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

Table of Contents

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.

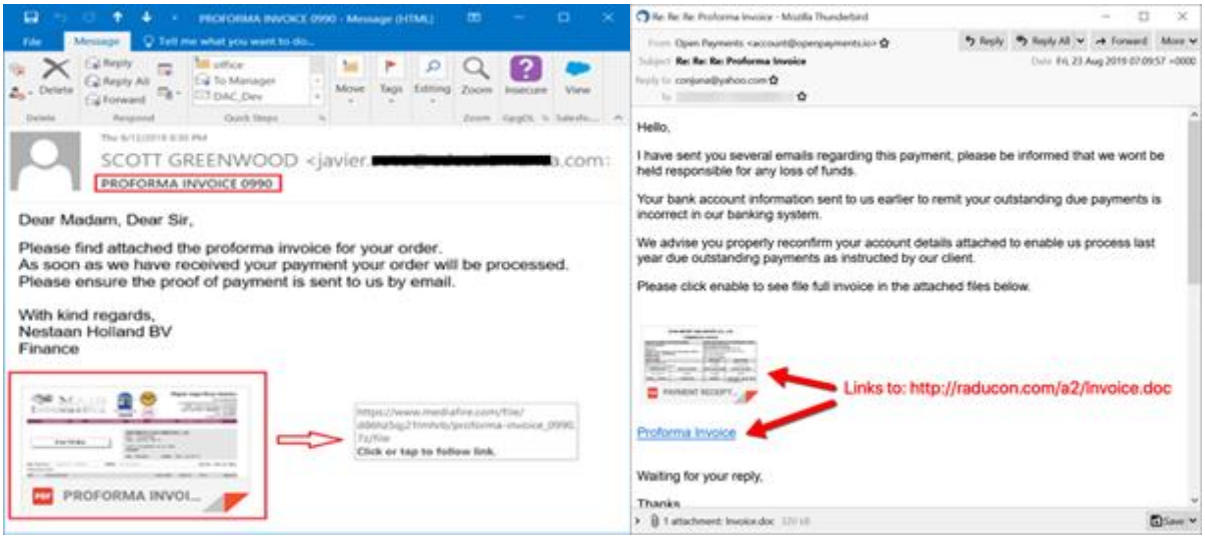


Figure 1: NetWire phishing templates

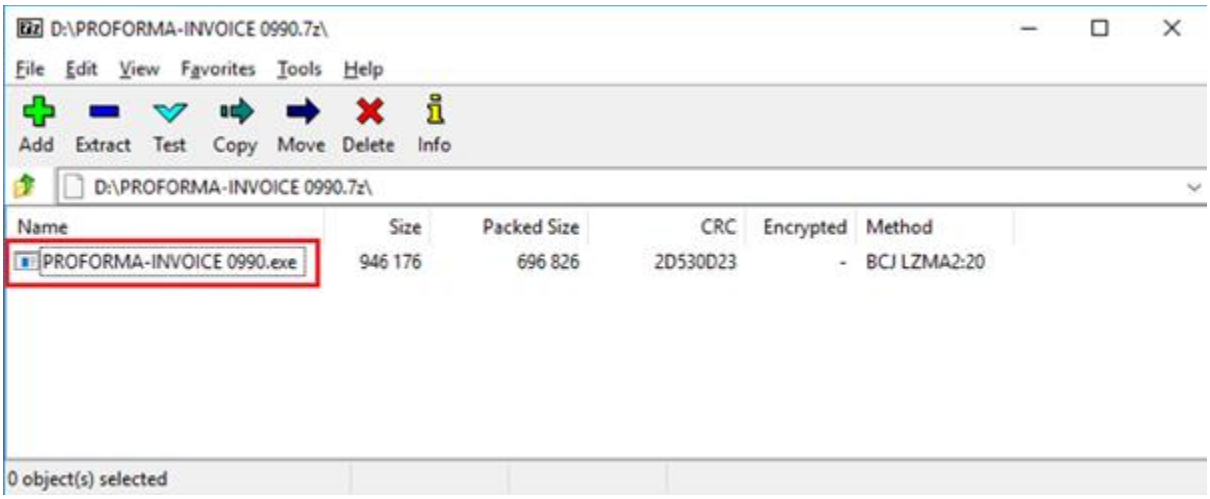


Figure 2: ZIP file containing the NetWire binary inside

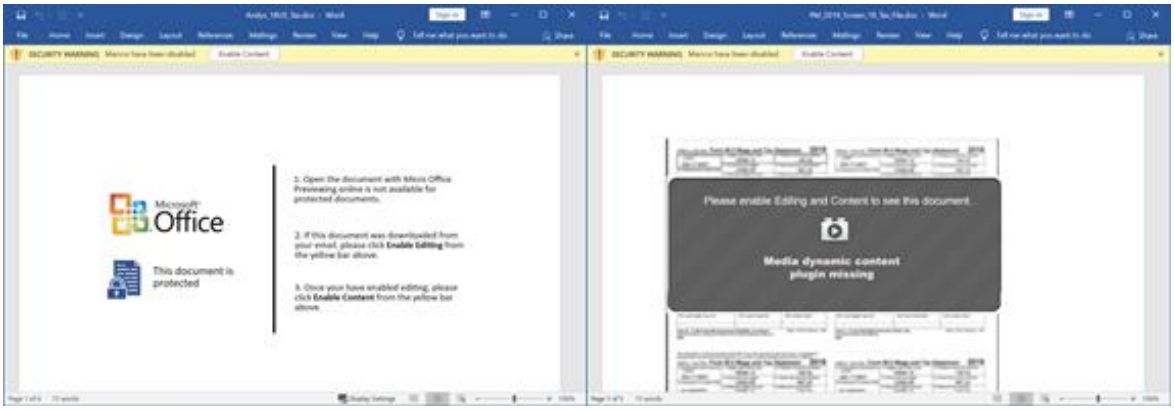


Figure 3: Word file with a malicious macro that will download the NetWire binary from the C2 server

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.

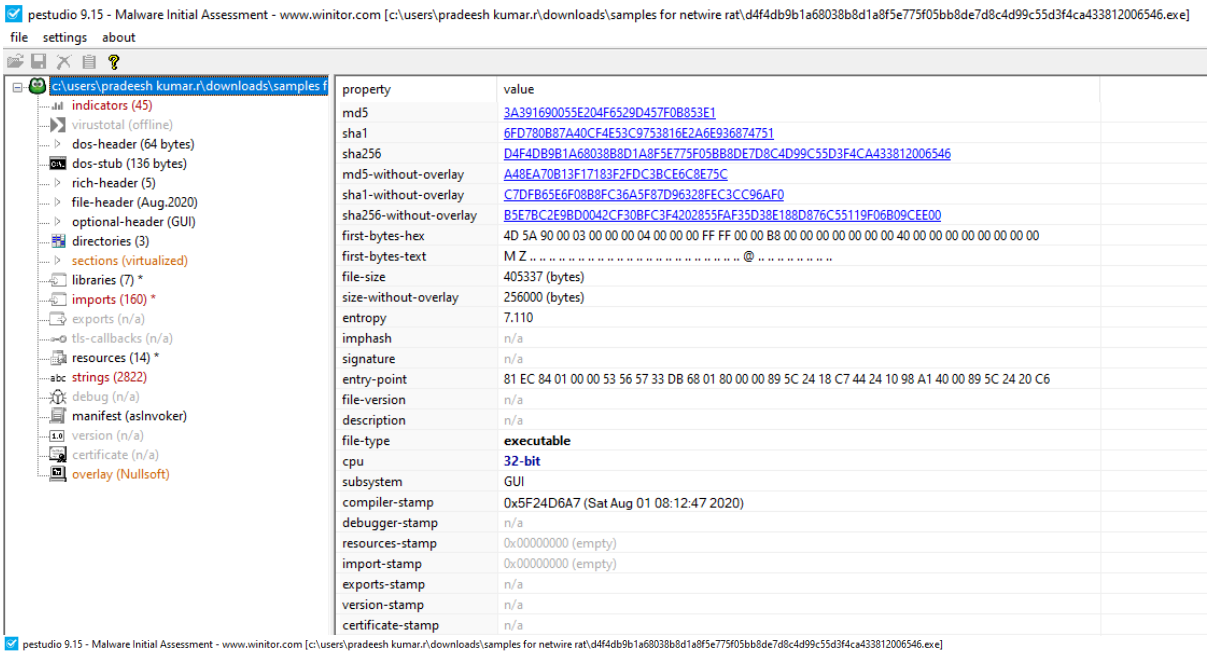
Strings for the samples are extracted and placed in the below location

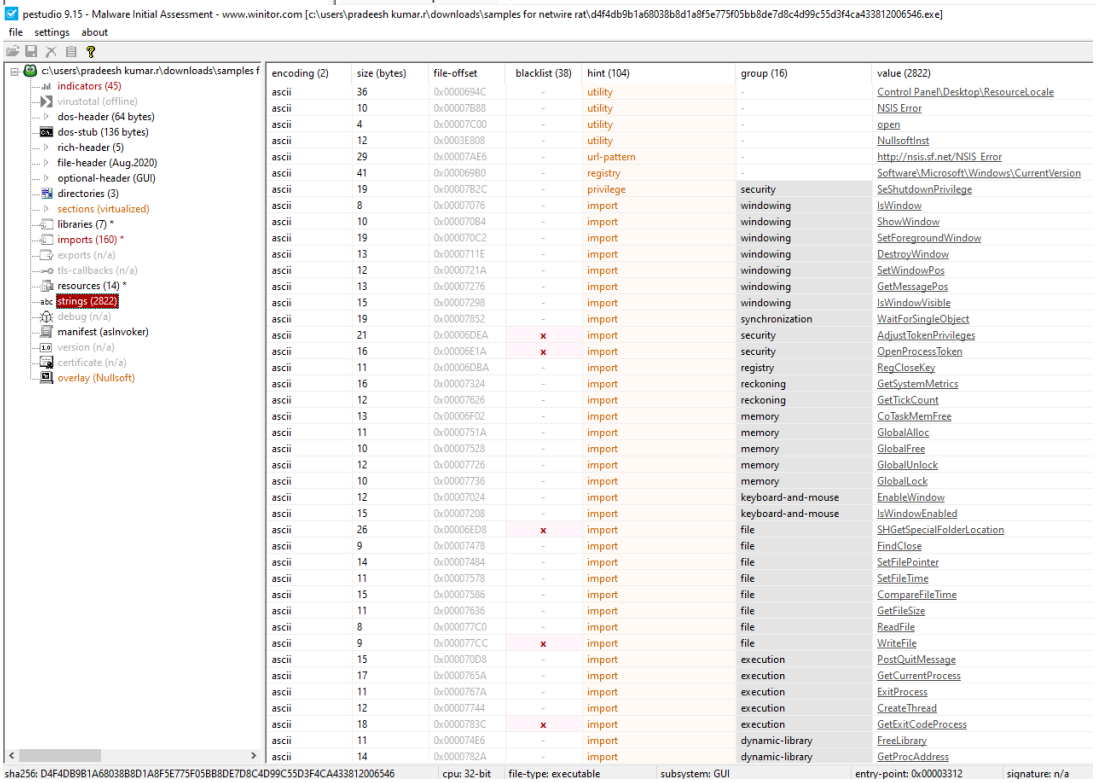
CS-5202-Threat-intelligence/StringsForNetWireRat.txt at main · PradeeshKumar-NIIT/CS-5202-Threat-intelligence (github.com)

PEStudio

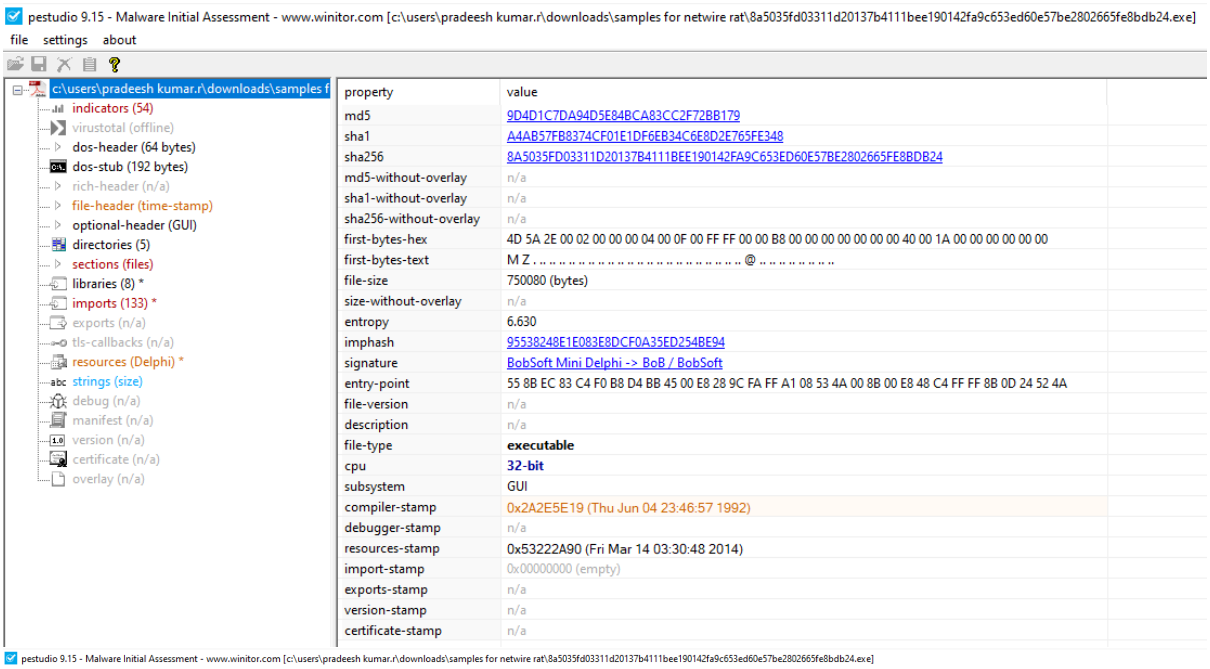
PEStudio is a portable tool that performs malware assessments on executable files. Since the target file is never launched during the investigation, you can safely evaluate the file, in addition to malware, without risk.

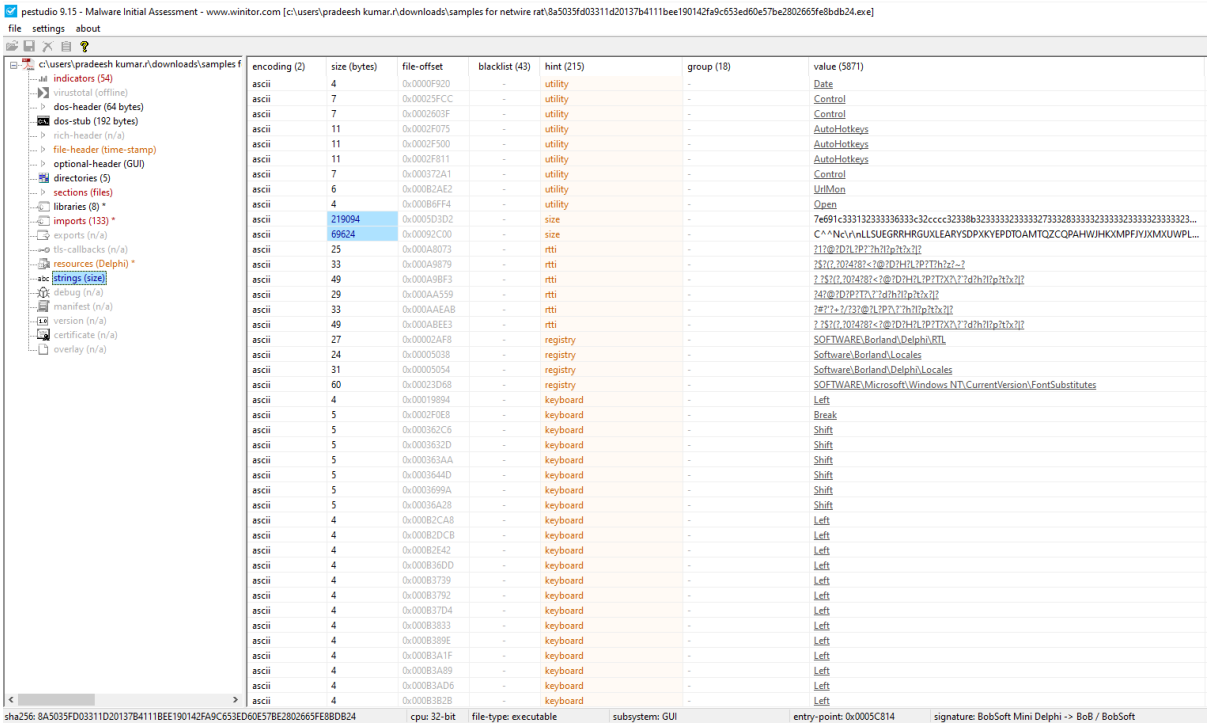
File Name	8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24.exe
MD5	9d4d1c7da94d5e84bca83cc2f72bb179
SHA1	a4ab57fb8374cf01e1df6eb34c6e8d2e765fe348
SHA256	8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24





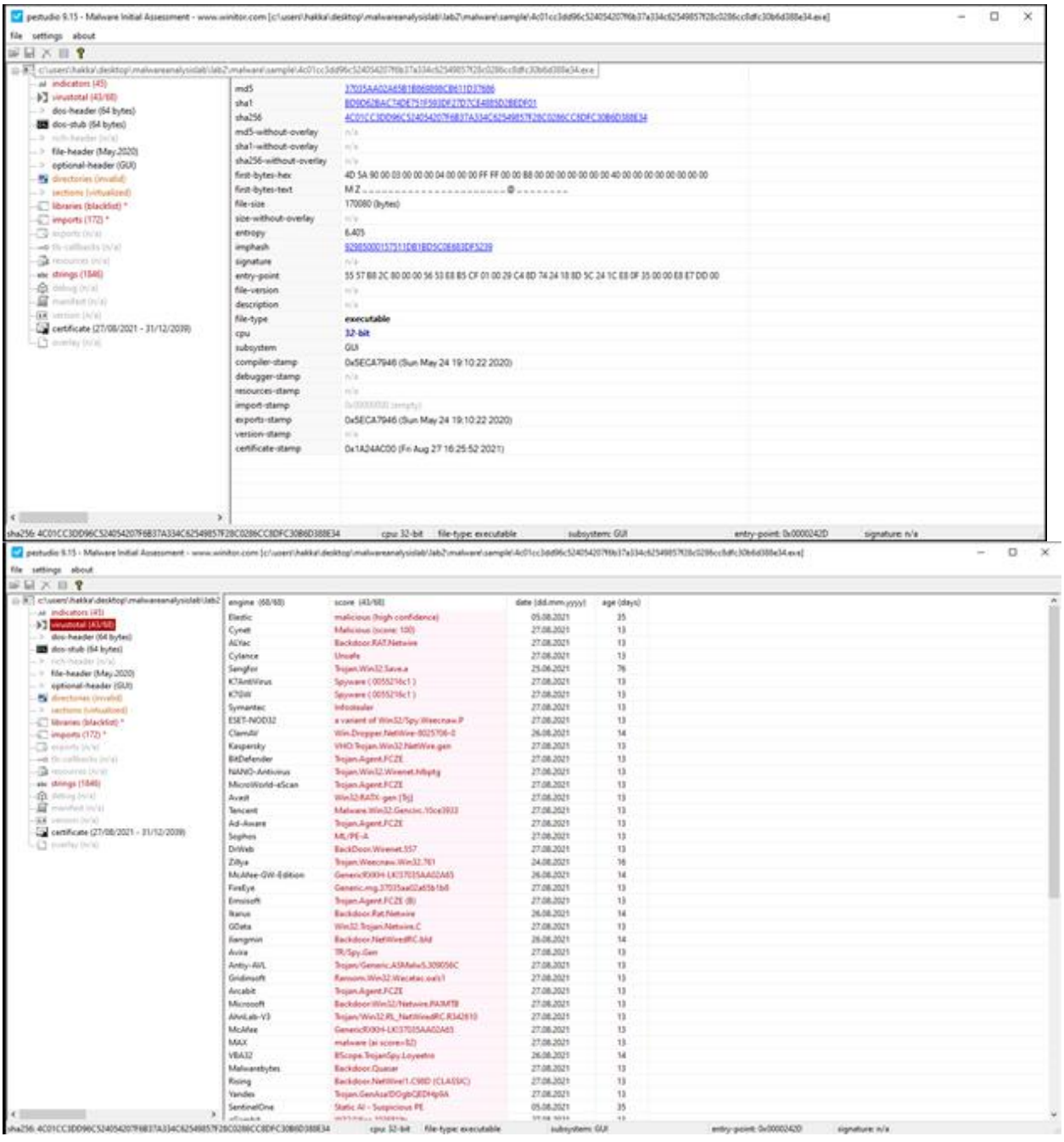
File Name	d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546.exe
MD5	3a391690055e204f6529d457f0b853e1
SHA1	6fd780b87a40cf4e53c9753816e2a6e936874751
SHA256	d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546

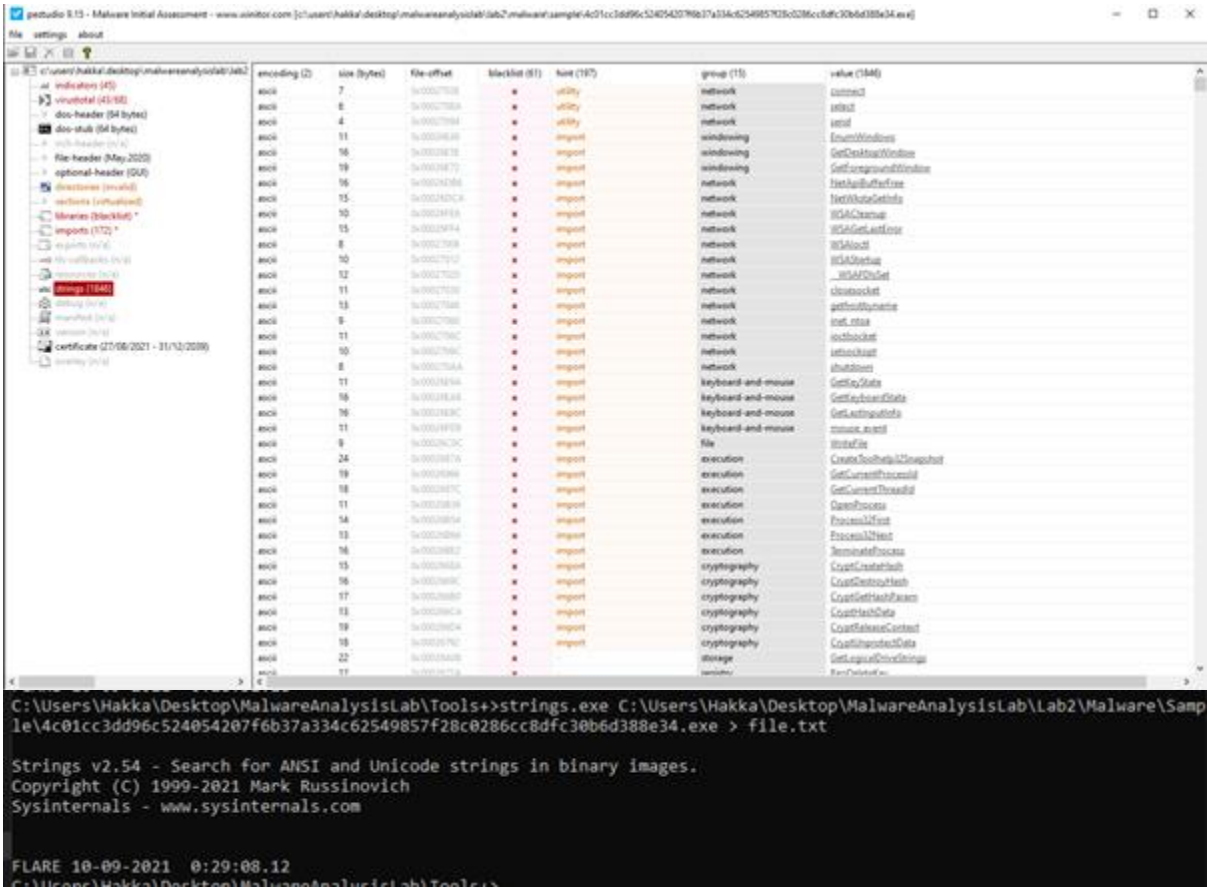

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\pradeesh kumar.r\downloads\samples for netwire rat\8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24.exe]
file settings about
c:\users\pradeesh kumar.r\downloads\samples f
indicators (54)
virustotal (offline)
dos-header (64 bytes)
dos-stub (192 bytes)
rich-header (n/a)
file-header (time-stamp)
optional-header (GUI)
directories (5)
sections (files)
libraries (8) *
imports (133) *
exports (n/a)
tls-callbacks (n/a)
resources (Delphi) *
strings (size)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)
property value
md5 9D4D1C7DA94D5E84BCA83CC2F72BB179
sha1 A4AB57FB8374CF01E1DF6EB34C6E8D2E765FE348
sha256 8A5035FD03311D20137B4111BEE190142FA9C653ED60E57BE2802665FE8BDB24
md5-without-overlay n/a
sha1-without-overlay n/a
sha256-without-overlay n/a
first-bytes-hex 4D 5A 2E 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00
first-bytes-text M Z . . . . . @ . . . . . .
file-size 750080 (bytes)
size-without-overlay n/a
entropy 6.630
imphash 95538248E1E083E8DCF0A35ED254BE94
signature BobSoft Mini Delphi -> BoB / BobSoft
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
file-version n/a
description n/a
file-type executable
cpu 32-bit
subsystem GUI
compiler-stamp 0x2A2E5E19 (Thu Jun 04 23:46:57 1992)
debugger-stamp n/a
resources-stamp 0x53222A90 (Fri Mar 14 03:30:48 2014)
import-stamp 0x00000000 (empty)
exports-stamp n/a
version-stamp n/a
certificate-stamp n/a


pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\pradeesh kumar.r\downloads\samples for netwire rat\8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24.exe]
file settings about
encoding (2) size (bytes) file-offset blacklist (43) hint (215) group (18) value (5871)
sha256: 8A5035FD03311D20137B4111BEE190142FA9C653ED60E57BE2802665FE8BDB24
cpu: 32-bit
file-type: executable
subsystem: GUI
entry-point: 0x0005C814
signature: BobSoft Mini Delphi -> BoB / BobSoft

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

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




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

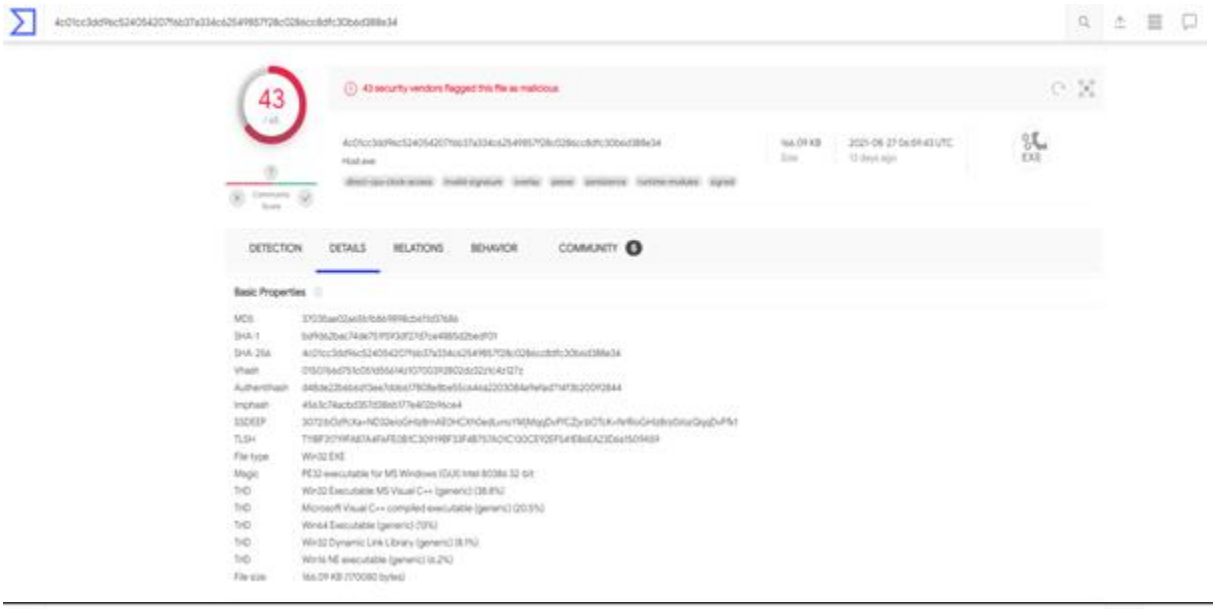
file.txt - Notepad

File Edit Format View Help

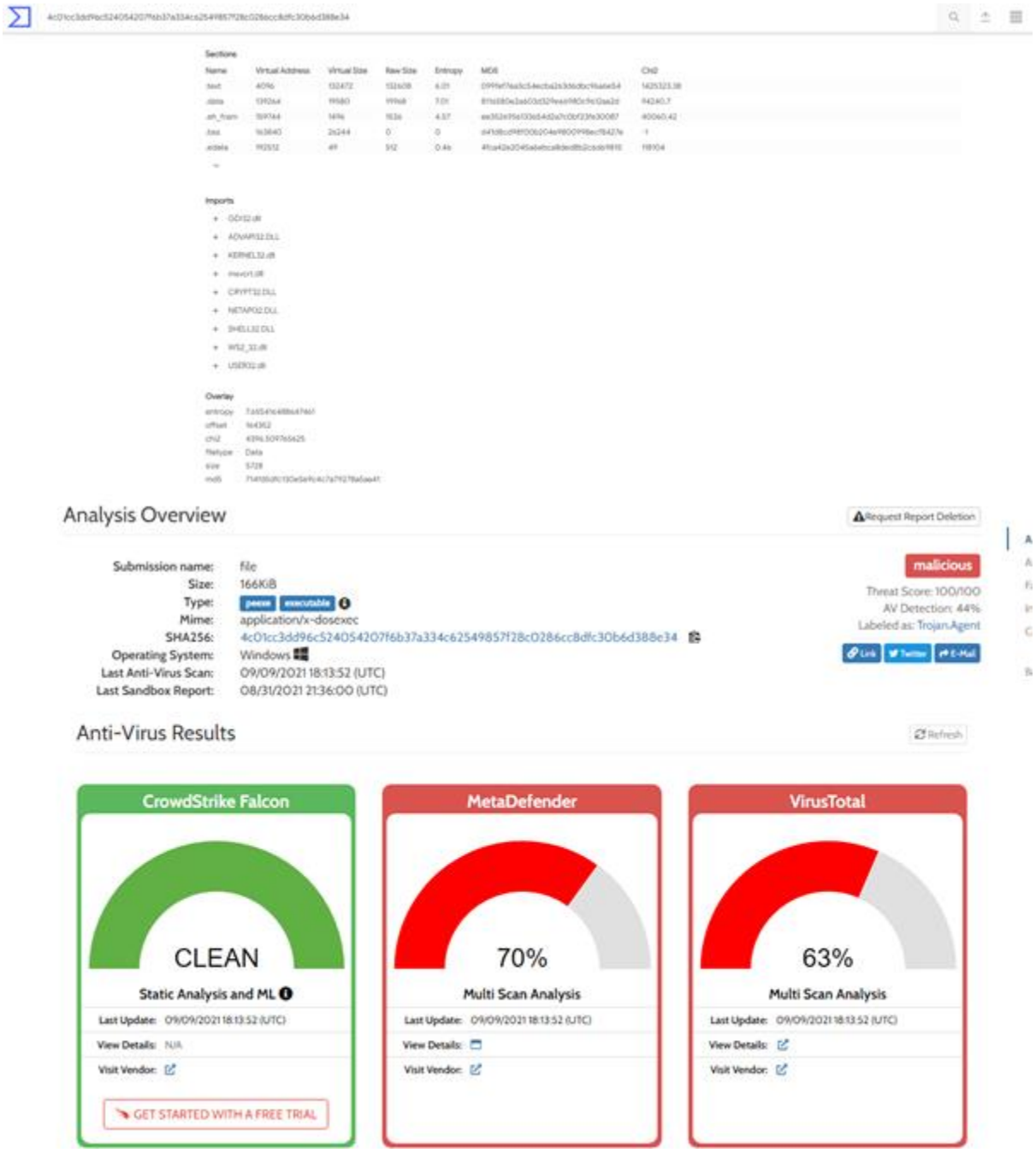
```
!This program cannot be run in DOS mode.
.text
P`.data
.eh_fram
@@.bss
.edata
@@.idata
.reloc
VS1
D(B
D(B
Fi<R
t$L
D$(D
l$$
|$
$N=A
$nt@
$=u@
D$0
D$41
l$0
l$0
D$8
T$8
D$<
D$0
D$0
D$<
D$0)
D$4
[^_]
D(B
9D$
```

File Edit Format View Help

```
/8r!
%F<,
~MB
9UH^
lLh
o1_X
zJrRJe
:Aj
;gR
"]\
http://%s%s
ssdaClass
%lu
%.2d/%.2d/%d %.2d:%.2d:%.2d
JpM
(>B
P>B
q>B
=?B
_?B
-@B
O@B
q@B
"AB
LAB
zAB
(BB
JBB
jBB
%CB
.CB
;CB
A%s
%c%.8x%s
```

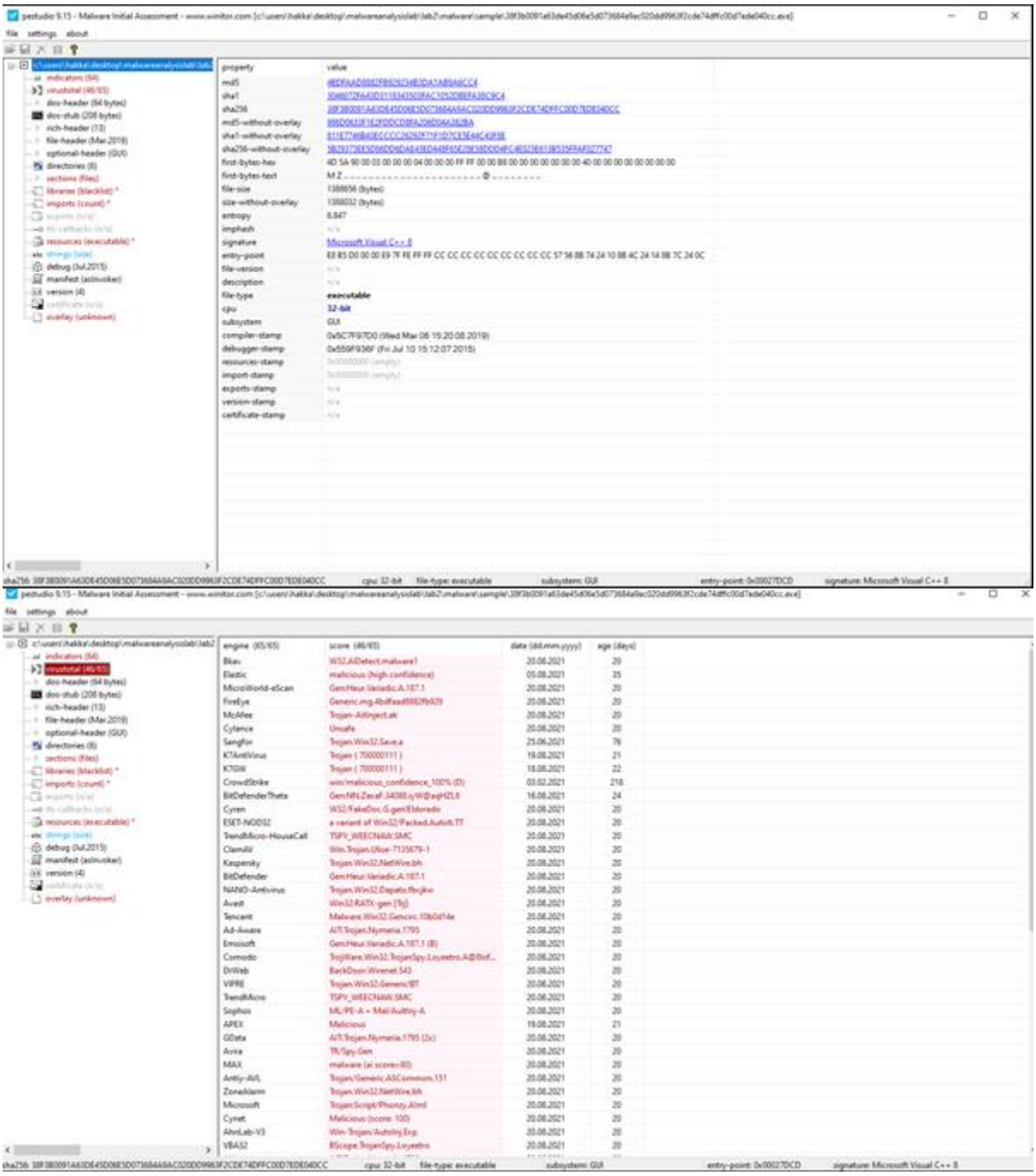

4c01cc3dd9ec524054207feb37a334ca2549857f28c026ccc8dfc30b6d388e34
43
43 security vendors flagged this file as malicious
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Basic Properties

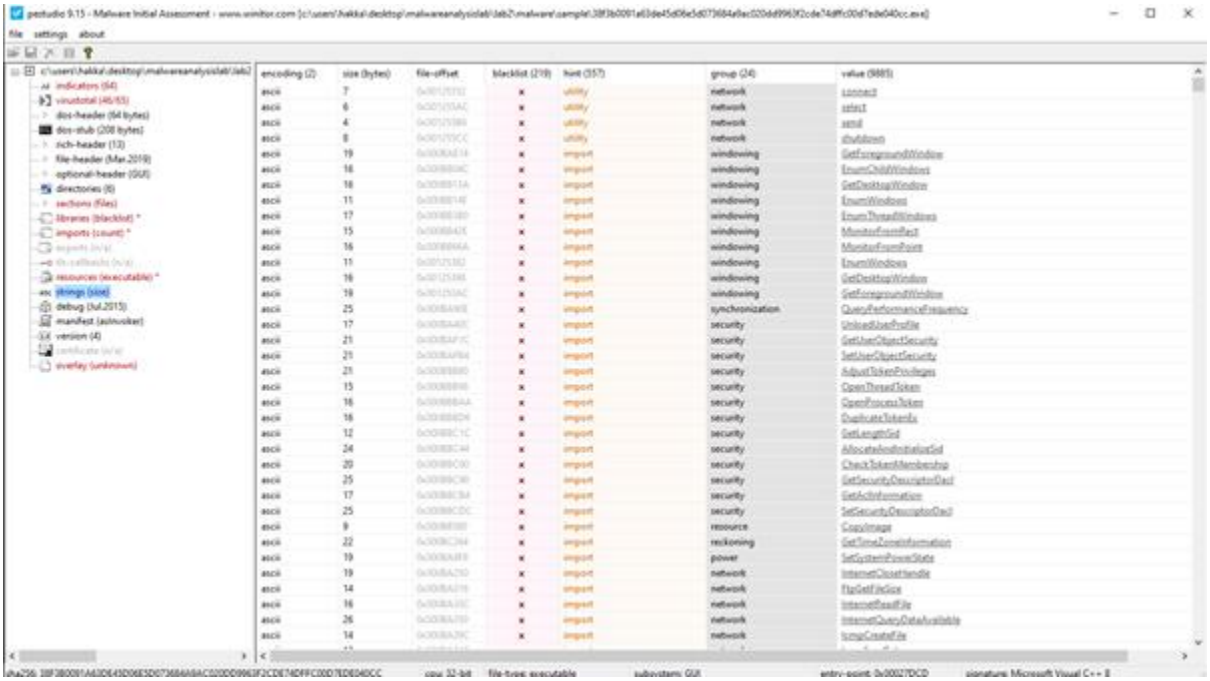

4c01cc3dd9ec524054207feb37a334ca2549857f28c026ccc8dfc30b6d388e34
Names
Host.exe
crack.exe
Signature Info
Signature Verification
A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.
File Version Information
Signers
google
X509 Certificates
google
Sectigo RSA Time Stamping CA
Sectigo RSA Time Stamping Signer #2
Portable Executable Info
Header
Target Machine
Intel 386 or later processors and compatible processors
Compilation Timestamp
2020-05-24 13:40:22
Entry Point
92d1
Contained Sections
7


Analysis Overview
Request Report Deletion
Submission name: file
Size: 166KiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: 4c01cc3dd96c52405420 7f6b37a334c62549857f28c0286cc8dfc30b6d388e34
Operating System: Windows
Last Anti-Virus Scan: 09/09/2021 18:13:52 (UTC)
Last Sandbox Report: 08/31/2021 21:36:00 (UTC)
malicious
Threat Score: 100/100
AV Detection: 44%
Labeled as: Trojan.Agent
Link
Twitter
E-Mail
Anti-Virus Results
Refresh
CrowdStrike Falcon
CLEAN
Static Analysis and ML
Last Update: 09/09/2021 18:13:52 (UTC)
View Details: N/A
Visit Vendor:
GET STARTED WITH A FREE TRIAL
MetaDefender
70%
Multi Scan Analysis
Last Update: 09/09/2021 18:13:52 (UTC)
View Details:
Visit Vendor:
VirusTotal
63%
Multi Scan Analysis
Last Update: 09/09/2021 18:13:52 (UTC)
View Details:
Visit Vendor:

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

File Name	38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe
MD5	4bdfaad8882fb929234b3da1ab9a6cc4
SHA1	3046072fa43d3118343503fac1052dbefa38c9c4
SHA256	38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc





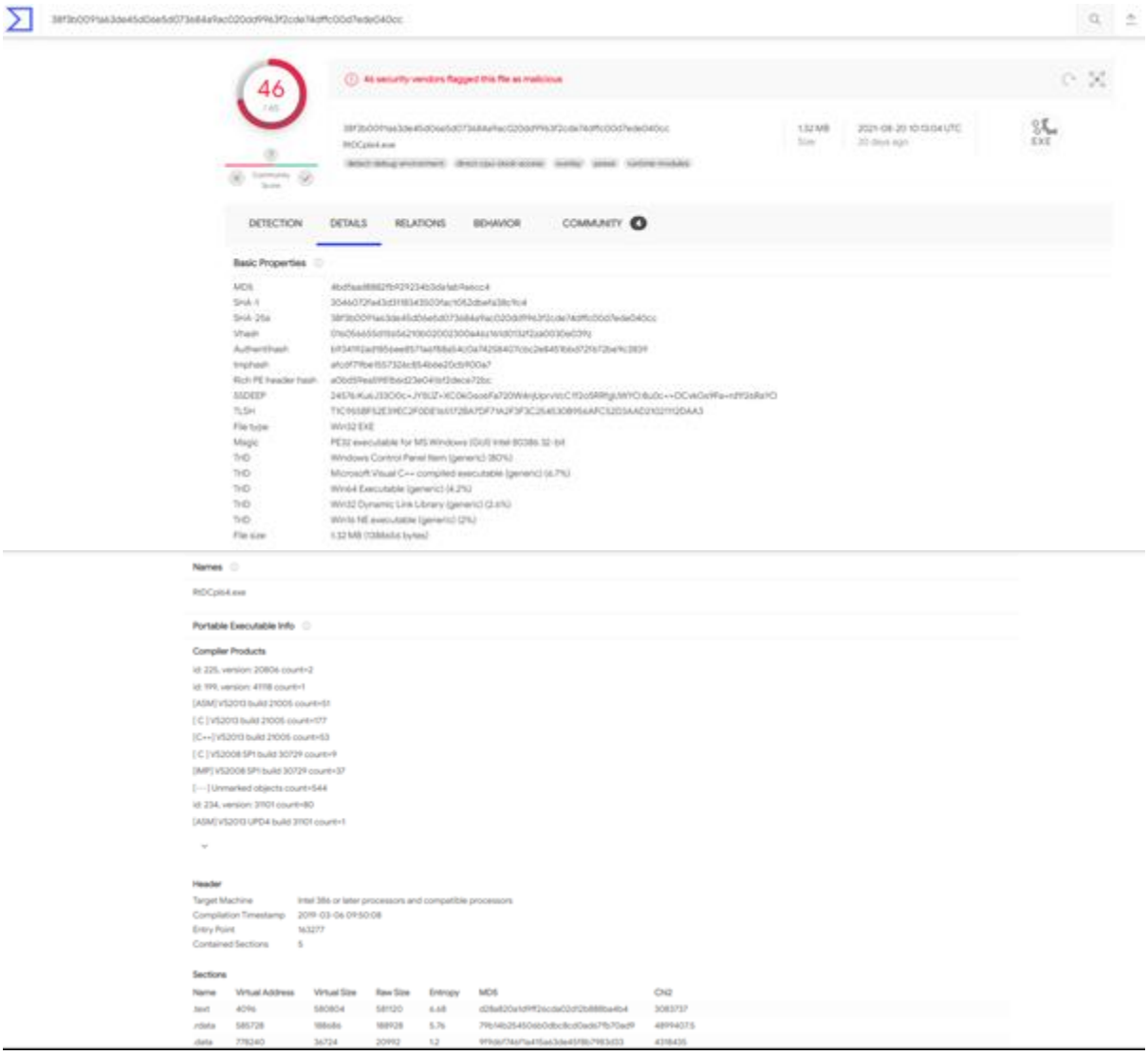
```
C:\Users\Hakka\Desktop\MalwareAnalysisLab\Tools+>strings.exe C:\Users\Hakka\Desktop\MalwareAnalysisLab\Lab2\Malware\Sample\38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe > file1.txt

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
```

File Edit Format View Help

```
!This program cannot be run in DOS m
4,"
r}T
Richr}
.text
`.rdata
@.data
.rsrc
@.reloc
DAL
SVW
F|U
u/;u
j V
9=tXL
dXL
pXL
=tXL
5xXL
uej
QPV
dXL
=lXL
hXL
lXL
=lXL
lXL
hXL
t+P
5dXL
%hXL
```

File Edit Format View Help

```
kernel32.dll
-DraUDrj\ajMPrX9qXTL\MZ65dl\PdR50Ci90WYd66W0\y
ProcessorNameString
DiiWYC5dDRSXR454Ci4kdM4S
advapi32.dll
PIdYwqWwdRFdlVd06I4s
_0ddM4S
PATH
WINDIR
%I64u
%I64u
%I64u
%s*
%d:%s%s;
%s%s\
%d:%I64u:%s%s;
rb+
%c%llu
%llu
Host.exe
CryptAcquireContextA
CryptCreateHash
CryptDestroyHash
CryptGetHashParam
CryptHashData
CryptReleaseContext
RegCloseKey
RegCreateKeyExA
RegDeleteKeyA
RegDeleteValueA
RegEnumKeyExA
```


46
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Basic Properties
Names
Portable Executable Info
Header
Sections

.data	778240	36724	20992	1.2	919d6f746f1a415a63de45f8b7983d33	4318435
.rsrc	815104	566296	566784	6.71	41dec4c706782fde5dc6056fa54d3087	2548158.5
.reloc	1384448	28956	29184	6.78	6fcae3cbbf6bfbabf5ec5bbe7cfe12c3	110480.01

Imports

- MPR.dll
- COMDLG32.dll
- IPHLPAPI.DLL
- KERNEL32.dll
- UxTheme.dll
- OLEAUT32.dll
- SHELL32.dll
- ole32.dll
- COMCTL32.dll
- VERSION.dll

Contained Resources By Type

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

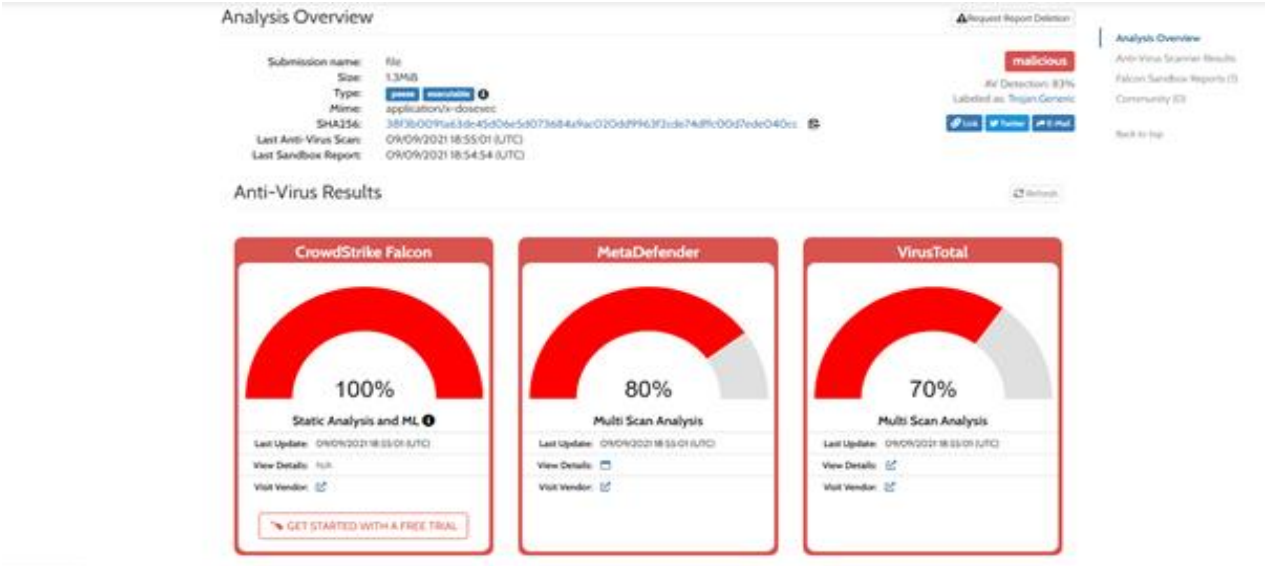
ENGLISH UK	13
NEUTRAL	5

Contained Resources

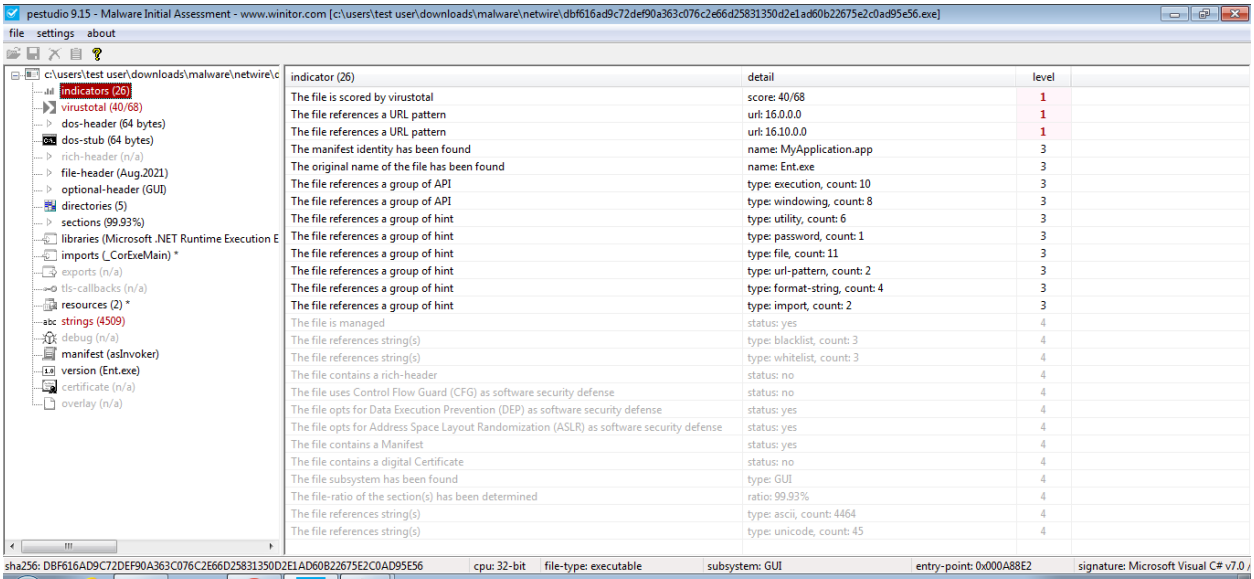
SHA-256	File Type	Type	Language	Entropy	Chi2
245fc49e4e955e1db3f75b826dcf27ad2eb32a6831caa4cbab501a3f14bcfaa9	Data	RT_ICON	ENGLISH UK	2.25	39565.58
903559c5b0ff6dc4123dac1f436a6bf563685c1570298475b71d2a15de38c36b1	Data	RT_ICON	ENGLISH UK	4.09	2511220
317bb0b285a5fea8986b4dd1abd9f7d524bd261c83298daacc0f972a8b7958d7	ASCII text	RT_DIALOG	NEUTRAL	4	1003939.94
1a3c94b10aafdf9707c9bf6258e2273c5cab8afbd953fe78c3f5e431f7c5185a77	ASCII text	RT_DIALOG	NEUTRAL	4	1003821.44
caf31ff9a78bb9f6b2e90f30d9451a78138e42dcb1b9584bba8ce865fd9795759f	ASCII text	RT_DIALOG	NEUTRAL	4	1003965.81

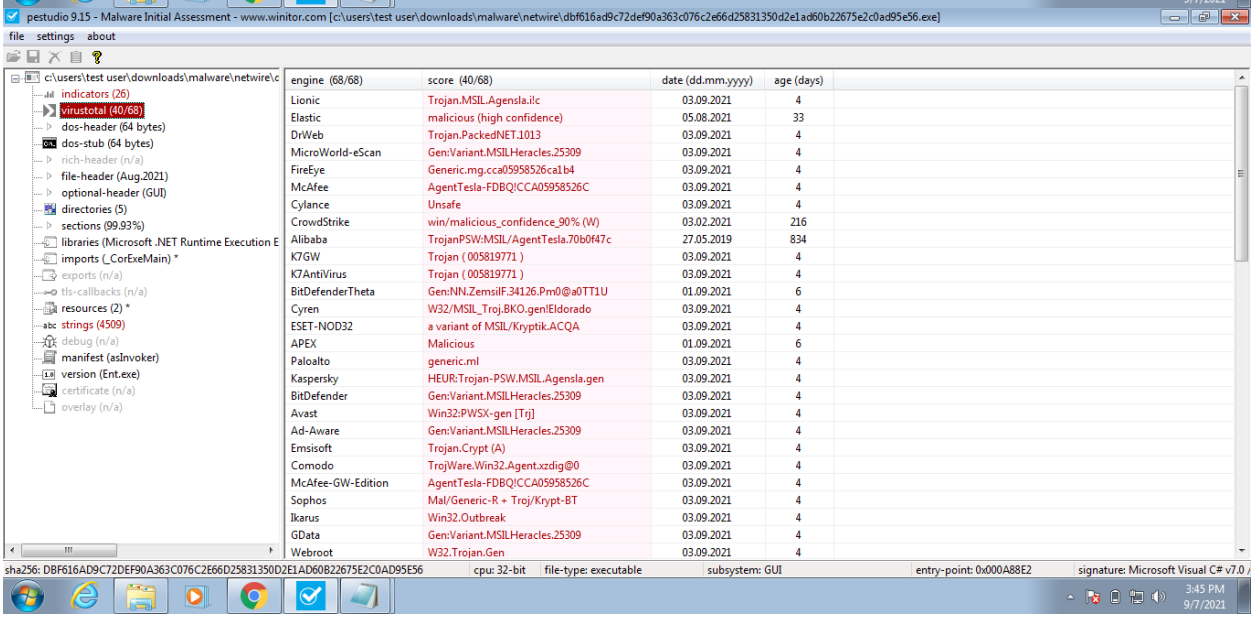
Overlay

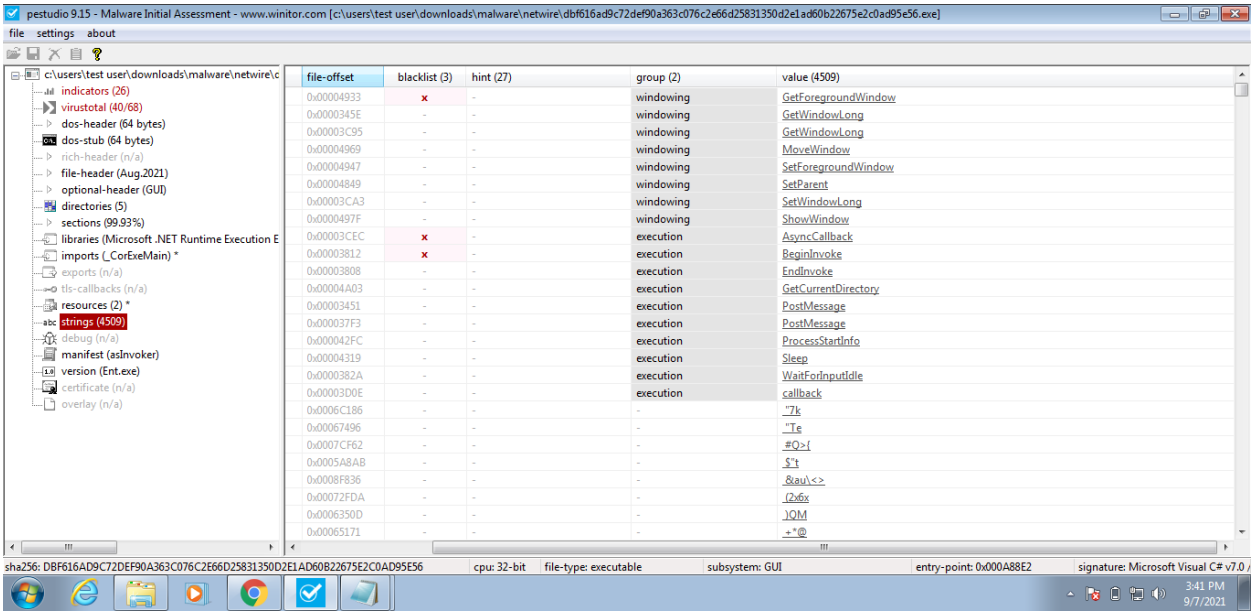
entropy	6.151355266571045
offset	1388032
chi2	7615.586425781125
filetype	Data
md5	a8489f4833085ba48cabef4625cb0d1c
size	624



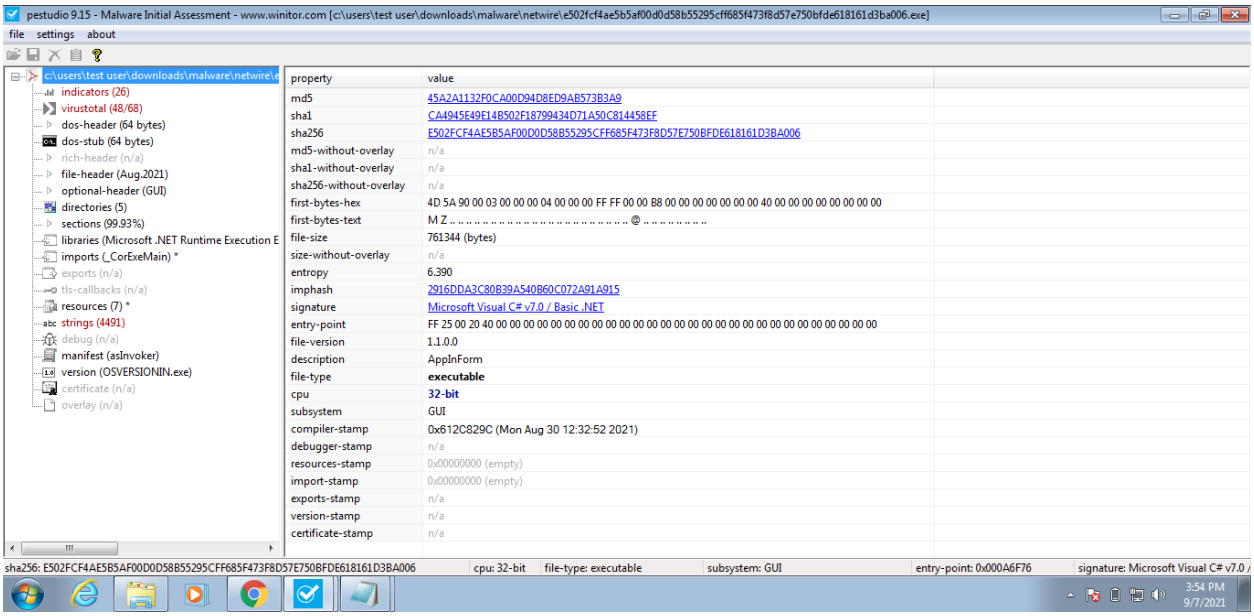
File Name	dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe
MD5	cca05958526ca1b406317bbc8137c6fe
SHA1	409794c9962f28780176be4a82b3fdd7d7b41427
SHA256	dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56

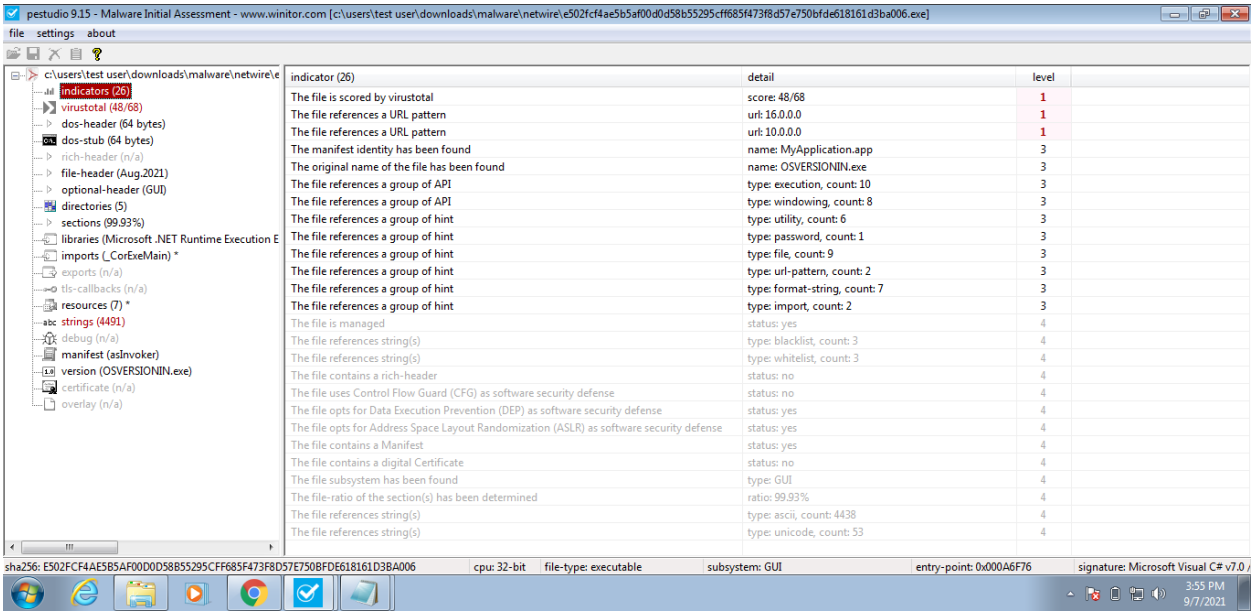


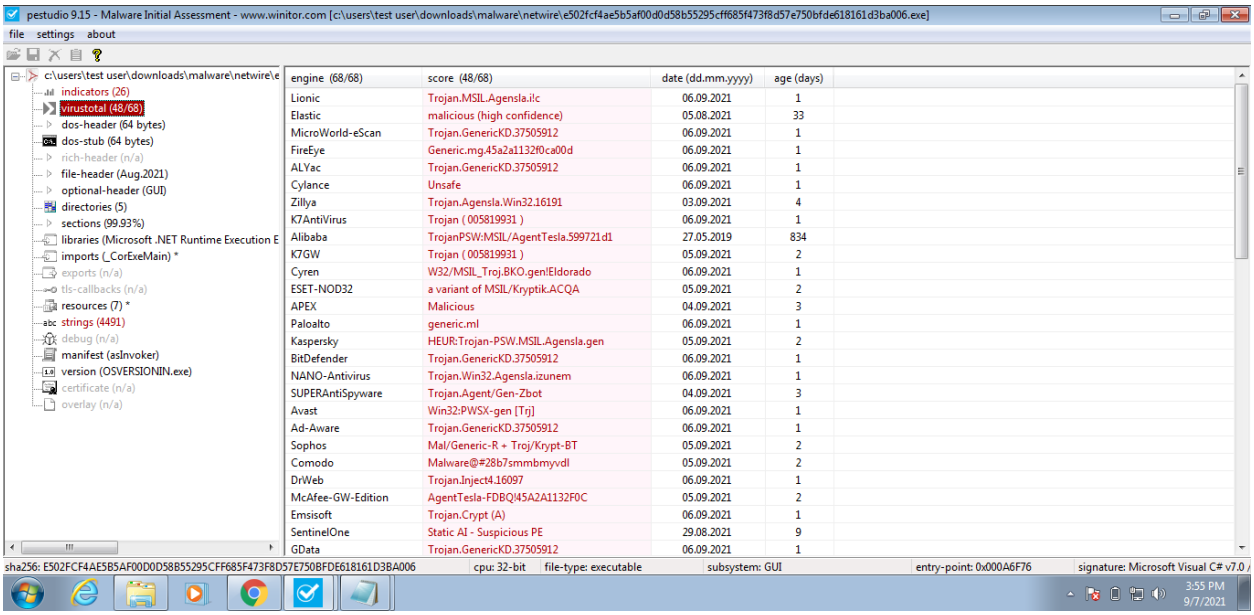




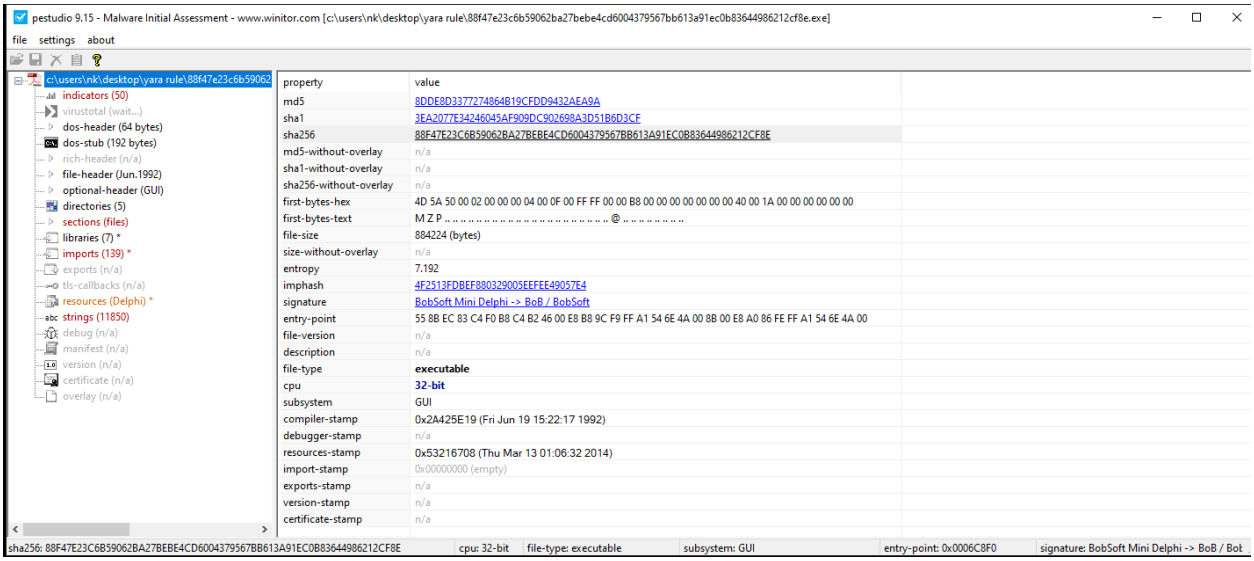
File Name	e502fcf4ae5b5af00d0d58b55295cff685f473f8d57e750bfde618161d3ba006exe
MD5	45a2a1132f0ca00d94d8ed9ab573b3a9
SHA1	ca4945e49e14b502f18799434d71a50c814458ef
SHA256	e502fcf4ae5b5af00d0d58b55295cff685f473f8d57e750bfde618161d3ba006

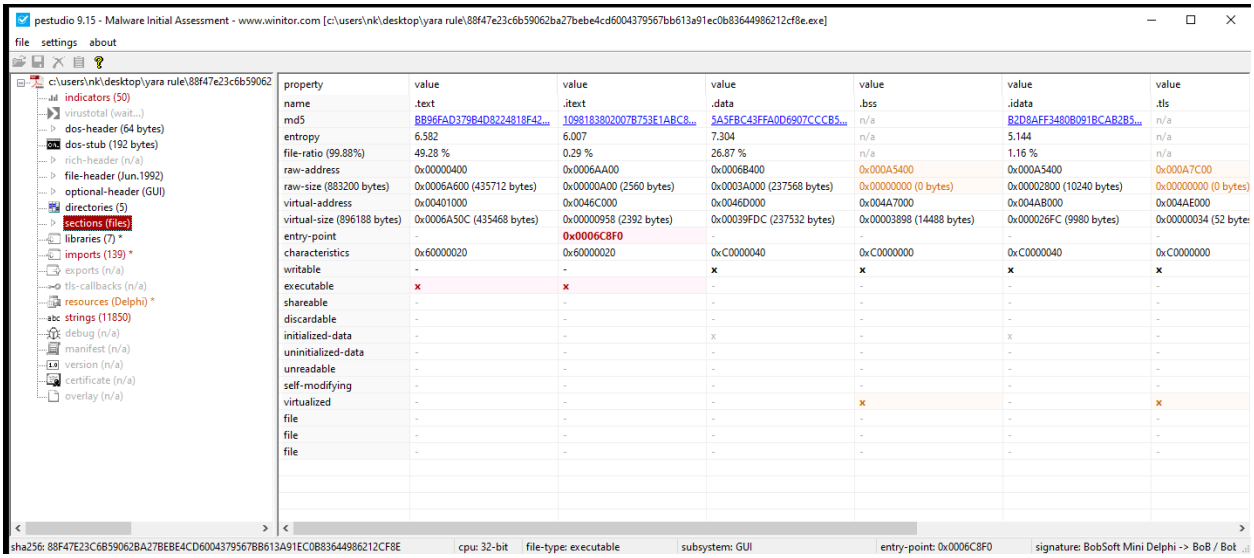


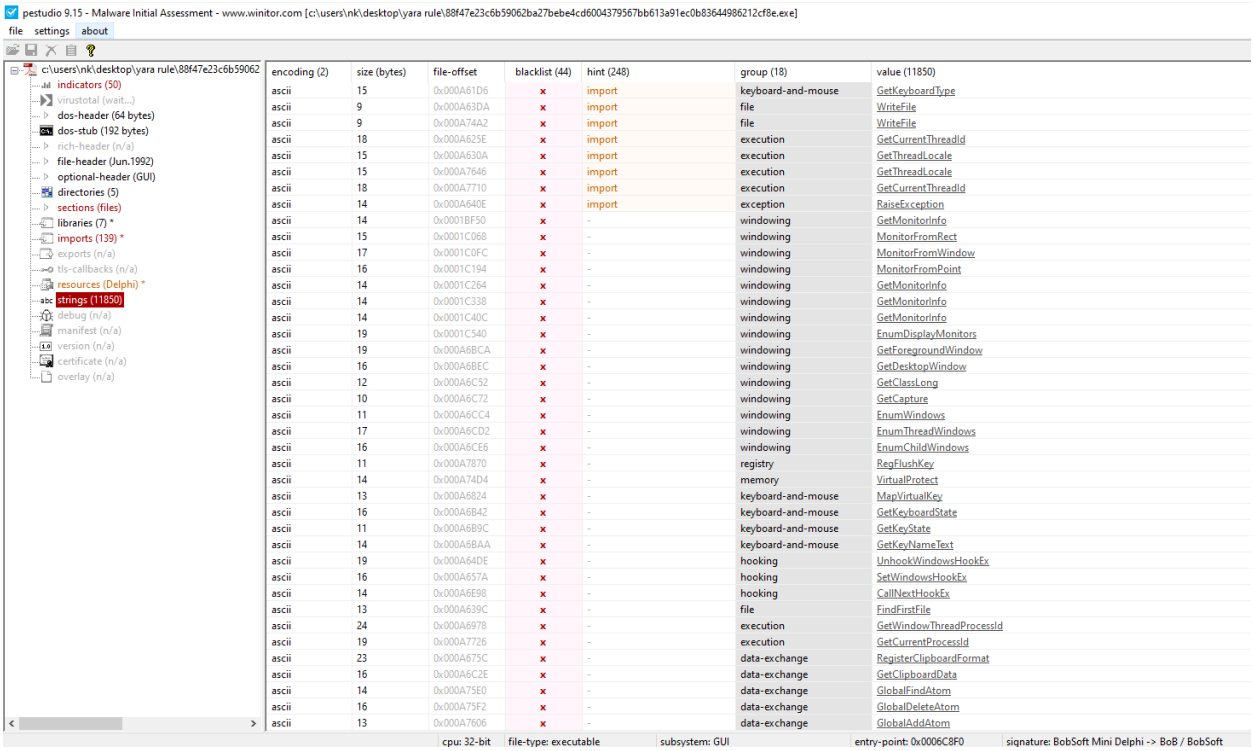




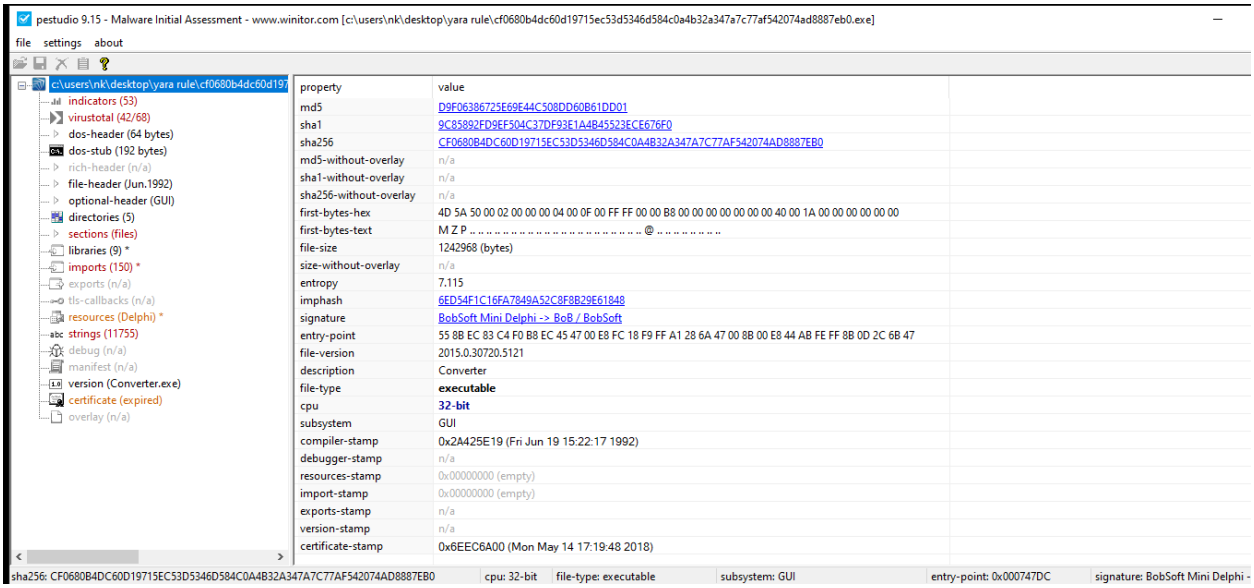
File Name	88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe
MD5	8DDE8D3377274864B19CFDD9432AEA9A
SHA1	3EA2077E34246045AF909DC902698A3D51B6D3CF
SHA256	88F47E23C6B59062BA27BEBE4CD6004379567BB613A91EC0B83644986212CF8E

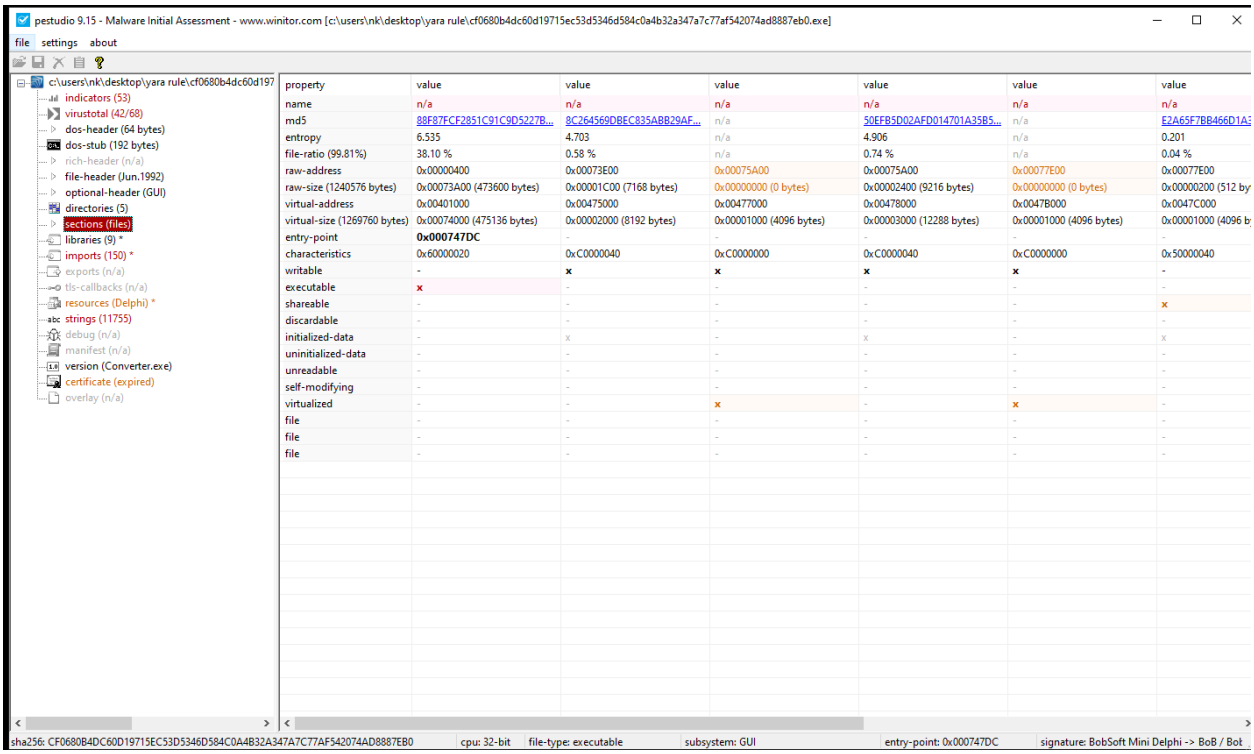

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe]
file settings about
c:\users\nk\desktop\yara rule\88f47e23c6b59062
indicators (50)
virustotal (wait...)
dos-header (64 bytes)
dos-stub (192 bytes)
rich-header (n/a)
file-header (Jun.1992)
optional-header (GUI)
directories (5)
sections (files)
libraries (7) *
imports (139) *
exports (n/a)
tls-callbacks (n/a)
resources (Delphi) *
strings (11850)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)
property value
md5 8DDE8D3377274864B19CFDD9432AEA9A
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 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00
first-bytes-text M Z P @
file-size 884224 (bytes)
size-without-overlay n/a
entropy 7.192
imphash 4F2513FDBEF880329005EEFEE49057E4
signature BobSoft Mini Delphi -> BoB / BobSoft
entry-point 55 8B EC 83 C4 F0 B8 C4 B2 46 00 E8 B8 9C F9 FF A1 54 6E 4A 00 8B 00 E8 A0 86 FE FF A1 54 6E 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

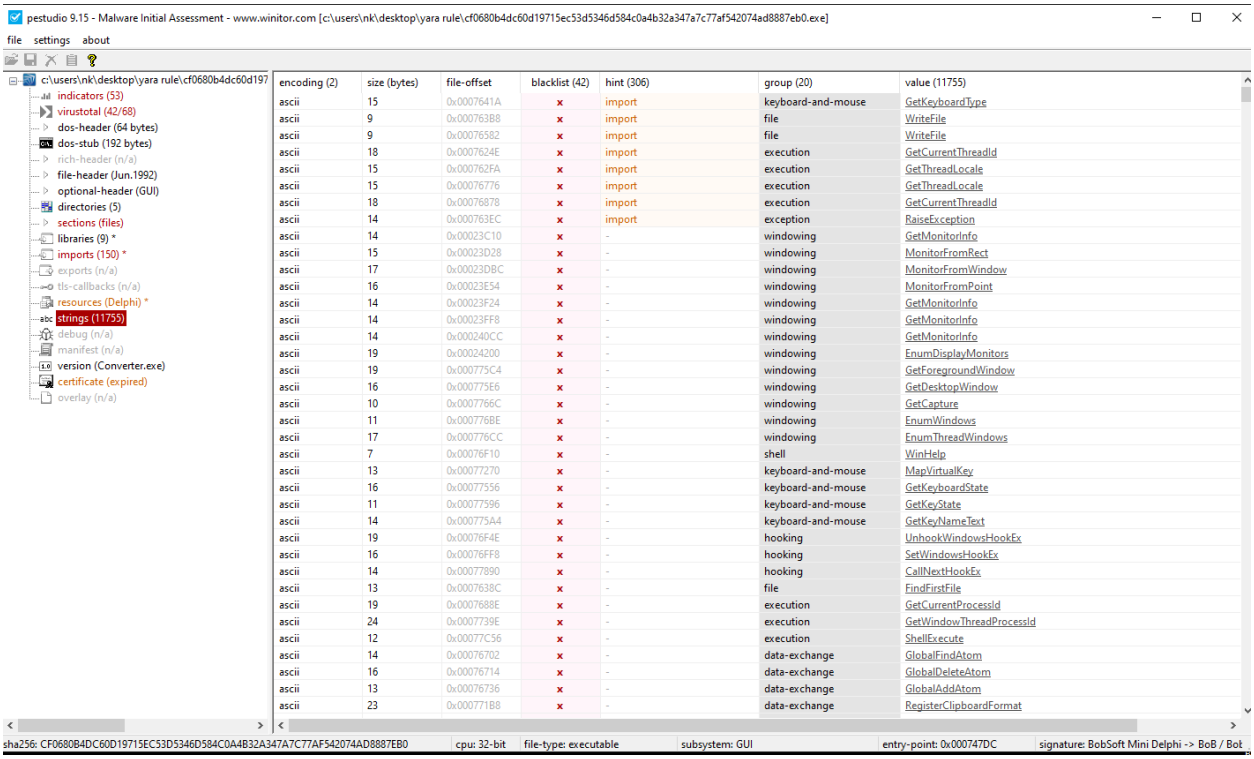

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule\88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe]
file settings about
c:\users\nk\desktop\yara rule\88f47e23c6b59062
indicators (50)
virustotal (wait...)
dos-header (64 bytes)
dos-stub (192 bytes)
rich-header (n/a)
file-header (Jun.1992)
optional-header (GUI)
directories (5)
sections (files)
libraries (7) *
imports (139) *
exports (n/a)
tls-callbacks (n/a)
resources (Delphi) *
strings (11850)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)
property value value value value value value
name .text .itext .data .bss .idata .tls
md5 BB96FAD379B4D8224818F42... 1098183802007B753E1ABC8... 5A5FBC43FFA0D6907CCCB5... n/a B2D8AFF3480B091BCAB2B5... 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) 0x00000A00 (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) 0x00003898 (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



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

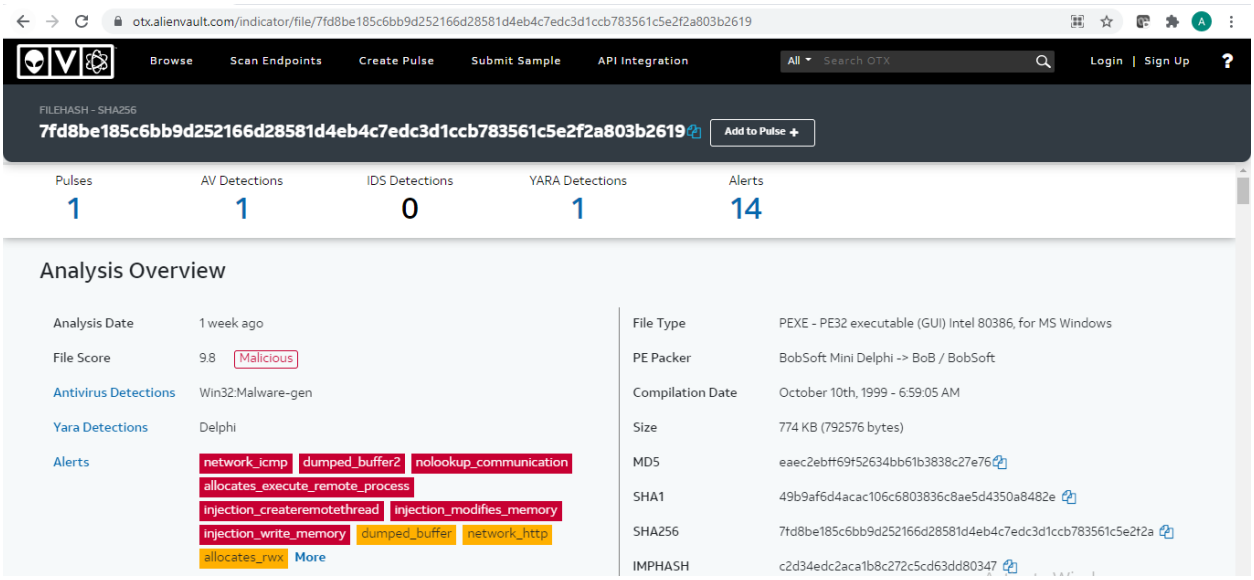

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule\cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe]
file settings about
c:\users\nk\desktop\yara rule\cf0680b4dc60d197
indicators (53)
virustotal (42/68)
dos-header (64 bytes)
dos-stub (192 bytes)
rich-header (n/a)
file-header (Jun.1992)
optional-header (GUI)
directories (5)
sections (files)
libraries (9) *
imports (150) *
exports (n/a)
tls-callbacks (n/a)
resources (Delphi) *
strings (11755)
debug (n/a)
manifest (n/a)
version (Converter.exe)
certificate (expired)
overlay (n/a)
property value
md5 D9F06386725E69E44C508DD60B61DD01
sha1 9C85892FD9EF504C37DF93E1A4B45523ECE676F0
sha256 CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0
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 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00
first-bytes-text M Z P ... @ ...
file-size 1242968 (bytes)
size-without-overlay n/a
entropy 7.115
imphash 6ED54F1C16FA7849A52C8F8B29E61848
signature BobSoft Mini Delphi -> BoB / BobSoft
entry-point 55 8B EC 83 C4 F0 B8 EC 45 47 00 E8 FC 18 F9 FF A1 28 6A 47 00 8B 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 0x00000000 (empty)
import-stamp 0x00000000 (empty)
exports-stamp n/a
version-stamp n/a
certificate-stamp 0x6EEC6A00 (Mon May 14 17:19:48 2018)
sha256: CF0680B4DC60D19715EC53D5346D584C0A4B32A347A7C77AF542074AD8887EB0
cpu: 32-bit
file-type: executable
subsystem: GUI
entry-point: 0x000747DC
signature: BobSoft Mini Delphi -

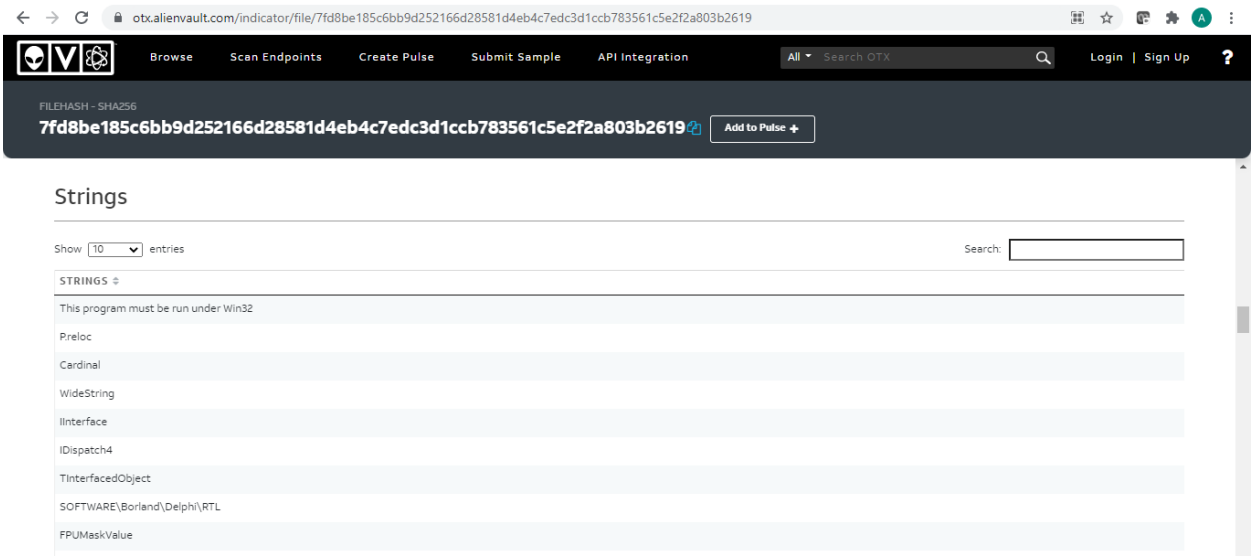

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\nk\desktop\yara rule\cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe]
file settings about
c:\users\nk\desktop\yara rule\cf0680b4dc60d197
indicators (53)
virustotal (42/68)
dos-header (64 bytes)
dos-stub (192 bytes)
rich-header (n/a)
file-header (Jun.1992)
optional-header (GUI)
directories (5)
sections (files)
libraries (9) *
imports (150) *
exports (n/a)
tls-callbacks (n/a)
resources (Delphi) *
strings (11755)
debug (n/a)
manifest (n/a)
version (Converter.exe)
certificate (expired)
overlay (n/a)
property value value value value value value
name n/a n/a n/a n/a n/a n/a
md5 88F87FCF2851C91C9D5227B... 8C264569DBEC835ABB29AF... n/a 50EFB5D02AFD014701A35B5... n/a E2A65F7BB466D1A
entropy 6.535 4.703 n/a 4.906 n/a 0.201
file-ratio (99.81%) 38.10 % 0.58 % n/a 0.74 % n/a 0.04 %
raw-address 0x00000400 0x00073E00 0x00075A00 0x00075A00 0x00077E00 0x00077E00
raw-size (1240576 bytes) 0x00073A00 (473600 bytes) 0x00001C00 (7168 bytes) 0x00000000 (0 bytes) 0x00002400 (9216 bytes) 0x00000000 (0 bytes) 0x00000200 (512 by
virtual-address 0x00401000 0x00475000 0x00477000 0x00478000 0x0047B000 0x0047C000
virtual-size (1269760 bytes) 0x00074000 (475136 bytes) 0x00002000 (8192 bytes) 0x00001000 (4096 bytes) 0x00003000 (12288 bytes) 0x00001000 (4096 bytes) 0x00001000 (4096 b
entry-point 0x000747DC
characteristics 0x60000020 0xC0000040 0xC0000000 0xC0000040 0xC0000000 0x50000040
writable x x x x
executable x
shareable x
discardable
initialized-data x x x
uninitialized-data
unreadable
self-modifying
virtualized x x
file
file
file
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

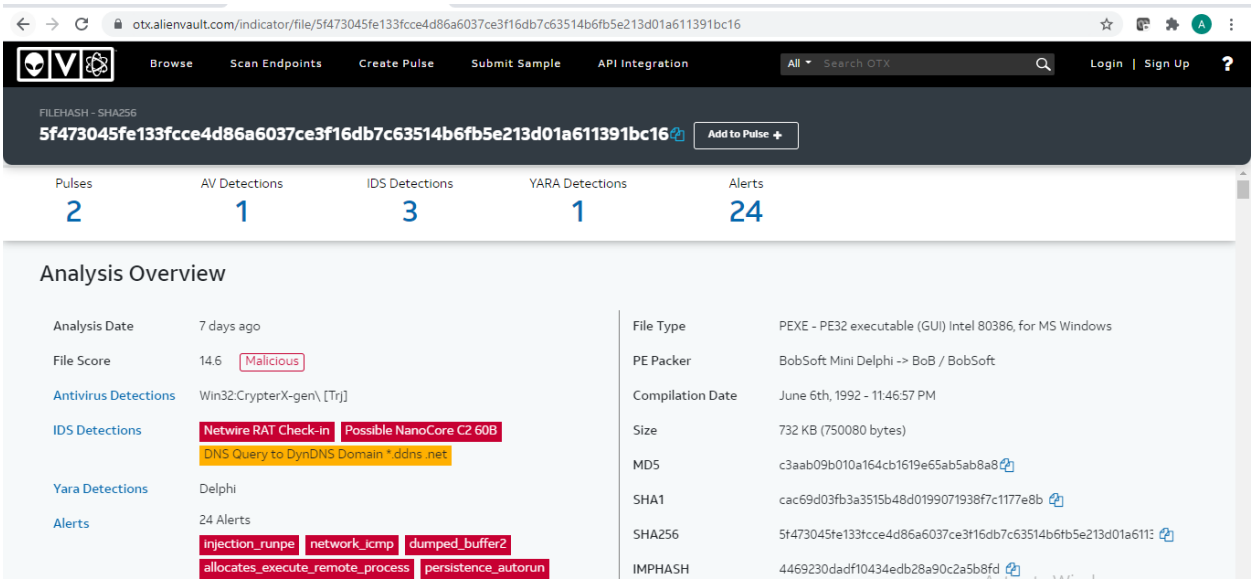
Alien Vault Static Analysis Report

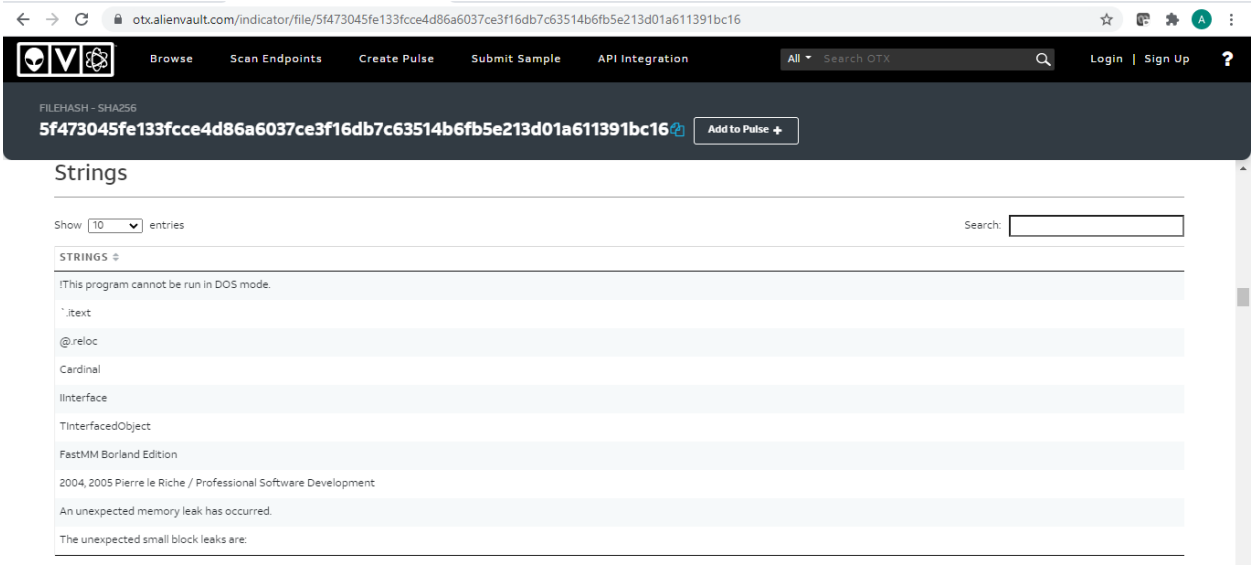




File Name	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16.exe
MD5	c3aab09b010a164cb1619e65ab5ab8a8
SHA1	cac69d03fb3a3515b48d0199071938f7c1177e8b
SHA256	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16

Alien Vault Static Analysis Report





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

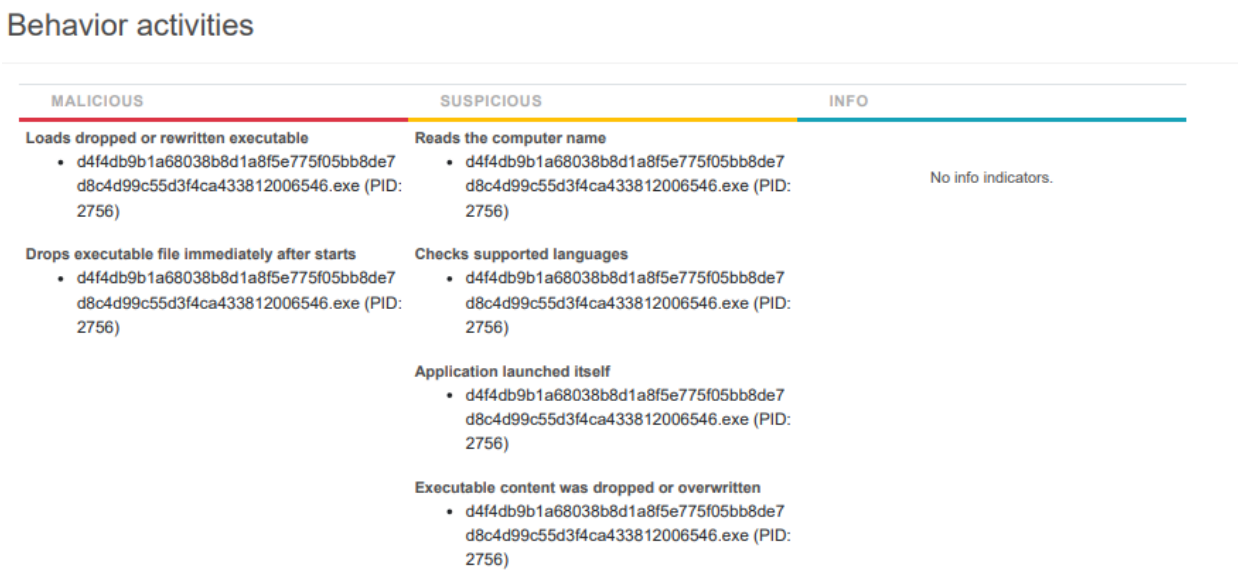


Figure : Behavior Activities for NetWire Rat d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546

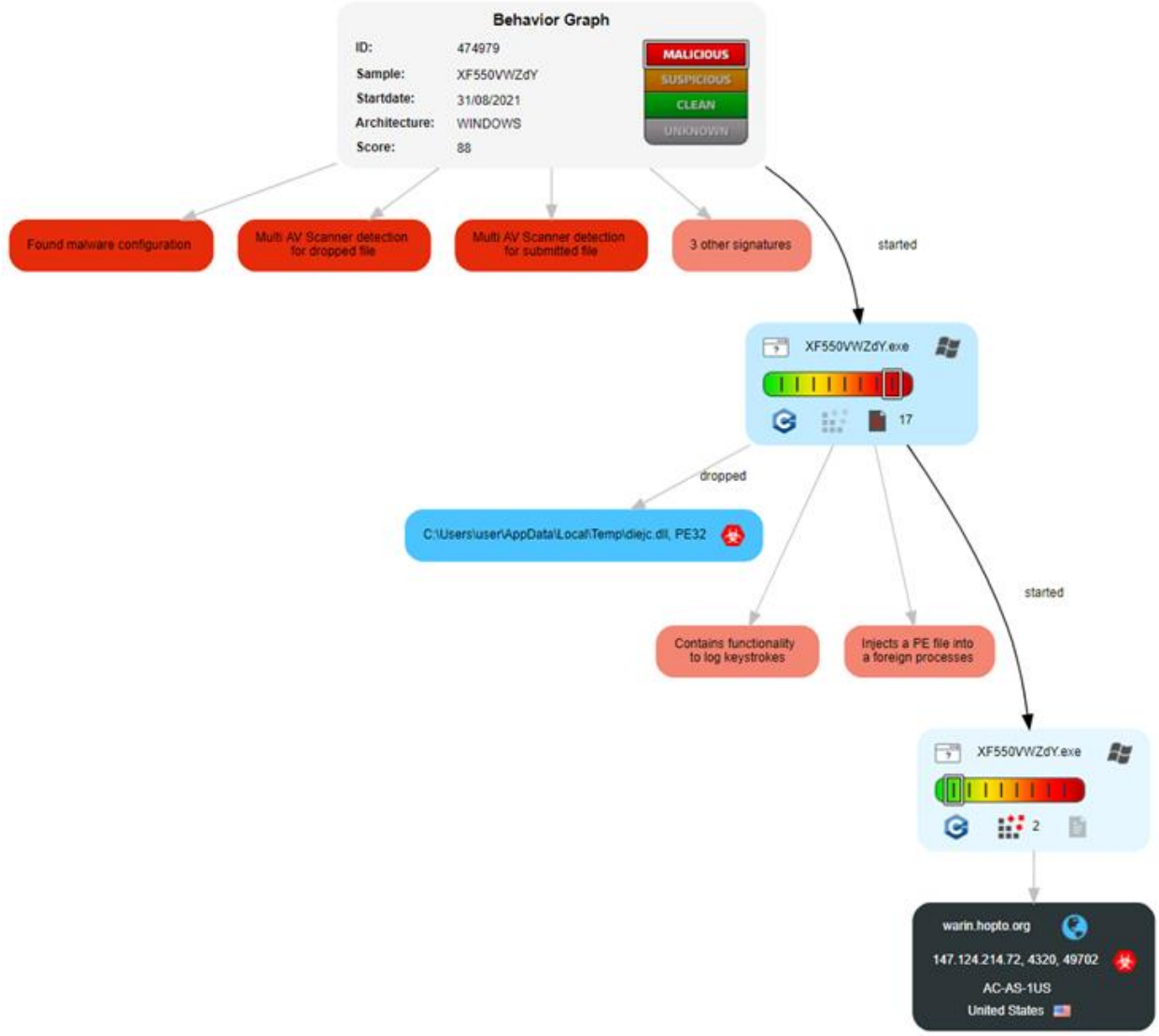


Figure : Behavior Graph for NetWire Rat
d4f4db9b1a68038b8d1a8f5e775f05bb8de7d8c4d99c55d3f4ca433812006546

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

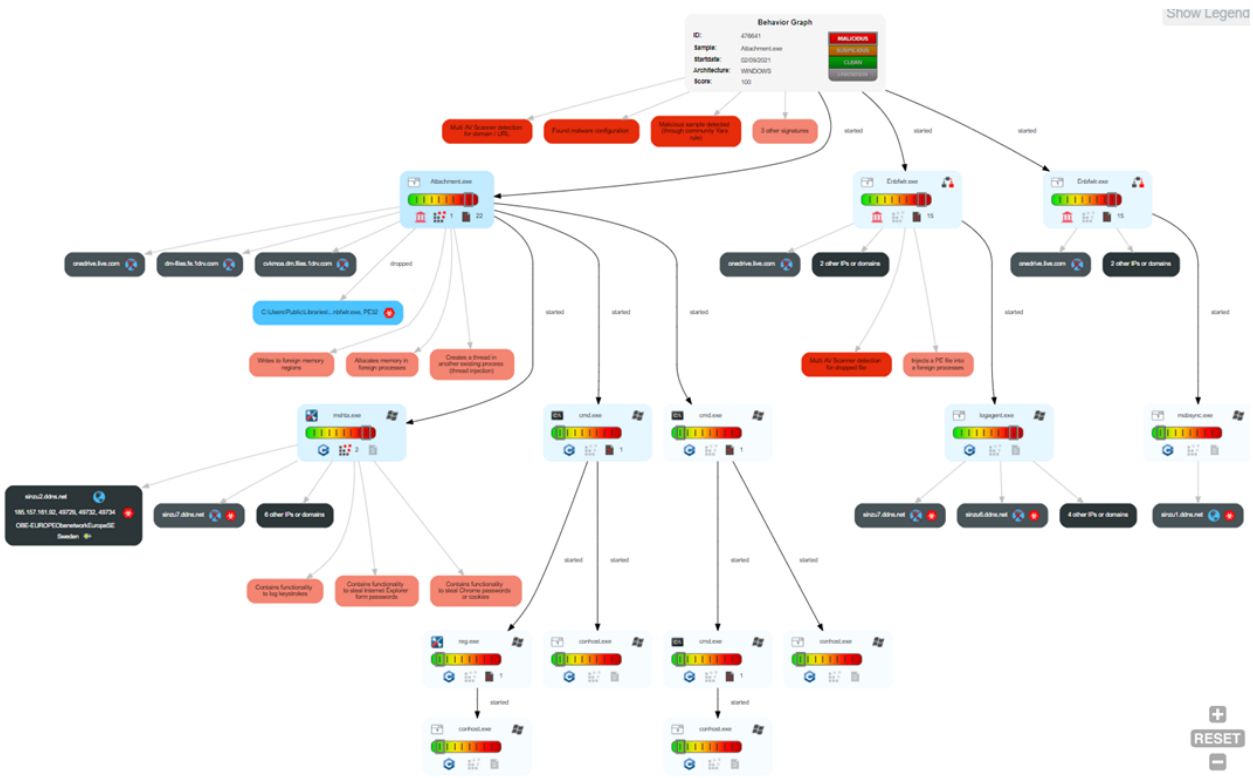


Figure : Behavior Graph for NetWire RAT
8a5035fd03311d20137b4111bee190142fa9c653ed60e57be2802665fe8bdb24

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

Automated Malware Analysis Report for XF550VWZdY - Generated by Joe Sandbox

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...

ANY RUN
Interactive malware hunting service

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	EAEC2EBFF69F52634BB61B3838C27E76
SHA1	49B9AF6D4ACAC106C6803836C8AE5D4350A8482E
SHA256	7FD8BE185C6BB9D252166D28581D4EB4C7EDC3D1CCB783561C5E2F2A803B2619
SSDEEP	12288:ECMJCATKJTH4B6XG3N7YBODV9CPDGMKUE03S0XJVWRSQAE6MZF5:EBI94ZYSFCFGM6NZA2

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	**Checks supported languages** • 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 3724) • 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332) **Application launched itself** • 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 3724) **Reads the computer name** • 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332)	**Reads settings of System Certificates** • 7fd8be185c6bb9d252166d28581d4eb4c7edc3d1ccb783561c5e2f2a803b2619.exe (PID: 1332) **Checks Windows Trust Settings** • 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...

ANY RUN
Interactive malware hunting service

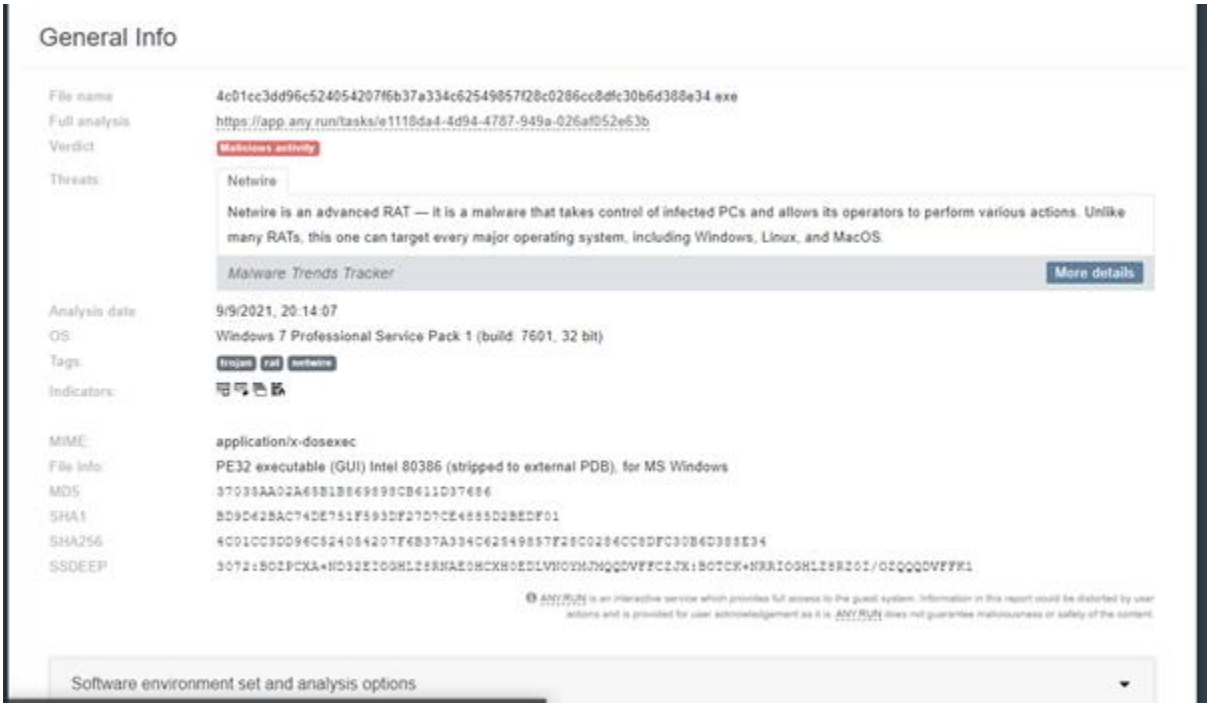
General Info

File name	5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16
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	5F473045FE133FCCE4D86A6037CE3F16DB7C63514B6FB5E213D01A611391BC16
SSDEEP	12288:WYL+XIUEKT8A+CSSPYGAP6VXD85PZM4ECXGI+8IXY:JS4TKT7GSHAMDQPZMLCQI3Q

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	**Checks supported languages** • 5f473045fe133fcce4d86a6037ce3f16db7c63514b6fb5e213d01a611391bc16.scr (PID: 3676)	No info indicators.

Dynamic analysis of 4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34 using ANYRUN and Joe sandbox



General Info

File name:	4c01cc3dd96c5240542071f6b37a334c62549857f28c0286cc8dfc30b6d388e34.exe
Full analysis:	https://app.any.run/tasks/e1118da4-4d94-4787-949a-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, netwire
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5:	37033AA02A65B1B869898CB611D37686
SHA1:	BD9D62BAC74DE751F593DF27D7CE4855D2BEDF01
SHA256:	4C01CC3DD96C5240542071F6B37A334C62549857F28C0286CC8DFC30B6D388E34
SSDEEP:	3072:BOIPCXA+ND32EIOGHLZ8RNAE0HCXH0EDLVHOYMJHQQDVFFCZJK:BOTCK+NRRIOGHLZ8RZOI/OZQQQDVFFK1

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.

Software environment set and analysis options

Summary

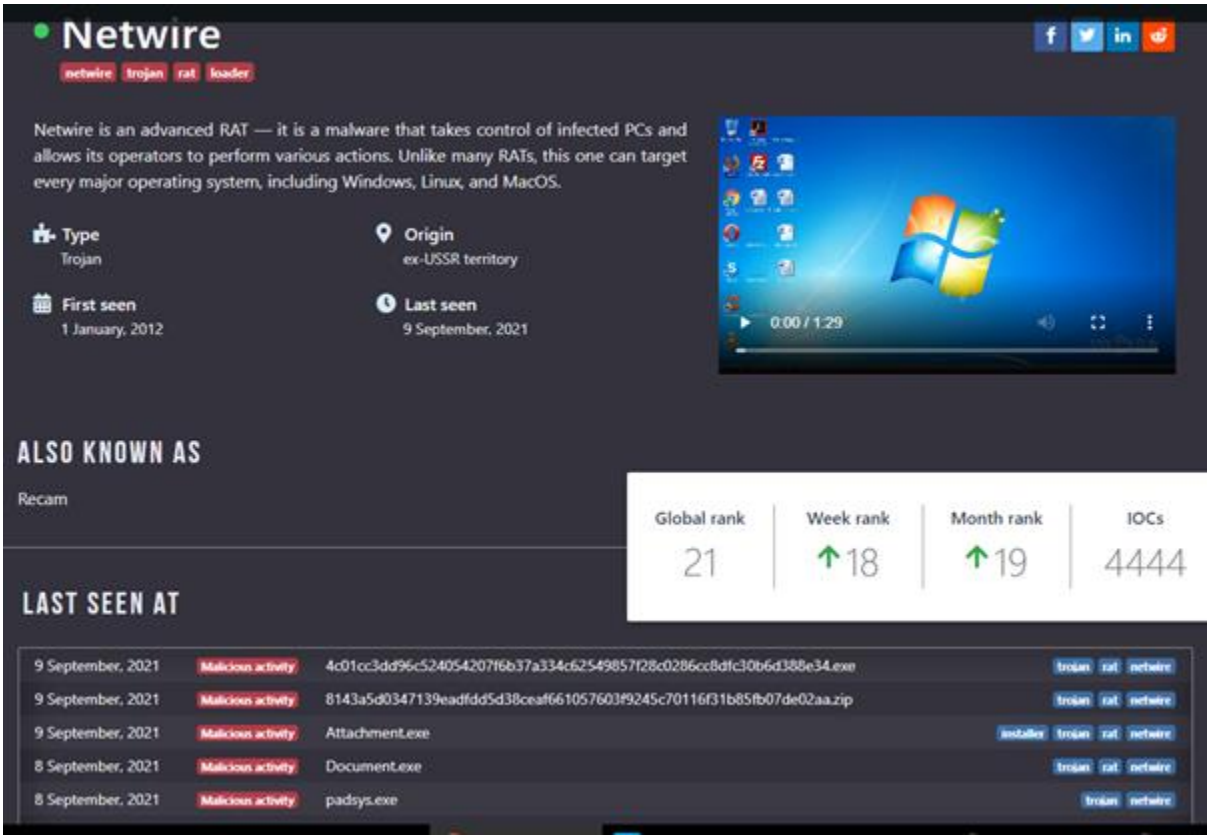
Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	24-May-2020 13:40:22

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 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:	0x00000080

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
0:00 / 1:29
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 8143a5d0347139eadfdd5d38ceaf661057603f9245c70116f31b85fb07de02aa.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 padsys.exe trojan netwire


Behavior activities
MALICIOUS
Drops executable file immediately after starts
4c01cc3dd96c524054207f6b37a334c62549857f28c 0286cc8dfc30b6d388e34.exe (PID: 3652)
NETWIRE was detected
Host.exe (PID: 3972)
Changes the autorun value in the registry
Host.exe (PID: 3972)
Connects to CnC server
Host.exe (PID: 3972)
SUSPICIOUS
Starts itself from another location
4c01cc3dd96c524054207f6b37a334c62549857f28c 0286cc8dfc30b6d388e34.exe (PID: 3652)
Reads the computer name
4c01cc3dd96c524054207f6b37a334c62549857f28c 0286cc8dfc30b6d388e34.exe (PID: 3652)
Host.exe (PID: 3972)
Creates files in the user directory
4c01cc3dd96c524054207f6b37a334c62549857f28c 0286cc8dfc30b6d388e34.exe (PID: 3652)
Checks supported languages
4c01cc3dd96c524054207f6b37a334c62549857f28c 0286cc8dfc30b6d388e34.exe (PID: 3652)
Host.exe (PID: 3972)
Executable content was dropped or overwritten
4c01cc3dd96c524054207f6b37a334c62549857f28c 0286cc8dfc30b6d388e34.exe (PID: 3652)
INFO
No info indicators.

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

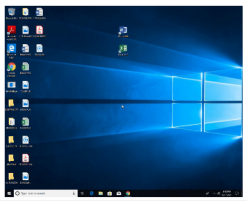
PID	Process	Class	Message
—	—	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.hopto .org

Overview

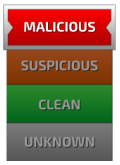
General Information

Sample Name:	5sNHlrfRwn.exe
Analysis ID:	475363
MD5:	37035aa02a65b1b869898c...
SHA1:	bd9d62bac74de751f593df2...
SHA256:	4c01cc3dd96c524054207f...
Tags:	exe NetWire RAT
Infos:	

Most interesting Screenshot:



Detection



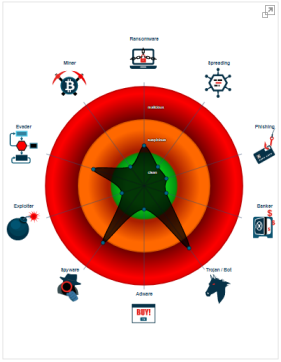
NetWire

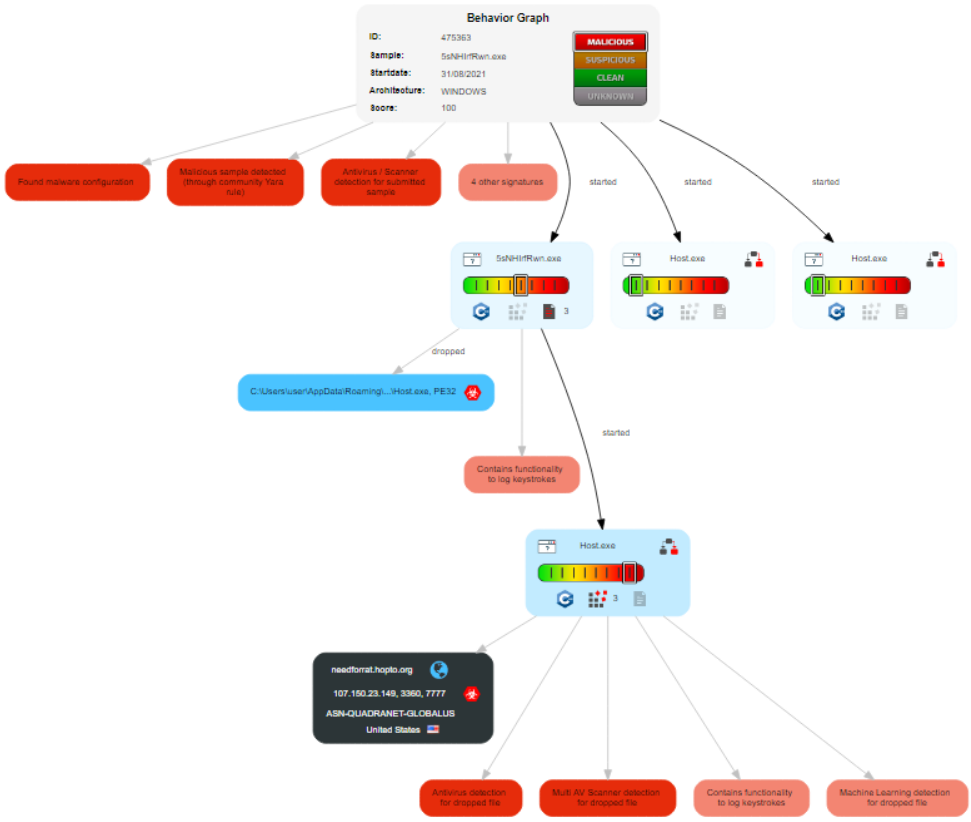
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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

Classification





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 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc using ANYRUN and Joe sandbox

General Info

File name	38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.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:KU6J33O0C+JY5UZ+XC0KGSO6FA720W4NJUPRVVCC1F2O5RRFGUWYO: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

Uses Task Scheduler to run other applications
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)
- RtDCpl64.exe (PID: 3332)

Drops executable file immediately after starts
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)
- Blasthost.exe (PID: 3620)

Application was injected by another process
- Explorer.EXE (PID: 1288)

Application was dropped or rewritten from another process
- Blasthost.exe (PID: 3620)
- Host.exe (PID: 1828)
- Blasthost.exe (PID: 3576)

Runs injected code in another process
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 1920)
- RtDCpl64.exe (PID: 2068)

Loads the Task Scheduler COM API
- schtasks.exe (PID: 2680)
- schtasks.exe (PID: 1860)

SUSPICIOUS

Executable content was dropped or overwritten
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)
- Blasthost.exe (PID: 3620)

Starts itself from another location
- Blasthost.exe (PID: 3620)

Checks supported languages
- Blasthost.exe (PID: 3620)
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)
- Host.exe (PID: 1828)
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 1920)
- RtDCpl64.exe (PID: 3332)
- Blasthost.exe (PID: 3576)
- RtDCpl64.exe (PID: 2068)

Creates files in the user directory
- Blasthost.exe (PID: 3620)
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)

Reads mouse settings
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)
- RtDCpl64.exe (PID: 3332)

Reads the computer name
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 3636)
- Host.exe (PID: 1828)
- 38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc.exe (PID: 1920)
- RtDCpl64.exe (PID: 3332)
- Blasthost.exe (PID: 3576)

INFO

Reads the computer name
- schtasks.exe (PID: 2680)
- schtasks.exe (PID: 1860)

Checks supported languages
- schtasks.exe (PID: 2680)
- schtasks.exe (PID: 1860)

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

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:	0x00000110

PE Headers

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
Wealthy2019.com.strangled.net	No response	unknown
wealth.warzonedns.com	No response	malicious
wealthyme.ddns.net	No response	malicious

Overview

General Information

Sample Name:	cURJKOIXLM (renamed file extension from none to exe)
Analysis ID:	473860
MD5:	4bdfaad8882fb929234b3d...
SHA1:	3046072fa43d3118343503f...
SHA256:	38f3b0091a63de45d06e5d...
Tags:	exe NetWire
Infos:	

Most interesting Screenshot:

Detection

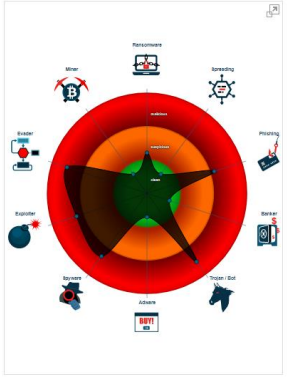
AveMaria Netwire UACMe

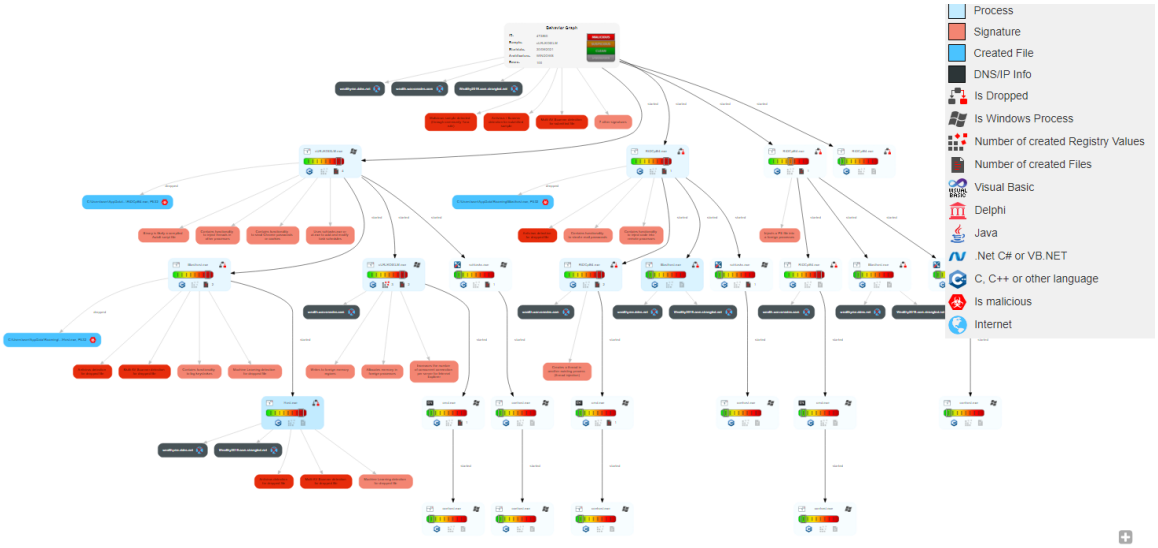
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 inj...
- 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,
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:	• 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:	• Successful, ratio: 48% (good quality ratio 38.8%) • Quality average: 73.3% • Quality standard deviation: 39.1%
HCA Information:	• Successful, ratio: 54% • Number of executed functions: 90

General

Entrypoint:	0x427dcd
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:	afcdf79be1557326c854b6e20cb900a7

Dynamic analysis of cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0 using ANYRUN and Joe sandbox

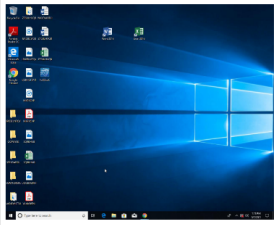
Windows Analysis Report HzXQbzCHJQ

Overview

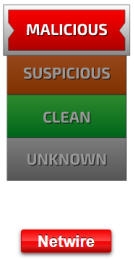
General Information

Sample Name:	HzXQbzCHJQ (renamed file extension from none to exe)
Analysis ID:	478966
MD5:	d9f06386725e69e44c50...
SHA1:	9c85892fd9ef504c37df9...
SHA256:	cf0680b4dc60d19715ec...
Tags:	exe NetWire
Infos:	

Most interesting Screenshot:



Detection

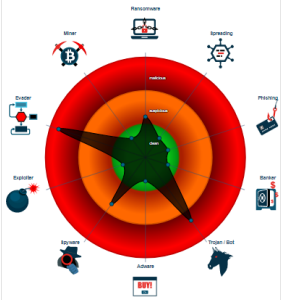


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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

