ID: 1436772
Sample Name: Gj8P0mbklo.exe
Cookbook: default.jbs
Time: 15:19:09
Date: 06/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

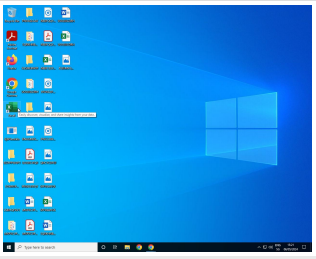
Windows Analysis Report

Gj8P0mbklo.exe

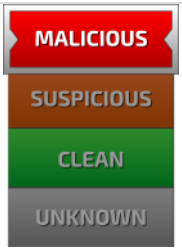
Overview

General Information

Sample name:	Gj8P0mbklo.exerenamed because original name is a hash value
Original sample name:	f7d15a3027d3a..
Analysis ID:	1436772
MD5:	bad3fa5127efc…
SHA1:	c5f49dd54b71e..
SHA256:	f7d15a3027d3a..
Tags:	ACRStealer exe
Infos:	



Detection



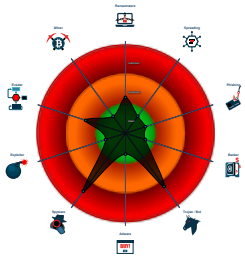
Arc Stealer

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Arc Stealer
- Found many strings related to Crypt…
- Machine Learning detection for sam…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Crypto Currency Walle…
- Contains functionality to call native …
- Contains functionality to check if a d…
- Contains functionality to query CPU…
- Contains functionality to query local…

Classification



Process Tree

- **System is w10x64**
- Gj8P0mbklo.exe (PID: 6256 cmdline: "C:\Users\user\Desktop\Gj8P0mbklo.exe" MD5: BAD3FA5127EFCC9C678C5D71FCE0D0B2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.2152455570.00000000027B1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Gj8P0mbklo.exe PID: 6256	JoeSecurity_ArcStealer	Yara detected Arc Stealer	Joe Security	
Process Memory Space: Gj8P0mbklo.exe PID: 6256	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Stealing of Sensitive Information

Yara detected Arc Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

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

Tries to harvest and steal ftp login credentials

Tries to steal Crypto Currency Wallets

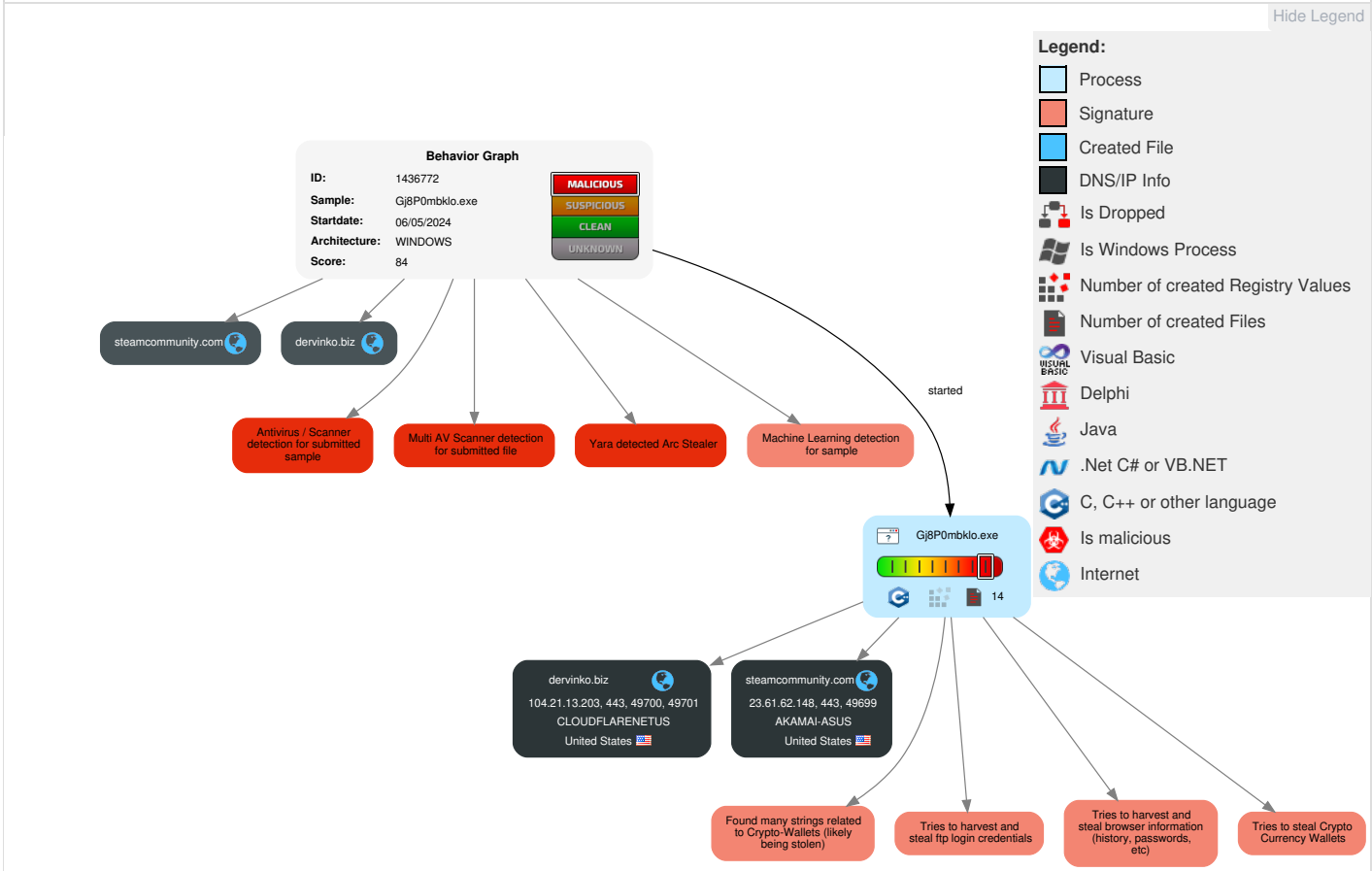
Remote Access Functionality

Yara detected Arc Stealer

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	1 DLL Side-Loading	1 Masqueradi ng	2 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate /Decode Files or Information	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	4 Data from Local System	2 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 Process Discovery	SMB/Windo ws Admin Shares	Data from Network Shared Drive	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	1 File and Directory 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	Software Packing	LSA Secrets	2 2 System Information Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact

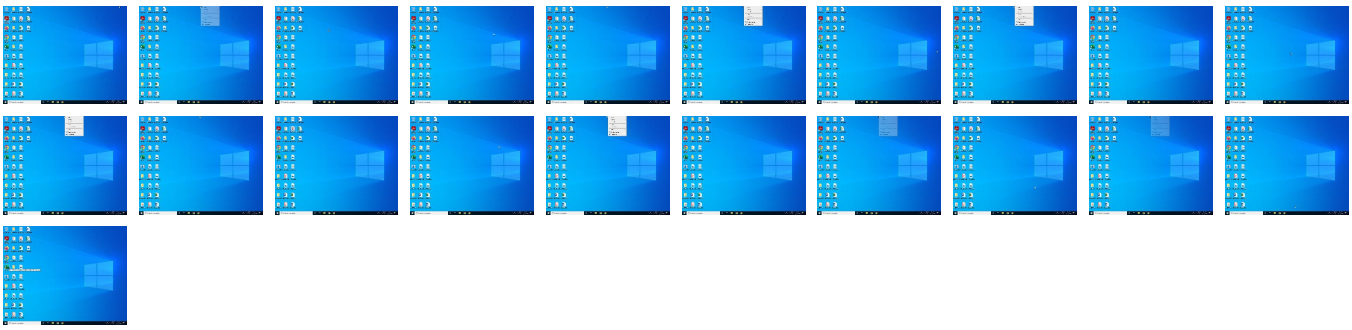
Behavior Graph



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
Gj8P0mbklo.exe	58%	ReversingLabs	Win32.Trojan.Barys	
Gj8P0mbklo.exe	62%	Virustotal		Browse
Gj8P0mbklo.exe	100%	Avira	TR/PSW.Coins.ujryq	
Gj8P0mbklo.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dervinko.biz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.rootca1.amazontrust.com/rootca1.crl0	0%	URL Reputation	safe	
http://https://broadcast.st.dl.eccdnx.com	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://https://recaptcha.net	0%	URL Reputation	safe	
http://https://s.ytimg.com;	0%	Avira URL Cloud	safe	
http://https://www.gstatic.cn/recaptcha/	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up/b_	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up/bAW	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up/bistAndAuditAlarmByHandle	0%	Avira URL Cloud	safe	
http://https://steam.tv/	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/ujs/89737b57-777d-400d-bb7f-77b7e024920e	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up	0%	Virustotal		Browse
http://https://lv.queniujq.cn	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/q	0%	Avira URL Cloud	safe	
http://https://steam.tv/	0%	Virustotal		Browse
http://https://www.gstatic.cn/recaptcha/	0%	Virustotal		Browse
http://https://dervinko.biz	0%	Avira URL Cloud	safe	
http://https://recaptcha.net/recaptcha/;	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up/bistAndAuditAlarmByHandleerta	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/ujs/89737b57-777d-400d-bb7f-77b7e024920e	0%	Virustotal		Browse
http://https://medal.tv	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/Up/byDllc	0%	Avira URL Cloud	safe	
http://https://recaptcha.net/recaptcha/;	0%	Virustotal		Browse
http://https://dervinko.biz	0%	Virustotal		Browse
http://https://medal.tv	0%	Virustotal		Browse
