ID: 435325
Sample Name:
US1pwXib6h.exe
Cookbook: default.jbs
Time: 12:17:51
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

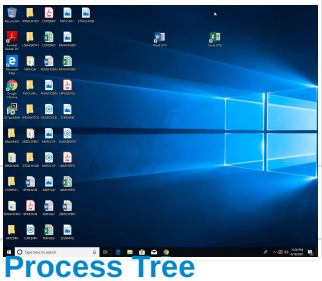
Windows Analysis Report US1pwXib6h.exe

Overview

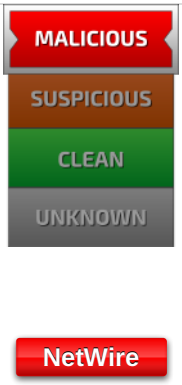
General Information

Sample Name:	US1pwXib6h.exe
Analysis ID:	435325
MD5:	91514b3627e78e..
SHA1:	b48882a3d65606..
SHA256:	e0e0ca8ec32475..
Tags:	exe NetWire RAT
Infos:	

Most interesting Screenshot:



Detection

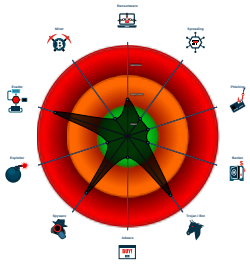


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected NetWire RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to log keystro…
- Contains functionality to steal Chrom…
- Contains functionality to steal Intern…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- US1pwXib6h.exe (PID: 6476 cmdline: 'C:\Users\user\Desktop\US1pwXib6h.exe' MD5: 91514B3627E78E42CB05BC608737A47F)
  - US1pwXib6h.exe (PID: 6548 cmdline: 'C:\Users\user\Desktop\US1pwXib6h.exe' MD5: 91514B3627E78E42CB05BC608737A47F)
- ioldfli.exe (PID: 6768 cmdline: 'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe' MD5: 91514B3627E78E42CB05BC608737A47F)
  - ioldfli.exe (PID: 6824 cmdline: 'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe' MD5: 91514B3627E78E42CB05BC608737A47F)
- ioldfli.exe (PID: 7012 cmdline: 'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe' MD5: 91514B3627E78E42CB05BC608737A47F)
  - ioldfli.exe (PID: 7088 cmdline: 'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe' MD5: 91514B3627E78E42CB05BC608737A47F)
- **cleanup**

Malware Configuration

Threatname: NetWire


```
{
  "C2 list": [
    "netno.ddns.net:6577",
    "ddns.dbcdubai.com:6577",
    "netsecond.duckdns.org:6577"
  ],
  "Password": "Trinidado1@",
  "Host ID": "OJ",
  "Mutex": "oCTboYgC",
  "Install Path": "-",
  "Startup Name": "-",
  "ActiveX Key": "-",
  "KeyLog Directory": "%AppData%\\Logs\\"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000001.363673900.0000000000400000.00000040.00020000.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000007.00000002.406739098.00000000023A0000.00000004.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000006.00000002.394088134.0000000000400000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000006.00000001.393727825.0000000000400000.00000040.00020000.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000004.00000002.395120542.00000000024E0000.00000004.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.US1pwXib6h.exe.24c0000.2.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
2.1.US1pwXib6h.exe.400000.0.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
4.2.ioldfli.exe.24e0000.2.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
6.1.ioldfli.exe.400000.0.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
2.2.US1pwXib6h.exe.400000.0.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
Click to see the 10 entries				

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

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Contains functionality to steal Chrome passwords or cookies

Contains functionality to steal Internet Explorer form passwords

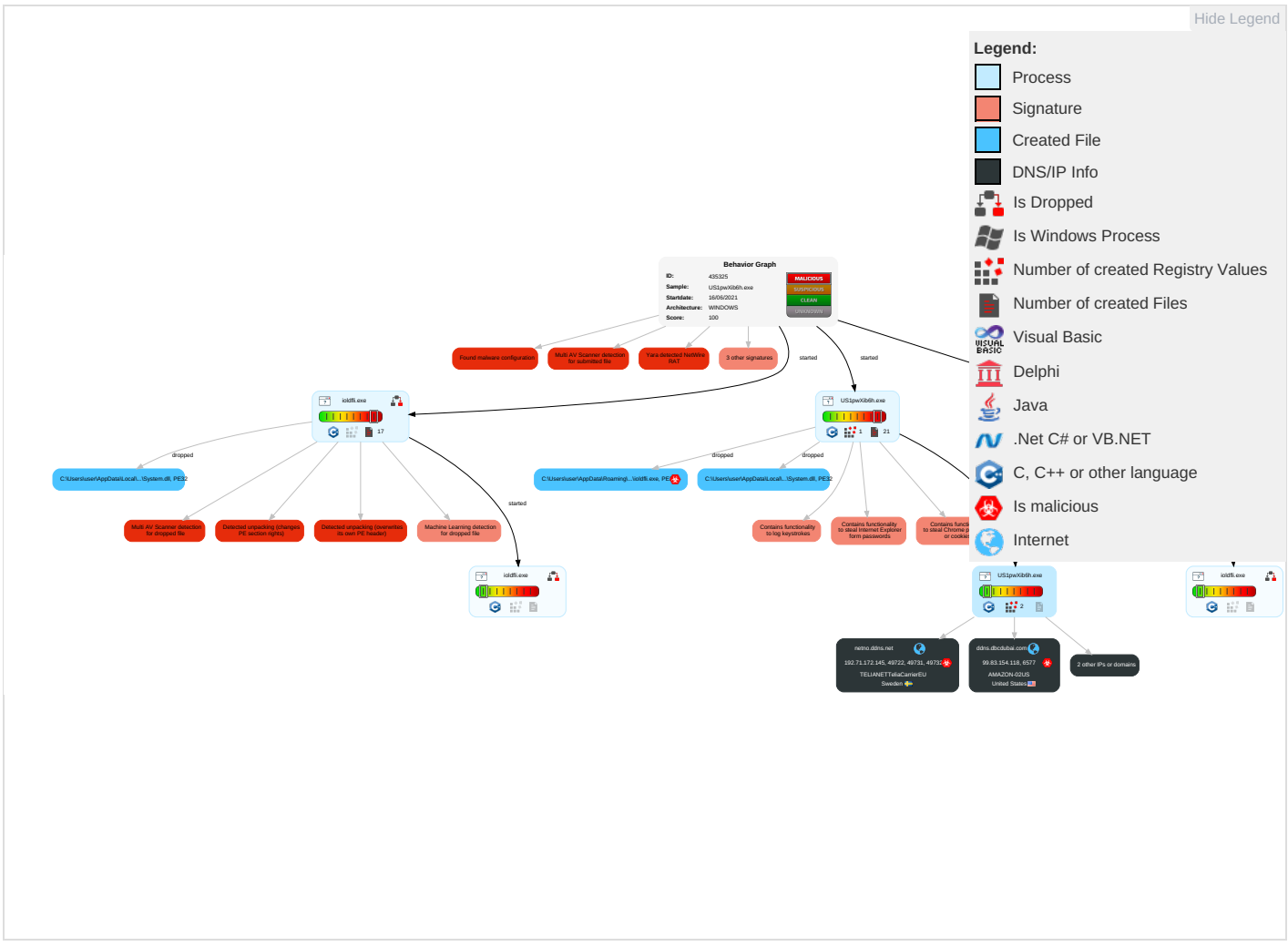
Remote Access Functionality:

Yara detected NetWire RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Input Capture 1 4 1	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2 1	Credentials In Files 2	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1 4 1	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 5	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 1	LSA Secrets	Security Software Discovery 1 1 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	F E

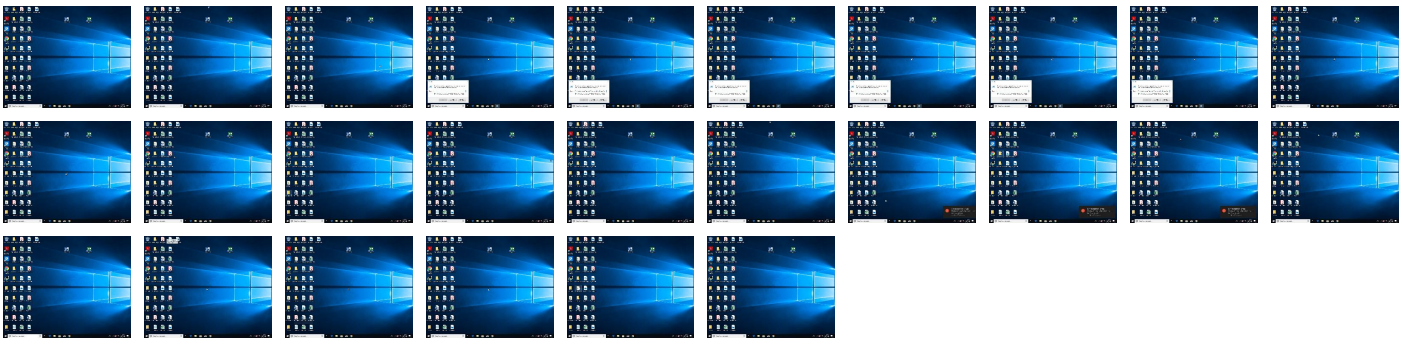
Behavior Graph



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
US1pwXib6h.exe	15%	Virustotal		Browse
US1pwXib6h.exe	27%	ReversingLabs	Win32.Backdoor.NetWiredRc	
US1pwXib6h.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nsmBB29.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsmBB29.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nst9B9A.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nst9B9A.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsu6AA7.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsu6AA7.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe	27%	ReversingLabs	Win32.Backdoor.NetWiredRc	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.US1pwXib6h.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.2.US1pwXib6h.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.2.US1pwXib6h.exe.24c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.ioldfli.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
7.2.ioldfli.exe.23a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.1.ioldfli.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
2.2.US1pwXib6h.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
6.0.ioldfli.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.0.US1pwXib6h.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
4.0.ioldfli.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
4.2.ioldfli.exe.24e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.1.US1pwXib6h.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
7.0.ioldfli.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
9.2.ioldfli.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
6.2.ioldfli.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
9.0.ioldfli.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.2.US1pwXib6h.exe.99d0000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.ioldfli.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
9.1.ioldfli.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
netsecond.duckdns.org	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
ddns.dbcdubai.com:6577	0%	Avira URL Cloud	safe	
netno.ddns.net:6577	0%	Avira URL Cloud	safe	
http://www.yandex.comsocks=	0%	Avira URL Cloud	safe	
netsecond.duckdns.org:6577	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
netsecond.duckdns.org	192.71.172.145	true	true	• 3%, Virustotal, Browse	unknown
ddns.dbcdubai.com	99.83.154.118	true	true		unknown
netno.ddns.net	192.71.172.145	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ddns.dbcdubai.com:6577	true	• Avira URL Cloud: safe	unknown
netno.ddns.net:6577	true	• Avira URL Cloud: safe	unknown
netsecond.duckdns.org:6577	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.71.172.145	netsecond.duckdns.org	Sweden		1299	TELIANETTeliaCarrierEU	true
99.83.154.118	ddns.dbcdubai.com	United States		16509	AMAZON-02US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435325
Start date:	16.06.2021
Start time:	12:17:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	US1pwXib6h.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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/10@14/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 62.1% (good quality ratio 32.6%) • Quality average: 42.7% • Quality standard deviation: 44.4%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:19:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run goqkksd C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
12:19:03	API Interceptor	13x Sleep call for process: US1pwXib6h.exe modified
12:19:08	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run goqkksd C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
