ID: 1435169
Sample Name:
yZcecBUXN7.exe
Cookbook: default.jbs
Time: 08:23:06
Date: 02/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

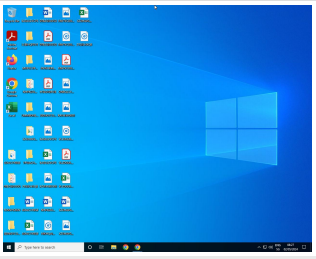
Windows Analysis Report

yZcecBUXN7.exe

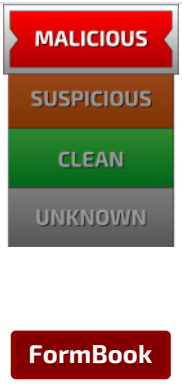
Overview

General Information

Sample name:	yZcecBUXN7.exerenamed because original name is a hash value
Original sample name:	9cd48f0d93c28..
Analysis ID:	1435169
MD5:	9cd48f0d93c28..
SHA1:	a6a625d2dce7…
SHA256:	3ed0095ee2de…
Tags:	32 exe
Infos:	



Detection

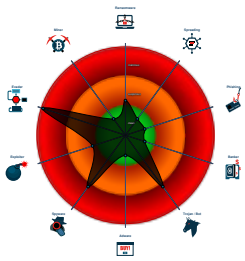


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code references suspic…
- Deletes itself after installation
- Found direct / indirect Syscall (likely…
- Injects a PE file into a foreign proce…
- Machine Learning detection for sam…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- yZcecBUXN7.exe (PID: 6640 cmdline: "C:\Users\user\Desktop\yZcecBUXN7.exe" MD5: 9CD48F0D93C28AE6559409DE23414554)
  - yZcecBUXN7.exe (PID: 6712 cmdline: "C:\Users\user\Desktop\yZcecBUXN7.exe" MD5: 9CD48F0D93C28AE6559409DE23414554)
    - jBaxmaKIzqHZYEOPQcTTJTXx.exe (PID: 3688 cmdline: "C:\Program Files (x86)\DUKoqSpezAPdkEeQLfXbQJktRyLdTGIcgkgDcRWuknrvtOsFOYoJLHQwvsoW\jBaxmaKIzqHZYEOPQcTTJTXx.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
      - netsh.exe (PID: 6760 cmdline: "C:\Windows\SysWOW64\netsh.exe" MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
        - jBaxmaKIzqHZYEOPQcTTJTXx.exe (PID: 916 cmdline: "C:\Program Files (x86)\DUKoqSpezAPdkEeQLfXbQJktRyLdTGIcgkgDcRWuknrvtOsFOYoJLHQwvsoW\jBaxmaKIzqHZYEOPQcTTJTXx.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
        - firefox.exe (PID: 3020 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://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/https://asec.ahnlab.com/en/32149/	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
00000007.00000002.4125352041.00000000055B0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000007.00000002.4125352041.00000000055B0000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x90f43:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x7a482:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01
00000001.00000002.1897755674.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000001.00000002.1897755674.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2da63:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x16fa2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01
00000004.00000002.4122807420.0000000000C00000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.yZcecBUXN7.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
1.2.yZcecBUXN7.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2da63:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x16fa2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01
0.2.yZcecBUXN7.exe.3ae4f90.2.raw.unpack	MALWARE_Win_DLInjector02	Detects downloader injector	ditekSHen	• 0x6be6b:$x1: In$J$ct0r
1.2.yZcecBUXN7.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
1.2.yZcecBUXN7.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x2cc63:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x161a2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01

Click to see the 5 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

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)

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

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)

