ID: 830842
Sample Name:
CsTapHIkAO.exe
Cookbook: default.jbs
Time: 18:26:16
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

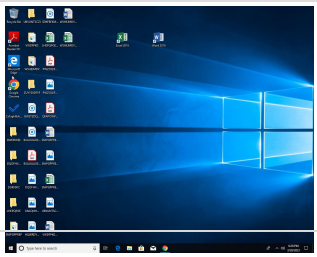
Windows Analysis Report

CsTapHIkAO.exe

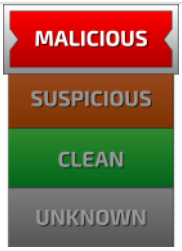
Overview

General Information

Sample Name:	CsTapHIkAO.exe
Original Sample Name:	fc7ad54f4f2e78..
Analysis ID:	830842
MD5:	fc7ad54f4f2e78..
SHA1:	890ab6267da7...
SHA256:	745334ebcf459..
Tags:	AgentTesla exe
Infos:	



Detection



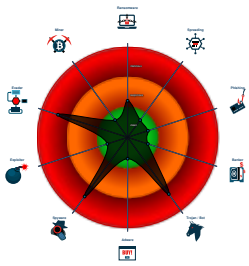
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Machine Learning detection for sam…
- May check the online IP address of…
- Injects a PE file into a foreign proce…
- Machine Learning detection for drop…
- Hides that the sample has been dow…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- CsTapHIkAO.exe (PID: 2416 cmdline: C:\Users\user\Desktop\CsTapHIkAO.exe MD5: FC7AD54F4F2E785AD748D952945CC888)
  - CsTapHIkAO.exe (PID: 4496 cmdline: C:\Users\user\Desktop\CsTapHIkAO.exe MD5: FC7AD54F4F2E785AD748D952945CC888)
- BKEDEaL.exe (PID: 1244 cmdline: "C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe" MD5: FC7AD54F4F2E785AD748D952945CC888)
  - BKEDEaL.exe (PID: 5316 cmdline: C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe MD5: FC7AD54F4F2E785AD748D952945CC888)
- BKEDEaL.exe (PID: 3408 cmdline: "C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe" MD5: FC7AD54F4F2E785AD748D952945CC888)
  - BKEDEaL.exe (PID: 5116 cmdline: C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe MD5: FC7AD54F4F2E785AD748D952945CC888)
  - BKEDEaL.exe (PID: 5576 cmdline: C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe MD5: FC7AD54F4F2E785AD748D952945CC888)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.spjsv.ro",
  "Username": "psihiatrie@spjsv.ro",
  "Password": "Qpgi1i[5KoaZ"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.527846084.000000000311C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.527846084.000000000311C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000C.00000002.529011306.0000000002DCC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.527812814.0000000002D1C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CsTapHlkAO.exe PID: 4496	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

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 browser information (history, passwords, etc)

