

---

---

# Malware Analysis

---

---

Analysis of PE Virus Share Sample  
VirusShare\_00fad140e44ea8ff485639c00d2632ab

EDITED BY

Joshua Mol

*Malicious Code; Design & Defense*

2020  
Joshua Mol

## Table of Contents

<b>VirusShare_00fad140e44ea8ff485639c00d2632ab (PE Sample)</b> .....	<b>3</b>
Virus-Total & PE Info .....	3
Summary of Analysis.....	5
Static Analysis Output.....	6
Strings Output.....	7
Dynamic Analysis .....	15

## VirusShare 00fad140e44ea8ff485639c00d2632ab (PE Sample):

### Virus Total Submission:

VirusTotal

https://www.virustotal.com/gui/file/6a633d1f7d9a4090bf9b2fce4b0b412ad1fe93687222e26375899f1764b5d4d0

6a633d1f7d9a4090bf9b2fce4b0b412ad1fe93687222e26375899f1764b5d4d0

#### Basic Properties

MD5	00fad140e44ea8ff485639c00d2632ab
SHA-1	d5c942bcb3a4f52d9344fa8318c040940ef5af7
SHA-256	6a633d1f7d9a4090bf9b2fce4b0b412ad1fe93687222e26375899f1764b5d4d0
Vhash	015046651d1c1b2572303287z
Authenticash	cd6638b9c3e611e8802ac77a61e11875de8f893bef112a204bcec27f5ef936e
Imphash	0239fd611af3d0e9b0c46c5837c80e09
SSDEEP	1536:czvQSZpGS4/31A6mQgL2eYCGDwRcMkVQd8YhY0/EqKlzmnd:nSHIG6mQwGmfOQd8YhY0/EnUG
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	104.00 KB (106496 bytes)

#### History

Creation Time	2016-06-23 16:04:21
First Submission	2019-06-28 01:28:41
Last Submission	2019-06-28 01:28:41
Last Analysis	2019-08-05 23:20:48

#### Portable Executable Info

##### Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2016-06-23 16:04:21
Entry Point	80350
Contained Sections	4

##### Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	79605	79872	6.49	94fa411af1cc6bb168a3ea0e66e80f78
.rdata	86016	16480	16896	4.27	e98728080737698bec00f33c7685cfe9
.data	106496	548388	512	0.94	6f6a918ed1358864f48dc3dd3b6a853b
.x	655360	8192	8192	0.22	043902a75236d9b2b186b7129a1061de

##### Imports

### Indicators:


xml-id	indicator (27)	detail	level
1430	The file references string(s) tagged as blacklist	count: 43	1
1269	The file references blacklist library(ies)	count: 1	1
1434	The file references a URL pattern	url: http://noniwire8.beget.tech/Brokenskull/fre.php	1
1120	The file is scored by virustotal	score: 62/71	1
1266	The file imports symbol(s) tagged as blacklist	count: 9	1
1245	The file contains a blacklist section	section: .x	1
1124	The file references MITRE Technique(s)	count: 1	2
1262	The file imports anonymous function(s)	count: 9	2
1036	The file checksum is invalid	checksum: 0x00000000	2

### Suspicious Sections:


property	value	value	value	value
name		.rdata	.data	.x
md5	94FA411AF1CC6BB168A3EA...	E98728080737698BEC00F33C...	6F6A918ED1358864F48DC3D...	043902A75236D9B2B186B71...
entropy	6.492	4.269	0.944	0.217
file-ratio (99.04%)	75.00 %	15.87 %	0.48 %	7.69 %
raw-address	0x00000400	0x00013C00	0x00017E00	0x00018000
raw-size (105472 bytes)	0x00013800 (79872 bytes)	0x00004200 (16896 bytes)	0x00000200 (512 bytes)	0x00002000 (8192 bytes)
virtual-address	0x00401000	0x00415000	0x0041A000	0x004A0000
virtual-size (652665 bytes)	0x000136F5 (79605 bytes)	0x00004060 (16480 bytes)	0x00085E24 (548388 bytes)	0x00002000 (8192 bytes)
entry-point	0x000139DE	-	-	-
writable	-	-	x	x
executable	x	-	-	-

Suspicious Libraries:


The ws2\_32.dll is a networking library that allows the executable to have internet access.

 c:\users\joshu\desktop\virussware_00fad140e44e	indicators (6/27)	library (4)	blacklist (1)	type (1)	imports (19)
	virustotal (62/71)	ws2_32.dll	x	implicit	8
	> dos-header (64 bytes)	kernel32.dll	-	implicit	5
	> dos-stub (176 bytes)	ole32.dll	-	implicit	3
	> file-header (Jun.2016)	oleaut32.dll	-	implicit	3
	> optional-header (file-checksum)				
	> directories (2)				
	> sections (blacklist)				
	> libraries (1/4)				
	> imports (9/19)				

Used Networking Functionality:

 c:\users\joshu\desktop\virussware_00fad140e44e	indicators (6/27)	name (19)	group (3)	MITRE-Technique (0)	type (1)	anonymous (9)	blacklist (9)
	virustotal (62/71)	getaddrinfo	network	-	implicit	-	x
	> dos-header (64 bytes)	freeaddrinfo	network	-	implicit	-	x
	> dos-stub (176 bytes)	3 (closesocket)	network	-	implicit	x	x
	> file-header (Jun.2016)	115 (WSAStartup)	network	-	implicit	x	x
	> optional-header (file-checksum)	23 (socket)	network	-	implicit	x	x
	> directories (2)	19 (send)	network	-	implicit	x	x
	> sections (blacklist)	16 (recv)	network	-	implicit	x	x
	> libraries (1/4)	4 (connect)	network	-	implicit	x	x
	> imports (9/19)	SetLastError	diagnostic	-	implicit	-	x
	> exports (n/a)	GetProcessHeap	memory	-	implicit	-	-
	> tls-callbacks (n/a)	HeapFree	memory	-	implicit	-	-
	> resources (n/a)	HeapAlloc	memory	-	implicit	-	-
	abc strings (43/1549)	GetLastError	diagnostic	-	implicit	-	-

DOS Header:

pestudio 8.99 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\desktop\virussware_00fad140e44e44ea8ff485639c00d2632ab]		
file help		
 c:\users\ieuser\desktop\virussware_00fad140e44e		
indicators (5/26)	property	value
virustotal (offline)	md5	C71DBF70F255AAAE2BD8EDDE53E90DF3
> dos-header (64 bytes)	sha1	F354F1A5D35E308381CD1F9DA57E34F32F1CC345
> dos-stub (176 bytes)	sha256	38BD2AC08737CB9460DE15EC665103A8947107107696261BF42D77E70F42F26D
> file-header (Jun.2016)	size	0x40 (64 bytes)
> optional-header (file-checksum)	entropy	4.678
> directories (2)	file-ratio	0.00 %
> sections (blacklist)	file-header-offset	0x000000F0
> libraries (1/4)		
> imports (9/19)		
> exports (n/a)		
> tls-callbacks (n/a)		
> resources (n/a)		
abc strings (43/1549)		
> debug (n/a)		
> manifest (n/a)		
> version (n/a)		

## Summary of Analysis:

### All Dynamic Analysis was Done Securely Before Allowing the Virus to Communicate with the Internet

This is a 32bit PE executable virus, that checks for debuggers and has built-in anti-debugging prevention measures through-out the code.

Once executed outside of a debugger, in my case as a regular .exe. The executable begins by assessing its environment and checking if the system has already been infected. If the executable determines that it's the first time being executed it will then add registry keys enabling shell execution.

The executable then begins to attempt a buffer overflow. After which 21 "HKCU\Software\" keys are set. This is followed by 3 additional attempts of the buffer overflow, which consists of making 2 RegQueryValue queries of the same entry.

The executable then spawns a 32bit background process named "578B2E.exe" which is executed from a new hidden directory "%AppData%\Roaming\213B95\" along a companion file 578B2E.lck. The companion file is a 'Lock File' used to disable 2 or more users from editing a Database at the same time. It has been determined the '.lck' file is associated to a specific Database type being SQLite. This database SQLite was referenced within the static analysis strings output and thus assumed to be the database being locked by the ".lck" file. It was also discovered that the naming of these files and directory are randomly generated upon execution, providing enhanced heuristic detection from antivirus engines. Possibly a strategy from the "<https://FuckAV.ru>" website URL that was hardcoded into the executable.

Next the Idle process configures 2 alternate IPv6 interfaces and advertises one of the new addresses to the router, using this new interface and address the process begins to make 2 DNS queries routing the traffic through the newly created interface. The first of which requests utilizing IPv6, then one using IPv4. Only the IPv6 obtained a response consisting of "No such name A noniwire8.beget.tech SOA ns1.beget.com". After attempting a manual request, it was determined that the host to which the process contacts was shutdown. Possible reasoning for this routing of data through newly generated IP's is so that companies that monitor PC's network traffic won't be able to determine the PC of which the traffic originated. As for the second IPv6 address it seems to be used to assign the SQLite database an IP address, to allow the infected device to send new database entries to the device without creating external network traffic. Next communication begins with another IPv4 address "20.36.219.28" this connection uses TLS on port 443 and is encrypted, 14 packets are exchanged in total, with 4 containing application data. Navigating to this IP using HTTPS yields an XML error page with the message "No HTTP resource was found that matches the request url <http://20.36.219.28/>". This indicates the server is waiting for a specific URL to be within the request.

Next the executable removes itself from the hard disk.

Further investigation into the idle process indicates that this idle process is a possible American banking key logger. Indicators for this were CPU activity during the loading of: "[https://global.americanexpress.com/login?inav=ca\\_utility\\_login](https://global.americanexpress.com/login?inav=ca_utility_login)", other Canadian logins were excluded from this activity. During the POST of the Login form of the banking website the process begins to communicate with a different host through use of an IPv4 address "23.6.90.65" without the use of DNS. All traffic within this connection is encrypted. Attempting to navigate the IP in a web browser yields an Invalid Response page. I believe this may be an FTP server used to send harvested credentials to a central server.

## Static Analysis Output:

PE32 executable (GUI) Intel 80386, for MS Windows

File: 'VirusShare\_00fad140e44ea8ff485639c00d2632ab'

Size: 106496      Blocks: 208      IO Block: 4096   regular file

Device: 801h/2049d   Inode: 1448106   Links: 1

Access: (0644/-rw-r--r--)   Uid: ( 1000/   remnux)   Gid: ( 1000/   remnux)

Access: 2020-03-29 20:17:42.953730855 -0400

Modify: 2020-03-23 07:38:32.000000000 -0400

Change: 2020-03-29 20:17:42.949730855 -0400

Birth: -

Type: PE32,

Arc: executable,

MD5: 00fad140e44ea8ff485639c00d2632ab,

SHA1: d5c942bcb3a4f52d9344fa8318c040940efd5af7,

SHA256: 6a633d1f7d9a4090bf9b2fce4b0b412ad1fe93687222e26375899f1764b5d4d0,

SHA512:

65b01f075e2b940ada2b8c0be678c20042d9fe7a6c91835e74deaca9263dd91521ae8a6876e92d  
694836efd89b5dd214c77e76b836497ce675c04c0727fef0d4,

## Strings Output:

!This program cannot be run in DOS mode.

Rich

.text

`.rdata

@.data

UVW3

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

\$@0123456789ABCDEF

open

.tmp

%s\\*

Windows

Program Files

%s\%s

%s\%s\%s%\$

%s\%s%\$

UNIQUE

SQLite format 3

DIRycq1tP2vSeogj5bEUFzQiHT9dmKCn6uf7xsOY0  
hpwr43VINX8JGBAKLMZW

U2XpekVvtYq0fwsx7EDuZjrCo9GcF1B6HI358mbzn  
yLWdMANa4TSKJhliOPgQR

http://

https://

MachineGuid

SOFTWARE\Microsoft\CryptographySeDebugPrivil  
ege

ntdll.dll

LdrGetProcedureAddress

RtlNtStatusToDosError

RtlSetLastWin32Error

ZwQueryInformationProcess

RtlCreateUserThread

ZwAllocateVirtualMemory

NtFreeVirtualMemory

NtWriteVirtualMemory

ZwReadVirtualMemory

ZwResumeThread

/%s>

last\_compatible\_version

password\_value

username\_value

origin\_url

logins

%s\%s\User Data\Default\Login Data

%s\%s\User Data\Default\Web Data

%s%\$Login Data

%s%\$Default\Login Data

Comodo\Dragon

MapleStudio\ChromePlus

Google\Chrome

Nichrome

RockMelt

Spark

Chromium

Titan Browser

Torch  
Yandex\YandexBrowser  
Epic Privacy Browser  
CocCoc\Browser  
Vivaldi  
Comodo\Chromodo  
Superbird  
Coowon\Coowon  
Mustang Browser  
360Browser\Browser  
CatalinaGroup\Citrio  
Google\Chrome SxS  
Orbitum  
Iridium  
\Opera\Opera Next\data  
\Opera Software\Opera Stable  
\Fenrir  
Inc\Sleipnir\setting\modules\ChromiumViewer  
\Fenrir  
Inc\Sleipnir5\setting\modules\ChromiumViewer  
vaultcli.dll  
VaultEnumerateItems  
VaultEnumerateVaults  
VaultFree  
VaultGetItem  
VaultOpenVault  
VaultCloseVaultSoftware\Microsoft\Internet Explorer\IntelliForms\Storage2  
%s%02X  
file:///  
Software\Microsoft\Internet Explorer\TypedURLs

SELECT encryptedUsername, encryptedPassword, formSubmitURL, hostname FROM moz\_logins  
hostname  
encryptedUsername  
encryptedPassword  
%s\logins.json  
%s\prefs.js  
%s\signons.sqlite  
signons.txt  
signons2.txt  
signons3.txt  
%s\Mozilla\Firefox\profiles.ini  
%s\Mozilla\Firefox\Profiles\%s  
%s\Mozilla\SeaMonkey\profiles.ini  
%s\Mozilla\SeaMonkey\Profiles\%s  
%s\Flock\Browser\profiles.ini  
%s\Flock\Browser\Profiles\%s  
%s\Thunderbird\profiles.ini  
%s\Thunderbird\Profiles\%s  
%s\K-Meleon\profiles.ini  
%s\K-Meleon\%s  
%s\Comodo\IceDragon\profiles.ini  
%s\Comodo\IceDragon\Profiles\%s  
%s\NETGATE Technologies\BlackHawk\profiles.ini  
%s\NETGATE Technologies\BlackHawk\Profiles\%s  
%s\Postbox\profiles.ini  
%s\Postbox\Profiles\%s  
%s\8pecxstudios\Cyberfox\profiles.ini  
%s\8pecxstudios\Cyberfox\Profiles\%s  
%s\Moonchild Productions\Pale Moon\profiles.ini



%s\Moonchild Productions\Pale  
Moon\Profiles\%s

%s\FossaMail\profiles.ini

%s\FossaMail\Profiles\%s

%s\Lunascap6\Lunascap6\plugins\{9BDD5314-  
20A6-4d98-AB30-8325A95771EE}\data

Profile%i

Path

Profiles/

PATH

%s\nss3.dll

NSS\_Init

NSS\_Shutdown

PK11\_GetInternalKeySlot

PK11\_FreeSlot

PK11\_Authenticate

PK11SDR\_Decrypt

PK11\_CheckUserPassword

SECITEM\_FreeItem

sqlite3.dll

mozsqlite3.dll

nss3.dll

sqlite3\_finalize

sqlite3\_step

sqlite3\_close

sqlite3\_column\_text

sqlite3\_open16

sqlite3\_prepare\_v2

sqlite3\_prepareCurrentVersion

SOFTWARE\Mozilla\Mozilla Firefox

%s\%s\Main

Install Directory

PathToExe

SOFTWARE\Mozilla\Mozilla Thunderbird

SOFTWARE\Mozilla\FossaMail

SOFTWARE\Postbox\Postbox

SOFTWARE\Mozilla\Flock

SOFTWARE\Flock\Flock

(x86)

%ProgramW6432%

%s\NETGATE\Black Hawk

SOFTWARE\Mozilla\Pale Moon

%s\Lunascap6\Lunascap6\plugins\{9BDD5314-  
20A6-4d98-AB30-8325A95771EE}

SOFTWARE\K-Meleon

SetupPath

SOFTWARE\ComodoGroup\IceDragon\Setup

RootDir

SOFTWARE\8pecxstudios\Cyberfox86

SOFTWARE\8pecxstudios\Cyberfox

SOFTWARE\mozilla.org\SeaMonkey

%s\Mozilla\Profiles

SOFTWARE\Mozilla\SeaMonkey

SOFTWARE\Mozilla\Waterfox

ffffff

@@firefox.exe

kernel32.dll

CloseHandle

CreateFileW

WriteFile

ExitProcessCrypt32.dll

CryptStringToBinaryA

Shlwapi.dll

StrStrA

GetProcAddress

LoadLibraryW

%s\Opera

wand.dat

Xl2\$6\*9(SKiasb+lv<.qF58\_qwe~QsRTYvdeTYbfor  
m\_password\_control

form\_username\_control

Software\QtWeb.NET\QtWeb Internet  
Browser\AutoComplete

%s\QupZilla\profiles\default\browsedata.db

array

dict

data

string

Server

InstallDir

SOFTWARE\Apple Computer, Inc.\Safari

%s\Apple Computer\Preferences\keychain.plist

%s\Apple Application Support\plutil.exe

.xml

-convert xml1 -s -o %s "%s"

%s\Data\AccCfg\Accounts.tdat

%s\Storage

Account.rec0

%s\Foxmail\mail

\*.stg

%SYSTEMDRIVE%

Foxmail\*

EmailAddress

Technology

PopServer

PopPort

PopAccount

PopPassword

SmtpServer

SmtpPort

SmtpAccount

SmtpPassword

Software\IncrediMail\Identities

UserName

Passwd

POP3Server

POP3Port

Email

SMTP Email Address

SMTP Server

SMTP User Name

SMTP User

POP3 Server

POP3 User Name

POP3 User

NNTP Email Address

NNTP User Name

NNTP Server

IMAP Server

IMAP User Name

<u>IMAP User</u>	<u>*.bscp</u>
<u>HTTP User</u>	<u>LastUsedProfile</u>
<u>HTTP Server URL</u>	<u>Software\Bitvise\BvSshClient</u>
<u>HTTPMail User Name</u>	<u>%s\BlazeFtp\site.dat</u>
<u>HTTPMail Server</u>	<u>Software\FlashPeak\BlazeFtp\Settings</u>
<u>POP3 Port</u>	<u>LastPassword</u>
<u>SMTP Port</u>	<u>LastUser</u>
<u>IMAP Port</u>	<u>LastAddress</u>
<u>POP3 Password2</u>	<u>LastPort</u>
<u>IMAP Password2</u>	<u>Server</u>
<u>NNTP Password2</u>	<u>Password</u>
<u>HTTPMail Password2</u>	<u>_Password</u>
<u>SMTP Password2</u>	<u>Software\NCH Software\ClassicFTP\FTPAccounts</u>
<u>POP3 Password</u>	<u>settings</u>
<u>IMAP Password</u>	<u>name</u>
<u>NNTP Password</u>	<u>value</u>
<u>HTTP Password</u>	<u>%s\Cyberduck</u>
<u>SMTP Password</u>	<u>user.config</u>
<u>Software\Microsoft\Windows</u>	<u>%s\iterate_GmbH</u>
<u>NT\CurrentVersion\Windows Messaging</u>	<u>%s\EasyFTP\data</u>
<u>Subsystem\Profiles\Outlook</u>	<u>server</u>
<u>Software\Microsoft\Office\15.0\Outlook\Profiles\</u>	<u>username</u>
<u>Outlook</u>	<u>protocol</u>
<u>Software\Microsoft\Office\16.0\Outlook\Profiles\</u>	<u>%s\ExpanDrive</u>
<u>Outlook</u>	<u>*favorites.js</u>
<u>%s\32BitFtp.TMP</u>	<u>drives.js</u>
<u>%s\32BitFtp.ini</u>	<u>%s%c</u>
<u>%s\Estsoft\ALFTP\ESTdb2.dat</u>	<u>User</u>
<u>%s\site.xml</u>	<u>HostName</u>
<u>%s\BitKinex\bitkinex.ds</u>	<u>Software\Far\Plugins\FTP\Hosts</u>
<u>*.tlp</u>	

Software\Far2\Plugins\FTP\Hosts

%s\Far Manager\Profile\PluginsData\42E4AEB1-A230-44F4-B33C-F195BB654931.db

%s\FileZilla\Filezilla.xml

%s\FileZilla\filezilla.xml

%s\FileZilla\recentservers.xml

%s\FileZilla\sitemanager.xml

%s\FlashFXP

\*Sites.dat

\*quick.dat

FtpServer

FtpUserName

FtpPassword

\_FtpPassword

Software\NCH Software\Fling\Accounts

%s\FreshWebmaster\FreshFTP\FtpSites.SMF

%s\FTPBox\profiles.conf

%s\FTPGetter\Profile\servers.xml

%s\FTPGetter\servers.xml

%s\FTPInfo\ServerList.xml

%s\FTPInfo\ServerList.cfg

%s\FTP Navigator\Ftplist.txt

%s\FTP Now\sites.xml

%s\FTPShell\ftpshell.fsi

%s\.config\fullsync\profiles.xml

%s\DeluxeFTP\sites.xml

%s\GoFTP\settings\Connections.txt

JaSftp

AbleFTP

Automize

%s\%s%i\encPwd.jsd

%s\%s%i\data\settings\sshProfiles-j.jsd

%s\%s%i\data\settings\ftpProfiles-j.jsd

Pass

Host

Port

Software\LinusFTP\Site Manager

%s\oZone3D\MyFTP\myftp.ini

%s\NetDrive\NDSites.ini

%s\NetDrive2\drives.dat

%s\Fastream NETFile\My FTP Links

%s\NexusFile\userdata\ftpsite.ini

%s\NexusFile\ftpsite.ini

%s\INSoftware\NovaFTP\NovaFTP.db

%s\Notepad++\plugins\config\NppFTP\NppFTP.xml

%s\Odin Secure FTP Expert\QFDefault.QFQ

%s\Odin Secure FTP Expert\SiteInfo.QFP

PublicKeyFile

TerminalType

PortNumber

Software\9bis.com\KiTTY\Sessions

Software\SimonTatham\PuTTY\Sessions

\_dec

%s\_dec

Isasrv.dll

LsalCryptUnprotectData

Isass.exe

%s\Microsoft\Credentials

Config Path

Software\VanDyke\SecureFX

%s\Sessions

\*.ini

Port

UserName

Password

%s\SftpNetDrive

\*.cfg

%s\Sherrod Computers\sherrod FTP\favorites

#document.favoriteManager\*

%s\SmartFTP

{\*.xml

%s\Staff-FTP\sites.ini

%s\Steed\bookmarks.txt

%s\SuperPutty

Sessions\*

sftp://

ftp://

ftps://

http://

https://

{.:CRED:.:}

{CREN}

{CRDB}

Profiles

%s\Syncovery

Syncovery.ini

%s\wcx\_ftp.ini

%s\GHISLER\wcx\_ftp.ini

FtpIniName

Software\Ghisler\Total Commander

%s\UltraFXP\sites.xml

%s\WinFtp Client\Favorites.dat

FSProtocol

Software\Martin Prikryl

%s\WS\_FTP\WS\_FTP.INI

%s\WS\_FTP.INI

%s\lpswitch

ws\_ftp.ini

%s\NetSarang\Xftp\Sessions

\*xftp

%s\%s\%s.exe

.exe

.dll

Fuckav.ru

aPLib v1.01 - the smaller the better :)

Copyright (c) 1998-2009 by Joergen Ibsen, All Rights Reserved.

More information:

<http://www.ibsensoftware.com/>

DEST

DEST

getaddrinfo

freeaddrinfo

WS2\_32.dll

GetLastError

SetLastError

HeapAlloc

HeapFree

GetProcessHeap

KERNEL32.dll

CoInitialize

CoUninitialize

CoCreateInstance

ole32.dll

OLEAUT32.dll

t\$\$

<http://noniwire8.beget.tech/Brozenskull/fre.php>

## Dynamic Analysis Findings:

After starting the executable, its process is shown to be created below.

Monitoring for new Processes

Start	End	PID	User	CmdLine	Path
5:46:03 PM	5:47:03 PM	1840	joshu		C:\Windows\System32\backgroundTaskHost.exe
5:46:11 PM	5:46:13 PM	2200	joshu		C:\Users\joshu\Desktop\virusshare_00fad140e44ea8ff485639c00d2632ab.exe
5:47:41 PM		1928	joshu		C:\Windows\System32\SnippingTool.exe
5:47:44 PM	5:48:45 PM	1780	joshu		C:\Windows\System32\backgroundTaskHost.exe
5:48:12 PM		1CAC	SYSTEM		C:\Windows\System32\SearchProtocolHost.exe
5:48:12 PM	5:50:17 PM	228C	SYSTEM		C:\Windows\System32\SearchFilterHost.exe
5:50:17 PM		D7C	SYSTEM		C:\Windows\System32\SearchFilterHost.exe

Information 4/21/2020 5:46:11 PM Sysmon 1 Process Create (rule: ProcessCreate)  
Information 4/21/2020 5:46:00 PM Sysmon 1 Process Create (rule: ProcessCreate)  
Information 4/21/2020 5:44:43 PM Sysmon 1 Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

Process Create:  
RuleName:  
UtcTime: 2020-04-21 21:46:11.274  
ProcessGuid: {50edb7cc-69a3-5e9f-0000-00105d9c5000}  
ProcessId: 8908  
Image: C:\Users\joshu\Desktop\VirusShare\_00fad140e44ea8ff485639c00d2632ab.exe  
FileVersion: ?  
Description: ?

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 4/21/2020 5:46:11 PM  
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)  
Level: Information Keywords:  
User: SYSTEM Computer: DESKTOP-KVHR0R1  
OpCode: Info  
More Information: [Event Log Online Help](#)

5:46:11.28975...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND
5:46:11.29056...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND
5:46:11.29319...	VirusShare_00f...	8908	Load Image	C:\Windows\System32\wow64.dll	SUCCESS
5:46:11.29341...	VirusShare_00f...	8908	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS
5:46:11.29549...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\86\VirusShare_00fad140e44ea8f48563c00d2632ab.exe	NAME NOT FOUND
5:46:11.29552...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\86\Default	SUCCESS
5:46:11.29707...	VirusShare_00f...	8908	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS
5:46:11.30086...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS
5:46:11.30089...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND
5:46:11.30119...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS
5:46:11.30121...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND
5:46:11.30268...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS
5:46:11.30299...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS
5:46:11.30481...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS
5:46:11.30504...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS
5:46:11.30506...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\FileSystem\LongPathsEnabled	SUCCESS
5:46:11.30567...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
5:46:11.30694...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS
5:46:11.30699...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\LogFlags	NAME NOT FOUND
5:46:11.30731...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS
5:46:11.30733...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ShowDebugInfo	NAME NOT FOUND
5:46:11.30966...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS
5:46:11.30969...	VirusShare_00f...	8908	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CACHE	SUCCESS
5:46:11.31039...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS
5:46:11.31041...	VirusShare_00f...	8908	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CACHE	SUCCESS
5:46:11.31100...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS
5:46:11.31102...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND
5:46:11.31177...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS

5:46:11.32938...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Notifications\418A073AA38C8075		BUFFER TOO SMALL	L
5:46:11.32947...	VirusShare_00f...	8908	RegQueryValue	HKLM\System\CurrentControlSet\Control\Notifications\418A073AA38C8075		SUCCESS	T
5:46:11.32970...	VirusShare_00f...	8908	RegSetInfoKey	HKLM		SUCCESS	K
5:46:11.33006...	VirusShare_00f...	8908	RegSetInfoKey	HKCU		SUCCESS	K
5:46:11.33049...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Classes\Local Settings\Software\Microsoft		SUCCESS	K
5:46:11.33269...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\wm32.dll		SUCCESS	K
5:46:11.33452...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize		SUCCESS	K
5:46:11.33455...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles		NAME NOT FOUND	L
5:46:11.33506...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32\VirusShare_00fad140e...		NAME NOT FOUND	L
5:46:11.33624...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows		SUCCESS	K
5:46:11.33627...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs		SUCCESS	T
5:46:11.33944...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\shell32.dll		SUCCESS	K
5:46:11.33986...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\cfmgpr32.dll		SUCCESS	Ir
5:46:11.34022...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\SHCore.dll		SUCCESS	Ir
5:46:11.34065...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\windows.storage.dll		SUCCESS	Ir
5:46:11.34101...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\profapi.dll		SUCCESS	Ir
5:46:11.34129...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\powrprof.dll		SUCCESS	Ir
5:46:11.34155...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\umpdc.dll		SUCCESS	Ir
5:46:11.34180...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\shlwapi.dll		SUCCESS	Ir
5:46:11.34209...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\kernel.appcore.dll		SUCCESS	Ir
5:46:11.34239...	VirusShare_00f...	8908	Load Image	C:\Windows\SysWOW64\cryptsp.dll		SUCCESS	Ir
5:46:11.34626...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001		SUCCESS	K
5:46:11.34628...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name		BUFFER OVERFLOW	L
5:46:11.34631...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name		SUCCESS	T
5:46:11.34634...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name		BUFFER OVERFLOW	L
5:46:11.34637...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name		SUCCESS	T
5:46:11.34657...	VirusShare_00f...	8908	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro...		SUCCESS	K
5:46:11.34659...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro...		SUCCESS	T
5:46:11.34662...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro...		BUFFER OVERFLOW	L
5:46:11.34664...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro...		SUCCESS	T
5:46:11.34667...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro...		BUFFER OVERFLOW	L
5:46:11.34669...	VirusShare_00f...	8908	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro...		SUCCESS	T

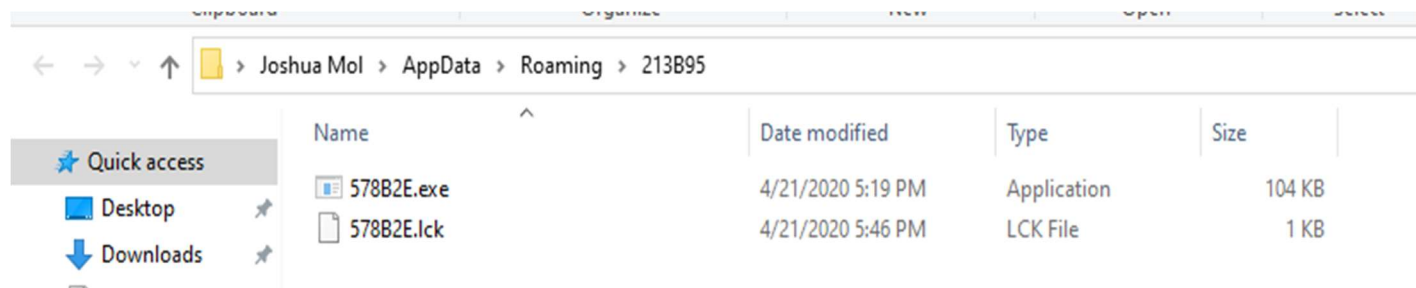
5:46:12.04914...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\7-Zip	SUCCESS
5:46:12.05442...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\AppDataLow	SUCCESS
5:46:12.05909...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Google	SUCCESS
5:46:12.06348...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Hex-Rays	SUCCESS
5:46:12.06802...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\JetBrains	SUCCESS
5:46:12.07241...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\McAfee	SUCCESS
5:46:12.07684...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Microsoft	SUCCESS
5:46:12.08205...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\vnasm	SUCCESS
5:46:12.08805...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Nmap	SUCCESS
5:46:12.09320...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Node.js	SUCCESS
5:46:12.09828...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Policies	SUCCESS
5:46:12.10337...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\QtProject	SUCCESS
5:46:12.10824...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Realtek	SUCCESS
5:46:12.11303...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\RegisteredApplications	SUCCESS
5:46:12.11781...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\SweetScape	SUCCESS
5:46:12.12343...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Synaptics	SUCCESS
5:46:12.12903...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Sysinternals	SUCCESS
5:46:12.13394...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\VB and VBA Program Settings	SUCCESS
5:46:12.13958...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\WJR	SUCCESS
5:46:12.14482...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Wow6432Node	SUCCESS
5:46:12.15037...	VirusShare_00f...	8908	RegSetInfoKey	HKCU\Software\Classes	SUCCESS







During this process a new executable was created.



This new executable starts by making 2 new IPv6 interfaces.

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : cgocable.net
IPv6 Address. . . . . : 2001:1970:55e6:0:242f:f61d:cc30:9e73
IPv6 Address. . . . . : 2001:1970:55e6:0:c1fb:e11d:3124:e3e5
Temporary IPv6 Address. . . . . : 2001:1970:55e6:0:602f:7cf7:bbbc:6ae8
Link-local IPv6 Address . . . . . : fe80::242f:f61d:cc30:9e73%11
IPv4 Address. . . . . : 192.168.0.99
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::481d:70ff:feae:efba%11
                             192.168.0.1
```

Next the executable starts its initial communications.

7	5.067389	2001:1970:55e6:0:e0f...	2001:1970:c06e:c0::93	DNS	100 Standard query 0xdf74 A noniwire8.beget.tech
8	5.091906	2001:1970:55e6:0:e0f...	2001:1970:c0c0:6ec0::...	DNS	100 Standard query 0xdf74 A noniwire8.beget.tech
9	5.110532	2001:1970:c0c0:6ec0::...	2001:1970:55e6:0:e0fa...	DNS	160 Standard query response 0xdf74 No such name A noniwire8.beget.tech SOA ns1.beget.com
10	6.058773	fe80::481d:70ff:feae...	ff02::1	ICMPv6	150 Router Advertisement from 4a:1d:70:ae:ef:ba
11	6.749330	192.168.0.99	20.36.219.28	TCP	1494 50220 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1440 [TCP segment of a reassembled PDU]
12	6.749333	192.168.0.99	20.36.219.28	TLSv1.2	217 Application Data
13	6.749567	192.168.0.99	20.36.219.28	TCP	1494 50220 → 443 [ACK] Seq=1604 Ack=1 Win=258 Len=1440 [TCP segment of a reassembled PDU]
14	6.749569	192.168.0.99	20.36.219.28	TCP	1494 50220 → 443 [ACK] Seq=3044 Ack=1 Win=258 Len=1440 [TCP segment of a reassembled PDU]
15	6.749578	192.168.0.99	20.36.219.28	TLSv1.2	689 Application Data
16	6.803227	20.36.219.28	192.168.0.99	TCP	56 443 → 50220 [ACK] Seq=1 Ack=1604 Win=2053 Len=0
17	6.804286	20.36.219.28	192.168.0.99	TCP	56 443 → 50220 [ACK] Seq=1 Ack=5119 Win=2053 Len=0
18	6.817805	20.36.219.28	192.168.0.99	TLSv1.2	1407 [TCP Previous segment not captured] , Ignored Unknown Record
19	6.817916	192.168.0.99	20.36.219.28	TCP	66 [TCP Dup ACK 11#1] 50220 → 443 [ACK] Seq=5119 Ack=1 Win=258 Len=0 SLE=2921 SRE=4274
20	6.818296	20.36.219.28	192.168.0.99	TCP	1514 [TCP Out-Of-Order] 443 → 50220 [ACK] Seq=1 Ack=5119 Win=2053 Len=1460
21	6.818341	192.168.0.99	20.36.219.28	TCP	66 50220 → 443 [ACK] Seq=5119 Ack=1461 Win=258 Len=0 SLE=2921 SRE=4274
22	6.822352	20.36.219.28	192.168.0.99	TCP	1514 [TCP Retransmission] 443 → 50220 [ACK] Seq=1461 Ack=5119 Win=2053 Len=1460
23	6.822488	192.168.0.99	20.36.219.28	TCP	54 50220 → 443 [ACK] Seq=5119 Ack=4274 Win=258 Len=0
24	6.845840	192.168.0.99	20.36.219.28	TCP	1494 50220 → 443 [ACK] Seq=5119 Ack=4274 Win=258 Len=1440 [TCP segment of a reassembled PDU]
25	6.845843	192.168.0.99	20.36.219.28	TLSv1.2	204 Application Data
26	6.887196	20.36.219.28	192.168.0.99	TCP	60 443 → 50220 [ACK] Seq=4274 Ack=6709 Win=2053 Len=0
27	6.916615	20.36.219.28	192.168.0.99	TLSv1.2	1252 Application Data
28	6.961761	192.168.0.99	20.36.219.28	TCP	54 50220 → 443 [ACK] Seq=6709 Ack=5472 Win=254 Len=0
29	9.089278	fe80::481d:70ff:feae...	ff02::1	ICMPv6	150 Router Advertisement from 4a:1d:70:ae:ef:ba
30	10.118502	fe80::481d:70ff:feae...	2001:1970:55e6:0:e0fa...	ICMPv6	86 Neighbor Solicitation for 2001:1970:55e6:0:e0fa:b8e4:f3f2:ba9e from 4a:1d:70:ae:ef:ba
31	10.118646	2001:1970:55e6:0:e0f...	fe80::481d:70ff:feae...	ICMPv6	86 Neighbor Advertisement 2001:1970:55e6:0:e0fa:b8e4:f3f2:ba9e (sol, ovr) is at b0:10:41:2a:77:d5
32	10.427014	192.168.0.226	255.255.255.255	UDP	82 57621 → 57621 Len=40
33	12.121057	fe80::481d:70ff:feae...	ff02::1	ICMPv6	150 Router Advertisement from 4a:1d:70:ae:ef:ba
34	13.246894	192.168.0.177	239.255.255.250	SSDP	167 M-SEARCH * HTTP/1.1
35	15.150519	fe80::481d:70ff:feae...	ff02::1	ICMPv6	150 Router Advertisement from 4a:1d:70:ae:ef:ba
36	15.210296	2600:141b:5000:592::...	2001:1970:55e6:0:e0fa...	TLSv1.2	105 Encrypted Alert
37	15.210466	2001:1970:55e6:0:e0f...	2600:141b:5000:592::1...	TCP	74 50221 → 443 [ACK] Seq=1 Ack=32 Win=1023 Len=0

After this it begins to make 2 DNS queries.

Event 22, Sysmon

Level	Date and Time	Source	Event ID	Task Category
Information	4/21/2020 5:46:14 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	4/21/2020 5:46:14 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	4/21/2020 5:46:13 PM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	4/21/2020 5:46:11 PM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/21/2020 5:46:11 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/21/2020 5:46:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/21/2020 5:44:43 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Dns query:  
RuleName:  
UtcTime: 2020-04-21 21:46:13.169  
ProcessGuid: {50edb7cc-69a3-5e9f-0000-00105d9c5000}  
ProcessId: 8908  
QueryName: noniwire8.beget.tech  
QueryStatus: 9003  
QueryResults:

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon  
Event ID: 22  
Level: Information  
User: SYSTEM  
OpCode: Info  
More Information: [Event Log Online Help](#)

Event 22, Sysmon

Level	Date and Time	Source	Event ID	Task Category
Information	4/21/2020 5:46:18 PM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/21/2020 5:46:14 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	4/21/2020 5:46:14 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	4/21/2020 5:46:13 PM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	4/21/2020 5:46:11 PM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/21/2020 5:46:11 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/21/2020 5:46:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/21/2020 5:44:43 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Dns query:  
RuleName:  
UtcTime: 2020-04-21 21:46:12.888  
ProcessGuid: {50edb7cc-69a3-5e9f-0000-00105d9c5000}  
ProcessId: 8908  
QueryName: noniwire8.beget.tech  
QueryStatus: 123  
QueryResults:

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon  
Event ID: 22  
Level: Information  
User: SYSTEM  
OpCode: Info  
More Information: [Event Log Online Help](#)

14	8.194300	2001:1970:55e6:0:602...	2001:1970:c06e:c0::93	DNS	100	Standard query 0x5029 A noniwire8.beget.tech
15	8.213673	192.168.0.99	24.226.1.93	DNS	80	Standard query 0x5029 A noniwire8.beget.tech
16	8.380510	2001:1970:c06e:c0::93	2001:1970:55e6:0:602f...	DNS	160	Standard query response 0x5029 No such name A noniwire8.beget.tech SOA ns1.beget.com

Followed by the original executable process terminating.

Event 5, Sysmon

Level	Date and Time	Source	Event ID	Task Category
Information	4/21/2020 5:46:13 PM	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	4/21/2020 5:46:11 PM	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/21/2020 5:46:11 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/21/2020 5:46:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/21/2020 5:44:43 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Process terminated:  
RuleName:  
UtcTime: 2020-04-21 21:46:13.456  
ProcessGuid: {50edb7cc-69a3-5e9f-0000-00105d9c5000}  
ProcessId: 8908  
Image: C:\Users\joshu\Desktop\VirusShare\_00fad140e44ea8ff485639c00d2632ab.exe

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon  
Event ID: 5  
Level: Information  
User: SYSTEM  
OpCode: Info  
More Information: [Event Log Online Help](#)

After the original process terminates the new process remains idle.

>  Windows Command Processor ...	0%	2.7 MB	0 MB/s	0 Mbps	Very low	Very low
>  Windows Explorer	0.5%	40.0 MB	0 MB/s	0 Mbps	Very low	Very low
Background processes (40)						
>  64-bit Synaptics Pointing Enhancer...	0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
578B2E.exe (32 bit)	0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
AMD External Events Client Mo...	0%	1.0 MB	0 MB/s	0 Mbps	Very low	Very low

Once the American express login page is visited, the idle process begins to send the traffic shown below, I also navigated to the site where it didn't show a valid certificate, as well as didn't except a basic / directory in the url.

← → ↻ 🏠 🔍 | https://23.6.91.236/ | ☆ ⚙️

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

[Go to your Start page](#)

Details

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination
650	14.410183	2001:1970:55e6:0:602...	2600:140a:0:780::1e80
651	14.416954	2600:140a:0:780::1e80	2001:1970:55e6:0:602f...
652	14.417045	2001:1970:55e6:0:602...	2600:140a:0:780::1e80
653	14.417115	2001:1970:55e6:0:602...	2600:140a:0:780::1e80
654	14.439304	2600:140a:0:780::1e80	2001:1970:55e6:0:602f...
655	14.725982	23.6.91.236	192.168.0.99
656	14.726078	192.168.0.99	23.6.91.236
657	14.726883	23.6.91.236	192.168.0.99
658	14.726975	192.168.0.99	23.6.91.236
659	14.727025	192.168.0.99	23.6.91.236
660	14.759688	23.6.91.236	192.168.0.99
661	15.472335	23.6.90.65	192.168.0.99
662	15.472503	192.168.0.99	23.6.90.65
663	15.473374	23.6.90.65	192.168.0.99
664	15.473516	192.168.0.99	23.6.90.65
665	15.473591	192.168.0.99	23.6.90.65
666	15.490131	23.6.90.65	192.168.0.99