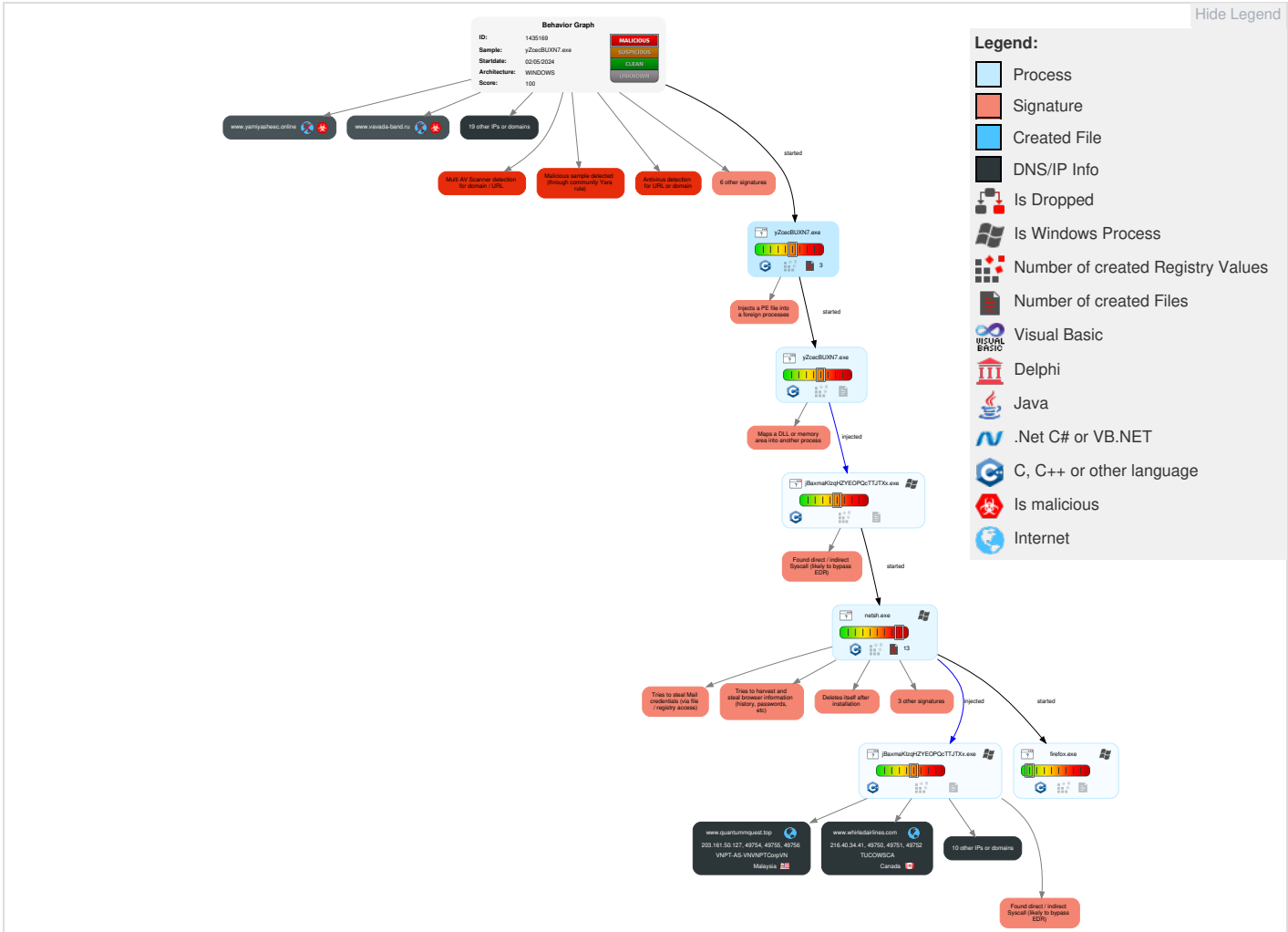
Remote Access Functionality

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	1 Native API	1 DLL Side-Loading	1 Abuse Elevation Control Mechanism	1 1 Disable or Modify Tools	1 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	3 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 3 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	4 1 2 Process Injection	1 Abuse Elevation Control Mechanism	Security Account Manager	2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	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 Obfuscated Files or Information	NTDS	2 Process 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	2 Software Packing	LSA Secrets	5 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Timestomp	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 DLL Side-Loading	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 File Deletion	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 Masquerading	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	5 1 Virtualization/Sandbox Evasion	Network Sniffing	Network Service Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement
Network Security Appliances	Domains	Compromise Software Dependencies and Development Tools	AppleScript	Launchd	Launchd	4 1 2 Process Injection	Input Capture	System Network Connections Discovery	Software Deployment Tools	Remote Data Staging	Mail Protocols	Exfiltration Over Unencrypted Non-C2 Protocol	Firmware Corruption

