ID: 620776
Sample Name: OqkraVUzxi
Cookbook: default.jbs
Time: 08:10:40
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

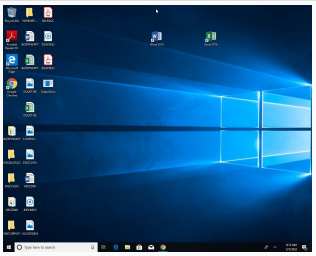
Windows Analysis Report

OqkraVUzxi

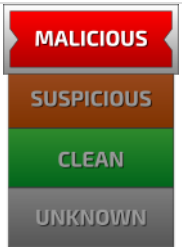
Overview

General Information

Sample Name:	OqkraVUzxi (renamed file extension from none to exe)
Analysis ID:	620776
MD5:	0f6c975dd9dc51…
SHA1:	ec4b675e8eb45d..
SHA256:	b7c3b077777303..
Tags:	32 exe trojan
Infos:	



Detection



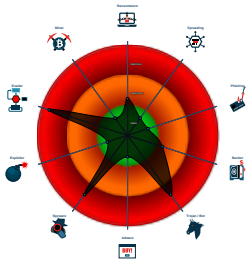
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- OqkraVUzxi.exe (PID: 5864 cmdline: "C:\Users\user\Desktop\OqkraVUzxi.exe" MD5: 0F6C975DD9DC51BC14522C8F55864724)
  - OqkraVUzxi.exe (PID: 1540 cmdline: C:\Users\user\Desktop\OqkraVUzxi.exe MD5: 0F6C975DD9DC51BC14522C8F55864724)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "home@hardroot.biz",
  "Password": "bigboy247",
  "Host": "mail.hardroot.biz"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.420279361.0000000002EF1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.420374833.0000000002F73000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000000.414987619.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.414987619.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.633632378.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.OqkraVUzxi.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.OqkraVUzxi.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.OqkraVUzxi.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b42:$s10: logins • 0x325a9:$s11: credential • 0x2eba7:$g1: get_Clipboard • 0x2ebb5:$g2: get_Keyboard • 0x2ebc2:$g3: get_Password • 0x2fe9f:$g4: get_CtrlKeyDown • 0x2feaf:$g5: get_ShiftKeyDown • 0x2fec0:$g6: get_AltKeyDown
3.0.OqkraVUzxi.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.OqkraVUzxi.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 31 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

