ID: 383833
Sample Name:
C6RET8T1Wi.exe
Cookbook: default.jbs
Time: 10:46:53
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

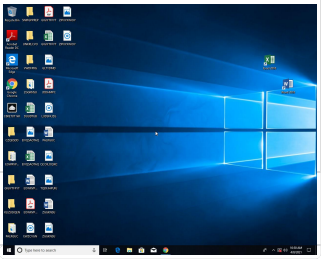
Analysis Report C6RET8T1Wi.exe

Overview

General Information

Sample Name:	C6RET8T1Wi.exe
Analysis ID:	383833
MD5:	133b4a863e9a9c..
SHA1:	d4db04a031b652..
SHA256:	db6863fdde8111c.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

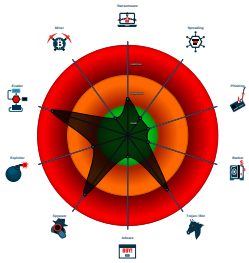
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- C6RET8T1Wi.exe (PID: 6460 cmdline: 'C:\Users\user\Desktop\C6RET8T1Wi.exe' MD5: 133B4A863E9A9C74B7320F54ABF199D7)
  - schtasks.exe (PID: 6860 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ePVIisXwKSPaua' /XML 'C:\Users\user\AppData\Local\Temp\tmp8430.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - C6RET8T1Wi.exe (PID: 6968 cmdline: C:\Users\user\Desktop\C6RET8T1Wi.exe MD5: 133B4A863E9A9C74B7320F54ABF199D7)
  - C6RET8T1Wi.exe (PID: 7028 cmdline: C:\Users\user\Desktop\C6RET8T1Wi.exe MD5: 133B4A863E9A9C74B7320F54ABF199D7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "armyscheme3@yandex.combrowse9jasmtp.yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000D.00000002.528245994.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.294530199.0000000003F46000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.291906336.0000000002DFC000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

Unpacked PEs

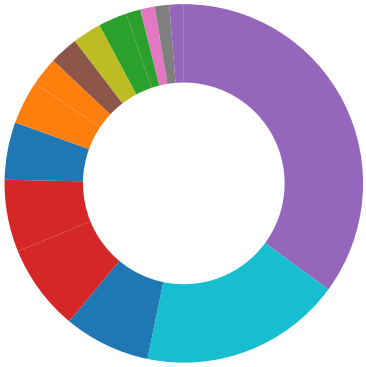
Source	Rule	Description	Author	Strings
13.2.C6RET8T1Wi.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.C6RET8T1Wi.exe.3fe82e0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.C6RET8T1Wi.exe.3fe82e0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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:

- Injects a PE file into a foreign processes

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)

