MALICIOUS

Classifications: -

Threat Names: Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**L6lPO0G6AZQT4KWU.exe**
ID	#10321196
MD5	1b4a6ef2016871752a20acd5988e18b8
SHA1	509f8ed40fd772e1b5705092cae6749da9defe41
SHA256	005802da1bc8ec882fe467078704f2fb32975ce8538b3d7c3422b1cfb87bb334
File Size	1843.50 KB
Report Created	2024-04-28 14:59 (UTC+2)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 54 matches)

Score	Category	Operation	Count	Classification
5/5	Anti Analysis	Makes indirect system call to possibly evade hooking based monitoring	2	-
	• (Process #1) l6lpo0g6azqt4kwu.exe makes an indirect system call to "NtQueryInformationProcess". • (Process #5) explorta.exe makes an indirect system call to "NtQueryInformationProcess".			
4/5	Reputation	Malicious host or URL detected via reputation	1	-
	• Reputation analysis labels the URL "hxxp://193[.]233[.]132[.]139/sev56rkm/index.php" which was contacted by (process #5) explorta.exe as Mal/HTMLGen-A.			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #1) l6lpo0g6azqt4kwu.exe hides thread via API "NtSetInformationThread".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	11	-
	• (Process #5) explorta.exe tries to detect Avast by file artifact. • (Process #5) explorta.exe tries to detect Avira by file artifact. • (Process #5) explorta.exe tries to detect Kaspersky by file artifact. • (Process #5) explorta.exe tries to detect ESET by file artifact. • (Process #5) explorta.exe tries to detect Panda by file artifact. • (Process #5) explorta.exe tries to detect AVG by file artifact. • (Process #5) explorta.exe tries to detect 360TotalSecurity by file artifact. • (Process #5) explorta.exe tries to detect Bitdefender by file artifact. • (Process #5) explorta.exe tries to detect Norton by file artifact. • (Process #5) explorta.exe tries to detect Sophos by file artifact. • (Process #5) explorta.exe tries to detect Comodo by file artifact.			
3/5	Anti Analysis	Modifies native system functions	1	-
	• (Process #1) l6lpo0g6azqt4kwu.exe modifies native system functions, possibly to evade hooking.			
2/5	Anti Analysis	Tries to detect virtual machine	5	-
	• (Process #1) l6lpo0g6azqt4kwu.exe reads out system information, commonly used to detect "VirtualBox" via registry. (Key is "HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__"). • (Process #5) explorta.exe reads out system information, commonly used to detect "VirtualBox" via registry. (Key is "HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__"). • (Process #10) explorta.exe reads out system information, commonly used to detect "VirtualBox" via registry. (Key is "HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__"). • (Process #1) l6lpo0g6azqt4kwu.exe is possibly trying to detect a VM via rdtsc. • Tries to detect VirtualPC via vpcext instruction at "0xb073f0f".			
2/5	Anti Analysis	Tries to detect debugger	12	-

Score	Category	Operation	Count	Classification
		• (Process #1) l6lpo0g6azqt4kwu.exe tries to detect debugger by checking for existence of window class "OLLYDBG". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect debugger by checking for existence of window class "GBDYLLO". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect debugger by checking for existence of window class "pediy06". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect a debugger via API "NtQueryInformationProcess". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect a debugger via API "IsDebuggerPresent". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent". • (Process #5) explorta.exe tries to detect debugger by checking for existence of window class "OLLYDBG". • (Process #5) explorta.exe tries to detect debugger by checking for existence of window class "GBDYLLO". • (Process #5) explorta.exe tries to detect debugger by checking for existence of window class "pediy06". • (Process #10) explorta.exe tries to detect debugger by checking for existence of window class "OLLYDBG". • (Process #10) explorta.exe tries to detect debugger by checking for existence of window class "GBDYLLO". • (Process #10) explorta.exe tries to detect debugger by checking for existence of window class "pediy06".		
2/5	Anti Analysis	Tries to detect a forensic tool	6	-
		• (Process #1) l6lpo0g6azqt4kwu.exe tries to detect forensic tool by checking for existence of window name "File Monitor - Sysinternals: www.sysinternals.com". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect forensic tool by checking for existence of window name "Process Monitor - Sysinternals: www.sysinternals.com". • (Process #1) l6lpo0g6azqt4kwu.exe tries to detect forensic tool by checking for existence of window name "Registry Monitor - Sysinternals: www.sysinternals.com". • (Process #5) explorta.exe tries to detect forensic tool by checking for existence of window name "File Monitor - Sysinternals: www.sysinternals.com". • (Process #5) explorta.exe tries to detect forensic tool by checking for existence of window name "Process Monitor - Sysinternals: www.sysinternals.com". • (Process #5) explorta.exe tries to detect forensic tool by checking for existence of window name "Registry Monitor - Sysinternals: www.sysinternals.com".		
2/5	Anti Analysis	Delays execution	2	-
		• (Process #1) l6lpo0g6azqt4kwu.exe has a thread which sleeps more than 5 minutes. • (Process #5) explorta.exe has a thread which sleeps more than 5 minutes.		
2/5	Discovery	Queries a host's domain name	1	-
		• (Process #5) explorta.exe queries the host's domain name.		
2/5	Task Scheduling	Schedules task	1	-
		• Schedules task for command "C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.		
1/5	Discovery	Enumerates running processes	3	-
		• (Process #1) l6lpo0g6azqt4kwu.exe enumerates running processes. • (Process #5) explorta.exe enumerates running processes. • (Process #10) explorta.exe enumerates running processes.		
1/5	Mutex	Creates mutex	2	-
		• (Process #1) l6lpo0g6azqt4kwu.exe creates mutex with name "006700e5a2ab05704bbb0c589b88924d". • (Process #5) explorta.exe creates mutex with name "006700e5a2ab05704bbb0c589b88924d".		
1/5	Hide Tracks	Creates process with hidden window	1	-
		• (Process #1) l6lpo0g6azqt4kwu.exe starts (process #5) explorta.exe with a hidden window.		
1/5	Network Connection	Downloads file	1	-
		• (Process #5) explorta.exe downloads file via http from hxxp://193[.]233[.]132[.]139/sev56rkm/index.php.		
1/5	Obfuscation	Obfuscates control flow	1	-
		• Modifies exception handler (e.g., the instruction pointer is modified within an exception handler filter).		

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Overwrites code	3	-
	• (Process #1) l6lpo0g6azqt4kwu.exe overwrites code to possibly hide behavior. • (Process #10) explorta.exe overwrites code to possibly hide behavior. • (Process #5) explorta.exe overwrites code to possibly hide behavior.			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

