Final Malware Analysis Report: Gen:Variant.MSIL.Packy.1

Name: Piyush Babele **Intern Id: 386**

□ Sample Overview

Field	: Value
Malware Name	: Gen:Variant.MSIL.Packy.1
SHA-256	: c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
File Type	: PE32 executable (.NET assembly) for Microsoft Windows
File Size	: 476 KB (487,442 bytes)
AV Detections	: 21/38 antivirus engines
Sandbox Verdict	: Malicious –Threat Score: 100/100

📖 Extended Executive Summary

Gen:Variant.MSIL.Packy.1 is a heavily packed malicious ***.NET trojan*** detected across multiple AV engines as ***MSIL.Packy.Generic***. The malware's capabilities focus on ***stealing credentials, establishing persistence, injecting processes, manipulating the Windows registry,*** and ***exfiltrating data to remote C2 servers.***

Key Authentic Observations:

1. Credential Theft:
   - Reads browser-stored sensitive information.
   - Extracts credentials from FTP clients, mail applications, Putty/Winscp, and instant messengers.
   - Reads and exfiltrates related registry keys.
2. Persistence & Registry Manipulation:
   - Modifies Run registry keys (HKCU/HKLM) to achieve auto-start.
   - Creates/edits extensive ***Tracing, StartupApproved,*** and ***Certificate keys.***
   - Deletes and modifies `AuthRoot\Certificates` keys to evade detection.
3. Process Injection & Mutex Usage:

  - Spawns multiple processes including `explorer.exe`, `svchost.exe`, `wuapihost.exe`.
  - Injects into temporary executables (e.g., EB93A6J996E.exe) to hide payload execution.
  - Creates and checks for mutexes like `Global\.net clr networking`, `ShimCacheMutex` to avoid reinfection.

4. Anti-Analysis:
   - Uses sleep/delay mechanisms to evade sandbox detection.
   - Modifies tracing settings and console tracing masks to erase evidence.
   - Deletes registry keys, schedules tasks, and cleans temporary files.
5. Data Exfiltration & Network Behavior:
   - Uses web protocols (HTTP/HTTPS) for C2 communication.
   - Contacts domains and IPs in Turkey and the USA, sending stolen information and receiving commands.

Risk: High – The sample shows advanced techniques across multiple MITRE ATT&CK tactics, leading to ***credential theft, long-term persistence, and lateral movement risk.***

🔎 Static Analysis Details

- Type: .NET packed executable (PE32 GUI)
- MD5: 7c0f36e996d94d01723372eda8309d81
- SHA1: d31c4ec96b75c6ec8c7e8e7f3d4b62983db040
- Packing: Custom .NET packer with high-entropy sections
- Extracted File: Log file written at `%LOCALAPPDATA%\Microsoft\CLR_v2.0_32\UsageLogs\<hash>.unknown.exe.log`

💣 Dynamic Analysis Details

Processes Observed:

- Main process: `jaga.exe` (PID: 3740)
- Spawned: `explorer.exe`, `svchost.exe`, `wuapihost.exe`, multiple temp executables
- Process injection:
  - Injected into `EB93A6J996E.exe`

  - Injected into other user-space processes

Mutexes:

- Opened:
  - `Global\.net clr networking`
  - `Global\CLR_CASOFF_MUTEX`
  - `ShimCacheMutex`
  - `.MSFTHISTORY.`
- Created:
  - `Global\SQMWindowsConsolidator`
  - `Local\MSCTF.Asm.MutexDefault0`
  - Numerous `CTF.Asm.MutexDefaults-<SID>`

Registry Keys (Persistence & Evasion):

- Created/Modified:
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\International Business Machines Corp`
  - `HKLM\SOFTWARE\Microsoft\SQMClient\Windows\AdaptiveSqm\ManifestInfo\Version`
  - Multiple keys under `HKLM\SOFTWARE\Microsoft\Tracing` (EnableConsoleTracing, FileDirectory, MaxFileSize)
  - Tracing, StartupApproved, Explorer\StartupApproved\Run keys modified
- Deleted:
  - `HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\*`
  - `HKLM\Software\WOW6432Node\Microsoft\Tracing` keys (to evade logging)

Shell Commands Executed:

- Executed payload from `%SAMPLEPATH%`
- Scheduled tasks via `schtasks.exe`
- Cleaned up traces with `schtasks.exe /delete`
- Ran from temp locations: `sbiizwpf.exe`

Privileges:

- Requested SE_DEBUG_PRIVILEGE to inject into system processes

---

🌐 Network Indicators (IOCs)

Domains Queried:

- `hailmofset.com.tr` → IP: `185.150.128.28` (Turkey)
- `checkip.dyndns.org` → IP: `216.146.38.70` (United States)

Contacted Hosts:

- `185.150.128.28` – TCP/443 (HTTPS) – associated with data exfiltration
- `216.146.38.70` – TCP/80 (HTTP) – associated with external IP checks

🕵️‍♀️ MITRE ATT&CK Mapping (Matched)

Technique Id	Technique Description	Tactic Description	Malicious Indicators Count	Suspicious Indicators Count	Informative Indicators Count
T1590.005	IP Addresses	Reconnaissance	0	1	0
T1583.001	Domains	Resource Development	0	0	1
T1106	Native API	Execution	0	0	10
T1047	Windows Management Instrumentation	Execution	0	1	1
T1569.002	Service Execution	Execution	0	0	2
T1059.003	Windows Command Shell	Execution	0	0	1
T1129	Shared Modules	Execution	0	0	5
T1059	Command and Scripting Interpreter	Execution	0	0	1
T1204.002	Malicious File	Execution	2	0	0
T1543.003	Windows Service	Persistence	0	0	2
T1205.002	Socket Filters	Persistence	0	0	1
T1112	Modify Registry	Persistence	1	1	1
T1547	Boot or Logon Autostart Execution	Persistence	0	2	0
T1547.001	Registry Run Keys /	Persistence	0	1	0

	Startup Folder				
T1546.015	Component Object Model Hijacking	Persistence	0	0	2
T1543.003	Windows Service	Privilege Escalation	0	0	2
T1134.001	Token Impersonation/Theft	Privilege Escalation	0	0	1
T1055.001	Dynamic-link Library Injection	Privilege Escalation	0	0	1
T1055.015	ListPlanting	Privilege Escalation	0	0	1
T1055	Process Injection	Privilege Escalation	2	2	2
T1055.011	Extra Window Memory Injection	Privilege Escalation	0	1	0
T1547	Boot or Logon Autostart Execution	Privilege Escalation	0	2	0
T1134	Access Token Manipulation	Privilege Escalation	0	0	2
T1055.003	Thread Execution Hijacking	Privilege Escalation	0	0	1
T1055.002	Portable Executable Injection	Privilege Escalation	0	0	1
T1547.001	Registry Run Keys / Startup Folder	Privilege Escalation	0	1	0
T1055.012	Process Hollowing	Privilege Escalation	1	0	0
T1055.004	Asynchronous Procedure Call	Privilege Escalation	0	0	1
T1546.015	Component Object Model Hijacking	Privilege Escalation	0	0	2
T1205.002	Socket Filters	Defense Evasion	0	0	1

T1027	Obfuscated Files or Information	Defense Evasion	0	2	9
T1070.006	Timestomp	Defense Evasion	0	1	1
T1620	Reflective Code Loading	Defense Evasion	0	0	1
T1134.001	Token Impersonation/Theft	Defense Evasion	0	0	1
T1055.001	Dynamic-link Library Injection	Defense Evasion	0	0	1
T1112	Modify Registry	Defense Evasion	1	1	1
T1055.015	ListPlanting	Defense Evasion	0	0	1
T1562.001	Disable or Modify Tools	Defense Evasion	0	1	3
T1497.001	System Checks	Defense Evasion	0	0	1
T1497.002	User Activity Based Checks	Defense Evasion	0	0	2
T1055	Process Injection	Defense Evasion	2	2	2
T1140	Deobfuscate/Decode Files or Information	Defense Evasion	0	1	3
T1497	Virtualization/Sandbox Evasion	Defense Evasion	0	1	2
T1564.003	Hidden Window	Defense Evasion	0	0	1
T1070.004	File Deletion	Defense Evasion	1	1	1
T1564	Hide Artifacts	Defense Evasion	0	0	1
T1055.011	Extra Window Memory Injection	Defense Evasion	0	1	0
T1134	Access Token Manipulation	Defense Evasion	0	0	2

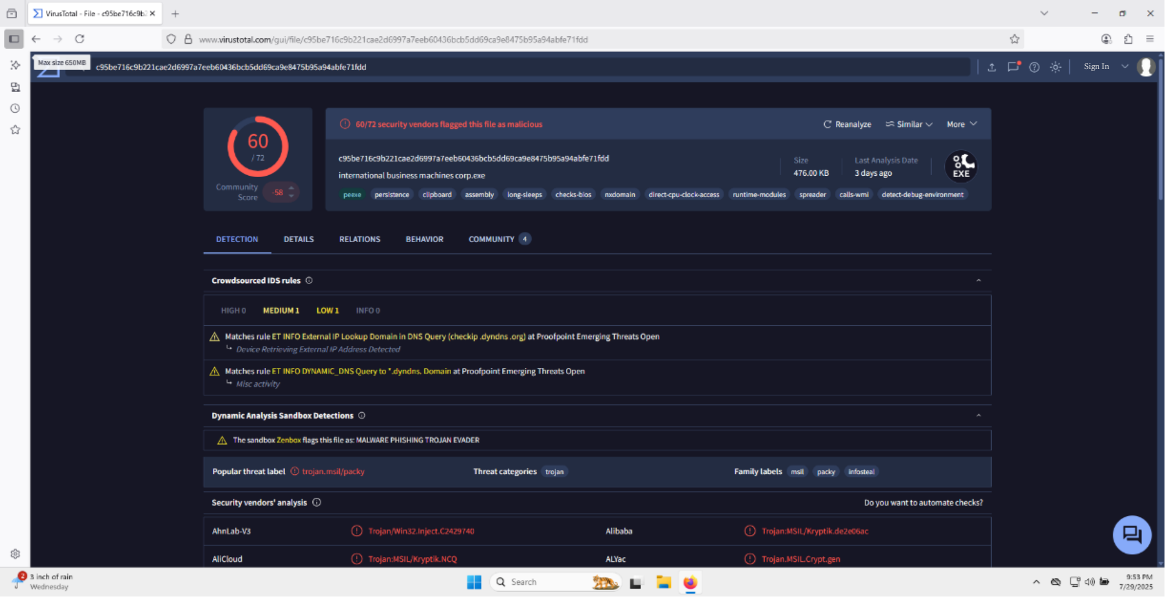
T1055.003	Thread Execution Hijacking	Defense Evasion	0	0	1
T1055.002	Portable Executable Injection	Defense Evasion	0	0	1
T1497.003	Time Based Evasion	Defense Evasion	0	1	1
T1480	Execution Guardrails	Defense Evasion	0	0	2
T1055.012	Process Hollowing	Defense Evasion	1	0	0
T1055.004	Asynchronous Procedure Call	Defense Evasion	0	0	1
T1622	Debugger Evasion	Defense Evasion	0	1	0
T1553.002	Code Signing	Defense Evasion	0	0	1
T1027.002	Software Packing	Defense Evasion	0	1	1
T1027.009	Embedded Payloads	Defense Evasion	0	1	1
T1036.008	Masquerade File Type	Defense Evasion	0	1	0
T1027.005	Indicator Removal from Tools	Defense Evasion	0	0	1
T1036	Masquerading	Defense Evasion	0	0	1
T1056.001	Keylogging	Credential Access	0	1	2
T1003	OS Credential Dumping	Credential Access	0	0	1
T1558	Steal or Forge Kerberos Tickets	Credential Access	0	0	1
T1555	Credentials from Password Stores	Credential Access	0	0	2
T1555.003	Credentials from Web Browsers	Credential Access	1	0	0
T1552.002	Credentials in Registry	Credential Access	2	0	0

T1082	System Information Discovery	Discovery	1	2	20
T1083	File and Directory Discovery	Discovery	0	1	10
T1010	Application Window Discovery	Discovery	0	0	3
T1057	Process Discovery	Discovery	1	2	9
T1016	System Network Configuration Discovery	Discovery	2	0	1
T1497.001	System Checks	Discovery	0	0	1
T1012	Query Registry	Discovery	1	1	6
T1497.002	User Activity Based Checks	Discovery	0	0	2
T1497	Virtualization/Sandbox Evasion	Discovery	0	1	2
T1614.001	System Language Discovery	Discovery	0	0	2
T1124	System Time Discovery	Discovery	0	0	1
T1007	System Service Discovery	Discovery	0	0	2
T1614	System Location Discovery	Discovery	0	0	1
T1497.003	Time Based Evasion	Discovery	0	1	1
T1622	Debugger Evasion	Discovery	0	1	0
T1033	System Owner/User Discovery	Discovery	0	0	1
T1518	Software Discovery	Discovery	0	0	1
T1570	Lateral Tool Transfer	Lateral Movement	0	0	1
T1074.001	Local Data Staging	Collection	0	0	4

T1113	Screen Capture	Collection	0	0	1
T1114	Email Collection	Collection	1	1	1
T1005	Data from Local System	Collection	2	2	1
T1056.001	Keylogging	Collection	0	1	2
T1213	Data from Information Repositories	Collection	0	0	1
T1119	Automated Collection	Collection	0	1	1
T1071	Application Layer Protocol	Command and Control	0	1	7
T1205.002	Socket Filters	Command and Control	0	0	1
T1090	Proxy	Command and Control	0	0	1
T1071.001	Web Protocols	Command and Control	0	4	5
T1573	Encrypted Channel	Command and Control	0	1	2
T1105	Ingress Tool Transfer	Command and Control	0	1	2
T1573.002	Asymmetric Cryptography	Command and Control	0	1	0
T1568.002	Domain Generation Algorithms	Command and Control	0	0	1
T1132	Data Encoding	Command and Control	0	0	1
T1071.004	DNS	Command and Control	0	0	1
T1571	Non-Standard Port	Command and Control	0	1	0
T1573.001	Symmetric Cryptography	Command and Control	0	0	1

T1029	Scheduled Transfer	Exfiltration	0	0	1
T1489	Service Stop	Impact	0	1	3
T1486	Data Encrypted for Impact	Impact	0	2	3
T1529	System Shutdown/Reboot	Impact	0	0	1

VirusTotal Summary



60/72 security vendors flagged this file as malicious

c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

international business machines corp.exe

Size 476.00 KB — Last Analysis Date 3 days ago

peexe persistence clipboard assembly long-sleeps checks-bios nxdomain direct-cpu-clock-access runtime-modules spreader calls-wmi detect-debug-environment

Crowdsourced IDS rules

HIGH 0 MEDIUM 1 LOW 1 INFO 0

⚠ Matches rule ET INFO External IP Lookup Domain in DNS Query (checkip .dyndns .org) at Proofpoint Emerging Threats Open
↳ *Device Retrieving External IP Address Detected*

⚠ Matches rule ET INFO DYNAMIC_DNS Query to *.dyndns. Domain at Proofpoint Emerging Threats Open
↳ *Misc activity*

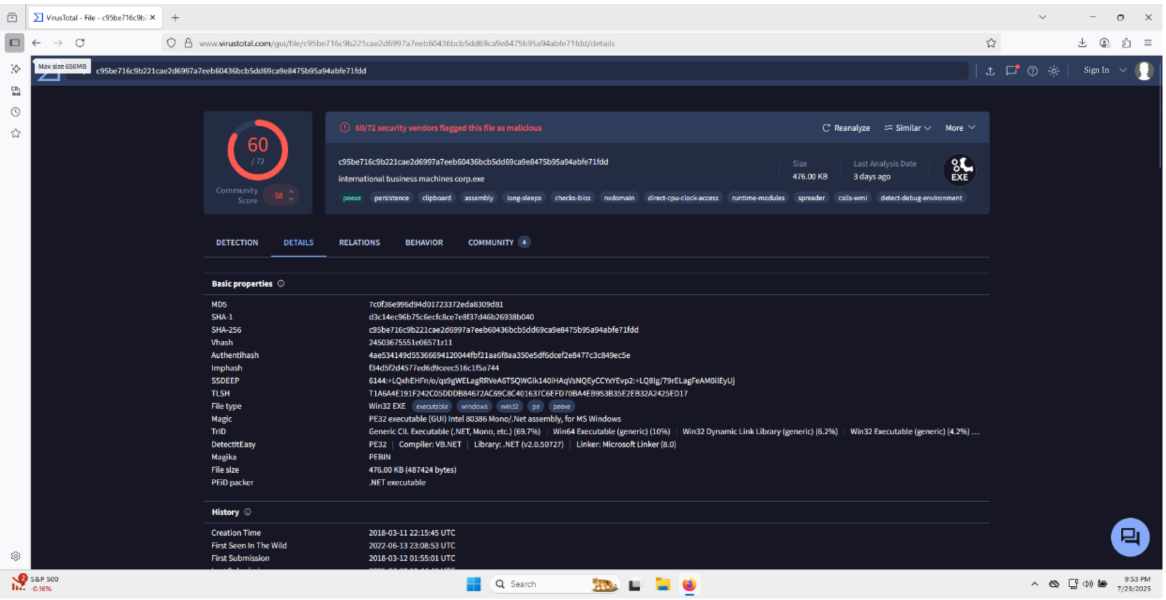
Dynamic Analysis Sandbox Detections

⚠ The sandbox Zenbox flags this file as: MALWARE PHISHING TROJAN EVADER

Popular threat label: trojan.msil/packy — Threat categories: trojan — Family labels: msil packy infosteal

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Inject.C2429740	Alibaba	Trojan:MSIL/Kryptik.de2e06ac
AliCloud	Trojan:MSIL/Kryptik.NCQ	ALYac	Trojan.MSIL.Crypt.gen



60/72 security vendors flagged this file as malicious

c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

international business machines corp.exe

Size 476.00 KB — Last Analysis Date 3 days ago

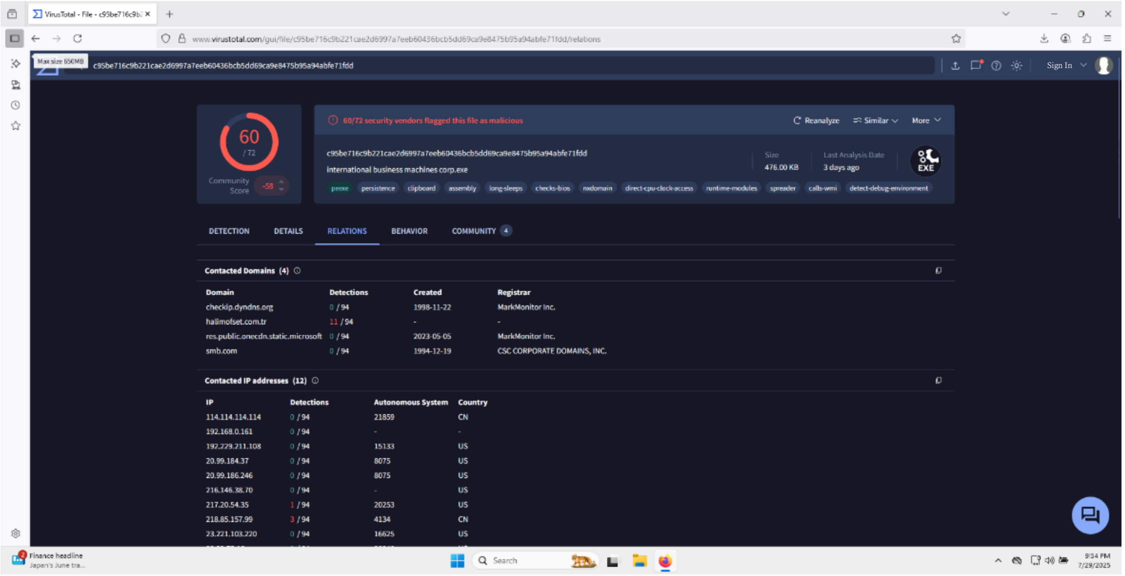
peexe persistence clipboard assembly long-sleeps checks-bios nxdomain direct-cpu-clock-access runtime-modules spreader calls-wmi detect-debug-environment

Basic properties

MD5	7c0f36e996d94d01723372eda8309d81
SHA-1	d3c14ec96b75c6ecfc8ce7e8f37d46b26938b040
SHA-256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
Vhash	24503675551e06571z11
Authentihash	4ae534149d55366694120044fbf21aa6f8aa350e5df6dcef2e8477c3c849ec5e
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	6144:+LQxhEHFn/o/qs9gWELagRRVeA6TSQWGlk140iHAqVsNQEyCCYxYEvp2:+LQ8lg/79rELagFeAM0ilEyUj
TLSH	T1A6A4E191F242C05DDDB84672AC69C8C401637C6EFD70BA4EB953B35E2EB32A2425ED17
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (69.7%) | Win64 Executable (generic) (10%) | Win32 Dynamic Link Library (generic) (6.2%) | Win32 Executable (generic) (4.2%) ...
DetectItEasy	PE32 | Compiler: VB.NET | Library: .NET (v2.0.50727) | Linker: Microsoft Linker (8.0)
Magika	PEBIN
File size	476.00 KB (487424 bytes)
PEiD packer	.NET executable

History

Creation Time	2018-03-11 22:15:45 UTC
First Seen In The Wild	2022-06-13 23:08:53 UTC
First Submission	2018-03-12 01:55:01 UTC


VirusTotal - File - c95be716c9b
www.virustotal.com/gui/file/c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd/relations
Max size 650MB
Sign In
60
/ 72
Community Score
-58
Reanalyze
Similar
More
EXE
Finance headline
Japan's June tra...
Search
9:54 PM
7/29/2025

c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

60/72 security vendors flagged this file as malicious

c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
international business machines corp.exe

Size: 476.00 KB
Last Analysis Date: 3 days ago

peexe persistence clipboard assembly long-sleeps checks-bios nxdomain direct-cpu-clock-access runtime-modules spreader calls-wmi detect-debug-environment

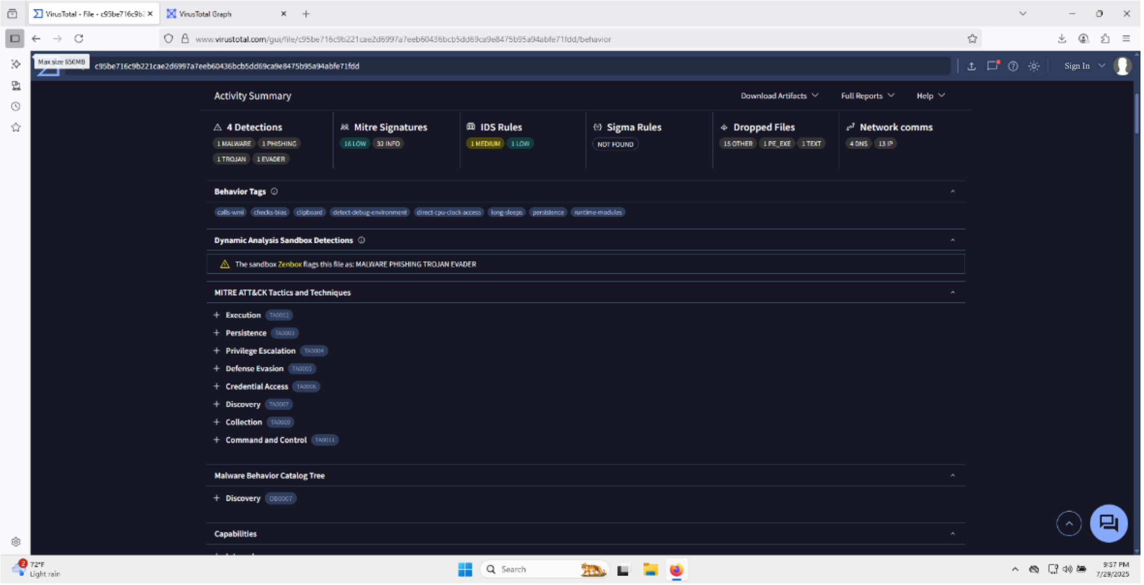
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

Contacted Domains (4)

Domain	Detections	Created	Registrar
checkip.dyndns.org	0 / 94	1998-11-22	MarkMonitor Inc.
halimofset.com.tr	11 / 94	-	-
res.public.onecdn.static.microsoft	0 / 94	2023-05-05	MarkMonitor Inc.
smb.com	0 / 94	1994-12-19	CSC CORPORATE DOMAINS, INC.

Contacted IP addresses (12)

IP	Detections	Autonomous System	Country
114.114.114.114	0 / 94	21859	CN
192.168.0.161	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
20.99.184.37	0 / 94	8075	US
20.99.186.246	0 / 94	8075	US
216.146.38.70	0 / 94	-	US
217.20.54.35	1 / 94	20253	US
218.85.157.99	3 / 94	4134	CN
23.221.103.220	0 / 94	16625	US


VirusTotal - File - c95be716c9b
VirusTotal Graph
www.virustotal.com/gui/file/c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd/behavior
Max size 650MB
Sign In
Download Artifacts
Full Reports
Help
72°F
Light rain
Search
9:57 PM
7/29/2025

c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

Activity Summary

4 Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
1 MALWARE 1 PHISHING 1 TROJAN 1 EVADER	16 LOW 32 INFO	1 MEDIUM 1 LOW	NOT FOUND	15 OTHER 1 PE_EXE 1 TEXT	4 DNS 13 IP

Behavior Tags

calls-wmi checks-bios clipboard detect-debug-environment direct-cpu-clock-access long-sleeps persistence runtime-modules

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE PHISHING TROJAN EVADER

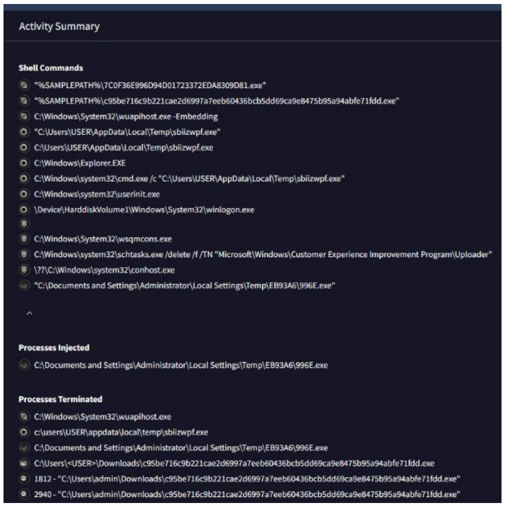
MITRE ATT&CK Tactics and Techniques

- Execution TA0002
- Persistence TA0003
- Privilege Escalation TA0004
- Defense Evasion TA0005
- Credential Access TA0006
- Discovery TA0007
- Collection TA0009
- Command and Control TA0011

Malware Behavior Catalog Tree

- Discovery OB0007

Capabilities



Activity Summary

Shell Commands

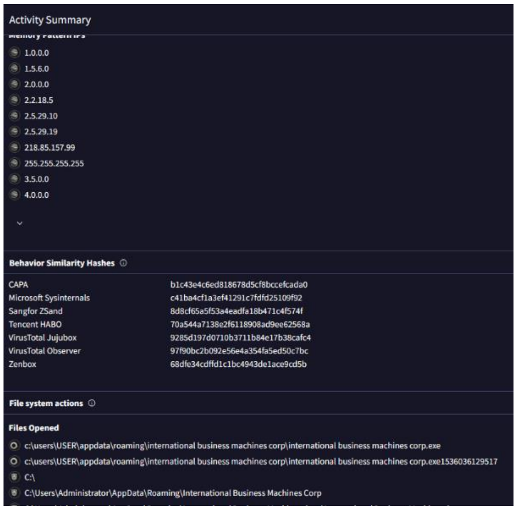
```
"%SAMPLEPATH%\7C0F36E996D94D01723372EDA8309D81.exe"
"%SAMPLEPATH%\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe"
C:\Windows\System32\wuapihost.exe -Embedding
"C:\Users\USER\AppData\Local\Temp\sbiizwpf.exe"
C:\Users\USER\AppData\Local\Temp\sbiizwpf.exe
C:\Windows\Explorer.EXE
C:\Windows\system32\cmd.exe /c "C:\Users\USER\AppData\Local\Temp\sbiizwpf.exe"
C:\Windows\system32\userinit.exe
\Device\HarddiskVolume1\Windows\System32\winlogon.exe

C:\Windows\System32\wsqmcons.exe
C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"
\??\C:\Windows\system32\conhost.exe
"C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe"
```

Processes Injected

```
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
```

Processes Terminated

```
C:\Windows\System32\wuapihost.exe
c:\users\USER\appdata\local\temp\sbiizwpf.exe
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
C:\Users\<USER>\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe
1812 - "C:\Users\admin\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe"
2940 - "C:\Users\admin\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe"
```



Activity Summary

Memory Pattern IPs

- 1.0.0.0
- 1.5.6.0
- 2.0.0.0
- 2.2.18.5
- 2.5.29.10
- 2.5.29.19
- 218.85.157.99
- 255.255.255.255
- 3.5.0.0
- 4.0.0.0

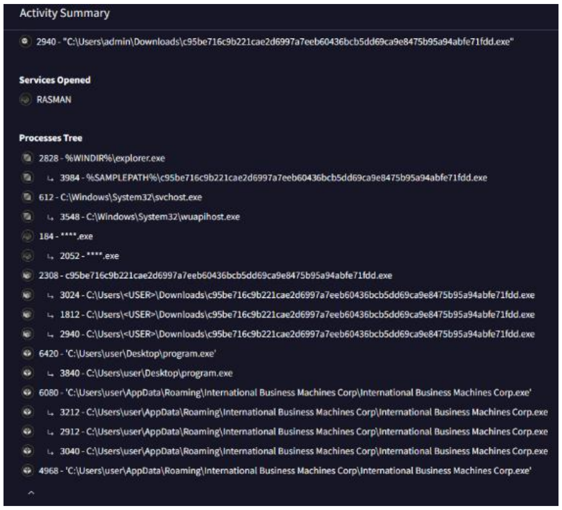
Behavior Similarity Hashes

CAPA	b1c43e4c6ed818678d5cf8bccefcada0
Microsoft Sysinternals	c41ba4cf1a3ef41291c7fdfd25109f92
Sangfor ZSand	8d8cf65a5f53a4eadfa18b471c4f574f
Tencent HABO	70a544a7138e2f6118908ad9ee62568a
VirusTotal Jujubox	9285d197d0710b3711b84e17b38cafc4
VirusTotal Observer	97f90bc2b092e56e4a354fa5ed50c7bc
Zenbox	68dfe34cdffd1c1bc4943de1ace9cd5b

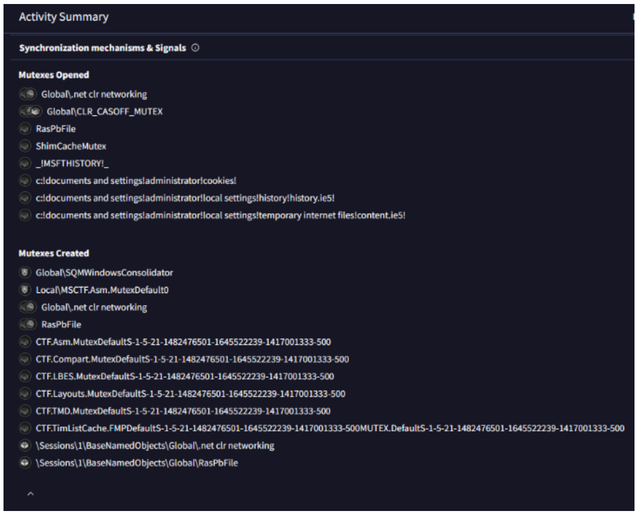
File system actions

Files Opened

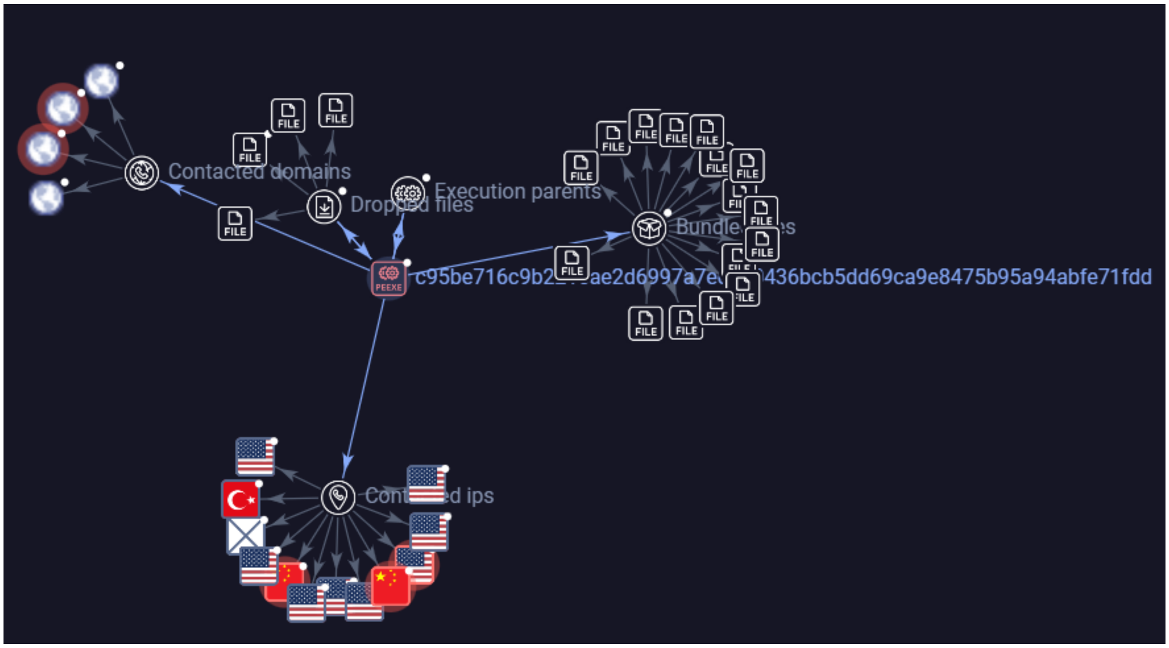
```
c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe
c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe1536036129517
C:\
C:\Users\Administrator\AppData\Roaming\International Business Machines Corp
```

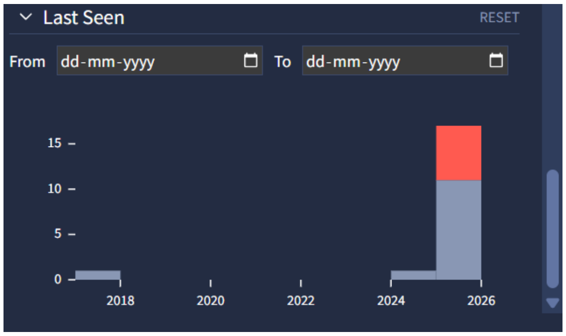


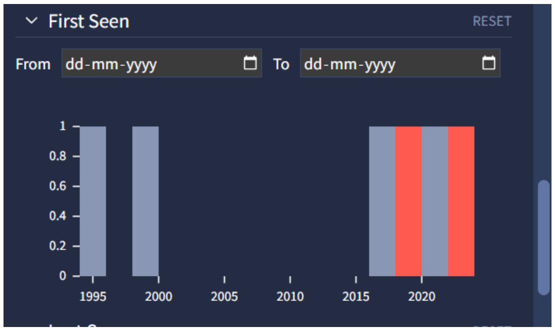
```
Activity Summary
2940 - "C:\Users\admin\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe"

Services Opened
RASMAN

Processes Tree
2828 - %WINDIR%\explorer.exe
  ↳ 3984 - %SAMPLEPATH%\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe
612 - C:\Windows\System32\svchost.exe
  ↳ 3548 - C:\Windows\System32\wuapihost.exe
184 - ****.exe
  ↳ 2052 - ****.exe
2308 - c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe
  ↳ 3024 - C:\Users\<USER>\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe
  ↳ 1812 - C:\Users\<USER>\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe
  ↳ 2940 - C:\Users\<USER>\Downloads\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.exe
6420 - 'C:\Users\user\Desktop\program.exe'
  ↳ 3840 - C:\Users\user\Desktop\program.exe
6080 - 'C:\Users\user\AppData\Roaming\International Business Machines Corp\International Business Machines Corp.exe'
  ↳ 3212 - C:\Users\user\AppData\Roaming\International Business Machines Corp\International Business Machines Corp.exe
  ↳ 2912 - C:\Users\user\AppData\Roaming\International Business Machines Corp\International Business Machines Corp.exe
  ↳ 3040 - C:\Users\user\AppData\Roaming\International Business Machines Corp\International Business Machines Corp.exe
4968 - 'C:\Users\user\AppData\Roaming\International Business Machines Corp\International Business Machines Corp.exe'
```

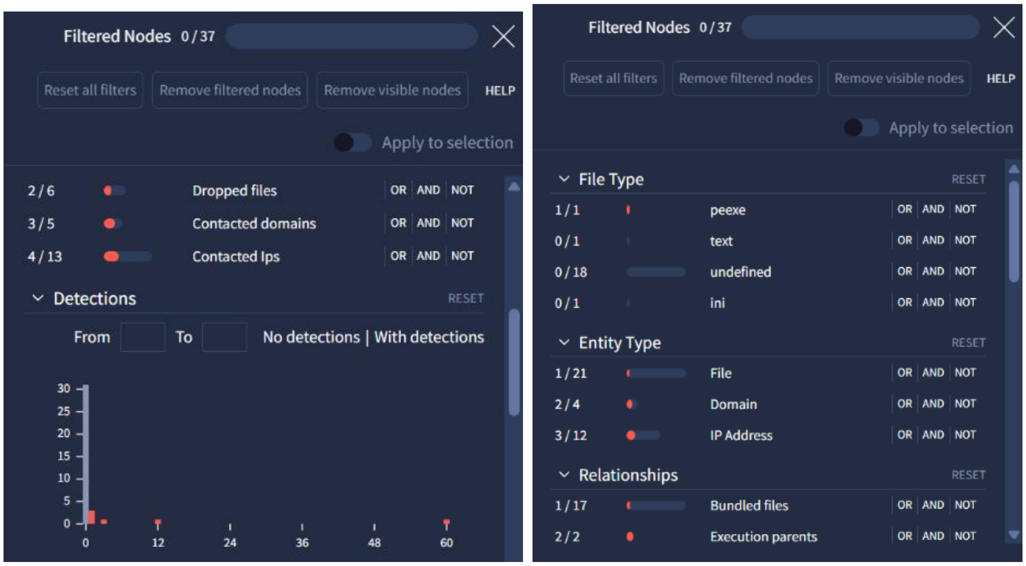


```
Activity Summary
Synchronization mechanisms & Signals ⓘ

Mutexes Opened
Global\.net clr networking
Global\CLR_CASOFF_MUTEX
RasPbFile
ShimCacheMutex
_!MSFTHISTORY!_
c:!documents and settings!administrator!cookies!
c:!documents and settings!administrator!local settings!history!history.ie5!
c:!documents and settings!administrator!local settings!temporary internet files!content.ie5!

Mutexes Created
Global\SQMWindowsConsolidator
Local\MSCTF.Asm.MutexDefault0
Global\.net clr networking
RasPbFile
CTF.Asm.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
CTF.Compart.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
CTF.LBES.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
CTF.Layouts.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
CTF.TMD.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
CTF.TimListCache.FMPDefaultS-1-5-21-1482476501-1645522239-1417001333-500MUTEX.DefaultS-1-5-21-1482476501-1645522239-1417001333-500
\Sessions\1\BaseNamedObjects\Global\.net clr networking
\Sessions\1\BaseNamedObjects\Global\RasPbFile
```









2 / 6 Dropped files
3 / 5 Contacted domains
4 / 13 Contacted Ips

Detections

From To No detections | With detections

File Type

1 / 1 peexe
0 / 1 text
0 / 18 undefined
0 / 1 ini

Entity Type

1 / 21 File
2 / 4 Domain
3 / 12 IP Address

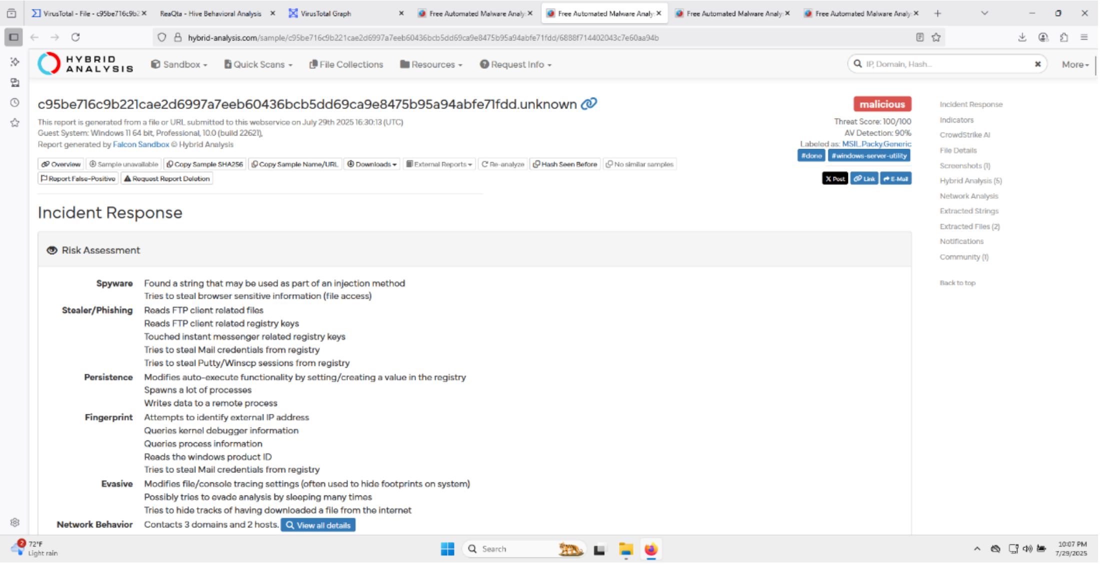
Relationships

1 / 17 Bundled files
2 / 2 Execution parents

VirusTotal Analysis with Graphs

- 60/72 AV engines flagged the sample.
- Observed mutex creation, process injection, and registry persistence (Run keys, Tracing keys).
- Deletes certificate registry keys and uses `schtasks.exe` for persistence and evidence removal.

Hybrid Analysis (Falcon Sandbox) Summary



c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown

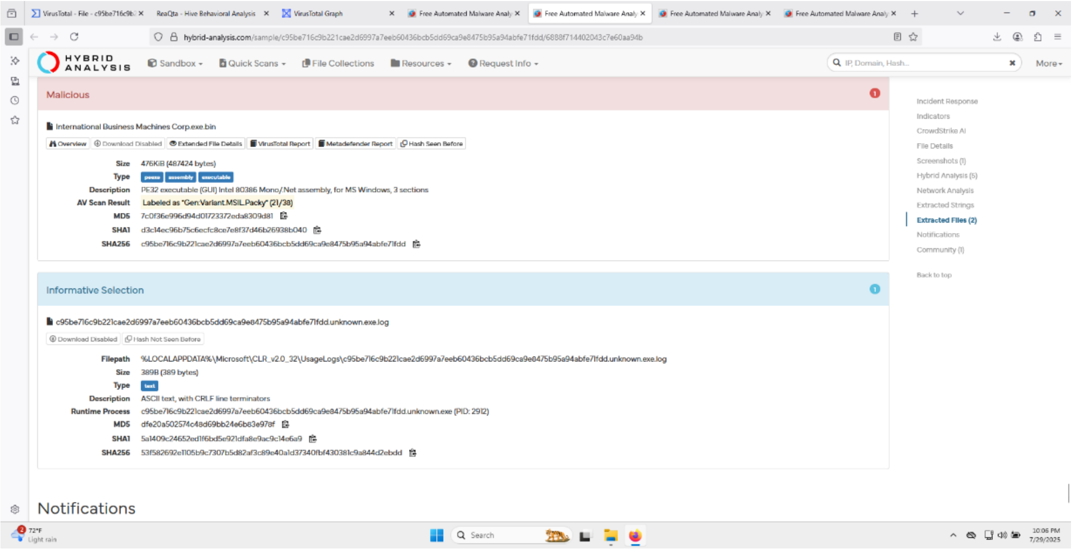
This report is generated from a file or URL submitted to this webservice on July 29th 2025 16:30:13 (UTC)
Guest System: Windows 11 64 bit, Professional, 10.0 (build 22621),
Report generated by Falcon Sandbox © Hybrid Analysis

malicious
Threat Score: 100/100
AV Detection: 90%
Labeled as: MSIL.Packy.Generic
#done #windows-server-utility

Incident Response

Risk Assessment

Spyware	Found a string that may be used as part of an injection method Tries to steal browser sensitive information (file access)
Stealer/Phishing	Reads FTP client related files Reads FTP client related registry keys Touched instant messenger related registry keys Tries to steal Mail credentials from registry Tries to steal Putty/Winscp sessions from registry
Persistence	Modifies auto-execute functionality by setting/creating a value in the registry Spawns a lot of processes Writes data to a remote process
Fingerprint	Attempts to identify external IP address Queries kernel debugger information Queries process information Reads the windows product ID Tries to steal Mail credentials from registry
Evasive	Modifies file/console tracing settings (often used to hide footprints on system) Possibly tries to evade analysis by sleeping many times Tries to hide tracks of having downloaded a file from the internet
Network Behavior	Contacts 3 domains and 2 hosts.



Malicious

International Business Machines Corp.exe.bin

Overview | Download Disabled | Extended File Details | VirusTotal Report | Metadefender Report | Hash Seen Before

Size	476KiB (487424 bytes)
Type	peexe assembly executable
Description	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
AV Scan Result	Labeled as "Gen:Variant.MSIL.Packy" (21/38)
MD5	7c0f36e996d94d01723372eda8309d81
SHA1	d3c14ec96b75c6ecfc8ce7e8f37d46b26938b040
SHA256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

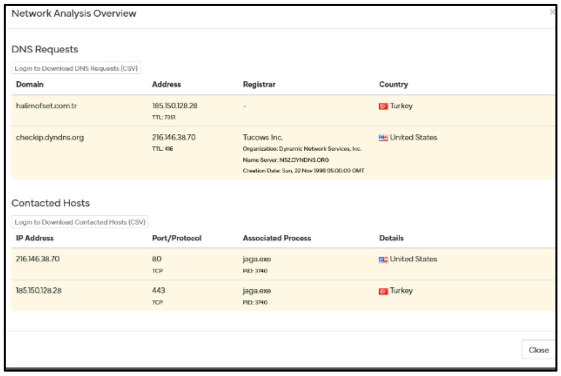
Informative Selection

c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe.log

Download Disabled | Hash Not Seen Before

Filepath	%LOCALAPPDATA%\Microsoft\CLR_v2.0_32\UsageLogs\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe.log
Size	389B (389 bytes)
Type	text
Description	ASCII text, with CRLF line terminators
Runtime Process	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe (PID: 2912)
MD5	dfe20a502574c48d69bb24e6b83e978f
SHA1	5a1409c24652ed1f6bd5e921dfa8e9ac9c14e6a9
SHA256	53f582692e1105b9c7307b5d82af3c89e40a1d37340fbf430381c9a844d2ebdd

Notifications


Login to Download DNS Requests (CSV)
Login to Download Contacted Hosts (CSV)
Close

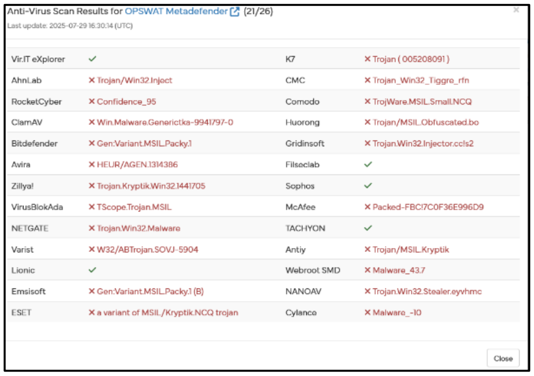
Network Analysis Overview

DNS Requests

Domain	Address	Registrar	Country
halimofset.com.tr	185.150.128.28 TTL: 7351	-	Turkey
checkip.dyndns.org	216.146.38.70 TTL: 416	Tucows Inc. Organization: Dynamic Network Services, Inc. Name Server: NS2.DYNDNS.ORG Creation Date: Sun, 22 Nov 1998 05:00:00 GMT	United States

Contacted Hosts

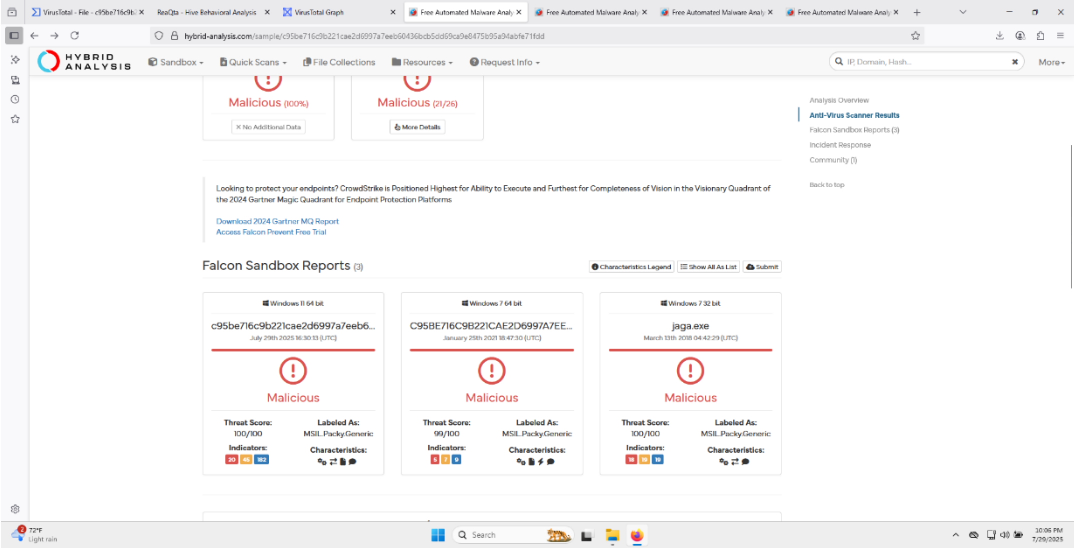
IP Address	Port/Protocol	Associated Process	Details
216.146.38.70	80 TCP	jaga.exe PID: 3740	United States
185.150.128.28	443 TCP	jaga.exe PID: 3740	Turkey



Anti-Virus Scan Results for OPSWAT Metadefender (21/26)

Last update: 2025-07-29 16:30:14 (UTC)

Vir.IT eXplorer	✓	K7	✗ Trojan (005208091)
AhnLab	✗ Trojan/Win32.Inject	CMC	✗ Trojan_Win32_Tiggre_rfn
RocketCyber	✗ Confidence_95	Comodo	✗ TrojWare.MSIL.Small.NCQ
ClamAV	✗ Win.Malware.Generictka-9941797-0	Huorong	✗ Trojan/MSIL.Obfuscated.bo
Bitdefender	✗ Gen:Variant.MSIL.Packy.1	Gridinsoft	✗ Trojan.Win32.Injector.cc!s2
Avira	✗ HEUR/AGEN.1314386	Filseclab	✓
Zillya!	✗ Trojan.Kryptik.Win32.1441705	Sophos	✓
VirusBlokAda	✗ TScope.Trojan.MSIL	McAfee	✗ Packed-FBC!7C0F36E996D9
NETGATE	✗ Trojan.Win32.Malware	TACHYON	✓
Varist	✗ W32/ABTrojan.SOVJ-5904	Antiy	✗ Trojan/MSIL.Kryptik
Lionic	✓	Webroot SMD	✗ Malware_43.7
Emsisoft	✗ Gen:Variant.MSIL.Packy.1 (B)	NANOAV	✗ Trojan.Win32.Stealer.eyvhmc
ESET	✗ a variant of MSIL/Kryptik.NCQ trojan	Cylance	✗ Malware_-10



Malicious (100%)

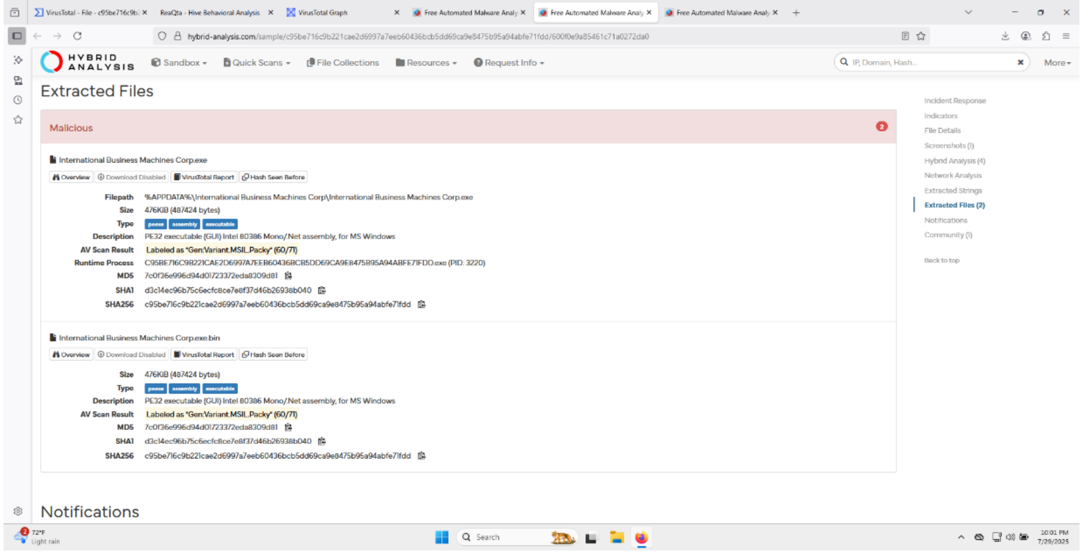
Malicious (21/26)

Looking to protect your endpoints? CrowdStrike is Positioned Highest for Ability to Execute and Furthest for Completeness of Vision in the Visionary Quadrant of the 2024 Gartner Magic Quadrant for Endpoint Protection Platforms

Download 2024 Gartner MQ Report
Access Falcon Prevent Free Trial

Falcon Sandbox Reports (3)

Windows 11 64 bit	Windows 7 64 bit	Windows 7 32 bit
c95be716c9b221cae2d6997a7eeb6...	C95BE716C9B221CAE2D6997A7EE...	jaga.exe
July 29th 2025 16:30:13 (UTC)	January 25th 2021 18:47:30 (UTC)	March 13th 2018 04:42:29 (UTC)
Malicious	Malicious	Malicious
Threat Score: 100/100	Threat Score: 99/100	Threat Score: 100/100
Labeled As: MSIL.Packy.Generic	Labeled As: MSIL.Packy.Generic	Labeled As: MSIL.Packy.Generic
Indicators: 20 45 182	Indicators: 5 7 9	Indicators: 18 10 19
Characteristics:	Characteristics:	Characteristics:



Extracted Files

Malicious

International Business Machines Corp.exe

Overview | Download Disabled | VirusTotal Report | Hash Seen Before

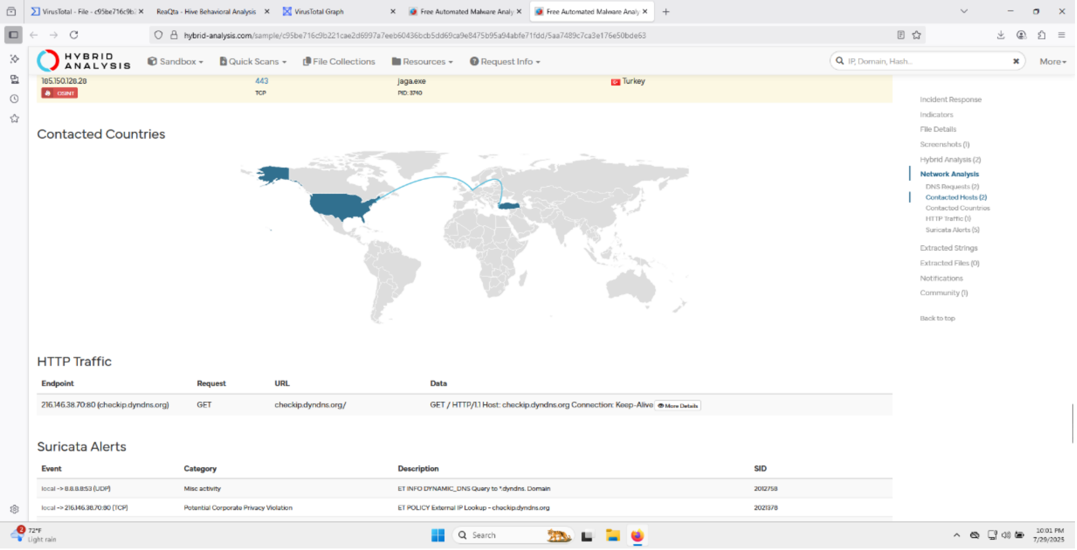
Filepath	%APPDATA%\International Business Machines Corp\International Business Machines Corp.exe
Size	476KiB (487424 bytes)
Type	peexe assembly executable
Description	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
AV Scan Result	Labeled as "Gen:Variant.MSIL.Packy" (60/71)
Runtime Process	C95BE716C9B221CAE2D6997A7EEB60436BCB5DD69CA9E8475B95A94ABFE71FDD.exe (PID: 3220)
MD5	7c0f36e996d94d01723372eda8309d81
SHA1	d3c14ec96b75c6ecfc8ce7e8f37d46b26938b040
SHA256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

International Business Machines Corp.exe.bin

Overview | Download Disabled | VirusTotal Report | Hash Seen Before

Size	476KiB (487424 bytes)
Type	peexe assembly executable
Description	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
AV Scan Result	Labeled as "Gen:Variant.MSIL.Packy" (60/71)
MD5	7c0f36e996d94d01723372eda8309d81
SHA1	d3c14ec96b75c6ecfc8ce7e8f37d46b26938b040
SHA256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

Notifications



185.150.128.28 OSINT	443 TCP	jaga.exe PID: 3740	Turkey

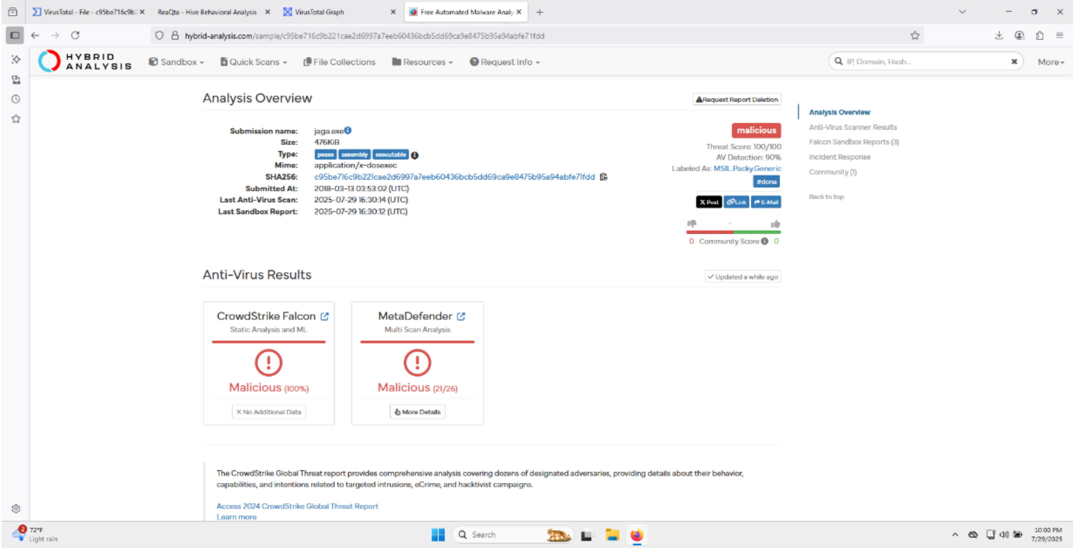
Contacted Countries

HTTP Traffic

Endpoint	Request	URL	Data
216.146.38.70:80 (checkip.dyndns.org)	GET	checkip.dyndns.org/	GET / HTTP/1.1 Host: checkip.dyndns.org Connection: Keep-Alive More Details

Suricata Alerts

Event	Category	Description	SID
local -> 8.8.8.8:53 (UDP)	Misc activity	ET INFO DYNAMIC_DNS Query to *.dyndns. Domain	2012758
local -> 216.146.38.70:80 (TCP)	Potential Corporate Privacy Violation	ET POLICY External IP Lookup - checkip.dyndns.org	2021378



Analysis Overview

Submission name:	jaga.exe
Size:	476KiB
Type:	peexe assembly executable
Mime:	application/x-dosexec
SHA256:	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
Submitted At:	2018-03-13 03:53:02 (UTC)
Last Anti-Virus Scan:	2025-07-29 16:30:14 (UTC)
Last Sandbox Report:	2025-07-29 16:30:12 (UTC)

malicious

Threat Score: 100/100

AV Detection: 90%

Labeled As: MSIL.Packy.Generic

#done

0 Community Score 0

Anti-Virus Results

✓ Updated a while ago

CrowdStrike Falcon

Static Analysis and ML

Malicious (100%)

✕ No Additional Data

MetaDefender

Multi Scan Analysis

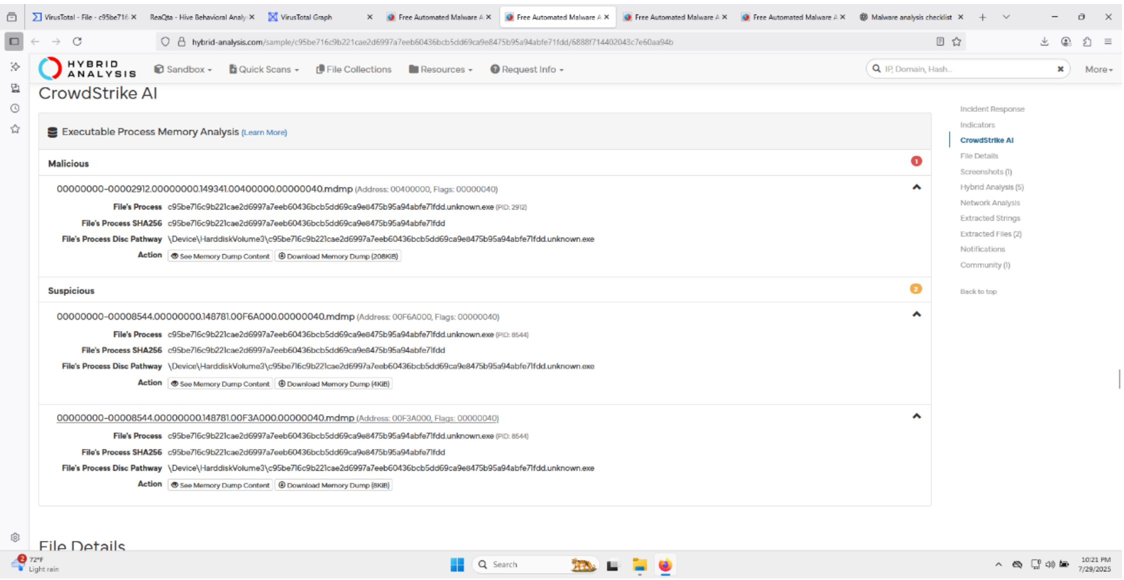
Malicious (21/26)

More Details

The CrowdStrike Global Threat report provides comprehensive analysis covering dozens of designated adversaries, providing details about their behavior, capabilities, and intentions related to targeted intrusions, eCrime, and hacktivist campaigns.

Access 2024 CrowdStrike Global Threat Report

Learn more



CrowdStrike AI

Executable Process Memory Analysis (Learn More)

Malicious

00000000-00002912.00000000.149341.00400000.00000040.mdmp (Address: 00400000, Flags: 00000040)

File's Process	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe (PID: 2912)
File's Process SHA256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
File's Process Disc Pathway	\Device\HarddiskVolume3\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe
Action	See Memory Dump Content · Download Memory Dump (208KiB)

Suspicious

00000000-00008544.00000000.148781.00F6A000.00000040.mdmp (Address: 00F6A000, Flags: 00000040)

File's Process	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe (PID: 8544)
File's Process SHA256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
File's Process Disc Pathway	\Device\HarddiskVolume3\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe
Action	See Memory Dump Content · Download Memory Dump (4KiB)

00000000-00008544.00000000.148781.00F3A000.00000040.mdmp (Address: 00F3A000, Flags: 00000040)

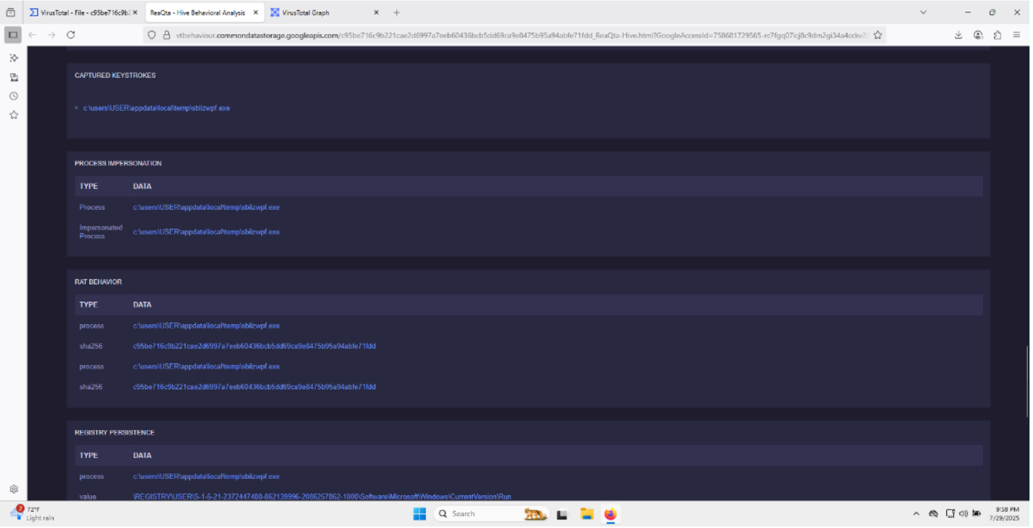
File's Process	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe (PID: 8544)
File's Process SHA256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
File's Process Disc Pathway	\Device\HarddiskVolume3\c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd.unknown.exe
Action	See Memory Dump Content · Download Memory Dump (8KiB)

File Details

Hybrid Analysis Results

- Threat Score 100/100 (Malicious).
- Credential theft from browsers, FTP, mail, instant messengers, and SSH tools.
- Network IOCs: `hailmofset.com.tr` (Turkey) and `checkip.dyndns.org` (USA).
- Uses registry modifications for persistence and evades sandbox detection with tracing settings and sleep delays.

ReaQta (Hive Behavioral Analysis) Summary


VirusTotal - File - c95be716c9b
ReaQta - Hive Behavioral Analysis
VirusTotal Graph

CAPTURED KEYSTROKES

c:\users\USER\appdata\local\temp\sbiizwpf.exe

PROCESS IMPERSONATION

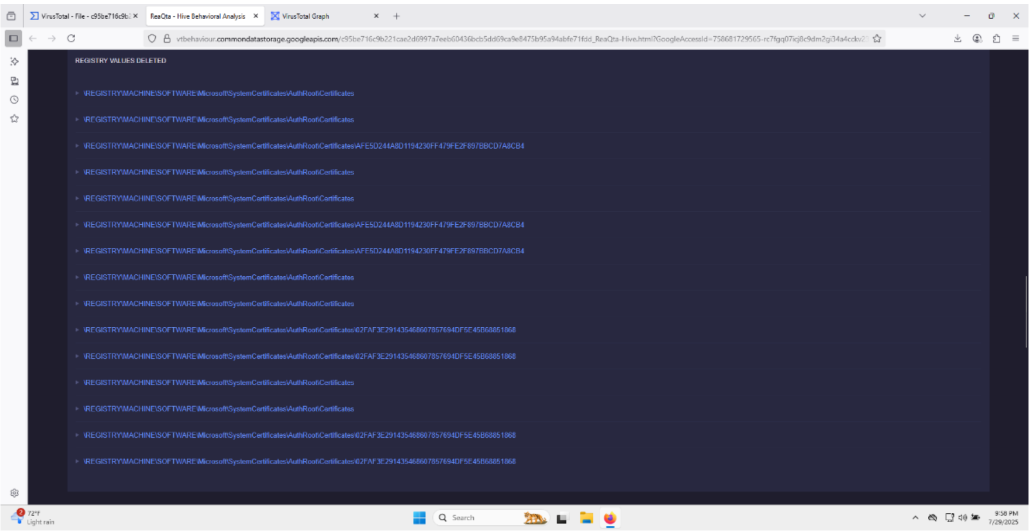
TYPE	DATA
Process	c:\users\USER\appdata\local\temp\sbiizwpf.exe
Impersonated Process	c:\users\USER\appdata\local\temp\sbiizwpf.exe

RAT BEHAVIOR

TYPE	DATA
process	c:\users\USER\appdata\local\temp\sbiizwpf.exe
sha256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
process	c:\users\USER\appdata\local\temp\sbiizwpf.exe
sha256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd

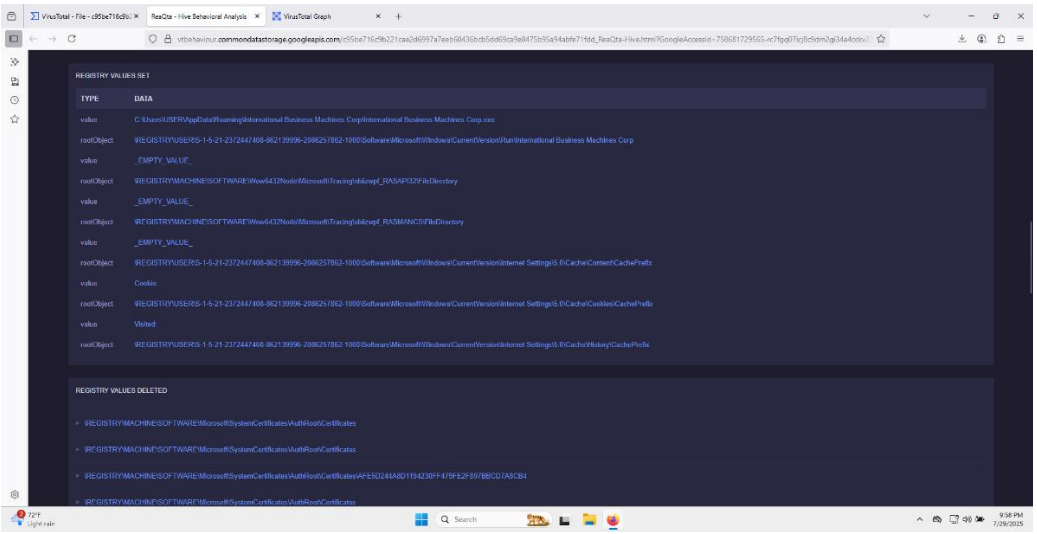
REGISTRY PERSISTENCE

TYPE	DATA
process	c:\users\USER\appdata\local\temp\sbiizwpf.exe
value	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Run


VirusTotal - File - c95be716c9b
ReaQta - Hive Behavioral Analysis
VirusTotal Graph
vtbehaviour.commondatastorage.googleapis.com/c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd_ReaQta-Hive.html?GoogleAccessId=758681729565-rc7fgq07icj8c9dm2gi34a4cckv2
72°F
Light rain
Search
9:58 PM
7/29/2025

REGISTRY VALUES DELETED

```
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\AFE5D244A8D1194230FF479FE2F897BBCD7A8CB4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\AFE5D244A8D1194230FF479FE2F897BBCD7A8CB4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\AFE5D244A8D1194230FF479FE2F897BBCD7A8CB4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E291435468607857694DF5E45B68851868
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E291435468607857694DF5E45B68851868
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E291435468607857694DF5E45B68851868
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\02FAF3E291435468607857694DF5E45B68851868
```

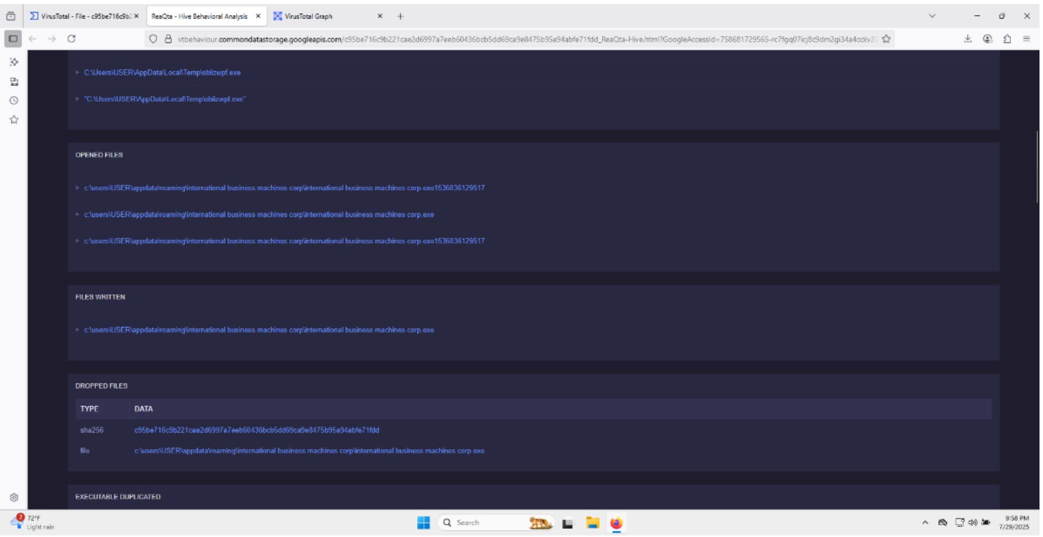

VirusTotal - File - c95be716c9b
ReaQta - Hive Behavioral Analysis
VirusTotal Graph
vtbehaviour.commondatastorage.googleapis.com/c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd_ReaQta-Hive.html?GoogleAccessId=758681729565-rc7fgq07icj8c9dm2gi34a4cckv2
72°F
Light rain
Search
9:58 PM
7/29/2025

REGISTRY VALUES SET

TYPE	DATA
value	C:\Users\USER\AppData\Roaming\International Business Machines Corp\International Business Machines Corp.exe
rootObject	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Run\International Business Machines Corp
value	_EMPTY_VALUE_
rootObject	\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\sbiizwpf_RASAPI32\FileDirectory
value	_EMPTY_VALUE_
rootObject	\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\sbiizwpf_RASMANCS\FileDirectory
value	_EMPTY_VALUE_
rootObject	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix
value	Cookie:
rootObject	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix
value	Visited:
rootObject	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix

REGISTRY VALUES DELETED

```
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\AFE5D244A8D1194230FF479FE2F897BBCD7A8CB4
\REGISTRY\MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates
```


VirusTotal - File - c95be716c9b
ReaQta - Hive Behavioral Analysis
VirusTotal Graph
vtbehaviour.commondatastorage.googleapis.com/c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd_ReaQta-Hive.html?GoogleAccessId=758681729565-rc7fgq07icj8c9dm2gi34a4cckv2
72°F
Light rain
Search
9:58 PM
7/29/2025

```
C:\Users\USER\AppData\Local\Temp\sbiizwpf.exe
"C:\Users\USER\AppData\Local\Temp\sbiizwpf.exe"
```

OPENED FILES

```
c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe1536036129517
c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe
c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe1536036129517
```

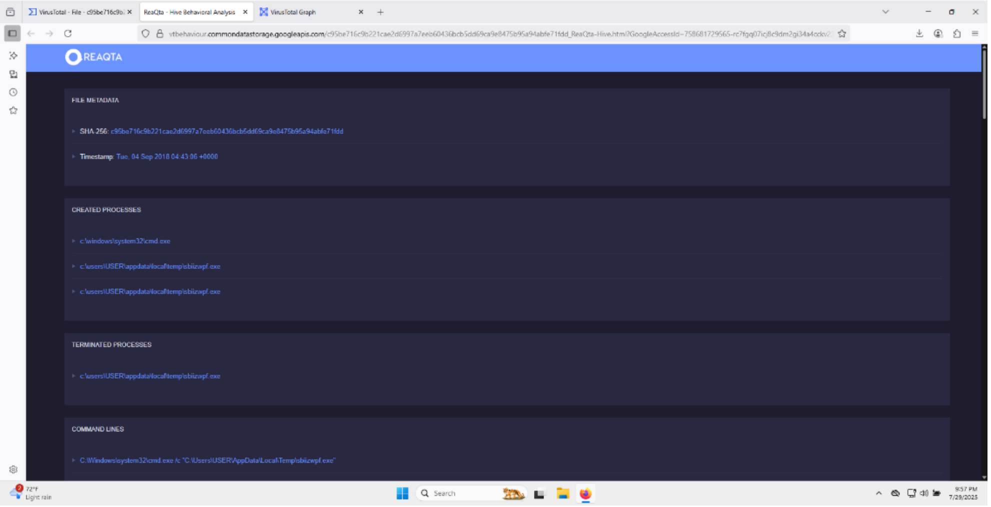
FILES WRITTEN

```
c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe
```

DROPPED FILES

TYPE	DATA
sha256	c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
file	c:\users\USER\appdata\roaming\international business machines corp\international business machines corp.exe

EXECUTABLE DUPLICATED



VirusTotal - File - c95be716c9b
ReaQta - Hive Behavioral Analysis
VirusTotal Graph
REAQTA
72°F
Light rain
Search

FILE METADATA

- SHA-256: c95be716c9b221cae2d6997a7eeb60436bcb5dd69ca9e8475b95a94abfe71fdd
- Timestamp: Tue, 04 Sep 2018 04:43:06 +0000

CREATED PROCESSES

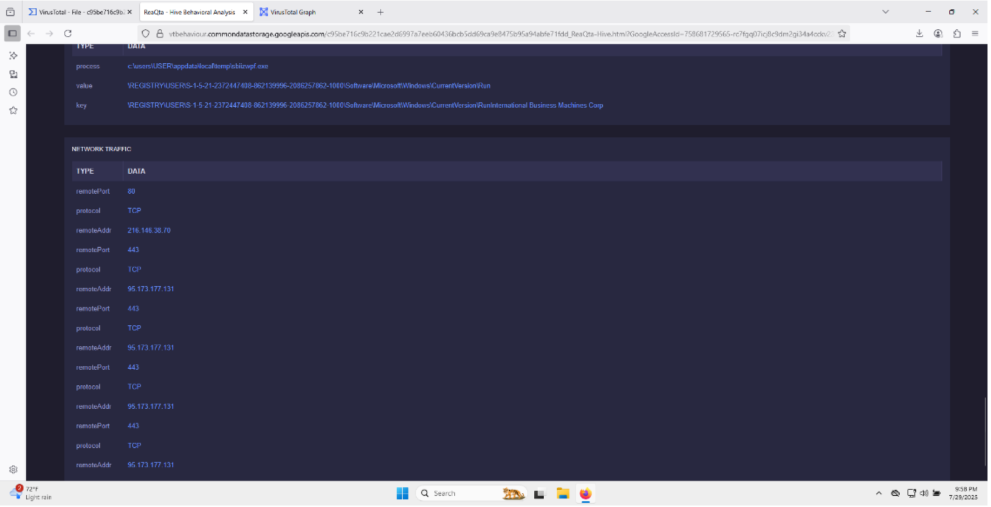
- c:\windows\system32\cmd.exe
- c:\users\USER\appdata\local\temp\sbiizwpf.exe
- c:\users\USER\appdata\local\temp\sbiizwpf.exe

TERMINATED PROCESSES

- c:\users\USER\appdata\local\temp\sbiizwpf.exe

COMMAND LINES

- C:\Windows\system32\cmd.exe /c "C:\Users\USER\AppData\Local\Temp\sbiizwpf.exe"



VirusTotal - File - c95be716c9b
ReaQta - Hive Behavioral Analysis
VirusTotal Graph
72°F
Light rain
Search

TYPE	DATA
process	c:\users\USER\appdata\local\temp\sbiizwpf.exe
value	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\Run
key	\REGISTRY\USER\S-1-5-21-2372447408-862139996-2086257862-1000\Software\Microsoft\Windows\CurrentVersion\RunInternational Business Machines Corp

NETWORK TRAFFIC

TYPE	DATA
remotePort	80
protocol	TCP
remoteAddr	216.146.38.70
remotePort	443
protocol	TCP
remoteAddr	95.173.177.131
remotePort	443
protocol	TCP
remoteAddr	95.173.177.131
remotePort	443
protocol	TCP
remoteAddr	95.173.177.131
remotePort	443
protocol	TCP
remoteAddr	95.173.177.131

ReaQta Analysis Report

- Tags: Info-stealer, persistence, anti-analysis.
- Performs system/network enumeration, privilege escalation, and code injection.
- Communicates with C2 servers over HTTP/HTTPS and disables tracing/debugging mechanisms.

📌 Risk & Impact

- Primary Impact:
  - Credential theft (browsers, FTP, mail, SSH tools)
  - System compromise with persistent backdoor access
- Secondary Impact:
  - Removal of certificates may break security infrastructure

    - Potential for lateral movement with stolen credentials
- Risk Level: 🔴 High

✅ Recommendations

- Immediate:
    - Disconnect infected machines from the network
    - Terminate jaga.exe and all associated processes
    - Block domains hailmofset.com.tr and checkip.dyndns.org and IPs 185.150.128.28 / 216.146.38.70
    - Reset all user and administrative credentials
- Forensic Actions:
    - Review registry for persistence keys
    - Restore deleted certificates and tracing keys if possible
    - Check for mutexes to confirm infection
- Long-term:
    - Deploy endpoint detection (EDR) capable of catching packed .NET binaries
    - Monitor outbound HTTPS traffic anomalies
    - Train users against malicious attachments and links

📚 Conclusion

Gen:Variant.MSIL.Packy.1 is a sophisticated, packed .NET trojan with proven capabilities for credential theft, persistence, registry manipulation, and advanced evasion techniques. It communicates with remote command-and-control servers, exfiltrates sensitive data, and disables system monitoring mechanisms, making detection and removal challenging.

Risk Level: High – capable of full system compromise and widespread credential theft.

Given its ability to compromise user credentials and maintain long-term access, this malware poses a severe threat to enterprise and personal systems. Immediate containment, thorough eradication, and comprehensive network-wide threat hunting are strongly recommended to prevent further compromise or data loss.