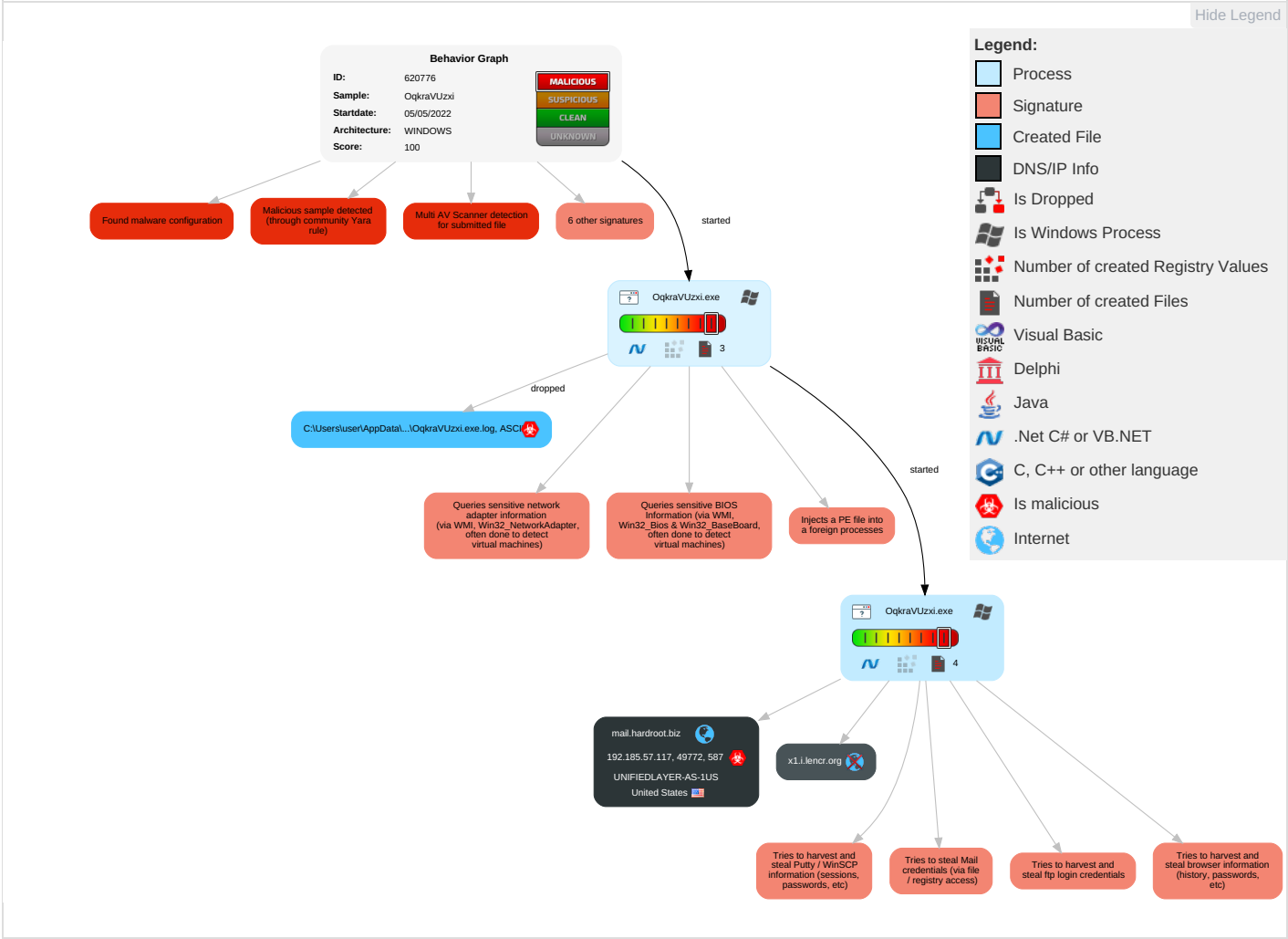
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
OqkraVUzxi.exe	43%	Virustotal		Browse
OqkraVUzxi.exe	17%	Metadefender		Browse
OqkraVUzxi.exe	45%	ReversingLabs	Win32.Trojan.AgentTesla	
OqkraVUzxi.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.OqkraVUzxi.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.OqkraVUzxi.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.OqkraVUzxi.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.OqkraVUzxi.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.OqkraVUzxi.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.OqkraVUzxi.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
x1.i.lencr.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://scB5z04k6dpJvRUp.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://x1.i.lencr.org/~	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.sandoll.co.krlX	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp//3	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.comei	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krn-ustp	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/vnoV	0%	Avira URL Cloud	safe	
http://www.carterandcone.comp	0%	URL Reputation	safe	
http://www.carterandcone.comr7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://https://scB5z04k6dpJvRUp.compx	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.fontbureau.coma0	0%	Avira URL Cloud	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/q	0%	URL Reputation	safe	
http://www.fontbureau.coma9	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krim	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/c	0%	URL Reputation	safe	
http://www.goodfont.co.krde	0%	Avira URL Cloud	safe	
http://www.fontbureau.comnc.9	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/3L	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com.	0%	URL Reputation	safe	
http://www.founder.com.cn/cnK	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnNC	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://fontfabrik.comH	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comdsed/3	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0h	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.goodfont.co.krom_X;7	0%	Avira URL Cloud	safe	
http://www.urwpp.deQF:7	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnthi	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0p	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/_	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnup	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://mail.hardroot.biz	0%	Avira URL Cloud	safe	
http://hdgJLE.com	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://https://scB5z04k6dpJvRUp.c	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/q	0%	URL Reputation	safe	
http://www.fontbureau.comTTFm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//3	0%	Avira URL Cloud	safe	
http://www.tiro.	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comtalik	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals9	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.carterandcone.comva#I	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.hardroot.biz	192.185.57.117	true	true		unknown
x1.i.lencr.org	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	OqkraVUzxi.exe, 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://scB5z04k6dpJvRUp.com	OqkraVUzxi.exe, 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessed	OqkraVUzxi.exe, 00000000.00000003.388738517.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388581203.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388888718.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388937002.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/~	OqkraVUzxi.exe, 00000003.00000003.455556956.000000000670A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	OqkraVUzxi.exe, 00000000.00000003.372310291.0000000005E62000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	OqkraVUzxi.exe, 00000000.00000003.383607711.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383104459.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383153536.0000000005E7C000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383322975.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krlX	OqkraVUzxi.exe, 00000000.00000003.377025473.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.377589487.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.377232453.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp//3	OqkraVUzxi.exe, 00000000.00000003.383607711.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385018673.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/	OqkraVUzxi.exe, 00000000.00000003.387790320.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.387582106.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ascendercorp.com/typedesigners.html	OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comei	OqkraVUzxi.exe, 00000000.00000003.380467379.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381012770.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380736011.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381273073.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381393520.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381153365.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380350704.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380911402.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380577993.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krn-ustp	OqkraVUzxi.exe, 00000000.00000003.377025473.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.377232453.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	OqkraVUzxi.exe, 00000000.00000003.379992495.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlk	OqkraVUzxi.exe, 00000000.00000003.388738517.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388581203.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388888718.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coma	OqkraVUzxi.exe, 00000000.00000003.380467379.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380736011.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380350704.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380911402.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380577993.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/	OqkraVUzxi.exe, 00000000.00000003.391148231.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	OqkraVUzxi.exe, 00000003.00000002.639324449.0000000003084000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.638181390.00000000010AC000.00000004.00000020.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.641996861.0000000006620000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	OqkraVUzxi.exe, 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/vnoV	OqkraVUzxi.exe, 00000000.00000003.383607711.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385018673.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383322975.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comp	OqkraVUzxi.exe, 00000000.00000003.380736011.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380577993.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comr7	OqkraVUzxi.exe, 00000000.00000003.380467379.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380736011.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380350704.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380577993.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/H	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385018673.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://scB5z04k6dpJvRUp.compx	OqkraVUzxi.exe, 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	OqkraVUzxi.exe, 00000000.00000003.378548225.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378673688.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/z	OqkraVUzxi.exe, 00000000.00000003.383607711.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383322975.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma0	OqkraVUzxi.exe, 00000000.00000003.388738517.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388581203.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388888718.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comituF	OqkraVUzxi.exe, 00000000.00000003.389202809.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388738517.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388581203.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388489651.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388888718.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389110922.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388241833.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388937002.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388286121.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comoitu	OqkraVUzxi.exe, 00000000.00000003.395700507.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.418879619.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395036184.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395590015.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395790338.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426428177.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395393640.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395287937.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/q	OqkraVUzxi.exe, 00000000.00000003.383607711.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.coma9	OqkraVUzxi.exe, 00000000.00000003.395700507.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.418879619.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395036184.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395590015.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395790338.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426428177.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395393640.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395287937.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krim	OqkraVUzxi.exe, 00000000.00000003.377589487.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.377746835.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.377232453.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/h	OqkraVUzxi.exe, 00000000.00000003.383104459.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383153536.0000000005E7C000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383322975.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.jiyu-kobo.co.jp/c	OqkraVUzxi.exe, 00000000.00000003.385408266.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385694446.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385471481.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385212858.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385625509.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385018673.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krde	OqkraVUzxi.exe, 00000000.00000003.377232453.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comnc.9	OqkraVUzxi.exe, 00000000.00000003.388206961.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/3L	OqkraVUzxi.exe, 00000000.00000003.378548225.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com.	OqkraVUzxi.exe, 00000000.00000003.372310291.0000000005E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnK	OqkraVUzxi.exe, 00000000.00000003.378335003.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378548225.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.379059574.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378673688.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378957354.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378844078.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnNC	OqkraVUzxi.exe, 00000000.00000003.378289568.0000000005E84000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378143620.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.comH	OqkraVUzxi.exe, 00000000.00000003.374305353.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374087270.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	OqkraVUzxi.exe, 00000000.00000003.380577993.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdsed/3	OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr.org/0	OqkraVUzxi.exe, 00000003.00000002.639324449.0000000003084000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.638181390.00000000010AC000.00000004.00000020.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.641996861.0000000006620000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	OqkraVUzxi.exe, 00000000.00000003.391596735.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0h	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krom_X;7	OqkraVUzxi.exe, 00000000.00000003.377232453.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deQF:7	OqkraVUzxi.exe, 00000000.00000003.386696435.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.386812380.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnthi	OqkraVUzxi.exe, 00000000.00000003.379992495.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.c.lencr.org/0	OqkraVUzxi.exe, 00000003.00000002.639324449.0000000003084000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.638181390.00000000010AC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	OqkraVUzxi.exe, 00000003.00000002.639324449.0000000003084000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.638181390.00000000010AC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0p	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	OqkraVUzxi.exe, 00000003.00000002.638783089.000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.o.lencr.org0	OqkraVUzxi.exe, 00000003.00000002.639324449.0000000003084000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.638181390.00000000010AC000.00000004.00000020.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000003.00000002.641996861.0000000006620000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/_	OqkraVUzxi.exe, 00000000.00000003.391148231.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnup	OqkraVUzxi.exe, 00000000.00000003.378335003.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.379340282.0000000005E84000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.379175934.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378548225.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.379059574.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378673688.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378957354.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378844078.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	OqkraVUzxi.exe, 00000000.00000003.377025473.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.377232453.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.comh	OqkraVUzxi.exe, 00000000.00000003.375031563.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374345110.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374434299.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.375209174.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374784818.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374872343.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.375123442.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374609367.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374556253.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374705130.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.374836486.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.375280428.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.urwpp.de	OqkraVUzxi.exe, 00000000.00000003.386696435.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.387174953.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.386812380.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.386998923.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.387582106.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

