ID: 635170
Sample Name:
INV00987890.exe
Cookbook: default.jbs
Time: 16:20:10
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

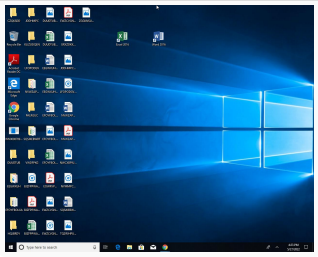
Windows Analysis Report

INV00987890.exe

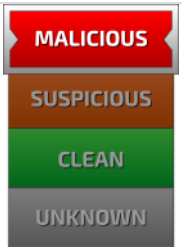
Overview

General Information

Sample Name:	INV00987890.exe
Analysis ID:	635170
MD5:	fe5cab253ef5708..
SHA1:	d7d0ba487169c5..
SHA256:	80f5923e2037f35.
Tags:	agenttesla exe
Infos:	



Detection



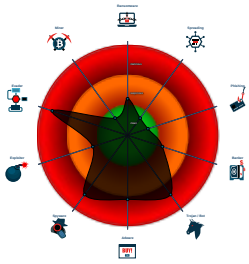
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- INV00987890.exe (PID: 6468 cmdline: "C:\Users\user\Desktop\INV00987890.exe" MD5: FE5CAB253EF5708D03DD6970E105B6C6)
  - INV00987890.exe (PID: 6764 cmdline: {path} MD5: FE5CAB253EF5708D03DD6970E105B6C6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@maviksel.com",
  "Password": "Ravi/1970",
  "Host": "mail.maviksel.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.526824095.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.526824095.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.295217525.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.295217525.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.296078130.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.INV00987890.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.INV00987890.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.INV00987890.exe.400000.10.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32cab:$s10: logins • 0x32712:$s11: credential • 0x2ecd3:$g1: get_Clipboard • 0x2ece1:$g2: get_Keyboard • 0x2ecee:$g3: get_Password • 0x2ffeb:$g4: get_CtrlKeyDown • 0x2fffb:$g5: get_ShiftKeyDown • 0x3000c:$g6: get_AltKeyDown
4.0.INV00987890.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.INV00987890.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