Remote Access Functionality

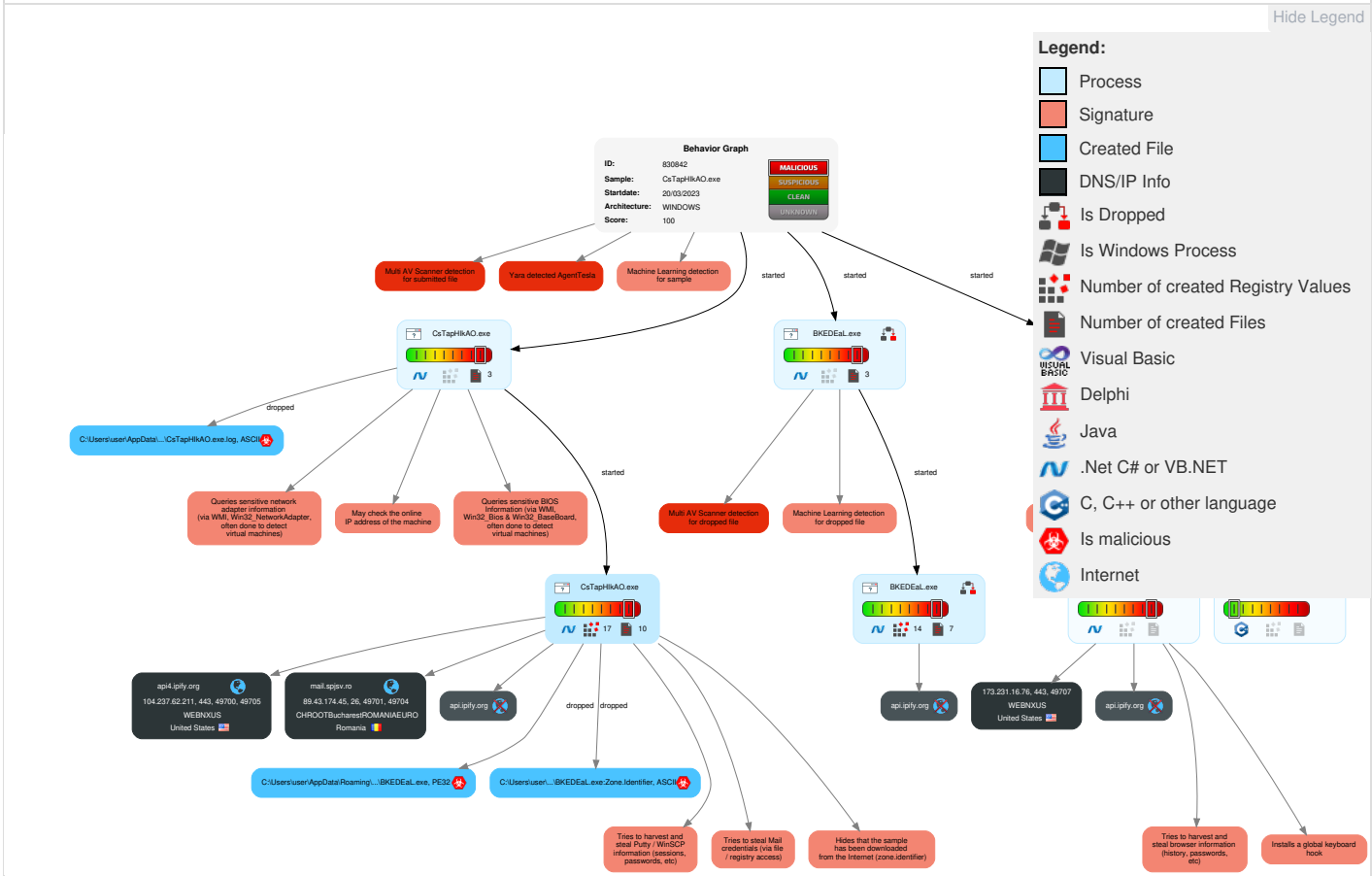
Yara detected AgentTesla

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	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	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 Software Packing	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Modify Registry	LSA Secrets	1 Process Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	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 1 1 Process Injection	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 Hidden Files and Directories	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