Behavior Graph



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
yZcecBUXN7.exe	29%	ReversingLabs		
yZcecBUXN7.exe	38%	Virustotal		Browse
yZcecBUXN7.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
vavada-band.ru	4%	Virustotal		Browse
www.dhleba51.ru	2%	Virustotal		Browse
applesolve.com	1%	Virustotal		Browse
www.bettaroom.ru	3%	Virustotal		Browse
dainikmirpur.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.applesolve.com	1%	Virustotal		Browse
www.dainikmirpur.com	0%	Virustotal		Browse
bnbuotqakx.shop	5%	Virustotal		Browse
www.vavada-band.ru	7%	Virustotal		Browse
www.vaesen.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.dhleba51.ru/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=bCD+TBjy8MosL0R8cjbFvxriDyPYhKFZsDVB2lzqkrb80jeseZ1xwY0K4Gv6crRSCTRNIEUsU3Jqelj2oHAe6QPTv8GQpjovQK3uiYXh6MxwvjeFy3ewRNM=	100%	Avira URL Cloud	malware	
http://www.yamiyasheec.online/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=XN/uN6nMvrGkpcBz+Thv1jYaxJtcZ3guzCEwk+wO1lePrLEfQ2dONhxJJ5MfI8SrhyY28ykjUI4nvFFhDsPQuo7fansGo7O9hSpOWy12njMGsYSDFVmwrLg=	0%	Avira URL Cloud	safe	
http://www.whirledairlines.com/0hhg/	0%	Avira URL Cloud	safe	
http://www.applesolve.com/0hhg/	0%	Avira URL Cloud	safe	
http://www.applesolve.com/0hhg/?ABqDW6A8=vkFwZ006WdHbpHCmjjBOYDeoX+Rn6aHsZLnu3NGBe2VBUm0fUZsnu3sABaHfjqCa4r+GKRPsyPs5e5gNT6h7MvS/nYKUeSlb7fRS9PCej43uXu++wSLzang=&nNWXl=ybhXiHipjHJ	0%	Avira URL Cloud	safe	
http://www.whirledairlines.com/0hhg/	0%	Virustotal		Browse
http://www.applesolve.com/0hhg/	2%	Virustotal		Browse
http://www.dk48.lol/0hhg/	0%	Avira URL Cloud	safe	
http://www.dk48.lol/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=Np3vqe/1Cu/OQ51upJR8Qsht1t6ybRV+pU7NEwPzo+CdnJXCrwJJ0q4TeA3yrjOGKQp+qts/DZNdYR5Nz+PtVR15bhmDHV5jmEZsuo4OBXvm+mP+YyhGbOc=	0%	Avira URL Cloud	safe	
http://www.xxaiai.top/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=4PSEdCTPIXdKXl7uh+LsBTwAtAbEEDmKYAJsxyVVq9bdmcYGjB9JHSE/ykX4VkYbcxwnxSFcyayelsVtdhVYibhKvsL7bWoBJw77jiRnpeIfkNF5+PYwYCo=	0%	Avira URL Cloud	safe	
http://www.bnbuotqakx.shop/0hhg/	100%	Avira URL Cloud	malware	
http://www.whirledairlines.com/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=OATZzJPiUUGU3mpjZciWUPZeXbT2MJCMteYhXkaeth47OgAuOtH7Ax1R5cSUzc8K7tJsdCLV7T20xyzuI8wSbYrVofQNfqyssPuErqT1NUPeqaem3KrcSl4=	0%	Avira URL Cloud	safe	
http://applesolve.com/0hhg/?ABqDW6A8=vkFwZ006WdHbpHCmjjBOYDeoX	0%	Avira URL Cloud	safe	
http://https://www.cucuzeus88.store/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=nRUqMZh05AeT5XBXy6tvbUigcs6hc4rC	0%	Avira URL Cloud	safe	
http://www.quantummquest.top/0hhg/	0%	Avira URL Cloud	safe	
http://www.quantummquest.top/0hhg/?ABqDW6A8=nDs+4sFgmC14rZAzdMtU+fOluyCTVoLAn9AW6ezlSd5l//pRDkDNUYKtMPmQp3hOJuHIoac+nQZfVGszaQStOPCeLqTfiXL51+ke6KS/qQDP30/ytVZd2Oc=&nNWXl=ybhXiHipjHJ	0%	Avira URL Cloud	safe	
http://www.dainikmirpur.com/0hhg/	0%	Avira URL Cloud	safe	
http://www.yamiyasheec.online/0hhg/	0%	Avira URL Cloud	safe	
http://www.dhleba51.ru/0hhg/	100%	Avira URL Cloud	malware	
http://www.xxaiai.top/0hhg/	0%	Avira URL Cloud	safe	
http://www.dainikmirpur.com/0hhg/	0%	Virustotal		Browse
http://www.quantummquest.top/0hhg/	1%	Virustotal		Browse
http://www.dainikmirpur.com/0hhg/?ABqDW6A8=3wBFJopWm5CMrZiTyKtS+1p+7hjS88lkxUD6z9EbhjEDI4ONso69BWfj9WDOW8yAnPP5dxxY4Y59DXJqqTyKGc0G8sgHpv85TbqwFJKqhW0zFRgOzII1BwU=&nNWXl=ybhXiHipjHJ	0%	Avira URL Cloud	safe	
http://www.yamiyasheec.online/0hhg/	3%	Virustotal		Browse
http://www.vavada-band.ru/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=ZgUGlv2SFtjYSXZ+sPWjrnmi9x4JTSAxK/4wkC6FqAYJ2g+qpBbYR3pK2HW+0dFnzG0fITqUvE2Gc/Yp1eE4tJw0C8fQ5yYHj2xbYtSMWmtqetVE9PQCl40=	100%	Avira URL Cloud	malware	
http://www.bnbuotqakx.shop	100%	Avira URL Cloud	malware	
http://www.bettaroom.ru/0hhg/	0%	Avira URL Cloud	safe	
http://www.dhleba51.ru/0hhg/	4%	Virustotal		Browse
http://www.cucuzeus88.store/0hhg/	0%	Avira URL Cloud	safe	
http://www.bettaroom.ru/0hhg/	8%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vavada-band.ru	148.251.36.121	true	false	• 4%, Virustotal, Browse	unknown
