



efrei

PARIS PANTHÉON-ASSAS UNIVERSITÉ

Architecture Sécurisé – Analyse d'un ransomware

Par David TEJEDA, Vincent LAGOGUE et Thomas PEUGNET

Table des matières

1. Installation de theZoo	3
2. Installation de clamav	4
3. Analyse Statique	5
3.1 File	5
3.2 Strings	5
3.3 Contenu du mail	5
3.4 CMS ciblés	6
3.5 Scan avec Clamav	6
3.6 Virus Total	7
3.7 Cas concret avec Ransomware.Rex	8
4. Analyse Dynamique.....	9
4.1 Observations de strace sur la commande whoami	9
4.1.1 Processus général.....	9
4.1.2 Interprétation	10
4.2 Application sur un ransomware (REX).....	10
4.2.1 Contexte et fichier strace.txt	10
4.2.2 Interprétation	10
5. Conclusion	11

1. Installation de theZoo

Clonage du repos github :

```
(kali@kali)-[~]
$ git clone https://www.github.com/ytisf/theZoo
Cloning into 'theZoo' ...
warning: redirecting to https://github.com/ytisf/theZoo.git/
remote: Enumerating objects: 3090, done.
remote: Counting objects: 100% (127/127), done.
remote: Compressing objects: 100% (100/100), done.
remote: Total 3090 (delta 25), reused 107 (delta 15), pack-reused 2963 (from 1)
Receiving objects: 100% (3090/3090), 1.06 GiB | 42.17 MiB/s, done.
Resolving deltas: 100% (668/668), done.
Updating files: 100% (1439/1439), done.
```

Installation des requirements :

```
(kali@kali)-[~/theZoo]
$ pip install --user -r requirements.txt
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (2.0.7)
Collecting pyminizip (from -r requirements.txt (line 2))
  Downloading pyminizip-0.2.6.tar.gz (261 kB)
  Preparing metadata (setup.py) ... done
Collecting pyzipper (from -r requirements.txt (line 3))
  Downloading pyzipper-0.3.6-py2.py3-none-any.whl.metadata (3.5 kB)
Requirement already satisfied: pycryptodomex in /usr/lib/python3/dist-packages (from pyzipper->r requirements.txt (line 3)) (3.11.0)
Downloading pyzipper-0.3.6-py2.py3-none-any.whl (67 kB)
Building wheels for collected packages: pyminizip
  Building wheel for pyminizip (setup.py) ... done
  Created wheel for pyminizip: filename=pyminizip-0.2.6-cp311-cp311-linux_x86_64.whl size=203781 sha256=bc6c69053da5989cff527f7b0533ba6a0d0f27cdf6dd34ec167583291dddb55e
  Stored in directory: /home/kali/.cache/pip/wheels/50/c4/3c/6fb797c8b35d61411c595e7b2074dc657e4395a7ff525bbace
Successfully built pyminizip
Installing collected packages: pyminizip, pyzipper
Successfully installed pyminizip-0.2.6 pyzipper-0.3.6
```

Nous avons bien installé theZoo :

```

      SMMS                      oMMY
      :ooooo/                  /ooooo:
      ~~~~+MMd~~~~~hMMo
      oNNNNNNNNNNNNNNNNNNNNNNNN
      /oodMMdooyMMMMMMMMMyoodMMdoo/
      ~..dMMMMMy.:MMMMMMMM/ sMMMMMM..~
      dmmMMMMMMNNmmNNNNNNNNmmNNNNNNmmmm
      NMMyoodMMMMMMMMMMMMMMMMMMMMdoosMMM
      NMM- sMMMMNNNNNNNNNNNNNNNNMMY .MMM
      NMM- sMMY~~~~~sMMY .MMM
      ooo. :oooooooo+ +oooooooo/ ~ooo
           /MMMMN mMMMM+

theZoo 0.6.0 'Moat'
DB ver. 1712294860000

https://github.com/ytisf/theZoo

authors: Yuval Nativ, Lahad Ludar, 5fingers
maintained by: Shahak Shalev, Yuval Nativ
github: https://github.com/ytisf/theZoo

mdb #> █
```

Malheureusement, nous ne parvenons pas à télécharger le code via theZoo :

```

mdb #> search rex
+-----+-----+-----+-----+-----+-----+
| # | Type | Language | Architecture | Platform | Name |
+-----+-----+-----+-----+-----+-----+
| 160 | ransomware | bin | x86 | linux | Rex |
+-----+-----+-----+-----+-----+-----+
[+] Total records found: 1

mdb #> use 160
mdb Rex#> info
+-----+-----+-----+-----+-----+-----+-----+-----+
| % | Name | Ver. | Author | Lang | Date | Arch. | Plat. | Tags |
+-----+-----+-----+-----+-----+-----+-----+-----+
| ransomware | Rex | NA | NA | bin | NA | x86 | linux | Drupal |
+-----+-----+-----+-----+-----+-----+-----+-----+
[+] Total records found: 1

mdb Rex#> get
[-] Error getting malware.
mdb Rex#> update-db
Traceback (most recent call last):
  File "/home/kali/theZoo/theZoo.py", line 109, in <module>
    main()
  File "/home/kali/theZoo/theZoo.py", line 104, in main
    terminalHandler.MainMenu()
  File "/home/kali/theZoo/imports/terminal_handler.py", line 91, in MainMenu
    self.actOnCommand(cmd)
  File "/home/kali/theZoo/imports/terminal_handler.py", line 121, in actOnCommand
    update_handler.update_db(db_ver)
  File "/home/kali/theZoo/imports/update_handler.py", line 67, in update_db
    print(red('[+]') + " A newer version is available: " + new_maldb_ver + "!")
                                                                    ^
TypeError: can only concatenate str (not "bytes") to str

```

Nous avons utilisé python 2.7 pour lancer theZoo et cette fois ça fonctionne :

```

mdb Rex#> get
Downloading: Ransomware.Rex.zip Bytes: 2843585
2843585 [100.00%]

Downloading: Ransomware.Rex.pass Bytes: 10
10 [100.00%]

Downloading: Ransomware.Rex.md5 Bytes: 53
53 [100.00%]

Downloading: Ransomware.Rex.sha256 Bytes: 85
85 [100.00%]

[+] Successfully downloaded a new friend.

```

Nous avons extrait le fichier :

```

(root@kali)-[/home/kali/theZoo]
# unzip Ransomware.Rex.zip
Archive: Ransomware.Rex.zip
[Ransomware.Rex.zip] WTEpZSFwgb password:
inflating: WTEpZSFwgb

```

2. Installation de clamav

Nous avons bien installé clamav :

```
(root@kali)-[/home/kali]
# sudo apt install clamav

The following packages were automatically installed and are no longer required:
ibverbs-providers libcephfs2 libglusterfs0 libpython3.11-dev python3-lib2to3 samba-vfs-modules
libassuan0 libgfpapi0 libgphoto2-l10n librados2 python3.11
libboost-iostreams1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev
libboost-thread1.83.0 libgfxdr0 libperl5.38t64 perl-modules-5.38 python3.11-minimal
Use 'sudo apt autoremove' to remove them.

Upgrading:
blueman libldb2 libss2 onboard-common python3-ldb samba-common zstd
dpkg-dev libminizip1t64 libtalloc2 onboard-data python3-minimal samba-common-bin
gnutls-bin libpcr2-16-0 libtdb1 p11-kit python3-nassl samba-libs
ldap-utils libpython3-dev libtevent0t64 python3 python3-samba samba-vfs-modules
libdpkg-perl libpython3-stdlib libwbclient0 python3-arc4 python3-talloc smbclient
libjs-sphinxdoc libsass2-modules libxml2-utils python3-brotli python3-tdb tdb-tools
libldap-common libsmclient0 onboard python3-dev samba xz-utils

Installing:
clamav

Installing dependencies:
clamav-base libnss-winbind python3.12 samba-ad-dc winbind
clamav-freshclam libpam-winbind python3.12-dev samba-ad-provision
libclamav12 libpython3.12-dev python3.12-minimal samba-dsdb-modules
```

3. Analyse Statique

3.1 File

```
(root@kali)-[/home/kali/theZoo]
# file WTF25FWgb
WTF25FWgb: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, Go BuildID=fc5a3d09dbaf04f6ec0587eae8c207fe211c5530, stripped
```

Le fichier analysé, nommé WTF25Payload, est un binaire exécutable au format ELF conçu pour s'exécuter sur des systèmes Linux. Il est destiné à une architecture x86 (32 bits), compatible avec les processeurs Intel 80386, et utilise un ordre des octets Little Endian (LSB). Ce fichier est statiquement lié, ce qui signifie qu'il contient toutes les bibliothèques nécessaires à son exécution, le rendant autonome. Par sa nature, il ne s'agit pas d'une librairie, mais d'un programme exécutable, probablement conçu pour cibler des systèmes Linux spécifiques.

3.2 Strings

On a utilisé string pour extraire toutes les chaînes de caractères du binaire et ensuite on a utilisé grep pour rechercher des mots clés.

3.3 Contenu du mail

```
09: failed to parse EC private key: x509: trailing data after X.509 key-idzip: unsupported compr
cause it doesn't contain any IP SANs%q is an incomplete or empty template%2006-01-02 15:04:05.9
77555756156289135105907917022705078125?n-admin/config/system/site-informationGobDecoder: length
rMSpan_Sweep: bad span state after sweepSubject: ATTENTION: Ransom request!!!
EDNS: version can't represent recursive pointer type Crypto/RSA: invalid options for Decryptgob
pointer of type http: putIdleConn: keep alives disabledinvalid indexed representation index %dm
n in MHeap_SysAllocmissing argument to repetition operatormultipart: can't write to finished par
```

Le sujet est : ATTENTION : Ransom request !!!

```

sponse to channel open. xtls: ECDSA signature contained zero or negative values: bad signature type for client
s ECDSA certificate: failed to create cipher while encrypting ticket: tls: found unknown private key type in PKC
S#8 wrapping: server resumed a session with a different version: unsupported signature type for client certifi
cate: cannot verify signature: algorithm unimplemented: trailing data after X.509 CRL distribution point$S
-----END PUBLIC KEY-----FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3
404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D0D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BF85A899F
A5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9
ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2B
CBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFFFORWARD THIS MAIL TO WHOEVER IS IMPORTA
NT IN YOUR COMPANY AND CAN MAKE DECISION!
rex/scanner.(*Drupal).SetEmail
rex/scanner.(*RansomScanner).extractMailto

```

On a l'expéditeur du mail et la mention « Forward to whoever is important in your company and can make decision! ».

```

(root@kali)-[/home/kali/theZoo]
# grep -i "bitcoin" output.txt
All your servers will be DDOS-ed starting {{ .Time.Weekday.String }} ({{ .Time.Format "Jan 2 2006" }}) if you don't
pay {{ .Amount }} Bitcoins @ {{ .Address }}
Bitcoin is anonymous, nobody will ever know you cooperated.abbradiogroupparamalignmarkbdialogaccept-charsetbodyaccess

```

Des menaces de DDOS sont envoyées et il est fait mention de Bitcoin.

3.4 CMS ciblés

```

security/cacert/3101070740334300047303007012370743
t power-of-2GET / HTTP/1.0
rex/scanner.NewWordPressModule
rex/scanner.(*WordPress).Validate
rex/scanner.(*WordPress).validateGenerator
rex/scanner.(*WordPress).validateReadme
rex/scanner.(*WordPress).PageStyles
rex/scanner.(*WordPress).Scan
rex/scanner.(*WordPress).uploadWPUF
rex/scanner.(*WordPress).ExecPHP

```

Wordpress est ciblé.

```

rex/scanner.(*Drupal).SetDefaultTheme
rex/scanner.(*Drupal).DoBatch
rex/scanner.(*Drupal).CompleteBatch
rex/scanner.(*Drupal).getMetaRefresh
rex/scanner.(*Drupal).ExecSQL
rex/scanner.(*Drupal).ExecPHP

```

Dupral est ciblé.

```

(root@kali)-[/home/kali/theZoo]
# grep -i "joomla" output_strings.txt
grep: output_strings.txt: No such file or directory

(root@kali)-[/home/kali/theZoo]
# grep -i "magento" output_strings.txt
grep: output_strings.txt: No such file or directory

```

Joomla et Magento ne sont pas ciblés.

3.5 Scan avec Clamav

Nous avons scanné Rex avec Clamav :

```
(root@kali)-[/home/kali/theZoo]
# grep -i "" clam.txt
Scanning /home/kali/theZoo/WTEpZSFwgb
/home/kali/theZoo/WTEpZSFwgb: Unix.Malware.Agent-1628853 FOUND

----- SCAN SUMMARY -----
Known viruses: 8704090
Engine version: 1.4.1
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 7.74 MB
Data read: 7.27 MB (ratio 1.06:1)
Time: 16.042 sec (0 m 16 s)
Start Date: 2025:01:28 09:22:41
End Date: 2025:01:28 09:22:57
```

Clamav détecte bien qu'il s'agit d'un ransomware.

