CLEAN
b27b2a975ad467a735c2680270c10afbbaaf04a8b38a2a5c7e369eedf457160e	c:\programdata\microsoft\network\downloader\edb.log	Dropped File	1280.00 KB	application/octet-stream	-	CLEAN
c20b11dff802aa472265f4e9f330244ec4aca81b0009f6efcb2cf8a36086f390	c:\windows\inf\wmiaprpl\wmiaprpl.ini, c:\windows\system32\wbem\performance\wmiaprpl_new.ini, c:\windows\system32\wbem\performance\wmiaprpl.ini	Dropped File	29.04 KB	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5d8988f2bcf7284cd96510e6735d7be5371103a83c85d04168d01f793becc960	c:\windows\system32\perfc009.dat	Modified File	118.55 KB	application/octet-stream	-	CLEAN
a4bbd4981bf03910e2a7ab2e87bd8b3415afbf371b56dd04ead9a4e6d9e10668	c:\windows\system32\perfh009.dat	Modified File	646.34 KB	application/octet-stream	-	CLEAN
ae2b6236d3eeb4822835714ae9444e5dcd21bc60f7a909f2962c43bc743c7b15	c:\windows\inf\wmiaprpl\wmiaprpl.h	Dropped File	3.36 KB	text/plain	-	CLEAN
34d047689cb731eead66c75e1daf1f2e0c6fd68155dd53dfd4fc352c39a4aa81	c:\windows\system32\perfstringbackup.ini, c:\windows\system32\perfstringbackup.tmp	Dropped File	777.09 KB	application/octet-stream	-	CLEAN
a57660cb5ec3beec908ee2fb8cbafded9afb23bd91d0273ccf31f17fe206ef1f	c:\windows\system32\perfc009.dat	Modified File	122.48 KB	application/octet-stream	-	CLEAN
b072e19af57494727c1fa78e2e6bd8fea07567b6d570fb1fba52e311736b5779	c:\windows\system32\perfh009.dat	Modified File	659.38 KB	application/octet-stream	-	CLEAN
e44b9feeddca3d2ea3c08f0e39822f448226b96069a953d0d82bb73ae9ccdd22	c:\windows\system32\winevt\logs\system.evtx	Dropped File	1092.00 KB	application/octet-stream	-	CLEAN
bf43158c8a3bfeebb7bf1066e1e6cd5ff315feb45021fa88a9e91c268930c037	c:\windows\system32\winevt\logs\microsoft-windows-security-spp-ux-notifications%4actioncenter.evtx	Dropped File	68.00 KB	application/octet-stream	-	CLEAN
79937c02c94cb6162edb647a1f29d3c6617d292f4ced22b263f93396b742a1ae	c:\windows\system32\winevt\logs\microsoft-windows-taskscheduler%4maintenance.evtx	Dropped File	68.00 KB	application/octet-stream	-	CLEAN
eb6662b420b9913a884263376b0cddac1ad9a60c8502d959235d2176241c1e0d	c:\windows\system32\winevt\logs\microsoft-windows-wmi-activity%4operational.evtx	Dropped File	1028.00 KB	application/octet-stream	-	CLEAN
b405130193b5c3e21954b931fc9c38f4d8d4cfc49a0ea0a5ed282599297f2b09	c:\windows\system32\winevt\logs\application.evtx	Dropped File	1092.00 KB	application/octet-stream	-	CLEAN
4d1dd315b78b6d3ab1a6bbd64acd522231215c4cf7e6e9356fe23672f267b4c4	c:\windows\system32\config\systemprofile\appdata\local\microsoft\windows\notifications\wpndatabase.db-wal	Dropped File	3005.56 KB	application/octet-stream	-	CLEAN
700e87284bf8d632e151f8010248b1b0e4c7d75f2184504f15dd463c83798a6e	c:\windows\system32\winevt\logs\microsoft-windows-storage-storport%4operational.evtx	Dropped File	1092.00 KB	application/octet-stream	-	CLEAN
8534891ff8f28d1628a922310641fcaf6d77bcfb976bdda9fe6774eaef5e91af	c:\windows\system32\winevt\logs\microsoft-windows-kernel-pnp%4driverwatchdog.evtx	Dropped File	68.00 KB	application/octet-stream	-	CLEAN
3d0f0e88e804ea98635b235aa732601dc2ebbf2c20738d2c1407cd5a00170d40	c:\windows\system32\winevt\logs\microsoft-windows-storage-storport%4health.evtx	Dropped File	1092.00 KB	application/octet-stream	-	CLEAN
52a36e9b8b80b0051e87dcb935a274d4d03e19df86e57b605364a58ee6b58130	c:\windows\system32\winevt\logs\microsoft-windows-wcmsvc%4operational.evtx	Dropped File	1028.00 KB	application/octet-stream	-	CLEAN
ba1b2f4cbbb9edd38138d1c183143652cac8e1bee29e7517470f7c35c5b5c316	c:\windows\system32\winevt\logs\microsoft-windows-diagnosis-dps%4operational.evtx	Dropped File	68.00 KB	application/octet-stream	-	CLEAN
a32073074e7c98a97ad5e73cf3a923f114ab66993e9a1732ca4d40faca55d0ee	c:\windows\system32\winevt\logs\microsoft-windows-resource-exhaustion-detector%4operational.evtx	Dropped File	68.00 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\OKLA.exe	Accessed File, Sample File	Access, Read	MALICIOUS

File Name	Category	Operations	Verdict
__tmp_rar_sfx_access_check_13795656	Accessed File, Dropped File	Access, Create, Delete	CLEAN
1.cmd	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
-	Accessed File, Dropped File	Access, Create, Write	CLEAN
xmrig.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask	Modified File	-	CLEAN
c:\programdata\microsoft\network\downloader\edb.chk	Modified File	-	CLEAN
c:\programdata\microsoft\network\downloader\qmgr.db	Dropped File	-	CLEAN
c:\programdata\microsoft\network\downloader\qmgr.jfm	Dropped File	-	CLEAN
c:\programdata\microsoft\network\downloader\edb.log	Dropped File	-	CLEAN
c:\windows\system32\wbem\performance\wmiaprpl_new.ini	Dropped File	-	CLEAN
c:\windows\system32\wbem\performance\wmiaprpl.ini	Dropped File	-	CLEAN
c:\windows\system32\perfc009.dat	Modified File	-	CLEAN
c:\windows\system32\perfh009.dat	Modified File	-	CLEAN
c:\windows\inf\wmiaprpl\wmiaprpl.h	Dropped File	-	CLEAN
c:\windows\inf\wmiaprpl\wmiaprpl.ini	Dropped File	-	CLEAN
c:\windows\system32\perfstringbackup.tmp	Dropped File	-	CLEAN
c:\windows\system32\perfstringbackup.ini	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\system.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-security-spp-ux-notifications%4actioncenter.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-taskscheduler%4maintenance.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-wmi-activity%4operational.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\application.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\config\systemprofile\appdata\local\microsoft\windows\notifications\wpndatabase.db-wal	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-storage-storport%4operational.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-kernel-pnp%4driver watchdog.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-storage-storport%4health.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-wcmsvc%4operational.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-diagnosis-dps%4operational.evtx	Dropped File, Modified File	-	CLEAN
c:\windows\system32\winevt\logs\microsoft-windows-resource-exhaustion-detector%4operational.evtx	Dropped File, Modified File	-	CLEAN
C:\Users\OqXZRaykm\Desktop\DXGIDebug.dll	Accessed File	Access	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN
C:\Users\OqXZRaykm	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop	Accessed File	Access, Create	CLEAN
"C:\Users\OqXZRaykm\Desktop\1.cmd"	Accessed File	Access	CLEAN
CONOUT$	Accessed File	Access	CLEAN
C:\Program Files\Common Files\SSL/openssl.cnf	Accessed File	Access	CLEAN
\\.\WinRing0_1_2_0	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wmiprvse.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://pool[.]hashvault[.]pro	Extracted	95.179.241.203, 45.76.89.70	Germany	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
pool[.]hashvault[.]pro	95.179.241.203, 45.76.89.70	Germany	TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.76.89.70	pool[.]hashvault[.]pro	Germany	TCP, DNS	CLEAN
95.179.241.203	pool[.]hashvault[.]pro	Germany	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\LogFlags	read, access	wmiprvse.exe	CLEAN

Process

Process Name	Commandline	Verdict
okla.exe	"C:\Users\OqXZRaykm\Desktop\OKLA.exe"	MALICIOUS
xmrig.exe	xmrig --url pool.hashvault.pro:80 --user 44nkuDevyMkUnE7Lc4kJThfZqW3zyQ62nZxB9Ca6ikxTK7SMYdLmb9eSdp3PcYDwziHMN1xyq3Yq7BNcbGXDCBhWMzEVEBX --pass TOP4	MALICIOUS
sppsvc.exe	C:\Windows\system32\sppsvc.exe	SUSPICIOUS
Registry	-	CLEAN
System	-	CLEAN
smss.exe	\SystemRoot\System32\smss.exe	CLEAN
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	CLEAN
wininit.exe	wininit.exe	CLEAN
csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	CLEAN
winlogon.exe	winlogon.exe	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN

Process Name	Commandline	Verdict
lsass.exe	C:\Windows\system32\lsass.exe	CLEAN
fontdrvhost.exe	"fontdrvhost.exe"	CLEAN
fontdrvhost.exe	"fontdrvhost.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS -p	CLEAN
dwm.exe	"dwm.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService -p	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k NetworkService -p	CLEAN
Memory Compression	-	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	CLEAN
sihost.exe	sihost.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	CLEAN
taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	CLEAN
startmenuexperiencehost.exe	"C: \Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca	CLEAN
runtimebroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	CLEAN
searchapp.exe	"C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca	CLEAN
runtimebroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding	CLEAN
sppextcomobj.exe	C:\Windows\system32\SppExtComObj.exe -Embedding	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
trustedinstaller.exe	C:\Windows\servicing\TrustedInstaller.exe	CLEAN
tiworker.exe	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.153_none_e74acfe72624a02b\TiWorker.exe -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p	CLEAN
audiodg.exe	C:\Windows\system32\AUDIODG.EXE 0x374 0x378	CLEAN

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\System32\svchost.exe -k NetworkService -p	CLEAN
wmiadap.exe	wmiadap.exe /F /T /R	CLEAN
taskhostw.exe	taskhostw.exe None	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\OqXZRaykm\Desktop\1.cmd" "	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k wsappx -p	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	CLEAN
useroobebroker.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k wusvcs -p	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	CLEAN

YARA / AV

YARA (4)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Dropped File	xmrig.exe	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	windows 10 (64bit 20H1 -EN-)
Architecture	x86 64-bit
Operating System	Windows 10 20H1
Kernel Version	10.0.19041.208 (dc9233f8-5819-e3d0-929a-7bde0b87f0b9)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.4.1
Dynamic Engine Version	2024.4.1 / 09/02/2024 04:30
Static Engine Version	2024.4.1.0 / 2024-09-02 03:01:08
AV Exceptions Version	2024.4.1.3 / 2024-08-31 15:08:44
Link Detonation Heuristics Version	2024.4.1.12 / 2024-09-19 15:05:45
Smart Memory Dumping Rules Version	2024.4.1.3 / 2024-08-31 15:08:44
Config Extractors Version	2024.4.1.13 / 2024-09-26 16:17:01
Signature Trust Store Version	2024.4.1.3 / 2024-08-31 15:08:44
VMRay Threat Identifiers Version	2024.4.1.13 / 2024-09-26 16:17:01
YARA Built-in Ruleset Version	2024.4.1.13

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.207.19041.0
Chrome Version	Not installed
Firefox Version	108.0
Flash Version	Not installed
Java Version	8.0.3610.9

System Information

Sample Directory	C:\Users\OqXZRaykm\Desktop
Computer Name	PXTHFFRYO7
User Domain	PXTHFFRYO7
User Name	OqXZRaykm
User Profile	C:\Users\OqXZRaykm
Temp Directory	C:\Users\OQXZRA~1\AppData\Local\Temp

System Root	C:\Windows