cucuzeus88.store	153.92.8.41	true	false		unknown
www.quantummquest.top	203.161.50.127	true	false		unknown
www.dhleba51.ru	195.24.68.5	true	false	• 2%, Virustotal, Browse	unknown
applesolve.com	188.116.38.155	true	false	• 1%, Virustotal, Browse	unknown
parkingpage.namecheap.com	91.195.240.19	true	false		high
www.bettaroom.ru	194.58.112.173	true	false	• 3%, Virustotal, Browse	unknown
bnbuotqakx.shop	101.99.93.157	true	false	• 5%, Virustotal, Browse	unknown
www.xxaiai.top	108.186.8.158	true	false		unknown
dainikmirpur.com	192.250.235.36	true	false	• 0%, Virustotal, Browse	unknown
www.whirledairlines.com	216.40.34.41	true	false		unknown
yamiyasheec.online	119.18.54.116	true	false		unknown
www.applesolve.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
www.cucuzeus88.store	unknown	unknown	true		unknown
www.bnbuotqakx.shop	unknown	unknown	true		unknown
www.dainikmirpur.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.dk48.lol	unknown	unknown	true		unknown
www.cluird.cloud	unknown	unknown	true		unknown
www.yamiyasheec.online	unknown	unknown	true		unknown
www.vavada-band.ru	unknown	unknown	true	• 7%, Virustotal, Browse	unknown
www.vaesen.net	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.whirledairlines.com/0hhg/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.yamiyasheec.online/0hhg/?nNWXI=ybhXiHipjHJ&ABqDW6A8=XN/uN6nMvrGkpcBz+Thv1jYaxJtcZ3guzCEwk+wO1IePrLEfQ2dONhxJJ5MfI8SrhyY28ykjUI4nvFFhDsPQuo7fansGo7O9hSpOWy12njMGsYSDFVmwrLg=	false	• Avira URL Cloud: safe	unknown
http://www.dhleba51.ru/0hhg/?nNWXI=ybhXiHipjHJ&ABqDW6A8=bCD+TBjy8MosL0R8cjbFvxriDyPYhKFZsDVB2lzqkrb80jeseZ1xwY0K4Gv6crRSCTRNIEUsU3Jqelj2oHAe6QPTv8GQpjovQK3uiYXh6MxwvjeFy3ewRNM=	false	• Avira URL Cloud: malware	unknown
http://www.applesolve.com/0hhg/?ABqDW6A8=vkFwZ006WdHbpHCmjjBOYDeoX+Rn6aHsZLnu3NGBe2VBUm0fUZsnu3sABaHfjqCa4r+GKRPsyPs5e5gNT6h7MvS/nYKUeSlb7fRS9PCej43uXu++wSLzang=&nNWXI=ybhXiHipjHJ	false	• Avira URL Cloud: safe	unknown
http://www.applesolve.com/0hhg/	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.dk48.lol/0hhg/	false	• Avira URL Cloud: safe	unknown
http://www.dk48.lol/0hhg/?nNWXI=ybhXiHipjHJ&ABqDW6A8=Np3vqe/1Cu/OQ51upJR8Qsht1t6ybRV+pU7NEwPzo+CdnJXCrwJJ0q4TeA3yrjOGKQp+qts/DZNdYR5Nz+PtVR15bhmDHV5jmEZsuo4OBXvm+mP+YyhGbOc=	false	• Avira URL Cloud: safe	unknown
http://www.xxaiai.top/0hhg/?nNWXI=ybhXiHipjHJ&ABqDW6A8=4PSEdCTPIXdKXl7uh+LsBTwAtAbEEDmKYAJsxyVVq9bdmcYGjB9JHSE/ykX4VkYbcxwnxSFcyayelsVtdhVYibhKvsL7bWoBJw77jiRnpeIfkNF5+PYwYCo=	false	• Avira URL Cloud: safe	unknown
http://www.bnbuotqakx.shop/0hhg/	false	• Avira URL Cloud: malware	unknown
http://www.whirledairlines.com/0hhg/?nNWXI=ybhXiHipjHJ&ABqDW6A8=OATZzJPiUUGU3mpjZciWUPZeXbT2MJCMteYhXkaeth47OgAuOtH7Ax1R5cSUzc8K7tJsdCLV7T20xyzul8wSbYrVofQNfqyssPuErqT1NUPeqaem3KrcSI4=	false	• Avira URL Cloud: safe	unknown
http://www.quantummquest.top/0hhg/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.quantummquest.top/0hhg/?ABqDW6A8=nDs+4sFgmC14rZAzdMtU+fOluyCTVoLAn9AW6ezlSd5l//pRDkDNUYKtMPmQp3hOJuHIoac+nQZfVGszaQStOPCeLqTfiXL51+ke6KS/qQDP30/ytVZd2Oc=&nNWXI=ybhXiHipjHJ	false	• Avira URL Cloud: safe	unknown
http://www.dainikmirpur.com/0hhg/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.yamiyasheec.online/0hhg/	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.dhleba51.ru/0hhg/	false	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.xxaiai.top/0hhg/	false	• Avira URL Cloud: safe	unknown
http://www.dainikmirpur.com/0hhg/?ABqDW6A8=3wBFJopWm5CMrZiTyKtS+1p+7hjS88lkxUD6z9EbhjEDI4ONso69BWfj9WDOW8yAnPP5dxxY4Y59DXJqqTyKGc0G8sgHpv85TbqwFJKqhW0zFRgOzII1BwU=&nNWXI=ybhXiHipjHJ	false	• Avira URL Cloud: safe	unknown
http://www.vavada-band.ru/0hhg/?nNWXI=ybhXiHipjHJ&ABqDW6A8=ZgUGIv2SFtjYSXZ+sPWjrnmi9x4JTSAxK/4wkC6FqAYJ2g+qpBbYR3pK2HW+0dFnzG0fITqUvE2Gc/Yp1eE4tJw0C8fQ5yYHj2xbYtSMWmtqetVE9PQCI40=	false	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.bettaroom.ru/0hhg/	false	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.cucuzeus88.store/0hhg/	false	• Avira URL Cloud: safe	unknown

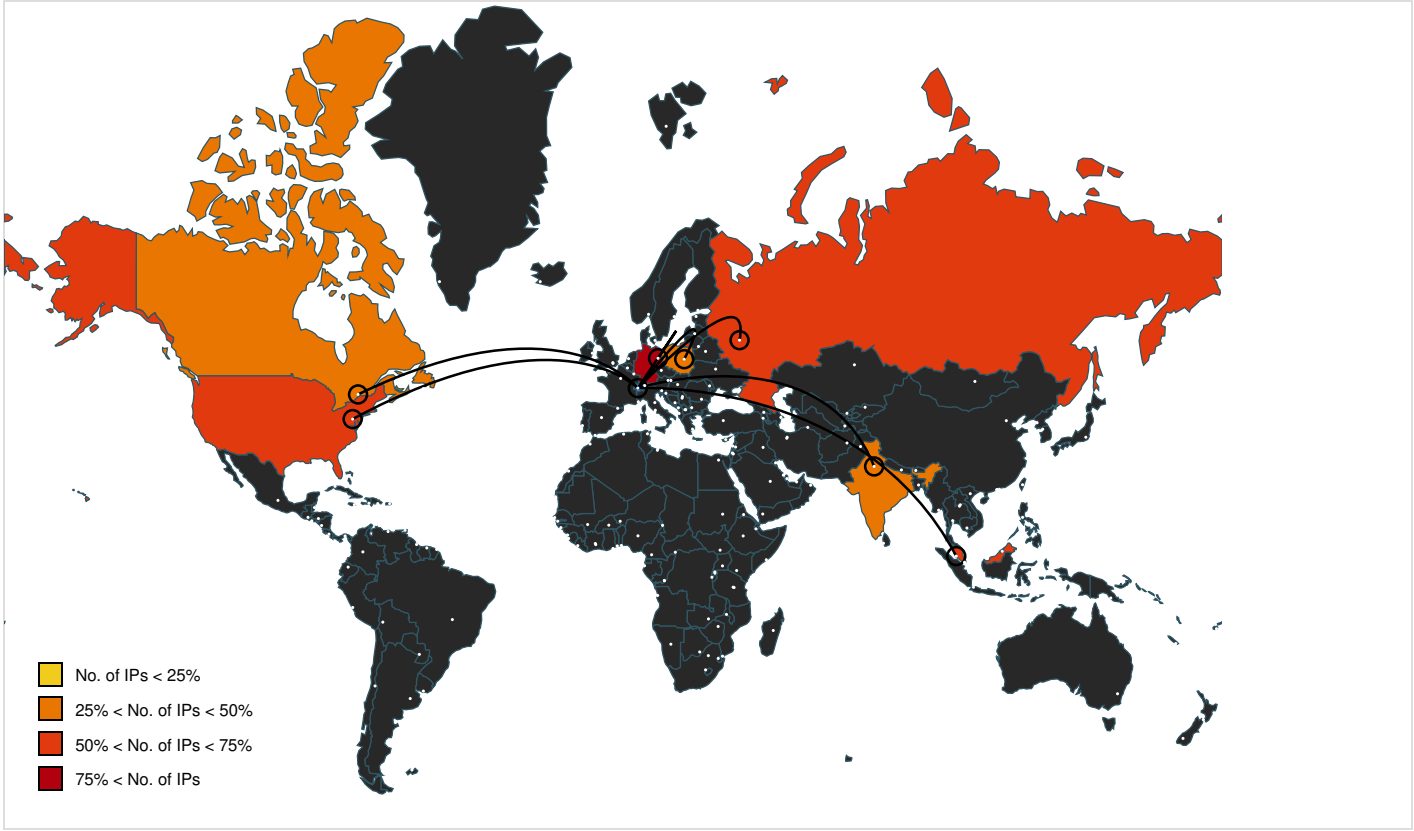
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.instagram.com/hover_domains	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/ssl/	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.nic.ru/	jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://push.zhanzhang.baidu.com/push.js	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.0000000004DE4000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.00000000041F4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/email?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/about?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/domains/	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/help/oshibka-404_8500.html	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/domains/results	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nic.ru/catalog/hosting/shared/	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css	netsh.exe, 00000004.00000002.4124592339.000000000492E000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.00000000003D3E000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/tools?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://help.hover.com/home?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://yastatic.net/pcode/adfox/loader.js	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/domain_pricing?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/privacy?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://twitter.com/hover	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://applesolve.com/0hhg/?ABqDW6A8=vkFwZ006WdHbpHCmjjBOYDeoX	netsh.exe, 00000004.00000002.4124592339.0000000004C52000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000004062000.00000004.00000001.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.hover.com/transfer_in?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/renew?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cucuzeus88.store/0hhg/?nNWXl=ybhXiHipjHJ&ABqDW6A8=nRUqMZh05AeT5XBXy6tvbUigcs6hc4rC	netsh.exe, 00000004.00000002.4124592339.000000000542C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.000000000483C000.00000004.00000001.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://zz.bdstatic.com/linksubmit/push.js	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.0000000004DE4000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.00000000041F4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/hosting/dedicated/	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.00000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.ecosia.org/newtab/	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.nic.ru/catalog/hosting/vds-vps/	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.00000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.hover.com/tos?source=parked	netsh.exe, 00000004.00000002.4126359612.0000000006640000.00000004.00000800.00020000.00000000.sdmp, netsh.exe, 00000004.00000002.4124592339.000000000479C000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high
http://www.bnbuotqakx.shop	jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4125352041.0000000005661000.00000040.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.nic.ru/catalog/hosting/	netsh.exe, 00000004.00000002.4124592339.0000000004478000.00000004.10000000.00040000.00000000.sdmp, jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.00000000003888000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	netsh.exe, 00000004.00000002.4126442386.0000000008078000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hover.com/?source=parked	jBaxmaKIzqHZYEOPQcTTJTXx.exe, 00000007.00000002.4123946344.0000000003BAC000.00000004.00000001.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.161.50.127	www.quantummquest.top	Malaysia		45899	VNPT-AS-VNVNPTCorpVN	false
195.24.68.5	www.dhleba51.ru	Russian Federation		48287	RU-CENTERRU	false
153.92.8.41	cucuzeus88.store	Germany		47583	AS-HOSTINGERLT	false
101.99.93.157	bnbuotqakx.shop	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false
188.116.38.155	applesolve.com	Poland		43333	NEPHAX-ASPL	false
148.251.36.121	vavada-band.ru	Germany		24940	HETZNER-ASDE	false
119.18.54.116	yamiyasheec.online	India		394695	PUBLIC-DOMAIN-REGISTRYUS	false
108.186.8.158	www.xxaiai.top	United States		54600	PEGTECHINCUS	false
192.250.235.36	dainikmirpur.com	United States		36454	CNSV-LLCUS	false
91.195.240.19	parkingpage.namecheap.com	Germany		47846	SEDO-ASDE	false
194.58.112.173	www.bettaroom.ru	Russian Federation		197695	AS-REGRU	false
216.40.34.41	www.whirledairlines.com	Canada		15348	TUCOWSCA	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1435169
Start date and time:	2024-05-02 08:23:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 11m 8s
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 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	8
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:	yZcecBUXN7.exerenamed because original name is a hash value
Original Sample Name:	9cd48f0d93c28ae6559409de23414554.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/2@14/12
EGA Information:	• Successful, ratio: 75%
HCA Information:	• Successful, ratio: 85% • 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, WMIADAP.exe, SIHClient.exe, conhost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- 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
08:25:02	API Interceptor	6957285x Sleep call for process: netsh.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\yZcecBUXN7.exe.log	
Process:	C:\Users\user\Desktop\yZcecBUXN7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.349842958726647
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPTAq1KDLI4M9XKbbDLI4MWuPJKAVKhat92n4M6:MLUE4K5E4KH1qE4qXKDE4KhKiKhg84j
MD5:	9BA266AD16952A9A57C3693E0BCFED48
SHA1:	5DB70A3A7F1DB4E3879265AB336B2FA1AFBCECD5
SHA-256:	A6DFD14E82D7D47195A1EC7F31E64C2820AB8721EF4B5825E21E742093B55C0E
SHA-512:	678E1F639379FC24919B7CF562FA19CE53363CBD4B0EAB66486F6F8D5DD5958DE3AAE8D7842EE868EFCC39D907FDC1A3ACF464E29D37B0DAEE9874C39730F 8E
Malicious:	false
Reputation:	moderate, 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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df07665 68\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..2 ,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\1-00F23L	
Process:	C:\Windows\SysWOW64\netsh.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):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Reputation:	high, 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):	7.622095379937431
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	yZcecBUXN7.exe
File size:	631'808 bytes
MD5:	9cd48f0d93c28ae6559409de23414554
SHA1:	a6a625d2dce72bf9f7deee747c95ed7f7cf36cd0
SHA256:	3ed0095ee2de05e81ac2c954eb0df312d6b919d871b60ce4265acd266be09d3c
SHA512:	1204b683f15e89bb0f09b1be5fd3a18afbe83c72e95023cc58864924bec0f2dd3f228983365f654e22e822e7c0438c0b4d37660b8e2d875881ab859a488f4c34
SSDEEP:	12288:vDo1nsbnnnnncQlbt7WD31NYfr2S+K/WKBGEnnnnnnnnnnnnnnnnnnnnnnnnnnnO:LAnsbnnnnnXtaDFNYjnTzBNnnnnnnnnU
TLSH:	5DD4E03D9BD84A39D9AFCB3BD0F05911F632F2E2158AD34E5095A3B91D07790EA0235B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.....0..... .....@.. .....@.....