12:19:09	API Interceptor	2x Sleep call for process: ioldfli.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
99.83.154.118	ITAPQJikGw.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?CFQHg=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsaG2+azAf30S&Pr980v=G2MtWNVHS
	Letter 1019.xlsx	Get hash	malicious	Browse	• www.defenestration.world/p2io/?9rx=lrOqxb+UJCh0p+XgaZ1tkMjkgx31NOkXgmck/5zOeb61pSaxp+mpU6ffv/qKl6HzQ2hiJA==&1bPx7=ifrhEpc0Hv8pf4
	WitNwYLlo9.exe	Get hash	malicious	Browse	• www.polkaface.network/ja3b/?hFN=ECSUTdLZYyvinGuxW602g0mhH6E+mNbiPpMr3Rm0jNJJ/jQZLEblo9xFFzyyk5FaoEXR&0vuXs2=8pt8MNg0
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• www.copinginfula.trade/owws/?y8z=te8+upsAlz11VMhTlIAnFNqzP7h21ZncoD0/naXG+u8xg9oMIJdghVQVRMs3z6YMH4+L&UDKPKv=04i8JpzhsHVX
	Compliance - Notice 06-03.xlsx	Get hash	malicious	Browse	• www.defenestration.world/p2io/?eXNPCd=lrOqxb+UJCh0p+XgaZ1tkMjkgx31NOkXgmck/5zOeb61pSaxp+mpU6ffv/qKl6HzQ2hiJA==&g48=Rzu8Zr0hP
	xgpUaKh6tH.dll	Get hash	malicious	Browse	• networkspeed.live/judhygdfsvhvgytrdgflkijh
	1092991(JB#082).exe	Get hash	malicious	Browse	• www.francedeliverydhl.xyz/3edq/?JfEt9j6h=VGpD3cDxk+WQQnSbGEZ6RzsTI6tD4lieCm7QRd3bliZsykliVadFEeoi23HkozfQytXm&ojn0d=RzuliD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL4198278Err-PDF.exe	Get hash	malicious	Browse	• www.bakergirlsocialclub.com/ubqx/?VR-T5=lhf8xpGpMnD8mnA&XR-xe0lh=WnoIvCh7C4a+M1FCGYfg8Er+mfNEnZG31lLhOnu48mFBzd+Jpay6aKeImEu2q9SCEyoBWBEjrg==
	RFQ - 001.xlsx	Get hash	malicious	Browse	• www.defenestration.world/p2io/?bdm=lrOqxb+UJCh0p+XgaZ1tkMjkgx31NOkXgmck/5zOeb61pSaxp+mpU6ffv/qKl6HzQ2hiJA==&CDH=oPR8Arf
	b02c0831_by_Libranalysis.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?Bv=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsZq1iq/4SWJEQ9G3xQ==&M6AIS=yVFP-hwh
	2UPdDxaAmt.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?CN9=7nH8PLV&s0=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsaGchqDAb18S
	invoice.exe	Get hash	malicious	Browse	• www.francedeliverydhl.xyz/3edq/?URZh=VGpD3cDxk+WQQnSbGEZ6RzsTl6tD4lieCm7QRd3bliZsykliVadFEeoi20n0nSPosl+h&jL30vv=afhhplx
	e759c6e8_by_Libranalysis.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?RPx=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsZmMuLT4FQVV&rVLp5Z=S0GhCH_

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	92270fdd_by_Libranalysis.exe	Get hash	malicious	Browse	• www.defenestration.world/p2io/?SR=lrOqxb+RJFhwpubsYZ1tkMjkgx31NOkXgmE0j6vPa760pj23uu3lC+ndsaG2+azAf30S&2d=9rj0CBJ
	1bb71f86_by_Libranalysis.exe	Get hash	malicious	Browse	• www.mythree-informationupdates.com/njhr/?_89pb=/zO4UNfgdHCPEreRZ95iML5TdeDdCZBMXXzBOiwQzcrtbsVzRUIeP21tWMju+8f1ac1K&FPWl=Cd8tG
	Documento.xlsx	Get hash	malicious	Browse	• indifoods.net/wp-includes/images/wlw/otedollars.exe
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• www.destek-taleplerimiz.com/ccr/?y4O4=cWavVGQKmIqDppXzWyVy8r7Kst7Id+XyOUJHTBkcFhMzlMGfnIsimvg2OkFJfjv7X60kTQ==&pHE=kv2pMLCxOn
	shipping document pdf.exe	Get hash	malicious	Browse	• www.kcgertfarm.com/htl/?_6Ax4N=YJE87vjpATZ&QFQL4Z=Y7TDP+px4JC/SSqVeQPAJJ3lS8rxz+cXHWUOWGnTGVC5LdKUNGbP50uDVhtUgmD5Xmz46i5nLA==
	lBXZjiCuW0.exe	Get hash	malicious	Browse	• www.mythree-informationupdates.com/njhr/?uZWx=/zO4UNfgdHCPEreRZ95iML5TdeDdCZBMXXzBOiwQzcrtbsVzRUIeP21tWMjEhMv1ee9K&9r6LE=FbYDOl6

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
netsecond.duckdns.org	draftdocumentsofladingdocumentsMay11052021Sca.exe	Get hash	malicious	Browse	• 193.183.217.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 44.227.65.245
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	• 52.8.83.187
	Enquiry_014821-23.exe	Get hash	malicious	Browse	• 52.58.78.16
	SKM_4050210326102400 jpg.exe	Get hash	malicious	Browse	• 52.58.78.16
	Lithium battery silkscreen of AQ04.exe	Get hash	malicious	Browse	• 76.76.21.21
	Agenda1.docx	Get hash	malicious	Browse	• 3.142.86.140
	Agenda1.docx	Get hash	malicious	Browse	• 3.142.86.140

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tj.jpg	Get hash	malicious	Browse	• 52.41.131.191
	tj.jpg	Get hash	malicious	Browse	• 52.222.158.83
	YoWeTN6Lg8.exe	Get hash	malicious	Browse	• 3.68.95.191
	INQUIRY for IFM 20207.xlsx	Get hash	malicious	Browse	• 13.114.206.192
	WGOc4eHYqX.exe	Get hash	malicious	Browse	• 3.34.12.41
	ekeson and sons.exe	Get hash	malicious	Browse	• 75.2.26.18
	IDWCH1.exe	Get hash	malicious	Browse	• 52.219.64.127
	TTObk2.dll	Get hash	malicious	Browse	• 34.209.29.159
	WP7IsjaUga.exe	Get hash	malicious	Browse	• 3.143.65.214
	PnvWsz61G6.exe	Get hash	malicious	Browse	• 52.14.32.15
	hG6FzLXtsf.xls	Get hash	malicious	Browse	• 18.136.132.202
	hG6FzLXtsf.xls	Get hash	malicious	Browse	• 18.136.132.202
	Proforma Invoice & Bank Swift Copy.exe	Get hash	malicious	Browse	• 13.59.53.244
TELIANETTeliaCarrierEU	YZ8OvkljWm.exe	Get hash	malicious	Browse	• 193.183.217.83
	SHIPPING_BILL_SCAN_INVNO_MAY-11-2021_KKW HHGDHGSGSGTEME998726.exe	Get hash	malicious	Browse	• 193.104.197.77
	PO-13916.jpeg.exe	Get hash	malicious	Browse	• 193.104.222.76
	draftdocumentsofladingdocumentsMay11052021Sca.exe	Get hash	malicious	Browse	• 193.183.217.73
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 213.155.15 6.184
	Avis de Paiement (1).xlsx	Get hash	malicious	Browse	• 213.155.15 6.183
	okRrstWWbY.exe	Get hash	malicious	Browse	• 193.181.35.58
	p3m2rgfEWw.exe	Get hash	malicious	Browse	• 192.121.10 2.215
	VJyJRFzlxy.exe	Get hash	malicious	Browse	• 192.121.102.94
	kKi1s98we9.exe	Get hash	malicious	Browse	• 192.121.102.72
	http:// https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 213.155.15 6.168
	http:// perpetual.veteran.az/673616c6c792e64756e6e6540706572706 57475616c2e636f6d2e6175	Get hash	malicious	Browse	• 104.75.89.37
	http://https://sharelink.sn.am/lYPBgpwGauq	Get hash	malicious	Browse	• 80.239.201.33
	http://https://sharelink.sn.am/lYPBgpwGauq	Get hash	malicious	Browse	• 80.239.201.95
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	• 213.155.15 6.180
	9NwJV5ylmm.exe	Get hash	malicious	Browse	• 193.181.35.196
	IoPfa6cOoR.exe	Get hash	malicious	Browse	• 193.181.35.204
	U3Y2RA3qE2.exe	Get hash	malicious	Browse	• 193.181.35.82
	6rbntANVME.exe	Get hash	malicious	Browse	• 193.181.35.82
	qpjx2E9SPd.exe	Get hash	malicious	Browse	• 193.181.35.237

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsmBB29.tmp\System.dll	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	
	7ujc2szSQX.exe	Get hash	malicious	Browse	
	TT0900090000090.exe	Get hash	malicious	Browse	
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	
	PO-006 dtd-15.06.2021.exe	Get hash	malicious	Browse	
	SKM_4050210326102400 jpg.exe	Get hash	malicious	Browse	
	IMGG087 76543.exe	Get hash	malicious	Browse	
	yfr02XrveJ.exe	Get hash	malicious	Browse	
	LCdraft6152021_pdf.exe	Get hash	malicious	Browse	
	LCdraft6152021_pdf.exe	Get hash	malicious	Browse	
	Consigment Details_pdf.exe	Get hash	malicious	Browse	
	bigfish.exe	Get hash	malicious	Browse	
	INQUIRY for IFM 20207.xlsx	Get hash	malicious	Browse	
	gz7dLhKlSQ.exe	Get hash	malicious	Browse	
	WGOc4eHYqX.exe	Get hash	malicious	Browse	
	Purchase_Order.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ojmanoq.exe	Get hash	malicious	Browse	
	linkfuq.exe	Get hash	malicious	Browse	
	takwqaytr.exe	Get hash	malicious	Browse	
	PO_403.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nst9B9A.tmp\System.dll	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	
	7ujc2szSQX.exe	Get hash	malicious	Browse	
	TT0900090000090.exe	Get hash	malicious	Browse	
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	
	PO-006 dtd-15.06.2021.exe	Get hash	malicious	Browse	
	SKM_4050210326102400 jpg.exe	Get hash	malicious	Browse	
	IMGG087 76543.exe	Get hash	malicious	Browse	
	yfr02XrveJ.exe	Get hash	malicious	Browse	
	LCdraft6152021_pdf.exe	Get hash	malicious	Browse	
	LCdraft6152021_pdf.exe	Get hash	malicious	Browse	
	Consigment Details_pdf.exe	Get hash	malicious	Browse	
	bigfish.exe	Get hash	malicious	Browse	
	INQUIRY for IFM 20207.xlsx	Get hash	malicious	Browse	
	gz7dLhKlSQ.exe	Get hash	malicious	Browse	
	WGOc4eHYqX.exe	Get hash	malicious	Browse	
	Purchase_Order.xlsx	Get hash	malicious	Browse	
	ojmanoq.exe	Get hash	malicious	Browse	
	linkfuq.exe	Get hash	malicious	Browse	
	takwqaytr.exe	Get hash	malicious	Browse	
	PO_403.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\kg0wilfv6c51ffl5	
Process:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.99888202272782**
Encrypted:	**true**
SSDEEP:	3072:nuGFc5H2AvwfIf88feBN9eovlP9T+8yzKAnmKWBysmcz+d6OObWJjhY7dLHm:qHNItf88WBtvd9r4nmKNeyPObWhqxm
MD5:	7A4AE896CD2EBACFFD6D78170B53FCAA
SHA1:	A445DBFA51502DCEF66EE058BAE9139B6EC93B8D
SHA-256:	98E678F95E223D306BD6DB6FA9D8CBEC4F109E02B00761A0A248E3281D68D10B
SHA-512:	2968A5A7AF0EBD95A0188BC8E538E9F0F88B74DCC0C6029FF461848AA1D6AC60F9377D0979CBDC92131F7419AE5F3878DA9DC1FEA6C51D41B2D37B7F38E40BF
Malicious:	false
Reputation:	low
Preview:	...].bX..ys...a..e.w.AP..^.x9y.'...A....h.#.l.....7Q..E.nx....Ml.X.N..%.b...T...zq|...s.D..e.+...../..IGk^D.:.1...y...;..O._8>..{.....?.....>../..O.zR..`..Aqp.B+.....E<l...<.v.L..TH.I..q...z~{v.7..t#...HM-...@.b.....ISZ...6... b3@.!f.I...8..6`..^..K.F.....?...U....i.G.t .f.....!.[.....+..mrrlk.W."H.....T..`d...nn..Hj.....X0._...p.qCX'h...C~.*./8p^dj>.U...+..)yH.&.....+....8H. ... ..Kg..-X.L..rg..Ip...$O.....%.P.....H..-...R.m..>.....X~yt..'....yK...|...=7..#n.~WA@.4... .....9..0....@..M....+...>...g..FnE.N...~.J..p....(.(.....a L.....D..meO.....5E.)..... .HG..VH.{}...c.c..9w.....8...i..|.....MS8.d>.uv.x.9y..._.G0...(...IKTY5.d1u.....iD7(^.P.!.++..?.....avc.|1.....%.D...[f..|....-.;".!".b.^...Q+.,H.q[A.O_z..>'....O..r.fQv.Hx.i..>....z.3@ 0.&.A`Z*..(..d.L..{.kW....R.e..{%..n...o\.-F....b..v...g}+..t6...;=...`...:p.....B..M.....X.R..clJ.v.EK...*.e.&..r...8.._.(..K.....:.P.....'.P.#<..}.

C:\Users\user\AppData\Local\Temp\nhde	
Process:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
File Type:	data
Category:	dropped
Size (bytes):	59441
Entropy (8bit):	4.972654246459409
Encrypted:	false
SSDEEP:	768:QWeteWZ6yuLDwhWeHhYFIaxTtGU5/nxWEFdGv6ypEK+U5/YpNfVXw6M+oLLmuNyF:UfWLDwsceGEFd2Zl/cfjovQFJTpkAB
MD5:	F88C142D13998842037A6149E08A7AF3
SHA1:	DEB11C8456734B9D77CA451764145BCAE2C8A3D5
SHA-256:	0321365F007604FAC07BC584931929CDFA7C2DE6C2DE31DE24CE36168DDD24F8
SHA-512:	643742D7C2FE77F0C6D2424C3947391DD1E1D03CADAE388A43FB3CCD5F2BB63B13C476311F3510C7BA57812C33715465EAFCE5CD37E242B48D508B1F3DBD23E
Malicious:	false

C:\Users\user\AppData\Local\Temp\nhde	
Reputation:	low
Preview:	U..P!.....*....,_.....x....2.....*.....*....z....1.....W.....q.....~.....J.....f..... .....~.....f....t.....f.....f.....~.....~....-.....q.....F.....9....9....9.....r..... .....F.....r....t.....r.....r.....F.....F....-.....q..... ...n.!...>."....#....$....%....&....'...R.(...9.)...9.*...9.+.....,.. ...-...z...../....0...n.1....2....3....4....5....6...z.7...t.8....9....:....;....<...z

C:\Users\user\AppData\Local\Temp\nsmBB29.tmp\System.dll	
Process:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: RFQ-BCM 03122020.exe, Detection: malicious, Browse • Filename: 7ujc2szSQX.exe, Detection: malicious, Browse • Filename: TT0900090000090.exe, Detection: malicious, Browse • Filename: Poczta Polska Informacje o transakcjach2021.exe, Detection: malicious, Browse • Filename: PO-006 dtd-15.06.2021.exe, Detection: malicious, Browse • Filename: SKM_4050210326102400 jpg.exe, Detection: malicious, Browse • Filename: IMGG087 76543.exe, Detection: malicious, Browse • Filename: yfr02XrveJ.exe, Detection: malicious, Browse • Filename: LCdraft6152021_pdf.exe, Detection: malicious, Browse • Filename: LCdraft6152021_pdf.exe, Detection: malicious, Browse • Filename: Consigment Details_pdf.exe, Detection: malicious, Browse • Filename: bigfish.exe, Detection: malicious, Browse • Filename: INQUIRY for IFM 20207.xlsx, Detection: malicious, Browse • Filename: gz7dLhKlSQ.exe, Detection: malicious, Browse • Filename: WGOc4eHYqX.exe, Detection: malicious, Browse • Filename: Purchase_Order.xlsx, Detection: malicious, Browse • Filename: ojmanoq.exe, Detection: malicious, Browse • Filename: linkfuq.exe, Detection: malicious, Browse • Filename: takwqaytr.exe, Detection: malicious, Browse • Filename: PO_403.xlsx, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nst9B9A.tmp\System.dll	
Process:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nst9B9A.tmp\System.dll	
Joe Sandbox View:	• Filename: RFQ-BCM 03122020.exe, Detection: malicious, Browse • Filename: 7ujc2szSQX.exe, Detection: malicious, Browse • Filename: TT0900090000090.exe, Detection: malicious, Browse • Filename: Poczta Polska Informacje o transakcjach2021.exe, Detection: malicious, Browse • Filename: PO-006 dtd-15.06.2021.exe, Detection: malicious, Browse • Filename: SKM_4050210326102400 jpg.exe, Detection: malicious, Browse • Filename: IMGG087 76543.exe, Detection: malicious, Browse • Filename: yfr02XrveJ.exe, Detection: malicious, Browse • Filename: LCdraft6152021_pdf.exe, Detection: malicious, Browse • Filename: LCdraft6152021_pdf.exe, Detection: malicious, Browse • Filename: Consigment Details_pdf.exe, Detection: malicious, Browse • Filename: bigfish.exe, Detection: malicious, Browse • Filename: INQUIRY for IFM 20207.xlsx, Detection: malicious, Browse • Filename: gz7dLhKlSQ.exe, Detection: malicious, Browse • Filename: WGOc4eHYqX.exe, Detection: malicious, Browse • Filename: Purchase_Order.xlsx, Detection: malicious, Browse • Filename: ojmanoq.exe, Detection: malicious, Browse • Filename: linkfuq.exe, Detection: malicious, Browse • Filename: takwqaytr.exe, Detection: malicious, Browse • Filename: PO_403.xlsx, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-D.-D.-D...J.*.D.-E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsu6AA7.tmp\System.dll	
Process:	C:\Users\user\Desktop\US1pwXib6h.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-D.-D.-D...J.*.D.-E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe	
Process:	C:\Users\user\Desktop\US1pwXib6h.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	218807
Entropy (8bit):	7.899471179052997
Encrypted:	false
SSDEEP:	6144:cQqTMHNItf88WBtvd9r4nmKNeyPObWhqxD4cft:yMHCtf88WBtvd9c5NJhAJ
MD5:	91514B3627E78E42CB05BC608737A47F
SHA1:	B48882A3D656068E30B88671AEE71010E5602D32
SHA-256:	E0E0CA8EC324752ED823C7E503992398E817663828F94B4CA699FF1965095C31
SHA-512:	B50BE6BED7809B76697B4E9849453A12ADE782AFD43F63AE1C8207EE11E26F95E374293CDC4523F5A5B00030D564E67C04EFC0F80C5B2571EE37D19ECB08FC7E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L. .....K.....Z.....0.....p....@.....s.....h.....p.....text... .X.....Z..... ..`.rdata.....p.....^.....@..@.data...x.....p.....@....ndata.....@.....rsrc...h.....t.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.899471179052997
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	US1pwXib6h.exe
File size:	218807
MD5:	91514b3627e78e42cb05bc608737a47f
SHA1:	b48882a3d656068e30b88671aee71010e5602d32
SHA256:	e0e0ca8ec324752ed823c7e503992398e817663828f94b4ca699ff1965095c31
SHA512:	b50be6bed7809b76697b4e9849453a12ade782afd43f63e1c8207ee11e26f95e374293cdc4523f5a5b00030d564e67c04efc0f80c5b2571ee37d19ecb08fc7e
SSDEEP:	6144:cQqTMHNItf88WBtvd9r4nmKNeyPObWhqxD4cft:yMHCtf88WBtvd9c5NJhAJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....Z.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030cb
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:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C1 [Sat Dec 5 22:50:41 2009 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x58d2	0x5a00	False	0.665234375	data	6.43310034828	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.17976375781	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af78	0x400	False	0.55078125	data	4.6178023207	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0xc68	0xe00	False	0.407087053571	data	3.98321239368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

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 12:19:02.181119919 CEST	192.168.2.6	8.8.8.8	0xa981	Standard query (0)	netno.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:03.857049942 CEST	192.168.2.6	8.8.8.8	0x153f	Standard query (0)	ddns.dbcdubai.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:25.109397888 CEST	192.168.2.6	8.8.8.8	0xd759	Standard query (0)	netsecond.duckdns.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:26.901343107 CEST	192.168.2.6	8.8.8.8	0xef55	Standard query (0)	netno.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:28.439774036 CEST	192.168.2.6	8.8.8.8	0xbe9c	Standard query (0)	ddns.dbcdubai.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:49.807735920 CEST	192.168.2.6	8.8.8.8	0xfd2a	Standard query (0)	netsecond.duckdns.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:51.366024971 CEST	192.168.2.6	8.8.8.8	0xeb32	Standard query (0)	netno.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:53.751140118 CEST	192.168.2.6	8.8.8.8	0x9e36	Standard query (0)	ddns.dbcdubai.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:15.064660072 CEST	192.168.2.6	8.8.8.8	0x26bb	Standard query (0)	netsecond.duckdns.org	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:16.798211098 CEST	192.168.2.6	8.8.8.8	0xd59b	Standard query (0)	netno.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:18.346585035 CEST	192.168.2.6	8.8.8.8	0x38ae	Standard query (0)	ddns.dbcdubai.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:39.602674007 CEST	192.168.2.6	8.8.8.8	0x142c	Standard query (0)	netsecond.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:20:41.307471037 CEST	192.168.2.6	8.8.8.8	0xdce	Standard query (0)	netno.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:42.847150087 CEST	192.168.2.6	8.8.8.8	0x2e10	Standard query (0)	ddns.dbcdu bai.com	A (IP address)	IN (0x0001)

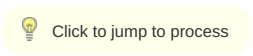
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:19:02.244160891 CEST	8.8.8.8	192.168.2.6	0xa981	No error (0)	netno.ddns.net		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:03.941929102 CEST	8.8.8.8	192.168.2.6	0x153f	No error (0)	ddns.dbcdu bai.com		99.83.154.118	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:25.335073948 CEST	8.8.8.8	192.168.2.6	0xd759	No error (0)	netsecond. duckdns.org		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:26.965903997 CEST	8.8.8.8	192.168.2.6	0xef55	No error (0)	netno.ddns.net		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:28.531289101 CEST	8.8.8.8	192.168.2.6	0xbe9c	No error (0)	ddns.dbcdu bai.com		99.83.154.118	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:49.877819061 CEST	8.8.8.8	192.168.2.6	0xfd2a	No error (0)	netsecond. duckdns.org		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:51.425685883 CEST	8.8.8.8	192.168.2.6	0xeb32	No error (0)	netno.ddns.net		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:19:53.814482927 CEST	8.8.8.8	192.168.2.6	0x9e36	No error (0)	ddns.dbcdu bai.com		99.83.154.118	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:15.285846949 CEST	8.8.8.8	192.168.2.6	0x26bb	No error (0)	netsecond. duckdns.org		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:16.868933916 CEST	8.8.8.8	192.168.2.6	0xd59b	No error (0)	netno.ddns.net		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:18.406245947 CEST	8.8.8.8	192.168.2.6	0x38ae	No error (0)	ddns.dbcdu bai.com		99.83.154.118	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:39.823373079 CEST	8.8.8.8	192.168.2.6	0x142c	No error (0)	netsecond. duckdns.org		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:41.377844095 CEST	8.8.8.8	192.168.2.6	0xdce	No error (0)	netno.ddns.net		192.71.172.145	A (IP address)	IN (0x0001)
Jun 16, 2021 12:20:42.909445047 CEST	8.8.8.8	192.168.2.6	0x2e10	No error (0)	ddns.dbcdu bai.com		99.83.154.118	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: US1pwXib6h.exe PID: 6476 Parent PID: 5980

General

Start time:	12:18:56
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\US1pwXib6h.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\US1pwXib6h.exe'
Imagebase:	0x400000
File size:	218807 bytes
MD5 hash:	91514B3627E78E42CB05BC608737A47F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000001.00000002.367065114.00000000024C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: US1pwXib6h.exe PID: 6548 Parent PID: 6476

General

Start time:	12:18:57
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\US1pwXib6h.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\US1pwXib6h.exe'
Imagebase:	0x400000
File size:	218807 bytes
MD5 hash:	91514B3627E78E42CB05BC608737A47F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000002.00000001.363673900.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000002.00000002.621612280.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: ioldfli.exe PID: 6768 Parent PID: 3440

General

Start time:	12:19:08
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe'
Imagebase:	0x400000
File size:	218807 bytes
MD5 hash:	91514B3627E78E42CB05BC608737A47F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000004.00000002.395120542.00000000024E0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: ioldfli.exe PID: 6824 Parent PID: 6768

General

Start time:	12:19:10
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe'
Imagebase:	0x400000
File size:	218807 bytes
MD5 hash:	91514B3627E78E42CB05BC608737A47F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000006.00000002.394088134.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000006.00000001.393727825.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ioldfli.exe PID: 7012 Parent PID: 3440

General

Start time:	12:19:16
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe'
Imagebase:	0x400000
File size:	218807 bytes
MD5 hash:	91514B3627E78E42CB05BC608737A47F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000007.00000002.406739098.00000000023A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: ioldfli.exe PID: 7088 Parent PID: 7012

General

Start time:	12:19:18
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\fatbtifdnumsa\ioldfli.exe'
Imagebase:	0x400000
File size:	218807 bytes
MD5 hash:	91514B3627E78E42CB05BC608737A47F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000001.405669006.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000002.406157548.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis