ID: 756282
Sample Name: REMITTANCE COPY.exe
Cookbook: default.jbs
Time: 23:18:09
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

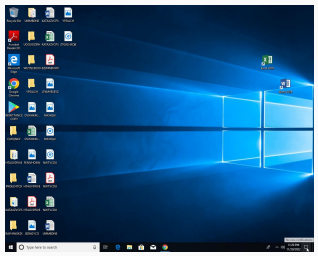
Windows Analysis Report

REMITTANCE COPY.exe

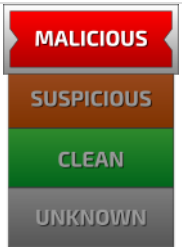
Overview

General Information

Sample Name:	REMITTANCE COPY.exe
Analysis ID:	756282
MD5:	e54ca4f235a687..
SHA1:	b91ce873b8a93b..
SHA256:	6acfd9ea1b8807..
Tags:	agenttesla exe
Infos:	



Detection



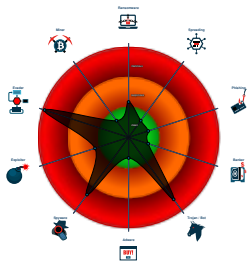
AgentTesla

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
- Sigma detected: Scheduled temp fil…
- 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…
- .NET source code references suspic…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- REMITTANCE COPY.exe (PID: 2820 cmdline: C:\Users\user\Desktop\REMITTANCE COPY.exe MD5: E54CA4F235A6878E6C4913B4DDCBA055)
  - schtasks.exe (PID: 5524 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\FSmZIJwnxoJulr" /XML "C:\Users\user\AppData\Local\Temp\tmp72FE.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5924 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- FSmZIJwnxoJulr.exe (PID: 3804 cmdline: C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe MD5: E54CA4F235A6878E6C4913B4DDCBA055)
  - schtasks.exe (PID: 5020 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\FSmZIJwnxoJulr" /XML "C:\Users\user\AppData\Local\Temp\tmp77E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 64 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 2316 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 5856 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- yGbzOMp.exe (PID: 5256 cmdline: "C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- yGbzOMp.exe (PID: 4296 cmdline: "C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.orogenicgroup-bd.com",
  "Username": "amir.hossain@orogenicgroup-bd.com",
  "Password": "Hossain$3400"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.334243836.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000000.334243836.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000A.00000000.334243836.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31d44:$a13: get_DnsResolver • 0x3043b:$a20: get_LastAccessed • 0x32772:$a27: set_InternalServerPort • 0x32aa7:$a30: set_GuidMasterKey • 0x3054d:$a33: get_Clipboard • 0x3055b:$a34: get_Keyboard • 0x31928:$a35: get_ShiftKeyDown • 0x31939:$a36: get_AltKeyDown • 0x30568:$a37: get_Password • 0x31083:$a38: get_PasswordHash • 0x321a6:$a39: get_DefaultCredentials
00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
10.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
10.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
10.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x34a83:$s10: logins • 0x344fd:$s11: credential • 0x3074d:$g1: get_Clipboard • 0x3075b:$g2: get_Keyboard • 0x30768:$g3: get_Password • 0x31b18:$g4: get_CtrlKeyDown • 0x31b28:$g5: get_ShiftKeyDown • 0x31b39:$g6: get_AltKeyDown
10.0.RegSvcs.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31f44:$a13: get_DnsResolver • 0x3063b:$a20: get_LastAccessed • 0x32972:$a27: set_InternalServerPort • 0x32ca7:$a30: set_GuidMasterKey • 0x3074d:$a33: get_Clipboard • 0x3075b:$a34: get_Keyboard • 0x31b28:$a35: get_ShiftKeyDown • 0x31b39:$a36: get_AltKeyDown • 0x30768:$a37: get_Password • 0x31283:$a38: get_PasswordHash • 0x323a6:$a39: get_DefaultCredentials
1.2.REMITTANCE COPY.exe.3f453a0.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 13 entries

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

.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

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

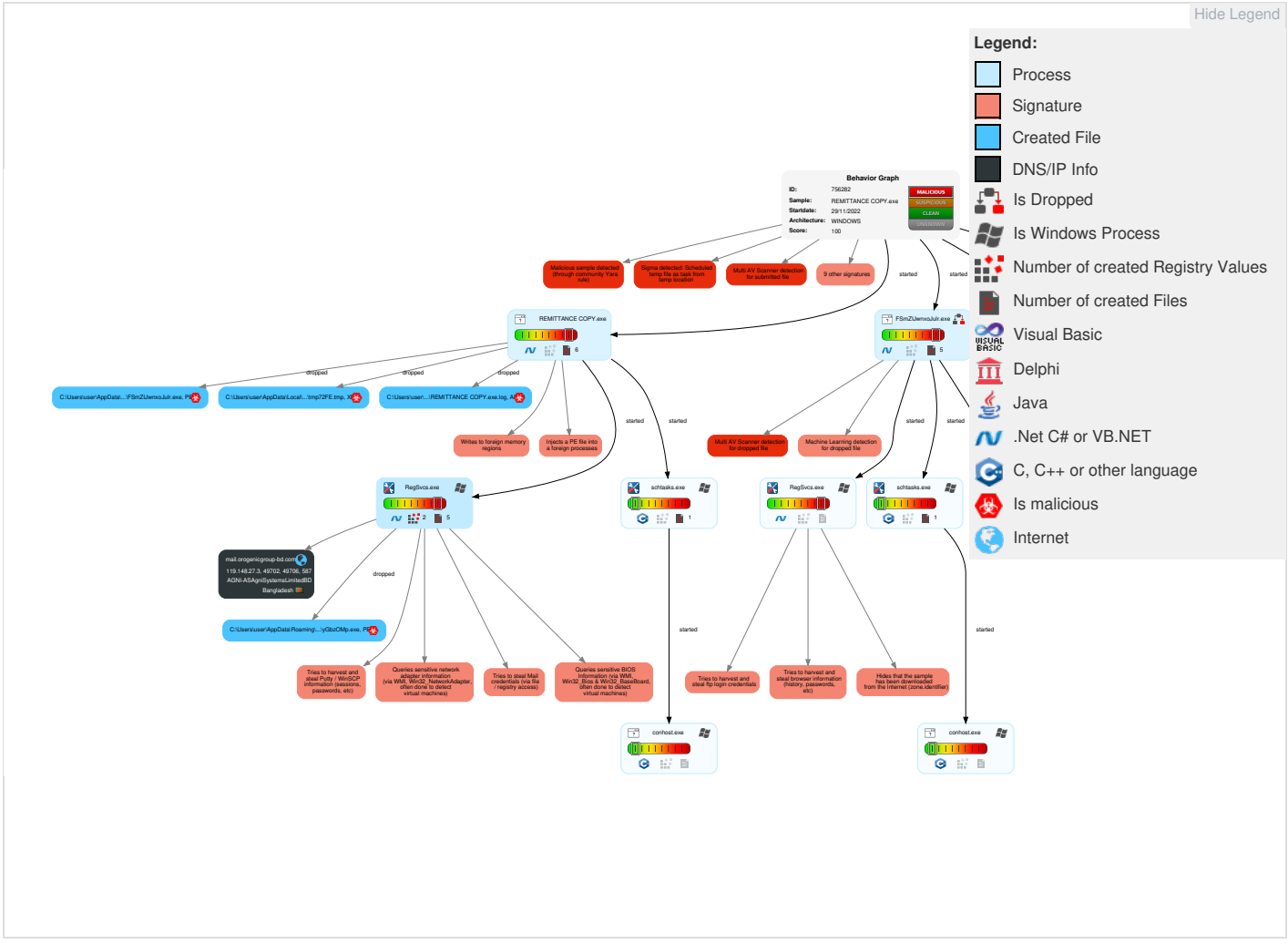
Remote Access Functionality

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 Disable or Modify Tools	2 OS Credential Dumping	1 Account 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	1 Native API	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 File and Directory 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	4 Obfuscated Files or Information	Security Account Manager	1 1 4 System Information 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)	2 3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

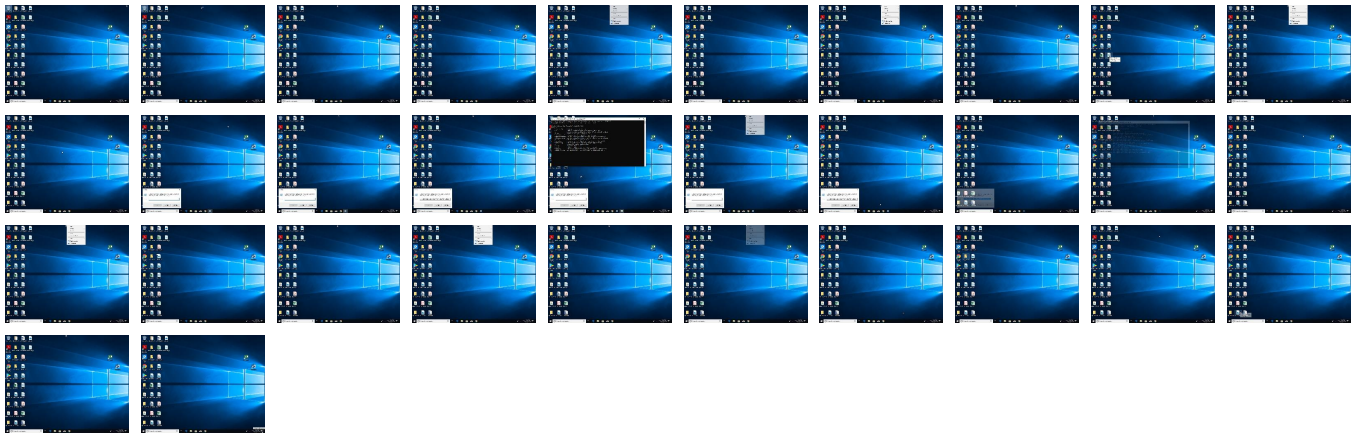
Behavior Graph



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
REMITTANCE COPY.exe	22%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
REMITTANCE COPY.exe	49%	Virustotal		Browse
REMITTANCE COPY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe	22%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe	0%	ReversingLabs		

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com8	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com4	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnorm	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.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://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comK	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://microsoft.co	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.carterandcone.comr	0%	URL Reputation	safe	
http://www.fonts.comW	0%	URL Reputation	safe	
http://www.carterandcone.comn	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comorm	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnX	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cncro	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.O	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnava	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cniUI	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/i-	0%	Avira URL Cloud	safe	
http://BUBAorlAmTfYEKM.org	0%	Avira URL Cloud	safe	
http://mail.orogenicgroup-bd.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.comll	0%	Avira URL Cloud	safe	
http://www.carterandcone.come-d	0%	Avira URL Cloud	safe	
http://www.agfamonotype.E	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna-e8	0%	Avira URL Cloud	safe	
http://fontfabrik.com8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnormX	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnft	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comOp8	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTyp	0%	Avira URL Cloud	safe	
http://JXqRNJ.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.orogenicgroup-bd.com	119.148.27.3	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 0000000A.00000002.429075662.0000000003331000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cncro	REMITTANCE COPY.exe, 00000001.00000003.292241305.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-u	REMITTANCE COPY.exe, 00000001.00000003.292316798.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com8	REMITTANCE COPY.exe, 00000001.00000003.287595714.00000000014BD000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	REMITTANCE COPY.exe, 00000001.00000003.304551334.0000000005DBB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.com4	REMITTANCE COPY.exe, 00000001.00000003.292842829.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	REMITTANCE COPY.exe, 00000001.00000003.293125528.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292709953.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292496560.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292316798.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnorm	REMITTANCE COPY.exe, 00000001.00000003.290883555.0000000005D83000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.290780334.0000000005D83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	REMITTANCE COPY.exe, 00000001.00000003.287595714.00000000014BD000.00000004.00000020.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.335473766.0000005D8F000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.300945403.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.302829024.0000000005D8B000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.300842991.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.301785961.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346313308.0000000005D94000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.305138593.0000000005D8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cniUI	REMITTANCE COPY.exe, 00000001.00000003.291102483.0000000005D91000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersVr	REMITTANCE COPY.exe, 00000001.00000003.304433086.0000000005DBB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	REMITTANCE COPY.exe, 00000001.00000003.288206696.0000000005DBD000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.288094280.0000000005DBD000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.288042735.0000000005DBD000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.287982024.0000000005DBD000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	REMITTANCE COPY.exe, 00000001.00000003.292241305.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	REMITTANCE COPY.exe, 00000001.00000002.337033733.0000000002CF1000.00000004.00000800.00020000.00000000.sdmp, FSmZlJwnxoJulr.exe, 0000000B.00000002.423245986.0000000002A11000.00000004.00000800.00020000.00000000.sdmp	false		high