File Icon

Icon Hash:	90cececece8e8eb0

Static PE Info

General

Entrypoint:	0x49b6de
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:	0xCA00A32F [Sun May 23 23:50:07 2077 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9b68c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x642	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9e000	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	0x996e4	0x99800	6d9456d015054223a50697288d2ae862	False	0.7322914546009772	data	7.633926656601929	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x642	0x800	af09505b4658a694da8a50f0e7f65376	False	0.349609375	data	3.5330423110083116	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	e968bd63315dda314fc03eb83b10c2fd	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

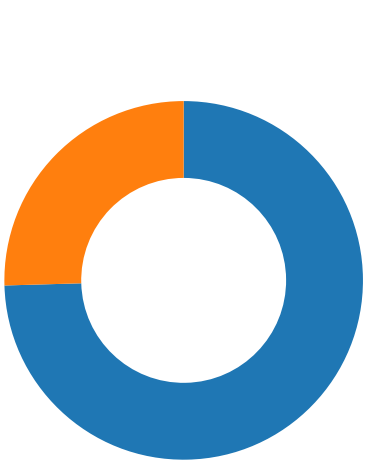
Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0x9c0a0	0x3b8	COM executable for DOS			0.42436974789915966
RT_MANIFEST	0x9c458	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 08:24:43.249557972 CEST	49736	80	192.168.2.4	148.251.36.121
May 2, 2024 08:24:43.424362898 CEST	80	49736	148.251.36.121	192.168.2.4
May 2, 2024 08:24:43.424546957 CEST	49736	80	192.168.2.4	148.251.36.121
May 2, 2024 08:24:43.587449074 CEST	49736	80	192.168.2.4	148.251.36.121
May 2, 2024 08:24:43.762599945 CEST	80	49736	148.251.36.121	192.168.2.4
May 2, 2024 08:24:43.763344049 CEST	80	49736	148.251.36.121	192.168.2.4
May 2, 2024 08:24:43.763531923 CEST	80	49736	148.251.36.121	192.168.2.4
May 2, 2024 08:24:43.763606071 CEST	49736	80	192.168.2.4	148.251.36.121
May 2, 2024 08:24:44.548010111 CEST	49736	80	192.168.2.4	148.251.36.121
May 2, 2024 08:24:44.722882986 CEST	80	49736	148.251.36.121	192.168.2.4
May 2, 2024 08:25:02.053174019 CEST	49738	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:02.264493942 CEST	80	49738	194.58.112.173	192.168.2.4
May 2, 2024 08:25:02.264668941 CEST	49738	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:02.266545057 CEST	49738	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:02.475363970 CEST	80	49738	194.58.112.173	192.168.2.4
May 2, 2024 08:25:02.513768911 CEST	80	49738	194.58.112.173	192.168.2.4
May 2, 2024 08:25:02.513788939 CEST	80	49738	194.58.112.173	192.168.2.4
May 2, 2024 08:25:02.513833046 CEST	49738	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:03.779613972 CEST	49738	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:04.798501015 CEST	49739	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:05.002785921 CEST	80	49739	194.58.112.173	192.168.2.4
May 2, 2024 08:25:05.002911091 CEST	49739	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:05.004878998 CEST	49739	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:05.208945036 CEST	80	49739	194.58.112.173	192.168.2.4
May 2, 2024 08:25:05.224226952 CEST	80	49739	194.58.112.173	192.168.2.4
May 2, 2024 08:25:05.224246025 CEST	80	49739	194.58.112.173	192.168.2.4
May 2, 2024 08:25:05.224351883 CEST	49739	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:05.225511074 CEST	49739	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:06.628921986 CEST	49739	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:09.596995115 CEST	49740	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:09.801656961 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:09.801799059 CEST	49740	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:09.804352999 CEST	49740	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:10.009121895 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009144068 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009156942 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009166956 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009188890 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009258986 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009270906 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.009371042 CEST	80	49740	194.58.112.173	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 08:25:10.009432077 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.032634020 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.032651901 CEST	80	49740	194.58.112.173	192.168.2.4
May 2, 2024 08:25:10.032741070 CEST	49740	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:11.310885906 CEST	49740	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:12.329361916 CEST	49741	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:12.531092882 CEST	80	49741	194.58.112.173	192.168.2.4
May 2, 2024 08:25:12.531203032 CEST	49741	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:12.829895973 CEST	49741	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:13.031876087 CEST	80	49741	194.58.112.173	192.168.2.4
May 2, 2024 08:25:13.080692053 CEST	80	49741	194.58.112.173	192.168.2.4
May 2, 2024 08:25:13.080713987 CEST	80	49741	194.58.112.173	192.168.2.4
May 2, 2024 08:25:13.080780029 CEST	49741	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:13.792197943 CEST	49741	80	192.168.2.4	194.58.112.173
May 2, 2024 08:25:13.993874073 CEST	80	49741	194.58.112.173	192.168.2.4
May 2, 2024 08:25:19.750816107 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:19.958864927 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:19.959019899 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:19.965226889 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.173122883 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.175931931 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.175975084 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.175988913 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176024914 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.176028967 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176043987 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176070929 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.176079988 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176120043 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.176145077 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176199913 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176213026 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176227093 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.176242113 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.176259995 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384119987 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384149075 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384219885 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384248018 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384330988 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384344101 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384378910 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384380102 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384454966 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384501934 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384520054 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384532928 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384572983 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384588003 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384602070 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384637117 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384661913 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384722948 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384762049 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384785891 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384841919 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384880066 CEST	49742	80	192.168.2.4	195.24.68.5
May 2, 2024 08:25:20.384896994 CEST	80	49742	195.24.68.5	192.168.2.4
May 2, 2024 08:25:20.384965897 CEST	80	49742	195.24.68.5	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 2, 2024 08:24:42.305643082 CEST	61840	53	192.168.2.4	1.1.1.1
May 2, 2024 08:24:43.243988991 CEST	53	61840	1.1.1.1	192.168.2.4
May 2, 2024 08:25:00.439603090 CEST	63275	53	192.168.2.4	1.1.1.1
May 2, 2024 08:25:01.043719053 CEST	53	63275	1.1.1.1	192.168.2.4
May 2, 2024 08:25:18.798521042 CEST	51423	53	192.168.2.4	1.1.1.1
May 2, 2024 08:25:19.747693062 CEST	53	51423	1.1.1.1	192.168.2.4
May 2, 2024 08:25:33.814400911 CEST	49662	53	192.168.2.4	1.1.1.1
May 2, 2024 08:25:34.013406992 CEST	53	49662	1.1.1.1	192.168.2.4
May 2, 2024 08:25:51.518388987 CEST	61308	53	192.168.2.4	1.1.1.1
May 2, 2024 08:25:51.734960079 CEST	53	61308	1.1.1.1	192.168.2.4
May 2, 2024 08:26:05.378520966 CEST	64909	53	192.168.2.4	1.1.1.1
May 2, 2024 08:26:05.568423986 CEST	53	64909	1.1.1.1	192.168.2.4
May 2, 2024 08:26:19.580396891 CEST	52001	53	192.168.2.4	1.1.1.1
May 2, 2024 08:26:20.311863899 CEST	53	52001	1.1.1.1	192.168.2.4
May 2, 2024 08:26:36.080804110 CEST	64257	53	192.168.2.4	1.1.1.1
May 2, 2024 08:26:36.639506102 CEST	53	64257	1.1.1.1	192.168.2.4
May 2, 2024 08:26:51.503310919 CEST	54883	53	192.168.2.4	1.1.1.1
May 2, 2024 08:26:52.157618999 CEST	53	54883	1.1.1.1	192.168.2.4
May 2, 2024 08:27:07.446336031 CEST	55174	53	192.168.2.4	1.1.1.1
May 2, 2024 08:27:07.570497036 CEST	53	55174	1.1.1.1	192.168.2.4
May 2, 2024 08:27:15.830028057 CEST	64728	53	192.168.2.4	1.1.1.1
May 2, 2024 08:27:16.118583918 CEST	53	64728	1.1.1.1	192.168.2.4
May 2, 2024 08:27:30.429325104 CEST	61035	53	192.168.2.4	1.1.1.1
May 2, 2024 08:27:30.992764950 CEST	53	61035	1.1.1.1	192.168.2.4
May 2, 2024 08:27:39.048943996 CEST	60092	53	192.168.2.4	1.1.1.1
May 2, 2024 08:27:39.328984022 CEST	53	60092	1.1.1.1	192.168.2.4
May 2, 2024 08:27:57.249764919 CEST	57423	53	192.168.2.4	1.1.1.1
May 2, 2024 08:27:57.446818113 CEST	53	57423	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
May 2, 2024 08:24:42.305643082 CEST	192.168.2.4	1.1.1.1	0xf080	Standard query (0)	www.vavada-band.ru	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:00.439603090 CEST	192.168.2.4	1.1.1.1	0xcb70	Standard query (0)	www.bettaroom.ru	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:18.798521042 CEST	192.168.2.4	1.1.1.1	0xa6af	Standard query (0)	www.dhleba51.ru	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:33.814400911 CEST	192.168.2.4	1.1.1.1	0xfbd3	Standard query (0)	www.dainikmirpur.com	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:51.518388987 CEST	192.168.2.4	1.1.1.1	0x2cc1	Standard query (0)	www.whirledairlines.com	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:05.378520966 CEST	192.168.2.4	1.1.1.1	0x31a	Standard query (0)	www.quantummquest.top	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:19.580396891 CEST	192.168.2.4	1.1.1.1	0x9a84	Standard query (0)	www.yamiyasheec.online	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:36.080804110 CEST	192.168.2.4	1.1.1.1	0xb152	Standard query (0)	www.applesolve.com	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:51.503310919 CEST	192.168.2.4	1.1.1.1	0x839a	Standard query (0)	www.xxaiai.top	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:07.446336031 CEST	192.168.2.4	1.1.1.1	0x5260	Standard query (0)	www.vaesen.net	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:15.830028057 CEST	192.168.2.4	1.1.1.1	0xe6b5	Standard query (0)	www.dk48.lol	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:30.429325104 CEST	192.168.2.4	1.1.1.1	0x7837	Standard query (0)	www.cluird.cloud	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:39.048943996 CEST	192.168.2.4	1.1.1.1	0xa81d	Standard query (0)	www.cucuzeus88.store	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:57.249764919 CEST	192.168.2.4	1.1.1.1	0xee7b	Standard query (0)	www.bnbuotqakx.shop	A (IP address)	IN (0x0001)	false