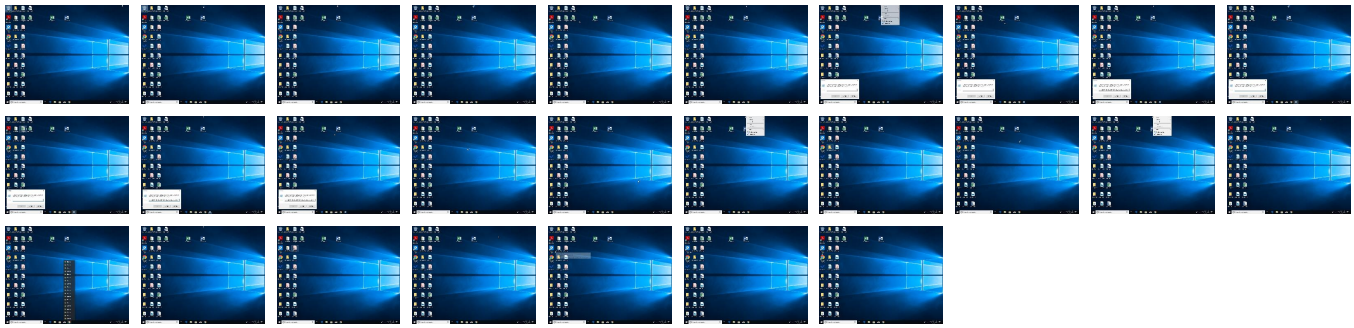
Behavior Graph



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
CsTapHlkAO.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
CsTapHlkAO.exe	41%	Virustotal		Browse
CsTapHlkAO.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe	41%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mail.spjsv.ro	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/ocsp0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/DPCyPoliticas0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://ocsp.ncdc.gov.sa0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.uce.gub.uy/acrn/acrn.crl0	0%	URL Reputation	safe	
http://mail.spjsv.ro	0%	Avira URL Cloud	safe	
http://mail.spjsv.ro	3%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api4.ipify.org	104.237.62.211	true	false		high
mail.spjsv.ro	89.43.174.45	true	false	• 3%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certplus.com/CRL/class3.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-me.lv/repository0	CsTapHIkAO.exe, 00000001.00000003.311379654.0000000006B38000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	CsTapHIkAO.exe, 00000001.00000003.312211064.0000000007B6A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007BA1000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.553888439.0000000007AEA000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.320377682.0000000007AEA000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	CsTapHIkAO.exe, 00000001.00000003.312211064.0000000007B6A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	CsTapHIkAO.exe, 00000001.00000003.312268892.0000000007B64000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	CsTapHIkAO.exe, 00000001.00000003.312268892.0000000007B64000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	CsTapHIkAO.exe, 00000001.00000003.311379654.0000000006B38000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	CsTapHIkAO.exe, 00000001.00000003.310786837.0000000006BC4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	CsTapHIkAO.exe, 00000001.00000003.312268892.0000000007B64000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.globaltrust.info0=	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	CsTapHIkAO.exe, 00000001.00000003.312211064.0000000007B6A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CsTapHIkAO.exe, 00000001.00000002.527846084.00000000030D1000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.0000000002D8C000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002CD1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	CsTapHIkAO.exe, 00000001.00000003.311379654.0000000006B38000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.root-x1.letsencrypt.org0	CsTapHIkAO.exe, 00000001.00000002.527846084.0000000003174000.00000004.00000800.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.319867307.0000000007B60000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.549357958.0000000006AF9000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.553888439.0000000007B62000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.318417707.000000006B20000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.527846084.0000000034F000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000003.374393467.0000000001015000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.523570604.0000000001008000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.0000000002E19000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.0000000002E03000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.523570604.0000000000FCC000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.549038631.0000000006578000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002D53000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002D69000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.549149990.0000000006870000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.523285694.0000000001022000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000003.397265850.00000000010D8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.com0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ssc.lt/cps03	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	CsTapHIkAO.exe, 00000001.00000003.312211064.0000000007B6A000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.312330521.0000000007B71000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.312211064.0000000007B6A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

