MALICIOUS

Classifications: Keylogger, Spyware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**READ ME! (List of free things).exe**
ID	#10314644
MD5	68c1b029a29c360bf98551ff87031eee
SHA1	f39190ed310e9d2244ebfb9edd360de3f7f810a0
SHA256	6efb57a28434d238a6fcd58c8aa90a1f1cda4d5897ecdce5351fb11a9a5abef2
File Size	334.00 KB
Report Created	2024-04-27 13:51 (UTC+2)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 20 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe logs keys and potentially exfiltrates data.			
4/5	Defense Evasion	Modifies Windows Defender configuration	2	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe uses (Process #8) powershell.exe to add C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe to Windows Defender exclusions. • (Process #4) live-windowsplayer-version-492b7f0827474659.exe uses (Process #13) powershell.exe to add process LIVE-WindowsPlayer-version-492b7f0827474659.exe to Windows Defender exclusions.			
4/5	Reputation	Malicious file detected via reputation	2	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • File "C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe" is a known malicious file.			
3/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe queries hardware properties via WMI: Select * from Win32_ComputerSystem.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe tries to detect "Sandboxie" by checking for existence of module "SbieDll.dll".			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe queries OS version via WMI query: select * from Win32_OperatingSystem.			
1/5	Mutex	Creates mutex	2	-
	• (Process #1) read me! (list of free things).exe creates mutex with name "XcFcvKAEG7NAYbzpz". • (Process #4) live-windowsplayer-version-492b7f0827474659.exe creates mutex with name "6NHmHkn9OEtCyHGw".			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe starts (process #8) powershell.exe with a hidden window. • (Process #4) live-windowsplayer-version-492b7f0827474659.exe starts (process #13) powershell.exe with a hidden window.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe resolves hostname "ip-api.com" to IP "208.95.112.1".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe opens an outgoing TCP connection to host "208.95.112.1:80".			
1/5	Obfuscation	Resolves API functions dynamically	1	-

Score	Category	Operation	Count	Classification
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe resolves 52 API functions by name.			
1/5	Execution	Drops PE file	1	-
	• (Process #1) read me! (list of free things).exe drops file "C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe".			
1/5	Discovery	Checks external IP address	1	-
	• (Process #4) live-windowsplayer-version-492b7f0827474659.exe checks external IP by asking IP info service at "http://ip-api.com/line/?fields=hosting".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe".			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