DNS Answers

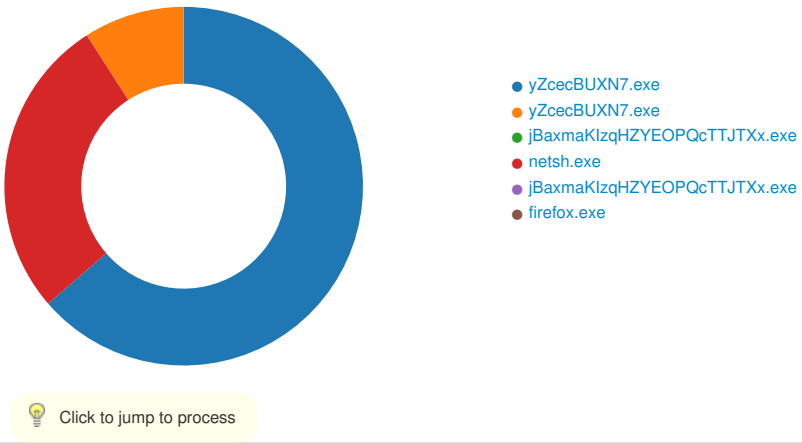
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 2, 2024 08:24:43.243988991 CEST	1.1.1.1	192.168.2.4	0xf080	No error (0)	www.vavada-band.ru	vavada-band.ru		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:24:43.243988991 CEST	1.1.1.1	192.168.2.4	0xf080	No error (0)	vavada-band.ru		148.251.36.121	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:01.043719053 CEST	1.1.1.1	192.168.2.4	0xcb70	No error (0)	www.bettaroom.ru		194.58.112.173	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:19.747693062 CEST	1.1.1.1	192.168.2.4	0xa6af	No error (0)	www.dhleba51.ru		195.24.68.5	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:34.013406992 CEST	1.1.1.1	192.168.2.4	0xfbd3	No error (0)	www.dainikmirpur.com	dainikmirpur.com		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:25:34.013406992 CEST	1.1.1.1	192.168.2.4	0xfbd3	No error (0)	dainikmirpur.com		192.250.235.36	A (IP address)	IN (0x0001)	false
May 2, 2024 08:25:51.734960079 CEST	1.1.1.1	192.168.2.4	0x2cc1	No error (0)	www.whirledairlines.com		216.40.34.41	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:05.568423986 CEST	1.1.1.1	192.168.2.4	0x31a	No error (0)	www.quantummquest.top		203.161.50.127	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:20.311863899 CEST	1.1.1.1	192.168.2.4	0x9a84	No error (0)	www.yamiyasheec.online	yamiyasheec.online		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:26:20.311863899 CEST	1.1.1.1	192.168.2.4	0x9a84	No error (0)	yamiyasheec.online		119.18.54.116	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:36.639506102 CEST	1.1.1.1	192.168.2.4	0xb152	No error (0)	www.applesolve.com	applesolve.com		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:26:36.639506102 CEST	1.1.1.1	192.168.2.4	0xb152	No error (0)	applesolve.com		188.116.38.155	A (IP address)	IN (0x0001)	false
May 2, 2024 08:26:52.157618999 CEST	1.1.1.1	192.168.2.4	0x839a	No error (0)	www.xxaiai.top		108.186.8.158	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:07.570497036 CEST	1.1.1.1	192.168.2.4	0x5260	Name error (3)	www.vaesen.net	none	none	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:16.118583918 CEST	1.1.1.1	192.168.2.4	0xe6b5	No error (0)	www.dk48.lol	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:27:16.118583918 CEST	1.1.1.1	192.168.2.4	0xe6b5	No error (0)	parkingpage.namecheap.com		91.195.240.19	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:30.992764950 CEST	1.1.1.1	192.168.2.4	0x7837	Name error (3)	www.cluird.cloud	none	none	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:39.328984022 CEST	1.1.1.1	192.168.2.4	0xa81d	No error (0)	www.cucuzeus88.store	cucuzeus88.store		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:27:39.328984022 CEST	1.1.1.1	192.168.2.4	0xa81d	No error (0)	cucuzeus88.store		153.92.8.41	A (IP address)	IN (0x0001)	false
May 2, 2024 08:27:57.446818113 CEST	1.1.1.1	192.168.2.4	0xee7b	No error (0)	www.bnbuotqakx.shop	bnbuotqakx.shop		CNAME (Canonical name)	IN (0x0001)	false
May 2, 2024 08:27:57.446818113 CEST	1.1.1.1	192.168.2.4	0xee7b	No error (0)	bnbuotqakx.shop		101.99.93.157	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.vavada-band.ru
- www.bettaroom.ru
- www.dhleba51.ru
- www.dainikmirpur.com
- www.whirledairlines.com
- www.quantummquest.top
- www.yamiyasheec.online
- www.applesolve.com
- www.xxaiai.top
- www.dk48.lol
- www.cucuzeus88.store
- www.bnbuotqakx.shop