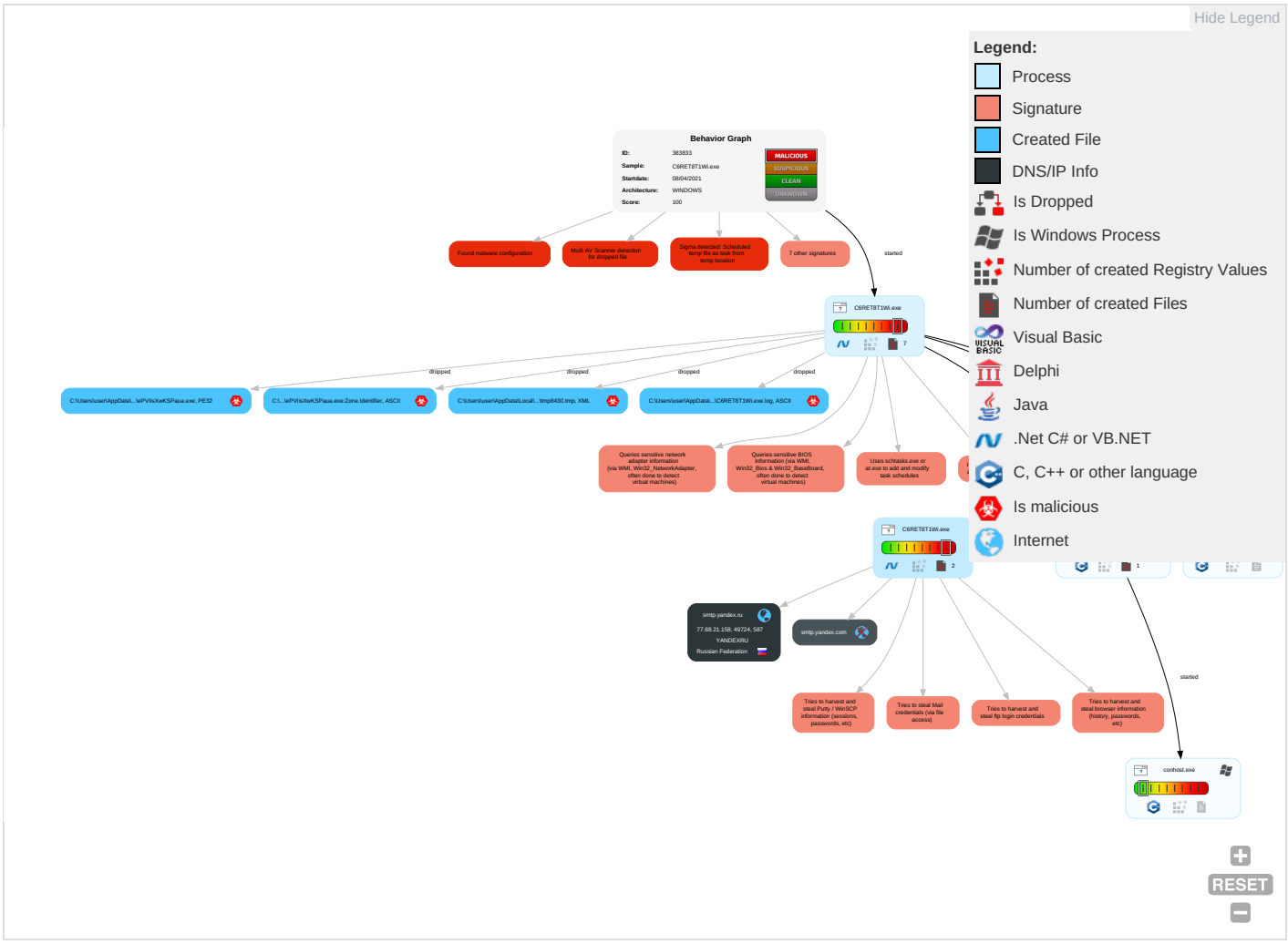
Remote Access Functionality:

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

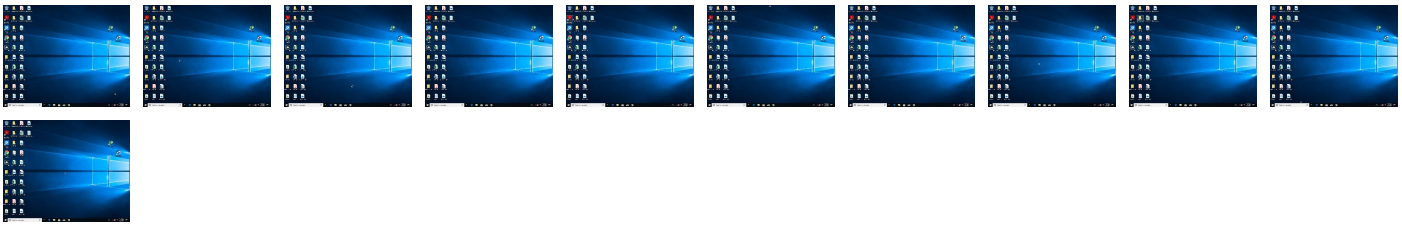
Behavior Graph



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
C6RET8T1Wi.exe	41%	Virustotal		Browse
C6RET8T1Wi.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	
C6RET8T1Wi.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ePVIisXwKSPaua.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ePVIisXwKSPaua.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.C6RET8T1Wi.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/Verdx	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnP	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0rsT	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comrz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/alny	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnb-n	0%	Avira URL Cloud	safe	
http://O4Irimjy3mfmBZ0.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.fontbureau.comt)	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cns	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sandoll.co.krC	0%	Avira URL Cloud	safe	
http://www.fonts.comx	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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://www.founder.com.cn/cnGK1	0%	Avira URL Cloud	safe	
http://NmvONo.com	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://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://www.sajatypeworks.comw	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	Avira URL Cloud	safe	
http://www.tiro.como	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Verdx	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnP	C6RET8T1Wi.exe, 00000001.00000003.266803258.0000000005EED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

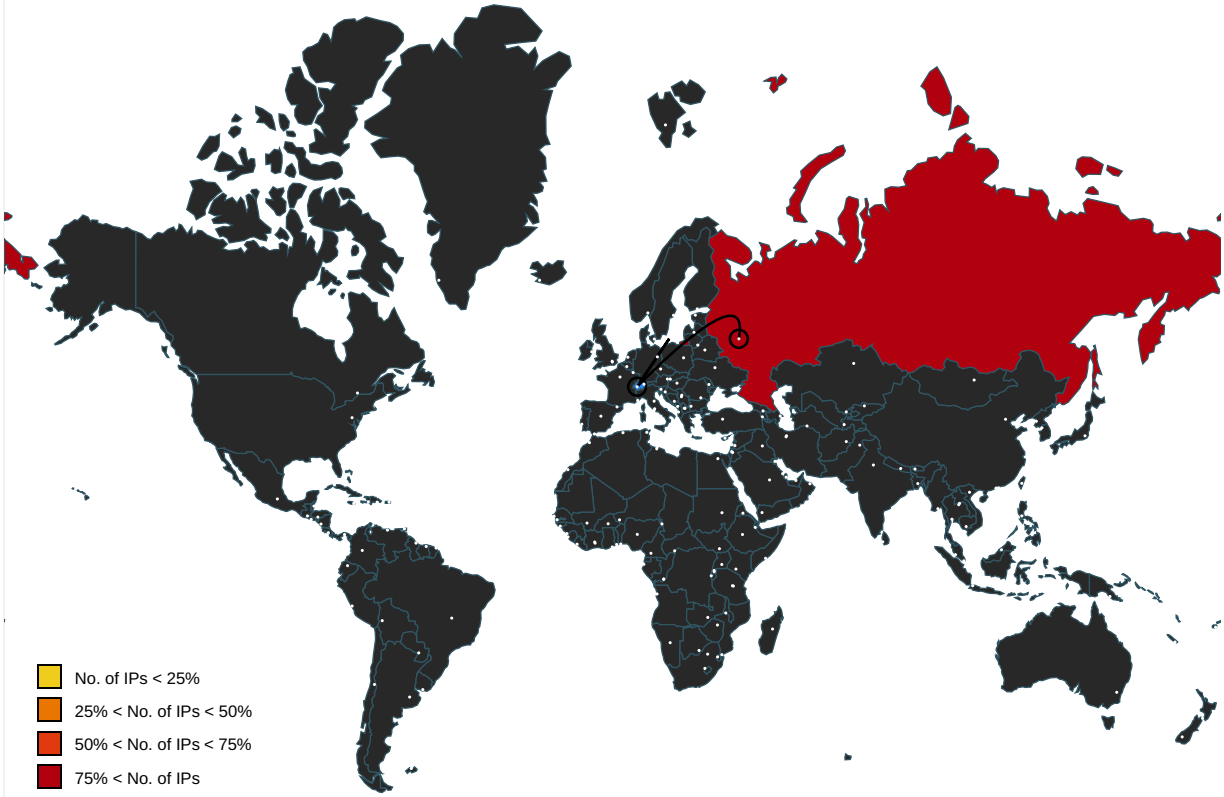
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cr	C6RET8T1Wi.exe, 00000001.00000003.267169299.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://yandex.crl.certum.pl/ycasha2.crl0q	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0rsT	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	C6RET8T1Wi.exe, 00000001.00000002.291953862.0000000002E13000.00000004.00000001.sdmp	false		high
http://www.tiro.com	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 00000001.00000003.271921494.0000000005EBD000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 00000001.00000003.271468846.0000000005EB9000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersuJ	C6RET8T1Wi.exe, 00000001.00000003.271921494.0000000005EBD000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comrz	C6RET8T1Wi.exe, 00000001.00000002.298526461.0000000005EB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	C6RET8T1Wi.exe, 00000001.00000002.291906336.0000000002DFC000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/alny	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 00000001.00000003.265303167.0000000005ECB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnb-n	C6RET8T1Wi.exe, 00000001.00000003.266803258.0000000005EED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://O4Irimjy3mfmBZ0.com	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 0000000D.00000002.535134278.000000000354E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comS	C6RET8T1Wi.exe, 00000001.00000003.264798854.0000000005ECB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/0	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comt)	C6RET8T1Wi.exe, 00000001.00000002.298526461.0000000005EB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cns	C6RET8T1Wi.exe, 00000001.00000003.266803258.0000000005EED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnt	C6RET8T1Wi.exe, 00000001.00000003.266823416.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	C6RET8T1Wi.exe, 00000001.00000002.291795607.0000000002DB1000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 00000001.00000002.291953862.0000000002E13000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krC	C6RET8T1Wi.exe, 00000001.00000003.266153350.0000000005EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comx	C6RET8T1Wi.exe, 00000001.00000003.265008386.0000000005ECB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	C6RET8T1Wi.exe, 00000001.00000002.294530199.0000000003F46000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 0000000D.00000002.528245994.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnGK1	C6RET8T1Wi.exe, 00000001.00000003.266823416.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://NmvONo.com	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.certum.pl/ycasha2.cer0	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	C6RET8T1Wi.exe, 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comw	C6RET8T1Wi.exe, 00000001.00000003.264798854.0000000005ECB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/M	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.como	C6RET8T1Wi.exe, 00000001.00000003.265303167.0000000005ECB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/F	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certum.pl/CPS0	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comX	C6RET8T1Wi.exe, 00000001.00000003.265008386.0000000005ECB000.00000004.00000001.sdmp	false		unknown
http://www.jiyu-kobo.co.jp/?	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.yandex.com	C6RET8T1Wi.exe, 0000000D.00000002.534943909.0000000003520000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.ocsp-responder.com03	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comj	C6RET8T1Wi.exe, 00000001.00000002.298526461.0000000005EB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnNK&	C6RET8T1Wi.exe, 00000001.00000003.266823416.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 00000001.00000003.266823416.0000000005EB4000.00000004.00000001.sdmp, C6RET8T1Wi.exe, 00000001.00000003.266803258.0000000005EED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/ico	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/k	C6RET8T1Wi.exe, 00000001.00000003.268941436.0000000005EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	C6RET8T1Wi.exe, 00000001.00000002.299365680.00000000070C2000.00000004.00000001.sdmp	false		high
http://crl.certum.pl/ca.crl0h	C6RET8T1Wi.exe, 0000000D.00000002.535007261.000000000352A000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comsed~	C6RET8T1Wi.exe, 00000001.00000003.264798854.0000000005ECB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383833
Start date:	08.04.2021
Start time:	10:46:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 56s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	C6RET8T1Wi.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@8/4@2/1
EGA Information:	Failed
HDC Information:	Failed
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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 93.184.220.29, 204.79.197.200, 13.107.21.200, 20.50.102.62, 104.43.139.144, 52.255.188.83, 23.54.113.53, 104.42.151.234, 52.147.198.201, 95.100.54.203, 20.82.210.154, 23.10.249.26, 23.10.249.43, 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, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:48:13	API Interceptor	706x Sleep call for process: C6RET8T1Wi.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	Payment _Advice (2).exe	Get hash	malicious	Browse	
	cricket.exe	Get hash	malicious	Browse	
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	
	Shandong CIRS Form.exe	Get hash	malicious	Browse	
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	
	Q99Eljz7IT.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	
	kfMrlKSN4F.exe	Get hash	malicious	Browse	
	xjvIB3Wkvk.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158
	Q99Eljz7IT.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	kfMrlKSN4F.exe	Get hash	malicious	Browse	• 77.88.21.158
	xjvIB3Wkvk.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 77.88.21.179
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158
	Q99Eljz7IT.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	scan-100218.docm	Get hash	malicious	Browse	• 93.158.134.119
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\C6RET8T1Wi.exe.log	
Process:	C:\Users\user\Desktop\C6RET8T1Wi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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

C:\Users\user\AppData\Local\Temp\tmp8430.tmp	
Process:	C:\Users\user\Desktop\C6RET8T1Wi.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.172916200556988
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBi0tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3L
MD5:	0DA72E8020ACC34E9DF0550E2446BF92
SHA1:	33C2C9C78819261F163B778AADC7E7FA0E289C20
SHA-256:	E7D5394DC8C71CE85A1CB3DA70F23E1D016CD5E51136A17D41E9177F04FDA18C

C:\Users\user\AppData\Local\Temp\tmp8430.tmp	
SHA-512:	AD60907A0468FFEB0950A60A247F61E46ECB9DBFE9B24365966867DDA7A9B6A4DEEE2E007210CF9BCF26A443EBBF04E4B0B3F428791C469B4D0329D503E0E14B
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\ePVlisXwKSPaua.exe	
Process:	C:\Users\user\Desktop\C6RET8T1Wi.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1031168
Entropy (8bit):	7.5599836445937
Encrypted:	false
SSDEEP:	24576:N1TbhttyDnl8+3Jsesv+1yrA/Jp/jO9BvLe:NTttonlvsGX//bOvL
MD5:	133B4A863E9A9C74B7320F54ABF199D7
SHA1:	D4DB04A031B65254B4194BB2F1CA81A487A7FE50
SHA-256:	DB6863FDDE8111C668522696E503145C0F988AD14C248FBBA9ECD4A23DE83613
SHA-512:	C24F5DC2C8D27D7DA9A8D4B91201E33A4748B67368605ABE016256DE73066E9E99E9FD9012444A1548320ECB0C60CF9494635B0071F656EB4632177AEADC2C5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....;m`.....P..8.....^W... ...`....@.. ....@.....W..O....`..... ..... ..H.....text...d7... ...8..... ..`.rsrc.....`.....:.....@..@.rel oc.....@..B.....@W.....H.....|<...O.....\.....0.....(....(.....(.....o....*.....(.....(!.....("......(#.....($....*N..(. ...o....(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<..... ...~.....(1.....,!r...p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\ePVlisXwKSPaua.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\C6RET8T1Wi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.5599836445937
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:	C6RET8T1Wi.exe

General

File size:	1031168
MD5:	133b4a863e9a9c74b7320f54abf199d7
SHA1:	d4db04a031b65254b4194bb2f1ca81a487a7fe50
SHA256:	db6863fdde8111c668522696e503145c0f988ad14c248fbba9ecd4a23de83613
SHA512:	c24f5dc2c8d27d7da9a8d4b91201e33a4748b67368605abe016256de73066e9e99e9fd9012444a1548320ecb0c60cf9494635b0071f656eb4632177aeadc2c57
SSDEEP:	24576:N1TbhttyDnl8+3Jsesv+1yrA/Jp/jO9BvLe:NTttonlvsGX//bOvL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....;m`.....P..8.....^W... ...`....@.. .....@.....

File Icon

Icon Hash:	d28ab3b0e0ab96c4

Static PE Info

General

Entrypoint:	0x4d575e
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:	0x606D3B0F [Wed Apr 7 04:54:39 2021 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd570c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x28000	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfe000	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	0xd3764	0xd3800	False	0.852953466681	data	7.77629150782	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x28000	0x28000	False	0.348266601562	data	5.33199734146	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	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	0xd6280	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xe6aa8	0x94a8	data		
RT_ICON	0xeff50	0x5488	data		
RT_ICON	0xf53d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xf9600	0x25a8	data		
RT_ICON	0xfbba8	0x10a8	data		
RT_ICON	0xfcc50	0x988	data		
RT_ICON	0xfd5d8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xfda40	0x76	data		
RT_VERSION	0xfdab8	0x35c	data		
RT_MANIFEST	0xfde14	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

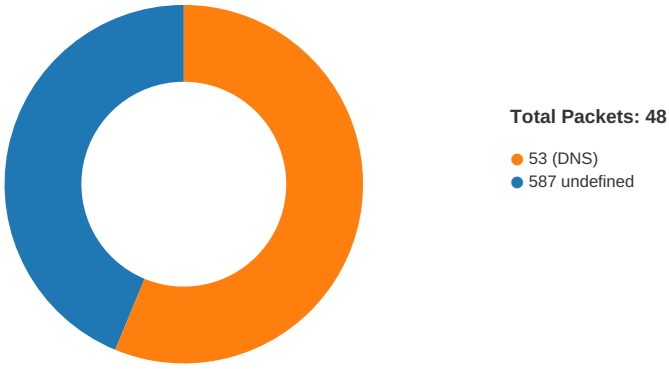
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	7.0.0.1
InternalName	TypeUnion.exe
FileVersion	7.0.0.1
CompanyName	FileCodeGroup
LegalTrademarks	
Comments	FileCodeGroup
ProductName	Major Project
ProductVersion	7.0.0.1
FileDescription	Major Project
OriginalFilename	TypeUnion.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:50:04.697968960 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:04.757010937 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:04.757100105 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:04.956531048 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:04.957103968 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.016175985 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.016228914 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.016913891 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.075756073 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.131339073 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.189738035 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.250076056 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.250133038 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.250169992 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.250202894 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.250351906 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.250478029 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.321717978 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.381097078 CEST	587	49724	77.88.21.158	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:50:05.429044008 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.727226019 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.786475897 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.788240910 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.847610950 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.848956108 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.919176102 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.923804998 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:05.990900993 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:05.991934061 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:06.057542086 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:06.058021069 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:06.116939068 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:06.120604038 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:06.120918989 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:06.121618986 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:06.121798038 CEST	49724	587	192.168.2.5	77.88.21.158
Apr 8, 2021 10:50:06.179809093 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:06.180265903 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:06.493727922 CEST	587	49724	77.88.21.158	192.168.2.5
Apr 8, 2021 10:50:06.537614107 CEST	49724	587	192.168.2.5	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:47:45.395198107 CEST	52704	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:45.407685995 CEST	53	52704	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:45.516362906 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:45.529778957 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:45.551681995 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:45.563613892 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:45.584640026 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:45.598089933 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:45.763812065 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:45.789467096 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:46.132524967 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:46.145257950 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:47.134906054 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:47.148159027 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 10:47:52.575403929 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:47:52.589293003 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:02.747829914 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:02.759968996 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:04.927238941 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:04.940278053 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:06.155400038 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:06.167747021 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:07.196096897 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:07.217538118 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:08.452764988 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:08.465712070 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:19.151809931 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:19.164824963 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:20.287110090 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:20.300358057 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:22.635272026 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:22.647893906 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:23.028289080 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:23.040791988 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:29.042406082 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:29.060874939 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:30.959913969 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:48:30.973500013 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 10:48:43.710974932 CEST	55161	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:48:43.723860979 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 10:49:04.555234909 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:49:04.567758083 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 10:49:07.309771061 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:49:07.329549074 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 10:49:22.174190998 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:49:22.200989008 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 10:49:43.669694901 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:49:43.682336092 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 10:49:45.390861034 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:49:45.404653072 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 10:50:04.505937099 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:50:04.519083023 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 10:50:04.538531065 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 10:50:04.552460909 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
Apr 8, 2021 10:50:04.505937099 CEST	192.168.2.5	8.8.8.8	0xf1a2	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:04.538531065 CEST	192.168.2.5	8.8.8.8	0x7614	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:50:04.519083023 CEST	8.8.8.8	192.168.2.5	0xf1a2	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:50:04.519083023 CEST	8.8.8.8	192.168.2.5	0xf1a2	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:04.552460909 CEST	8.8.8.8	192.168.2.5	0x7614	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:50:04.552460909 CEST	8.8.8.8	192.168.2.5	0x7614	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

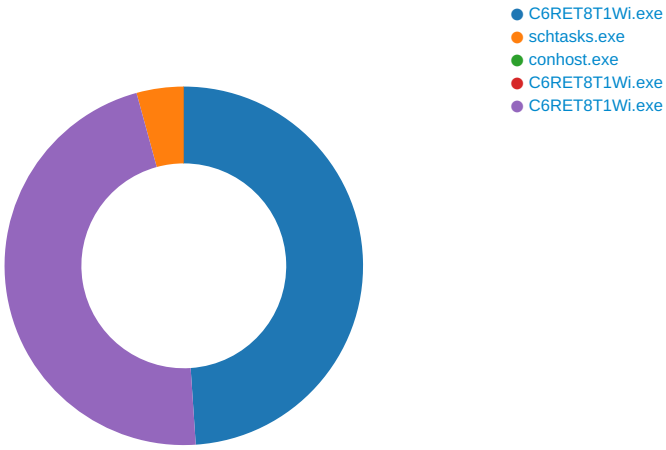
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 10:50:04.956531048 CEST	587	49724	77.88.21.158	192.168.2.5	220 vla3-3dd1bd6927b2.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Apr 8, 2021 10:50:04.957103968 CEST	49724	587	192.168.2.5	77.88.21.158	EHLO 888683
Apr 8, 2021 10:50:05.016228914 CEST	587	49724	77.88.21.158	192.168.2.5	250-vla3-3dd1bd6927b2.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Apr 8, 2021 10:50:05.016913891 CEST	49724	587	192.168.2.5	77.88.21.158	STARTTLS
Apr 8, 2021 10:50:05.075756073 CEST	587	49724	77.88.21.158	192.168.2.5	220 Go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: C6RET8T1Wi.exe PID: 6460 Parent PID: 5628

General

Start time:	10:48:04
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\C6RET8T1Wi.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\C6RET8T1Wi.exe'
Imagebase:	0x900000
File size:	1031168 bytes
MD5 hash:	133B4A863E9A9C74B7320F54ABF199D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.294530199.0000000003F46000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.291906336.0000000002DFC000.00000004.00000001.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	6DD1CF06	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	6DD1CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ePVIisXwKSPaua.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CB6DD66	CopyFileW
C:\Users\user\AppData\Roaming\ePVIisXwKSPaua.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8430.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\C6RET8T1Wi.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8430.tmp	success or wait	1	6CB66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ePVIisXwKSPaua.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0f 3b 6d 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 38 0d 00 00 82 02 00 00 00 00 00 5e 57 0d 00 00 20 00 00 00 60 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....;m`.......... ....P..8..........^W... ...`.. ..@.. ....@................	success or wait	4	6CB6DD66	CopyFileW
C:\Users\user\AppData\Roaming\ePVIisXwKSPaua.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CB6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8430.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6CB61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\C6RET8T1Wi.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	6E02C907	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	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile

Analysis Process: schtasks.exe PID: 6860 Parent PID: 6460

General

Start time:	10:48:15
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ePVIisXwKSPaua' /XML 'C: \Users\user\AppData\Local\Temp\tmp8430.tmp'
Imagebase:	0xac0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8430.tmp	unknown	2	success or wait	1	ACAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8430.tmp	unknown	1652	success or wait	1	ACABD9	ReadFile

Analysis Process: conhost.exe PID: 6888 Parent PID: 6860

General

Start time:	10:48:16
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: C6RET8T1Wi.exe PID: 6968 Parent PID: 6460

General

Start time:	10:48:16
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\C6RET8T1Wi.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\C6RET8T1Wi.exe
Imagebase:	0x350000
File size:	1031168 bytes
MD5 hash:	133B4A863E9A9C74B7320F54ABF199D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: C6RET8T1Wi.exe PID: 7028 Parent PID: 6460

General

Start time:	10:48:17
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\C6RET8T1Wi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\C6RET8T1Wi.exe
Imagebase:	0xcb0000
File size:	1031168 bytes
MD5 hash:	133B4A863E9A9C74B7320F54ABF199D7
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: 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.532839988.00000000031B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.528245994.0000000000402000.00000040.00000001.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	6DD1CF06	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	6DD1CF06	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	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB61B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\a6cfe84f-50a6-4592-a341-880fb1f850b3	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB61B4F	ReadFile

Disassembly

Code Analysis