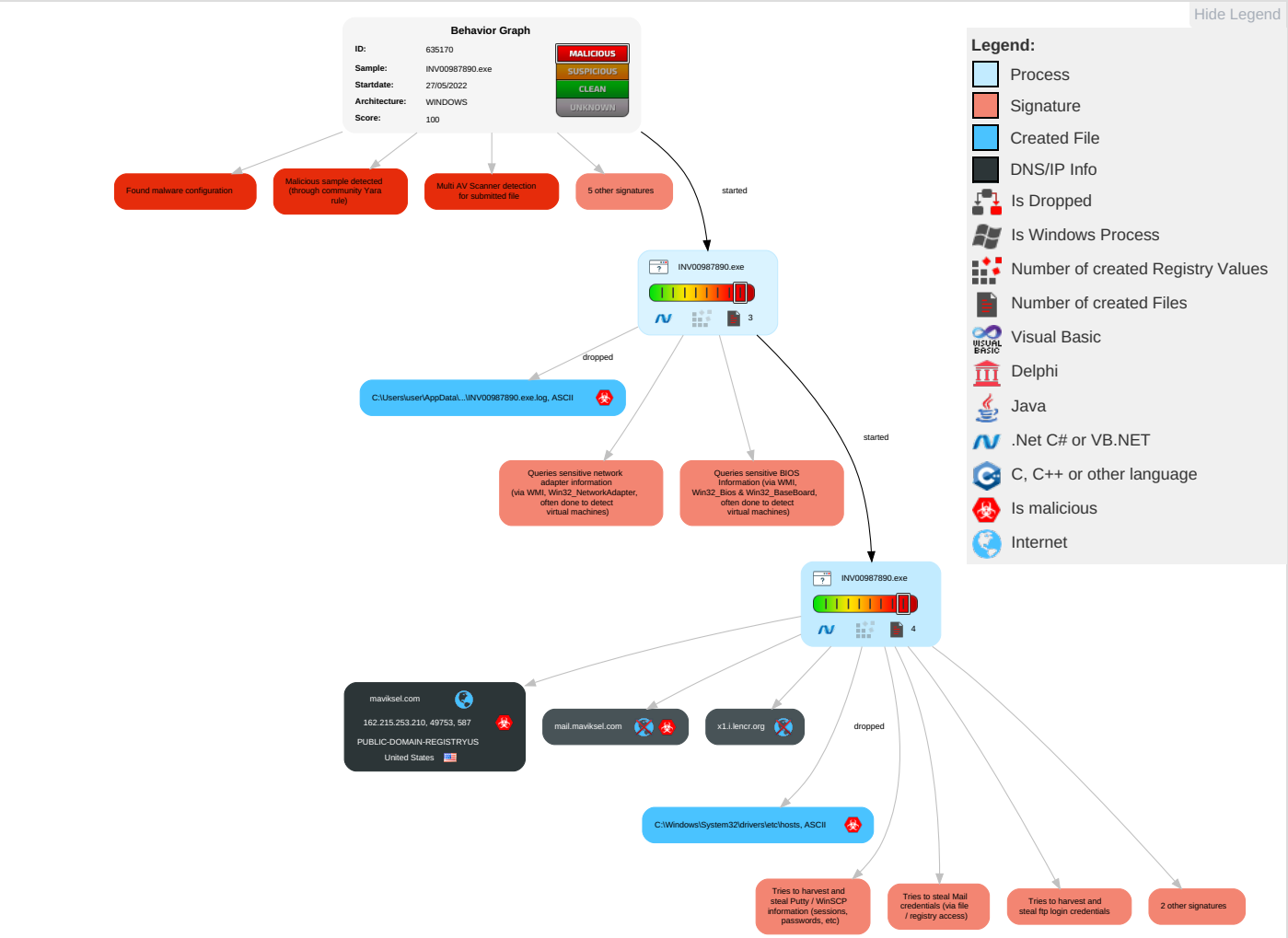
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	1 Credentials in Registry	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 1 Virtualization/Sandbox Evasion	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 Remote System Discovery	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	3 Obfuscated Files or Information	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
INV00987890.exe	31%	Virustotal		Browse
INV00987890.exe	27%	ReversingLabs		
INV00987890.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.INV00987890.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.INV00987890.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.INV00987890.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.INV00987890.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.INV00987890.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.INV00987890.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
maviksel.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnR	0%	URL Reputation	safe	
http://https://BJANwyE880kOV.net	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.tiro.comA	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnk	0%	URL Reputation	safe	
http://www.fonts.comnr2	0%	Avira URL Cloud	safe	
http://www.urwpp.de.	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://NEjfKK.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.fontbureau.commn	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krati	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.comalsdw	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://maviksel.com	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d%	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.fontbureau.comueta	0%	URL Reputation	safe	
http://www.fontbureau.comM	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdw	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.fonts.comnte	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comeM	0%	Avira URL Cloud	safe	
http://mail.maviksel.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://BJANwyE880kOV.net853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.urwpp.dem	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cns-m	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
maviksel.com	162.215.253.210	true	true	• 0%, Virustotal, Browse	unknown
x1.i.lencr.org	unknown	unknown	false		unknown
mail.maviksel.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	INV00987890.exe, 00000004.00000002.52929 2759.0000000003171000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnR	INV00987890.exe, 00000000.00000003.26740 9325.000000000540D000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://BJANwyE880kOV.net	INV00987890.exe, 00000004.00000002.53137 1637.00000000034F3000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.c	INV00987890.exe, 00000000.00000003.26743 6367.00000000053D4000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%%startupfolder%	INV00987890.exe, 00000004.00000002.52929 2759.0000000003171000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	INV00987890.exe, 00000000.00000003.27110 7327.00000000053DD000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.270816122.00000000053 DD000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.270557812.00000000053DD000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comA	INV00987890.exe, 00000000.00000003.26541 0217.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.265488221.00000000053 EB000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr.org/0	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	INV00987890.exe, 00000000.00000003.26489 0640.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	INV00987890.exe, 00000000.00000003.26541 0217.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000002.309175319.00000000066 62000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comic	INV00987890.exe, 00000000.00000003.26509 9327.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.265126207.00000000053 EB000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnk	INV00987890.exe, 00000000.00000003.26783 6467.00000000053D4000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.267986661.00000000053 DB000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.267436367.00000000053D4000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comnr2	INV00987890.exe, 00000000.00000003.26502 9682.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de.	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.c.lencr.org/0	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcom	INV00987890.exe, 00000000.00000003.27494 3515.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.276313639.00000000053 D9000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.275367663.00000000053DA000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://NEjfKK.com	INV00987890.exe, 00000004.00000002.52929 2759.0000000003171000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	INV00987890.exe, 00000004.00000002.52929 2759.0000000003171000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.o.lencr.org0	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commn	INV00987890.exe, 00000000.00000003.27494 3515.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.276313639.00000000053 D9000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.275367663.00000000053DA000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krati	INV00987890.exe, 00000000.00000003.26656 4650.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	INV00987890.exe, 00000000.00000003.26502 9682.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000002.309175319.00000000066 62000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.264949600.00000000053EB000.00000004.0 0000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.266564650.00000000053 D9000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsdw	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	INV00987890.exe, 00000004.00000002.52929 2759.0000000003171000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	low

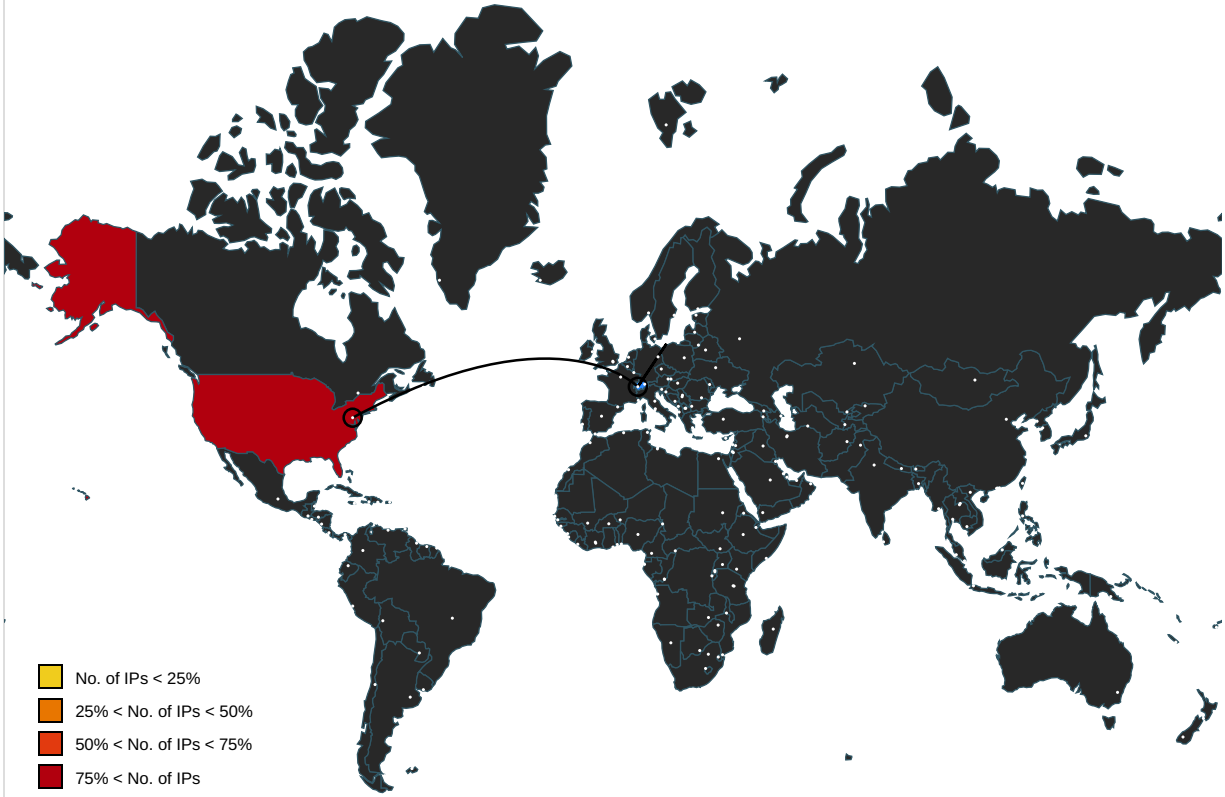
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/de	INV00987890.exe, 00000000.00000003.27852 7778.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.278472905.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.281901697.0000000005402000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.279181554.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.280387812.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.28128 6258.000000000540D000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.280312610.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.278741035.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.281875487.000 00000053FF000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.278224495.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.28012 0374.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.279720695.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.278188080.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.278682189.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.279603178.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.27815 5597.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.278710128.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.279112580.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.278278704.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.279325032.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.28170 7943.000000000540D000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://maviksel.com	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000002.309175319.00000000066 62000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 02.308767318.00000000053D0000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.298547621.000 00000053D0000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://x1.i.lencr.org/	2D85F72862B55C4EADD9E66E06947F3D0.4.dr	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.coma-d%	INV00987890.exe, 00000000.00000003.26502 9682.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.265085729.00000000053 F4000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.264743780.00000000053EB000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.264685681.000 00000053EB000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.264814672.00000000053EB000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.26485 2176.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.264630003.00000000053 EB000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.264949600.00000000053EB000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.264890640.000 00000053EB000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/cabarga.htmlp	INV00987890.exe, 00000000.00000003.27652 6018.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.275998575.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.277261918.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.276292788.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.277989711.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.27614 5647.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.275621528.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.276978947.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.277921796.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.277735473.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.27655 3761.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.275946542.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.276699756.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.277295426.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.275437800.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.27776 1576.0000000005405000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.276877803.00000000054 05000.00000004.00000800.00020000.0000000 0.sdmp, INV00987890.exe, 00000000.000000 03.275842686.0000000005405000.00000004.0 0000800.00020000.00000000.sdmp, INV00987 890.exe, 00000000.00000003.275718248.000 0000005405000.00000004.00000800.00020000 .00000000.sdmp, INV00987890.exe, 0000000 0.00000003.275888860.0000000005405000.00 000004.00000800.00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.27609 8140.0000000005405000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://cps.letsencrypt.org0	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comueta	INV00987890.exe, 00000000.00000003.27494 3515.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.275367663.00000000053 DA000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comM	INV00987890.exe, 00000000.00000002.30876 7318.00000000053D0000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.298547621.00000000053 D0000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdw	INV00987890.exe, 00000000.00000003.27494 3515.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.275367663.00000000053 DA000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbr owser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	INV00987890.exe, 00000004.00000002.52929 2759.0000000003171000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comnte	INV00987890.exe, 00000000.00000003.26502 9682.00000000053EB000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.264949600.00000000053 EB000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	INV00987890.exe, 00000000.00000002.30876 7318.00000000053D0000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.298547621.00000000053 D0000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comeM	INV00987890.exe, 00000000.00000003.27399 1474.00000000053D8000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.274943515.00000000053 D9000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.maviksel.com	INV00987890.exe, 00000004.00000002.53111 8006.00000000034D1000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	INV00987890.exe, 00000000.00000003.26783 6467.00000000053D4000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp, INV00987890.exe, 00000000.00000003.267409325.00000000054 0D000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	INV00987890.exe, 00000000.00000003.27543 7800.0000000005405000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://BJANwyE880kOV.net853321935-2125563209-4053062332-1002_Classes	INV00987890.exe, 00000004.00000003.31744 8459.00000000014C4000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers8	INV00987890.exe, 00000000.00000002.30917 5319.0000000006662000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.comalic	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.dem	INV00987890.exe, 00000000.00000003.27631 3639.00000000053D9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cns-m	INV00987890.exe, 00000000.00000003.26740 9325.000000000540D000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.215.253.210	maviksel.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635170
Start date and time: 27/05/202216:20:10	2022-05-27 16:20:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV00987890.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:	24
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.adwa.spyw.evad.winEXE@3/6@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 60.8% • Quality standard deviation: 30.7%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.50.97.168, 93.184.221.240, 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): fs.microsoft.com, e8652.dscx.akamaiedge.net, wu.ec.azureedge.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, sls.update.microsoft.com, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, crl.root-x1.letsencrypt.org.edgekey.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:21:31	API Interceptor	693x Sleep call for process: INV00987890.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\INV00987890.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...150604110438Z..350604110438Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....I.....*.A..v.....5/(.l....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".'].y...p..N..:.'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ')..au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