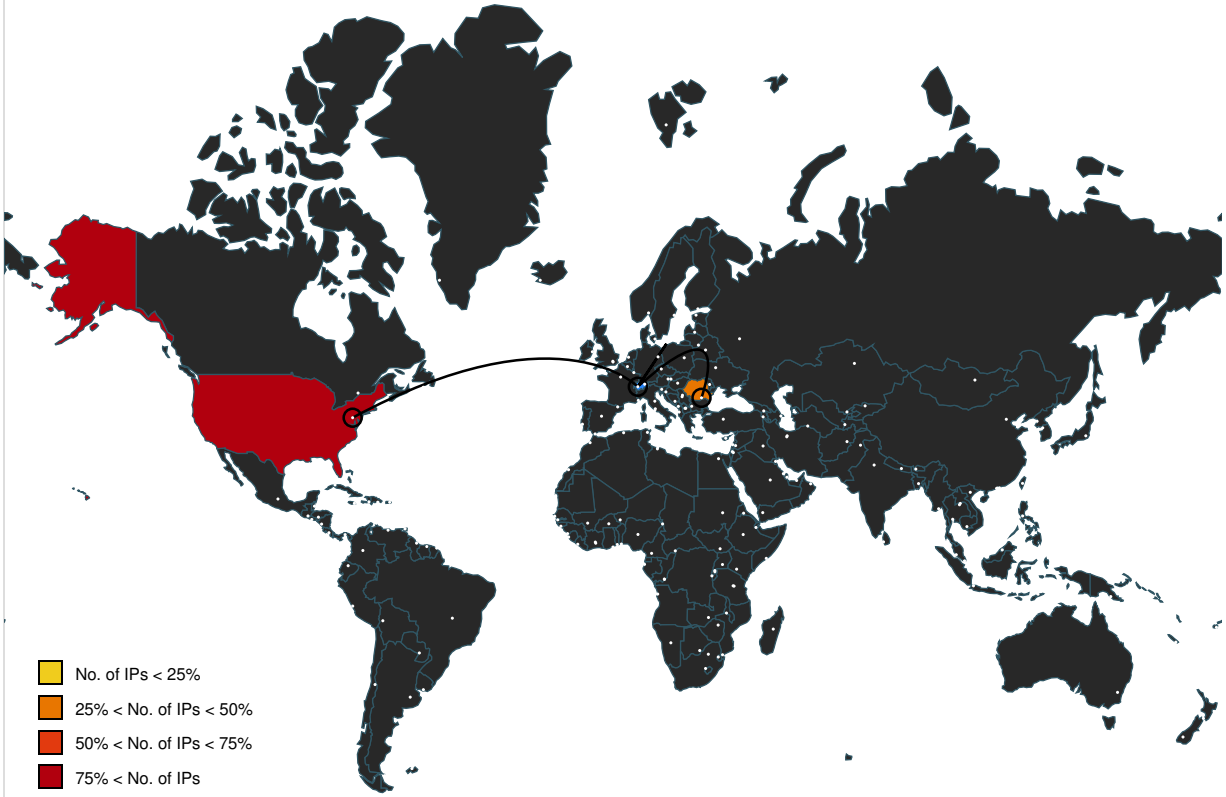
Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.spjsv.ro	CsTapHIkAO.exe, 00000001.00000002.527846084.0000000003174000.00000004.00000800.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.527846084.000000000311C000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.0000000002DE4000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.0000000002E19000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002D34000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002D69000.00000004.00000800.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	CsTapHIkAO.exe, 00000001.00000002.527846084.0000000003160000.00000004.00000800.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.320377682.0000000007AEA000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.550487471.0000000006B35000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.527846084.0000000003174000.00000004.00000800.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.319867307.0000000007B60000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.553888439.0000000007B62000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000002.527846084.000000000314F000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.549038631.00000000655F000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.523570604.0000000001008000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.00000000002E19000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.529011306.0000000002E03000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.523570604.00000000000FCC000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000C.00000002.549038631.0000000006578000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000003.397265850.00000000010BA000.00000004.00000020.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002D53000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.527812814.0000000002D69000.00000004.00000800.00020000.00000000.sdmp, BKEDEaL.exe, 0000000F.00000002.523285694.0000000001022000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007B5F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ca.mtin.es/mtin/DPCyPoliticas0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	CsTapHIkAO.exe, 00000001.00000002.553832121.0000000007AD2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://crl.anf.es/AC/ANFServerCA.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/pc-root2.pdf0	CsTapHIkAO.exe, 00000001.00000003.310786837.0000000006BC4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ac.economia.gob.mx/last.crl0G	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.catcert.net/verarrel	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca0f	CsTapHIkAO.exe, 00000001.00000003.312268892.0000000007B64000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	CsTapHIkAO.exe, 00000001.00000003.311686118.0000000006B2E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.accv.es00	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007BA1000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.319867307.0000000007B9F000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.312330521.0000000007B9F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.netlock.net/docs	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007B69000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	CsTapHIkAO.exe, 00000001.00000003.311064572.0000000006B42000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.312211064.0000000007B6A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.ncdc.gov.sa0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignCA.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007ADC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	CsTapHIkAO.exe, 00000001.00000003.312665362.0000000007B5B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007BA1000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp, CsTapHIkAO.exe, 00000001.00000003.311516680.0000000007B92000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	CsTapHIkAO.exe, 00000001.00000003.312268892.0000000007B64000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://repository.luxtrust.lu0	CsTapHIkAO.exe, 00000001.00000003.311379654.0000000006B38000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.eca.hinet.net/OCSP/ocspG2sha20	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.firmaprofesional.com/cps0	CsTapHIkAO.exe, 00000001.00000003.312268892.0000000007B64000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	CsTapHIkAO.exe, 00000000.00000002.295374704.0000000006BB2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.uce.gub.uy/acrn/acrn.crl0	CsTapHIkAO.exe, 00000001.00000003.311829916.0000000007B72000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.237.62.211	api4.ipify.org	United States		18450	WEBNXUS	false
89.43.174.45	mail.spjsv.ro	Romania		56430	CHROOTBucharestROMANIAEURO	false
173.231.16.76	unknown	United States		18450	WEBNXUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830842
Start date and time:	2023-03-20 18:26:16 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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
Sample file name:	CsTapHIkAO.exe
Original Sample Name:	fc7ad54f4f2e785ad748d952945cc888.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/9@12/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.10.249.161, 23.10.249.147, 8.238.191.126, 8.238.88.254, 8.238.189.126, 8.238.88.248, 8.238.85.126, 209.197.3.8
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile 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
18:27:19	API Interceptor	750x Sleep call for process: CsTapHIkAO.exe modified
18:27:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run BKEDEaL C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
18:27:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run BKEDEaL C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
18:27:42	API Interceptor	1099x Sleep call for process: BKEDEaL.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\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\CsTapHIkAO.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62582 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62582
Entropy (8bit):	**7.996063107774368**
Encrypted:	**true**
SSDEEP:	1536:Jk3XPi43VgGp0gB2itudTSRAn/TWTdWftu:CHa43V5p022iZ4CgA
MD5:	E71C8443AE0BC2E282C73FAEAD0A6DD3
SHA1:	0C110C1B01E68EDFACAEAE64781A37B1995FA94B
SHA-256:	95B0A5ACC5BF70D3ABDFD091D0C9F9063AA4FDE65BD34DBF16786082E1992E72
SHA-512:	B38458C7FA2825AFB72794F374827403D5946B1132E136A0CE075DFD351277CF7D957C88DC8A1E4ADC3BCAE1FA8010DAE3831E268E910D517691DE24326391A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....v.....,.....I.....BVrl .authroot.stl....oJ5..CK..8U....a..3.1.P. J.".t..2F2e.dHH.....$E.KB.2D..-SJE....^..'..y.}..,{m.....\...]4.G.....h....148...e.gr.....48:.L. ..g.....Xef.x:..t...J...6-....kW6Z>....&.....ye.U.Q&z:.vZ..._....a...]..T.E.....B.h.,...[....V.O.3..EW.x.?.Q..$.@.W..=.B.f..8a.Y.JK..g./%p..C.4CD.s..Jd.u..@.g=...a.. .h%..'.xjy7.E ..\.....A..':.4TdW?Ko3$.Hg.z.d~...../q..C.....`...A[ W(.....9...GZ.;....I&?.....F...p?... .p.....{S.L4..v.+...7.T?.....p..`..&..9.....f...0+.L.....1.2b)..vX5L'.~....2vz.,E.Ni.{#...o..w.?.#.3 ..h.v<.S%.].tD@!Le.w.q.7.8....QW.FT.....hE.....Y...../.%Q...k...*.Y.n..v.A..../...>B..5\..-Ko.....O<.b.K.{.O.b...._.7...4.;%9N..K.X>.....kg-9..r.c.g.G|.*[.-...HT...",?.q...ad. ...7RE.....!f..#../....?.-.^.K.c^...+{.g.....]<..$.=.O....ii7.wJ+S..Z..d.....>..J*...T..Q7..`.r,<$....\d:K`..T.n....N.....C..j.;.1SX..j....1...R....+....Yg....]....3..9..S..D..`.

