

Hash: e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf

Malware family name: Ramnit

Classification: Worm/Trojan

## Tools

### Static Analysis Tools

Strings – Extracted strings to identify potential API calls, registry paths, persistence mechanisms, and referenced filenames

CFF Explorer – Analysis the PE structure, including headers, imports, and exported functions

VirusTotal, HybridAnalysis, CAPE Sandbox – Performed hash-based analysis across multiple antivirus engines

### Dynamic Analysis Tools

X32dbg – Debugged the sample at runtime to observe execution flow and confirm process creation attempts

RegShot – Compared registry states before and after execution to identify persistence-related modifications

AutoRuns – Inspected startup locations post-reboot to identify persistence mechanisms

Process Explorer – Monitored running processes post-reboot to verify whether the malware executed in memory

## Executive Summary

The executable is a Windows-based malware sample that demonstrates multiple malicious behaviors, including unauthorized process creation, registry modification, privilege escalation attempts, and persistence establishment. Static analysis revealed extensive use of Windows API functions related to memory manipulation, registry access, and process execution. Dynamic analysis confirmed that the malware attempts to spawn additional processes and modify system configuration settings, triggering User Account Control prompts during execution. Registry analysis and startup inspection showed that the malware successfully configured multiple persistence mechanisms; however, post-reboot analysis using AutoRuns and Process Explorer indicated that the malware did not successfully execute after system restart. This was likely due to environmental constraints such as disabled network connectivity preventing retrieval or execution of a secondary payload.

## Analysis Findings

After submitting the hash sample to VirusTotal, Hybrid Analysis, and CAPE Sandbox, multiple security engines flagged the hash as malicious. Sandbox reports associated the hash with behaviors including registry modifications, process execution, and persistence-related activity.

VirusTotal and HybridAnalysis indicate the file as malicious, with HybridAnalysis linking it to a file named “loader.exe”. HybridAnalysis detected many DNS queries for domains that cannot be resolved. Since the file is named “loader”, it’s possible that this malware’s intention is simply to weaken defenses and establish persistence within the system, before then reaching the network to download a second payload without the user’s knowledge.

Search results for `e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf`

59 / 71 Community Score

59/71 security vendors flagged this file as malicious

Reanalyze Similar More

`e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf`  
`e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf.exe`

Size: 216.00 KB | Last Analysis Date: 1 day ago

peexe persistence mxdomain suspicious-dns runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: `trojan.ramnit/evotob` | Threat categories: trojan virus dropper | Family labels: ramnit evotob lebag

Security vendors' analysis

Vendor	Detection	Family Labels
AhnLab-V3	Malware/Win32_RL_Generic.R282894	TrojanDropper:Win32/Lebag.572315b5
AlIcloud	Virus:Win/Evotob.AZ	Trojan.Win32.Crypt.N
Antiy-AVL	Trojan/Win32.Agent	Trojan.Win32.Crypt.N
Arctic Wolf	Unsafe	Win32:Ramnit-F
AVG	Win32:Ramnit-F	TR/HJacker.Gen
BitDefender	Trojan.Win32.Crypt.N	W32.AIDetect/Malware
ClamAV	Win.Malware.Ramnit-699753-0	Win/malicious_confidence_100% (W)

HYBRID ANALYSIS

Search results for `e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf`

Timestamp	Input	Threat level	Analysis Summary
July 12th 2025 20:37:56 (UTC)	<code>lrgetw.exe.bin</code> PE32 executable (GUI) Intel 80386, for MS Windows	malicious	AV Detection: 91% Trojan.Crypt Matched 209 Indicators
July 12th 2025 20:36:20 (UTC)	<code>e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf.bin</code> PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections	malicious	Threat Score: 100/100 AV Detection: 91% Trojan.Crypt Matched 209 Indicators
October 2nd 2024 09:53:16 (UTC)	<code>loader.exe</code> PE32 executable (GUI) Intel 80386, for MS Windows	malicious	Threat Score: 100/100 AV Detection: 91% Trojan.Crypt Matched 203 Indicators
August 6th 2023 22:07:14 (UTC)	<code>00000000.exe</code> PE32 executable (GUI) Intel 80386, for MS Windows	malicious	Threat Score: 100/100 AV Detection: 91% Trojan.Crypt Matched 217 Indicators
October 27th 2019 00:14:07 (UTC)	<code>trppp6a7ppp</code> PE32 executable (GUI) Intel 80386, for MS Windows	malicious	Threat Score: 100/100 AV Detection: 91% Trojan.Crypt Matched 42 Indicators

Network Analysis Overview

DNS Requests

Domain	TTL	Country
hbbyutchow.com	-	-
ipcovfhs.com	-	-
lue62876tgbdtou.com	-	-
iwobkgnbkckct.com	-	-
javtqaxboyqyxubai.com	72,26,218,70 TTL: 900	United States
joykvtfdkymfmpvi.com	-	-
jeurjqeoyllrmy.com	-	-
jyortffmmirahqdmf.com	-	-
krybghymmua.com	-	-
lhrxwændtjeaa.com	-	-

Contacted Hosts

IP Address	Port/Protocol	Associated Process	Details
142.251.32.46	80 TCP	svchost.exe PID: 1892	United States
46.165.254.208	443 TCP	svchost.exe PID: 736	Germany
162.249.66.17	443 TCP	svchost.exe PID: 736	United States

CAPE Sandbox also flagged the file as malicious, under the Ramnit family. PE information on CAPE indicates loader.exe as the exported DLL name.

cape Dashboard

Quick Overview Behavioral Analysis Network Analysis Compare this analysis to...

Detection(s): **Ramnit**

Analysis

Category	Package	Started	Completed	Duration	Log(s)
FILE	exe	2025-07-14 13:45:45	2025-07-14 13:46:55	70 seconds	Show Analysis Log

Machine

Name	Label	Manager	Started On	Shutdown On
win10-2	win10-2	KVM	2025-07-14 13:45:45	2025-07-14 13:46:55

File Details

Type	Ramnit Payload: 32-bit executable
File Name	<code>e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf</code>
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
File Size	221184 bytes
MD5	118962ea993ca48914c068235b1a8397
SHA1	0f61c338895c6f483b15e6a358accfd0a83de6
SHA256	<code>e142a1e51ce0e8d28fd852683b65688dcc97a6b705e8adc799d5af0bdefefcf</code> [VT] [MWDB] [Bazaar]



The file is a valid 32-bit Windows Portable Executable (PE32) with standard sections (.text, .rdata, .data, .rsrc) and no evidence of packing. Import table analysis showed use of kernel32.dll, advapi32.dll, shell32.dll, user32.dll, and shlwapi.dll, indicating capabilities for process creation, registry access, and shell interaction.

The left screenshot shows the Import Directory for sample.exe:

Module Name	Imports	OFs	TimeDateStamp	ForwarderChain	Name RVA	FFs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	87	00000000	00000000	00000000	0002F7B0	0002E990
advapi32.dll	26	00000000	00000000	00000000	0002F7BD	0002E000
gdi32.dll	8	00000000	00000000	00000000	0002F7CA	0002E09C
shell32.dll	1	00000000	00000000	00000000	0002F7D4	0002E1F0
shlwapi.dll	3	00000000	00000000	00000000	0002F7E0	0002E1F8
user32.dll	28	00000000	00000000	00000000	0002F7EC	0002E208

The right screenshot shows the PE headers and a hex dump of the file content:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	LineNumbers	Relocations N...	LineNumbers ...	Characteristics
Byte[1]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
text	0002C9F4	00001000	0002C900	00000400	00000000	00000000	0000	0000	80000020
.data	00002243	00002000	00002000	00002000	00000000	00000000	0000	0000	40000040
.data	00000774	00003000	00006400	00003000	00000000	00000000	0000	0000	C0000040
.rsrc	00000520	00009000	00000600	00009000	00000000	00000000	0000	0000	C0000040

Export table analysis revealed executable export functions named “\_ApplyExploit@4” and “\_CheckBypassed@0”. The presence of exploit-related function names within an executable suggests that the sample may be intended to function as an exploit helper or secondary component invoked by another process.

The screenshot shows the Export Directory for sample.exe:

Member	Offset	Size	Value
Characteristics	0002F440	Dword	00000000
TimeDateStamp	0002F444	Dword	56438158
MajorVersion	0002F448	Word	0000
MinorVersion	0002F44A	Word	0000
Name	0002F44C	Dword	0003027C
Base	0002F450	Dword	00000001
NumberOfFunctions	0002F454	Dword	00000002
NumberOfNames	0002F458	Dword	00000002
AddressOfFunctions	0002F45C	Dword	00030268

Detailed view of the export table:

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	0002DC9E	0000	00030287	_ApplyExploit@4
00000002	0002DBCE	0001	00030297	_CheckBypassed@0

Extracted strings revealed references to process execution functions (CreateProcessA, ShellExecuteExA, runas), memory allocation and protection APIs (VirtualAlloc, VirtualProtect, ZwAllocateVirtualMemory), registry persistence locations (Software\Microsoft\Windows\CurrentVersion\Run, Winlogon), Windows Defender exclusion paths, and HTTP-related strings suggesting potential outbound communication. Strings analysis also revealed references to loader.exe, suggesting that the analyzed sample may function as a loader or helper component rather than a complete standalone payload.

```

Line 1045: %APPDATA%
Line 2060: %APPDATA%
Line 2149: %APPDATA%\Apple Computer\Safari\Cookies\Cookies.plist
Line 2150: %APPDATA%\Mozilla\Firefox\
Line 2158: 1APPDATA%\Macromedia\Flash Player\#SharedObjects
Line 2159: %APPDATA%\Opera\

Line 945: GetTempFileNameA
Line 946: GetTempPathA
Line 1858: GetTempFileNameA
Line 1859: GetTempPathA
Line 2666: %temp%\..\..\LocalLow\cmd.%username%.bat
Line 2738: PsInitialSystemProcess
Line 2801: GetTempPathA
Line 2802: GetTempFileNameA

Line 2684: system32
Line 2687: \system32\sdbinst.exe"

Line 926: CreateProcessA
Line 1832: CreateProcessA
Line 2788: CreateProcessA

Line 1965: ShellExecuteA
Line 2873: ShellExecuteExA

Line 958: LoadLibraryA
Line 1871: LoadLibraryA
Line 2791: LoadLibraryA
Line 2830: LoadLibraryExA

Line 943: GetProcAddress
Line 1855: GetProcAddress
Line 2803: GetProcAddress

Line 980: VirtualAlloc
Line 981: VirtualFree
Line 982: VirtualProtect
Line 2698: ZwAllocateVirtualMemory

Line 2739: NtFreeVirtualMemory
Line 2741: NtAllocateVirtualMemory
Line 2770: VirtualAlloc
Line 2771: VirtualAllocEx
Line 2772: VirtualFree
Line 2773: VirtualProtect
Line 2774: VirtualProtectEx
Line 2815: VirtualQueryEx
Line 2816: VirtualFreeEx
Line 2932: ZwProtectVirtualMemory
Line 2934: ZwFreeVirtualMemory
Line 2965: ZwWriteVirtualMemory

Line 976: Sleep
Line 1891: Sleep
Line 2767: Sleep

```

Strings analysis also revealed multiple registry modification commands targeting Microsoft Defender and Antimalware exclusion lists. The malware attempts to exclude trusted Windows binaries such as svchost.exe, rundll32.exe, and explorer.exe, as well as entire file extensions (\*.exe, \*.dll), indicating a clear attempt to evade host-based security controls prior to executing additional payloads.

svchost.exe

```

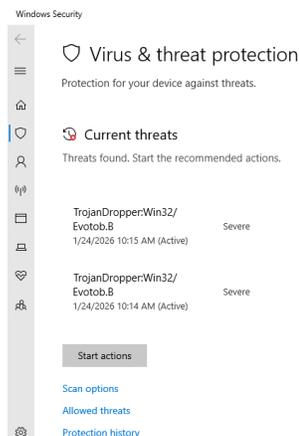
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v svchost.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v consent.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v rundll32.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v spoolsv.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v explorer.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v rgjdu.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes" /v afwqs.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions" /v *.tmp /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions" /v *.dll /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions" /v *.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v svchost.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v consent.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v rundll32.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v spoolsv.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v explorer.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v rgjdu.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes" /v afwqs.exe /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions" /v *.tmp /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions" /v *.dll /t REG_DWORD /d 0
REG ADD "HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions" /v *.exe /t REG_DWORD /d 0

```

spoolsv.exe

msseces.exe

Windows Defender showed severe threats before it was disabled for dynamic analysis.