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

Process:	C:\Users\user\Desktop\INV00987890.exe
File Type:	Microsoft Cabinet archive data, 61476 bytes, 1 file
Category:	dropped
Size (bytes):	61476
Entropy (8bit):	**7.995018321729444**
Encrypted:	**true**
SSDEEP:	1536:NATLwfiuePkACih0/8uIwf5CiqGLhk1V/AFnGegJR:N7nePk5gKsoBha/0GTf
MD5:	308336E7F515478969B24C13DED11EDE
SHA1:	8FB0CF42B77DBBEF224A1E5FC38ABC2486320775
SHA-256:	889B832323726A9F10AD03F85562048FDCFE20C9FF6F9D37412CF477B4E92FF9
SHA-512:	61AD97228CD6C3909EF3AC5E4940199971F293BDD0D5EB7916E60469573A44B6287C0FA1E0B6C1389DF35EB6C9A7D2A61FDB318D4A886A3821EF5A9DAB3AC2F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....$.....,.....I.....w.....Tp. .authroot.stl.H#F..4..CK..<Tk...c_.d....A.F...,.&K..*i.RJJ..J.".%.KY"{n...."{..Lu3.Ln.....y.....M.:...<. v...H..~.#Ov.a0xN....)..C.. t.z.,x.00.1``L.....L.\..1.|..2.1.0mD...H1/.....G..UT7!...r.X:....D.0.0...M....I(.-.+..v#...(.r.....z.Y`&hw..Gl+.je.e.j..{.1.....9f=.&.....s.W...L.].+...).f...u.....8....}R...w.X..>.A.Yw...a.x.. .T8V.e...^.7.q..t^.+....f.q).B.M.....64.<!W(.....D!.0.t "X...l....D0.....+...A.....0.o..t93.v..O1V x}H.S)....GH.6.I...p2.(4k....!,.L`.....h:.a]?.....J9.\..Ww.....%.....a4E...q.*...#..a. .y..M..R.t..Z2!.T.Ua.k.'O..\./ d.F>.V...3...._.J....."....wI..'..z...j..Ds...qZ...[.....O<.d.K..hH@c1....[w7..z...I....h,.b.....'.w.....bO.i{.....+.-...H..."<...L.Tu}.Y.lB.]3..4..G.3..`E. .NF.....{o.h]}p....G..$..4....;..&.O.d....v:Ik.T..ObLq..&.j.j...B9.(..!..\.:K`.....:O..N....C..jD:.i.....1.....eCo.c..3o.....nN.D..3.7...

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

Process:	C:\Users\user\Desktop\INV00987890.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.759454828358771
Encrypted:	false
SSDEEP:	3:kkFklFgPvfllXlE/zMcjxrXNNX8RolJuRdyo1dlUKlGXJlDdt:kKjPk1NpNMa8Rdy+UKcXP
MD5:	1E734632A3B797F921CA36FCBA267555
SHA1:	FB8E9CB639A6BD642026CB80134C8954087CD7B7
SHA-256:	94D9398F502DE05859F4976BC6DFE4CB72FF4D3E80B898C3A8404B3DA3F63965
SHA-512:	DE4945AF965CDACAF1C5C82D56ED577CDFF533364D4E5247F66813878AC3729EE2DC39DFC01C9121218446EB3A46011F22AD0F78B1B12B54546AA0A70093446B
Malicious:	false
Reputation:	low
Preview:	p..... .....v.h.%r..(..... .....~....T.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

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

Process:	C:\Users\user\Desktop\INV00987890.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.0985636032074564
Encrypted:	false
SSDEEP:	6:kKnmN+SkQlPlEGYRMY9z+4KlDA3RUecl7PG1:9kPlE99SNxAhUecl61
MD5:	C02354F3A48768C5598D49EEFEA51317
SHA1:	F03F057C0EC871499B069FC065FB34B0974B3F47
SHA-256:	14E0058B73254FC3210F10EB51D5558E82481428D694CB368361CBCCEF22C8F9
SHA-512:	FA8A54F6F4F8431B1778FEFB0A2CB8AFC88B88EB12054C87E28384A2B1AA45E0C7FA4B8766FFF15C084B5688CB4C2BD58CD8CFA82FAEEF764668A74A4EFFF618
Malicious:	false
Reputation:	low
Preview:	p..... .....S.8&r..(..... .....3f..o.....&.....$...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...".0.3.3.6.6.b.4.9.0.6.f.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INV00987890.exe.log

Process:	C:\Users\user\Desktop\INV00987890.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\INV00987890.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FAF
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.457754043877134
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:	INV00987890.exe
File size:	518144
MD5:	fe5cab253ef5708d03dd6970e105b6c6
SHA1:	d7d0ba487169c56e33e92064b482c2d56d5dba5e
SHA256:	80f5923e2037f3596f2bebec849a1a55221c37c714d14eca6bdd35e12351ec7d
SHA512:	d522c952a8f8b0b619b488fde6571182ed27628a66f9b309dfb204e13cf211be29800eb01493294937579a227fe5a928dbbd4228de6344e31c7c0f376a3565d8
SSDEEP:	12288:VYEEIBxW7R0OfmlLBhek6U02K+olrtM5Jj:VxEMxW7WUmxHBH0lrtM5l
TLSH:	90B4DF013BAC7A12E66BDB3550A1804453F2844FBA33E51E3EDF2CDF16A6B149760B79
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'..b.....P.....&.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47fd26
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:	0x6290BC27 [Fri May 27 11:55:19 2022 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7fcd4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x80000	0x5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x82000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7dd2c	0x7de00	False	0.779971837761	data	7.4693135193	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5c0	0x600	False	0.427734375	data	4.12439241181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x80090	0x330	data		
RT_MANIFEST	0x803d0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

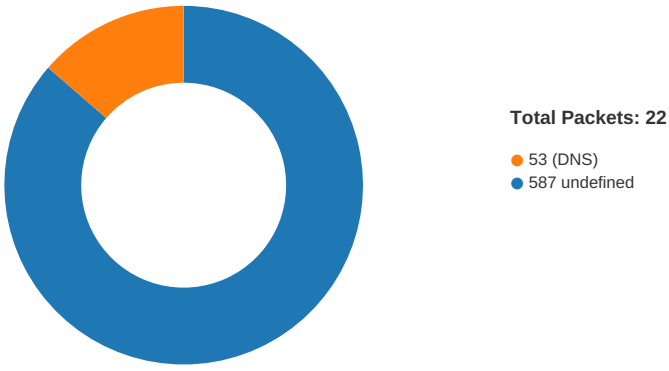
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright HP Inc. 2019
Assembly Version	1.0.4.0
InternalName	TNVeK.exe
FileVersion	1.0.4.0
CompanyName	HP Inc.
LegalTrademarks	
Comments	
ProductName	Final Setup
ProductVersion	1.0.4.0
FileDescription	Final Setup
OriginalFilename	TNVeK.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:21:53.984049082 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:54.153772116 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:54.153924942 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:55.639431953 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:55.639763117 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:55.807671070 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:55.807991028 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:55.977329969 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:56.085055113 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:56.274815083 CEST	587	49753	162.215.253.210	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:21:56.274930000 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:56.274964094 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:56.278034925 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:56.304992914 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:21:56.473186970 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:21:56.603131056 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:00.993542910 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:01.161530018 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:01.163355112 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:01.331542015 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:01.336613894 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:01.544559956 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:01.627439976 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:01.628704071 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:01.796606064 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:01.805218935 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:02.006067038 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.006397963 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:02.175856113 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.177301884 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:02.177412033 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:02.178045988 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:02.178121090 CEST	49753	587	192.168.2.3	162.215.253.210
May 27, 2022 16:22:02.345071077 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.345103025 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.345554113 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.345643044 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.346275091 CEST	587	49753	162.215.253.210	192.168.2.3
May 27, 2022 16:22:02.400403976 CEST	49753	587	192.168.2.3	162.215.253.210

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:21:53.303886890 CEST	65358	53	192.168.2.3	8.8.8.8
May 27, 2022 16:21:53.604362011 CEST	53	65358	8.8.8.8	192.168.2.3
May 27, 2022 16:21:53.684684038 CEST	53802	53	192.168.2.3	8.8.8.8
May 27, 2022 16:21:53.965389967 CEST	53	53802	8.8.8.8	192.168.2.3
May 27, 2022 16:21:57.851927996 CEST	65266	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 16:21:53.303886890 CEST	192.168.2.3	8.8.8.8	0x6cd5	Standard query (0)	mail.maviksel.com	A (IP address)	IN (0x0001)
May 27, 2022 16:21:53.684684038 CEST	192.168.2.3	8.8.8.8	0xb842	Standard query (0)	mail.maviksel.com	A (IP address)	IN (0x0001)
May 27, 2022 16:21:57.851927996 CEST	192.168.2.3	8.8.8.8	0x5f8f	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 16:21:53.604362011 CEST	8.8.8.8	192.168.2.3	0x6cd5	No error (0)	mail.maviksel.com	maviksel.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 16:21:53.604362011 CEST	8.8.8.8	192.168.2.3	0x6cd5	No error (0)	maviksel.com		162.215.253.210	A (IP address)	IN (0x0001)
May 27, 2022 16:21:53.965389967 CEST	8.8.8.8	192.168.2.3	0xb842	No error (0)	mail.maviksel.com	maviksel.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 16:21:53.965389967 CEST	8.8.8.8	192.168.2.3	0xb842	No error (0)	maviksel.com		162.215.253.210	A (IP address)	IN (0x0001)

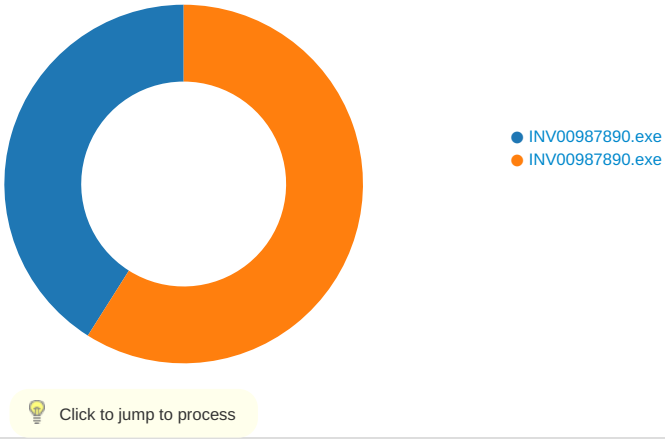
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 16:21:57.876038074 CEST	8.8.8.8	192.168.2.3	0x5f8f	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 16:21:55.639431953 CEST	587	49753	162.215.253.210	192.168.2.3	220-bh-73.webhostbox.net ESMTP Exim 4.94.2 #2 Fri, 27 May 2022 14:21:55 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 16:21:55.639763117 CEST	49753	587	192.168.2.3	162.215.253.210	EHLO 141700
May 27, 2022 16:21:55.807671070 CEST	587	49753	162.215.253.210	192.168.2.3	250-bh-73.webhostbox.net Hello 141700 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 27, 2022 16:21:55.807991028 CEST	49753	587	192.168.2.3	162.215.253.210	STARTTLS
May 27, 2022 16:21:55.977329969 CEST	587	49753	162.215.253.210	192.168.2.3	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: INV00987890.exe PID: 6468, Parent PID: 6136

General

Target ID:	0
Start time:	16:21:17
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\INV00987890.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INV00987890.exe"
Imagebase:	0x160000
File size:	518144 bytes
MD5 hash:	FE5CAB253EF5708D03DD6970E105B6C6
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: 00000000.00000002.306417687.000000000345F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.306417687.000000000345F000.00000004.00000800.00020000.00000000.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	6DC5CF06	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	6DC5CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INV00987890.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF6C78D	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\INV00987890.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	6DF6C907	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	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB903DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C231B4F	ReadFile

Analysis Process: INV00987890.exe PID: **6764**, Parent PID: **6468**

General

Target ID:	4
Start time:	16:21:34
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\INV00987890.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe30000
File size:	518144 bytes
MD5 hash:	FE5CAB253EF5708D03DD6970E105B6C6
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: 00000004.00000002.526824095.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.526824095.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.295217525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.295217525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.296078130.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.296078130.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.295669546.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.295669546.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.296713839.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.296713839.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.529292759.0000000003171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.529292759.0000000003171000.00000004.00000800.00020000.00000000.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	6DC5CF06	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	6DC5CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6C231B4F	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	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C231B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C231B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C231B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C231B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C231B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C231B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C231B4F	ReadFile

Disassembly

No disassembly