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

Process:	C:\Users\user\Desktop\CsTapHIkAO.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1335351732898324
Encrypted:	false
SSDEEP:	6:kKLFGry/7UN+SkQlPlEGYRMY9z+4KlDA3RUecZUt:8CvkPlE99SNxAhUext
MD5:	8F9C6E370F1D7C5E4C781D6EB5CA40B6
SHA1:	F1481D2A7389EF1EA5BBABCEB9EB68E003EF0F7F
SHA-256:	8756E1D44F7190F0AC920D89A89F3A59F31E31C7AD4725C62E5806683B6B76D9
SHA-512:	E836FE0C57DF529A59CE06BB8E7797B82F587ED9C34E88FD2CC44BC81105C81BB2C5D21B8BEEABF7C05A359B7C1B088DD09BF5C4298ADB9007F1BDB755AA8 424
Malicious:	false
Reputation:	low
Preview:	p..... .....`M.\..(..... .....).K.....&.....v...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...".0.d.2.f.9.2.9.a.7.4.b.d.9.1.:.0."...

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

Process:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178 FF6
Malicious:	false

Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Desktop\CsTapHIkAO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network\Cookies

Process:	C:\Users\user\Desktop\CsTapHIkAO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	modified
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe

Process:	C:\Users\user\Desktop\CsTapHIkAO.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	752128
Entropy (8bit):	7.860252795159179
Encrypted:	false
SSDEEP:	12288:J5lmYMUnFW/NDMsa/S5MZJ+1ghNBtVyML3H1vY/ADhm1of1OWHBP/28dEQvYbow:J5lUVMsyS50vXV3Fvqx1vWHJ/28dh5
MD5:	FC7AD54F4F2E785AD748D952945CC888
SHA1:	890AB6267DA79E151B8C42E9F7F6A19D59A0EB4A
SHA-256:	745334EBCF459EC748D00EAF3BCB94045CEBDD6275ACA548255C1C922F0F9D9D
SHA-512:	63D3BD6456259FC7CC34086ED24C46D0B9B59A124D3431CC22C192A868E6157C130D79796EBF240FF23AEF66E6D312BBE778BFB3692A1B6ED6D087BF479C0BB
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31% • Antivirus: Virustotal, Detection: 41%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..d..... .....@.. ....@.....3...O..... n..T..... ....H.....text....b... ...d..... ..`.rsrc.....f.....@..@.rel oc.....x.....@..B.....g.....H.....@V...1.....".....0..R.....4...%..{....{L....%.r...p.%..|....(.....%.r...p.%..{.....X...(.....(.....+..*...0 ..&.....{.....,...{.....+....{....Z.+..*".(.....*..0..z.....}.....}.....}.....(.....(.....{.....s!...%.d}M...%r!..p}L...%.{....}P...%.{....}O.....{.....s!...%.d}M...%r)..p}L...%.{....}P...%.{.. ..}O.....{.....s!...%.d}M...%r1..p}L...%.{....}P...%.{....}O.....{.....+.....o....&.

C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\CsTapHIkAO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network\Cookies

Process:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BFI
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\Roaming\tgixmeao.ntk\Chrome\Default\Network\Cookies

Process:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BFI
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.860252795159179
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:	CsTapHlkAO.exe
File size:	752128
MD5:	fc7ad54f4f2e785ad748d952945cc888
SHA1:	890ab6267da79e151b8c42e9f7f6a19d59a0eb4a
SHA256:	745334ebcf459ec748d00eaf3bcb94045cebdd6275aca548255c1c922f0f9d9d
SHA512:	63d3bd6456259fc7cc34086ed24c46d0b9b59a124d3431cc22c192a868e6157c130d79796ebf240ff23aef66e6d312bbe778bfb3692a1b6ed6d087bf479c0b0b
SSDEEP:	12288:J5lmYMUnFW/NDMsa/S5MZJ+1ghNBtVyML3H1vY/ADhm1of1OWHBP/28dEQvYbow:J5lUVMsyS50vXV3Fvqx1vWHJ/28dh5
TLSH:	63F402382F9B4236F53257BD85E02680677E77B36723D95D04B121CE5BB37029AD0A2B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..d..... .....@.. .....@.....

File Icon

Icon Hash:	209480e66eb84902

Static PE Info

General

Entrypoint:	0x4b8286
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6417BEAA [Mon Mar 20 02:02:18 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xb8233	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x1110	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb6e20	0x54	.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	0xb628c	0xb6400	False	0.9273874206961591	data	7.86900119148787	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x1110	0x1200	False	0.7306857638888888	data	6.633755365364255	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xbc000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

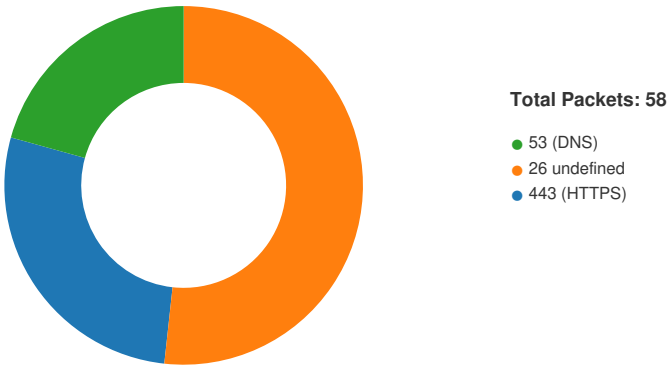
Name	RVA	Size	Type	Language	Country
RT_ICON	0xba100	0xa79	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbab8c	0x14	data		
RT_VERSION	0xbabb0	0x360	data		
RT_MANIFEST	0xbaf20	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:27:23.942231894 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:23.942292929 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:23.942411900 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:24.007399082 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:24.007443905 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:24.728410959 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:24.728621006 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:24.732671022 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:24.732700109 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:24.733073950 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:24.861732006 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:25.112267017 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:25.112309933 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:25.280256033 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:25.280361891 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:25.280431032 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:25.281380892 CET	49700	443	192.168.2.3	104.237.62.211

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:27:37.027848005 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.067028046 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.067150116 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.512274981 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.513009071 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.551852942 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.552182913 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.592528105 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.593195915 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.638087988 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.638134956 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.638170004 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.638186932 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.638231993 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.638274908 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.638979912 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.663780928 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:37.702769995 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:37.862869024 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:41.386651039 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:41.425951958 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:41.441111088 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:41.482404947 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:41.482830048 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:41.579770088 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:43.337220907 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:43.337676048 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:43.376271963 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:43.376332045 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:43.377685070 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:43.377856016 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:43.417109013 CET	49701	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:43.463438034 CET	26	49701	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.121768951 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.160450935 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.160610914 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.230684996 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.230947971 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.269793987 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.270059109 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.310445070 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.310969114 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.357144117 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.357218981 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.357255936 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.357301950 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.357319117 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.357460976 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.360599995 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:44.401413918 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:44.457210064 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:45.016462088 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:45.059911013 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:45.060256958 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:45.149873972 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:49.103950977 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:49.160787106 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:49.894712925 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:49.933489084 CET	26	49704	89.43.174.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:27:51.441457033 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:51.441847086 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:51.480488062 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:51.480618954 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:51.481302977 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:51.481391907 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:51.481463909 CET	49704	26	192.168.2.3	89.43.174.45
Mar 20, 2023 18:27:51.519972086 CET	26	49704	89.43.174.45	192.168.2.3
Mar 20, 2023 18:27:51.623965025 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:51.624037027 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:51.624146938 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:51.643871069 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:51.643932104 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:52.333190918 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:52.333317995 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:52.340928078 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:52.340950966 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:52.341305017 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:52.546730042 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:52.546859026 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:52.847053051 CET	49705	443	192.168.2.3	104.237.62.211
Mar 20, 2023 18:27:52.847134113 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:53.015525103 CET	443	49705	104.237.62.211	192.168.2.3
Mar 20, 2023 18:27:53.015774965 CET	443	49705	104.237.62.211	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:27:23.871232986 CET	58921	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:27:23.894016027 CET	53	58921	8.8.8.8	192.168.2.3
Mar 20, 2023 18:27:23.903903961 CET	62704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:27:23.925348997 CET	53	62704	8.8.8.8	192.168.2.3
Mar 20, 2023 18:27:36.987834930 CET	49977	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:27:37.013712883 CET	53	49977	8.8.8.8	192.168.2.3
Mar 20, 2023 18:27:44.058130026 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:27:44.120850086 CET	53	52387	8.8.8.8	192.168.2.3
Mar 20, 2023 18:27:51.552333117 CET	56924	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:27:51.573849916 CET	53	56924	8.8.8.8	192.168.2.3
Mar 20, 2023 18:27:51.584722996 CET	60625	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:27:51.604175091 CET	53	60625	8.8.8.8	192.168.2.3
Mar 20, 2023 18:28:02.055280924 CET	53975	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:28:02.074980974 CET	53	53975	8.8.8.8	192.168.2.3
Mar 20, 2023 18:28:02.082792044 CET	51139	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:28:02.102576971 CET	53	51139	8.8.8.8	192.168.2.3
Mar 20, 2023 18:28:04.026057005 CET	52955	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:28:04.043845892 CET	53	52955	8.8.8.8	192.168.2.3
Mar 20, 2023 18:28:10.749948025 CET	60582	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:28:10.813093901 CET	53	60582	8.8.8.8	192.168.2.3
Mar 20, 2023 18:28:17.866210938 CET	57134	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:28:17.888845921 CET	53	57134	8.8.8.8	192.168.2.3
Mar 20, 2023 18:28:21.180830956 CET	62050	53	192.168.2.3	8.8.8.8
Mar 20, 2023 18:28:21.199157953 CET	53	62050	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 18:27:23.871232986 CET	192.168.2.3	8.8.8.8	0x1edc	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:23.903903961 CET	192.168.2.3	8.8.8.8	0xf875	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 18:27:36.987834930 CET	192.168.2.3	8.8.8.8	0x9ffe	Standard query (0)	mail.spjsv.ro	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:44.058130026 CET	192.168.2.3	8.8.8.8	0x311b	Standard query (0)	mail.spjsv.ro	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.552333117 CET	192.168.2.3	8.8.8.8	0xfae1	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.584722996 CET	192.168.2.3	8.8.8.8	0x6f39	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.055280924 CET	192.168.2.3	8.8.8.8	0xf9fd	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.082792044 CET	192.168.2.3	8.8.8.8	0x378a	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:04.026057005 CET	192.168.2.3	8.8.8.8	0x68f6	Standard query (0)	mail.spjsv.ro	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:10.749948025 CET	192.168.2.3	8.8.8.8	0x6279	Standard query (0)	mail.spjsv.ro	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:17.866210938 CET	192.168.2.3	8.8.8.8	0x1001	Standard query (0)	mail.spjsv.ro	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:21.180830956 CET	192.168.2.3	8.8.8.8	0x6fbb	Standard query (0)	mail.spjsv.ro	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
Mar 20, 2023 18:27:23.894016027 CET	8.8.8.8	192.168.2.3	0x1edc	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:27:23.894016027 CET	8.8.8.8	192.168.2.3	0x1edc	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:23.894016027 CET	8.8.8.8	192.168.2.3	0x1edc	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:23.894016027 CET	8.8.8.8	192.168.2.3	0x1edc	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:23.925348997 CET	8.8.8.8	192.168.2.3	0xf875	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:27:23.925348997 CET	8.8.8.8	192.168.2.3	0xf875	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:23.925348997 CET	8.8.8.8	192.168.2.3	0xf875	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:23.925348997 CET	8.8.8.8	192.168.2.3	0xf875	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:37.013712883 CET	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	mail.spjsv.ro		89.43.174.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:44.120850086 CET	8.8.8.8	192.168.2.3	0x311b	No error (0)	mail.spjsv.ro		89.43.174.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.573849916 CET	8.8.8.8	192.168.2.3	0xfae1	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:27:51.573849916 CET	8.8.8.8	192.168.2.3	0xfae1	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.573849916 CET	8.8.8.8	192.168.2.3	0xfae1	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.573849916 CET	8.8.8.8	192.168.2.3	0xfae1	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.604175091 CET	8.8.8.8	192.168.2.3	0x6f39	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:27:51.604175091 CET	8.8.8.8	192.168.2.3	0x6f39	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 18:27:51.604175091 CET	8.8.8.8	192.168.2.3	0x6f39	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:27:51.604175091 CET	8.8.8.8	192.168.2.3	0x6f39	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.074980974 CET	8.8.8.8	192.168.2.3	0xf9fd	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:28:02.074980974 CET	8.8.8.8	192.168.2.3	0xf9fd	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.074980974 CET	8.8.8.8	192.168.2.3	0xf9fd	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.074980974 CET	8.8.8.8	192.168.2.3	0xf9fd	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.102576971 CET	8.8.8.8	192.168.2.3	0x378a	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 18:28:02.102576971 CET	8.8.8.8	192.168.2.3	0x378a	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.102576971 CET	8.8.8.8	192.168.2.3	0x378a	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:02.102576971 CET	8.8.8.8	192.168.2.3	0x378a	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:04.043845892 CET	8.8.8.8	192.168.2.3	0x68f6	No error (0)	mail.spjsv.ro		89.43.174.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:10.813093901 CET	8.8.8.8	192.168.2.3	0x6279	No error (0)	mail.spjsv.ro		89.43.174.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:17.888845921 CET	8.8.8.8	192.168.2.3	0x1001	No error (0)	mail.spjsv.ro		89.43.174.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:28:21.199157953 CET	8.8.8.8	192.168.2.3	0x6fbb	No error (0)	mail.spjsv.ro		89.43.174.45	A (IP address)	IN (0x0001)	false

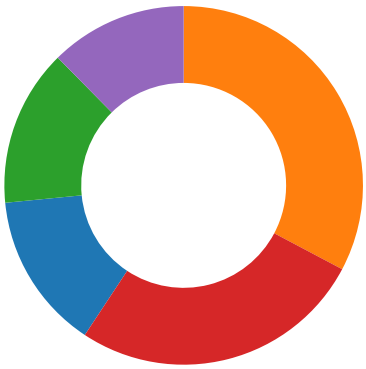
HTTP Request Dependency Graph

- api.ipify.org

Statistics

Behavior

- CsTapHIkAO.exe
- CsTapHIkAO.exe
- BKEDEaL.exe
- BKEDEaL.exe
- BKEDEaL.exe
- BKEDEaL.exe
- BKEDEaL.exe



Click to jump to process

System Behavior

Analysis Process: CsTapHIkAO.exe PID: **2416**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:27:12
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\CsTapHIkAO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CsTapHIkAO.exe
Imagebase:	0x650000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	72AECF06	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	72AECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CsTapHIkAO.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72DFC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CsTapHIkAO.exe.log	0	1216	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	72DFC907	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	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72AC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72ACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71A31B4F	ReadFile

Analysis Process: CsTapHIkAO.exe PID: **4496**, Parent PID: **2416**

General

Target ID:	1
Start time:	18:27:21
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\CsTapHIkAO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CsTapHIkAO.exe
Imagebase:	0xd60000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
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: 00000001.00000002.527846084.000000000311C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.527846084.000000000311C000.00000004.00000800.00020000.00000000.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	72AECF06	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	72AECF06	unknown
C:\Users\user\AppData\Roaming\BKEDEaL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71A3DD66	CopyFileW
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	71A3DD66	CopyFileW
C:\Users\user\AppData\Roaming\3rtvr542.vzr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71A3DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe:Zone.Identifier	success or wait	1	6F46AA2	DeleteFileW
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network\Cookies	success or wait	1	71A36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 17 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 0b 00 00 14 00 00 00 00 00 00 fd fd 0b 00 00 20 00 00 00 fd 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELd0d @ @	success or wait	3	71A3DD66	CopyFileW
C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	71A3DD66	CopyFileW
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 11 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5g$	success or wait	1	71A3DD66	CopyFileW

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	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72AC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72ACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72A203DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network\Cookies	unknown	16384	success or wait	2	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\3rtvr542.vzr\Chrome\Default\Network\Cookies	unknown	16384	end of file	1	71A31B4F	ReadFile

Registry Activities

Analysis Process: BKEDEaL.exe PID: 1244, Parent PID: 3452

General

Target ID:	11
Start time:	18:27:39
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe"
Imagebase:	0x110000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs • Detection: 41%, Virustotal, Browse
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	72AECF06	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	72AECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BKEDEaL.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72DFC78D	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\BKEDEaL.exe.log	0	1216	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	72DFC907	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	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72AC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72ACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71A31B4F	ReadFile

Analysis Process: BKEDEaL.exe PID: **5316**, Parent PID: **1244**

General

Target ID:	12
Start time:	18:27:45
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Imagebase:	0x790000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.529011306.0000000002DCC000.00000004.00000800.00020000.00000000.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	72AECF06	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	72AECF06	unknown
C:\Users\user\AppData\Roaming\d210uggn.oho	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71A3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71A3DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network\Cookies	success or wait	1	71A36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 11 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5g$	success or wait	1	71A3DD66	CopyFileW

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	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72AC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72ACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network\Cookies	unknown	16384	success or wait	2	71A31B4F	ReadFile
C:\Users\user\AppData\Roaming\d210uggn.oho\Chrome\Default\Network\Cookies	unknown	16384	end of file	1	71A31B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: BKEDEaL.exe PID: 3408, Parent PID: 3452

General

Target ID:	13
Start time:	18:27:48
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe"
Imagebase:	0x9e0000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
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	72AECF06	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	72AECF06	unknown

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	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72AC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72ACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71A31B4F	ReadFile

Analysis Process: BKEDEaL.exe PID: 5116, Parent PID: 3408

General

Target ID:	14
Start time:	18:27:58
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Imagebase:	0x7ff651c80000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BKEDEaL.exe PID: **5576**, Parent PID: **3408**

General

Target ID:	15
Start time:	18:27:58
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\BKEDEaL\BKEDEaL.exe
Imagebase:	0x960000
File size:	752128 bytes
MD5 hash:	FC7AD54F4F2E785AD748D952945CC888
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.527812814.0000000002D1C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly