ID: 635135
Sample Name: VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
Cookbook: default.jbs
Time: 15:34:08
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

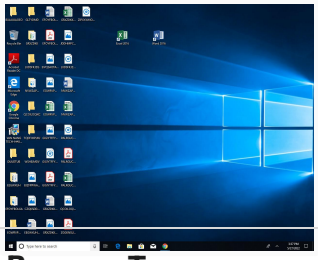
Windows Analysis Report

VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe

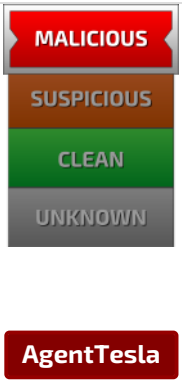
Overview

General Information

Sample Name:	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
Analysis ID:	635135
MD5:	9c4dccd93ae444..
SHA1:	c9caa8238fc581…
SHA256:	78990521b8fd82..
Tags:	exe
Infos:	



Detection



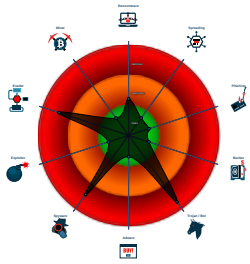
AgentTesla

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 Telegram RAT
- Yara detected AgentTesla
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Contains functionality to register a lo…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe (PID: 6448 cmdline: "C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe" MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
  - VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe (PID: 6472 cmdline: C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
- 231.exe (PID: 6296 cmdline: "C:\Users\user\AppData\Roaming\231\231.exe" MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
- 231.exe (PID: 6744 cmdline: "C:\Users\user\AppData\Roaming\231\231.exe" MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
  - 231.exe (PID: 6496 cmdline: C:\Users\user\AppData\Roaming\231\231.exe MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
- 231.exe (PID: 5000 cmdline: "C:\Users\user\AppData\Roaming\231\231.exe" MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
- 231.exe (PID: 6908 cmdline: "C:\Users\user\AppData\Roaming\231\231.exe" MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
  - 231.exe (PID: 476 cmdline: C:\Users\user\AppData\Roaming\231\231.exe MD5: 9C4DCCD93AE4440B5DBC580A85F53B94)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1338829993:AAGkgJ80sLaIYwBfp79Ps5EtdSP1XH6jBV8/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "-449207656",
  "Chat URL": "https://api.telegram.org/bot1338829993:AAGkgJ80sLaIYwBfp79Ps5EtdSP1XH6jBV8/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.253607505.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.253607505.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001B.00000002.515903120.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001B.00000002.515903120.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001A.00000002.367814812.00000000037D9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 59 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
27.0.231.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
27.0.231.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
27.0.231.exe.400000.10.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
27.0.231.exe.400000.10.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30433:$s1: get_kbok • 0x30d67:$s2: get_CHoo • 0x319c2:$s3: set_passwordIsSet • 0x30237:$s4: get_enableLog • 0x34957:$s8: torbrowser • 0x3333a:$s10: logins • 0x32c08:$s11: credential • 0x2f622:$g1: get_Clipboard • 0x2f630:$g2: get_Keyboard • 0x2f63d:$g3: get_Password • 0x30c15:$g4: get_CtrlKeyDown • 0x30c25:$g5: get_ShiftKeyDown • 0x30c36:$g6: get_AltKeyDown
21.0.231.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 109 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