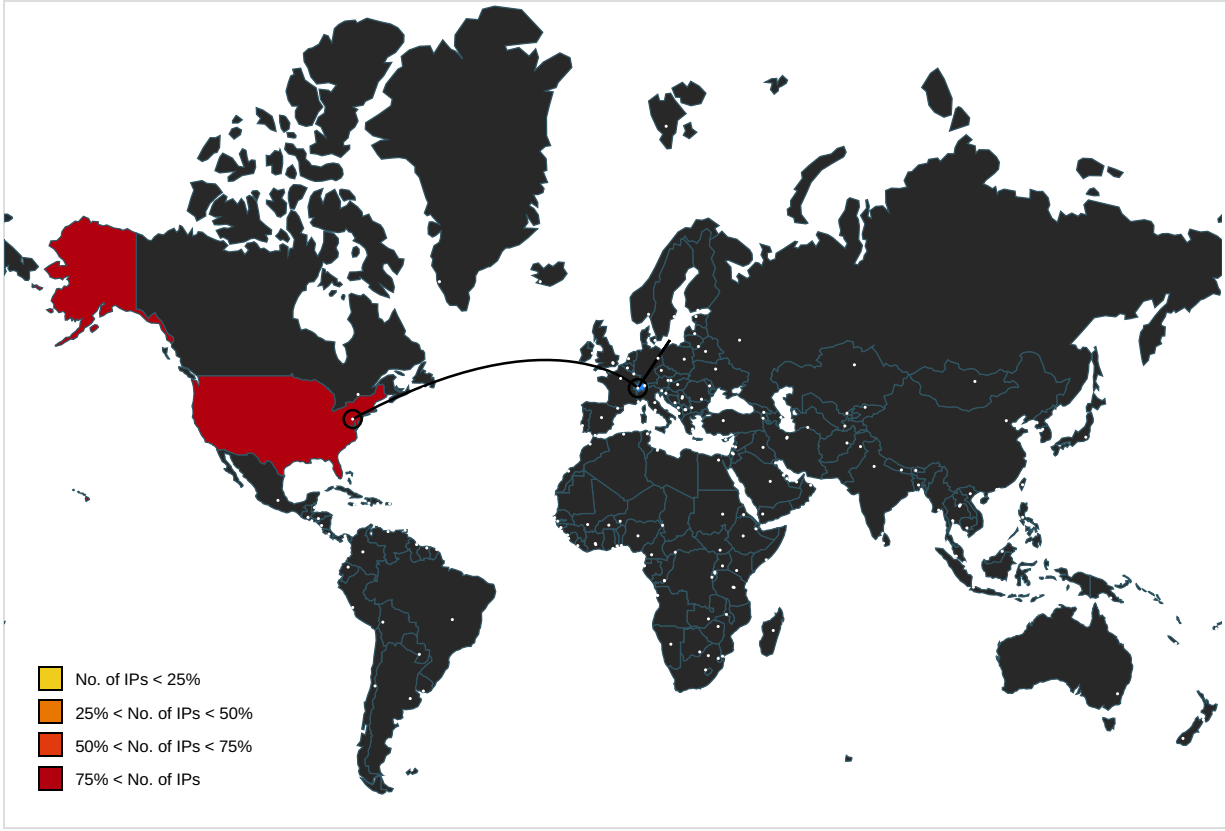
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385018673.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.hardroot.biz	OqkraVUzxi.exe, 00000003.00000002.639324449.0000000003084000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://hdgJLE.com	OqkraVUzxi.exe, 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	OqkraVUzxi.exe, 00000000.00000003.379592669.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.379430046.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	OqkraVUzxi.exe, 00000000.00000003.390552809.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390394721.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389202809.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.395036184.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390148599.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388738517.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388581203.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389462715.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388489651.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388888718.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390222105.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.387790320.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389397395.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390596085.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389110922.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389045175.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388241833.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.i.lencr.org/	OqkraVUzxi.exe, 00000003.00000002.638111079.0000000001034000.00000004.00000020.00020000.00000000.sdmp, 2D85F72862B55C4EADD9E66E06947F3D0.3.dr	false	• URL Reputation: safe	unknown
http://https://scB5z04k6dpJvRUp.c	OqkraVUzxi.exe, 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	OqkraVUzxi.exe, 00000000.00000003.389202809.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390148599.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389462715.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390222105.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389397395.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389110922.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389045175.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.c	OqkraVUzxi.exe, 00000000.00000003.377589487.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmly	OqkraVUzxi.exe, 00000000.00000003.389202809.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389110922.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389045175.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/q	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comTTFm	OqkraVUzxi.exe, 00000000.00000003.390148599.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389462715.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390222105.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389397395.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/oi	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	OqkraVUzxi.exe, 00000000.00000003.384490211.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383974650.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384849907.0000000005E81000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383820214.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384973698.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384929440.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385018673.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	OqkraVUzxi.exe, 00000000.00000003.388241833.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388286121.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388206961.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/z	OqkraVUzxi.exe, 00000000.00000003.384250639.0000000005E7D000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.384181623.0000000005E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//3	OqkraVUzxi.exe, 00000000.00000003.383104459.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383153536.0000000005E7C000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383322975.0000000005E83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.	OqkraVUzxi.exe, 00000000.00000003.379059574.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378957354.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	OqkraVUzxi.exe, 00000000.00000003.378335003.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378548225.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378289568.0000000005E84000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.378143620.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtalik	OqkraVUzxi.exe, 00000000.00000003.387582106.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comals9	OqkraVUzxi.exe, 00000000.00000003.390148599.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389462715.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390222105.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.390343893.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	OqkraVUzxi.exe, 00000000.00000003.389462715.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389716173.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389901729.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389397395.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comva#l	OqkraVUzxi.exe, 00000000.00000003.380467379.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381012770.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380736011.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381273073.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381393520.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.381153365.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380350704.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380911402.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.380577993.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	OqkraVUzxi.exe, 00000000.00000003.388738517.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388581203.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388489651.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388888718.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388527227.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.389110922.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388241833.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388937002.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.388286121.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	OqkraVUzxi.exe, 00000000.00000003.385147979.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000003.383322975.0000000005E83000.00000004.00000800.00020000.00000000.sdmp, OqkraVUzxi.exe, 00000000.00000002.426632208.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.57.117	mail.hardroot.biz	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620776
Start date and time: 05/05/202208:10:40	2022-05-05 08:10:40 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OqkraVUzxi (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/5@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.5%) • Quality average: 20.5% • Quality standard deviation: 20.5%

HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.50.97.168, 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, e8652.dscx.akamaiedge.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, crl.root-x1.letsencrypt.org.edgekey.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:12:10	API Interceptor	665x Sleep call for process: OqkraVUzxi.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\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Users\user\Desktop\OqkraVUzxi.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false

SSDEEP:	24:ooVdTH2NMU+l3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...1506041104 38Z..3506041104 38Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....I.....*.A..v.....5/(.l....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".].y...p..N..:..'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ')..au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\OqkraVUzxi.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....l_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:'..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....,_.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri...]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Users\user\Desktop\OqkraVUzxi.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.7842198674325394
Encrypted:	false
SSDEEP:	3:kkFkl3CBzHE/XfllXlE/zMcl/XNNX8RolJuRdyo1dlUKlGXJlDdt:kKNFHE/81lVNMa8Rdy+UKcXP
MD5:	80417EE2B67F45B91BBE7D013BAEDB34
SHA1:	C43FA9F934D300737204D2721F566FE97AB3DD4F
SHA-256:	99A7BB29FAD860846C4C1BAB62CA2E34FC2902936EE1AB75E33ADBD804ED715C
SHA-512:	CA3C13E0EFBC2FDD9A6A1A50B00074756E474E05CAE142869CFA47E275AF0A5E7EEFA4C0A16C4D412734BF319B11AD0F1DD374E8BF78DC1EBDD759F796502610
Malicious:	false
Reputation:	low
Preview:	p..... .....'..`..(..... .....~...d.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\OqkraVUzxi.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.128394965284737
Encrypted:	false
SSDEEP:	6:kKNaCoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:kMkPlE99SNxAhUesE1
MD5:	3BFB95F2A18BF200B34519DA4CDE58AE
SHA1:	B6AB4602C1352D556BC2A4FCFE3432A8D54E480A

SHA-256:	E60E66B5BA3D1409A273A248422C2AF855146EA74458FD26AC34BA72F9A3BD40
SHA-512:	A9877966E7900703C25E13F9410D7AA3B31FC42E6CD0ABB2CE38C116C02C7AE9A6BD30BC18C92D5081AC778034D57A328DA018A57000221D1AF78119AC18E2 2
Malicious:	false
Reputation:	low
Preview:	p..... .....F.0.`..(..... .....3k/"[.....(.....(...h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

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

Process:	C:\Users\user\Desktop\OqkraVUzxi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC 2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.820984380864883
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	OqkraVUzxi.exe
File size:	616448
MD5:	0f6c975dd9dc51bc14522c8f55864724
SHA1:	ec4b675e8eb45d4caf359e0cf897b855db29dff7
SHA256:	b7c3b077777303227947d62064fea23a1473f57c07575476e97c92a811b37c46
SHA512:	867d95e8525e045575f2f9fe7f165f6840e5df9ada790ca1e79bb28581a6088a77e042ddf63a72659d24384dc72f05990f8b56eaa3511b86c938125596cec6d1
SSDEEP:	12288:b2L2Ij3hfA94QJVU+s5vgXesxzh3ptsXBGP6Oznh9a7g83bUe:b2p3iR1+g9Fp1Rzh9QgE/
TLSH:	32D40200B066C77ADB3457F1662A429013F63ABF7051F1687CD497CBB666BB81E00EA7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..P.....o... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x496fa2

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xAB1BAE9C [Sun Dec 19 21:41:48 2060 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x96f50	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0x1244	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x96f34	0x1c	.text
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	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x94fa8	0x95000	False	0.887400377517	data	7.83234323723	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x1244	0x1400	False	0.359765625	data	4.83055616258	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x98090	0x388	data		
RT_MANIFEST	0x98428	0xe15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright HP Inc. 2020
Assembly Version	1.0.0.0
InternalName	NonGenericToGenericEnumera.exe
FileVersion	1.0.0.0
CompanyName	HP Inc.
LegalTrademarks	
Comments	
ProductName	Snake Game
ProductVersion	1.0.0.0
FileDescription	Snake Game
OriginalFilename	NonGenericToGenericEnumera.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 08:12:29.244918108 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:29.381449938 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:29.381660938 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:29.525722980 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:29.526093006 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:29.663486004 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:29.663938046 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:29.804541111 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:29.845177889 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:29.875799894 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:30.036896944 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:30.036952019 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:30.036969900 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:30.037132025 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:30.182666063 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:30.320333004 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:30.454622030 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:33.895143986 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.032061100 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.033435106 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.170738935 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.171715975 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.311009884 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.311994076 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.449878931 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.463721991 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.614736080 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.616029978 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.752613068 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.767893076 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.768048048 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.768780947 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.768857002 CEST	49772	587	192.168.2.6	192.185.57.117
May 5, 2022 08:12:34.904400110 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.904426098 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.905081987 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.905097008 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.911026001 CEST	587	49772	192.185.57.117	192.168.2.6
May 5, 2022 08:12:34.954982996 CEST	49772	587	192.168.2.6	192.185.57.117

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 08:12:28.920574903 CEST	51971	53	192.168.2.6	8.8.8.8
May 5, 2022 08:12:29.214392900 CEST	53	51971	8.8.8.8	192.168.2.6
May 5, 2022 08:12:30.862104893 CEST	56591	53	192.168.2.6	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 08:12:28.920574903 CEST	192.168.2.6	8.8.8.8	0xe9f5	Standard query (0)	mail.hardroot.biz	A (IP address)	IN (0x0001)
May 5, 2022 08:12:30.862104893 CEST	192.168.2.6	8.8.8.8	0xc046	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 08:12:29.214392900 CEST	8.8.8.8	192.168.2.6	0xe9f5	No error (0)	mail.hardroot.biz		192.185.57.117	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 08:12:30.883352995 CEST	8.8.8.8	192.168.2.6	0xc046	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 5, 2022 08:12:29.525722980 CEST	587	49772	192.185.57.117	192.168.2.6	220-paseo.websitewelcome.com ESMTP Exim 4.94.2 #2 Thu, 05 May 2022 01:12:29 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 5, 2022 08:12:29.526093006 CEST	49772	587	192.168.2.6	192.185.57.117	EHLO 414408
May 5, 2022 08:12:29.663486004 CEST	587	49772	192.185.57.117	192.168.2.6	250-paseo.websitewelcome.com Hello 414408 [102.129.143.40] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 5, 2022 08:12:29.663938046 CEST	49772	587	192.168.2.6	192.185.57.117	STARTTLS
May 5, 2022 08:12:29.804541111 CEST	587	49772	192.185.57.117	192.168.2.6	220 TLS go ahead

Statistics

Behavior

OqkraVUzxi.exe
OqkraVUzxi.exe

Click to jump to process

System Behavior

Analysis Process: OqkraVUzxi.exe PID: 5864, Parent PID: 1776

General

Target ID:	0
Start time:	08:11:52
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\OqkraVUzxi.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OqkraVUzxi.exe"
Imagebase:	0xb60000
File size:	616448 bytes
MD5 hash:	0F6C975DD9DC51BC14522C8F55864724
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.420279361.0000000002EF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.420374833.0000000002F73000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.422759188.0000000003FDC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.422759188.0000000003FDC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6DAFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OqkraVUzxi.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE0C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OqkraVUzxi.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DE0C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DADCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DADCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C941B4F	ReadFile

Analysis Process: OqkraVUzxi.exe PID: **1540**, Parent PID: **5864**

General

Target ID:	3
Start time:	08:12:13
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\OqkraVUzxi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OqkraVUzxi.exe
Imagebase:	0x860000
File size:	616448 bytes
MD5 hash:	0F6C975DD9DC51BC14522C8F55864724
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.414987619.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.414987619.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.633632378.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.633632378.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.417769511.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.417769511.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.416951920.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.416951920.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.638783089.0000000002D31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.416164408.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.416164408.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6DAFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAFCF06	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DADCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C941B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C941B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C941B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C941B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\98bd75d2-ce84-459a-aada-2da99aef3201	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C941B4F	ReadFile

Disassembly

No disassembly