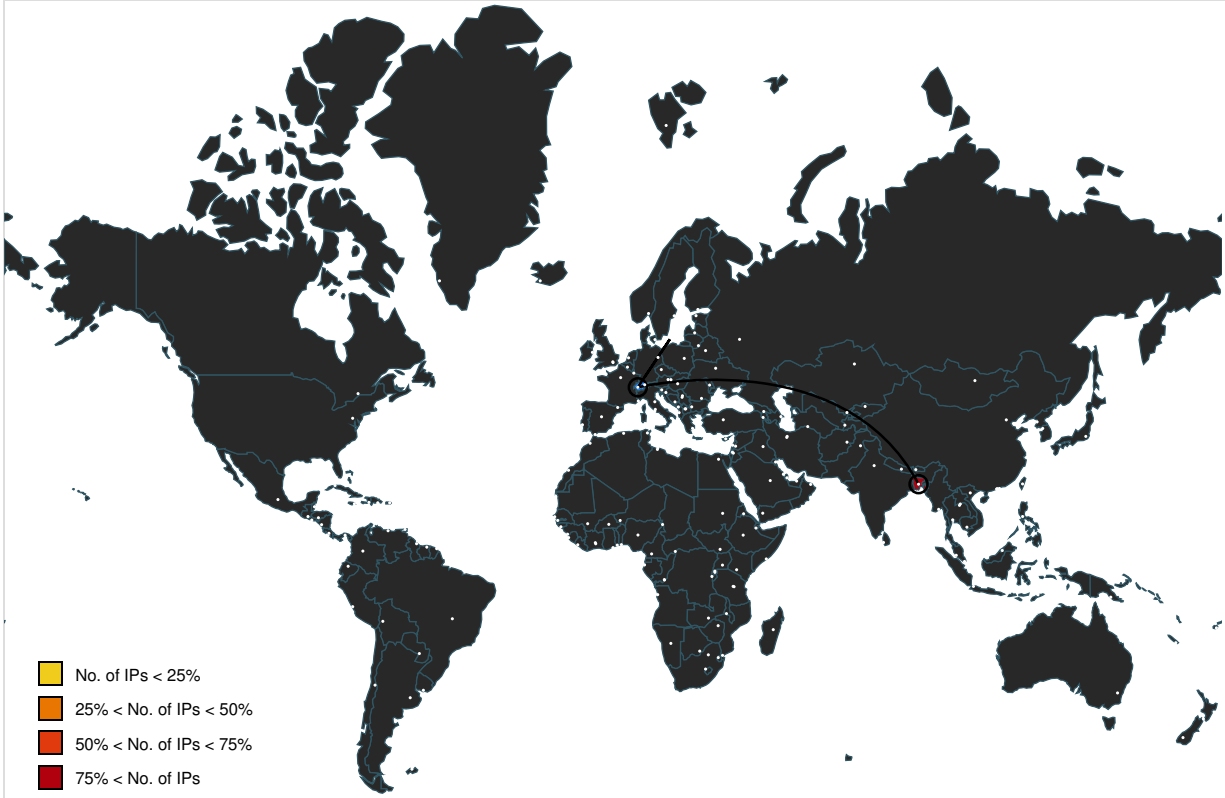
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnf	REMITTANCE COPY.exe, 00000001.00000003.291721850.0000000005D86000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.291634809.0000005D84000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnava	REMITTANCE COPY.exe, 00000001.00000003.290883555.0000000005D83000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.290780334.0000005D83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comK	REMITTANCE COPY.exe, 00000001.00000003.292842829.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292899850.0000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293206606.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293150130.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292552805.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292709953.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292496560.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	REMITTANCE COPY.exe, 00000001.00000003.291989862.0000000005D83000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346689888.0000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.O	REMITTANCE COPY.exe, 00000001.00000003.292552805.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292709953.0000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292496560.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.336773384.00000014B7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comp	REMITTANCE COPY.exe, 00000001.00000003.287595714.00000000014BD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersHr	REMITTANCE COPY.exe, 00000001.00000003.297504908.0000000005DBA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/i-	REMITTANCE COPY.exe, 00000001.00000003.300842991.0000000005D90000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	RegSvcs.exe, 0000000A.00000002.435455318.00000000036BF000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.443833244.0000000006799000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.427101571.0000000001514000.00000004.00000020.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000003.493495830.0000000005F1E000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.571211268.0000000005F22000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.566149106.0000000002B8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://microsoft.co	RegSvcs.exe, 00000013.00000003.493584481.0000000005F50000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.571466727.0000000005F56000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.orogenicgroup-bd.com	RegSvcs.exe, 0000000A.00000002.435455318.00000000036BF000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.566149106.0000000002B8D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://BUBAorlAmTfYEKM.org	RegSvcs.exe, 00000013.00000002.565816116.0000000002B54000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.566299272.0000000002BB0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 0000000A.00000002.429075662.0000000003331000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comr	REMITTANCE COPY.exe, 00000001.00000003.293206606.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comll	REMITTANCE COPY.exe, 00000001.00000003.292842829.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292899850.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293206606.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293150130.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292552805.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292709953.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comW	REMITTANCE COPY.exe, 00000001.00000003.287982024.0000000005DBD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comn	REMITTANCE COPY.exe, 00000001.00000003.292709953.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.come-d	REMITTANCE COPY.exe, 00000001.00000003.292316798.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.agfamonotype.E	REMITTANCE COPY.exe, 00000001.00000003.303771050.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.303959941.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.303624192.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.303913362.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.303859975.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.303721912.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.303668105.0000000005DD2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	REMITTANCE COPY.exe, 00000001.00000003.290883555.0000000005D83000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.290780334.0000000005D83000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cna-e8	REMITTANCE COPY.exe, 00000001.00000003.290883555.0000000005D83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com8	REMITTANCE COPY.exe, 00000001.00000003.288469959.0000000005DBD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comorm	REMITTANCE COPY.exe, 00000001.00000003.292316798.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	REMITTANCE COPY.exe, 00000001.00000003.296476214.0000000005D8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnX	REMITTANCE COPY.exe, 00000001.00000003.292241305.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292842829.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292899850.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293206606.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292552805.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292709953.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292496560.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.292316798.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnormX	REMITTANCE COPY.exe, 00000001.00000003.290883555.0000000005D83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000002.346689888.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnft	REMITTANCE COPY.exe, 00000001.00000003.290883555.0000000005D83000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTyp	REMITTANCE COPY.exe, 00000001.00000003.293206606.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293150130.0000000005D90000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://JXqRNJ.com	RegSvcs.exe, 00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers9	REMITTANCE COPY.exe, 00000001.00000003.299382446.0000000005DBB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersur	REMITTANCE COPY.exe, 00000001.00000003.297651784.0000000005DBB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cno.	REMITTANCE COPY.exe, 00000001.00000003.292241305.0000000005D87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	REMITTANCE COPY.exe, 00000001.00000002.348171972.0000000007105000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.298354512.0000000005DBB000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.298303175.0000000005DBB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers:	REMITTANCE COPY.exe, 00000001.00000003.297504908.0000000005DBA000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comOp8	REMITTANCE COPY.exe, 00000001.00000003.292899850.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293206606.0000000005D87000.00000004.00000800.00020000.00000000.sdmp, REMITTANCE COPY.exe, 00000001.00000003.293150130.0000000005D90000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.148.27.3	mail.orogenicgroup-bd.com	Bangladesh		23923	AGNI-ASAgniSystemsLimitedBD	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756282
Start date and time:	2022-11-29 23:18:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REMITTANCE COPY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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@18/9@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.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
23:19:13	API Interceptor	1x Sleep call for process: REMITTANCE COPY.exe modified
23:19:21	Task Scheduler	Run new task: FSmZIJwnxoJulr path: C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe
23:19:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run yGbzOMp C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe
23:19:35	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run yGbzOMp C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe
23:19:42	API Interceptor	357x Sleep call for process: RegSvcs.exe modified
23:19:47	API Interceptor	1x Sleep call for process: FSmZIJwnxoJulr.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.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:	false
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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, Cultur e=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.Con figuration.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\REMITTANCE COPY.exe.log

Process:	C:\Users\user\Desktop\REMITTANCE 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**
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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, Cultur e=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.Con figuration.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\yGbzOMp.exe.log

Process:	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.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\tmp72FE.tmp

Process:	C:\Users\user\Desktop\REMITTANCE COPY.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.1775098793092065
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3p
MD5:	269DCA092DD3F101BB67595918569AE5
SHA1:	C073FBB9C93034493E7D4F04F5FE1D070E71DD8C
SHA-256:	F2A7823946D9CC784D77659910E2DE48D2FF088AD0DE9FFD935C3EC2A43CEC27
SHA-512:	008E43586B89EF3D717CD3394B3D39B5CD2F42BF9CE9E35E9CDB67269C6F2C3D14D0DA8E61763CE7362BB162EB517681A17578C4D3C0C50749AD4085C00AFD3
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>t

C:\Users\user\AppData\Local\Temp\tmp77E.tmp

Process:	C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.1775098793092065
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVtn:cbhC7ZlNQF/rydbz9l3YODOLNdq3p
MD5:	269DCA092DD3F101BB67595918569AE5
SHA1:	C073FBB9C93034493E7D4F04F5FE1D070E71DD8C
SHA-256:	F2A7823946D9CC784D77659910E2DE48D2FF088AD0DE9FFD935C3EC2A43CEC27
SHA-512:	008E43586B89EF3D717CD3394B3D39B5CD2F42BF9CE9E35E9CDB67269C6F2C3D14D0DA8E61763CE7362BB162EB517681A17578C4D3C0C50749AD4085C00AFD3
Malicious:	false
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\FSmZIJwnxoJulr.exe

Process:	C:\Users\user\Desktop\REMITTANCE COPY.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	866816
Entropy (8bit):	7.470326450965344
Encrypted:	false
SSDEEP:	12288:5RfBQNcgqo2Fr5cE8LHWt/SEdRMA/LyVu6gtY1OaQ3vf8aCmlSVB8Xbc20/HIPPB:r+qopvLC9/L1t+xQFCmQPxHInQ
MD5:	E54CA4F235A6878E6C4913B4DDCBA055
SHA1:	B91CE873B8A93B46EBAC12B5D1E62F3A1A9DD27F
SHA-256:	6ACFD9EA1B88077926A542FD286DA3119B626792F71B09927CA252236245D43A
SHA-512:	989091A3525EA3E57554530DAB20D934E146CAADB4B67A01B612F132758CB5B040529063B3D0EAA3ABD782B04B6C11B7EA51A53330160B3CB75BC313201D49DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....P.....T..... ... .@.. ....@.....K.... .. P..... .....H.....text...4.... ....`.rsrc... P... ...R.....@..@.rel oc.....8.....@..B.....H.....C.....Z(....8.....(....8....*.&~.....*...~....*.b(....8.....(....8.....*...&~.....*...~....*..0..y.....8.... ....E....=...88...(....8....s.....8....*s.....8....s.....8....s.....8....s..... ....9....&8.....0.....~....o.....8.....*8....8.....0.....~....o.....8.....*8....8.....0.....~....o.... ..8....8....8.....*..0..$.....8.....*8....8.....~....o.....8....

C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.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:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6lq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• 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]...

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.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:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F145
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):	7.470326450965344
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:	REMITTANCE COPY.exe
File size:	866816
MD5:	e54ca4f235a6878e6c4913b4ddcba055
SHA1:	b91ce873b8a93b46ebac12b5d1e62f3a1a9dd27f
SHA256:	6acfd9ea1b88077926a542fd286da3119b626792f71b09927ca252236245d43a
SHA512:	989091a3525ea3e57554530dab20d934e146caadb4b67a01b612f132758cb5b040529063b3d0eaa3abd782b04b6c11b7ea51a53330160b3cb75bc313201d49da
SSDEEP:	12288:5RfBQNcgqo2Fr5cE8LHWt/SEdRMA/LyVu6gtY1OaQ3vf8aCmlSVB8Xbc20/HIPPB:r+qopvLC9/L1t+xQFCmQPxHInQ
TLSH:	CB058D5673728863F58F01358495318C6EBCA583A6E6F2076B773A8056027FFFA9CE11

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......c..............P......T........... ... .@.. ....@................................

File Icon

Icon Hash:	4e3e72cace7e9e67

Static PE Info

General

Entrypoint:	0x4d032e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63858DB4 [Tue Nov 29 04:42:28 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd02e0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x5020	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd0297	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xce334	0xce400	False	0.7656486742424242	data	7.462745784487049	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x5020	0x5200	False	0.9108231707317073	data	7.661816841344986	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

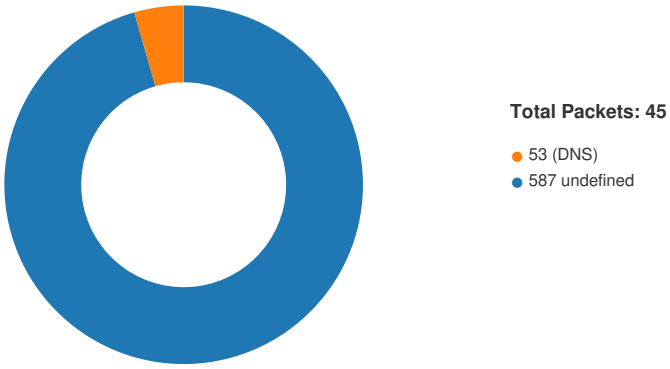
Name	RVA	Size	Type	Language	Country
RT_ICON	0xd2130	0x49b2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xd6ae4	0x14	data		
RT_VERSION	0xd6af8	0x33c	data		
RT_MANIFEST	0xd6e34	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 23:19:44.276021957 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:44.587918043 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:44.588063955 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:48.028115988 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:48.028467894 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:48.340773106 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:48.341048002 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:48.654963970 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:48.714406967 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:48.905726910 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:49.226938963 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:49.226977110 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:49.226994991 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:49.227008104 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:49.227170944 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:49.228629112 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:49.401873112 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:49.570498943 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:49.882066965 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:50.011343956 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:50.270930052 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:50.582626104 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:50.584830999 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:50.897109032 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:51.011531115 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:51.817368984 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:52.167968988 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:52.174232960 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:52.486279011 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:52.486763954 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:52.806159973 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:52.806565046 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:53.117810011 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:53.119280100 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:53.119713068 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:53.120037079 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:19:53.120125055 CET	49702	587	192.168.2.5	119.148.27.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 23:19:53.431646109 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:53.431699991 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:53.431736946 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:53.431775093 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:53.628751040 CET	587	49702	119.148.27.3	192.168.2.5
Nov 29, 2022 23:19:53.714818001 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:12.958915949 CET	49702	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:30.887084961 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:31.192751884 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:31.192878962 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:31.505937099 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:31.508374929 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:31.814308882 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:31.814596891 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:32.122059107 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.141771078 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:32.462547064 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.462631941 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.462693930 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.462743998 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.462865114 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:32.462865114 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:32.465277910 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.482307911 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:32.788265944 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:32.843096972 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:32.866729021 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:33.172338009 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:33.172903061 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:33.478811026 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:33.479494095 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:33.824166059 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:33.862101078 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:33.862700939 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:34.168560028 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:34.168592930 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:34.169233084 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:34.484185934 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:34.484831095 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:34.791023016 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:34.792371035 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:34.792440891 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:34.792514086 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:34.792606115 CET	49706	587	192.168.2.5	119.148.27.3
Nov 29, 2022 23:20:35.098450899 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:35.098514080 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:35.098743916 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:35.206922054 CET	587	49706	119.148.27.3	192.168.2.5
Nov 29, 2022 23:20:35.249504089 CET	49706	587	192.168.2.5	119.148.27.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 23:19:44.056919098 CET	60649	53	192.168.2.5	8.8.8.8
Nov 29, 2022 23:19:44.226650953 CET	53	60649	8.8.8.8	192.168.2.5
Nov 29, 2022 23:20:30.696413040 CET	61452	53	192.168.2.5	8.8.8.8
Nov 29, 2022 23:20:30.867413998 CET	53	61452	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 23:19:44.056919098 CET	192.168.2.5	8.8.8.8	0x4265	Standard query (0)	mail.orogenicgroup-bd.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 23:20:30.696413040 CET	192.168.2.5	8.8.8.8	0xa6f0	Standard query (0)	mail.orogenicgroup-bd.com	A (IP address)	IN (0x0001)	false

DNS Answers

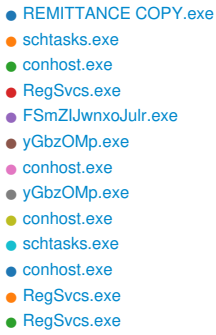
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 23:19:44.226650953 CET	8.8.8.8	192.168.2.5	0x4265	No error (0)	mail.orogenicgroup-bd.com		119.148.27.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 23:20:30.867413998 CET	8.8.8.8	192.168.2.5	0xa6f0	No error (0)	mail.orogenicgroup-bd.com		119.148.27.3	A (IP address)	IN (0x0001)	false

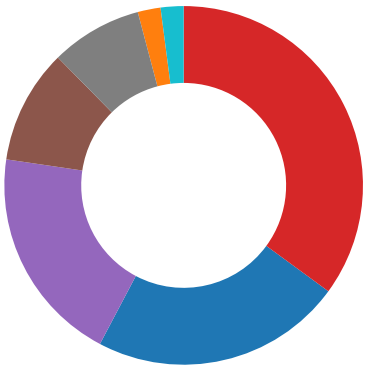
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 23:19:48.028115988 CET	587	49702	119.148.27.3	192.168.2.5	220-panel2.agni.com ESMTP Exim 4.95 #2 Wed, 30 Nov 2022 04:19:47 +0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 23:19:48.028467894 CET	49702	587	192.168.2.5	119.148.27.3	EHLO 618321
Nov 29, 2022 23:19:48.340773106 CET	587	49702	119.148.27.3	192.168.2.5	250-panel2.agni.com Hello 618321 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Nov 29, 2022 23:19:48.341048002 CET	49702	587	192.168.2.5	119.148.27.3	STARTTLS
Nov 29, 2022 23:19:48.654963970 CET	587	49702	119.148.27.3	192.168.2.5	220 TLS go ahead
Nov 29, 2022 23:20:31.505937099 CET	587	49706	119.148.27.3	192.168.2.5	220-panel2.agni.com ESMTP Exim 4.95 #2 Wed, 30 Nov 2022 04:20:31 +0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 23:20:31.508374929 CET	49706	587	192.168.2.5	119.148.27.3	EHLO 618321
Nov 29, 2022 23:20:31.814308882 CET	587	49706	119.148.27.3	192.168.2.5	250-panel2.agni.com Hello 618321 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Nov 29, 2022 23:20:31.814596891 CET	49706	587	192.168.2.5	119.148.27.3	STARTTLS
Nov 29, 2022 23:20:32.122059107 CET	587	49706	119.148.27.3	192.168.2.5	220 TLS go ahead

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: REMITTANCE COPY.exe PID: **2820**, Parent PID: **3324**

General

Target ID:	1
Start time:	23:18:56
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\REMITTANCE COPY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\REMITTANCE COPY.exe
Imagebase:	0x930000
File size:	866816 bytes
MD5 hash:	E54CA4F235A6878E6C4913B4DDCBA055
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: 00000001.00000002.340679547.0000000003E1C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.340679547.0000000003E1C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.340679547.0000000003E1C000.00000004.00000800.00020000.00000000.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	6CBCCF06	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	6CBCCF06	unknown
C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BA11E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp72FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BA17038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REMITTANCE COPY.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp72FE.tmp	success or wait	1	6BA16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe	0	866816	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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 50 00 00 fd 0c 00 00 54 00 00 00 00 00 00 2e 03 0d 00 00 20 00 00 00 20 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 fd 0d 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.$PELcPT. @ @	success or wait	1	6BA11B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp72FE.tmp	0	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	6BA11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\REMITTANCE 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	6CEDC907	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	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA11B4F	ReadFile
C:\Users\user\Desktop\REMITTANCE COPY.exe	unknown	866816	success or wait	1	6BA11B4F	ReadFile

Analysis Process: schtasks.exe PID: **5524**, Parent PID: **2820**

General

Target ID:	8
Start time:	23:19:19
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\FSmZIJwnxoJulr" /XML "C:\Users\user\AppData\Local\Temp\tmp72FE.tmp
Imagebase:	0x9c0000
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\tmp72FE.tmp	unknown	2	success or wait	1	9CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp72FE.tmp	unknown	1652	success or wait	1	9CABD9	ReadFile

Analysis Process: conhost.exe PID: **5624**, Parent PID: **5524**

General

Target ID:	9
Start time:	23:19:19
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5924**, Parent PID: **2820**

General

Target ID:	10
Start time:	23:19:19
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xee0000
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: 0000000A.00000000.334243836.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.334243836.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000A.00000000.334243836.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.429075662.0000000003331000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.429075662.0000000003331000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6CBCCF06	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	6CBCCF06	unknown
C:\Users\user\AppData\Roaming\yGbzOMp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BA1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.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	6BA1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFF93.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BA17038	GetTempFileNameW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.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 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	6BA1DD66	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	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6BA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6BA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CBA5705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BA11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	6BA11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BA11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BA11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BA11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6BA11B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	yGbzOMp	unicode	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe	success or wait	1	6BA1646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	yGbzOMp	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BA1DE2E	RegSetValueExW

Analysis Process: FSmZIJwnxoJulr.exe PID: **3804**, Parent PID: **1084**

General

Target ID:	11
Start time:	23:19:21
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\FSmZIJwnxoJulr.exe
Imagebase:	0x650000
File size:	866816 bytes
MD5 hash:	E54CA4F235A6878E6C4913B4DDCBA055
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6CBCCF06	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	6CBCCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp77E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BA17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FSmZIJwnxoJulr.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp77E.tmp	success or wait	1	6BA16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp77E.tmp	0	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	6BA11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FSmZIJwnxoJulr.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	6CEDC907	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	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA11B4F	ReadFile

Analysis Process: yGbzOMp.exe PID: **5256**, Parent PID: **3324**

General

Target ID:	12
Start time:	23:19:35
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe"
Imagebase:	0xed0000
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%, 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\yGbzOMp.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEDC78D	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	6BA11B4F	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	6BA11B4F	WriteFile
\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 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 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 2f	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. /	success or wait	3	6BA11B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BA11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yGbzOMp.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	6CEDC907	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	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBACA54	ReadFile

Analysis Process: conhost.exe PID: **5612**, Parent PID: **5256**

General

Target ID:	13
Start time:	23:19:35
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: yGbzOMp.exe PID: **4296**, Parent PID: **3324**

General

Target ID:	14
Start time:	23:19:43
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe"
Imagebase:	0x430000
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	6BA11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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 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	6BA11B4F	WriteFile
\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 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 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 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	6BA11B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BA11B4F	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	6CBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBACA54	ReadFile

Analysis Process: conhost.exe PID: **1008**, Parent PID: **4296**

General

Target ID:	15
Start time:	23:19:43
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: schtasks.exe PID: **5020**, Parent PID: **3804**

General

Target ID:	16
Start time:	23:19:58
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\FSmZIJwnxoJulr" /XML "C:\Users\user\AppData\Local\Temp\tmp77E.tmp
Imagebase:	0x7ff7c8a30000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
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\tmp77E.tmp	unknown	2	success or wait	1	9CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp77E.tmp	unknown	1652	success or wait	1	9CABD9	ReadFile

Analysis Process: conhost.exe PID: **64**, Parent PID: **5020**

General

Target ID:	17
Start time:	23:19:58
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: RegSvcs.exe PID: **2316**, Parent PID: **3804**

General

Target ID:	18
Start time:	23:19:58
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}

Imagebase:	0x3f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **5856**, Parent PID: **3804**

General	
Target ID:	19
Start time:	23:19:59
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x500000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.560149553.00000000027CC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly