

Malware Countermeasures

Nico Ferrari

I. MALWARE MITIGATION RESEARCH

Computer security is a field which is growing day by day, constantly enhancing and developing new countermeasures techniques to protect the systems, but still, malicious software are succeeding in their destructive objectives. In fact, as well as computer security, attacking techniques are overcoming the new challenges imposed by the enhancement of the new security techniques, becoming an endless race between the security experts and the attackers. The goal of malwares is to infect the computer system or resources, deleting the data, slow down the working system or steal the important information, affecting then confidentiality, integrity and availability of the systems and resources.

The research of countermeasures against malware attacks, trying to protect data and operations, is typically divided in:

- securing the targeted systems against the attacks,
- respond to the attacks against the target systems.

Comparing traditional malwares with the modern ones, we notice that nowadays they are harder to detect and very targeted (i.e. affecting specific versions of software), exploiting zero-day vulnerabilities, persistent and stealthy, having the ability to change their code as they propagate and capable of propagating through the network and easily bypassing the defenses [1]. When viruses are known, it is possible to track their behaviour and save it in a database as signature. Static, Dynamic and Hybrid (static+dynamic) analysis can detect malicious behavior at runtime inside a safe environment, such as a VM. But nowadays, malwares are able to change their behaviour according to the target, making the analysis of their 'pattern' and their identification becomes much more difficult. As shown in [2], there are mainly two types of mitigation techniques:

- Sandboxig: where malwares are analyzed in a safe environment
- Application hardening techniques: to help programs be more resilient against exploits.

II. SANDBOXING

Once a safe environment called sandbox is set up, the software can be analyzed, examining the files for signs of malicious behaviours. The analysis may be conducted in a manner that is static, dynamic or a hybrid of the two. Basic static analysis does not require that the code is actually running. Each file of the software is analyzed, often with the help of tools like disassemblers and network analyzers, used to observe the malware without actually running it, with the goal to collect information on how it works. With modern malwares, malicious runtime behaviour can run

undetected, therefore, for a complete understanding of the malicious behaviour, dynamic analysis is used. Dynamic analysis involves the execution of malware in order to study its behaviour at runtime. To overcome to this, adversaries had to face this new challenges and become very good at detecting them. In fact, to deceive a sandbox, adversaries hide code inside them that may remain dormant until certain conditions are met and only then does the code is executed. Now days the two analysis techniques are used together and this is called hybrid analysis. Once the malware is detected in the sandbox environment, some tools such as YARA [3] can be used in order to detect them.

III. APPLICATION HARDENING TECHNIQUES

There are several techniques used to make the systems more resilient against malware [4]. A common technique is Data Execution Prevention, an host based system level memory protection feature designed to prevent the local copy of malicious code into a foreign process space and subsequently executing it [5]. This technique can be implemented via hardware and software. Complementary to the data execution prevention, Address Space Layout Randomization creates high randomness in memory addresses of a target process, helping to reduce the access of determined addresses of memory which could be know for their vulnerabilities.

Some malwares aim to infect the heap memory with malicious code then exploits a different vulnerability to cause the exploit to call the commands in the heap memory. To reduce this kind of attacks, the heap is filled with *NOP* (no operation) instructions.

Other hardening techniques try instead to prevent that malicious libraries such as DLL are preloaded by the malware. In fact, if an application dynamically load DLL without a full qualified path, OSs like Windows try to find it in specific directories. In order to limit this attacks, could be necessary to always specify the full path of the DLL and have total control of those directories.

IV. GENERAL COUNTERMEASURES

In order to mitigate the risk of being affected by malicious software, one of the most powerful countermeasures is the user awareness. Given that users of non-technical backgrounds might not be sufficiently aware of the cybersecurity risks they face, they can be the easy target of the attacker. Therefore, educating these personnel to be cautious of malware and unknown hardware with an introduction to cybersecurity, could greatly reduce the risks of institutions. Due to the low costs and availability of malicious software and how easy and fast is the diffusion process of the

malicious code, attackers of any level can cause several problems on the targeted systems. Therefore, being able to recognize the different malware categories, their features and countermeasures could help the users to understand the consequences of careless operations.

Often the attacker writes malicious code exploiting vulnerabilities in the software loaded in systems. For this reason, a Patch Management process becomes vital in order to keep the system functioning. The patch management process is usually divided in the following phases:

- scan of the system for missing security patches;
- determine the severity of the issue(s) addressed by the patch, evaluating the threat to the current environment. In fact, sometimes, patches could interfere with the current processes.
- if the decision goes to mitigate the threat using the patch, this patch must be downloaded;
- the patch is installed and tested, in order to evaluate how it affects the environment and actual configuration/workflow;
- the system is backed up and then the patch will be deployed.

In order to find malwares in the system, anti-virus becomes necessary. In fact, they will look for patterns matching with the known malicious code and will try to prevent the attacks.

Keeping controlled log files, could help to recognize the activity of malicious software. For example, a keylogger will probably try to sent the data acquired to an external entity,

and observing the established connections from the logs, it could be possible to find weird behaviours. Firewalls will help to restrict the interaction of a remote control program with system. In fact, some malwares try to communicate with the target systems through some special ports, and blocking the unused ones using a firewall will reduce these kind of risks.

Another countermeasure consists in the implementation of system access controls, and the policy of running applications with least privilege, trying to minimize the damage caused by malicious software [6].

REFERENCES

- [1] E. Gandotra, D. Bansal, and S. Sofat, "Malware Analysis and Classification: A Survey," *Journal of Information Security*, vol. 05, no. 02, pp. 56–64, 2014.
- [2] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," pp. 1–23, 5 2019.
- [3] VirusTotal, "YARA in a nutshell. [Online]," 2019. [Online]. Available: <https://virustotal.github.io/yara>
- [4] K. Jørgen, "Toward Anti-fragility: A Malware-Halting Technique," Tech. Rep. [Online]. Available: www.computer.org/security
- [5] F. C. Colon Osorio, IEEE Computer Society, Wireless Systems Security Research Laboratory, Microsoft Corporation, and Institute of Electrical and Electronics Engineers, "Host-Based Code Injection Attacks: A Popular Technique Used By Malware."
- [6] M. Souppaya and K. Scarfone, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 7 2013. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>

Since Metadefender was not available, i used as first attempt avira and ClamWin as antivirus. The first malwares i tried to analyze were eh.exe and bx89.exe. Both malwares have been recognized by the AVs and it has been possible to get more informations regarding them with Avira. In fact, avira redirected to an online page explaining which kind of malwares they were and then, searching on internet, it was possible to find their signatures. This would have been possible also with clamWin, querying the name of the malware in his database.

Avira Security Alert

! Date/Time: 10/6/2020, 2:46:08 PM
Type: Detection

Access to file 'C:\Users\nic\Desktop\eh.exe' containing the pattern of 'TR/Dropper.Gen' was blocked.

We moved the file to quarantine

You can get more information about the problem:

[Go to Avira Support](#)

[Details](#)

Static Details:

FILE TYPE	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5	2dc681805db26c87477be210d4fc9655
SHA1	e8a5c752a6d46a2632c9f54337fa5f97ab5e478

SECTION

.Kiki md5:	cffdc55c7cb193af65739bc4483c68c66 sha1: 788ad8e628d5a00020b75ff1318a584fa17c63d
.Kiki md5:	17a3d3cc7a6599f48e4992a52546a3e4 sha1: 7641dea2d4467af7030d758c8ff82f1f40df582
.Kiki md5:	bafe90c9b67578bc1ce612396a075df sha1: 2839c9bcc21fe69b20d0a4b58b97e6c6c723bacb size: 77824
.Kiki md5:	bcb671f0ea47bda87c220ace5a985341 sha1: 0ffb5644b3162e11e44ee36b241da3e0059cb8 size: 16384
.Kiki md5:	eb0da733015cd480b1f6144867aebcb8 sha1: 69023982ee1bd883f1eb0bdb12bd6d657112adc size: 4096
.Kiki md5:	c74a108c2d743772b73e82bf5aa0bf6 sha1: b4ed8a43a4703ca5e6f04b2e9acb60a2aa22403 size: 4096
.text md5:	bbb2e1606d996dbae934f8081b5e620 sha1: bbc331be3997fd1e81bbdbd13549277037e34d7f size: 4096

