ID: 1670143
Sample Name: PO 407.exe
Cookbook: default.jbs
Time: 07:46:13
Date: 21/04/2025
Version: 42.0.0 Malachite

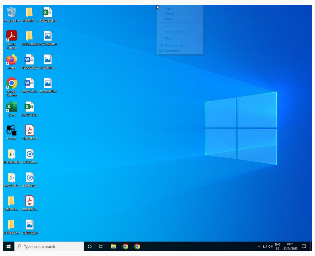
Table of Contents

Windows Analysis Report

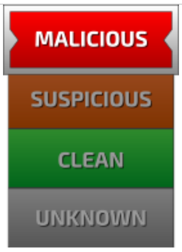
PO 407.exe

Overview

General Information

Sample name:	PO 407.exe
Analysis ID:	1670143
MD5:	fc64631b5ce7f…
SHA1:	0fc75e05d363c..
SHA256:	4f8641371c70d..
Tags:	exe Formbook user-threatcat_ch
Infos:	YARA
	

Detection



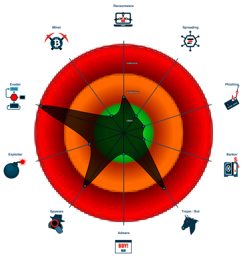
FormBook

Score:	100
Range:	0 - 100
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia…
- Found direct / indirect Syscall (likely…
- Injects a PE file into a foreign proce…
- Joe Sandbox ML detected suspiciou…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w10x64**
- PO 407.exe (PID: 6308 cmdline: "C:\Users\user\Desktop\PO 407.exe" MD5: FC64631B5CE7F552F93D752C53B8ED93)
  - PO 407.exe (PID: 2692 cmdline: "C:\Users\user\Desktop\PO 407.exe" MD5: FC64631B5CE7F552F93D752C53B8ED93)
    - EWLj7U1v.exe (PID: 3004 cmdline: "C:\Program Files (x86)\GAJDnjEsaNAhWTWIZUYGKSOsbceUADSEnVhAweMOpxtoqtnfuoIjJnpOaLlxfD\GDmwDTEh5Oezc.exe" MD5: 9C98D1A23EFAF1B156A130CEA7D2EE3A)
      - Utilman.exe (PID: 7496 cmdline: "C:\Windows\SysWOW64\Utilman.exe" MD5: 4F59EE095E37A83CDCB74091C807AFA9)
        - EWLj7U1v.exe (PID: 3112 cmdline: "C:\Program Files (x86)\GAJDnjEsaNAhWTWIZUYGKSOsbceUADSEnVhAweMOpxtoqtnfuoIjJnpOaLlxfD\BxcWjTIQKgU.exe" MD5: 9C98D1A23EFAF1B156A130CEA7D2EE3A)
        - firefox.exe (PID: 7628 cmdline: "C:\Program Files\Mozilla Firefox\Firefox.exe" MD5: C86B1BE9ED6496FE0E0CBE73F81D8045)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://0xmrmagnezi.github.io/malware%20analysis/FormBook/https://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

⊘ **No configs have been found**

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.1413842825.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0000000B.00000002.3606158959.0000000003350000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000001.00000002.1414413612.0000000001220000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0000000C.00000002.3607956719.0000000005120000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0000000B.00000002.3604567886.0000000002D50000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PO 407.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
1.2.PO 407.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	

Sigma Signatures

⊘ **No Sigma rule has matched**

Suricata Signatures

⊘ **No Suricata rule has matched**

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Joe Sandbox ML detected suspicious sample

Networking

- Performs DNS queries to domains with low reputation

E-Banking Fraud

Yara detected FormBook

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

Switches to a custom stack to bypass stack traces

HIPS / PFW / Operating System Protection Evasion

Found direct / indirect Syscall (likely to bypass EDR)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file / registry access)

Remote Access Functionality

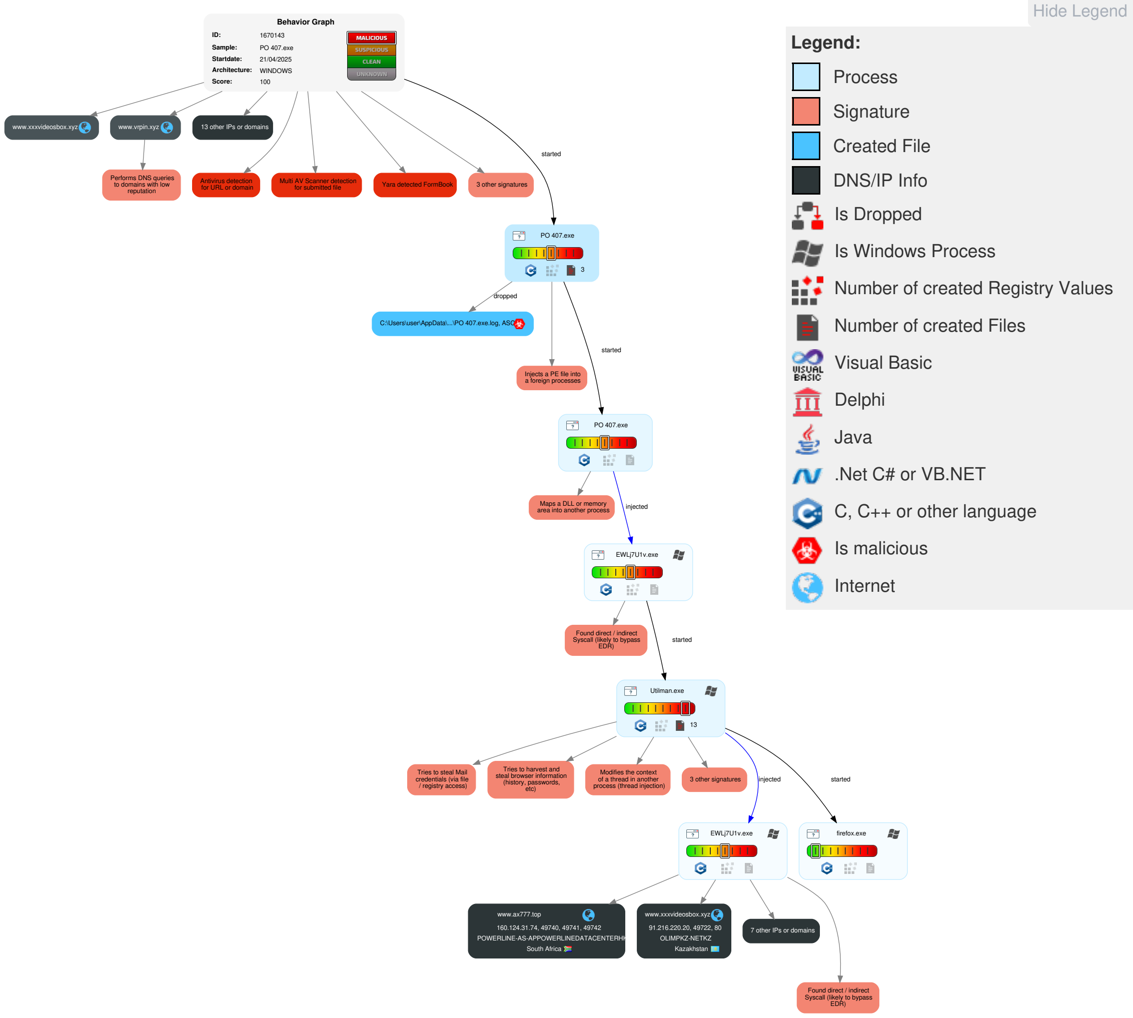
Yara detected FormBook

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	2 Command and Scripting Interpreter	1 DLL Side-Loading	4 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Abuse Elevation Control Mechanism	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	3 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 DLL Side-Loading	4 1 Virtualization/Sandbox Evasion	Security Account Manager	4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	4 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	4 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Abuse Elevation Control Mechanism	Cached Domain Credentials	1 1 3 System Information Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	4 Obfuscated Files or Information	DCSync	Remote System Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 2 Software Packing	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 DLL Side-Loading	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

Behavior Graph


Hide Legend
Behavior Graph
ID: 1670143
Sample: PO 407.exe
Startdate: 21/04/2025
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
www.xxxvideosbox.xyz
www.vrpin.xyz
13 other IPs or domains
Performs DNS queries to domains with low reputation
Antivirus detection for URL or domain
Multi AV Scanner detection for submitted file
Yara detected FormBook
3 other signatures
started
PO 407.exe
3
dropped
C:\Users\user\AppData\...\PO 407.exe.log, ASC
Injects a PE file into a foreign processes
started
PO 407.exe
Maps a DLL or memory area into another process
injected
EWLj7U1v.exe
Found direct / indirect Syscall (likely to bypass EDR)
started
Utilman.exe
13
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)
Modifies the context of a thread in another process (thread injection)
3 other signatures
injected
started
EWLj7U1v.exe
firefox.exe
www.ax777.top
160.124.31.74, 49740, 49741, 49742
POWERLINE-AS-APPOWERLINEDATACENTERHK
South Africa
www.xxxvideosbox.xyz
91.216.220.20, 49722, 80
OLIMPKZ-NETKZ
Kazakhstan
7 other IPs or domains
Found direct / indirect Syscall (likely to bypass EDR)

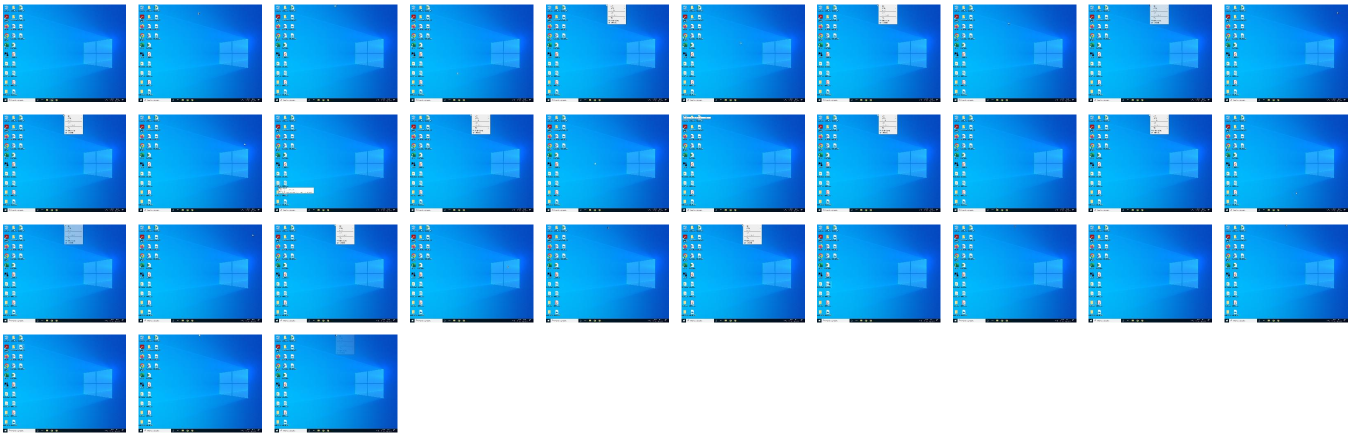
Legend:

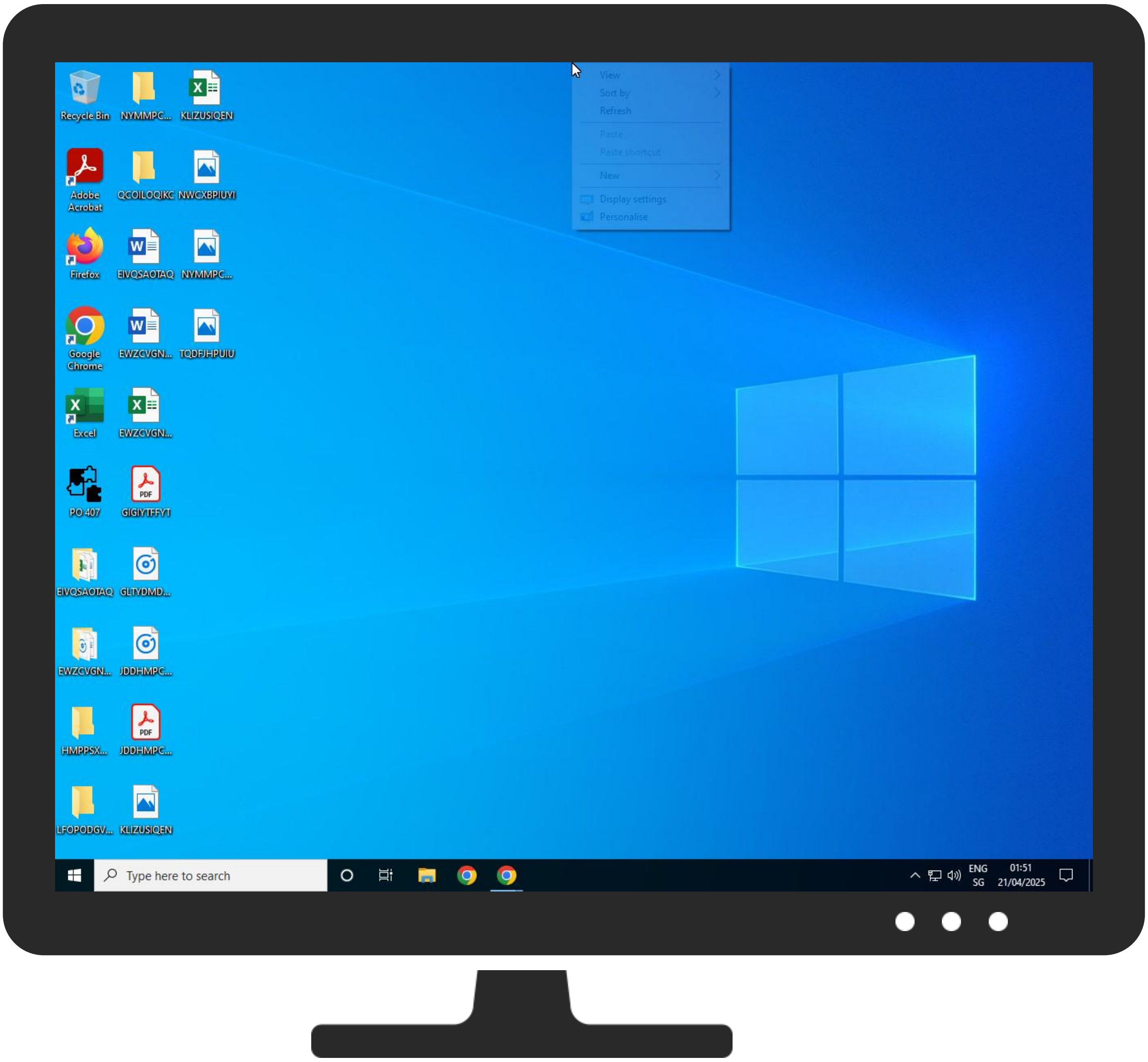
▢	Process
🟥	Signature
🟦	Created File
■	DNS/IP Info
	Is Dropped
	Is Windows Process
	Number of created Registry Values
	Number of created Files
	Visual Basic
	Delphi
	Java
	.Net C# or VB.NET
	C, C++ or other language
	Is malicious
	Internet

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO 407.exe	36%	ReversingLabs	Win32.Trojan.Generic	
PO 407.exe	31%	Virustotal		Browse
SAMPLE	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.bjogo.xyz/lbak/?LJ=RiladI41rhE6y2eLHZ8PC8MX2Ywduh9KijWZkCuW0O23919AnrZ1a/kf6h3+yuZgiwfSvtsq848N9KQYabsmuw/VXs8lZBaVTXW2buIYIuciUsIy4zE0yo8=&nfQ=62VLitKX3ZQtD8P0	0%	Avira URL Cloud	safe	
http://www.031234912.xyz/rxqp/?nfQ=62VLitKX3ZQtD8P0&LJ=yNPDi0FdWVqm/NJHoQwWe9CJio47JBRaDAkSlWMNRo5hReSnGh8CdZXLFNAJOOuO+XCRLDSE17WkbvE519aJbIDpc4Zt02V4dKj2L1UwfjXgdG6iB2so0mQ=	100%	Avira URL Cloud	malware	
http://https://login.live.co	0%	Avira URL Cloud	safe	
http://https://www.werdienmachine.net/68yf/?nfQ=62VLitKX3ZQtD8P0&LJ=3FdVNtuqhX/OwQ0CsUdSe	0%	Avira URL Cloud	safe	
http://www.mslgdkor.xyz/9y3c/?LJ=Uxo1tjvQSOjHJBx/WL1Z4aTyqnUIfCKEew3PLayvGrhDG1kktUG/q5smNt5QZYm19xNTf7YleFFlbZBl4hDMzxotodt35qa9wClulzv4bs3vcfzQM082dco=&nfQ=62VLitKX3ZQtD8P0	100%	Avira URL Cloud	malware	
http://www.xxxvideosbox.xyz/r1zl/?nfQ=62VLitKX3ZQtD8P0&LJ=RMtocHhLv4PviDOIzD6yKdwQdedkbqGuCdUbVP3porp0rsRMSXBGxxdZR279wH8k7MV0UwICfeYC4O3VpK1XVPrPjdWbkMsoQcQuvLibN/AidLM/+9JUY2Q=	0%	Avira URL Cloud	safe	
http://www.werdienmachine.net/68yf/?nfQ=62VLitKX3ZQtD8P0&LJ=3FdVNtuqhX/OwQ0CsUdSe+pIVTMT8TbyudsUPAIxvbc74rs8+oKFjm0JHDHCybUUYrL0pYrXwy0Xcu3Z7znVP5o4vtGhf9ErW+kRSUddUWDZ7eS70buf048=	0%	Avira URL Cloud	safe	
http://www.kpa-aution.online/128e/?nfQ=62VLitKX3ZQtD8P0&LJ=s9McBJLMjVEkDg5ofsJgzIncb0tOp4vhhsS0K++y3mc9Clik8aHmC8Xx5lnrAKhG2I2Dce0nREOtuOgdst9KiVaHtpD64erfg0NqQC2fyE+aJ4gWzuFGQt4=	0%	Avira URL Cloud	safe	
http://www.vrpin.xyz/cifg/?LJ=qm8XEd3ZjOm+BH2sAmNcXkAKLFxe70eGrXFy4Pa4QdhoscEF9kSXvMz8sD/pAOaMKWrVSNXRHDa31zUiavOGkZAK7pMpc4Er4zEZ9zAxY/s27eN7YaeqOlE=&nfQ=62VLitKX3ZQtD8P0	0%	Avira URL Cloud	safe	
http://www.ax777.top/aob6/?LJ=XhIC4rw+QypbzuMVivQNGvvbt21XFOITR846vIosIB7Puaxny8N7Vqc5r96i8ZZbKK7HlnBg0X//wL8UJwmx2iB5WpadJZJ+12OlBS2kZX/LxwBlaoZ7JKo=&nfQ=62VLitKX3ZQtD8P0	0%	Avira URL Cloud	safe	
http://www.teksto.xyz	0%	Avira URL Cloud	safe	
http://www.reampul.live/fr2z/?LJ=b7jrB6wL5i9ET2tr+2VKnIGpMifPfxMKpM6EaP6DOHoTXwTSM6BKj7xdLyCXdIl9KJV+S8D0nqYPi4NNKef3/3JhOeOx26kNnwzkHFmue+Y+emVHJmiFyjk=&nfQ=62VLitKX3ZQtD8P0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bjogo.xyz	172.67.183.195	true	false		high
www.teksto.xyz	13.248.169.48	true	false		high
www.mslgdkor.xyz	104.21.22.160	true	false		high
www.ax777.top	160.124.31.74	true	false		high
www.vrpin.xyz	13.248.169.48	true	false		high
www.reampul.live	159.198.64.72	true	false		high
www.xxxvideosbox.xyz	91.216.220.20	true	false		high
031234912.xyz	144.76.229.203	true	false		high
www.werdienmachine.net.cdn.hstgr.net	84.32.84.126	true	false		high
www.kpa-aution.online	67.205.3.239	true	false		high
www.globedesign.xyz	13.248.169.48	true	false		high
www.031234912.xyz	unknown	unknown	false		high
www.funnyjunk.pics	unknown	unknown	false		high
www.werdienmachine.net	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mrguider.pics	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.031234912.xyz/rxqp/?nfQ=62VLitKX3ZQtD8P0&LJ=yNPDi0FdWVqm/NJHoQwWe9CJio47JBRaDAkSlWMNRo5hReSnGh8CdZXLFNAJOOuO+XCRLDSE17WkbvE519aJbIDpc4Zt02V4dKj2L1UwfjXgdG6iB2so0mQ=	false	- Avira URL Cloud: malware	unknown
http://www.vrpin.xyz/cifg/	false		high
http://www.bjogo.xyz/lbak/?LJ=RiladI41rhE6y2eLHZ8PC8MX2Ywduh9KijWZkCuW0O23919AnrZ1a/kf6h3+yuZgiwfSvtsq848N9KQYabsmuw/VXs8lZBaVTXW2buIYluciUsIy4zE0yo8=&nfQ=62VLitKX3ZQtD8P0	false	- Avira URL Cloud: safe	unknown
http://www.kpa-aution.online/128e/?nfQ=62VLitKX3ZQtD8P0&LJ=s9McBJLMjVEkDg5ofsJgzIncb0tOp4vhhsS0K++y3mc9Clik8aHmC8Xx5lnrAKhG2I2Dce0nREOtuOgdst9KiVaHtpD64erfg0NqQC2fyE+aJ4gWzuFGQt4=	false	- Avira URL Cloud: safe	unknown
http://www.ax777.top/aob6/	false		high
http://www.reampul.live/fr2z/	false		high
http://www.xxxvideosbox.xyz/r1zl/?nfQ=62VLitKX3ZQtD8P0&LJ=RMtocHhLv4PviDOIzD6yKdwQdedkbqGuCdUbVP3porp0rsRMSXBGxxdZR279wH8k7MV0UwICfeYC4O3VpK1XVPrPjdWbkMsoQcQuvLibN/AidLM/+9JUY2Q=	false	- Avira URL Cloud: safe	unknown
http://www.mslgdkor.xyz/9y3c/?LJ=Uxo1tjvQSOjHJBx/WL1Z4aTyqnUIfCKEew3PLayvGrhDG1kktUG/q5smNt5QZYm19xNTf7YleFFlbZBl4hDMzxotodt35qa9wClulzv4bs3vcfzQM082dco=&nfQ=62VLitKX3ZQtD8P0	false	- Avira URL Cloud: malware	unknown
http://www.werdienmachine.net/68yf/?nfQ=62VLitKX3ZQtD8P0&LJ=3FdVNtuqhX/OwQ0CsUdSe+pIVTMT8TbyudsUPAIxvbc74rs8+oKFjm0JHDHCybUUYrL0pYrXwy0Xcu3Z7znVP5o4vtGhf9ErW+kRSUddUWDZ7eS70buf048=	false	- Avira URL Cloud: safe	unknown
http://www.kpa-aution.online/128e/	false		high
http://www.031234912.xyz/rxqp/	false		high
http://www.mslgdkor.xyz/9y3c/	false		high
http://www.vrpin.xyz/cifg/?LJ=qm8XEd3ZjOm+BH2sAmNcXkAKLFxe70eGrXFy4Pa4QdhoscEF9kSXvMz8sD/pAOaMKWrVSNXRHDa31zUiavOGkZAK7pMpc4Er4zEZ9zAxY/s27eN7YaeqOlE=&nfQ=62VLitKX3ZQtD8P0	false	- Avira URL Cloud: safe	unknown
http://www.ax777.top/aob6/?LJ=XhIC4rw+QypbzuMVivQNGvvbt21XFOITR846vIosIB7Puaxny8N7Vqc5r96i8ZZbKK7HlnBg0X//wL8UJwmx2iB5WpadJZJ+12OlBS2kZX/LxwBlaoZ7JKo=&nfQ=62VLitKX3ZQtD8P0	false	- Avira URL Cloud: safe	unknown
http://www.globedesign.xyz/l81p/	false		high
http://www.teksto.xyz/h2jy/	false		high
http://www.werdienmachine.net/68yf/	false		high
http://www.reampul.live/fr2z/?LJ=b7jrB6wL5i9ET2tr+2VKnIGpMifPfxMKpM6EaP6DOHoTXwTSM6BKj7xdLyCXdIl9KJV+S8D0nqYPi4NNKef3/3JhOeOx26kNnwzkHFmue+Y+emVHJmiFyjk=&nfQ=62VLitKX3ZQtD8P0	false	- Avira URL Cloud: safe	unknown
http://www.bjogo.xyz/lbak/	false		high

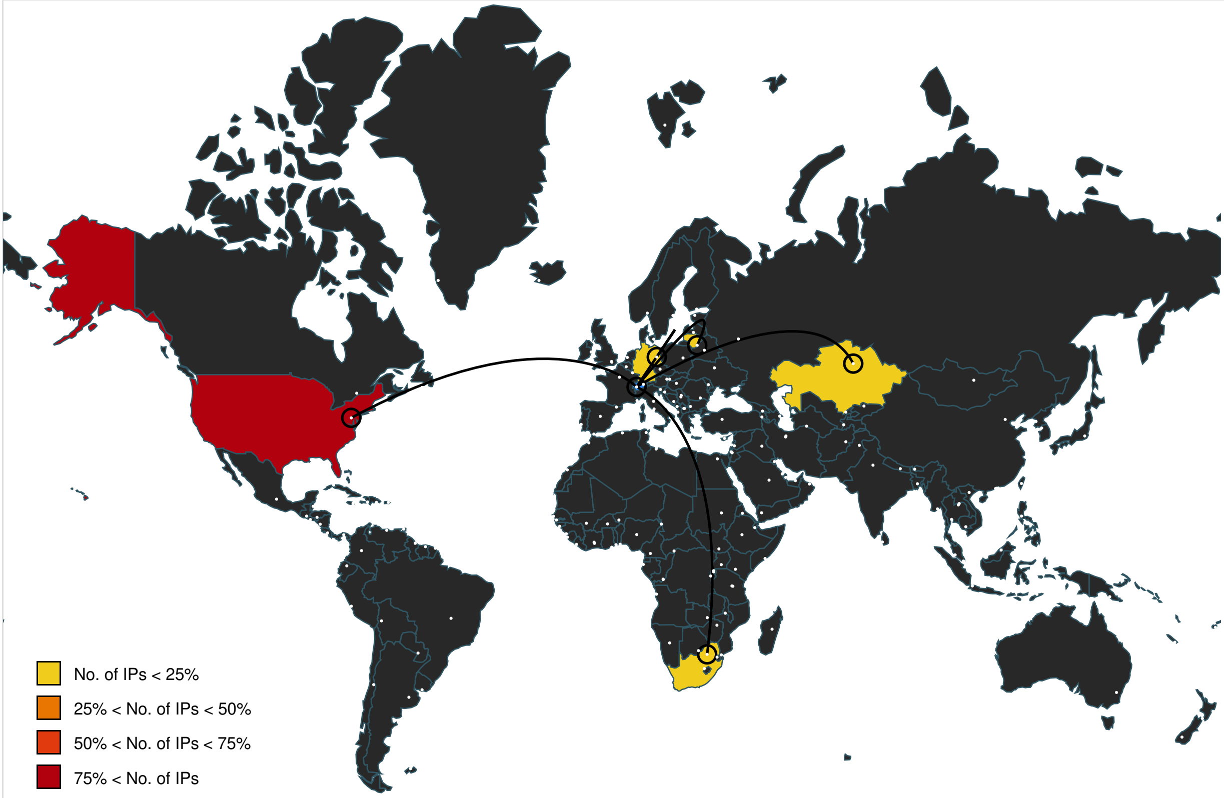
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://login.live.co	Utilman.exe, 0000000B.00000002.3604921036.0000000003252000.00000004.00000020.00020000.00000000.sdmp	false	- Avira URL Cloud: safe	unknown
http://www.typography.netD	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_alldp.ico	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.werdienmachine.net/68yf/?nfQ=62VLitKX3ZQtD8P0&LJ=3FdVNtuqhX/OwQ0CsUdSe	Utilman.exe, 0000000B.00000002.3606968277.0000000006594000.00000004.10000000.00040000.00000000.sdmp, EWLj7U1v.exe, 0000000C.00000002.3606511387.0000000003D64000.00000004.00000001.00040000.00000000.sdmp	false	- Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org?q=	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.ecosia.org/newtab/v20	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-user.html	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.teksto.xyz	EWLj7U1v.exe, 0000000C.00000002.3607956719.00000000051A5000.00000040.80000000.00040000.00000000.sdmp	false	- Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtabv20	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers8	PO 407.exe, 00000000.00000002.1177179153.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gemini.google.com/app?q=	Utilman.exe, 0000000B.00000003.1599102433.000000000804E000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.229.203	031234912.xyz	Germany	🇩🇪	24940	HETZNER-ASDE	false
84.32.84.126	www.werdienmachine.net. cdn.hstgr.net	Lithuania	🇱🇹	33922	NTT-LT-ASLT	false
172.67.183.195	www.bjogo.xyz	United States	🇺🇸	13335	CLOUDFLARENETUS	false
13.248.169.48	www.teksto.xyz	United States	🇺🇸	16509	AMAZON-02US	false
160.124.31.74	www.ax777.top	South Africa	🇿🇦	132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
91.216.220.20	www.xxxvideosbox.xyz	Kazakhstan	🇰🇿	51236	OLIMPKZ-NETKZ	false
159.198.64.72	www.reampul.live	United States	🇺🇸	131090	CAT-IDC-4BYTENET-AS-APCATTELECOMPublicCompanyLtdCATT	false
67.205.3.239	www.kpa-aution.online	United States	🇺🇸	26347	DREAMHOST-ASUS	false
104.21.22.160	www.mslgdkor.xyz	United States	🇺🇸	13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox version:	42.0.0 Malachite
Analysis ID:	1670143
Start date and time:	2025-04-21 07:46:13 +02:00

Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 134, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	PO 407.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/2@13/9
EGA Information:	• Successful, ratio: 75%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240000 for current running targets taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sppsvc.exe, WMIADAP.exe, SIHClient.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 184.29.183.29, 4.175.87.197
- Excluded domains from analysis (whitelisted): a-ring-fallback.msedge.net, fs.microsoft.com, ocsp.digicert.com, slscr.update.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target EWLj7U1v.exe, PID 3004 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.

Simulations

Behavior and APIs

Time	Type	Description
01:47:10	API Interceptor	1x Sleep call for process: PO 407.exe modified
01:48:11	API Interceptor	11938459x Sleep call for process: Utilman.exe modified

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO 407.exe.log

Process:	C:\Users\user\Desktop\PO 407.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.34331486778365
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KH1qE4qXKDE4KhKiKhPKIE4oKNzKoZAE4Kze0E4x84j:MIHK5HKH1qHiYHKh3oPtHo6hAHKze0HJ
MD5:	1330C80CAAC9A0FB172F202485E9B1E8
SHA1:	86BAFDA4E4AE68C7C3012714A33D85D2B6E1A492
SHA-256:	B6C63ECE799A8F7E497C2A158B1FFC2F5CB4F745A2F8E585F794572B7CF03560
SHA-512:	75A17AB129FE97BBAB36AA2BD66D59F41DB5AFF44A705EF3E4D094EC5FCD056A3ED59992A0AC96C9D0D40E490F8596B07DCA9B60E606B67223867B061D9D0 B2
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02

C:\Users\user\AppData\Local\Temp\1b71Jp

Process:	C:\Windows\SysWOW64\Utilman.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	139264
Entropy (8bit):	0.951889861146889
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaWtPqfPk:CfJ6a9xpnQLqtzKWJntPqfM
MD5:	2791D27717CAB5981A0EA5AD07EE6B64
SHA1:	1ACFA3E6B2D3A682CA918D6C1AA4AEBFBA2D9B75
SHA-256:	A2D12FE1A445318E2A559FA65998843F50469BEDB41B0F8EBEF008DB6EEE1A7F
SHA-512:	74FE33DD01CD441635EA88876E743B755C1092EAE29C8CA71E108995550C7994B1911295FC68F8B6688F0AC1CDB9313FC9A6714FB65BEA3F4956865978006E6F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3......@ ....8...........$..O}...........4..