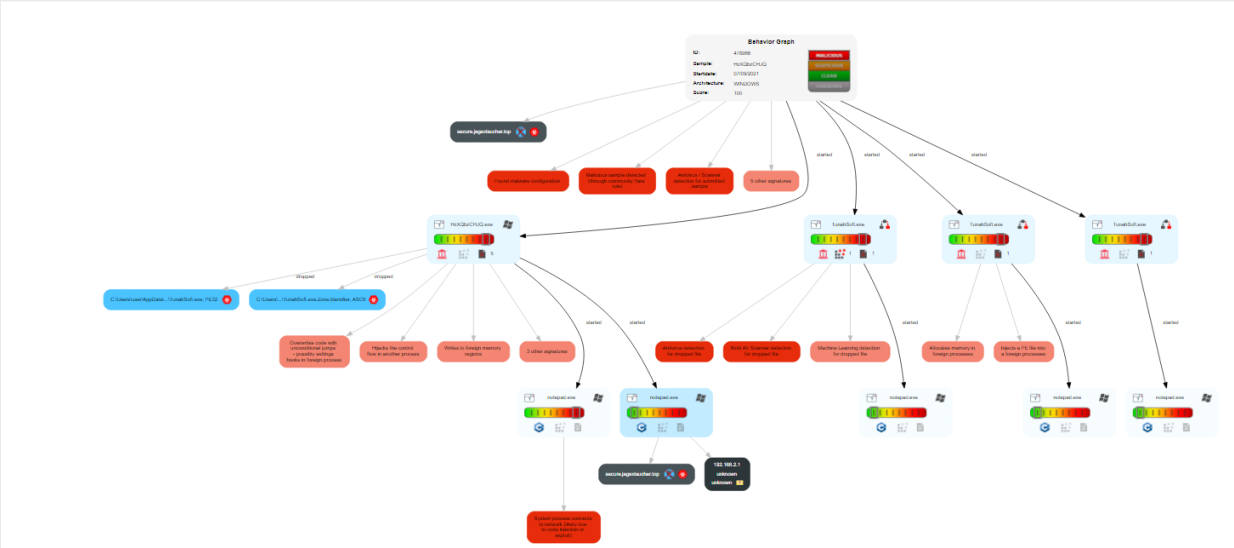
- System is w10x64
- HzXQbzCHJQ.exe (PID: 4780 cmdline: 'C:\Users\user\Desktop\HzXQbzCHJQ.exe' MD5: D9F06386725E69E44C508DD60B61DD01)
  - notepad.exe (PID: 6920 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
  - notepad.exe (PID: 6656 cmdline: notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
- TunahSoft.exe (PID: 5568 cmdline: 'C:\Users\user\AppData\Roaming\TunahSoft\TunahSoft.exe' MD5: D9F06386725E69E44C508DD60B61DD01)
  - notepad.exe (PID: 4972 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)
- cleanup

Malware Configuration

Threatname: NetWire

```
{
  "C2 list": [
    "secure.jagexlaucher.top:4066"
  ],
  "Password": "nigger",
  "Host ID": "HostId-%Rand%",
  "Mutex": "QDCvsrUh",
  "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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@14/3@40/1
EGA Information:	Failed

Anyrun 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 sys
actions and is provided for user acknowledgement as it is. ANY.RUN do

Behavior activities

MALICIOUS

Writes to a start menu file
- cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836)

SUSPICIOUS

Reads the computer name
- cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836)

Checks supported languages
- cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836)

Drops a file with too old compile date
- cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836)

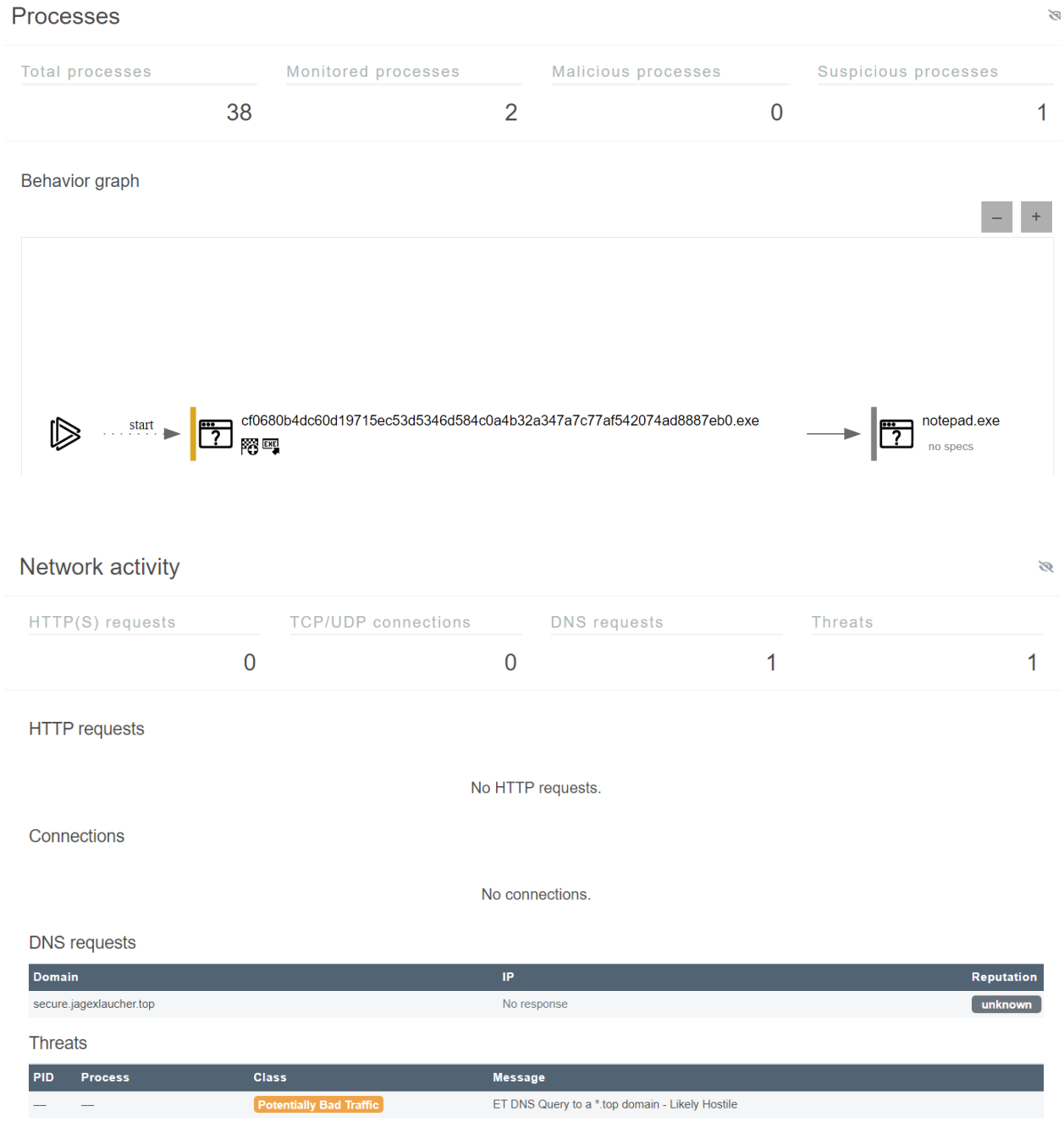
Creates files in the user directory
- cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836)

Executable content was dropped or overwritten
- cf0680b4dc60d19715ec53d5346d584c0a4b32a347a7c77af542074ad8887eb0.exe (PID: 2836)

INFO

Reads the computer name
- notepad.exe (PID: 1908)

Checks supported languages
- notepad.exe (PID: 1908)



Dynamic analysis of 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e using ANYRUN and Joe sandbox

Windows Analysis Report Uvnjtdnyzzyrqntxmdlgahpbcyrosnjtqn.exe

Create Interactive Tour

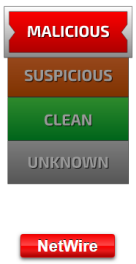
Overview

General Information

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

Most interesting Screenshot:

Detection

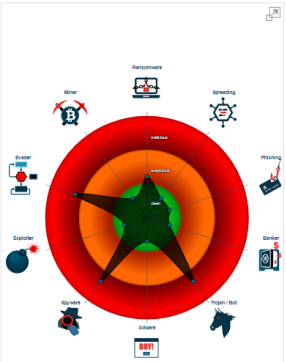


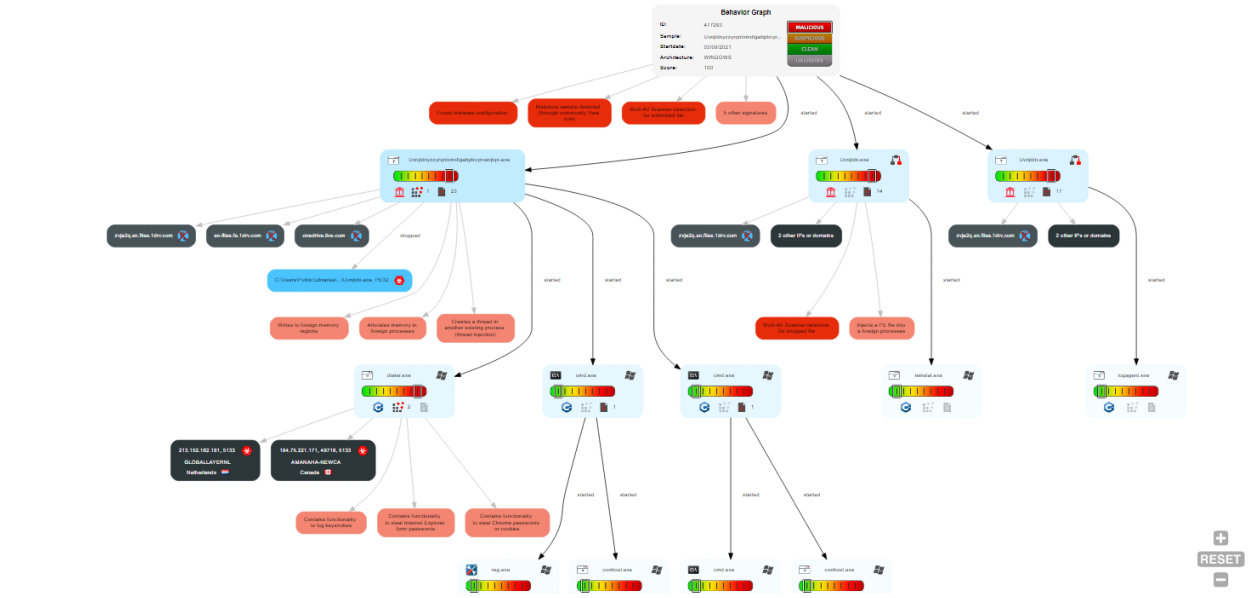
Score:	100
Range:	0 - 100
Whitelisted:	false

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





URLs

Source	Detection	Scanner	Label	Link
213.152.162.181:5133	0%	Avira URL Cloud	safe	
http://crl3.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+UZWWLYX9/EISFJI3916W3WOSA0QLEKPWAGKQA/Y21PKQCJ2VNCY:+BFYX9TGJI39DMOS5KTGKQX27CSC

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	**Checks supported languages** • 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152)	**Reads settings of System Certificates** • 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152)
	Reads the computer name • 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152)	**Checks Windows Trust Settings** • 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr (PID: 2152)
	Creates files in the user directory • 88f47e23c6b59062ba27bebe4cd6004379567bb613a91ec0b83644986212cf8e.exe.scr	

Screenshots

Processes

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

For File : e502fcf4ae5b5af00d0d58b55295cff685f473f8d57e750bfde618161d3ba006

Behavior activities

MALICIOUS

Uses Task Scheduler to run other applications
- Payment Notification.scr.exe (PID: 2740)
- Host.exe (PID: 1120)

Loads the Task Scheduler COM API
- schtasks.exe (PID: 3748)
- schtasks.exe (PID: 3580)

Drops executable file immediately after starts
- Payment Notification.scr.exe (PID: 3792)

NETWIRE was detected
- Host.exe (PID: 3620)

Connects to CnC server
- Host.exe (PID: 3620)

SUSPICIOUS

Reads the computer name
- Payment Notification.scr.exe (PID: 2740)
- Payment Notification.scr.exe (PID: 3792)
- Host.exe (PID: 1120)
- Host.exe (PID: 3620)

Checks supported languages
- Payment Notification.scr.exe (PID: 2740)
- Payment Notification.scr.exe (PID: 3792)
- Host.exe (PID: 1120)
- Host.exe (PID: 3620)

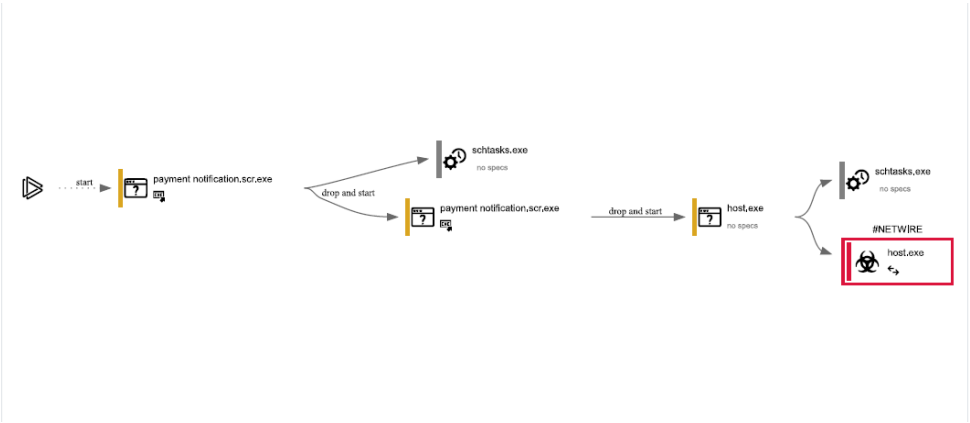
Creates files in the user directory
- Payment Notification.scr.exe (PID: 2740)
- Payment Notification.scr.exe (PID: 3792)

Application launched itself
- Payment Notification.scr.exe (PID: 2740)
- Host.exe (PID: 1120)

INFO

Checks supported languages
- schtasks.exe (PID: 3748)
- schtasks.exe (PID: 3580)

Reads the computer name
- schtasks.exe (PID: 3748)
- schtasks.exe (PID: 3580)



For File: dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56

Memory Forensics

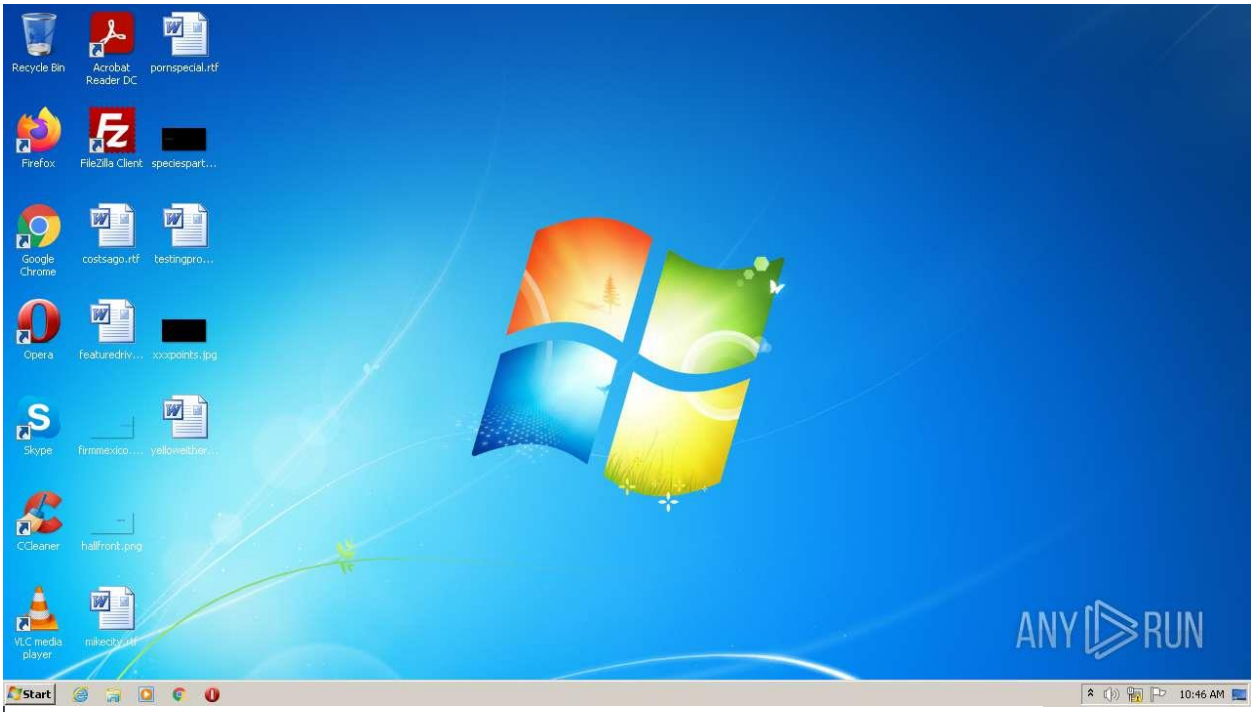
PID: 2528, Report UID: 00000000-00002528
Stream UID: cca05958526ca1b406317bbc8137c6fe-6000041-SessionsControl~tsbNewSSHSession_Click
File Name: dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.bin
@60007b2: ldstr ;Session
@60007b3: newobj System.Void System.Random.ctor()
@60007b4: ldc.i4.0
@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: ldfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@600063d: callvirt 0A000068
@600063e: pop
@600063f: ldarg.0
@6000640: ldfld System.Diagnostics.Process AppInForm.PuttyPanelm_Process
@6000641: callvirt 0A000069
@6000642: pop
@6000643: ldarg.0
@6000644: ldarg.0
@6000645: ldfld 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

Uses Task Scheduler to run other applications
- dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe (PID: 3452)

Loads the Task Scheduler COM API
- schtasks.exe (PID: 3680)

NETWIRE was detected
- RegSvcs.exe (PID: 3772)

SUSPICIOUS

Creates files in the user directory
- dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe (PID: 3452)

Executable content was dropped or overwritten
- dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe (PID: 3452)

Drops a file with a compile date too recent
- dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe (PID: 3452)

Checks supported languages
- dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe (PID: 3452)
- RegSvcs.exe (PID: 3772)

Reads the computer name
- dbf616ad9c72def90a363c076c2e66d25831350d2e1ad60b22675e2c0ad95e56.exe (PID: 3452)
- RegSvcs.exe (PID: 3772)

INFO

Checks supported languages
- schtasks.exe (PID: 3680)

Reads the computer name
- schtasks.exe (PID: 3680)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

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_0|O_O_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:%.2d|%u.%u%s%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

- $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/38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc
[12] https://www.virustotal.com/gui/file/4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34
[13] https://hybrid-analysis.com/sample/38f3b0091a63de45d06e5d073684a9ac020dd9963f2cde74dffc00d7ede040cc
[14] https://hybrid-analysis.com/sample/4c01cc3dd96c524054207f6b37a334c62549857f28c0286cc8dfc30b6d388e34