Dynamic analysis confirmed that the malware executed successfully, as evidenced by process and thread creation and multiple User Account Control (UAC) elevation prompts. This analysis was conducted in an isolated Windows virtual machine using x32dbg, Process Explorer, RegShot, and AutoRuns.

When executed under x32dbg, the malware reached its entry point and executed a bypass verification, as seen by “CheckBypassed ok”. The presence of “\_CheckBypassed@0” was noted earlier during static analysis in the CFF Explorer export directory. The application exited cleanly after verification.

```
Process Started: 15190000 C:\Users\main\Desktop\sample.exe
"C:\Users\main\Desktop\sample.exe"
argv[0]: C:\Users\main\Desktop\sample.exe
Breakpoint at 151B97B5 (entry breakpoint) set!
DLL Loaded: 773E0000 C:\Windows\SysWOW64\ntdll.dll
DLL Loaded: 760C0000 C:\Windows\SysWOW64\kernel32.dll
DLL Loaded: 768B0000 C:\Windows\SysWOW64\KernelBase.dll
DLL Loaded: 743F0000 C:\Windows\SysWOW64\apphelp.dll
DLL Loaded: 76230000 C:\Windows\SysWOW64\advapi32.dll
DLL Loaded: 77310000 C:\Windows\SysWOW64\msvcrt.dll
DLL Loaded: 75DB0000 C:\Windows\SysWOW64\sechost.dll
DLL Loaded: 75E30000 C:\Windows\SysWOW64\rpport4.dll
DLL Loaded: 75D60000 C:\Windows\SysWOW64\gdi32.dll
DLL Loaded: 75D40000 C:\Windows\SysWOW64\win32u.dll
DLL Loaded: 75840000 C:\Windows\SysWOW64\gdi32full.dll
Thread 5412 created, Entry: ntdll.77415940, Parameter: 0045C840
Thread 2552 created, Entry: ntdll.77415940, Parameter: 0045C840
DLL Loaded: 76B00000 C:\Windows\SysWOW64\msvcp_win.dll
DLL Loaded: 75A20000 C:\Windows\SysWOW64\ucrtbase.dll
DLL Loaded: 76E00000 C:\Windows\SysWOW64\user32.dll
DLL Loaded: 762B0000 C:\Windows\SysWOW64\shell32.dll
DLL Loaded: 75930000 C:\Windows\SysWOW64\shlwapi.dll
System breakpoint reached!
DLL Loaded: 75BB0000 C:\Windows\SysWOW64\imm32.dll
INT3 breakpoint "entry breakpoint" at <sample.OptionalHeader.AddressOfEntryPoint> (151B97B5)!
DebugString: "CheckBypassed ok"
DLL Loaded: 75250000 C:\Windows\SysWOW64\ntmarta.dll
Thread 5412 exit
Thread 2552 exit
Process stopped with exit code 0x0 (0)
Saving database to C:\Tools\Debugging\release\x32\db\sample.exe.dd32 0ms
Debugging stopped!
```

After execution, UAC prompts were triggered and a system restart was requested, indicating attempts to modify system-level or security-related settings.

Using RegShot, comparison of registry and filesystem state before and after execution revealed multiple file system changes associated with malware activity. A new directory was created at “C:\Users\main\AppData\Local\smhxfexa”, containing an executable file named “bsykpehn.exe”. Additional executables were written to user-writable locations, including “C:\Users\main\AppData\Local\Temp\ruxiloco.exe” and “C:\Users\main\AppData\Local\Temp\koqpwqnt.exe”. RegShot output also shows creation of startup persistence via placement of “bsykpehn.exe” in the user’s Startup folder.

```
-----
Files added: 16
-----
C:\Windows\apppatch\CustomSDR\{448a8c57-7c48-461c-9957-ab255dde986e}.sdb
C:\Windows\Prefetch\CMD_EXE-AC113AAB.pf
C:\Windows\Prefetch\LSICSLI_EXE-85AAS8D3.pf
C:\Windows\Prefetch\KOPQWQNT_EXE-09B305F8.pf
C:\Windows\Prefetch\RUKEILCO_EXE-41F46981.pf
C:\Windows\Prefetch\SAMPLE_EXE-AE7C9AF2.pf
C:\Windows\Prefetch\SOBTRST_EXE-9AB7A34F.pf
C:\Windows\Prefetch\SVCHOST_EXE-78C2C10D.pf
C:\Windows\Prefetch\X32DBG_EXE-80721DEB.pf
C:\Users\main\AppData\Local\Microsoft\Windows\ActionCenterCache\windows-systemtoast-securityandmaintenance_22_0.png
C:\Users\main\AppData\Local\Temp\koqpwqnt.exe
C:\Users\main\AppData\Local\Temp\ruxiloco.exe
C:\Users\main\AppData\Local\smhxfexa\bsykpehn.exe
C:\Users\main\AppData\Local\usenklp.log
C:\Users\main\AppData\Local\vj1bgfmm.log
C:\Users\main\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\bsykpehn.exe
-----
Files [attributes] modified: 17
-----
C:\Windows\bootstat.dat
C:\Windows\Logs\WindowsUpdate\WindowsUpdate_20260125_061153_467_1.etl
C:\Windows\Prefetch\ZG_EXE-0F6C0881.pf
C:\Windows\Prefetch\CONHOST_EXE-1F3E907E.pf
C:\Windows\Prefetch\CONSENT_EXE-531B09EA.pf
C:\Windows\Prefetch\DLHOST_EXE-5E46FAB0.pf
C:\Windows\Prefetch\WPDORBI_EXE-7401F8B4.pf
C:\Windows\Prefetch\SVCHOST_EXE-5AC388EC.pf
C:\Windows\Prefetch\SVCHOST_EXE-DCBDF9F5.pf
C:\Windows\ServiceProfiles\LocalService\HTUSER_DAT.LOG1
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\WpCmdRun.log
C:\Windows\SoftwareDistribution\DataStore\DataStore.edb
C:\Windows\SoftwareDistribution\DataStore\DataStore.jfm
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log
C:\Windows\Temp\WpCmdRun.log
C:\Users\main\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
-----
Folders added: 1
-----
C:\Users\main\AppData\Local\smhxfexa
```

After rebooting the system to test persistence, startup entries remained present; however, Process Explorer did not show any evidence of the malware executing in memory. This suggests that while the malware successfully configured persistence mechanisms, the execution phase of persistence failed, likely due to the network being disabled.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		2,924 K	72,460 K	92		
System Idle Process	100.00	60 K	8 K	0		
System	< 0.01	196 K	152 K	4		
smss.exe	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
Memory Compression		1,060 K	1,196 K	328		
csrss.exe		72 K	316 K	1828		
csrss.exe		1,636 K	5,212 K	424		
wininit.exe		1,368 K	7,152 K	500		
services.exe		4,368 K	9,616 K	636		
svchost.exe		10,496 K	31,456 K	752	Host Process for Windows S...	Microsoft Corporation
StartMenuExperienceHost.exe		18,808 K	61,380 K	4988		
RuntimeBroker.exe		3,452 K	21,040 K	5080	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	112,404 K	192,596 K	1692	Search application	Microsoft Corporation
RuntimeBroker.exe		6,898 K	27,176 K	4256	Runtime Broker	Microsoft Corporation
SkypeBackgroundHost.exe	Susp...	2,016 K	1,340 K	5136	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		3,308 K	16,712 K	5288	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe		7,468 K	26,308 K	6004	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Susp...	15,124 K	1,492 K	6028	Store	Microsoft Corporation
RuntimeBroker.exe		1,464 K	7,668 K	5656	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe		24,376 K	67,524 K	5808	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		4,736 K	23,484 K	5952	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	16,024 K	64,424 K	3196	Search application	Microsoft Corporation
SystemSettingsBroker.exe		4,764 K	24,520 K	5836	System Settings Broker	Microsoft Corporation
TextInputHost.exe		8,852 K	39,468 K	5592		
dllhost.exe		3,416 K	12,372 K	4692	COM Surrogate	Microsoft Corporation
smartscreen.exe		7,400 K	22,052 K	3292	Windows Defender SmartScr...	Microsoft Corporation

Name	Description	Company Name	Path
baseadv.dll	Windows NT BASE API Server DLL	Microsoft Corporation	C:\Windows\System32\baseadv.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
csrssv.dll	Client Server Runtime Process	Microsoft Corporation	C:\Windows\System32\csrssv.dll
csrss.exe	Client Server Runtime Process	Microsoft Corporation	C:\Windows\System32\csrss.exe
csrss.exe.mui	Client Server Runtime Process	Microsoft Corporation	C:\Windows\System32\en-US\csrss.exe.mui
gd32.dll	GD Client DLL	Microsoft Corporation	C:\Windows\System32\gd32.dll
gd32full.dll	GD Client DLL	Microsoft Corporation	C:\Windows\System32\gd32full.dll
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
msvcp_win.dll	Microsoft@ C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
sxs.dll	Fusion 2.5	Microsoft Corporation	C:\Windows\System32\sxs.dll
sxsrsrv.dll	Windows SxS Server DLL	Microsoft Corporation	C:\Windows\System32\sxsrsrv.dll
ucrtbase.dll	Microsoft@ C Runtime Library	Microsoft Corporation	C:\Windows\System32\ucrtbase.dll
user32.dll	Multi-User Windows USER API Cl...	Microsoft Corporation	C:\Windows\System32\user32.dll
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\System32\win32u.dll
winsrv.dll	Multi-User Windows Server DLL	Microsoft Corporation	C:\Windows\System32\winsrv.dll
winsrv.dll.mui	Multi-User Windows Server DLL	Microsoft Corporation	C:\Windows\System32\en-US\winsrv.dll.mui
winsrvext.dll	Multi-User Windows Server Extensi...	Microsoft Corporation	C:\Windows\System32\winsrvext.dll

State	Wait Reason	TID	User Time	Kernel Time	CPU	CPU Time	Start Time	Start Address	Base Pri	Dyn Pri	Service	Context Swit...	Susp...	Ideal ...	Cycles Delta	Cycl
Waiting	WtLpcReceive	436	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	13	14		916	1		260,259.5	
Waiting	WtLpcReply	472	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	15	15		6	0		1,371.2	
Waiting	UserRequest	480	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x0000000000000000	13	3		4	0		1,852.9	
Waiting	UserRequest	484	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	13	15		2	1		1,385.9	
Waiting	WtLpcReceive	488	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	13	14		4	0		1,249.7	
Waiting	WtLpcReceive	580	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	13	14		913	1		242,519.3	
Waiting	WtUserRequest	600	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	16	16		251	0		94,241.5	
Waiting	WtUserRequest	604	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	16	16		16	1		3,945.9	
Waiting	WtUserRequest	840	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	12	13		3	0		217.1	
Waiting	WtLpcReceive	808	00:00:00	00:00:00		00:00:00	01/25/26 06:...	0x00007FF882B22690	13	14		851	1		176,009.6	

Autoruns analysis revealed multiple persistence mechanisms established by the malware. These included a user-level Run key, modification of the Winlogon UserInit value, and placement of an executable in the user's Startup folder. All persistence entries referenced randomly named, unsigned executables located in user-writable directories. Although these mechanisms were successfully created, post-reboot process analysis did not show continued malware execution, suggesting the loader failed to retrieve or execute a secondary payload in the isolated environment.

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [DESKTOP-LMBL365\main]

Autoruns Entry	Description	Publisher	Image Path	Times
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Sun Ja
<input checked="" type="checkbox"/> Bsykpehn		(Not Verified)	C:\Users\main\AppData\Local\smhxfexa\bsykpehn.exe	Thu Ji
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\main\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Thu Ji
<input checked="" type="checkbox"/> Ruxiloco		(Not Verified)	C:\Users\main\AppData\Local\Temp\ruxiloco.exe	Thu Ji
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Sat De
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Sun D
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit				Sun Ja
<input checked="" type="checkbox"/> C:\Users\main\AppData\Local\smhxfexa\bsykpehn.exe		(Not Verified)	C:\Users\main\AppData\Local\smhxfexa\bsykpehn.exe	Thu Ji
<input checked="" type="checkbox"/> C:\Users\main\AppData\Local\Temp\ruxiloco.exe		(Not Verified)	C:\Users\main\AppData\Local\Temp\ruxiloco.exe	Thu Ji
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Sun D
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\Installer...	Thu A
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat De
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Sun D
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat De
C:\Users\main\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				Thu Ji
<input checked="" type="checkbox"/> bsykpehn.exe		(Not Verified)	C:\Users\main\AppData\Roaming\Microsoft\Windows\Start Menu\Pro...	Thu Ji