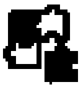
Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.77770120226535

TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01%
File name:	PO 407.exe
File size:	771'072 bytes
MD5:	fc64631b5ce7f552f93d752c53b8ed93
SHA1:	0fc75e05d363c7211e87eecbf9af1316e1c060d7
SHA256:	4f8641371c70db217c573c922367c68f799e0e31a62e99404a59015b47baa67a
SHA512:	8cf932365cf30dc68721fd86f63a6cc297a206dda4f180c4705de30dba0d7dd546618bae44489257cc194a22394494fe87a41a336cf9fbaf3407fbc0e7fce5df
SSDEEP:	12288:2kxCWp2SDhYK39sg1cqffR9bm36IQ69SmFWDjGcXCZe9IsY4ill8xUViA//swRU:/YWpNh9snqHRtw6IuDS4ql8xUVFUw
TLSH:	6FF4CFE03F36731ADEB55A719669DEB586F219787014BAE658CC379B31CC210AE0CF12
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......h..............0.................. ....@.. ....@...............................

File Icon

	
Icon Hash:	1d6155232c5c1998

Static PE Info

General

Entrypoint:	0x4bc486
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x68059DC2 [Mon Apr 21 01:22:10 2025 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc434	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x19c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xba48c	0xba600	5c4ee0d9fa2ba6afce35d671f8fd2529	False	0.8935723717303823	data	7.78318958850524	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x19c8	0x1a00	2ccd6c40349a31b7a1558d7cbecbd07d	False	0.8125	data	7.195129687109505	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	d5d4b0e8e2d3a69c8b8617ebcbf7ec28	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0xbe100	0x137c	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.921411387329591

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_GROUP_ICON	0xbf48c	0x14	data			1.05
RT_VERSION	0xbf4b0	0x318	data			0.5214646464646465
RT_MANIFEST	0xbf7d8	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

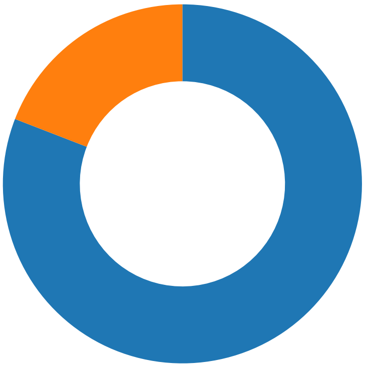
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
Comments	
CompanyName	
FileDescription	
FileVersion	1.4.2
InternalName	vJjH.exe
LegalCopyright	
LegalTrademarks	
OriginalFilename	vJjH.exe
ProductName	
ProductVersion	1.4.2
Assembly Version	1.4.0.0

Network Behavior

Network Port Distribution



Total Packets: 68

- ● 53 (DNS)
- ● 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 21, 2025 07:47:49.829072952 CEST	49722	80	192.168.2.4	91.216.220.20
Apr 21, 2025 07:47:50.097024918 CEST	80	49722	91.216.220.20	192.168.2.4
Apr 21, 2025 07:47:50.097122908 CEST	49722	80	192.168.2.4	91.216.220.20
Apr 21, 2025 07:47:50.112971067 CEST	49722	80	192.168.2.4	91.216.220.20
Apr 21, 2025 07:47:50.380932093 CEST	80	49722	91.216.220.20	192.168.2.4
Apr 21, 2025 07:47:50.424503088 CEST	80	49722	91.216.220.20	192.168.2.4
Apr 21, 2025 07:47:50.424515963 CEST	80	49722	91.216.220.20	192.168.2.4
Apr 21, 2025 07:47:50.424618959 CEST	49722	80	192.168.2.4	91.216.220.20
Apr 21, 2025 07:47:50.439564943 CEST	49722	80	192.168.2.4	91.216.220.20
Apr 21, 2025 07:47:50.707436085 CEST	80	49722	91.216.220.20	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 21, 2025 07:48:05.687134027 CEST	49724	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:05.934096098 CEST	80	49724	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:05.934185028 CEST	49724	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:05.968569040 CEST	49724	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:06.214544058 CEST	80	49724	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:06.214804888 CEST	80	49724	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:06.214868069 CEST	49724	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:07.475316048 CEST	49724	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:08.492902040 CEST	49725	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:08.742969036 CEST	80	49725	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:08.743081093 CEST	49725	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:08.754940987 CEST	49725	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:09.003829002 CEST	80	49725	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:09.003873110 CEST	80	49725	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:09.004035950 CEST	49725	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:10.271871090 CEST	49725	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:11.289534092 CEST	49726	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:11.539997101 CEST	80	49726	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:11.540093899 CEST	49726	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:11.552122116 CEST	49726	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:11.801045895 CEST	80	49726	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:11.801084995 CEST	80	49726	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:11.801095009 CEST	80	49726	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:11.801105022 CEST	80	49726	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:11.801175117 CEST	49726	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:13.068304062 CEST	49726	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:14.086707115 CEST	49727	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:14.334429026 CEST	80	49727	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:14.334522963 CEST	49727	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:14.341876030 CEST	49727	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:14.591203928 CEST	80	49727	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:14.591219902 CEST	80	49727	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:14.591423035 CEST	49727	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:14.593560934 CEST	49727	80	192.168.2.4	13.248.169.48
Apr 21, 2025 07:48:14.839212894 CEST	80	49727	13.248.169.48	192.168.2.4
Apr 21, 2025 07:48:20.285629034 CEST	49728	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:20.566289902 CEST	80	49728	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:20.566469908 CEST	49728	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:20.583334923 CEST	49728	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:20.863981962 CEST	80	49728	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:20.866652012 CEST	80	49728	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:20.866676092 CEST	80	49728	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:20.866727114 CEST	49728	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:22.099656105 CEST	49728	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:23.120079041 CEST	49729	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:23.400551081 CEST	80	49729	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:23.400676012 CEST	49729	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:23.413719893 CEST	49729	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:23.694076061 CEST	80	49729	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:23.696749926 CEST	80	49729	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:23.696883917 CEST	80	49729	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:23.696940899 CEST	49729	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:24.927731037 CEST	49729	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:25.946008921 CEST	49730	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:26.226645947 CEST	80	49730	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:26.226813078 CEST	49730	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:26.240545988 CEST	49730	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:26.521218061 CEST	80	49730	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:26.521240950 CEST	80	49730	144.76.229.203	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 21, 2025 07:48:26.521358013 CEST	80	49730	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:26.523650885 CEST	80	49730	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:26.523988008 CEST	80	49730	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:26.524046898 CEST	49730	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:27.799696922 CEST	49730	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:28.805349112 CEST	49731	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:29.086041927 CEST	80	49731	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:29.086174011 CEST	49731	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:29.094603062 CEST	49731	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:29.375113964 CEST	80	49731	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:29.376620054 CEST	80	49731	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:29.376635075 CEST	80	49731	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:29.376754045 CEST	49731	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:29.379012108 CEST	49731	80	192.168.2.4	144.76.229.203
Apr 21, 2025 07:48:29.659348965 CEST	80	49731	144.76.229.203	192.168.2.4
Apr 21, 2025 07:48:34.561883926 CEST	49732	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:34.701793909 CEST	80	49732	104.21.22.160	192.168.2.4
Apr 21, 2025 07:48:34.701910019 CEST	49732	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:34.714631081 CEST	49732	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:34.854370117 CEST	80	49732	104.21.22.160	192.168.2.4
Apr 21, 2025 07:48:36.224836111 CEST	49732	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:36.365765095 CEST	80	49732	104.21.22.160	192.168.2.4
Apr 21, 2025 07:48:36.365837097 CEST	49732	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:37.242794991 CEST	49733	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:37.382698059 CEST	80	49733	104.21.22.160	192.168.2.4
Apr 21, 2025 07:48:37.382908106 CEST	49733	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:37.394725084 CEST	49733	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:37.534662008 CEST	80	49733	104.21.22.160	192.168.2.4
Apr 21, 2025 07:48:38.896662951 CEST	49733	80	192.168.2.4	104.21.22.160
Apr 21, 2025 07:48:39.038019896 CEST	80	49733	104.21.22.160	192.168.2.4
Apr 21, 2025 07:48:39.038085938 CEST	49733	80	192.168.2.4	104.21.22.160

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 21, 2025 07:47:49.079591990 CEST	58372	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:47:49.822139025 CEST	53	58372	1.1.1.1	192.168.2.4
Apr 21, 2025 07:48:05.477817059 CEST	61519	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:48:05.684808969 CEST	53	61519	1.1.1.1	192.168.2.4
Apr 21, 2025 07:48:19.602725029 CEST	52699	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:48:20.282955885 CEST	53	52699	1.1.1.1	192.168.2.4
Apr 21, 2025 07:48:34.385137081 CEST	53798	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:48:34.555123091 CEST	53	53798	1.1.1.1	192.168.2.4
Apr 21, 2025 07:49:27.197973967 CEST	55539	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:49:27.384085894 CEST	53	55539	1.1.1.1	192.168.2.4
Apr 21, 2025 07:49:41.151436090 CEST	50595	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:49:41.947293043 CEST	53	50595	1.1.1.1	192.168.2.4
Apr 21, 2025 07:49:56.431715965 CEST	53260	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:49:56.594290972 CEST	53	53260	1.1.1.1	192.168.2.4
Apr 21, 2025 07:50:04.682737112 CEST	55894	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:50:04.848421097 CEST	53	55894	1.1.1.1	192.168.2.4
Apr 21, 2025 07:50:12.901885033 CEST	58921	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:50:13.174779892 CEST	53	58921	1.1.1.1	192.168.2.4
Apr 21, 2025 07:50:27.947333097 CEST	65334	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:50:28.149075985 CEST	53	65334	1.1.1.1	192.168.2.4
Apr 21, 2025 07:50:41.572638035 CEST	59838	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:50:41.880563021 CEST	53	59838	1.1.1.1	192.168.2.4
Apr 21, 2025 07:50:55.510360956 CEST	63982	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:50:55.751115084 CEST	53	63982	1.1.1.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 21, 2025 07:51:09.652977943 CEST	56659	53	192.168.2.4	1.1.1.1
Apr 21, 2025 07:51:09.829551935 CEST	53	56659	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Apr 21, 2025 07:47:49.079591990 CEST	192.168.2.4	1.1.1.1	0x9dee	Standard query (0)	www.xxxvideosbox.xyz	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:05.477817059 CEST	192.168.2.4	1.1.1.1	0xa855	Standard query (0)	www.globedesign.xyz	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:19.602725029 CEST	192.168.2.4	1.1.1.1	0x6c40	Standard query (0)	www.031234912.xyz	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:34.385137081 CEST	192.168.2.4	1.1.1.1	0x6203	Standard query (0)	www.mslgdkor.xyz	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:49:27.197973967 CEST	192.168.2.4	1.1.1.1	0xa705	Standard query (0)	www.reampul.live	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:49:41.151436090 CEST	192.168.2.4	1.1.1.1	0xdaf0	Standard query (0)	www.ax777.top	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:49:56.431715965 CEST	192.168.2.4	1.1.1.1	0xc437	Standard query (0)	www.funnyjunk.pics	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:04.682737112 CEST	192.168.2.4	1.1.1.1	0x13ea	Standard query (0)	www.mrguider.pics	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:12.901885033 CEST	192.168.2.4	1.1.1.1	0x80a4	Standard query (0)	www.werdienmachine.net	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:27.947333097 CEST	192.168.2.4	1.1.1.1	0x64a1	Standard query (0)	www.bjogo.xyz	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:41.572638035 CEST	192.168.2.4	1.1.1.1	0x190f	Standard query (0)	www.kpa-aution.online	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:55.510360956 CEST	192.168.2.4	1.1.1.1	0x48a	Standard query (0)	www.vrpin.xyz	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:51:09.652977943 CEST	192.168.2.4	1.1.1.1	0x8171	Standard query (0)	www.teksto.xyz	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Apr 21, 2025 07:47:49.822139025 CEST	1.1.1.1	192.168.2.4	0x9dee	No error (0)	www.xxxvideosbox.xyz		91.216.220.20	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:05.684808969 CEST	1.1.1.1	192.168.2.4	0xa855	No error (0)	www.globedesign.xyz		13.248.169.48	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:05.684808969 CEST	1.1.1.1	192.168.2.4	0xa855	No error (0)	www.globedesign.xyz		76.223.54.146	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:20.282955885 CEST	1.1.1.1	192.168.2.4	0x6c40	No error (0)	www.031234912.xyz	031234912.xyz		CNAME (Canonical name)	IN (0x0001)	false
Apr 21, 2025 07:48:20.282955885 CEST	1.1.1.1	192.168.2.4	0x6c40	No error (0)	031234912.xyz		144.76.229.203	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:34.555123091 CEST	1.1.1.1	192.168.2.4	0x6203	No error (0)	www.mslgdkor.xyz		104.21.22.160	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:48:34.555123091 CEST	1.1.1.1	192.168.2.4	0x6203	No error (0)	www.mslgdkor.xyz		172.67.205.132	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:49:27.384085894 CEST	1.1.1.1	192.168.2.4	0xa705	No error (0)	www.reampul.live		159.198.64.72	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:49:41.947293043 CEST	1.1.1.1	192.168.2.4	0xdaf0	No error (0)	www.ax777.top		160.124.31.74	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:49:56.594290972 CEST	1.1.1.1	192.168.2.4	0xc437	Name error (3)	www.funnyjunk.pics	none	none	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:04.848421097 CEST	1.1.1.1	192.168.2.4	0x13ea	Name error (3)	www.mrguider.pics	none	none	A (IP address)	IN (0x0001)	false