Statistics

Behavior



System Behavior

Analysis Process: yZcecBUXN7.exe PID: **6640**, Parent PID: **2580**

General

Target ID:	0
Start time:	08:23:52
Start date:	02/05/2024
Path:	C:\Users\user\Desktop\yZcecBUXN7.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\yZcecBUXN7.exe"
Imagebase:	0x6d0000
File size:	631'808 bytes
MD5 hash:	9CD48F0D93C28AE6559409DE23414554
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MALWARE_Win_DLInjector02, Description: Detects downloader injector, Source: 00000000.00000002.1627462031.0000000005140000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	low
Has exited:	true

File Activities

Analysis Process: yZcecBUXN7.exe PID: 6712, Parent PID: 6640

General

Target ID:	1
Start time:	08:23:52
Start date:	02/05/2024
Path:	C:\Users\user\Desktop\yZcecBUXN7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\yZcecBUXN7.exe"
Imagebase:	0x690000
File size:	631'808 bytes
MD5 hash:	9CD48F0D93C28AE6559409DE23414554
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: 00000001.00000002.1897755674.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.1897755674.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.1898683610.0000000001020000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.1898683610.0000000001020000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000001.00000002.1899804288.0000000001640000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.1899804288.0000000001640000.00000040.10000000.00040000.00000000.sdmp, Author: unknown
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	40A5E3	NtReadFile
C:\Windows\SysWOW64\netsh.exe	0	82432	success or wait	1	40A5E3	NtReadFile

Analysis Process: jBaxmaKIzqHZYEOPQcTTJTXx.exe PID: 3688, Parent PID: 6712

General

Target ID:	2
Start time:	08:24:07
Start date:	02/05/2024
Path:	C:\Program Files (x86)\DUKoqSpezAPdkEeQLfXbQJktRyLdTGIcgkgDcRWuknrvtOsFOYoJLHQwvsoW\jBaxmaKIzqHZYEOPQcTTJTXx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DUKoqSpezAPdkEeQLfXbQJktRyLdTGIcgkgDcRWuknrvtOsFOYoJLHQwvsoW\jBaxmaKIzqHZYEOPQcTTJTXx.exe"
Imagebase:	0x40000

File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
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: 00000002.00000002.4123873184.0000000002960000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.4123873184.0000000002960000.00000040.00000001.00040000.00000000.sdmp, Author: unknown
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: netsh.exe PID: **6760**, Parent PID: **3688**

General

Target ID:	4
Start time:	08:24:12
Start date:	02/05/2024
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\netsh.exe"
Imagebase:	0x1560000
File size:	82'432 bytes
MD5 hash:	4E89A1A088BE715D6C946E55AB07C7DF
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: 00000004.00000002.4122807420.0000000000C00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.4122807420.0000000000C00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.4123925036.0000000001320000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.4123925036.0000000001320000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.4123058161.0000000000F00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.4123058161.0000000000F00000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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\Desktop\yZcecBUXN7.exe	success or wait	1	C278DD	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1-00F23L	object name not found	1	C278DD	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1-00F23L	sharing violation	1	C278DD	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1-00F23L	sharing violation	1	C278DD	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1-00F23L	sharing violation	1	C278DD	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	C2783D	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: jBaxmaKIzqHZYEOPQcTTJTXx.exe PID: **916**, Parent PID: **6760**

General

Target ID:	7
Start time:	08:24:27
Start date:	02/05/2024
Path:	C:\Program Files (x86)\DUKoqSpezAPdkEeQLfXbQJktRyLdTGIcgkgDcRWuknrvtOsFOYoJLHQwvsoW\jBaxmaKIzqHZYEOPQcTTJTXx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DUKoqSpezAPdkEeQLfXbQJktRyLdTGIcgkgDcRWuknrvtOsFOYoJLHQwvsoW\jBaxmaKIzqHZYEOPQcTTJTXx.exe"
Imagebase:	0x40000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
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: 00000007.00000002.4125352041.00000000055B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000002.4125352041.00000000055B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high
Has exited:	false

Analysis Process: firefox.exe PID: **3020**, Parent PID: **6760**

General

Target ID:	8
Start time:	08:24:50
Start date:	02/05/2024
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Mozilla Firefox\Firefox.exe"
Imagebase:	0x7ff72bec0000
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