ID: 344851
Sample Name: HTG-9087650.exe
Cookbook: default.jbs
Time: 09:26:49
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

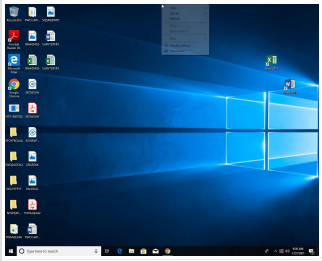
Analysis Report HTG-9087650.exe

Overview

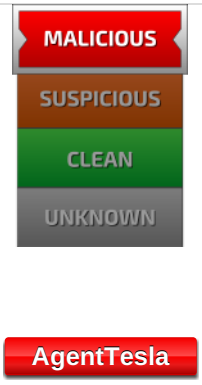
General Information

Sample Name:	HTG-9087650.exe
Analysis ID:	344851
MD5:	dcb57041d46889..
SHA1:	7c9a62b778db3d..
SHA256:	b9b2c05c193a6d..
Tags:	exe

Most interesting Screenshot:



Detection



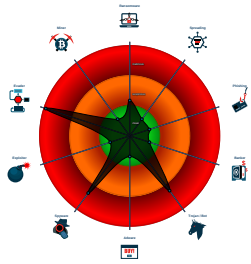
AgentTesla

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Found evasive API chain (trying to d…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- HTG-9087650.exe (PID: 6792 cmdline: 'C:\Users\user\Desktop\HTG-9087650.exe' MD5: DCB57041D46889E94CF100E4E0325176)
  - xidczjbzj.exe (PID: 6824 cmdline: C:\Users\user\AppData\Local\Temp\xidczjbzj.exe C:\Users\user\AppData\Local\Temp\syioy.pm MD5: C56B5F0201A3B3DE53E561FE76912BFD)
    - v04mldbd.exe (PID: 6852 cmdline: C:\Users\user\AppData\Local\Temp\xidczjbzj.exe C:\Users\user\AppData\Local\Temp\syioy.pm MD5: 535DD1329AEF11BF4654B3270F026D5B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "ExiSLgKrA56omq",
  "URL: ": "http://flF3mJWUOO3.net",
  "To: ": "",
  "ByHost: ": "smtp.kpce-co.com:587",
  "Password: ": "OrTFHBY80",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.609043006.0000000004CA2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.604206225.0000000000400000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000001.231786919.000000000041 4000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.608368856.0000000003B6 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.608962931.0000000004C6 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

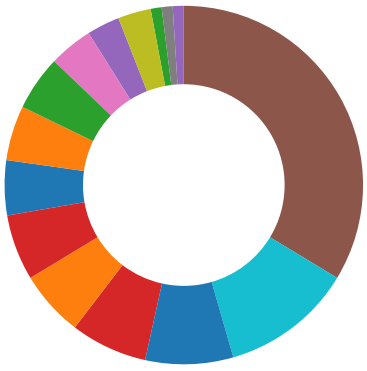
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.v04mldbd.exe.4ca0000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.v04mldbd.exe.4c60000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.v04mldbd.exe.400000.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.v04mldbd.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.v04mldbd.exe.4c60000.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

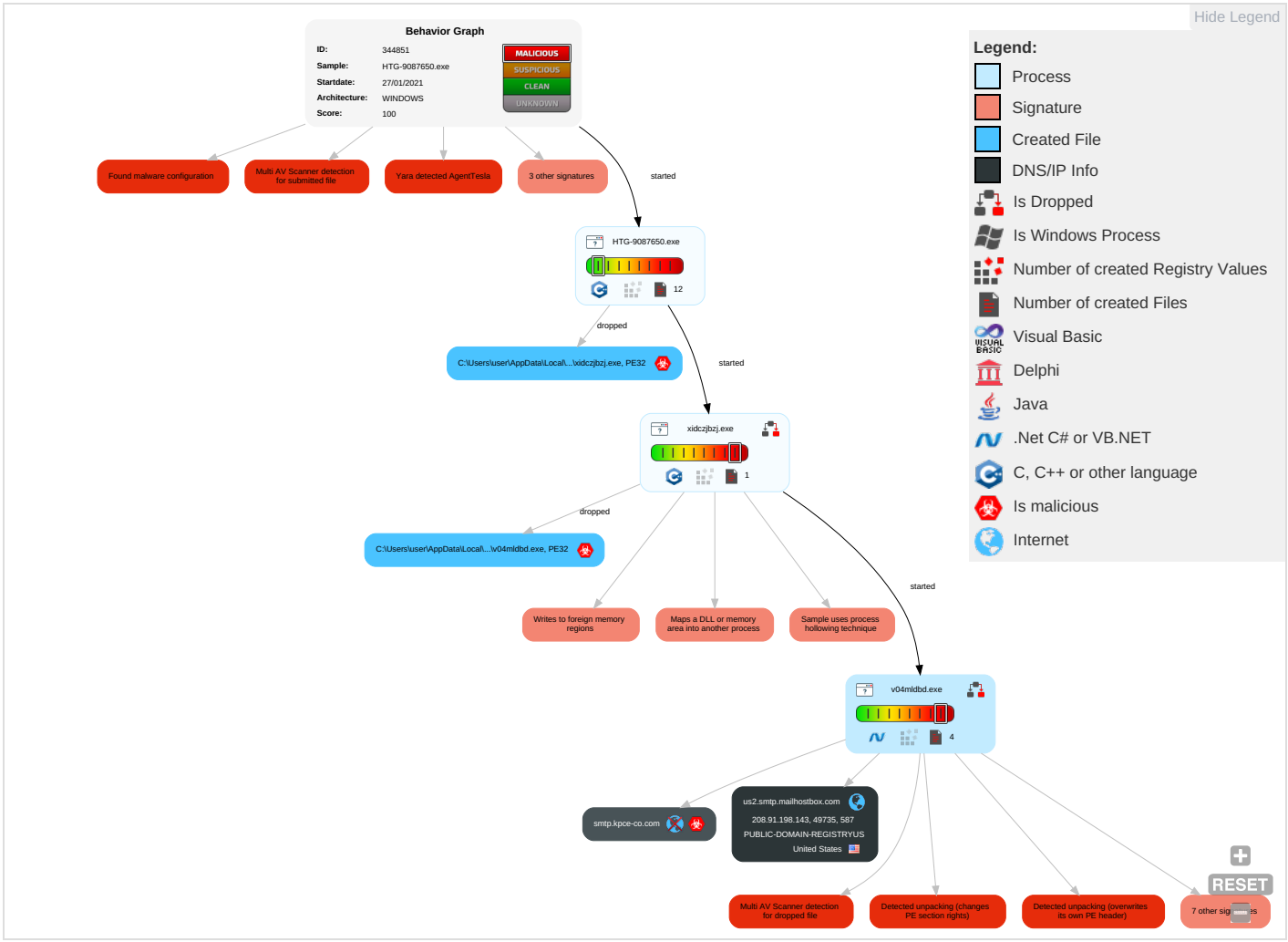
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 2 7	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Stand Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Non-Applic Layer Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4	LSA Secrets	Security Software Discovery 2 5 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Applicatio Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

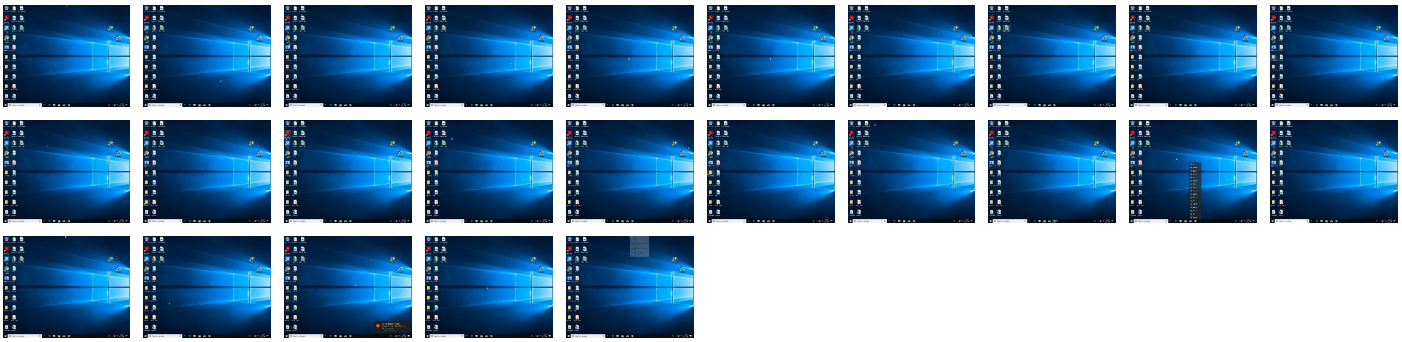
Behavior Graph



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
HTG-9087650.exe	21%	Virustotal		Browse
HTG-9087650.exe	20%	ReversingLabs		
HTG-9087650.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\v04mldbd.exe	21%	ReversingLabs	Win32.PUA.Wacapew	
C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.v04mldbd.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.v04mldbd.exe.4ca0000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.HTG-9087650.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.1.v04mldbd.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.HTG-9087650.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.kpce-co.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	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://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://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://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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://DpIPFD.com	0%	Avira URL Cloud	safe	
http://flF3mJWUOO3.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high
smtp.kpce-co.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

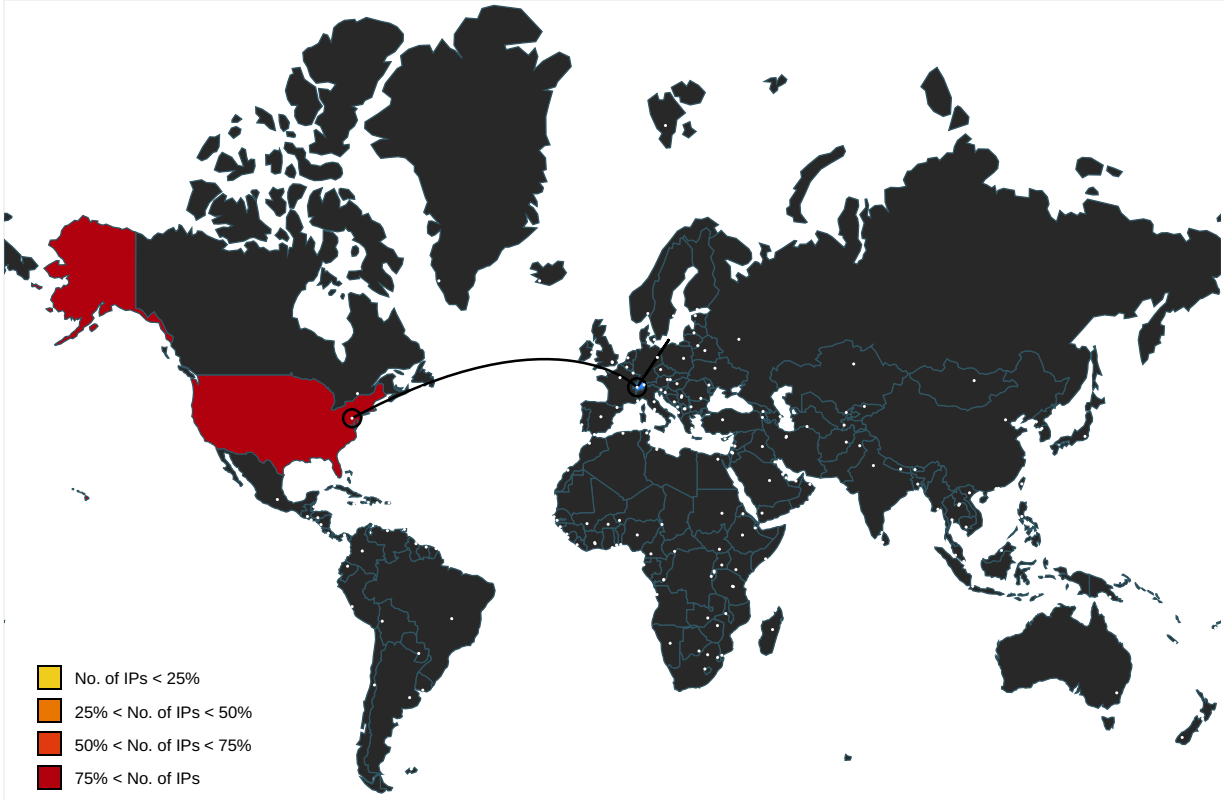
Name	Malicious	Antivirus Detection	Reputation
http://flF3mJWUOO3.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	xidczjbzj.exe, 00000001.00000002.236016980.0000000004843000.00000004.00000001.sdmp, v04mldbd.exe, 00000002.00000000.226659909.00000000004C9000.00000002.00020000.sdmp, nsx3578.tmp.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	v04mldbd.exe, 00000002.00000002.607044229.0000000002B61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	v04mldbd.exe, 00000002.00000002.607044229.0000000002B61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	HTG-9087650.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	HTG-9087650.exe	false		high
http://https://www.autoitscript.com/autoit3/	xidczjbzj.exe, 00000001.00000002.236016980.0000000004843000.00000004.00000001.sdmp, nsx3578.tmp.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	v04mldbd.exe, 00000002.00000002.607044229.0000000002B61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	xidczjbzj.exe, 00000001.00000002.232405939.0000000001190000.00000004.00000001.sdmp, v04mldbd.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DpIPFD.com	v04mldbd.exe, 00000002.00000002.607044229.0000000002B61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344851
Start date:	27.01.2021

Start time:	09:26:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HTG-9087650.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/5@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38.1% (good quality ratio 35.2%) • Quality average: 77.5% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 52.255.188.83, 92.122.144.200, 51.11.168.160, 95.101.22.203, 95.101.22.216, 20.54.26.129, 51.103.5.159, 51.104.144.132, 95.101.22.224, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus17.cloudapp.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:27:47	API Interceptor	1454x Sleep call for process: v04mldbd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	TACSAL.xlsx	Get hash	malicious	Browse	
	para.exe	Get hash	malicious	Browse	
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	
	HTMY-209871640.exe	Get hash	malicious	Browse	
	Payment slip.exe	Get hash	malicious	Browse	
	2Dd20YdQDR.exe	Get hash	malicious	Browse	
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	
	Z1cfHQnsLw.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42809.32039.exe	Get hash	malicious	Browse	
	MTC74989-1-19-21.exe	Get hash	malicious	Browse	
	IQzEWkxzNM.exe	Get hash	malicious	Browse	
	72-XV-032_Valves.exe	Get hash	malicious	Browse	
	sample2.exe	Get hash	malicious	Browse	
	invoice No 8882.exe	Get hash	malicious	Browse	
	DHL Delivery Confirmation.exe	Get hash	malicious	Browse	
	Verify Email.exe	Get hash	malicious	Browse	
	Statement of Account.doc	Get hash	malicious	Browse	
	vsl particulars.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	suk1MHq6DK.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	SSE_SOA2021.doc	Get hash	malicious	Browse	• 208.91.198.143
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SOA.exe	Get hash	malicious	Browse	• 208.91.199.225
	7xCBr7CChD.exe	Get hash	malicious	Browse	• 208.91.199.224
	Purchase Order no 7770022460.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment slip.exe	Get hash	malicious	Browse	• 208.91.198.143
	2Dd20YdQDR.exe	Get hash	malicious	Browse	• 208.91.198.143
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping_Details.exe	Get hash	malicious	Browse	• 204.11.58.28
	Request.xlsx	Get hash	malicious	Browse	• 103.53.40.13
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 216.10.246.131
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	k.dll	Get hash	malicious	Browse	• 162.215.252.76
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 43.225.55.205
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	certificado.doc	Get hash	malicious	Browse	• 162.215.254.66
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 162.215.254.66

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\v04mldbd.exe	Order-0S94442VD VictoryJSC.xlsx	Get hash	malicious	Browse	
	Purchase Order.xlsx	Get hash	malicious	Browse	
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	Order-0S94442VD VictoryJSC.xlsx	Get hash	malicious	Browse	
	Purchase Order.xlsx	Get hash	malicious	Browse	
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	
	tZy7EYc9Da.exe	Get hash	malicious	Browse	
	YMQ6XNETnU.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	BANK FORM.xlsx	Get hash	malicious	Browse	
	order0004345.xlsx	Get hash	malicious	Browse	
	Bill of Lading BL.xlsx	Get hash	malicious	Browse	
	Clntnjk.xlsx	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	
	vbc.exe	Get hash	malicious	Browse	
	HTMY-209871640.exe	Get hash	malicious	Browse	
	YOeg64zDX4.exe	Get hash	malicious	Browse	
	qZtylTGU0c.exe	Get hash	malicious	Browse	
	w2kN50kQQ4.exe	Get hash	malicious	Browse	
	EOJ55l6pzU.exe	Get hash	malicious	Browse	
	payload.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsx3578.tmp	
Process:	C:\Users\user\Desktop\HTG-9087650.exe
File Type:	data
Category:	dropped
Size (bytes):	1514736
Entropy (8bit):	7.0046337804895975

C:\Users\user\AppData\Local\Temp\nsx3578.tmp	
Encrypted:	false
SSDEEP:	24576:oT3E53Myyzl0hMf1tr7Caw8M0R8o48Qj5MIXZ:m3EZpBh211Waw30R8UQlMM
MD5:	DE404B14EF24DBCE1231D2DBC7DF9549
SHA1:	8C5F6441EE691F008E1D226E670B9799EB03CA67
SHA-256:	C22AFD2065716CD233F0A650EAC8166F2F61E70C775FB7FEA7F903886FC72E75
SHA-512:	D4E2B533A8B466517C7AF56C8B387A7723427E9271B5645ECA8E518544E92D4491026F6D70160EB4221B0617662EA3D5B341D3E3DB3676090FFE923FF1A102BD
Malicious:	false
Reputation:	low
Preview:	.....,.....&..... .....J.....r...j..... ....

C:\Users\user\AppData\Local\Temp\rvqhxxqejn.kiz	
Process:	C:\Users\user\Desktop\HTG-9087650.exe
File Type:	data
Category:	dropped
Size (bytes):	291328
Entropy (8bit):	**7.999350690035954**
Encrypted:	**true**
SSDEEP:	6144:0co8UsV2BvgdyQjOjMZ8aLNlqqObRofuYZel63XG9zHw:W8rcvgdyQj5ZzXCFWXCw
MD5:	7E9E9AB6D40F08F71C1B5259A92892FC
SHA1:	F9BE6A13D2C1B154F9962CAF492B534B19A8A79C
SHA-256:	FFB3E0949E358E291EBFFA43898BBA989C4FF3C72B96624F4EBF775598716E85
SHA-512:	EFC353841DEBB937DCCE91FCFD007B5C80E7ED5C1A010D18F20B773FA0D2654F9EF42030AD96E1FBCA3E5BCB07BEC8B3F63E2DCA8760FF890FCC2CDC909016F
Malicious:	false
Reputation:	low
Preview:	..Y.6..Zv@..e..f.q.'.\. 4.*.....+... ..D(._y.....xn.1.6..._.J.B...J....3{.'....m_..$...22.{..4....."...+v.Z..~...Wq...3.(S..4nvO3$CK0.7.x.....'...9..E..XR.....S..BH....<@.eD...ds.w.s....%B..3.....J$.\0.#a..t^tgu.JU...._..."..../..y.S.\...e..[-.....,z..0z<}..z.S.....S.yhlX...Ts...,H.l..r.....v...U.:.g..../.C...o.....~..W..S..B.:eG..|t..}.....G.....J.#9.0.\i]!.3.vNM.....Vc...q.\.H..u^.....Y.(9UX`..(.l.0*.,...s.....<'._..v..!.d.}1<W7....c&....-._.J'Q..lB.!...6K...Z..x....n...2Gg..G....."....Xu-...;LW;..a~..GS..i.....i,{.-.~..7..g8\..|.,!..H.....^../.C.D..A.\9{.Nl..U._S....._-_.+..1....[.<.4~....&C.....5..Wqu]g.M.l..M...U....{...Q..{.y.....w..h....E.....p. .P..&...o...n.a..@.....8...)....\R.I..]yo[rD..z!,<>....S.JV...-7KK.wN{K.K..Q..I.eH.x..t...j.=N.....+e.....u!..\2..n..D.1.....'p?...Y.....q".Q..a....:I.W.)....}+...../.(H...>d._:.D&,{...R.@....&.*.-..D.....#.L.V..rk..S.....[.-L.k...z..Z.....o.F...1

C:\Users\user\AppData\Local\Temp\syioy.pm	
Process:	C:\Users\user\Desktop\HTG-9087650.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	327244
Entropy (8bit):	3.991869527752463
Encrypted:	false
SSDEEP:	48:apeZufWhAJuhpu5kT7R5/8f90rphAfncxxrfxZcxxwAKhpArKrfAXkcxxwAKhpAt:apsuFTPHcYdfvfhHJ23hI
MD5:	3D0A9DA31E66605B88CF9D0DA3DE7776
SHA1:	7B5AEE2CD5A5DA63557AEAF8FEB5B7EF6F2AD918
SHA-256:	AE117B20E50ECB2CA5701D8B09D81882A2968B475008B814B48FC6F97094DD3C
SHA-512:	35EAFE8285C4518F74086FBB160100139382AFA0B0D60CF71D8056BD29D5FA7ED7CE65A7D1E9AC03A4A184D683E8408AA93D8C80AFBD9EBB00CF5F4A199AA401
Malicious:	false
Reputation:	low
Preview:	Global $MChr = Execute("Chr")..#NoTrayIcon..Global $M30ammmpxi, $Y31fqhop, $A32tgcldy, $J33oay, $S34adtadv, $V35jildc..For $M30ammmpxi = 0 To Random(5, 8, 1).. $A32tgcldy = 0.. For $J33oay = 2 To 100.. $Y31fqhop = True.. $S34adtadv = 2.. While $S34adtadv*$S34adtadv<=$M30ammmpxi.. If Mod($M30ammmpxi, $S34adtadv) == 0 Then.. $A32tgcldy = False.. ExitLoop.. EndIf.. $S34adtadv += 1.. WEnd.. If $Y31fqhop Then $A32tgcldy = $J33oay.. Next..Next..Dim $form1 = GUICreate($MChr((-402 + 481)) & $MChr((-364 + 481)) & $MChr((-365 + 481)) & $MChr((-383 + 481)) & $MChr((-364 + 481)) & $MChr((-382 + 481)) & $MChr((-374 + 481)) & $MChr((-449 + 481)) & $MChr((-408 + 481)) & $MChr((-371 + 481)) & $MChr((-382 + 481)), 102, 240, -99999, -99999, 0, 128)....GUISetState(@SW_SHOW)..Global $T3232kradcr = Execute($MChr((-412 + 481)) & $MChr((-361 + 481)) & $MChr((-380 + 481)) & $MChr((-382 + 481)) & $MChr((-364 + 481)) & $MChr((-365 + 481)) & $MChr((-380 + 481)))..Global $M3239rfkpgrfa = $T3232kr

C:\Users\user\AppData\Local\Temp\v04mldbd.exe	
Process:	C:\Users\user\AppData\Local\Temp\xidczjbzj.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.570843086702839
Encrypted:	false
SSDEEP:	12288:apVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M0:aT3E53Myyzl0hMf1tr7Caw8M0
MD5:	535DD1329AEF11BF4654B3270F026D5B

C:\Users\user\AppData\Local\Temp\v04mldbd.exe	
SHA1:	9C84DE0BDE8333F852120AB40710545B3F799300
SHA-256:	B31445FC4B8803D1B7122A6563002CFE3E925FFD1FDC9B84FBA6FC78F6A8B955
SHA-512:	A552E20A09A796A6E3E18DECE308880069C958CF9136BB4FC3EE726D6BC9B2F8EDDBCFF06FF9F9DED4DD268F5D0F39D516AD42ECCE6455A4BF5CF4F3CB4C ECC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Joe Sandbox View:	• Filename: Order-0S94442VD VictoryJSC.xlsx, Detection: malicious, Browse • Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....@.....@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	
Process:	C:\Users\user\Desktop\HTG-9087650.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Order-0S94442VD VictoryJSC.xlsx, Detection: malicious, Browse • Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: tZy7EYc9Da.exe, Detection: malicious, Browse • Filename: YMQ6XNETnU.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: BANK FORM.xlsx, Detection: malicious, Browse • Filename: order0004345.xlsx, Detection: malicious, Browse • Filename: Bill of Lading BL.xlsx, Detection: malicious, Browse • Filename: Clntnjk.xlsx, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse • Filename: vbc.exe, Detection: malicious, Browse • Filename: HTMY-209871640.exe, Detection: malicious, Browse • Filename: YOeg64zDX4.exe, Detection: malicious, Browse • Filename: qZtylTGU0c.exe, Detection: malicious, Browse • Filename: w2kN50kQQ4.exe, Detection: malicious, Browse • Filename: EOJ55l6pzU.exe, Detection: malicious, Browse • Filename: payload.vbs, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z....."....@.....@...@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.987319605724371

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	HTG-9087650.exe
File size:	797438
MD5:	dcb57041d46889e94cf100e4e0325176
SHA1:	7c9a62b778db3d6e08962749967c29c5f9084da7
SHA256:	b9b2c05c193a6df71266380c102c635199a45263722c6395a0b03de819a01ee1
SHA512:	bc72d91b843bbe6efb15c5bf147da9d48fd8ed92a4a9ff4d7529b0fb2d6d66e8f52adbe92521cb457e9aaee534d72240edd615fee8ff0f7d5d5351c7f1942d3
SSDEEP:	12288:s4y5IGtofjDTOQODX0wuyho9lyJ+DA8oziyS8rCvgdqQjJZhX+h5XCw:sh/mXTNODk3yhUlYMyS8m44QjJyDXZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..._.$_.....f...x.....4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403486
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D75F [Sat Aug 1 02:45:51 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh

Instruction
cmp ax, 00000006h
mov dword ptr [0042F44Ch], eax
je 00007F37FC79AC13h
push ebx
call 00007F37FC79DD8Eh
cmp eax, ebx
je 00007F37FC79AC09h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F37FC79DD0Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F37FC79ABEDh
push 0000000Bh
call 00007F37FC79DD62h
push 00000009h
call 00007F37FC79DD5Bh
push 00000007h
mov dword ptr [0042F444h], eax
call 00007F37FC79DD4Fh
cmp eax, ebx
je 00007F37FC79AC11h
push 0000001Eh
call eax
test eax, eax
je 00007F37FC79AC09h
or byte ptr [0042F44Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F518h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429878h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x6bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x29c	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x65ad	0x6600	False	0.675628063725	data	6.48593060343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4634765625	data	5.26110074066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25558	0x600	False	0.470052083333	data	4.21916068772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x6bc	0x800	False	0.41552734375	data	4.23392864293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38100	0x100	data	English	United States
RT_DIALOG	0x38200	0x11c	data	English	United States
RT_DIALOG	0x3831c	0x60	data	English	United States
RT_MANIFEST	0x3837c	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

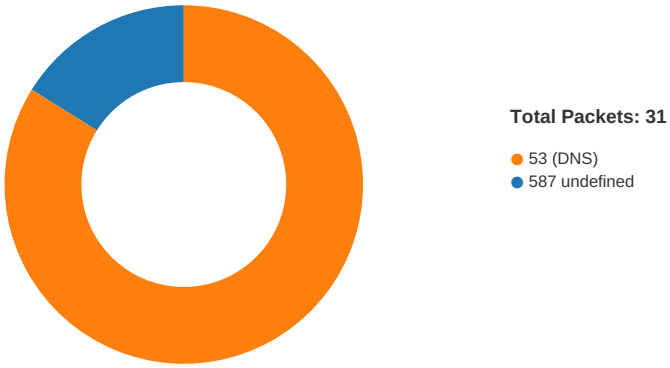
DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:29:10.684876919 CET	49735	587	192.168.2.5	208.91.198.143
Jan 27, 2021 09:29:10.849242926 CET	587	49735	208.91.198.143	192.168.2.5
Jan 27, 2021 09:29:10.849369049 CET	49735	587	192.168.2.5	208.91.198.143
Jan 27, 2021 09:29:10.910126925 CET	49735	587	192.168.2.5	208.91.198.143
Jan 27, 2021 09:29:11.074387074 CET	587	49735	208.91.198.143	192.168.2.5
Jan 27, 2021 09:29:11.186243057 CET	587	49735	208.91.198.143	192.168.2.5
Jan 27, 2021 09:29:11.186306000 CET	587	49735	208.91.198.143	192.168.2.5
Jan 27, 2021 09:29:11.186589003 CET	49735	587	192.168.2.5	208.91.198.143
Jan 27, 2021 09:29:11.186656952 CET	49735	587	192.168.2.5	208.91.198.143

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:27:30.987117052 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:31.038033009 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:31.797211885 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:31.845467091 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:32.684510946 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:32.732475042 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:33.489934921 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:33.538016081 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:37.337347031 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:37.388124943 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:38.850197077 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:38.898046017 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:56.313384056 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:56.379398108 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 09:27:59.354007959 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:27:59.404923916 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 09:28:03.129101038 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:28:03.186769962 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 09:28:16.517481089 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:28:16.573966026 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 09:28:20.976614952 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:28:21.033694983 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 09:28:22.258771896 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:28:22.306762934 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 09:28:24.962450027 CET	50463	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:28:25.023382902 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 09:28:57.970331907 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:28:58.020369053 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 09:29:00.178879976 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:29:00.246793032 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 09:29:10.465862036 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:29:10.663050890 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:11.241107941 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:11.297836065 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:11.978900909 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:12.038083076 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:12.772558928 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:12.829019070 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:13.367031097 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:13.426970005 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:14.113064051 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:14.169497013 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:14.892539978 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:14.948901892 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:15.757035017 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:15.815879107 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:17.029656887 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:17.086160898 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:18.898958921 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:18.955606937 CET	53	65086	8.8.8.8	192.168.2.5
Jan 27, 2021 09:30:19.594594955 CET	56432	53	192.168.2.5	8.8.8.8
Jan 27, 2021 09:30:19.651010036 CET	53	56432	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 09:29:10.465862036 CET	192.168.2.5	8.8.8.8	0x866e	Standard query (0)	smtp.kpce-co.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 09:29:10.663050890 CET	8.8.8.8	192.168.2.5	0x866e	No error (0)	smtp.kpce-co.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:29:10.663050890 CET	8.8.8.8	192.168.2.5	0x866e	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:29:10.663050890 CET	8.8.8.8	192.168.2.5	0x866e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:29:10.663050890 CET	8.8.8.8	192.168.2.5	0x866e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 09:29:10.663050890 CET	8.8.8.8	192.168.2.5	0x866e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

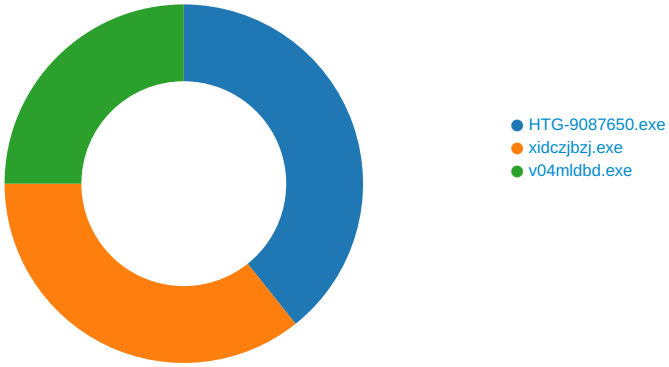
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 09:29:11.186243057 CET	587	49735	208.91.198.143	192.168.2.5	220 us2.outbound.mailhostbox.com ESMTP Postfix

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: HTG-9087650.exe PID: 6792 Parent PID: 5672

General

Start time:	09:27:36
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\HTG-9087650.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\HTG-9087650.exe'
Imagebase:	0x400000
File size:	797438 bytes
MD5 hash:	DCB57041D46889E94CF100E4E0325176
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx3577.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsx3578.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA

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	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\syioy.pm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\rvqhxxqejn.kiz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx3577.tmp	success or wait	1	4036FD	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx3578.tmp	unknown	27040	ec 09 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 08 00 00 00 a4 06 00 00 00 00 00 00 26 09 00 00 01 00 00 00 ec 09 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,..................... ....&..................	success or wait	59	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 16 73 44 90 52 12 2a c3 52 12 2a c3 52 12 2a c3 14 43 cb c3 50 12 2a c3 cc b2 ed c3 53 12 2a c3 5f 40 f5 c3 61 12 2a c3 5f 40 ca c3 e3 12 2a c3 5f 40 cb c3 67 12 2a c3 5b 6a a9 c3 5b 12 2a c3 5b 6a b9 c3 77 12 2a c3 52 12 2b c3 72 10 2a c3 e7 8c c0 c3 02 12 2a c3 e7 8c f5 c3 53 12 2a c3 5f 40 f1 c3 53 12 2a c3 52 12 bd c3 50 12 2a c3 e7 8c f4 c3 53 12 2a c3 52 69 63 68 52 12 2a	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........sD.R.*.R.*.R.*..C..P. *.....S.*._@..a.*._@....*._@ ..g.*.[j..[.*.[j..w.*.R.+.r.*... ....*.....S.*._@..S.*.R...P.*. ....S.*.RichR.*	success or wait	55	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	16384	47 6c 6f 62 61 6c 20 24 4d 43 68 72 20 3d 20 45 78 65 63 75 74 65 28 22 43 68 72 22 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 47 6c 6f 62 61 6c 20 24 4d 33 30 61 6d 6d 6d 70 78 69 2c 20 24 59 33 31 66 71 68 6f 70 2c 20 24 41 33 32 74 67 63 6c 64 79 2c 20 24 4a 33 33 6f 61 79 2c 20 24 53 33 34 61 64 74 61 64 76 2c 20 24 56 33 35 6a 69 6c 64 63 0d 0a 46 6f 72 20 24 4d 33 30 61 6d 6d 6d 70 78 69 20 3d 20 30 20 54 6f 20 52 61 6e 64 6f 6d 28 35 2c 20 38 2c 20 31 29 0d 0a 20 24 41 33 32 74 67 63 6c 64 79 20 3d 20 30 0d 0a 20 46 6f 72 20 24 4a 33 33 6f 61 79 20 3d 20 32 20 54 6f 20 31 30 30 0d 0a 20 20 24 59 33 31 66 71 68 6f 70 20 3d 20 54 72 75 65 0d 0a 20 20 24 53 33 34 61 64 74 61 64 76 20 3d 20 32 0d 0a 20 20 57 68 69 6c 65 20 24 53 33 34 61 64 74 61	Global $MChr = Execute("Chr"). .#NoTrayIcon..Global $M30ammmpxi, $Y31fqhop, $A32tgcldy, $J33oay, $S34adtadv, $V35jildc..For $M30ammmpxi = 0 To Random(5, 8, 1).. $A32tgcldy = 0.. For $J33oay = 2 To 100.. $Y31fqhop = True.. $S34adtadv = 2.. While $S34adta	success or wait	20	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rvqhxxqejn.kiz	unknown	16384	88 19 59 d0 36 b3 9c 5a 76 40 b1 d0 65 b8 bd 66 d3 71 8b 27 cc 5c e1 86 20 34 ed 2a 84 f9 96 ab 8c e3 09 12 e1 d5 85 0e 2b ff 9b 1b 20 fd 02 44 28 10 5f 79 f2 dc a3 c3 da 84 15 da 81 78 6e ce 31 a0 36 cb 14 b9 5f c5 4a 02 42 0f a1 e9 a4 bb 4a ee 90 bc 87 b6 bd 33 7b 0d 27 eb c1 c3 d3 6d 5f fb 02 24 bf c6 1d 32 32 e7 7b 88 8c 34 1c c3 f6 8b c1 22 9f 8b 1e 2b 76 d7 5a 13 8d 7e c1 db f3 57 71 e0 1d ba 33 0f 28 53 09 b8 34 6e 76 4f 33 24 43 4b 30 d4 84 37 a1 78 bf 90 b7 a5 19 d9 27 b7 96 2e 39 f1 2e 45 bd 90 58 52 a3 b0 95 8b 81 53 0f f0 42 48 a0 12 18 1c 3c 40 c0 65 44 ae 07 91 64 73 d4 b0 77 89 73 7f b4 ee f2 25 42 81 a0 33 00 d6 c1 db fe ad 4a 24 0f 5c 30 c2 23 61 c7 1d 74 5e 74 67 75 d4 4a 55 1e a6 0a ff 5f d1 ff e9 22 e7 f6 d1 af ff 2f 99 01 79 df 53 e6	..Y.6..Zv@..e..f.q.'.\.. 4.*.. .....+... ..D(._y..... .xn.1.6..._.J.B.....J.....3{. '....m_..$...22.{..4....."...+ v.Z..~...Wq...3. (S..4nvO3$CK0. .7.x.....'...9..E..XR.....S.. BH.... <@.eD...ds..w.s....%B..3 .....J$.\0.#a..t^tgu.JU...._. .."...../..y.S.	success or wait	18	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\HTG-9087650.exe	unknown	512	success or wait	71	405E78	ReadFile
C:\Users\user\Desktop\HTG-9087650.exe	unknown	16384	success or wait	47	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsx3578.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsx3578.tmp	unknown	2540	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsx3578.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsx3578.tmp	unknown	16384	success or wait	93	405E78	ReadFile

Analysis Process: xidczjbzj.exe PID: 6824 Parent PID: 6792

General

Start time:	09:27:37
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\xidczjbzj.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\xidczjbzj.exe C:\Users\user\AppData\Local\Temp\syioy.pm
Imagebase:	0x11f0000
File size:	893608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.232405939.0000000001190000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\v04mldbd.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1180243	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\v04mldbd.exe	unknown	893608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 16 73 44 90 52 12 2a c3 52 12 2a c3 52 12 2a c3 14 43 cb c3 50 12 2a c3 cc b2 ed c3 53 12 2a c3 5f 40 f5 c3 61 12 2a c3 5f 40 ca c3 e3 12 2a c3 5f 40 cb c3 67 12 2a c3 5b 6a a9 c3 5b 12 2a c3 5b 6a b9 c3 77 12 2a c3 52 12 2b c3 72 10 2a c3 e7 8c c0 c3 02 12 2a c3 e7 8c f5 c3 53 12 2a c3 5f 40 f1 c3 53 12 2a c3 52 12 bd c3 50 12 2a c3 e7 8c f4 c3 53 12 2a c3 52 69 63 68 52 12 2a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........sD.R.*.R.*.R.*..C..P. *.....S.*._@..a.*._@....*._@ ..g.*.[j..[.*.[j..w.*.R.+.r.*... ....*.....S.*._@..S.*.R...P.*. ....S.*.RichR.*	success or wait	1	1180263	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65536	success or wait	6	12212FD	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	4096	end of file	1	12212FD	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65024	end of file	1	12212FD	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65536	success or wait	6	12212FD	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	4096	end of file	1	12212FD	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65024	end of file	1	12212FD	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65536	success or wait	1	120427C	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65536	success or wait	4	12039EF	ReadFile
C:\Users\user\AppData\Local\Temp\syioy.pm	unknown	65536	end of file	2	12039EF	ReadFile
C:\Users\user\AppData\Local\Temp\rvqhxxqejn.kiz	unknown	291328	success or wait	1	118175A	ReadFile
C:\Users\user\AppData\Local\Temp\xidczjbzj.exe	unknown	893608	success or wait	1	118014A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1180AB5	ReadFile

Analysis Process: v04mldbd.exe PID: 6852 Parent PID: 6824

General

Start time:	09:27:38
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\v04mldbd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\xidczjbzj.exe C:\Users\user\AppData\Local\Temp\syioy.pm
Imagebase:	0x400000
File size:	893608 bytes
MD5 hash:	535DD1329AEF11BF4654B3270F026D5B
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: 00000002.00000002.609043006.0000000004CA2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.604206225.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.231786919.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.608368856.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.608962931.0000000004C60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.604739933.0000000000956000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.607044229.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.607044229.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 21%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	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	72B860AC	unknown
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	72B860AC	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	72B860AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	572162F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	572162F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	572162F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	572162F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	572162F	ReadFile

Disassembly

Code Analysis