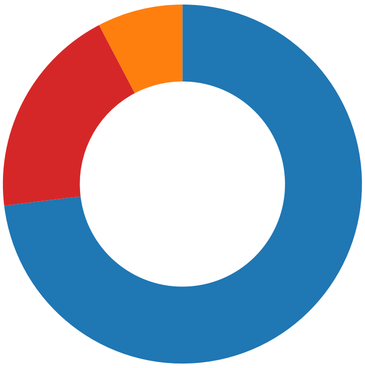
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Apr 21, 2025 07:50:13.174779892 CEST	1.1.1.1	192.168.2.4	0x80a4	No error (0)	www.werdienmachine.net	www.werdienmachine.net.cdn.hstgr.net		CNAME (Canonical name)	IN (0x0001)	false
Apr 21, 2025 07:50:13.174779892 CEST	1.1.1.1	192.168.2.4	0x80a4	No error (0)	www.werdienmachine.net.cdn.hstgr.net		84.32.84.126	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:28.149075985 CEST	1.1.1.1	192.168.2.4	0x64a1	No error (0)	www.bjogo.xyz		172.67.183.195	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:28.149075985 CEST	1.1.1.1	192.168.2.4	0x64a1	No error (0)	www.bjogo.xyz		104.21.56.101	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:41.880563021 CEST	1.1.1.1	192.168.2.4	0x190f	No error (0)	www.kpa-aution.online		67.205.3.239	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:55.751115084 CEST	1.1.1.1	192.168.2.4	0x48a	No error (0)	www.vrpin.xyz		13.248.169.48	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:50:55.751115084 CEST	1.1.1.1	192.168.2.4	0x48a	No error (0)	www.vrpin.xyz		76.223.54.146	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:51:09.829551935 CEST	1.1.1.1	192.168.2.4	0x8171	No error (0)	www.teksto.xyz		13.248.169.48	A (IP address)	IN (0x0001)	false
Apr 21, 2025 07:51:09.829551935 CEST	1.1.1.1	192.168.2.4	0x8171	No error (0)	www.teksto.xyz		76.223.54.146	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.xxxvideosbox.xyz
- www.globedesign.xyz
- www.031234912.xyz
- www.mslgdkor.xyz
- www.reampul.live
- www.ax777.top
- www.werdienmachine.net
- www.bjogo.xyz
- www.kpa-aution.online
- www.vrpin.xyz
- www.teksto.xyz

Statistics

Behavior



- ● PO 407.exe
- ● PO 407.exe
- ● EWLj7U1v.exe
- ● Utilman.exe
- ● EWLj7U1v.exe
- ● firefox.exe

Click to jump to process

System Behavior

Analysis Process: PO 407.exe PID: **6308**, Parent PID: **3964**

General

Target ID:	0
Start time:	01:47:09
Start date:	21/04/2025
Path:	C:\Users\user\Desktop\PO 407.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO 407.exe"
Imagebase:	0xe50000
File size:	771'072 bytes
MD5 hash:	FC64631B5CE7F552F93D752C53B8ED93
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: PO 407.exe PID: **2692**, Parent PID: **6308**

General

Target ID:	1
Start time:	01:47:11
Start date:	21/04/2025
Path:	C:\Users\user\Desktop\PO 407.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO 407.exe"
Imagebase:	0x880000
File size:	771'072 bytes
MD5 hash:	FC64631B5CE7F552F93D752C53B8ED93
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	- Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.1413842825.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.1414413612.0000000001220000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.1415532266.0000000002BA0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1699896	success or wait	1	40AB30	NtReadFile
C:\Windows\SysWOW64\Utilman.exe	0	97280	success or wait	1	40AB30	NtReadFile

Analysis Process: EWLj7U1v.exe PID: **3004**, Parent PID: **2692**

General

Target ID:	10
Start time:	01:47:27
Start date:	21/04/2025
Path:	C:\Program Files (x86)\GAJDnjEsaNAhWTWIZUYGKSOsbceUADSEnVhAweMOpxtoqtnfuoIjJnpOaLlxfD\EWLj7U1v.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\GAJDnjEsaNAhWTWIZUYGKSOsbceUADSEnVhAweMOpxtoqtnfuoIjJnpOaLlxfD\GDmwDTEh5Oezc.exe"
Imagebase:	0xea0000
File size:	143'872 bytes
MD5 hash:	9C98D1A23EFAF1B156A130CEA7D2EE3A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000A.00000002.3606214554.00000000039D0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	false

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Utilman.exe PID: **7496**, Parent PID: **3004**

General

Target ID:	11
Start time:	01:47:29
Start date:	21/04/2025
Path:	C:\Windows\SysWOW64\Utilman.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\Utilman.exe"
Imagebase:	0x970000
File size:	97'280 bytes
MD5 hash:	4F59EE095E37A83CDCB74091C807AFA9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000B.00000002.3606158959.0000000003350000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000B.00000002.3604567886.0000000002D50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000B.00000002.3606439530.0000000004D60000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1b71Jp	object name not found	1	2D79185	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1b71Jp	sharing violation	1	2D79185	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1b71Jp	sharing violation	1	2D79185	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1b71Jp	sharing violation	1	2D79185	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1699896	success or wait	1	2D790E5	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: EWLj7U1v.exe

PID: **3112**, Parent PID: **7496**

General

Target ID:	12
Start time:	01:47:42
Start date:	21/04/2025
Path:	C:\Program Files (x86)\GAJDnjEsaNAhWTWIZUYGKSOsbceUADSEnVhAweMOpxtoqtnfuoIjJnpOaLlxfD\EWLj7U1v.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\GAJDnjEsaNAhWTWIZUYGKSOsbceUADSEnVhAweMOpxtoqtnfuoIjJnpOaLlxfD\BxcWjTIQKgU.exe"
Imagebase:	0xea0000
File size:	143'872 bytes
MD5 hash:	9C98D1A23EFAF1B156A130CEA7D2EE3A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 0000000C.00000002.3607956719.0000000005120000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	false

Analysis Process: firefox.exe

PID: **7628**, Parent PID: **7496**

General

Target ID:	13
Start time:	01:47:54
Start date:	21/04/2025
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Mozilla Firefox\Firefox.exe"

Imagebase:	0x7ff76aab0000
File size:	676'768 bytes
MD5 hash:	C86B1BE9ED6496FE0E0CBE73F81D8045
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

⊘ **No disassembly**