3.6 Virus Total

762a42b5ea4f72fce674da1ad29f0b9357be18de4cd992d79198c56bb514

42/64 security vendors flagged this file as malicious

Community Score: 42 / 64

WTEpZSFwgb

Size: 7.28 MB | Last Analysis Date: 1 month ago

elf ssh-communication exploit

Popular threat label: trojan.elfreddos/mjss

Threat categories: trojan ransomware

Family labels: elfreddos mjss

Security vendors' analysis

Vendor	Detection
AhnLab-V3	Linux/Rex
Antiy-AVL	Trojan.Linux.Rex.a
Avast	ELF-Rex.A [Trj]
Avira (no cloud)	LINUX/Rex.mjss
ClamAV	Unix.Malware.Agent-1628853
SentinelOne (Static ML)	Static AI - Malicious ELF
Sophos	Mal/Generic-S
Tencent	Linux.Trojan.Rex.Qqil
Trellix (HX)	Trojan.Generic.35784193
TrendMicro-HouseCall	Ransom_ElfrExDDOS.A
VIPRE	Trojan.Generic.35784193
Xcitium	Malware@#2m1kdg0a2b61
Acronis (Static ML)	Undetected
Avast-Mobile	Undetected
Bkav Pro	Undetected
CrowdStrike Falcon	Undetected
Jiangmin	Undetected
K7GW	Undetected
MaxSecure	Undetected

Détection des menaces sur VirusTotal : comprendre les angles morts

Certains antivirus ne signalent pas un fichier suspect lors d'un scan. Plusieurs mécanismes expliquent ces faux négatifs. D'abord, le ransomware pourrait être une toute nouvelle version (*zero-day*), non répertoriée dans les bases de signatures.

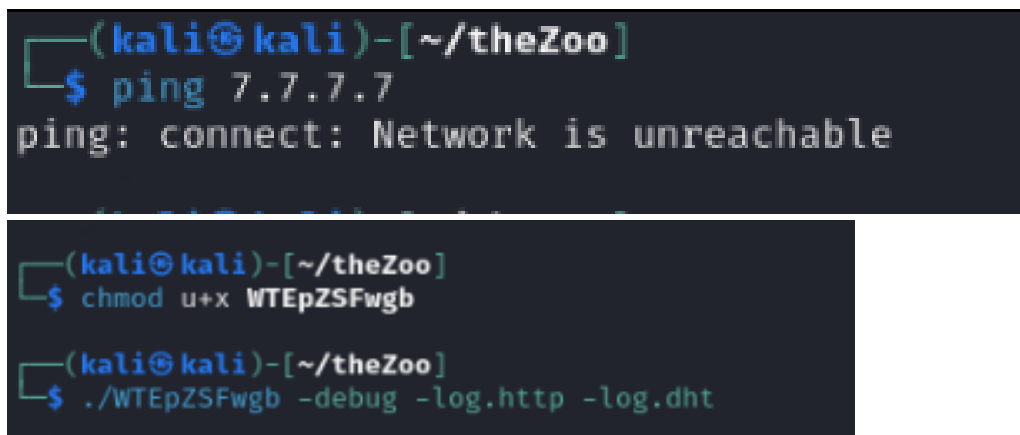
Certains éditeurs mettent parfois plusieurs jours à mettre à jour leurs définitions, surtout face à des codes polymorphes qui mutent à chaque infection.

Autre piste : les techniques d'obfuscation. En compressant ou chiffrant son code (via des packers comme UPX ou des outils maison), le malware devient une énigme pour les analyseurs statiques. Même l'analyse heuristique peut échouer si le moteur antivirus n'intègre pas les dernières règles de détection comportementale.

3.7 Cas concret avec Ransomware.Rex

Lors d'un test en sandbox, après avoir exécuté :

```
chmod u+x Ransomware.Rex
./Ransomware.Rex -debug -log.http -log.dht # (sans connexion réseau)
```

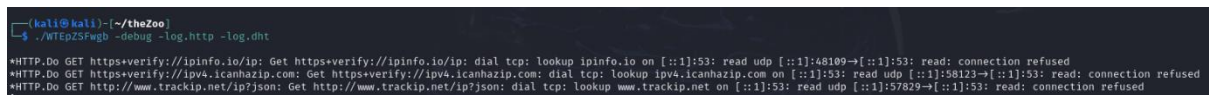


```
(kali@kali)-[~/theZoo]
$ ping 7.7.7.7
ping: connect: Network is unreachable

(kali@kali)-[~/theZoo]
$ chmod u+x WTEpZSFwgb

(kali@kali)-[~/theZoo]
$ ./WTEpZSFwgb -debug -log.http -log.dht
```

On observe un comportement révélateur : dès le lancement, le malware tente de contacter un serveur externe via HTTP ou le réseau DHT (comme un nœud BitTorrent). Mais sans internet, cette tentative échoue silencieusement.



```
(kali@kali)-[~/theZoo]
$ ./WTEpZSFwgb -debug -log.http -log.dht
*HTTP.Do GET https-verify://ipinfo.io/ip: Get https-verify://ipinfo.io/ip: dial tcp: lookup ipinfo.io on [::1]:53: read udp [::1]:48109->[::1]:53: read: connection refused
*HTTP.Do GET https-verify://ip4.icanhazip.com: Get https-verify://ip4.icanhazip.com: dial tcp: lookup ip4.icanhazip.com on [::1]:53: read udp [::1]:58123->[::1]:53: read: connection refused
*HTTP.Do GET http://www.trackip.net/ip7json: Get http://www.trackip.net/ip7json: dial tcp: lookup www.trackip.net on [::1]:53: read udp [::1]:57829->[::1]:53: read: connection refused
```

Ce qui est intrigant : le programme refuse de poursuivre son exécution sans avoir reçu une réponse spécifique, probablement une clé de géolocalisation ou un ordre du C&C (serveur de commandement). Cette dépendance explique pourquoi l'infection peut rester dormante dans certains environnements de test - une faille que les solutions antivirus traditionnelles ne captent pas toujours.

4. `openat("/etc/passwd") + read(...)` : Recherche du nom d'utilisateur associé à l'UID.
5. `write(1, "kali\n", 5)` : Écriture finale du résultat sur la sortie standard.

4.1.2 Interprétation

- whoami se contente de vérifier l'utilisateur courant via `/etc/passwd`.
- Les multiples `openat`, `mmap`, etc. relèvent surtout de la résolution dynamique des bibliothèques et de la configuration mémoire.
- Le programme n'initie aucune action « malveillante » : il se limite à renvoyer le nom de l'utilisateur en cours.

4.2 Application sur un ransomware (REX)

4.2.1 Contexte et fichier `strace.txt`

Pour un ransomware comme REX, on capture également les appels système avec `strace`. Dans le TP, on dispose déjà d'un fichier `strace.txt` qui montre ce que REX fait au démarrage :

- Ouverture de ressources réseau :
 - Par exemple, `openat(AT_FDCWD, "/proc/sys/net/core/somaxconn", ...)`, qui suggère une vérification du paramètre système sur le nombre maximal de connexions.
- Tentative de connexion à un C&C :

```
connect(8, {sa_family=AF_INET, sin_port=htons(5099),  
sin_addr=inet_addr("83.241.220.100")}, 16) = -1 EINPROGRESS.
```

- Cela indique que REX essaie de se connecter à un serveur distant.

4.2.2 Interprétation

REX pourrait évaluer la capacité du système à accepter de multiples connexions, ce qui est utile pour des attaques DDoS ou la propagation du ransomware. Ce dernier pourrait également communiquer avec un serveur de commande et de contrôle pour y récupérer des instructions ou signaler son activité. En outre, il pourrait effectuer des actions locales telles que la lecture ou l'écriture de fichiers spécifiques, comme une étape de préparation au chiffrement.

En analysant la trace, on comprend mieux quand et comment le malware se déclenche réellement (par exemple, seulement si la géolocalisation renvoie une certaine réponse, comme mentionné dans l'énoncé).

5. Conclusion

L'analyse de ransomware effectuée dans ce rapport met en lumière les différentes méthodologies utilisées pour comprendre le fonctionnement de logiciels malveillants, en combinant analyse statique et analyse dynamique. Grâce à l'utilisation d'outils comme *theZoo*, *ClamAV*, *VirusTotal* et *strace*, nous avons pu observer comment un ransomware comme REX fonctionne, depuis son exécution initiale jusqu'à ses tentatives de communication avec un serveur distant.