Mitre ATT&CK Matrix

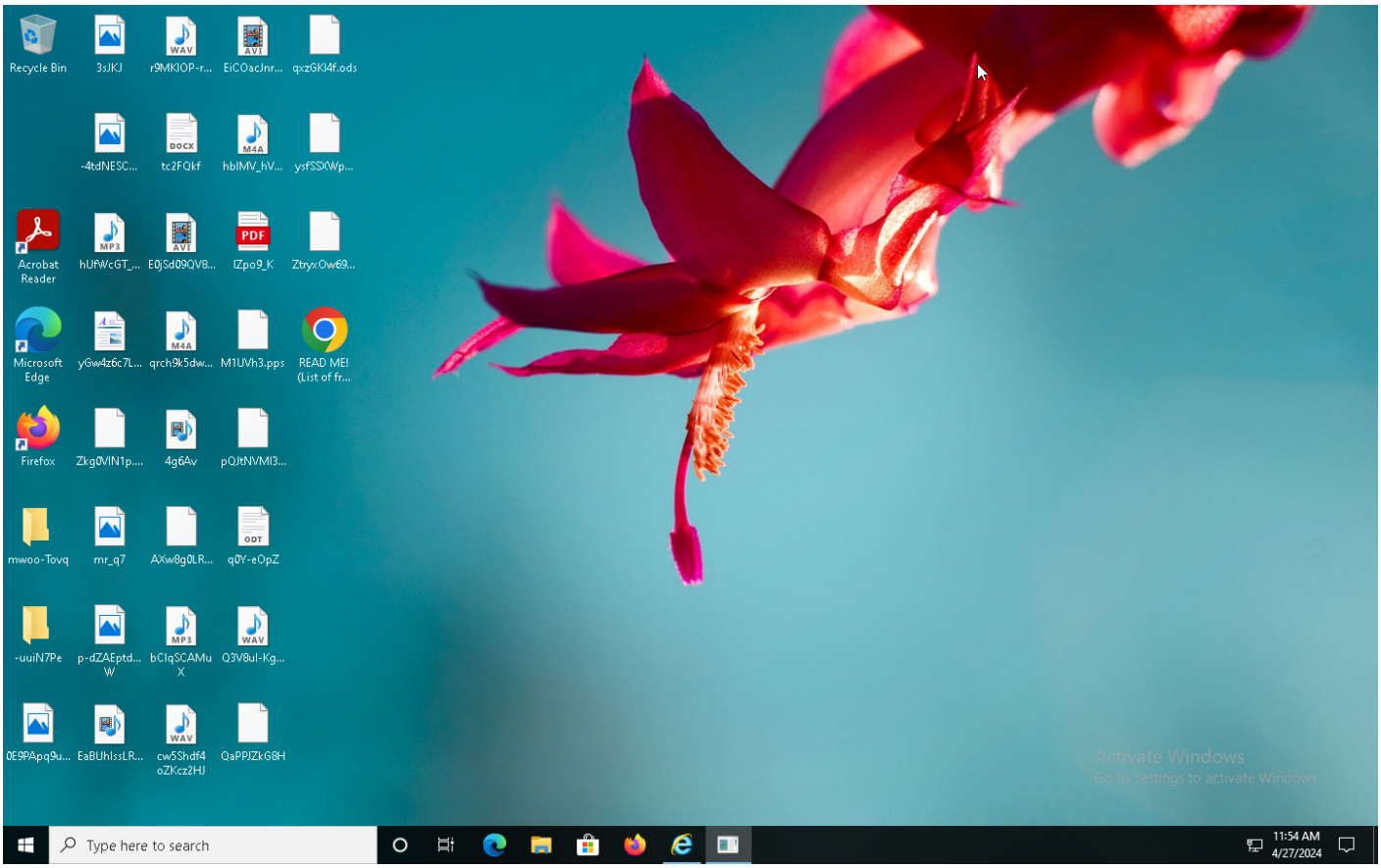
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1179 Hooking	#T1179 Hooking	#T1497 Virtualization/ Sandbox Evasion	#T1056 Input Capture	#T1082 System Information Discovery		#T1056 Input Capture			
				#T1143 Hidden Window	#T1179 Hooking	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection			
				#T1045 Software Packing		#T1016 System Network Configuration Discovery					

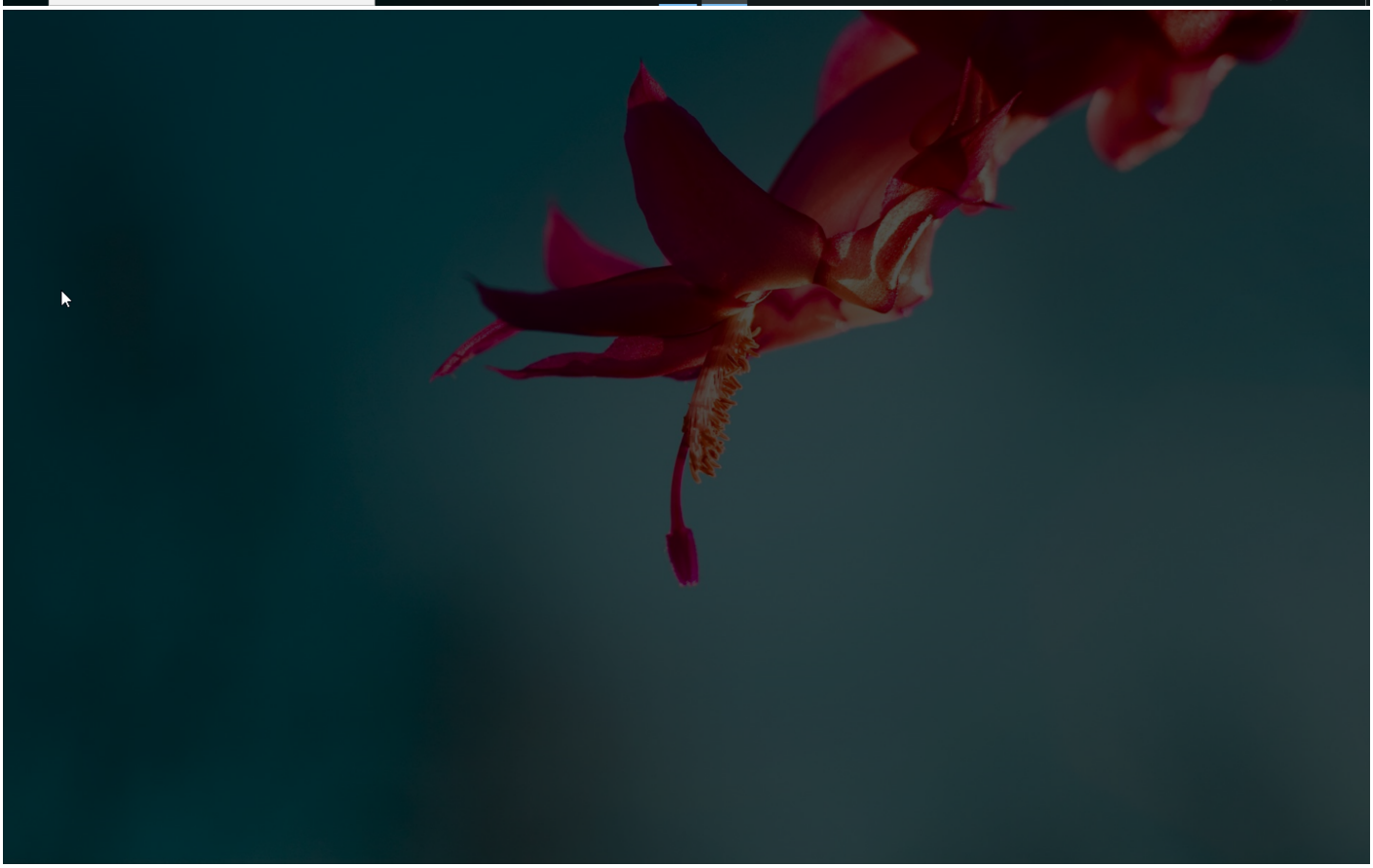
Sample Information

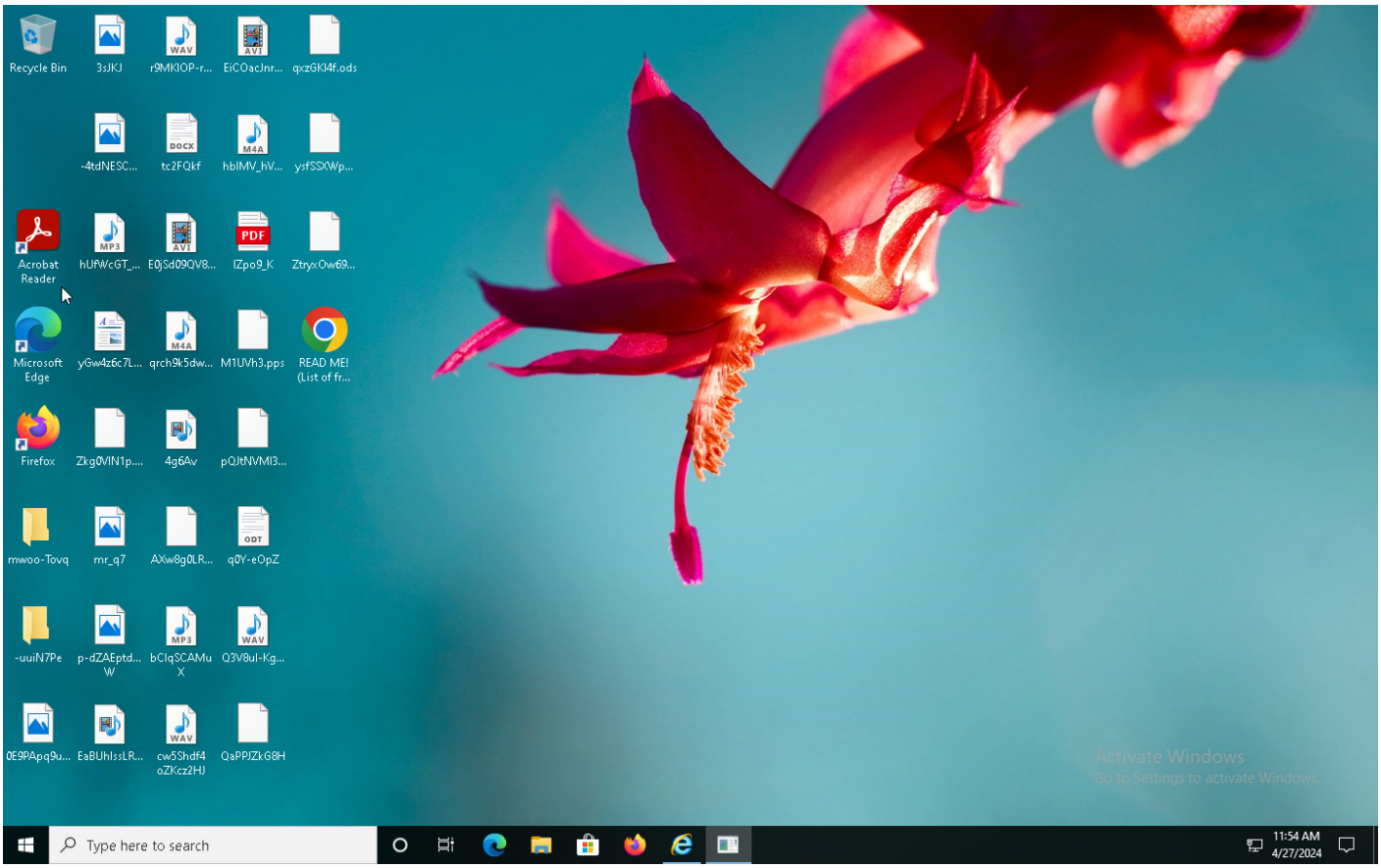
ID	#10314644
MD5	68c1b029a29c360bf98551ff87031eee
SHA1	f39190ed310e9d2244ebfb9edd360de3f7f810a0
SHA256	6efb57a28434d238a6fcd58c8aa90a1f1cda4d5897ecdce5351fb11a9a5abef2
SSDeep	6144:o/ipsG1aNuu239B0WHF06M+58VEhC8XVtyArpV8zbXqzNugVqwlL:ppsGB0N+5kGHVtbr7UXqxuAJ
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	READ ME! (List of free things).exe
File Size	334.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

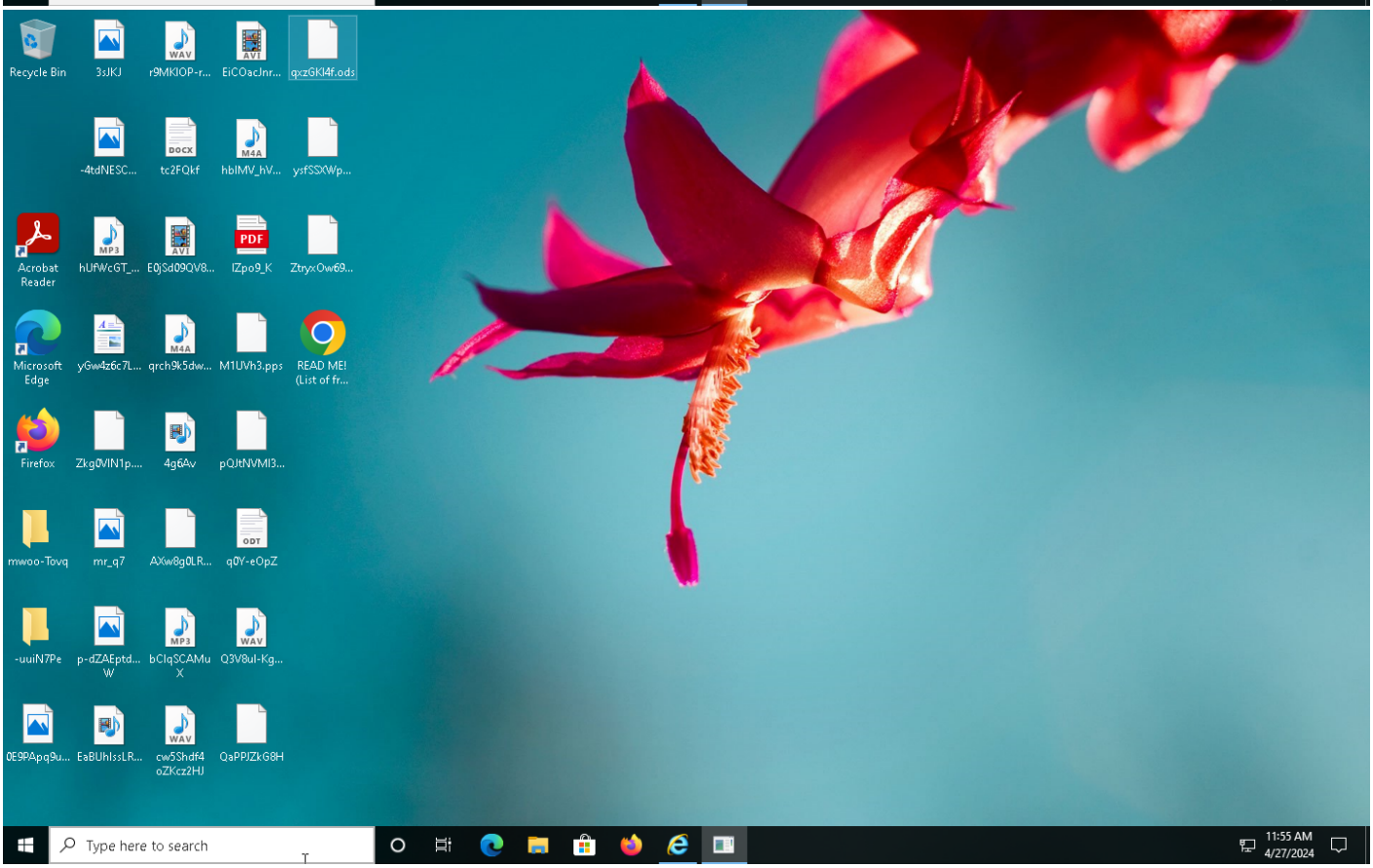
Analysis Information

Creation Time	2024-04-27 13:51 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	7
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
3sJKJ
r9MKlOP-r...
EiCOacJnr...
qxzGKl4f.ods
-4tdNESC...
tc2FQkf
hblMV_hV...
ysfSSXWp...
Acrobat Reader
hUPWcGT_...
E0jSd09QV8...
lZpo9_K
ZtryxOw69...
Microsoft Edge
yGw4z6c7L...
qrch9k5dw...
M1UVh3.pps
READ ME! (List of fr...
Firefox
Zkg0VIN1p....
4g6Av
pQJtNVMI3...
mwoo-Tovq
mr_q7
AXw8g0LR...
q0Y-eOpZ
-uuiN7Pe
p-dZAEptd...W
bClqSCAMuX
Q3V8ul-Kg...
0E9PApq9u...
EaBUhlssLR...
cw5Shdf4oZKcz2HJ
QaPPlZkG8H
Activate Windows
Go to Settings to activate Windows.
Type here to search
11:54 AM
4/27/2024







Screenshots truncated

NETWORK

General

348 bytes total sent

419 bytes total received

2 ports 80, 53

2 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 292 bytes sent, 347 bytes received

HTTP Requests

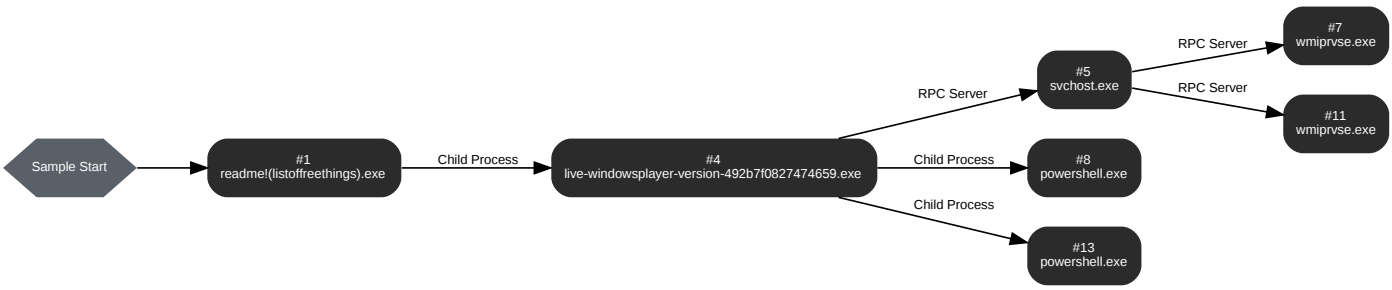
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://ip-api[.]com/line/?fields=hosting	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	ip-api[.]com	NO_ERROR	208.95.112.1	-	CLEAN

BEHAVIOR

Process Graph



Process #1: read me! (list of free things).exe

ID	1
File Name	c:\users\oqxzraykm\desktop\read me! (list of free things).exe
Command Line	"C:\Users\OqXZRaykm\Desktop\READ ME! (List of free things).exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 155850, Reason: Analysis Target
Unmonitor End Time	End Time: 187506, Reason: Terminated
Monitor duration	31.66s
Return Code	0
PID	5332
Parent PID	-
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe	204.00 KB	a830068f14771855442956a1d95b0222071ef7bc788910fabb6cc5a861cdcecd	✖

Host Behavior

Type	Count
Mutex	1
File	5
Registry	1
Process	1

Process #4: live-windowsplayer-version-492b7f0827474659.exe

ID	4
File Name	c:\users\oqxzraykm\appdata\roaming\live-windowsplayer-version-492b7f0827474659.exe
Command Line	"C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 184402, Reason: Child Process
Unmonitor End Time	End Time: 396868, Reason: Terminated by timeout
Monitor duration	212.47s
Return Code	Unknown
PID	5400
Parent PID	5332
Bitness	64 Bit

Host Behavior

Type	Count
Environment	5
User	3
System	8
Registry	61
Module	79
Mutex	1
-	16
COM	10
-	2
-	1
File	19
-	1
Process	2
Window	2

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	6

Process #5: svchost.exe

ID	5
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: 201353, Reason: RPC Server
Unmonitor End Time	End Time: 396868, Reason: Terminated by timeout
Monitor duration	195.51s
Return Code	Unknown
PID	8
Parent PID	5400
Bitness	64 Bit

Host Behavior

Type	Count
Registry	8
System	2

Process #7: wmiprvse.exe

ID	7
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: 201353, Reason: RPC Server
Unmonitor End Time	End Time: 396868, Reason: Terminated by timeout
Monitor duration	195.51s
Return Code	Unknown
PID	2340
Parent PID	8
Bitness	64 Bit

Host Behavior

Type	Count
Registry	2
System	8
File	2
COM	2

Process #8: powershell.exe

ID	8
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath 'C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe'
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 228361, Reason: Child Process
Unmonitor End Time	End Time: 315000, Reason: Terminated
Monitor duration	86.64s
Return Code	1
PID	3340
Parent PID	5400
Bitness	64 Bit

Host Behavior

Type	Count
Environment	53
Registry	70
File	529
System	44
-	26
Module	10
COM	4

Process #11: wmiprvse.exe

ID	11
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: 289728, Reason: RPC Server
Unmonitor End Time	End Time: 396868, Reason: Terminated by timeout
Monitor duration	107.14s
Return Code	Unknown
PID	4796
Parent PID	8
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Mutex	1
Module	22
Registry	6
File	1

Process #13: powershell.exe

ID	13
File Name	c:\windows\system32\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass Add-MpPreference -ExclusionProcess 'LIVE-WindowsPlayer-version-492b7f0827474659.exe'
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 313441, Reason: Child Process
Unmonitor End Time	End Time: 353942, Reason: Terminated
Monitor duration	40.50s
Return Code	1
PID	4488
Parent PID	5400
Bitness	64 Bit

Host Behavior

Type	Count
Environment	53
Registry	70
File	529
System	44
-	26
Module	10
COM	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6efb57a28434d238a6fcd58c8aa90a1f1cda4d5897ecdce5351fb11a9a5abef2	C:\Users\OqXZRaykm\Desktop\READ ME! (List of free things).exe	Sample File	334.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a830068f14771855442956a1d95b0222071ef7bc788910fabb6cc5a861cdcecd	C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe	Dropped File	204.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
7bcc141f3b818cd5833b2507492bc401ded8eb52f59c890730629e7d85b790ff	-	Extracted File	15.41 KB	image/png	-	CLEAN
2ed27c1421e6928dbe13dbfdb5c59e1045b30341fe7ebe05700006bc5ac572c0	-	Downloaded File	6 bytes	text/plain	-	CLEAN
4d830c2921ca9d1408dd409571f74a072c9bfb473f7d03bfb1a83a79ec1d9a63	-	Extracted File	67.39 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\READ ME! (List of free things).exe	Sample File	-	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\Desktop\READ ME! (List of free things).exe.config	Accessed File	Access	CLEAN
\??\C:\Windows\system32\OemInfo.Ini	Accessed File	Access	CLEAN
C:\Windows\system32\OemLogo.Bmp	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe.config	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Windows\System32\OpenSSH\	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Local\Microsoft\WindowsApps	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	Accessed File	Access	CLEAN
C:\Users\OqXZRaykm\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Accessed File	Access, Read	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\Microsoft.PowerShell.Operation.Validation.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\Microsoft.PowerShell.Operation.Validation.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\Microsoft.PowerShell.Operation.Validation.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\Microsoft.PowerShell.Operation.Validation.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\Microsoft.PowerShell.Operation.Validation.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\Microsoft.PowerShell.Operation.Validation.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.xaml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Pester\Pester.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PSReadline\PSReadline.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppvClient	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AssignedAccess	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitLocker	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BranchCache	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ConfigCI	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DeliveryOptimization	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Dism	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DnsClient	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\EventTracingManagement	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\International	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Kds	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MMAgent	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\MsDtc	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetAdapter	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetConnection	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetLbfo	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetNat	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetQos	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetSecurity	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetSwitchTeam	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetTCPIP	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkTransition	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PcsvDevice	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PersistentMemory	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PKI	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PnpDevice	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PrintManagement	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ProcessMitigations	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Provisioning	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflow	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ScheduledTasks	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SecureBoot	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbShare	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbWitness	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\StartLayout	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Storage	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\StorageBusCache	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TLS	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\UEV	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\VpnClient	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Wdac	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Whea	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsSearch	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\WindowsUpdate	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://ip-api[.]com/line/?fields=hosting	Extracted, Contacted	208.95.112.1	United States	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
ip-api[.]com	208.95.112.1	United States	HTTP, DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
208.95.112.1	ip-api[.]com	United States	HTTP, DNS, TCP	CLEAN
127.0.0.1	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
XcFcvKAEG7NAYbzpz	access	read me! (list of free things).exe	CLEAN
6NHmHkn9OEtCyHGw	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
-	access	wmiprvse.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	read me! (list of free things).exe, live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PagingFiles	read, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SystemDefaultTlsVersions	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Central European Standard Time	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Central European Standard Time\TZI	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Central European Standard Time\Dynamic DST	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Central European Standard Time\MUI_Display	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Central European Standard Time\MUI_Std	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Central European Standard Time\MUI_Dlt	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\AutoEnrollment\Debug	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Debug	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration	access	svchost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\AutoEnrollment\certenroll.log	read, access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	read, access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\ProtectedEventLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\appcompat	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	access, create	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM	access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\AmsiEnable	read, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\EnableObjectValidation	read, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	live-windowsplayer-version-492b7f0827474659.exe	CLEAN

Process

Process Name	Commandline	Verdict
read me! (list of free things).exe	"C:\Users\OqXZRaykm\Desktop\READ ME! (List of free things).exe"	MALICIOUS
live-windowsplayer-version-492b7f0827474659.exe	"C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe"	MALICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass Add-MpPreference -ExclusionProcess 'LIVE-WindowsPlayer-version-492b7f0827474659.exe'	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath 'C:\Users\OqXZRaykm\AppData\Roaming\LIVE-WindowsPlayer-version-492b7f0827474659.exe'	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs -p	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	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