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [DESKTOP-LMBL365\main]

Autoruns Entry	Description	Publisher	Image Path	Times
Task Scheduler				
<input checked="" type="checkbox"/> (Microsoft\Windows\SMB\UninstallSMB1ClientTask	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe	Sun D
<input checked="" type="checkbox"/> (Microsoft\Windows\SMB\UninstallSMB1ServerTask	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe	Sun D
<input checked="" type="checkbox"/> (Microsoft\Windows\Windows Defender\Windows Defender C...	Periodic maintenance task.	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat De
<input checked="" type="checkbox"/> (Microsoft\Windows\Windows Defender\Windows Defender Cl...	Periodic cleanup task.	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat De
<input checked="" type="checkbox"/> (Microsoft\Windows\Windows Defender\Windows Defender Sc...	Periodic scan task.	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat De
<input checked="" type="checkbox"/> (Microsoft\Windows\Windows Defender\Windows Defender Ve...	Periodic verification task.	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Defender\MpCmdRun.exe	Sat De
<input checked="" type="checkbox"/> (Microsoft\Windows\Windows Media Sharing\UpdateLibrary	This task updates the cached list of folder...	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Media Player\wmpnscfg.exe	Fri De
<input checked="" type="checkbox"/> MicrosoftEdgeUpdateTaskMachineCore	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu A
<input checked="" type="checkbox"/> MicrosoftEdgeUpdateTaskMachineUA	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu A
<input checked="" type="checkbox"/> OneDrive Standalone Update Task-5-1-5-21-1823742600-37192...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\main\AppData\Local\Microsoft\OneDrive\OneDriveStandalon...	Thu Ji

Overall analysis indicates that the examined sample functions as a loader-stage Windows malware designed to establish persistence, weaken defenses, and prepare the system for execution of a secondary payload. Static analysis revealed indicators of defense evasion, process execution, and network-aware behavior, while dynamic analysis confirmed successful execution of environment checks and the creation of multiple persistence mechanisms. Despite these activities, post-reboot analysis showed no continued malicious execution, likely due to the absence of network connectivity preventing retrieval or activation of a second-stage payload. This sample seems to be an initial component which performs setup tasks before handing off execution to a more fully featured payload under favorable conditions.

## Indicators of Compromise

### File Paths

- C:\Users\main\Desktop\sample.exe
- C:\Users\main\AppData\Local\smhxfexa\bsykpehn.exe
- C:\Users\main\AppData\Local\Temp\ruxiloco.exe
- C:\Users\main\AppData\Local\Temp\koqpwqnt.exe
- C:\Users\main\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\bsykpehn.exe
- C:\Users\main\AppData\Local\smhxfexa\

### Registry Keys/Values

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\BsyKpehn  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Ruxluco  
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit  
HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes  
HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions  
HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes  
HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions

### Associated Executables Referenced

svchost.exe  
rundll32.exe  
explorer.exe  
consent.exe  
spoolsv.exe

### Behavioral Indicators

Creation of randomly named executables in user-writable directories  
Multiple persistence mechanisms (Run key, Winlogon UserInit, Startup folder)  
Attempts to modify Microsoft Defender exclusion lists  
Repeated DNS resolution attempts prior to payload retrieval

### Recommendations

If this malware were encountered in a real world environment, recommended mitigation steps would focus on rapid isolation, removal of persistence mechanisms, and prevention of reinfection. The affected system should be immediately isolated from the network to prevent further communication and potential delivery of additional payloads. All identified persistence artifacts, including malicious registry Run keys and startup folder executables, should be removed. Additionally, all dropped files in directories such as AppData and Temp should be deleted. Security controls should then be reviewed to ensure no unauthorized Microsoft Defender or antimalware exclusions remain in place, followed by a full system scan with updated signatures. As a precaution, credentials associated with the affected user should be reset. To reduce future risk, systems should be kept fully up to date, the ability to run unknown programs should be limited, and software execution from temporary or user-writable directories should be restricted. User awareness should also be reinforced about the risks of executing untrusted downloads.