TIMESTAMP 2017-01-10 23:04:43

PEHASH b4392209089e3333d9d7d4ab2db4d9b14ef3b5cc

AV

avg	BackDoor.Generic_r.AFZ
avira	BDS/Morix.bh.1
clamav	WIN.Trojan.Morix

bx89.exe

File Home Share View

Malware > bx89.exe

Name	Date modified	Type
bx89	10/6/2020 3:01 PM	Application

1 item

C:\Users\nic\Downloads\Malware\bx89.exe\bx89.exe: Win.Trojan.Morix-1 FOUND

SCAN SUMMARY

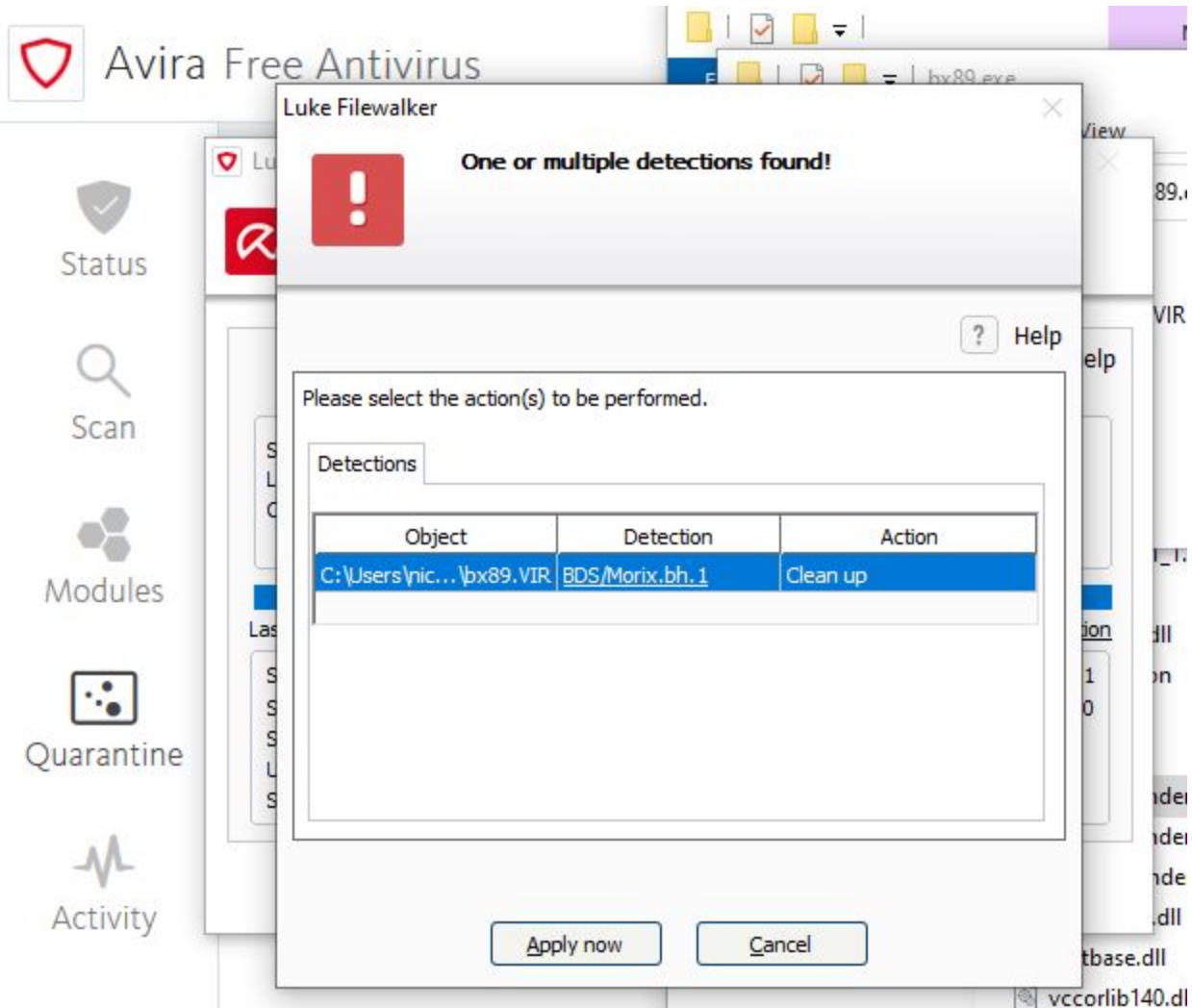
Known viruses: 8880807
Engine version: 0.99.4
Scanned directories: 0
Scanned files: 1
Infected files: 1

Data scanned: 0.13 MB
Data read: 0.28 MB (ratio 0.44:1)
Time: 89.017 sec (1 m 29 s)

Completed

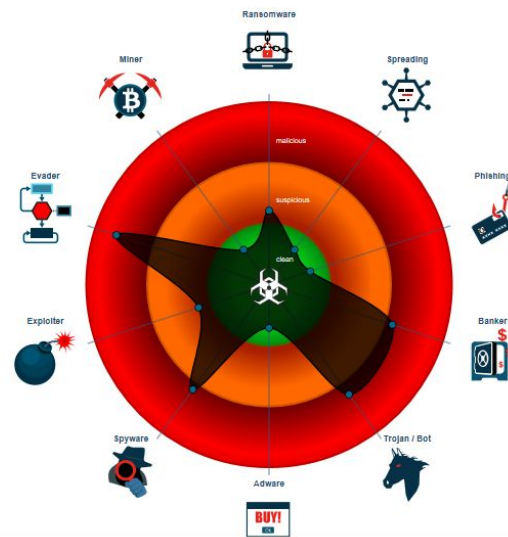
[Save Report](#) [Close](#)

As mitigation strategy, avira immediately asked to remove the malwares.



The attention focused on bx89.exe, a spyware classified as shown below.

Classification



Analysis Advice

Sample has functionality to log and monitor keystrokes, analyze it with the 'Simulates keyboard and window changes' cookbook

Sample may inject into Firefox, Chrome or IE. Choose the 'Browse malicious URL' cookbook for further analysis

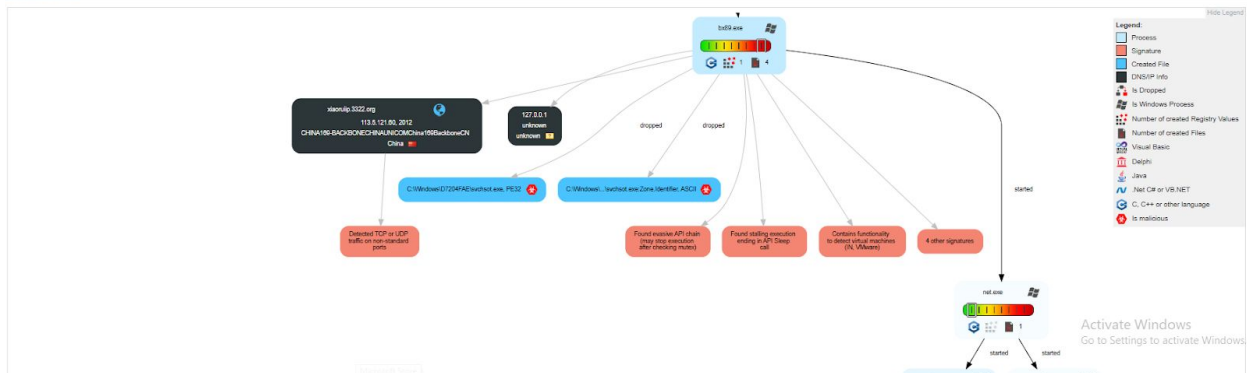
Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "-", "-")

Sample monitors Window changes (e.g. starting applications), analyze the sample with the 'Simulates keyboard and window changes' cookbook

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

and with the following behaviour:

Behavior Graph



Several other informations have been found regarding this malware, such as the files affected and the network traffic established during the infection.

Spreading:

- Contains functionality to enumerate / list files inside a directory [Show sources](#)
- Contains functionality to query local drives [Show sources](#)

Software Vulnerabilities:

- Found related log instructions (likely shell or obfuscated code) [Show sources](#)

Networking:

- Connects to country known for bullet proof hosting [Hide sources](#)
- Source: unknown Network traffic detected: IP: 113.5.121.80 China
- Detected TCP or UDP traffic on non-standard ports [Show sources](#)
- Uses dynamic DNS services [Show sources](#)
- Contains functionality to download additional files from the internet [Show sources](#)
- Performs DNS lookups [Show sources](#)
- Units found in memory or binary data [Show sources](#)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to capture and log keystrokes [Show sources](#)
- Contains functionality for real data from the clipboard [Hide sources](#)
- Source: C:\Users\User\Desktop\bx89.exe Code function: 0_2_10010200 OpenClipboard EmptyClipboard GlobalAlloc GlobalFree GlobalLock GlobalUnlock SetClipboardData GlobalFree CloseClipboard 0_2_10010200
- Contains functionality to read the clipboard data [Show sources](#)
- Contains functionality to retrieve information about pressed keystrokes [Show sources](#)

F-Banking Fraud:

- Checks if browser processes are running [Hide sources](#)
- Source: C:\Users\User\Desktop\bx89.exe Code function: RegOpenKeyEx RegQueryValue RegCloseKey Sleep WaitForSingleObject CreateProcess Applications\explorer.exe &&opencommand
- Source: C:\Users\User\Desktop\bx89.exe Code function: RegOpenKeyEx RegQueryValue RegCloseKey WaitForSingleObject CreateProcess Applications\explorer.exe &&opencommand

System Summary:

Running bx89.exe, doesn't shows any particular behaviour, but some background processes starts immediately to run using different names.



Background processes (82)

AliWangWang (32 bit)

- AntiVir shadow copy service
- > Antivirus Host Framework Servi...
- > Antivirus Host Framework Servi...
- Application Frame Host


⬅ Fewer details

version information. AliiM.exe's description (China) Network Technology Co.,Ltd.. AliiM (x86)\trademanager\ folder.

[ASIX AX88179 USB 3.0 to Gi](https://www.pcmatic.com/company)
<https://www.pcmatic.com/company>
PC Pitstop - PC Performance Roots. PC P diagnostics and maintenance. During the e tools were skyrocketing.
Missing: AliWangWang | Must include: AliW

[Alien Speech \(free\) downloa](https://en.freownloadmanager.or)
<https://en.freownloadmanager.or>

General Compatibility Security Details Previous Versions



Type of file: Application (.exe)

Description: AliWangWang

Location: C:\Users\nic\Desktop

Size: 291 KB (297,984 bytes)

Size on disk: 292 KB (299,008 bytes)


Created: Tuesday, October 6, 2020, 3:34:45 PM

Modified: Saturday, January 12, 2013, 9:48:10 AM

Accessed: Today, October 6, 2020, 13 minutes ago

Attributes: ☐ Read-only ☐ Hidden

In order to protect the system mitigating the thread, it was possible to turn on again the real time scan of the windows' AV

 **Threat quarantined**
10/7/2020 10:11 AM

Severe ^

Detected: Backdoor:Win32/Zegost.AD
Status: Quarantined
Quarantined files are in a restricted area where they can't harm your device.
They will be removed automatically.

Date: 10/7/2020 10:12 AM
Details: This program provides remote access to the computer it is installed on.

Affected items:

file: C:\Users\nic\Downloads\Malware\bx89.exe\bx89.exe

[Learn more](#)

Actions v

In order to obtain better information regarding the viruses, VirusTotal has been used. VirusTotal is an online scanner which scans the software that we send and tells us if it is a malicious one and then give us more informations regarding his behavior. This information could be important in order to manually remove or recognize malwares. During the execution of the lab, i tried to execute also a ransomware, which blocked all my VM. in order to remove the thread I reinstalled the whole system, an approach which could be dangerous in a production system. In fact, files could be infected and backing them up after the infection would mean spreading the virus. For this reason regular backups are fundamental also to help to recover infected machines. In order to avoid to infect my VM machine another time, I discovered any.run , an online platform which allows the user to test malwares and share the results, all contained in a sanboxed environment. i

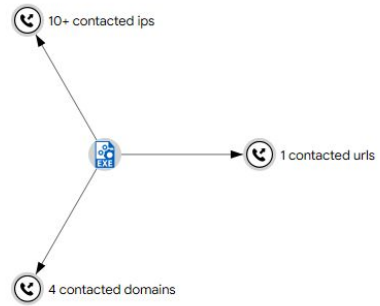


ae2086e8789ec946f5ed43bf09cc86f407836707169f10d17a3aa8beec05bea2

107.165.236.233	1 / 87	18779	US
184.168.221.89	1 / 87	26496	US
208.91.197.46	1 / 94	40034	VG
154.198.33.75	0 / 75	26484	US
127.0.0.1	0 / 94	-	-
156.232.24.75	0 / 87	26484	US
23.104.77.225	0 / 87	395954	US



Graph Summary ⓘ





ae2086e8789ec946f5ed43bf09cc86f407836707169f10d17a3aa8beec05bea2



bx89.exe

armadillo direct-cpu-clock-access long-sleeps peexe persistence runtime-modules

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 4

Contacted URLs 1

Scanned	Detections	URL
2013-04-26	3 / 37	http://xiaoruiip.3322.org/

Contacted Domains 1

Domain	Detections	Created	Registrar
xiaoruiip.3322.org	1 / 76	-	-
www.fz0575.com	2 / 94	2018-09-23	Network Solutions, LLC
www.wk1888.com	8 / 94	2019-10-30	Fujian Domains, Inc.
www.af0575.com	5 / 94	2019-10-11	DYNADOT, LLC

Contacted IPs 1

IP	Detections	Autonomous System	Country
113.5.121.60	0 / 75	4837	CN
185.245.180.55	0 / 75	46261	US
154.90.68.52	1 / 87	134548	US
107.165.236.233	1 / 87	18779	US
184.168.221.89	1 / 87	26496	US
208.91.197.46	1 / 94	40034	VG
154.198.33.75	0 / 75	26484	US
127.0.0.1	0 / 94	-	-
156.232.24.75	0 / 87	26484	US
208.101.255.255	0 / 87	26484	US



265041a4e943debd8b6b147085cb8549be110facde2288021e90ae65e87be235

API-MS-WIN-Service-Management-L1-1-0.dll

IPHLPAPI.DLL

API-MS-Win-Security-SDDL-L1-1-0.dll

WS2_32.dll

API-MS-Win-Security-LSALookup-L1-1-0.dll

CRYPTBASE.dll

OLEAUT32.dll

^

Highlighted Actions ⓘ

Calls Highlighted

GetTickCount

IsDebuggerPresent

SetFileTime

SetWindowsHookExW

GetAdaptersAddresses

Highlighted Text

C:\Windows\system32\cmd.exe

BL23

ransomware run in the sandboxed environment.

Warning

Network Stream

RAW data flow between two hosts

This computer has been detected as infected by malware. Please follow the next few pages to remove the malware. The next pages will allow you to remove the malware. [Click here to view the next page.](#)

136.243.249.66 : 80 ⇌ VM : 50091

files.homepagemodules.de

00000A40: F3 61 AA 30 83 5F 23 8E E5 EA 3E 85 06 8E B3 57 0a*0.#.àè>...W

00000A50: 3A E7 10 33 53 66 9C 4B A0 EA FD E4 AF 65 0F 92 :ç.3Sf.K.éyà'e..

00000A60: 75 D2 FE 41 8F D7 44 A5 28 BE 57 D1 B9 E8 BA B2 u0pA.>DW(\\N\\è**

00000A70: C7 69 1D 65 4B 11 22 71 40 10 E8 D1 BE C3 84 BC 01.e@."qè.eN\\A.%

00000A80: DF C0 64 2D 5D 63 BA 1C 06 34 E8 C0 49 9A BB EE 8Id=]e\$.4eEi.+s

00000A90: 08 35 50 5F 48 C0 19 5C 5C BD 2B 01 A8 20 91 70 .5P_Hf.\\\\s>.p

00000AA0: 23 2D 6C 89 43 34 C0 D1 8A 9A 68 78 54 A9 5E BA #-1'C4IN..hXTe^

00000AB0: 0F 74 51 9C A7 32 35 D5 96 F9 19 2E 8C 98 8B D9 .tQ.8250.ú....0

00000AC0: 75 6A 99 4E 57 1C B7 B6 CA 5C FE 77 23 63 06 10 uj.NW..\$E\\b#wc..

00000AD0: 13 20 30 EC 46 97 21 DF 73 63 0D 21 C1 BE E6 D3 . 01F.1Bsc.1A%0

00000AE0: AC F9 26 3D A6 E9 24 13 EE 29 3F 49 EF 2C 8B 93 ~0è=]e\$.1?1i. >

00000AF0: A8 F1 28 33 68 74 B8 7F C8 E8 4E FB E4 72 AC D1 "n(3ht>.AeN0ar-R

00000B00: C2 57 39 3A 0F 41 F2 FF 64 1E EF A2 F0 DA 4A C4 AW>:çAbjd-1cu0JA

00000B10: 07 33 54 06 B8 28 11 41 6F D2 36 FA F5 B7 3F B9 .3T-ç.Ao0u0:?'

00000B20: 2E 4E C8 B8 CE D1 40 E3 3E B8 E5 FA 58 B8 41 2C .NE>INMA>.aUX.A

00000B30: 77 8D A1 4E 7F 2B AE F3 ED C2 89 B4 72 A9 F9 DF w.N.++o1A.'re0ù

00000B40: F8 8D 37 0D 65 2B 03 10 D8 60 74 09 04 D6 32 FF e.7.e+..0't..02y

00000B50: 81 7C 23 F3 69 9B 5F 1A 0D B2 DE 45 C8 77 1C A7 .1#01...*BEw.s

00000B60: 08 A6 A2 08 0A 44 03 3D 8C A9 53 78 D6 D2 E3 CD .{c..D.=.eSx00sI

00000B70: 78 1F 2F 13 6D 5F 6E 58 B3 BC 8C 28 1D 9D F8 9F p./m.nX%...e

00000B80: AD DE 1F 03 4E 46 7A 09 90 EA FE A8 9F 4D 15 D1 .p..Nf...eb".M.R

00000B90: 4A C8 4A 38 36 5D F8 08 C4 07 6E 57 18 B5 81 84 JAJ8G10.A.NW.jz.

00000BA0: 58 5B E2 A8 E0 DC 10 86 CC D7 29 3E 83 34 2E FF X[a"au."1x">.4.y

00000BB0: D6 9C EB EB FA 12 B1 16 33 F0 33 DC 4D E8 D8 5E 0.èèè.±305UMed^

00000BC0: 7D BA 9D 68 44 D7 4E 0C A0 63 7E C3 38 BC AD DB }^hDxN..c-A8%.0

00000BD0: 7D 66 B5 19 31 D8 CC 8E 96 B0 D5 86 D5 81 CF 80 }fu.101..*0.0.I.

00000BE0: A4 E8 B4 7D B8 E5 28 77 F6 1E 16 FF C2 ED 82 0E ah")>à(w0..yA1..

00000BF0: 43 63 B8 4B 02 13 6C 69 82 B5 F2 4A 58 38 B7 57 Cc"K.11.p0JK8-W

00000C00: A8 3D A8 A8 23 3A 77 5A 73 F6 7A 92 7E A8 B6 F9 =."#wKrdL~e.0

Close

www.sp33d.com

localhost:80

Warning: [2188] ransomware.exe.malware.exe Starts CMD EXE for commands execution

HTTP Requests

Connections

DNS Requests

Threats

TimeShift

Protocol

Rep

PID

Process name

CN

IP

Port

1016 ms

TCP

?

2188

ransomware.exe.malware.exe

136.243.249.66

80

1024 ms

TCP

?

2188

ransomware.exe.malware.exe

104.28.25.95

80

22514 ms

TCP

?

2188

ransomware.exe.malware.exe

104.31.87.124

80

22517 ms

TCP

?

2188

ransomware.exe.malware.exe

104.31.87.124

443

Traffic

PCAP

↑ 358 b ↓ 12.6 Kb

↑ 326 b ↓ 64.8 Kb

↑ 365 b ↓ 887 b

↑ 671 b ↓ 5.36 Kb

General Info

File name	ransomware.exe.malware
Full analysis	https://app.any.run/tasks/8700ecfa-3fc7-435f-9423-f6d5c75965d6
Verdict	Suspicious activity
Analysis date	7/23/2018, 04:50:29
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, UPX compressed

MD5	63BAE74409C514ED8548B1F33D0ACEDC
SHA1	ABC6B8DD01FA83D7FD92182601B868D2B6DD1EA
SHA256	265041A4E943DEBD8B6B147085CB8549BE110FACDE2288021E90AE65E87BE235
SSDEEP	12288:S6WQ4AAE6KWYF5LOY2D1PQLVSV7UIKFGD9CFNU:QTHEVAPQLILUBGDYU

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

Behavior activities

1 MALICIOUS	2 SUSPICIOUS	3 INFO
Changes the autorun value in the registry <ul style="list-style-type: none">ransomware.exe.malware.exe (PID: 2188)	Reads Internet explorer settings <ul style="list-style-type: none">ransomware.exe.malware.exe (PID: 2188) Creates files in the user directory <ul style="list-style-type: none">ransomware.exe.malware.exe (PID: 2188) Starts CMD.EXE for commands execution <ul style="list-style-type: none">ransomware.exe.malware.exe (PID: 2188)	Dropped object may contain URL's <ul style="list-style-type: none">ransomware.exe.malware.exe (PID: 2188)

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

TRiD

.exe | Autolt3 compiled script executable (88.1%)
.exe | UPX compressed Win32 Executable (4.6%)
.exe | Win32 EXE Yoda's Crypter (4.6%)
.dll | Win32 Dynamic Link Library (generic) (1.1%)
.exe | Win32 Executable (generic) (0.7%)

EXIF

EXE

MachineType: Intel 386 or later, and compatibles
TimeStamp: 2012-01-29 22:32:28+01:00
PEType: PE32
LinkerVersion: 10
CodeSize: 274432
InitializedDataSize: 122880
UninitializedDataSize: 573440
EntryPoint: 0xcee90
OSVersion: 5
ImageVersion: null
SubsystemVersion: 5
Subsystem: Windows GUI
FileVersionNumber: 3.3.8.1
ProductVersionNumber: 3.3.8.1
FileFlagsMask: 0x0017
FileFlags: (none)
FileOS: Win32
ObjectFileType: Unknown
FileSubtype: null
LanguageCode: English (British)
CharacterSet: Unicode
FileDescription: null
FileVersion: 3, 3, 8, 1
CompiledScript: Autolt v3 Script: 3, 3, 8, 1

Summary

Architecture: IMAGE_FILE_MACHINE_I386
Subsystem: IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date: 29-Jan-2012 21:32:28
Detected languages: English - United Kingdom
English - United States
FileDescription: null
FileVersion: 3, 3, 8, 1
CompiledScript: Autolt v3 Script: 3, 3, 8, 1

PID	Process	Operation	Key	Name	Value
2188	ransomware.exe.malware.exe.write		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run C:\Users\admin\AppData\Local\Temp\ransomware.exe.malware.exe	ransomware.exe.malware.exe	
2188	ransomware.exe.malware.exe.write		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet	0
2188	ransomware.exe.malware.exe.write		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	1
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASAPI32	EnableFileTracing	0
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASAPI32	EnableConsoleTracing	0
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASAPI32	FileTracingMask	4294901760
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASAPI32	ConsoleTracingMask	4294901760
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASAPI32	MaxFileSize	1048576
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASAPI32	FileDirectory	%windir%\tracing
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASMANCS	EnableFileTracing	0
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASMANCS	EnableConsoleTracing	0
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASMANCS	FileTracingMask	4294901760
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASMANCS	ConsoleTracingMask	4294901760
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASMANCS	MaxFileSize	1048576
2188	ransomware.exe.malware.exe.write		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ransomware_RASMANCS	FileDirectory	%windir%\tracing
2188	ransomware.exe.malware.exe.write		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	ProxyEnable	0
2188	ransomware.exe.malware.exe.write		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	
46000000470000001000B096B6868EBD3010000000000000000000000000000000000FE800000000000007D6CB050D9C					
2188	ransomware.exe.malware.exe.write		HKEY_CLASSES_ROOT\Local Settings\MuiCache\59\52C64B7E	LanguageList	en-US

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	1	4	1

Dropped files

PID	Process	Filename	Type
2188	ransomware.exe.malware.exe	Users\admin\AppData\Roaming\Microsoft\Windows\IE\IECache\index.dat	dat
		MD5: D7A950FEFD60DBAA01DF2D65FEFB3862 SHA256: 75D0B1743F61B76A35B1FEDD32378837805DE58D79FA950CB6E8164BFA72073A	
2188	ransomware.exe.malware.exe	Users\admin\AppData\Local\Temp\scratch.cmd	—
		MD5: — SHA256: —	
2188	ransomware.exe.malware.exe	Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\GUFVP8I9\Glene[1].png	Image
		MD5: 2A21843D535267F62BA3D318C1FCC884 SHA256: 08A45DE65DD737899F4B167AB9E6BA502D96E0E10A23C2728789A9A444059D9E	
2188	ransomware.exe.malware.exe	Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XB3OCR2W\avatar-f6cfa349-11[1].png	Image

With all these informations would be possible to check all the registers and files created, removed and edited and manually trying to restore the normal conditions.

In the beginning clamWin was not detecting the malwares, and, if that happens, it is possible to load your own signatures from the .exe files and reperform the scan.

I tried to generate a simple signature following the commands suggested in the documentation and from online forums, but this didn't bring any success under windows environment. Here the commands executed:

```
.lsiqtool.exe --md5 C:\Users\nic\Downloads\Malware\bx89.exe\bx89.exe > custom.hdb
```

To generate the signature from a malware.

```
.\clamscan.exe -d 'C:\Program Files (x86)\ClamWin\bin\custom.hdb'
```

```
C:\Users\nic\Downloads\Malware\bx89.exe\bx89.exe
```

```
LibClamAV Error: cli_loadhash: Problem parsing database at line 1
```

```
LibClamAV Error: Can't load C:\Program Files (x86)\ClamWin\bin\custom.hdb: Malformed database
```

```
ERROR: Malformed database
```

The .hdb file has also been edited using the following format as suggested in the official documentation:

```
Name:Type:Offset:malware hex output
```

But still not working.