ID: 435322
Sample Name:
xax2K3BWhm.exe
Cookbook: default.jbs
Time: 12:16:42
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

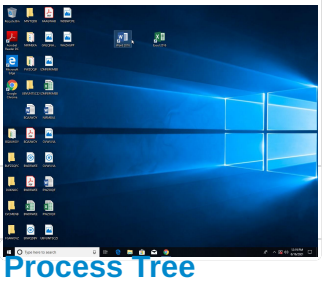
Windows Analysis Report xax2K3BWhm.exe

Overview

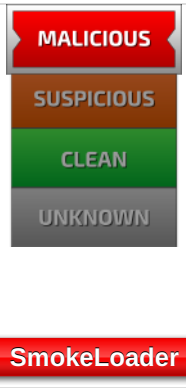
General Information

Sample Name:	xax2K3BWhm.exe
Analysis ID:	435322
MD5:	e3686e4e0ed04a..
SHA1:	7a6e59e6c01135..
SHA256:	1d1dbabc1c905c...
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

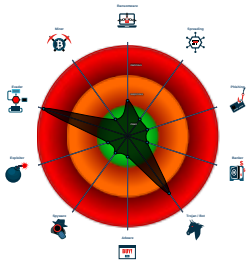


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Benign windows process drops PE f...
- DLL reload attack detected
- Detected unpacking (changes PE se...
- Found malware configuration
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- System process connects to networ...
- Yara detected SmokeLoader
- C2 URLs / IPs found in malware con...
- Checks for kernel code integrity (NtQ...
- Checks if the current machine is a v...
- Contains functionality to inject code ...

Classification



Process Tree

- **System is w10x64**
- xax2K3BWhm.exe (PID: 6992 cmdline: 'C:\Users\user\Desktop\xax2K3BWhm.exe' MD5: E3686E4E0ED04A1FD38BB5060CB2441E)
  - xax2K3BWhm.exe (PID: 6136 cmdline: 'C:\Users\user\Desktop\xax2K3BWhm.exe' MD5: E3686E4E0ED04A1FD38BB5060CB2441E)
- explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- ahafdus (PID: 6224 cmdline: C:\Users\user\AppData\Roaming\ahafdus MD5: E3686E4E0ED04A1FD38BB5060CB2441E)
  - ahafdus (PID: 4832 cmdline: C:\Users\user\AppData\Roaming\ahafdus MD5: E3686E4E0ED04A1FD38BB5060CB2441E)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "https://hewilldoit.xyz/zizi/",
    "https://hehasdoneit.xyz/zizi/"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.788412687.000000000004A0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000004.00000002.715843467.000000000058000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000004.00000002.715911224.0000000001F61000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000E.00000002.788476185.000000000052000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
4.1.xax2K3BWhm.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
14.1.ahafdus.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.2.xax2K3BWhm.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
14.2.ahafdus.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

Deletes itself after installation

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

Malware Analysis System Evasion:

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

Renames NTDLL to bypass HIPS

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

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)

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected SmokeLoader

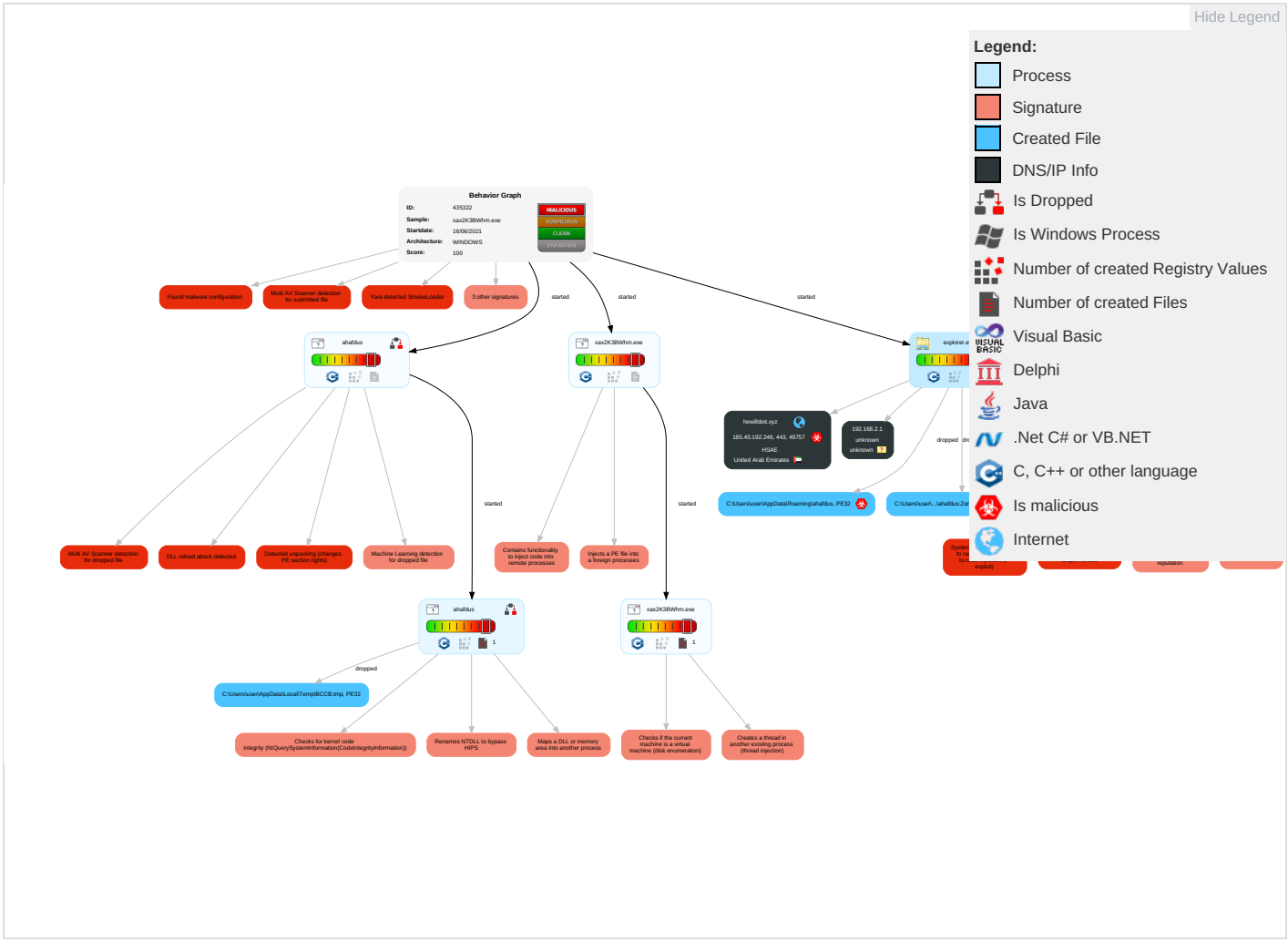
Remote Access Functionality:

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
Valid Accounts	Native API 1	DLL Side-Loading 1 1	Process Injection 5 1 2	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1 1	Virtualization/Sandbox Evasion 1 2	LSASS Memory	Security Software Discovery 4 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatic
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer 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
xax2K3BWhm.exe	45%	ReversingLabs	Win32.Trojan.Pwsx	
xax2K3BWhm.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ahafdus	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BCCB.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\BCCB.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Roaming\ahafdus	45%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.1.xax2K3BWhm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.1.ahafdus.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.xax2K3BWhm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.ahafdus.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://hewilldoit.xyz/zizi/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://https://hehasdoneit.xyz/zizi/	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hewilldoit.xyz	185.45.192.246	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://hewilldoit.xyz/zizi/	true	• Avira URL Cloud: safe	unknown
http://https://hehasdoneit.xyz/zizi/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.45.192.246	hewilldoit.xyz	United Arab Emirates		60117	HSAE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435322
Start date:	16.06.2021
Start time:	12:16:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xax2K3BWhm.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/4@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.2% (good quality ratio 13.2%) • Quality average: 51.7% • Quality standard deviation: 29.2%
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
12:18:19	Task Scheduler	Run new task: Firefox Default Browser Agent 52341AE72BE32359 path: C:\Users\user\AppData\Roaming\aha fdus

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hewilldoit.xyz	DEBIT NOTE.xlsx	Get hash	malicious	Browse	• 194.169.160.179

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	Cancellation_480942562_06082021.xlsm	Get hash	malicious	Browse	• 185.45.192.236
	Cancellation_480942562_06082021.xlsm	Get hash	malicious	Browse	• 185.45.192.236
	QB4b8Pxj7J.exe	Get hash	malicious	Browse	• 185.198.57.121
	T0DwfJpncn.exe	Get hash	malicious	Browse	• 185.198.57.121
	69d80bd2a76850dc24f4a91c82ef60f998afc28644394.exe	Get hash	malicious	Browse	• 185.198.57.121
	Document_06022021_228219382_Copy.xlsm	Get hash	malicious	Browse	• 185.183.98.25
	Document_06022021_228219382_Copy.xlsm	Get hash	malicious	Browse	• 185.183.98.25
	Document_06022021_1157730537_Copy.xlsm	Get hash	malicious	Browse	• 185.183.98.25
	Document_06022021_1157730537_Copy.xlsm	Get hash	malicious	Browse	• 185.183.98.25
	Overdue_Debt_1535591908_06012021.xlsm	Get hash	malicious	Browse	• 185.141.27.144
	Overdue_Debt_1535591908_06012021.xlsm	Get hash	malicious	Browse	• 185.141.27.144
	21305177357_05272021.xlsm	Get hash	malicious	Browse	• 185.117.73.134
	21305177357_05272021.xlsm	Get hash	malicious	Browse	• 185.117.73.134
	21881755902_05272021.xlsm	Get hash	malicious	Browse	• 185.117.73.134
	21881755902_05272021.xlsm	Get hash	malicious	Browse	• 185.117.73.134
	Decline_1491125237_05262021.xlsm	Get hash	malicious	Browse	• 185.183.96.223
	Decline_1491125237_05262021.xlsm	Get hash	malicious	Browse	• 185.183.96.223
	cc859408_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.198.57.83
	cc859408_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.198.57.83
	ZLiyQKv0K4.exe	Get hash	malicious	Browse	• 185.183.98.2

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\BCCB.tmp	Ed2zaPhzUD.exe	Get hash	malicious	Browse	
	ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe	Get hash	malicious	Browse	
	OcLtW2CNjy.exe	Get hash	malicious	Browse	
	pub2.exe	Get hash	malicious	Browse	
	42sB3Upj67.exe	Get hash	malicious	Browse	
	RE6WxoVS7v.exe	Get hash	malicious	Browse	
	VvaBHdJoGY.exe	Get hash	malicious	Browse	
	051y0i7M8q.exe	Get hash	malicious	Browse	
	RdtoOe8Lzj.exe	Get hash	malicious	Browse	
	MwcrHqpRj7.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jo3GzZMQBG.exe	Get hash	malicious	Browse	
	main_setup_x86x64.exe	Get hash	malicious	Browse	
	w4X8dxtGi6.exe	Get hash	malicious	Browse	
	BrBsL8sBvm.exe	Get hash	malicious	Browse	
	bL6FwQU4K5.exe	Get hash	malicious	Browse	
	3JDjILxXaA.exe	Get hash	malicious	Browse	
	o8RYFTZsuU.exe	Get hash	malicious	Browse	
	MrjC4jkPL8.exe	Get hash	malicious	Browse	
	qi3xLxAlDv.exe	Get hash	malicious	Browse	
	Yl6482CO6U.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\BCCB.tmp	
Process:	C:\Users\user\AppData\Roaming\ahafdus
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1622408
Entropy (8bit):	6.298350783524153
Encrypted:	false
SSDEEP:	24576:hNZ04UyDzGrVh8xsPCw3/dzcldJndozS35IW1q/kNVSYVEs4j13HLHGJImdV4q:dGrVr3hclvnqzS35IWk/LvRHb0
MD5:	BFA689ECA05147AFD466359DD4A144A3
SHA1:	B3474BE2B836567420F8DC96512AA303F31C8AFC
SHA-256:	B78463B94388FDDB34C03F5DDDD5D542E05CDED6D4E38C6A3588EC2C90F0070B
SHA-512:	8F09781FD585A6DFB8BBC34B9F153B414478B44B28D80A8B0BDC3BED687F3ADAB9E60F08CCEC5D5A3FD916E3091C845F9D96603749490B1F7001430408F711D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: Ed2zaPhzUD.exe, Detection: malicious, Browse • Filename: ccbf1853c703609eda36bc07ab8eb2faf692153b56ecf.exe, Detection: malicious, Browse • Filename: OcLtW2CNjy.exe, Detection: malicious, Browse • Filename: pub2.exe, Detection: malicious, Browse • Filename: 42sB3Upj67.exe, Detection: malicious, Browse • Filename: RE6WxoVS7v.exe, Detection: malicious, Browse • Filename: VvaBHdJoGY.exe, Detection: malicious, Browse • Filename: 051y0i7M8q.exe, Detection: malicious, Browse • Filename: RdtoOe8Lzj.exe, Detection: malicious, Browse • Filename: MwcrHqpRj7.exe, Detection: malicious, Browse • Filename: jo3GzZMQBG.exe, Detection: malicious, Browse • Filename: main_setup_x86x64.exe, Detection: malicious, Browse • Filename: w4X8dxtGi6.exe, Detection: malicious, Browse • Filename: BrBsL8sBvm.exe, Detection: malicious, Browse • Filename: bL6FwQU4K5.exe, Detection: malicious, Browse • Filename: 3JDjILxXaA.exe, Detection: malicious, Browse • Filename: o8RYFTZsuU.exe, Detection: malicious, Browse • Filename: MrjC4jkPL8.exe, Detection: malicious, Browse • Filename: qi3xLxAlDv.exe, Detection: malicious, Browse • Filename: Yl6482CO6U.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L!y>.@.m.@.m.@.m...l.@.mg$.l.@.mg$.lN@.mg$.l.A.mg$.l .@.mg$.l.@.mg$.m.@.mg$.l.@.mRich.@.m.....PE..L...s<s.....!.....P....(K.....@A.....&.....8.....h...Y.. .....N..`l..T.....text....).....*..... ..`RT.....@..... ..`.data...dW...P.....0.....@....mrdata.h#.....$...>..... ....@....00cfg.....b.....@..@.rsrc...8.....d.....@..@.reloc...N.....P.....@..B..... .....

C:\Users\user\AppData\Roaming\ahafdus	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	297984
Entropy (8bit):	5.6203884195953275
Encrypted:	false
SSDEEP:	3072:sZCIbJFbQUyeB5cq3Dey3GLtXWxQokuWaPrKrQ1xZB0YWi8y94rMtQiSrX3:sZCYGUyeB57iy3MloRrtxhjtQiSrX3
MD5:	E3686E4E0ED04A1FD38BB5060CB2441E
SHA1:	7A6E59E6C01135AB4EC685DC8C6BF7835429C916
SHA-256:	1D1DBABC1C905C7153847C6BB5B88905942D414C4DBF39E3784DC9A62E1120DB

C:\Users\user\AppData\Roaming\ahafdus	
SHA-512:	F3D6360449FE4DD742B653EBB7F6E7756D8E1145C9D96564917D23A01CC0F3DC6288B551BCD7727562E20213EC7433820933DD4F3F45B5FF7E7FECE0A8DC4C6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 45%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m..m..m.....m.....m.....m.....m..l...m.....m.....m.....m.Ric h..m.....PE..L.....^..... .....@.....`.....t2..P.....'.....0.....h*..@.....@..... .....text..... ..`.rdata.....@..@.data...<....@.....&.....@....rsrc....'.....(...B.....@..@.reloc... ...0..."..j.....@..B..... ....

C:\Users\user\AppData\Roaming\ahafdus:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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):	5.6203884195953275
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:	xax2K3BWhm.exe
File size:	297984
MD5:	e3686e4e0ed04a1fd38bb5060cb2441e
SHA1:	7a6e59e6c01135ab4ec685dc8c6bf7835429c916
SHA256:	1d1dbabc1c905c7153847c6bb5b88905942d414c4dbf39e3784dc9a62e1120db
SHA512:	f3d6360449fe4dd742b653ebb7f6e7756d8e1145c9d96564917d23a01cc0f3dc6288b551bcd7727562e20213ec7433820933dd4f3f45b5ff7e7fece0a8dc4c6b
SSDEEP:	3072:sZCIbJFbQUyeB5cq3Dey3GLtXWxQokuWaPrKrQ1xZB0YWi8y94rMtQiSrX3:sZCYGUyeB57iy3MloRrtxhjtQiSrX3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m...m...m.....m.....m.....m.....m...l...m.....m.....m.....m.Rich..m.....PE..L.....^.....

File Icon

Icon Hash:	aedaae9ee6a6aaa4

Static PE Info

General

Entrypoint:	0x401020
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:	0x5E00D3AA [Mon Dec 23 14:48:10 2019 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:	2ab857f73c9912dee0698f559b75c172

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x281ab	0x28200	False	0.58144713785	data	6.88203005979	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2a000	0x9fe8	0xa000	False	0.321801757812	data	4.72565628461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x34000	0x2debf3c	0x1c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2e20000	0x27b0	0x2800	False	0.765234375	data	6.4583593165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2e23000	0x12090	0x12200	False	0.0806438577586	data	1.03261740787	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
Oriya	India	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:18:18.631515026 CEST	192.168.2.4	8.8.8.8	0xb72	Standard query (0)	hewilldoit.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:18:18.697432995 CEST	8.8.8.8	192.168.2.4	0xb72	No error (0)	hewilldoit.xyz		185.45.192.246	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: xax2K3BWhm.exe PID: 6992 Parent PID: 6044

General

Start time:	12:17:26
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\xax2K3BWhm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\xax2K3BWhm.exe'
Imagebase:	0x400000
File size:	297984 bytes
MD5 hash:	E3686E4E0ED04A1FD38BB5060CB2441E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xax2K3BWhm.exe PID: 6136 Parent PID: 6992

General

Start time:	12:17:34
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\xax2K3BWhm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\xax2K3BWhm.exe'
Imagebase:	0x400000

File size:	297984 bytes
MD5 hash:	E3686E4E0ED04A1FD38BB5060CB2441E
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: 00000004.00000002.715843467.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.715911224.0000000001F61000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: explorer.exe PID: 3424 Parent PID: 6136

General

Start time:	12:17:41
Start date:	16/06/2021
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
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: ahafdus PID: 6224 Parent PID: 968

General

Start time:	12:18:19
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\ahafdus
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ahafdus
Imagebase:	0x400000
File size:	297984 bytes
MD5 hash:	E3686E4E0ED04A1FD38BB5060CB2441E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 45%, ReversingLabs
Reputation:	low

Analysis Process: ahafdus PID: 4832 Parent PID: 6224

General

Start time:	12:18:27
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\ahafdus
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ahafdus
Imagebase:	0x400000
File size:	297984 bytes
MD5 hash:	E3686E4E0ED04A1FD38BB5060CB2441E
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: 0000000E.00000002.788412687.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.788476185.0000000000521000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Disassembly

Code Analysis