http://https://dervinko.biz/Up/b	0%	Avira URL Cloud	safe	
http://https://lv.queniujq.cn	0%	Virustotal		Browse
http://127.0.0.1:27060	0%	Avira URL Cloud	safe	
http://https://dervinko.biz/	0%	Virustotal		Browse
http://127.0.0.1:27060	0%	Virustotal		Browse
http://https://dervinko.biz/Up/b	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	23.61.62.148	true	false		high
dervinko.biz	104.21.13.203	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dervinko.biz/Up	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dervinko.biz/ujs/89737b57-777d-400d-bb7f-77b7e024920e	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199609719039	false		high
http://https://dervinko.biz/Up/b	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://player.vimeo.com	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=_Vry	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://steamcommunity.com/?subsection=broadcasts	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://store.steampowered.com/subscriber_agreement/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://www.gstatic.cn/recaptcha/	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/libraries~b28b7af6	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/modalContent.js?v=L35TrLJDfqtD&l=engl	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://www.valvesoftware.com/legal.htm	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://www.youtube.com	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://www.google.com	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.208309434400000000028030000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://dervinko.biz/Up/bAW	Gj8P0mbklo.exe, 00000000.00000003.2151751922.000000000509F000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.215171246500000000509000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dervinko.biz/Up/b_	Gj8P0mbklo.exe, 00000000.00000003.2151826752.000000000507F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIIcMzCffX6&	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/profile.js?v=Iy1ies1ROjUT&l=english	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://steamcommunity.com/profiles/76561199609719039/badges	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://s.ytimg.com;	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://steam.tv/	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dervinko.biz/Up/bistAndAuditAlarmByHandle	Gj8P0mbklo.exe, 00000000.00000003.2151712465.00000000050CE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://store.steampowered.com/privacy_agreement/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://store.steampowered.com/points/shop/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.rootca1.amazontrust.com/rootca1.crl0	Gj8P0mbklo.exe, 00000000.00000003.2145279946.00000000052ED000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

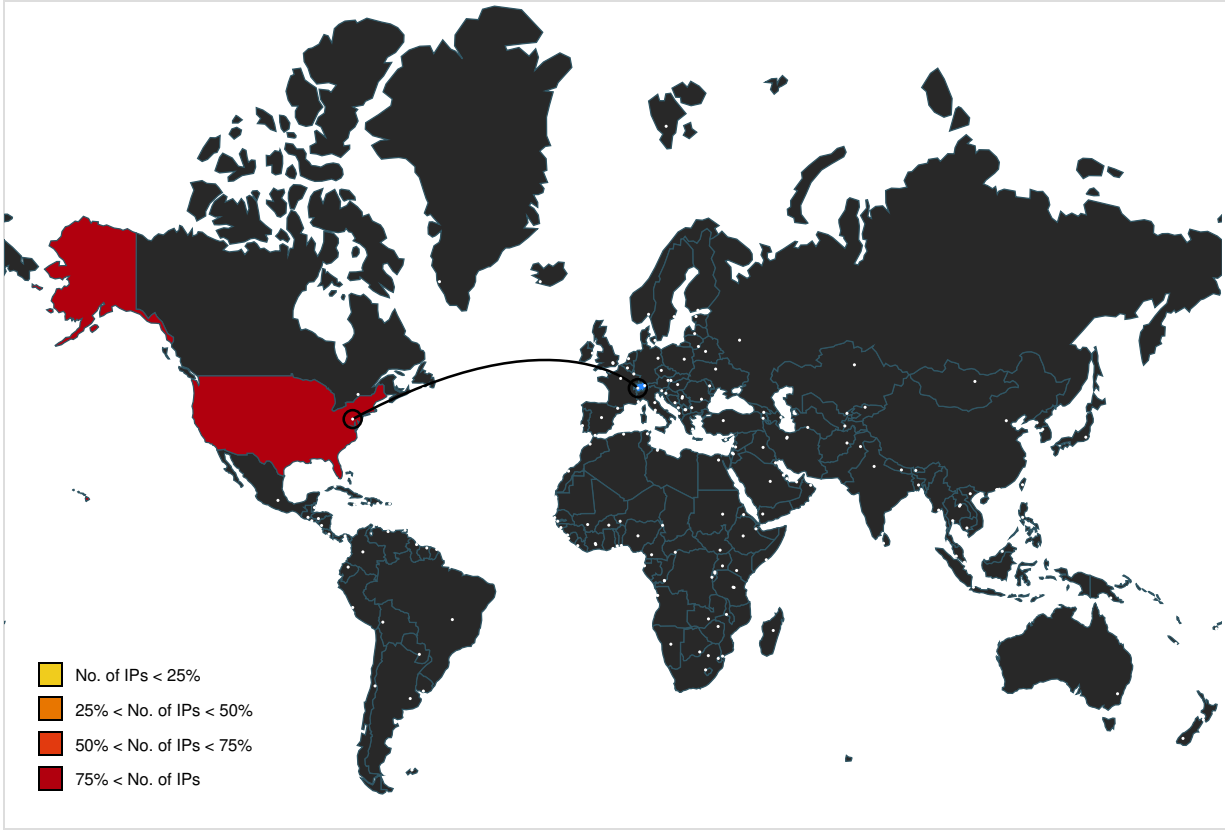
Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.rootca1.amazontrust.com0:	Gj8P0mbklo.exe, 00000000.00000003.214527 9946.00000000052ED000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sketchfab.com	Gj8P0mbklo.exe, 00000000.00000003.207752 3999.00000000027C8000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://www.ecosia.org/newtab/	Gj8P0mbklo.exe, 00000000.00000003.210884 4417.0000000005138000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://lv.queniujq.cn	Gj8P0mbklo.exe, 00000000.00000003.207752 3999.00000000027C8000.00000004.00000020. 00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.youtube.com/	Gj8P0mbklo.exe, 00000000.00000003.207752 3999.00000000027C8000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://avatars.akamai.steamstatic.com/fef49e7fa7e19 97310d705b2a6158ff8dc1cdfeb_full.jpg	76561199609719039[1].htm.0.dr	false		high
http://https://store.steampowered.com/privacy_agreement/	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/shar ed/javascript/tooltip.js?v=.zYHOpI1L3Rt0	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://dervinko.biz/q	Gj8P0mbklo.exe, 00000000.00000002.215286 4496.000000000507F000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2151826752.00000000050 7F000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shar ed/javascript/shared_global.js?v=REEGJU1hwkYI&am	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://www.google.com/recaptcha/	Gj8P0mbklo.exe, 00000000.00000003.207752 3999.00000000027C8000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://checkout.steampowered.com/	Gj8P0mbklo.exe, 00000000.00000003.207752 3999.00000000027C8000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/css/g lobalv2.css?v=PAcV2zMBzzSV&l=english	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/javas cript/modalv2.js?v=dfMhuy-Lrpyo&l=english	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/shar ed/images/responsive/header_logo.png	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/s kin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/javas cript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	Gj8P0mbklo.exe, 00000000.00000002.215245 5570.0000000002805000.00000004.00000020. 00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.00000000028 03000.00000004.00000020.00020000.0000000 0.sdmp, 76561199609719039[1].htm.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/;	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://store.steampowered.com/about/	76561199609719039[1].htm.0.dr	false		high
http://https://steamcommunity.com/my/wishlist/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://steamcommunity.com/-	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002794000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://help.steampowered.com/en/	Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://cdn.akamai.steamstatic.com/steamcommunity/public/assets/	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://steamcommunity.com/market/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://store.steampowered.com/news/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=roSu8uqw	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://dervinko.biz	Gj8P0mbklo.exe, 00000000.00000002.2152455570.00000000027B1000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high
http://store.steampowered.com/subscriber_agreement/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://recaptcha.net/recaptcha/;	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://steamcommunity.com/discussions/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://dervinko.biz/Up/bistAndAuditAlarmByHandleerta	Gj8P0mbklo.exe, 00000000.00000003.2145426350.00000000050CE000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2145176778.00000000050CA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.steampowered.com/stats/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://medal.tv	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://broadcast.st.dl.eccdnx.com	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://community.akamai.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://store.steampowered.com/steam_refunds/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://x1.c.lencr.org/0	Gj8P0mbklo.exe, 00000000.00000003.2145279946.00000000052ED000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	Gj8P0mbklo.exe, 00000000.00000003.2145279946.00000000052ED000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://steamcommunity.com/profiles/76561199609719039(	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002794000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dervinko.biz/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.00000000027B1000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000002.2152864496.000000005077F000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2151826752.000000000507F000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199609719039B	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002794000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://steamcommunity.com/workshop/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://login.steampowered.com/	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://store.steampowered.com/legal/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&l=e	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/css/applications/community/main.css?v=tIrWyaxi8ABA&a	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_responsive_adapter.js?v=pSv	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=engl	76561199609719039[1].htm.0.dr	false		high
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dervinko.biz/Up/byDllc	Gj8P0mbklo.exe, 00000000.00000003.2151751922.000000000509F000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2151712465.0000000005090000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://recaptcha.net	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://store.steampowered.com/	76561199609719039[1].htm.0.dr	false		high
http:// https://community.akamai.steamstatic.com/public/javascript/prototype-1.7.js?v=.55t44gwuwgvw	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http:// https://community.akamai.steamstatic.com/public/images/skin_1/arrowDn9x5.gif	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://127.0.0.1:27060	Gj8P0mbklo.exe, 00000000.00000003.2077523999.00000000027C8000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://steamcommunity.com/profiles/76561199609719039/inventory/	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http:// https://community.akamai.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http:// https://community.akamai.steamstatic.com/public/javascript/webui/clientcom.js?v=KyfgrihL0xta&l=e	Gj8P0mbklo.exe, 00000000.00000002.2152455570.0000000002805000.00000004.00000020.00020000.00000000.sdmp, Gj8P0mbklo.exe, 00000000.00000003.2083094344.0000000002803000.00000004.00000020.00020000.00000000.sdmp, 76561199609719039[1].htm.0.dr	false		high
http://https://ac.ecosia.org/autocomplete?q=	Gj8P0mbklo.exe, 00000000.00000003.2108844417.0000000005138000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.61.62.148	steamcommunity.com	United States		16625	AKAMAI-ASUS	false
104.21.13.203	dervinko.biz	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1436772
Start date and time:	2024-05-06 15:19:09 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 18s
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:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	Gj8P0mbklo.exerenamed because original name is a hash value
Original Sample Name:	f7d15a3027d3a430511630c91898c72b91b5fb42bf99315cc5a5ef009a473835.exe
Detection:	MAL
Classification:	mal84.troj.spyw.winEXE@1/2@2/2
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe
- 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
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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\Windows\INetCache\IE\8HXJSKQQ\76561199609719039[1].htm

Process:	C:\Users\user\Desktop\Gj8P0mbklo.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (2969), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34789
Entropy (8bit):	5.386073524863294
Encrypted:	false
SSDEEP:	768:/dpqm+0Ih3YAA9CWGEmfcDAfPzzgiJmDzJtxvrfJkPVoEAdmPzzgiJmDzJtxvJ2w:/d8m+0Ih3YAA9CWGEmFfPzzgiJmDzJtT
MD5:	A3CECEDB9036A82F050828BAA42E21D0
SHA1:	B4DE8B997C26E3CEAEB0C647B593E131E21BC6DB
SHA-256:	75F75C4403BFE3AFD61DDF8898252F488713CE759C5B3E08AD15657158912B6C
SHA-512:	7BA36300556F6BD255A6D414C70C032C276A72558F1457BEF08537B5A640A50D50C9A124736638696812A19A23C01722F4013DC96746567063053FC9A5C00949
Malicious:	false

Reputation:	low
Preview:	<!DOCTYPE html>..<html class=" responsive" lang="en">..<head>...<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.....<meta name="viewport" content="width=device-width,initial-scale=1">....<meta name="theme-color" content="#171a21">....<title>Steam Community :: 3e3 aHR0cHM6Ly9kZXJ2aW5rby5iaXo=</title>...<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">.....<link href="https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJlfhtcQn7W&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english" rel="stylesheet" type="text/css" >.<lin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\89737b57-777d-400d-bb7f-77b7e024920e[1].txt

Process:	C:\Users\user\Desktop\Gj8P0mbklo.exe
File Type:	ASCII text, with very long lines (47680), with no line terminators
Category:	dropped
Size (bytes):	47680
Entropy (8bit):	5.362966359018906
Encrypted:	false
SSDEEP:	768:vzsNZzFhOnDMIf19+kXSV0brSxnb22fnc6KWWhv6GYcnvabaMi9idvbU0nagalQb:v0zPO9f1ouYgLvRMymbU0ni4xKjo
MD5:	0B236AC4395E5E40F5AB3140CB892115
SHA1:	9AC2290905D9996E95291C84E14FF1006BFEE483
SHA-256:	ECB0B0F87288C16207310A58C67A25AC557A54FA328E74F592C051F1C44176FB
SHA-512:	87422C27CD7039C6A15CE32DE54E7733075F000A099191BE456594F2730F25559BB32862FE189159C2A8FADB3A52C863E052A44F66CE3CA24968A95FCE4F7E09
Malicious:	false
Reputation:	low
Preview:	Qz8SERZbFQgTWzIVEhEUQj0SEyAYFRITWhsNEhFiZGlRCRYVPRITIBgVEhNEGw0SEVxkeV1SVVVrbnRvV1JeVGhldFpBb1VQbm1hSlJAE0RZQVMTGDMXEhMgGBUQRRYDFwMfChgVEhEUGRVCXSICFRBSXEtYX1YuXU1XEz4ZFxITfRQ/EhEUGUw4EyAYFRIRFlcVCBMiWmluUgwbGzgTIBgVEhEWSRUIEyJkaX5eV1hbbm9HV1pVXVFla3FbcldYVxFnQWRub1VLUEARcFhDUxEsMhUSERQZFxBHIgIVAx0+GRcSEyAYF0JfFgMXEFBoSlpfVBpcT1cRChgVEhFJFT0SEyAYTjgRFBkXEhMiVhcIERZba25QOBoZOBEUGRcSEyJIFwgRFmVrflxjWVlubXNWWFVfZWRpcVlGVlpXE0JdQVNtaGxEV0EgfFRGUBYVPRITIBgVEhNAGw0SAiwyFRIRFBkXEENuGg8SE1dRRV1eZRZQSlQWMxcSEyBFGTgRFBkXSTkgGBUSERQbWRAJIBpXbm1XARUeOSAYFRIRFBtHEAkgGmlufVtaVl5vXH9aXVZYXGtucGhKWl9UFH1SRG9cbUZXQxR9VkZSIhQ/EhEUGRcSEXQaDxIAGDMXEhMgGBUQQVobDRIRY1BHXVxRF1JKViIyFRIRFEQbOBMgGBVJOxQZFxITIBpbEAsUG1Vub2MAFx47FBkXEhMgGkUQCxQba25/b1tUXm1oflhdVGxdaW5yXEtYX1YgbVtBRVVbW1dvXG1GV0MUfVZGUiIlUPxIRFBkXEhF0Gg8SABgzFxITIBgVEEFaGw0SEWNQR11cURdSSlYiMhUSERREGzgTIBgVSTsUGRcSEyAaWxALFBtVbm9jABceOxQZFxITIBpFEAsUG2tuf29bVF5taH5YXVRsXWluclxLWF9WIHtUXFBGQGtuZnNdRxJ1VU1WEB8KGBUSERQZFUYROhgEHjsUGRcSEyAaRVwTDhkVUVty

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.621191048042736
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Gj8P0mbklo.exe
File size:	362'496 bytes
MD5:	bad3fa5127efcc9c678c5d71fce0d0b2
SHA1:	c5f49dd54b71eaf4e1ba3a9fdfc51c7fb8afbea8
SHA256:	f7d15a3027d3a430511630c91898c72b91b5fb42bf99315cc5a5ef009a473835
SHA512:	5b6d5efa4dcf49a43e992652194d45a407e9482dcd21ff887ae709a98944c21d6b7ea67dc518493c0416e3fd2ee38ed0f02c3b75a762b6784af14f0ce69e78ab
SSDEEP:	6144:5OvAYHNayUljnWrd+VKTEK/AeI8eajd8j4xET4YAOqz/B:5mjNadljnWrd+V0EXzS+4CTNo7B
TLSH:	81747E11F182C032D4A202B11A65EFB696BCA93057A29CEF6BD05E7BDD342D26531F37
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K.....D.....D.....D.....@...D...@.....@.....D.....Rich.....

File Icon

Icon Hash:	00928e8e8686b000

Static PE Info

General

Entrypoint:	0x425140

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, REMOVABLE_RUN_FROM_SWAP
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x66115E48 [Sat Apr 6 14:38:00 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	2897cecb00338038ddfd70ec9000340f

Entrypoint Preview

Instruction
call 00007FBA6CC321B0h
jmp 00007FBA6CC31B6Eh
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00446568h
mov dword ptr [ecx], 00446560h
ret
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FBA6CC31CDFh
push 0045527Ch
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FBA6CC33095h
int3
push ebp
mov ebp, esp
and dword ptr [00458278h], 00000000h
sub esp, 24h
or dword ptr [0045700Ch], 01h
push 0000000Ah
call dword ptr [00446070h]
test eax, eax
je 00007FBA6CC31EB2h
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
nop
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi

Instruction
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-20h]
mov dword ptr [ebp-0Ch], eax
xor edi, 756E6547h
mov eax, dword ptr [ebp-18h]
xor eax, 49656E69h
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [ebp-1Ch]
xor eax, 6C65746Eh
mov dword ptr [ebp-08h], eax
xor eax, eax
inc eax
push ebx
cpuid
mov esi, ebx
pop ebx
nop
lea ebx, dword ptr [ebp-24h]
mov dword ptr [ebx], eax
mov eax, dword ptr [ebp-04h]
or eax, dword ptr [ebp-08h]
or eax, edi
mov dword ptr [ebx+04h], esi
mov dword ptr [ebx+08h], ecx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x55aa8	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x59000	0x2554	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x54078	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x53fb8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x46000	0x168	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4496a	0x44a00	6b6f1993190b3eaf82f607fed3374fc8	False	0.5182327242714025	data	6.601561733279373	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x46000	0x102ee	0x10400	1e6dbecf754d7dd193b7e04220f82d31	False	0.5084735576923077	data	5.746131858736808	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x57000	0x1cc4	0x1000	24b02a7a00e869dc523bbcf409d4920b	False	0.18701171875	data	3.063889339206937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

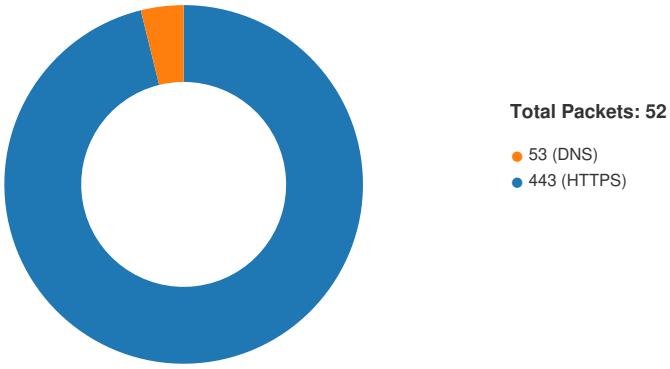
Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x59000	0x2554	0x2600	a0a7de2fc21f5b1845c1b665768ca164	False	0.7729235197368421	data	6.576489949652338	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	MultiByteToWideChar, HeapFree, OutputDebugStringA, lstrlenA, Sleep, GetTempPathA, HeapAlloc, GetProcessHeap, GetModuleHandleW, FreeLibrary, GetNativeSystemInfo, ExitProcess, TerminateProcess, OpenProcess, CreateToolhelp32Snapshot, Process32NextW, Process32FirstW, CloseHandle, WideCharToMultiByte, HeapSize, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetOEMCP, GetACP, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, GetStringTypeW, InitializeCriticalSectionEx, GetProcAddress, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, EncodePointer, DecodePointer, LCMapStringEx, GetCPInfo, RaiseException, RtlUnwind, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, SetEndOfFile, CreateFileW, GetFileType, GetModuleHandleExW, GetModuleFileNameW, GetStdHandle, WriteFile, GetCommandLineA, GetCommandLineW, SetStdHandle, GetConsoleOutputCP, GetConsoleMode, SetFilePointerEx, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetTimeZoneInformation, FlushFileBuffers, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, WriteConsoleW
SHELL32.dll	SHGetFolderPathA
WININET.dll	InternetWriteFile
SHLWAPI.dll	PathMatchSpecA

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 15:19:55.149740934 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.149780989 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.149878979 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.161875963 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.161890984 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.391609907 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.391819954 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.444205999 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.444225073 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.444700956 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.444834948 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.449176073 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.496125937 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.838845015 CEST	443	49699	23.61.62.148	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 15:19:55.838876009 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.838912010 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.839104891 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.839135885 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.839184046 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.962378979 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.962412119 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.962541103 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.962568045 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.962582111 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.962610960 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.967142105 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.967272043 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.967281103 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:55.967377901 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.972943068 CEST	49699	443	192.168.2.6	23.61.62.148
May 6, 2024 15:19:55.972974062 CEST	443	49699	23.61.62.148	192.168.2.6
May 6, 2024 15:19:56.155708075 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.155756950 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.155839920 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.156408072 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.156419992 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.393218040 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.393338919 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.398700953 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.398711920 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.399003029 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.399066925 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.405627012 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.448128939 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896373987 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896470070 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896505117 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896516085 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896526098 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896562099 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896565914 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896601915 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896605015 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896637917 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896641016 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896672964 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896675110 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896708012 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896709919 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896742105 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896752119 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896754980 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896773100 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896800995 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896804094 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896837950 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:56.896841049 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:56.896872997 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.005980968 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006058931 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006098032 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006108046 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006123066 CEST	49700	443	192.168.2.6	104.21.13.203

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 15:19:57.006171942 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006258965 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006299973 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006303072 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006347895 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006350994 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006392956 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006820917 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006869078 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006872892 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006906033 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006917953 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006956100 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.006958961 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.006994963 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.007008076 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.007049084 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.007666111 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.007711887 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.007720947 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.007752895 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.007771969 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.007808924 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.007812023 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.007847071 CEST	49700	443	192.168.2.6	104.21.13.203
May 6, 2024 15:19:57.007858038 CEST	443	49700	104.21.13.203	192.168.2.6
May 6, 2024 15:19:57.007891893 CEST	49700	443	192.168.2.6	104.21.13.203

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2024 15:19:55.033732891 CEST	62546	53	192.168.2.6	1.1.1.1
May 6, 2024 15:19:55.143752098 CEST	53	62546	1.1.1.1	192.168.2.6
May 6, 2024 15:19:55.987637043 CEST	53986	53	192.168.2.6	1.1.1.1
May 6, 2024 15:19:56.107733011 CEST	53	53986	1.1.1.1	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 6, 2024 15:19:55.033732891 CEST	192.168.2.6	1.1.1.1	0xa300	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false
May 6, 2024 15:19:55.987637043 CEST	192.168.2.6	1.1.1.1	0x52c	Standard query (0)	dervinko.biz	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 6, 2024 15:19:55.143752098 CEST	1.1.1.1	192.168.2.6	0xa300	No error (0)	steamcommunity.com		23.61.62.148	A (IP address)	IN (0x0001)	false
May 6, 2024 15:19:56.107733011 CEST	1.1.1.1	192.168.2.6	0x52c	No error (0)	dervinko.biz		104.21.13.203	A (IP address)	IN (0x0001)	false
May 6, 2024 15:19:56.107733011 CEST	1.1.1.1	192.168.2.6	0x52c	No error (0)	dervinko.biz		172.67.133.22	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com
- dervinko.biz

Statistics

No statistics

System Behavior

Analysis Process: Gj8P0mbklo.exe PID: 6256, Parent PID: 4004

General

Target ID:	0
Start time:	15:19:53
Start date:	06/05/2024
Path:	C:\Users\user\Desktop\Gj8P0mbklo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Gj8P0mbklo.exe"
Imagebase:	0x350000
File size:	362'496 bytes
MD5 hash:	BAD3FA5127EFCC9C678C5D71FCE0D0B2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.2152455570.00000000027B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36F6A3	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36F6A3	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36F6A3	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36F6A3	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36F6A3	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36F6A3	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\76561199609719039[1].htm	0	1024	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 20 72 65 73 70 6f 6e 73 69 76 65 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0d 0a 09 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 31 37 31 61 32 31 22 3e 0d 0a 09 09 3c	<!DOCTYPE html><html class=" responsive" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1"><meta name="theme-color" content="#171a21"><	success or wait	1	36F709	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\8HXJSKQQ\76561199609719039[1].htm	1024	1024	79 2e 61 6b 61 6d 61 69 2e 73 74 65 61 6d 73 74 61 74 69 63 2e 63 6f 6d 2f 70 75 62 6c 69 63 2f 63 73 73 2f 73 6b 69 6e 5f 31 2f 6d 6f 64 61 6c 43 6f 6e 74 65 6e 74 2e 63 73 73 3f 76 3d 2e 54 50 35 73 36 54 7a 58 36 4c 4c 68 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 6d 6d 75 6e 69 74 79 2e 61 6b 61 6d 61 69 2e 73 74 65 61 6d 73 74 61 74 69 63 2e 63 6f 6d 2f 70 75 62 6c 69 63 2f 63 73 73 2f 73 6b 69 6e 5f 31 2f 70 72 6f 66 69 6c 65 76 32 2e 63 73 73 3f 76 3d 4d 5f 71 4c 34 67 4f 32 73 4b 49 49 26 61 6d 70 3b 6c 3d 65 6e 67 6c 69 73 68 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f	y.akamai.steamstatic.com/public/css/skin_1/modalContent.css?v=.TP5s6TzX6LLh" rel="stylesheet" type="text/css" ><link href="https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=english" rel="stylesheet" type="text/	success or wait	32	36F79E	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\89737b57-777d-400d-bb7f-77b7e024920e[1].txt	0	1018	51 7a 38 53 45 52 5a 62 46 51 67 54 57 7a 49 56 45 68 45 55 51 6a 30 53 45 79 41 59 46 52 49 54 57 68 73 4e 45 68 46 69 5a 47 6c 52 43 52 59 56 50 52 49 54 49 42 67 56 45 68 4e 45 47 77 30 53 45 56 78 6b 65 56 31 53 56 56 56 72 62 6e 52 76 56 31 4a 65 56 47 68 6c 64 46 70 42 62 31 56 51 62 6d 31 68 53 6c 4a 41 45 30 52 5a 51 56 4d 54 47 44 4d 58 45 68 4d 67 47 42 55 51 52 52 59 44 46 77 4d 66 43 68 67 56 45 68 45 55 47 52 56 43 58 53 49 43 46 52 42 53 58 45 74 59 58 31 59 75 58 55 31 58 45 7a 34 5a 46 78 49 54 66 52 51 2f 45 68 45 55 47 55 77 34 45 79 41 59 46 52 49 52 46 6c 63 56 43 42 4d 69 57 6d 6c 75 55 67 77 62 47 7a 67 54 49 42 67 56 45 68 45 57 53 52 55 49 45 79 4a 6b 61 58 35 65 56 31 68 62 62 6d 39 48 56 31 70 56 58 56 46 6c 61 33 46 62 63 6c 64	Qz8SERZbFQgTWzIVEhEUQj0SEyAYFRITWhsNEhFiZGIRCRYVPRITIBgVEhNEGw0SEVxkeV1SVVVrbnRvV1JeVGhldFpBb1VQbm1hSlJAE0RZQVMTGDMXEhMgGBUQRRYDFwMfChgVEhEUGRVCXSICFRBSXEtYX1YuXU1XEz4ZFxITfRQ/EhEUGUw4EyAYFRIRFlcVCBMiWmluUgwbGzgTIBgVEhEWSRUIEyJkaX5eV1hbbm9HV1pVXVFla3Fbcld
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\BLNS00AZ\89737b57-777d-400d-bb7f-77b7e024920e[1].txt	1018	1024	77 59 4d 78 63 53 45 79 42 44 50 78 49 52 46 42 6b 58 45 68 46 75 47 67 38 53 45 31 5a 6c 61 31 45 42 4d 42 6f 5a 4f 42 45 55 47 52 63 53 45 79 4a 49 46 77 67 52 46 6d 56 72 66 6c 78 6a 57 56 6c 75 62 58 46 4a 58 6c 45 54 55 45 70 63 52 46 42 58 51 42 64 77 51 57 39 50 52 6c 64 44 61 47 56 69 51 56 5a 79 47 48 46 54 52 56 55 62 47 7a 7a 67 54 49 42 67 56 45 68 45 57 54 52 55 49 45 7a 45 55 50 78 49 52 46 42 6b 58 45 68 46 77 56 68 63 52 5a 63 52 31 74 51 4c 6c 31 4e 56 78 4d 2b 47 52 63 53 45 33 30 55 50 78 49 52 46 42 6c 4d 4f 42 4d 67 47 42 55 53 45 52 5a 58 46 51 67 54 49 6c 70 70 62 6c 49 46 44 42 55 65 4f 53 41 59 46 52 49 52 46 42 74 48 45 41 6b 67 6d 6c 75 66 56 74 61 56 6c 35 76 58 47 35 63 52 46 42 59 58 56 35 75 62 31 56 4c 55 45 41 52 63	wYMxcSEyBDPxIRFBkXEhFuGg8SE1Zla1EBMBoZOBEUGRcSEyJIFwgRFmVrflxjWVlubXFJXlETUEpcRFBXQBdwQW9PRldDaGViQVZyGHFTRVUbGzgTIBgVEhEWTRUIEzEUPxIRFBkXEhFwVhcIERZcR1tQLI1NVxM+GRcSE30UPxIRFBlMOBMgGBUSERZXFQgTIlppblIFDBUeOSAYFRIRFBtHEAkgGmlufVtaVl5vXG5cRFBYXV5ub1VLUEARc

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66860	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	0	20480	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	0	106496	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	0	40960	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	44455	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies	0	20480	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	0	196608	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	0	51200	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cookies.sqlite	0	98304	success or wait	1	373D9D	NtReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\key4.db	0	294912	success or wait	1	373D9D	NtReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cert9.db	0	229376	success or wait	1	373D9D	NtReadFile

Disassembly

No disassembly