Mitre ATT&CK Matrix

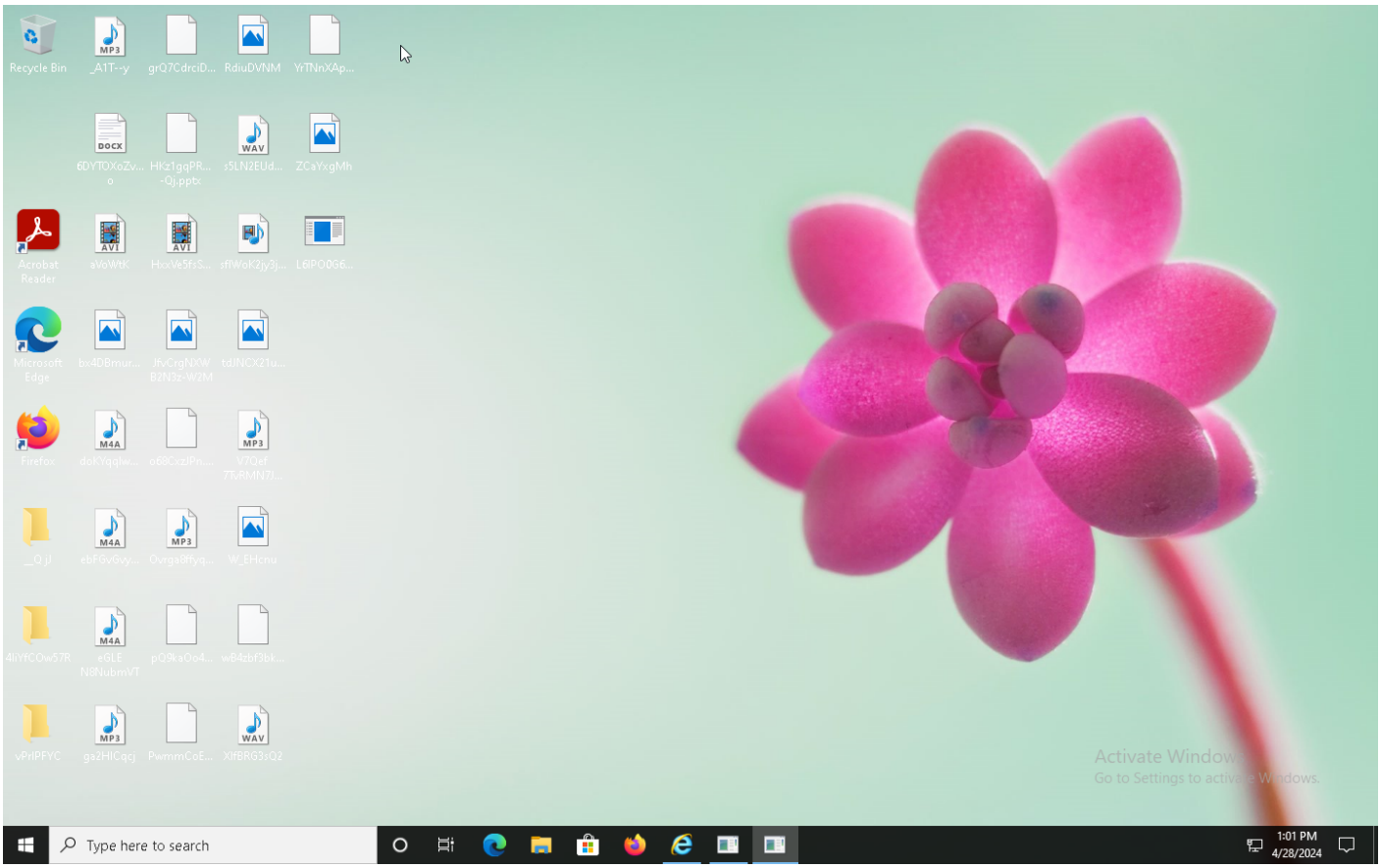
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
				#T1143 Hidden Window		#T1012 Query Registry			#T1105 Remote File Copy		
				#T1045 Software Packing		#T1010 Application Window Discovery					
				#T1027 Obfuscated Files or Information		#T1057 Process Discovery					
						#T1063 Security Software Discovery					
						#T1124 System Time Discovery					

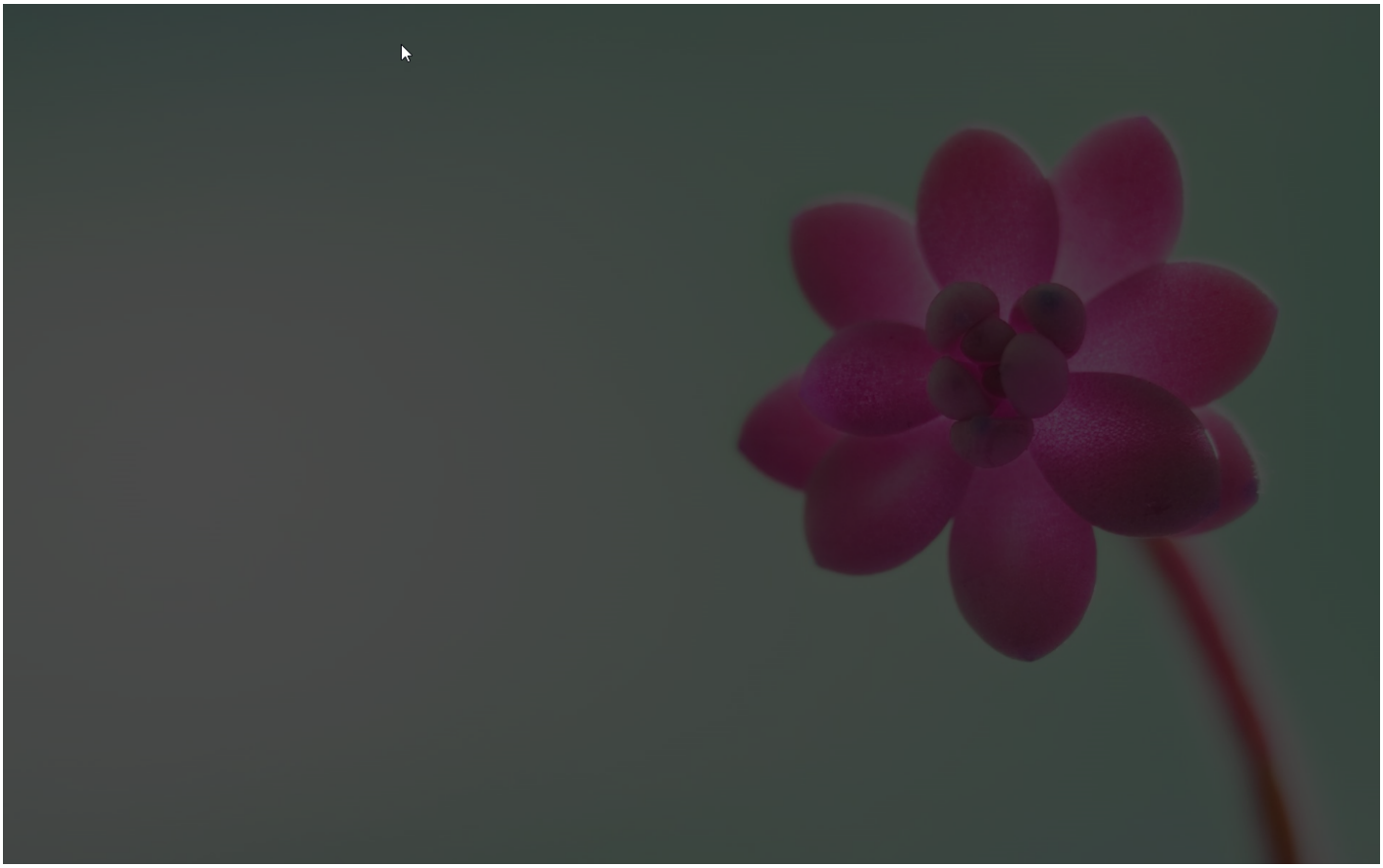
Sample Information

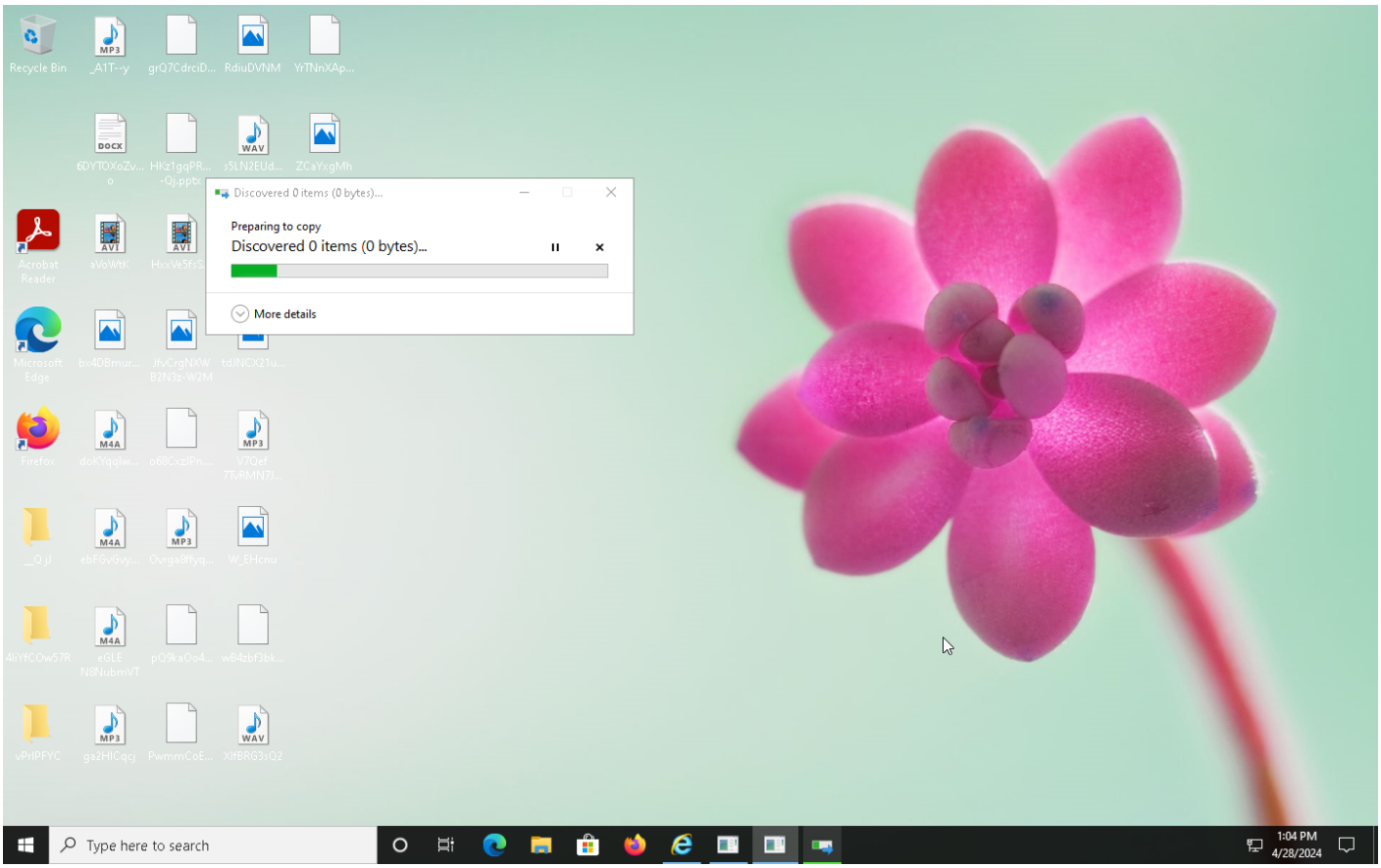
ID	#10321196
MD5	1b4a6ef2016871752a20acd5988e18b8
SHA1	509f8ed40fd772e1b5705092cae6749da9defe41
SHA256	005802da1bc8ec882fe467078704f2fb32975ce8538b3d7c3422b1cfb87bb334
SSDeep	49152:53/bnYpE7B2FmPv1WRiLZgSCz6sneXTcjpAbH/:5jnYpE7BMIGitgSCG8niT
ImpHash	2eabe9054cad5152567f0699947a2c5b
File Name	L6lPO0G6AZQT4KWU.exe
File Size	1843.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-04-28 14:59 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	5
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	0


Recycle Bin
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
1:01 PM
4/28/2024




Recycle Bin
Discovered 0 items (0 bytes)...
Preparing to copy
Discovered 0 items (0 bytes)...
More details
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
1:04 PM
4/28/2024

NETWORK

General

734 bytes total sent

627 bytes total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

4 files downloaded

1 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

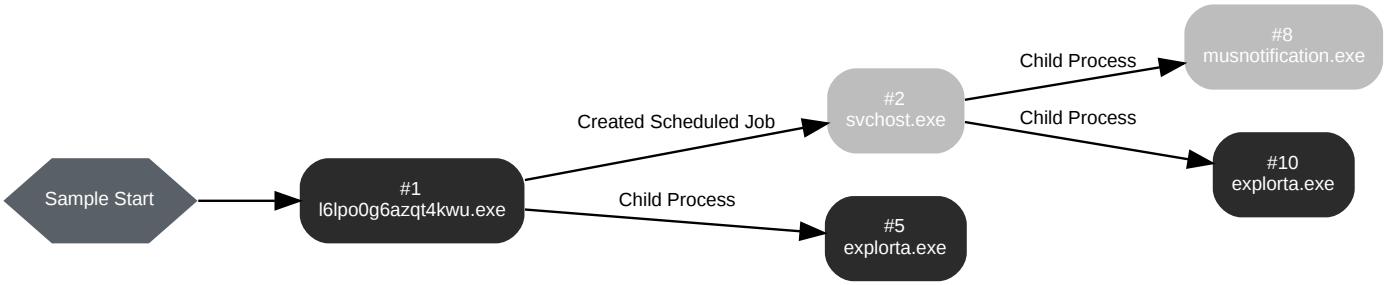
1 sessions, 1.43 KB sent, 1.22 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://193[.]233[.]132[.]139/sev56rkm/index.php	-	-	-	0 bytes	MALICIOUS

BEHAVIOR

Process Graph



Process #1: l6lpo0g6azqt4kwu.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\l6lpo0g6azqt4kwu.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\L6lPO0G6AZQT4KWU.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 120541, Reason: Analysis Target
Unmonitor End Time	End Time: 276830, Reason: Terminated
Monitor duration	156.29s
Return Code	0
PID	5552
Parent PID	-
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	306 bytes	33ef2eef1c2b8525d6e3e9213ed2519cfe8314508ad8b7f66381e847868b0a93	✖
C:\Users\OqXZRaykm\Desktop\L6lPO0G6AZQT4KWU.exe	1843.50 KB	005802da1bc8ec882fe467078704f2fb32975ce8538b3d7c3422b1cfb87bb334	✖

Host Behavior

Type	Count
Module	87
System	4268
File	15
Registry	14
-	17
-	222
Window	831
Process	5
Environment	1
Mutex	1
COM	1

Process #2: svchost.exe

ID	2
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: 243870, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 365687, Reason: Terminated by timeout
Monitor duration	121.82s
Return Code	Unknown
PID	8
Parent PID	5552
Bitness	64 Bit

Process #5: explorta.exe

ID	5
File Name	c:\users\oqxzraykm\appdata\local\temp\5454e6f062\explorta.exe
Command Line	"C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 270312, Reason: Child Process
Unmonitor End Time	End Time: 365687, Reason: Terminated by timeout
Monitor duration	95.38s
Return Code	Unknown
PID	2528
Parent PID	5552
Bitness	32 Bit

Host Behavior

Type	Count
Module	87
System	3520
File	23
Registry	20
-	17
-	148
Window	628
Process	4
Environment	1
Mutex	1

Network Behavior

Type	Count
HTTP	2

Process #8: musnotification.exe

ID	8
File Name	c:\windows\system32\musnotification.exe
Command Line	C:\Windows\system32\MusNotification.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 292430, Reason: Child Process
Unmonitor End Time	End Time: 365687, Reason: Terminated by timeout
Monitor duration	73.26s
Return Code	Unknown
PID	5256
Parent PID	8
Bitness	64 Bit

Process #10: explorta.exe

ID	10
File Name	c:\users\oqxzraykm\appdata\local\temp\5454e6f062\explorta.exe
Command Line	C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 310840, Reason: Child Process
Unmonitor End Time	End Time: 365687, Reason: Terminated by timeout
Monitor duration	54.85s
Return Code	Unknown
PID	5944
Parent PID	8
Bitness	32 Bit

Host Behavior

Type	Count
Module	24
System	837
File	3
Registry	8
-	17
-	1
Window	3
Process	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
005802da1bc8ec882fe467078704f2fb32975ce8538b3d7c3422b1cfb87bb334	C:\Users\OqXZRaykm\Desktop\L6lPO0G6AZQT4KWU.exe, C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe	Dropped File	1843.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
7d6253be97351663f4a32c47de12db0f3f2610f88c22279153d34497ce70215a	-	Downloaded File	4 bytes	text/plain	-	CLEAN
36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068	-	Downloaded File	1 bytes	application/octet-stream	-	CLEAN
385546f765fa7e7568297c6c3747ecd68cab772bb7953489d1053e813d441997	-	Downloaded File	170 bytes	text/plain	-	CLEAN
3a6d4f234efedc66d6a199f1620a8df575215f09e51a499d30c925c089aec358	-	Downloaded File	7 bytes	text/plain	-	CLEAN
33ef2eef1c2b8525d6e3e9213ed2519cfe8314508ad8b7f66381e847868b0a93	c:\windows\tasks\explorta.job	Dropped File	306 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\L6lPO0G6AZQT4KWU.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\tasks\explorta.job	Dropped File	-	CLEAN
\\.\SICE	Accessed File	Access	CLEAN
\\.\SIWVID	Accessed File	Access	CLEAN
\\.\NTICE	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access, Read	CLEAN
C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062	Accessed File	Access, Create	CLEAN
C:\ProgramData\AVAST Software	Accessed File	Access	CLEAN
C:\ProgramData\Avira	Accessed File	Access	CLEAN
C:\ProgramData\Kaspersky Lab	Accessed File	Access	CLEAN
C:\ProgramData\ESET	Accessed File	Access	CLEAN
C:\ProgramData\Panda Security	Accessed File	Access	CLEAN
C:\ProgramData\Doctor Web	Accessed File	Access	CLEAN
C:\ProgramData\AVG	Accessed File	Access	CLEAN
C:\ProgramData\360TotalSecurity	Accessed File	Access	CLEAN
C:\ProgramData\Bitdefender	Accessed File	Access	CLEAN
C:\ProgramData\Norton	Accessed File	Access	CLEAN
C:\ProgramData\Sophos	Accessed File	Access	CLEAN
C:\ProgramData\Comodo	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://193[.]233[.]132[.]139/sev56rkm/index.php	Contacted, Extracted	193.233.132.139	Russia	POST	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
193.233.132.139	-	Russia	TCP, HTTP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
006700e5a2ab05704bbb0c589b88924d	access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Wine	access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__	access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000	access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc	read, access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\Hardware\description\System	access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\Hardware\description\System\SystemBiosVersion	read, access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\Hardware\description\System\VideoBiosVersion	read, access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CurrentBuild	read, access	explorta.exe, l6lpo0g6azqt4kwu.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName	access	explorta.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName\ComputerName	read, access	explorta.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorta.exe	"C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe"	MALICIOUS
explorta.exe	C:\Users\OQXZRA~1\AppData\Local\Temp\5454e6f062\explorta.exe	MALICIOUS
l6lpo0g6azqt4kwu.exe	"C:\Users\OqXZRaykm\Desktop\L6lPO0G6AZQT4KWU.exe"	MALICIOUS
musnotification.exe	C:\Windows\system32\MusNotification.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p	CLEAN

YARA / AV

No YARA or AV matches available.

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	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

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