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

Networking

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

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

Boot Survival

Creates autostart registry keys with suspicious names

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

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

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

Remote Access Functionality

Yara detected Telegram RAT

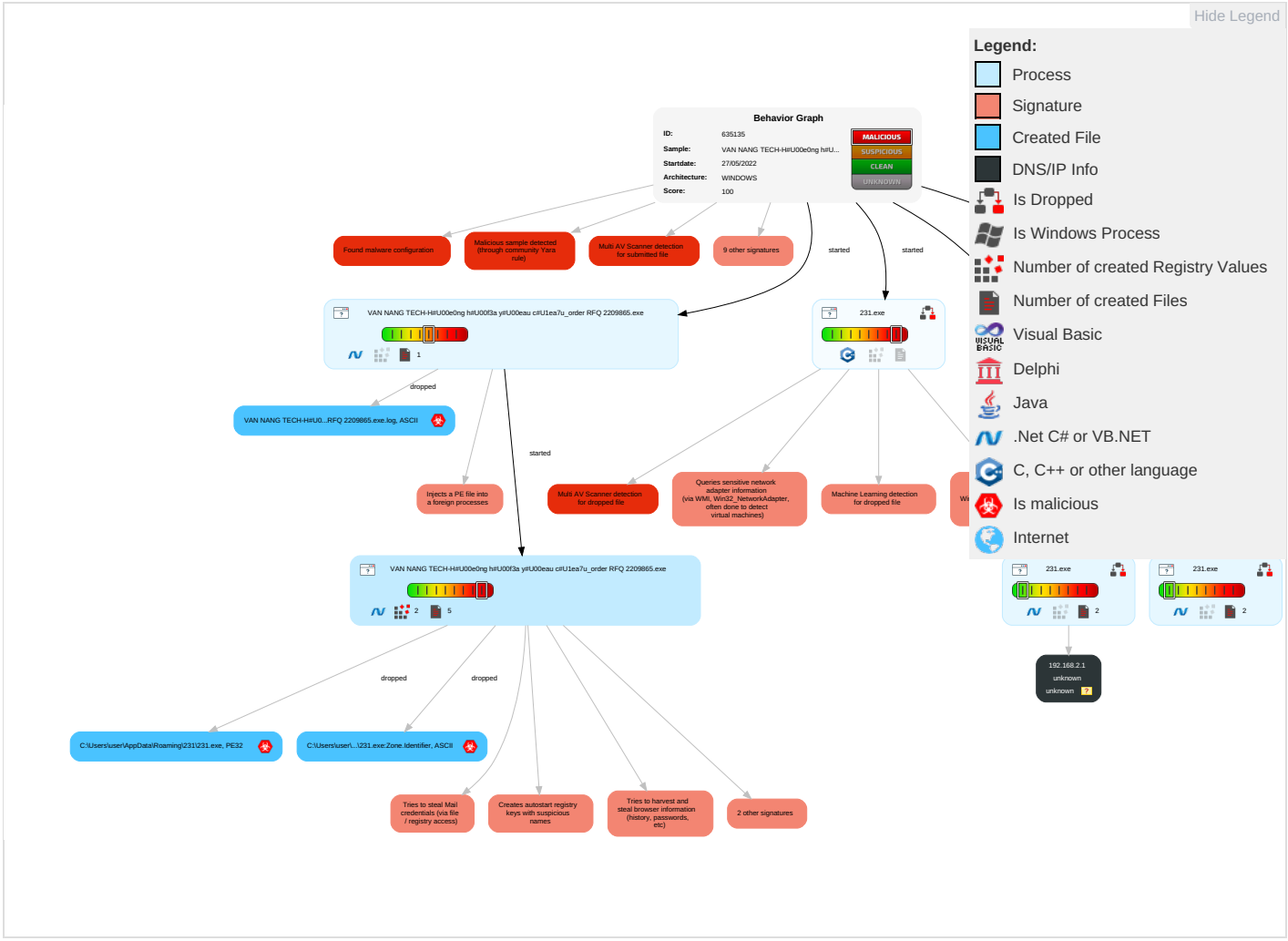
Yara detected AgentTesla

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Valid Accounts	1 Valid Accounts	1 Deobfuscate/Decode Files or Information	2 1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	2 Obfuscated Files or Information	Security Account Manager	2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 1 Process Injection	3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	2 1 1 Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Valid Accounts	DCSync	1 System Owner/User 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 Access Token Manipulation	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 3 1 Virtualization/Sandbox Evasion	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 1 1 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Hidden Files and Directories	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

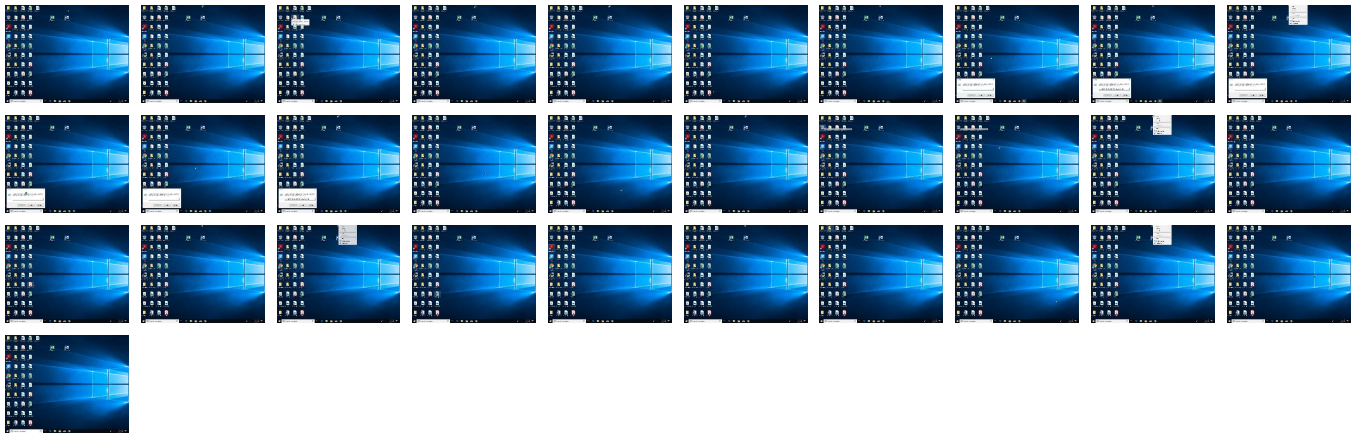
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe	51%	Virustotal		Browse
VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\231\231.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\231\231.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.0.231.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.2.231.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.0.231.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.0.231.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.0.231.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.0.231.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.0.231.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.0.231.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.0.231.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.0.231.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.2.231.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.0.231.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dsssdsa.fa)Uri	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/Reporting/UploadReport2	0%	URL Reputation	safe	
http://https://dsssdsa.fa	0%	Avira URL Cloud	safe	
http://www.smartassembly.com/webservices/Reporting/	0%	URL Reputation	safe	
http://kjcOuF.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/UploadReportLogin/	0%	URL Reputation	safe	
http://www.smartassembly.com/webservices/UploadReportLogin/GetServerURL	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

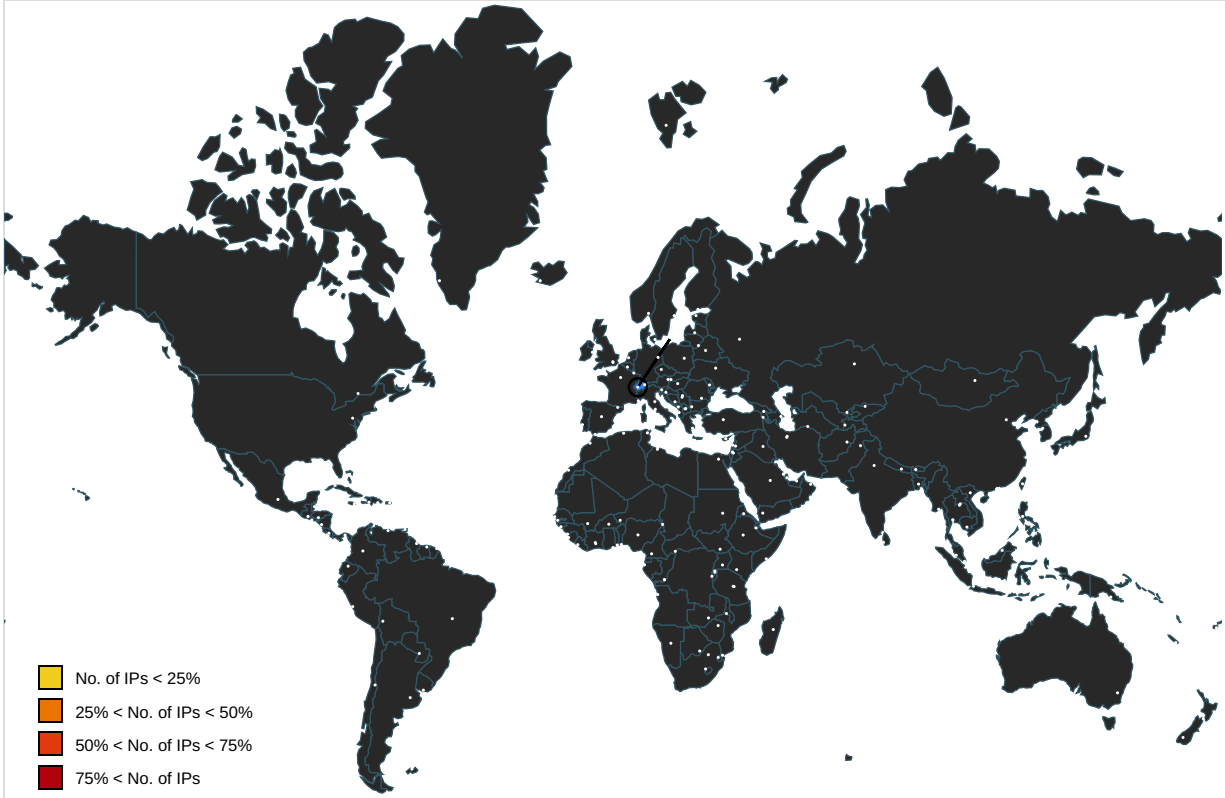
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dsssdsa.fa)Uri	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 231.exe.1.dr	false	• Avira URL Cloud: safe	low
http://127.0.0.1:HTTP/1.1	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 00000001.00000002.518792616.0000000002901000.00000004.00000800.00020000.00000000.sdmp, 231.exe, 00000015.00000002.371598282.00000000003061000.00000004.00000800.00020000.00000000.sdmp, 231.exe, 0000001B.00000002.518793277.0000000003381000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	231.exe, 0000001B.00000002.518793277.000 0000003381000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 000000 01.00000002.518792616.0000000002901000.0 0000004.00000800.00020000.00000000.sdmp, 231.exe, 00000015.00000002.371598282.00 00000003061000.00000004.00000800.0002000 0.00000000.sdmp, 231.exe, 0000001B.00000 002.518793277.0000000003381000.00000004. 00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://api.telegram.org/bot1338829993:AAGkgJ80sLaIYwBfp79Ps5EtdSP1XH6jBV8/sendDocumentdocument-----	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 000000 01.00000002.518792616.0000000002901000.0 0000004.00000800.00020000.00000000.sdmp, 231.exe, 00000015.00000002.371598282.00 00000003061000.00000004.00000800.0002000 0.00000000.sdmp, 231.exe, 0000001B.00000 002.518793277.0000000003381000.00000004. 00000800.00020000.00000000.sdmp	false		high
http://sawebservice.red-gate.com/	231.exe, 231.exe, 0000001B.00000000.3549 38229.0000000000FE2000.00000002.00000001 .01000000.00000008.sdmp, VAN NANG TECH-H #U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 231.exe.1.dr	false		high
http:// www.smartassembly.com/webservices/Reporting/UploadReport2	231.exe, 231.exe, 0000001B.00000000.3549 38229.0000000000FE2000.00000002.00000001 .01000000.00000008.sdmp, VAN NANG TECH-H #U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 231.exe.1.dr	false	• URL Reputation: safe	unknown
http://https://dsssdsa.fa	231.exe	false	• Avira URL Cloud: safe	unknown
http:// www.smartassembly.com/webservices/Reporting/	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 231.exe.1.dr	false	• URL Reputation: safe	unknown
http://kjcOuF.com	231.exe, 0000001B.00000002.518793277.000 0000003381000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 000000 00.00000002.261040909.00000000044D9000.0 0000004.00000800.00020000.00000000.sdmp, VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 00000 001.00000000.253607505.0000000000402000. 00000040.00000400.00020000.00000000.sdmp, 231.exe, 00000014.00000002.346293586.0 0000000003909000.00000004.00000800.000200 00.00000000.sdmp, 231.exe, 00000015.0000 0000.340208778.0000000000402000.00000040 .00000400.00020000.00000000.sdmp, 231.exe, 0000001A.00000002.367814812.000000000 37D9000.00000004.00000800.00020000.00000 000.sdmp, 231.exe, 0000001B.00000002.515 903120.0000000000402000.00000040.0000040 0.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// www.smartassembly.com/webservices/UploadReportLogin/	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 231.exe.1.dr	false	• URL Reputation: safe	unknown
http:// www.smartassembly.com/webservices/UploadReportLogin/GetServerURL	231.exe, 231.exe, 0000001B.00000000.3549 38229.0000000000FE2000.00000002.00000001 .01000000.00000008.sdmp, VAN NANG TECH-H #U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 231.exe.1.dr	false	• URL Reputation: safe	unknown
http:// https://api.telegram.org/bot1338829993:AAGkgJ80sLaIYwBfp79Ps5EtdSP1XH6jBV8/	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 000000 00.00000002.261040909.00000000044D9000.0 0000004.00000800.00020000.00000000.sdmp, VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe, 00000 001.00000000.253607505.0000000000402000. 00000040.00000400.00020000.00000000.sdmp, 231.exe, 00000014.00000002.346293586.0 0000000003909000.00000004.00000800.000200 00.00000000.sdmp, 231.exe, 00000015.0000 0000.340208778.0000000000402000.00000040 .00000400.00020000.00000000.sdmp, 231.exe, 0000001A.00000002.367814812.000000000 37D9000.00000004.00000800.00020000.00000 000.sdmp, 231.exe, 0000001B.00000002.515 903120.0000000000402000.00000040.0000040 0.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635135
Start date and time: 27/05/202215:34:08	2022-05-27 15:34:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.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:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@11/4@0/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.8%) • Quality average: 67.1% • Quality standard deviation: 37.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, BackgroundTransferHost.exe, consent.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- 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 231.exe, PID 5000 because there are no executed function
- Execution Graph export aborted for target 231.exe, PID 6296 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:35:28	API Interceptor	730x Sleep call for process: VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe modified
15:35:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 231 C:\Users\user\AppData\Roaming\231\231.exe
15:35:48	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 231 C:\Users\user\AppData\Roaming\231\231.exe
15:36:08	API Interceptor	396x Sleep call for process: 231.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\231.exe.log	
Process:	C:\Users\user\AppData\Roaming\231\231.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.345981753770044
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLUE4K5E4Ks2wKDE4KhK3VZ9pKhk
MD5:	044A637E42FE9A819D7E43C8504CA769
SHA1:	6FCA27B1A571B73563C8424C84F4F64F3CBCBE2F
SHA-256:	E88E04654826CE00CC7A840745254164DDBD175066D6E4EA6858BF0FE463EBB4
SHA-512:	C9A74FA4154FA5E5951B0EEAC5330CA4BAC981FF9AD24C08575A76AD5D99CFB68556B9857C9C8209A1BFCB43F82E00F14962987A18A92A715F45AD0D4E4A71 C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_3 2\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.log	
Process:	C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.345981753770044
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLUE4K5E4Ks2wKDE4KhK3VZ9pKhk
MD5:	044A637E42FE9A819D7E43C8504CA769
SHA1:	6FCA27B1A571B73563C8424C84F4F64F3CBCBE2F
SHA-256:	E88E04654826CE00CC7A840745254164DDBD175066D6E4EA6858BF0FE463EBB4
SHA-512:	C9A74FA4154FA5E5951B0EEAC5330CA4BAC981FF9AD24C08575A76AD5D99CFB68556B9857C9C8209A1BFCB43F82E00F14962987A18A92A715F45AD0D4E4A71 C
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_3 2\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Roaming\231\231.exe	
Process:	C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	316416
Entropy (8bit):	7.709057445187231
Encrypted:	false
SSDEEP:	6144:0n5tMcEzK2WHKjlc+m5+n9X029Vx+7HIuEmQEBYOqgHwWg4bR2:0n5tMVu6W+m5EERQ1gQWLR
MD5:	9C4DCCD93AE4440B5DBC580A85F53B94
SHA1:	C9CAA8238FC581CE3504A8513A2E3EE4701E9274
SHA-256:	78990521B8FD82B6F0EAE446FC6D3F4763764BD85F8820DC7D0A3EEB50D8933B
SHA-512:	B0AD33F099EB3EB31131AF80C4D72838E7923373D1B114BD2591A69C0BED73A5CA00FB26A1ED19F76020399D6CA90A91C581A7044D2404EA294657DC5C56A98 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...2..b..... .....@.. ....@.....}...J..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H..... ....w.....%.....0..d.....-=r...p+7+<+=+>+C.+C+ +B+C.+C.,..o.....(.....%,.X.-....,...i2.*s....+..+..+.o....+..+ ..+..+..+..+..0.._.....+2+3,.+6.+6.-...+.+3,.r...p+-z.-.+.+/.-.,.+/.(....*.+.(....+..+.(....+..+.s....+..+.(....+..+...0..X.....-.++.-/&+/r5..p+++0rI..p+,.-..-.++.G.1...+%.-.*s....+..+..+.o....+ ..+.o....+..+.o....+..0.....+.+.+.+.*s....+..+..+.o....+.....+.&*(....+..0.....rQ..prq..p8....&r...

C:\Users\user\AppData\Roaming\231\231.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.709057445187231
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:	VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
File size:	316416
MD5:	9c4dccd93ae4440b5dbc580a85f53b94
SHA1:	c9caa8238fc581ce3504a8513a2e3ee4701e9274
SHA256:	78990521b8fd82b6f0eae446fc6d3f4763764bd85f8820dc7d0a3eeb50d8933b
SHA512:	b0ad33f099eb3eb31131af80c4d72838e7923373d1b114bd2591a69c0bed73a5ca00fb26a1ed19f76020399d6ca90a91c581a7044d2404ea294657dc5c56a981
SSDEEP:	6144:0n5tMcEzK2WHKjlc+m5+n9X029Vx+7HIuEmQEBYOqgHwWg4bR2:0n5tMVu6W+m5EERQ1gQWLR
TLSH:	2164021457DD9A42C6FE087AC4D204B45732A43A7CABE75FADCC112D2B337C64922B9B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...2..b..... .....@.. ....@.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x44d2c7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

Time Stamp:	0x628F9F32 [Thu May 26 15:39:30 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4d27d	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4e000	0x1b02	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x50000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x4b2cd	0x4b400	False	0.850991486711	data	7.7588479864	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4e000	0x1b02	0x1c00	False	0.322684151786	data	4.27348228895	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x50000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4e084	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x4e1d0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x4e75c	0x2e8	data		
RT_ICON	0x4ea68	0x8a8	data		
RT_GROUP_ICON	0x4f35e	0x3e	data		
RT_VERSION	0x4f3d8	0x4f4	data		
RT_MANIFEST	0x4f908	0x1fa	XML 1.0 document, ASCII text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

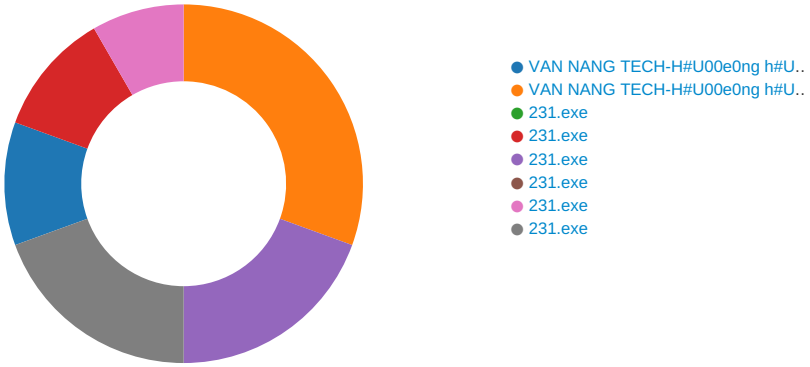
Description	Data
LegalCopyright	
FileVersion	
CompanyName	SoftOrbits
Comments	This installation was built with Inno Setup.
ProductName	Add Text to Video PRO
ProductVersion	1.4
FileDescription	Add Text to Video PRO Setup
Translation	0x0000 0x04b0

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe PID: **6448**, Parent PID: **5248**

General

Target ID:	0
Start time:	15:35:11
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe"
Imagebase:	0xfb0000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
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: 00000000.00000002.261040909.00000000044D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.261040909.00000000044D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA6C78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe.log	0	520	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 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	6DA6C907	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	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D735705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D73CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6903DE	ReadFile

Analysis Process: VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe PID: **6472**, Parent PID: **6448**

General

Target ID:	1
Start time:	15:35:13
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\VAN NANG TECH-H#U00e0ng h#U00f3a y#U00eau c#U1ea7u_order RFQ 2209865.exe
Imagebase:	0x510000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.253607505.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.253607505.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.254906680.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.254906680.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.518792616.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000002.518792616.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.518792616.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000001.00000002.518792616.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.519047597.00000000029B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.515882418.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.515882418.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.253095019.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.253095019.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.254062993.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.254062993.0000000000402000.00000040.00000400.00020000.00000000.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	6D75CF06	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	6D75CF06	unknown
C:\Users\user\AppData\Roaming\231	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C5ABEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\231\231.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	6C5ADD66	CopyFileW
C:\Users\user\AppData\Roaming\231\231.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C5ADD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

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\231\231.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 32 fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 04 00 00 1e 00 00 00 00 00 00 fd fd 04 00 00 20 00 00 00 fd 04 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 20 05 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.$PEL2b @ @	success or wait	3	6C5ADD66	CopyFileW
C:\Users\user\AppData\Roaming\231\231.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	6C5ADD66	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	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D735705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D73CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C5A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C5A1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	231	unicode	C:\Users\user\AppData\Roaming\231\231.exe	success or wait	1	6C5A646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	231	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C5ADE2E	RegSetValueExW

Analysis Process: 231.exe PID: **6296**, Parent PID: **3968**

General

Target ID:	15
Start time:	15:35:48
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\231\231.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\231\231.exe"
Imagebase:	0xce0000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 81%, ReversingLabs
Reputation:	low

Analysis Process: 231.exe PID: **6744**, Parent PID: **3968**

General

Target ID:	20
Start time:	15:35:52
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\231\231.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\231\231.exe"
Imagebase:	0x390000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
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: 00000014.00000002.346293586.0000000003909000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.346293586.0000000003909000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\231.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA6C78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\231.exe.log	0	520	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 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	6DA6C907	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	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D735705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D73CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6903DE	ReadFile

Analysis Process: 231.exe PID: **6496**, Parent PID: **6744**

General

Target ID:	21
Start time:	15:35:53
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\231\231.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\231\231.exe
Imagebase:	0xd90000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
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: 00000015.00000000.340208778.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000015.00000000.340208778.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.370461628.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000015.00000002.370461628.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000000.339810964.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000015.00000000.339810964.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000000.339477661.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000015.00000000.339477661.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000000.339160538.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000015.00000000.339160538.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.371598282.0000000003061000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000015.00000002.371598282.0000000003061000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.371598282.0000000003061000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000015.00000002.371598282.0000000003061000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6D75CF06	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	6D75CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D735705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D73CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C5A1B4F	ReadFile

Analysis Process: 231.exe PID: **5000**, Parent PID: **3968**

General

Target ID:	22
Start time:	15:35:57
Start date:	27/05/2022

Path:	C:\Users\user\AppData\Roaming\231\231.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\231\231.exe"
Imagebase:	0x570000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 231.exe PID: **6908**, Parent PID: **3968**

General

Target ID:	26
Start time:	15:35:59
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\231\231.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\231\231.exe"
Imagebase:	0x2e0000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
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: 0000001A.00000002.367814812.00000000037D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000002.367814812.00000000037D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D735705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D73CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6903DE	ReadFile

Analysis Process: 231.exe PID: **476**, Parent PID: **6908**

General

Target ID:	27
Start time:	15:36:01
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\231\231.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\231\231.exe
Imagebase:	0xfe0000
File size:	316416 bytes
MD5 hash:	9C4DCCD93AE4440B5DBC580A85F53B94
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: 0000001B.00000002.515903120.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001B.00000002.515903120.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000000.356681363.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001B.00000000.356681363.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000000.355665401.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001B.00000000.355665401.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000000.356011581.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001B.00000000.356011581.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000000.356342873.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001B.00000000.356342873.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000002.518793277.0000000003381000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000001B.00000002.518793277.0000000003381000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001B.00000002.518793277.0000000003381000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 0000001B.00000002.518793277.0000000003381000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6D75CF06	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	6D75CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D735705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D73CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D735705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C5A1B4F	ReadFile

Disassembly

No disassembly