

Commencé le mardi 9 avril 2024, 18:24**État** Terminé**Terminé le** mardi 9 avril 2024, 20:37**Temps mis** 2 heures 12 min**QUESTION 0**

Terminé

Non noté

Entrez le nom de votre groupe ainsi que les noms de famille des participants séparés par des virgules

Réponse : Ferreira, Giorgis, Piga, Augsburg (Groupe 15)

DESCRIPTION

Les maliciels

QUESTION 2.1

Terminé

Noté sur 1,00

Décrire ce qu'est un maliciel ainsi que ses caractéristiques.

Un maliciel (ou malware) est un programme informatique "malveillant", qui a pour but d'endommager un système informatique, altérer le comportement d'un terminal/système informatique. Il a une capacité de propagation, c'est un code exécutable.

QUESTION 2.2

Terminé

Noté sur 1,00

Quelles sont les différentes catégories et fonctionnalités des maliciels.

Il y a plusieurs catégories de malware, Trojan qui a la particularité d'être un programme qui semble normale, mais qui en vérité cache une fonctionnalité malveillante, backdoor qui est un programme qui a pour objectif de gérer/espionner une machine à distance, rootkit qui modifie l'OS pour ne pas être repéré. Une fonctionnalité intéressante que certains malwares possèdent est le concept de "polymorphisme" qui permet au maliciel de se modifier après chaque infection pour ne pas être repéré.

QUESTION 2.3

Terminé

Noté sur 1,00

Tenter de trouver des fonctionnalités non données en cours, faire travailler son imagination !

Il peut avoir une fonctionnalité de rançon "Ransomware", ce genre de malware a pour but de chiffrer les données de la victime, le seul moyen pour la victime de récupérer l'accès à ces données est que l'attaquant donne la clé de chiffrement pour pouvoir déchiffrer les données, et c'est en contrepartie d'argent, d'une rançon, souvent demandé en bitcoin

DESCRIPTION

Analyse du Malware « Live Messenger »

DESCRIPTION

Scène 1 : analyse de l'exécutable

QUESTION 5.1

Terminé

Noté sur 1,00

Illustrer et expliquer les manipulations effectuées.

(La majorité des images ne passent pas à l'envoi, nous avons donc créé un gist afin de passer les images par lien. Voici l'url si vous voulez vous assurer qu'il n'y ait pas de révision entre temps. <https://gist.github.com/Mondotosz/78b7048b578c8b3eb194d29d5b58c831>)

`md5sum $pathToFile` calcule l'empreinte md5 du fichier

`sha256sum $pathToFile` calcule l'empreinte sha256 du fichier

Les empreintes md5 et sha256 ne correspondent pas à ce que l'on attend.

QUESTION 5.2

Terminé

Noté sur 1,00

Que peut-on déduire du fait que les empreintes ne correspondent pas ?

Il ne s'agit pas du fichier auquel on s'attend. Soit il s'agit d'un fichier totalement différent soit il est corrompu. Dans les deux cas, on ne peut pas faire confiance au fichier.

QUESTION 5.3

Terminé

Noté sur 1,00

À votre avis, pourquoi est-il utile de vérifier l'intégrité d'un programme téléchargé ?

Afin de confirmer l'intégrité du fichier. On s'assure que le fichier que l'on reçoit est bien celui que l'on veut.

DESCRIPTION

Scène 2 : analyse par snapshots

QUESTION 5.4

Terminé

Noté sur 1,00

À quoi sert l'outil « Regshot » ?

A faire des snapshots de l'état du système de fichiers / registres Windows et à observer les changements.

QUESTION 5.5

Terminé

Noté sur 1,00

Pourquoi utiliser un environnement de « test » cloisonné ?

Pourquoi utilise-t-on le « snapshot » dans les logiciels de virtualisation (Virtualbox, VMware, . . .) ?

L'environnement de test est répliquable et peut facilement être recrée. Cela permet de :

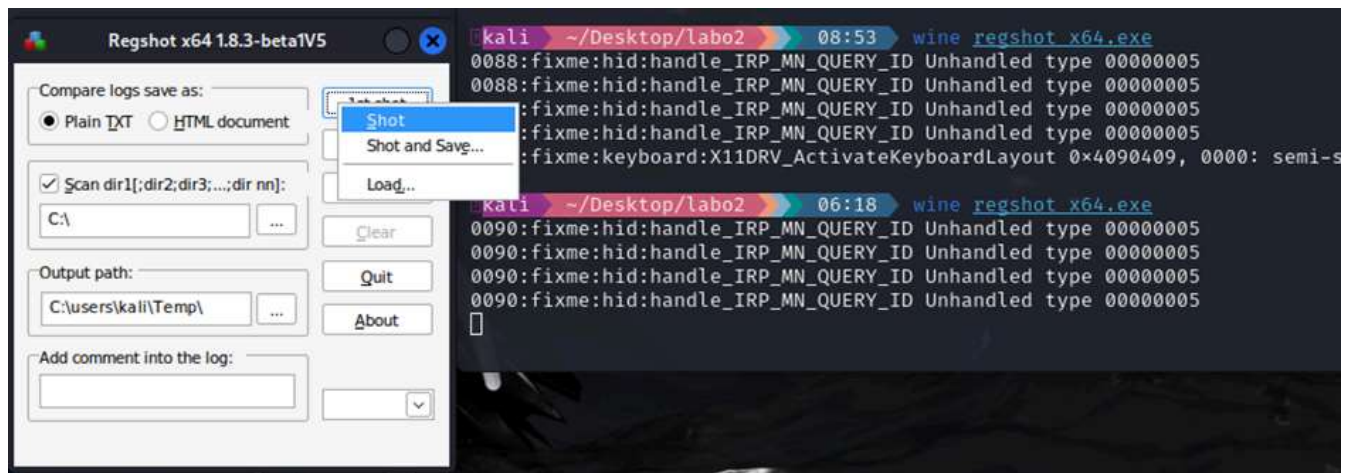
- Réduire les chances de compromettre notre système (l'os que l'on utilise réellement)
- Facilite l'observation des changements car l'état initial est connu et tout changement provient des logiciels que l'on exécute
- Si le système est détruit à un point de non-retour on peut facilement retourner à l'état initial (malwares destructeurs ou simples erreurs de manipulation)
- On va souvent essayer plusieurs approches différentes pour analyser un malware, avoir une snapshot nous permet de facilement partir dans différentes directions sans devoir setup l'environnement à nouveau.

QUESTION 5.6

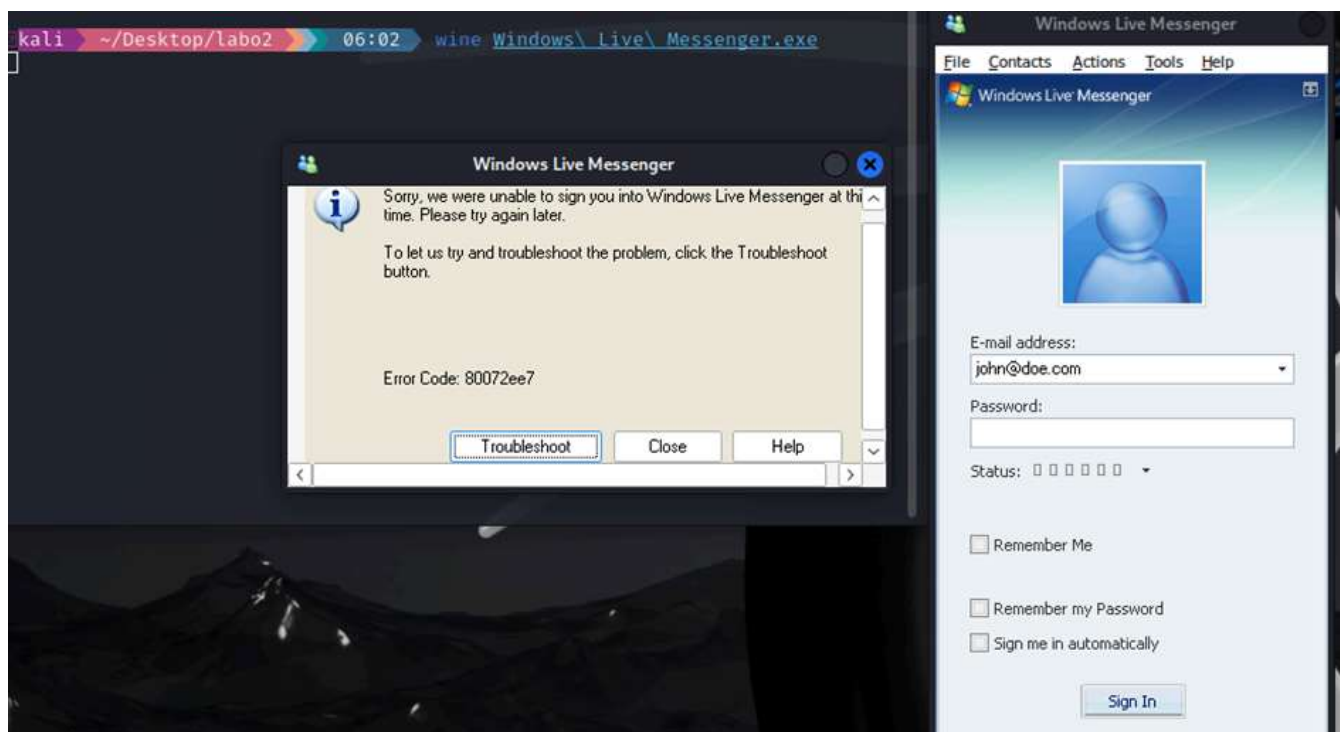
Terminé

Noté sur 1,00

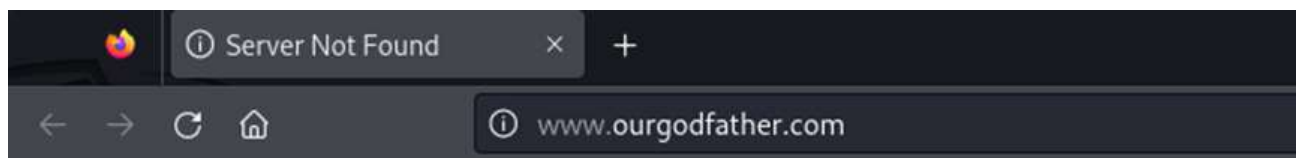
Illustrer et expliquer les manipulations effectuées.



On lance regshot et on fait une snapshot de la partition montée en C:\



On lance le malware et on essaie différents logins qui nous affichent des messages d'erreur de connexion.



Lorsque l'on ferme la fenêtre Windows Live Messenger, le logiciel essaie de nous faire aller sur la page web ci-dessus.

```
~res-x64.txt - Notepad
File Edit Search View Help
Regshot x64 1.8.3-beta1V5
Comments:
Datetime:2024/3/16 10:00:22 , 2024/3/16 10:02:53
Computer:KALI , KALI
Username: ,

Keys added:1
HKU\S-1-5-21-0-0-1000\Software\Wine\Temporary System Parameters\Control Panel\Sound

Files added:2
C:\windows\msnsettings.dat
C:\pas.txt

Total changes:3
```

On lance la deuxième snapshot et lorsque l'on clique sur compare pour voir ce qui a été modifié.

QUESTION 5.7

Terminé

Noté sur 1,00

Que constatez-vous dans le rapport généré par Regshot ?

Une clé de registre et deux fichiers ont été ajoutés. En l'occurrence, la clé de registre ne fait probablement pas partie du comportement du malware et est ajoutée par Wine directement pour des questions d'audio (potentiellement lors de l'affichage du message d'erreur ?) On peut utiliser wine regedit pour explorer les clés de registre et en l'occurrence, celle-ci ne contient rien.

QUESTION 5.8

Terminé

Noté sur 1,00

Que contiennent les fichiers créés par le maliciel ?

Indice : Pour rappel, le dossier C : \ se trouve à l'emplacement "/home/<username>/wine/drive_c"

```
kali ~/.wine/drive_c 06:29 cat pas.txt
www.ourgodfather.com
Username: john@doe.com
Password: somePassword
www.ourgodfather.com

kali ~/.wine/drive_c 06:29 cat windows/msnsettings.dat
hello
0
0
-1
-1
0
0
-1
Please type in an error message
C:\Program Files\MSN Messenger\msnmsgr.exe
0

0
0
0
C:/
```

Le fichier pas.txt contient la dernière adresse mail utilisée et son mot de passe associé.

```
kali ~/.wine/drive_c 06:33 strings windows/msnsettings.dat
hello
Please type in an error message
C:\Program Files\MSN Messenger\msnmsgr.exe
```

Le fichier msnsettings.dat n'est pas trop clair pour l'instant. Il contient 2 path, dont un vers l'exécutable pour MSN Messenger, ainsi que « hello ». Le reste des données est 0 et -1, ce qui correspond potentiellement aux valeurs de retour de l'appel de différents programmes. (Par bonne pratique, un programme est sensé retourner un code de résultat et 0 implique un bon résultat alors que -1 est un code fréquemment utilisé pour indiquer une erreur.)

DESCRIPTION

Scène 3 : analyse comportementale

QUESTION 5.9

Terminé

Noté sur 1,00

À quoi sert « strace » ?

Strace permet de suivre tous les appels système réalisés par un programme.

QUESTION 5.10

Terminé

Noté sur 1,00

Illustrer et expliquer les manipulations effectuées.

trace -e trace=%file wine Windows\ Live\ Messenger.exe 1>data.txt 2>&1

```
~/ISI/ISI_1_0002_Virus/ISI24_labo2_malware_kali_files 23s 15:55:16
< grep -i "pas.txt" output_file
statx(AT_FDCWD, "/home/kali/.wine/dosdevices/c:/pas.txt", AT_STATX_SYNC_AS_STAT|AT_NO_AUTOMOUNT, STATX_BASIC_STATS, {stx_mask=STATX_BASIC_STATS|S
TATX_MNT_ID, stx_attributes=0, stx_mode=S_IFREG|0644, stx_size=84, ...}) = 0
statx(AT_FDCWD, "/home/kali/.wine/dosdevices/c:/pas.txt", AT_STATX_SYNC_AS_STAT|AT_NO_AUTOMOUNT, STATX_BASIC_STATS, {stx_mask=STATX_BASIC_STATS|S
TATX_MNT_ID, stx_attributes=0, stx_mode=S_IFREG|0644, stx_size=84, ...}) = 0

~/ISI/ISI_1_0002_Virus/ISI24_labo2_malware_kali_files 15:55:38
> grep -i "pas.txt" output_file > strace_notes.txt

~/ISI/ISI_1_0002_Virus/ISI24_labo2_malware_kali_files 15:55:41
> grep -i "msnsettings.dat" output_file
statx(AT_FDCWD, "msnsettings.dat", AT_STATX_SYNC_AS_STAT|AT_NO_AUTOMOUNT, STATX_BASIC_STATS, {stx_mask=STATX_BASIC_STATS|STATX_MNT_ID, stx_attri
butes=0, stx_mode=S_IFREG|0644, stx_size=129, ...}) = 0
statx(AT_FDCWD, "msnsettings.dat", AT_STATX_SYNC_AS_STAT|AT_SYMLINK_NOFOLLOW|AT_NO_AUTOMOUNT, STATX_BASIC_STATS, {stx_mask=STATX_BASIC_STATS|STA
X_MNT_ID, stx_attributes=0, stx_mode=S_IFREG|0644, stx_size=129, ...}) = 0
getxattr("msnsettings.dat", "user.DOSATTRIB", 0x22f794, 64) = -1 ENODATA (No data available)
statx(AT_FDCWD, "/home/kali/.wine/dosdevices/c:/windows/msnsettings.dat", AT_STATX_SYNC_AS_STAT|AT_NO_AUTOMOUNT, STATX_BASIC_STATS, {stx_mask=STA
TX_BASIC_STATS|STATX_MNT_ID, stx_attributes=0, stx_mode=S_IFREG|0644, stx_size=129, ...}) = 0
```

Cette commande affiche tous les appels système liés aux fichiers (écriture, lecture, fermeture, etc ...). Etant donné que l'on savait que 2 fichiers étaient créés, il suffisait de chercher leur nom dans le fichier data.txt à l'aide de la commande grep.

Noté sur 1,00

Quel type de filtre a été utile et efficace pour réaliser la capture ?

Le filtre concernant les appels système open et write nous ont permis de rendre le fichier plus clair.

```
strace -e trace=open,write -y wine Windows\ Live\ Messenger.exe 1>data.txt 2>&1
```

Ou bien, ouvrir le fichier créé par la commande à la question 5.10 et chercher les mots “write” ou “read” qui concernent les fichiers créés/utilisés par le malware.

[illegible]

Noté sur 1,00

Dans l'output de strace, qu'est-il possible de visualiser pour ce cas ? Expliquer en détail.

Indice : Regarder la taille des fichiers

Dans le fichier généré par strace, il est possible d'analyser le contenu écrit et lu depuis des fichiers, les arguments ainsi que le code de retour de chaque appel système. Dans la capture d'écran précédente, on voit que la chaîne "www.ourgodfather.com..." est écrite dans le fichier dont le "file descriptor" est 14. En l'occurrence, le fichier pass.txt qui se trouve dans ~/wine/drive_c.

DESCRIPTION

Scène 4 : étude du fichier de configuration

QUESTION 5.13

Terminé

Noté sur 1,00

Tenter de comprendre comment le maliciel traite le fichier « msnsettings.dat ».

Le malware utilise le fichier msnsettings.dat comme un fichier de configuration.

QUESTION 5.14

Terminé

Noté sur 1,00

Quels types d'informations le fichier comprend-il ?

Ce fichier contient le nom de domaine du serveur SMTP et le destinataire. Il s'agit d'informations que l'hacker utilise pour exfiltrer les données volées, en l'occurrence, les identifiants de la victime.

QUESTION 5.15

Terminé

Noté sur 1,00

Quelles conclusions en tirez-vous ? Pouvez-vous affirmer ces conclusions ?

Nous pouvons affirmer que ce fichier est utilisé en tant de fichier de configuration. En analysant les appels système, on remarque qu'il est ouvert en mode lecture. Puis, si nous le lançons et que nous mettons en place un environnement "fake" et qu'on analyse le trafic réseau, on voit des requêtes SMTP envoyées à un serveur de messagerie.

DESCRIPTION

Scène 5 : analyse des communications réseau

QUESTION 5.16

Terminé

Noté sur 1,00

Comment fonctionne « fakedns » ?

“fakdns” permet « d’enfermer » le malware. Le but est de simuler un vrai serveur DNS qui résoudra les requêtes du malware. Le but sera ensuite d’analyser les requêtes que le malware transmet. Pour cela, il écoute sur le port 53 et répond avec l’adresse désirée pour toutes les demandes de résolution qu’il reçoit.

QUESTION 5.17

Terminé

Noté sur 1,00

Illustrer et expliquer les manipulations effectuées.

Changement du serveur DNS (qui pointe vers le serveur local).

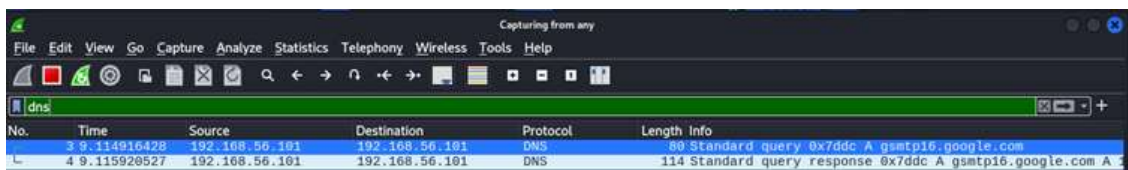
```
kali@kali: ~/Documents/ISI_l_0002_Virus/ISI24_lab02_malware_kali_files
~/Documents/ISI_l_0002_Virus/ISI24_lab02_malware_kali_files
> cat /etc/resolv.conf
# Generated by NetworkManager
###nameserver 127.0.0.1
nameserver 192.168.56.101

~/Documents/ISI_l_0002_Virus/ISI24_lab02_malware_kali_files
> |
```

Lancement du service fakedns

```
kali@kali: ~/Documents/ISI_l_0002_Virus/ISI24_lab02_malware_kali_files
~/Documents/ISI_l_0002_Virus/ISI24_lab02_malware_kali_files
> python fakedns.py 192.168.56.101
Started DNS server.
push.services.mozilla.com
push.services.mozilla.com
push.services.mozilla.com
push.services.mozilla.com
push.services.mozilla.com
push.services.mozilla.com
push.services.mozilla.com
```

Capture de la requête DNS réalisée par le malware.



The image shows a Wireshark packet capture window with the filter 'dns'. Two packets are visible in the list:

No.	Time	Source	Destination	Protocol	Length	Info
3	9.114916428	192.168.56.101	192.168.56.101	DNS	80	Standard query 0x7ddc A gsmtip6.google.com
4	9.115928527	192.168.56.101	192.168.56.101	DNS	114	Standard query response 0x7ddc A gsmtip6.google.com A

QUESTION 5.18

Terminé

Noté sur 1,00

Quels types d'informations ont été capturées grâce à Wireshark ?

Plusieurs types, notamment DNS, où il va essayer de transmettre plusieurs informations en faisant des requêtes à notre serveur DNS. Des requêtes SMTP pour pouvoir transmettre par mail les informations de connexions que nous avons entrées pour utiliser Windows Live Messenger

QUESTION 5.19

Terminé

Noté sur 1,00

Expliquer de manière détaillée le comportement du maliciel.

Après avoir entré la donnée nécessaire pour utiliser le Windows Live Messenger, le malware va directement tenter de se connecter à un serveur SMTP pour pouvoir ensuite envoyer par mail les données que nous avons entré précédemment.

DESCRIPTION

Scène 6 : simulation de services Web

QUESTION 5.20

Terminé

Noté sur 1,00

Illustrer et expliquer les manipulations effectuées.

```
kali ~ 09:02 sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 27255) ===
Session ID: 27255
Listening on: 127.0.0.1
Real Date/Time: 2024-03-22 09:02:25
Fake Date/Time: 2024-03-22 09:02:25 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 27267)
* smtp_25_tcp - started (PID 27268)
* dns_53_tcp_udp - started (PID 27265)
deprecated method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
can't setup TCP socket: Address already in use at /usr/share/perl5/Net/DNS/Nameserver.pm line 417.
can't setup UDP socket: Address already in use at /usr/share/perl5/Net/DNS/Nameserver.pm line 467.
* pop3s_995_tcp - started (PID 27271)
* ident_113_tcp - started (PID 27278)
* http_80_tcp - started (PID 27266)
* syslog_514_udp - started (PID 27279)
* irc_6667_tcp - started (PID 27275)
* finger_79_tcp - started (PID 27277)
* ntp_123_udp - started (PID 27276)
* time_37_tcp - started (PID 27282)
* daytime_13_udp - started (PID 27285)
* echo_7_tcp - started (PID 27286)
* tftp_69_udp - started (PID 27274)
* pop3_110_tcp - started (PID 27270)
* ftp_21_tcp - started (PID 27272)
* chargen_19_udp - started (PID 27293)
* chargen_19_tcp - started (PID 27292)
* dummy_1_udp - started (PID 27295)
* quotd_17_tcp - started (PID 27290)
* echo_7_udp - started (PID 27287)
* dummy_1_tcp - started (PID 27294)
* time_37_udp - started (PID 27283)
* discard_9_tcp - started (PID 27288)
* daytime_13_tcp - started (PID 27284)
* discard_9_udp - started (PID 27289)
* smtps_465_tcp - started (PID 27269)
* ftps_990_tcp - started (PID 27273)
* quotd_17_udp - started (PID 27291)
done.
Simulation running.
```

Lancement de inetsim pour simuler les différents services web potentiellement utilisés par le malware (serveur SMTP dans notre cas)

No.	smtp	Source	Destination	Protocol	Length	Info
10	13.636279231	127.0.0.1	127.0.0.1	SMTP	116	S: 220 mail.inetisn.org Inetisn Mail Service ready.
12	13.655067845	127.0.0.1	127.0.0.1	SMTP	77	C: EML0 kali
14	13.659084580	127.0.0.1	127.0.0.1	SMTP	88	S: 250-mail.inetisn.org
16	13.701265655	127.0.0.1	127.0.0.1	SMTP	239	S: 250-SIZE 162400000 8BITMIME DSN AUTH PLAIN LOGIN ANONYMOUS CRAM-MD5 CRAM-SHA1 HELP STARTTLS VRFY ENHANCEDSTATUSCODES ETRN
18	13.703076183	127.0.0.1	127.0.0.1	SMTP	72	C: RSET
19	13.706630839	127.0.0.1	127.0.0.1	SMTP	80	S: 250 2.0.0 OK
20	13.706632323	127.0.0.1	127.0.0.1	SMTP	105	C: MAIL FROM:<yourpassword@password.com>
21	13.706363910	127.0.0.1	127.0.0.1	SMTP	80	S: 250 2.1.0 OK
22	13.708723961	127.0.0.1	127.0.0.1	SMTP	97	C: RCPT TO:<isi_lab16@gmail.com>
23	13.710764495	127.0.0.1	127.0.0.1	SMTP	80	S: 250 2.1.5 OK
24	13.711836576	127.0.0.1	127.0.0.1	SMTP	72	C: DATA
25	13.712894951	127.0.0.1	127.0.0.1	SMTP	103	S: 354 End data with <CR><LF>.<CR><LF>
26	13.713279332	127.0.0.1	127.0.0.1	SMTP	95	C: DATA fragment, 33 bytes
27	13.735304045	127.0.0.1	127.0.0.1	SMTP	170	from: yourpassword@password.com, subject: Username: kali@linux.com, Password: password ..
30	13.750819307	127.0.0.1	127.0.0.1	SMTP	100	S: 250 2.6.0 OK: queued as 5F57D4E6
31	13.760703616	127.0.0.1	127.0.0.1	SMTP	72	C: QUIT
32	13.761773320	127.0.0.1	127.0.0.1	SMTP	97	S: 221 2.0.0 closing connection.

<ul style="list-style-type: none"> Frame 28: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface lo, id 0 Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00) Internet Protocol Version 4, Seq: 127.0.0.1, Dst: 127.0.0.1 Transmission Control Protocol, Src Port: 41697, Dst Port: 25, Seq: 127, Ack: 325, Len: 164 Simple Mail Transfer Protocol Internet Message Format <ul style="list-style-type: none"> From: yourpassword@password.com, 1 item Subject: Username: kali@linux.com To: isi_lab16@gmail.com, 1 item Date: Fri, 22 Mar 2024 09:02:59 -0400 Unknown-Extension: X-Priority: 3 (Contact Wireshark developers if you want this supported.) Unknown-Extension: X-Library: Indy 9.00.10 (Contact Wireshark developers if you want this supported.) Message-Text password: password 	<pre> 0000 46 72 6f 64 3a 20 79 6f 75 72 70 61 73 73 77 6f From: yo urpasswo 0010 72 64 40 70 61 73 77 6f 72 64 2e 63 6f 6d 6d rdpassword.com 0020 0a 53 70 62 4a 65 63 74 3a 20 55 7a 65 72 6e 61 -Subject: Userna 0030 66 65 3a 20 66 61 6c 69 40 6c 69 6e 75 78 2e 53 me: kali@linux.c 0040 6f 6d 6d 6a 54 6f 3a 20 69 73 69 5f 6c 61 62 31 on-To: isi_lab1 0050 36 40 67 6d 61 69 6c 2e 63 6f 6d 6a 44 61 74 69 gmail.com> Dst 0060 65 3a 20 46 72 69 2c 20 32 32 20 61 72 20 32 61 Fri, 22 Mar 2 0070 30 32 34 20 30 39 3a 20 32 3a 35 30 20 2d 30 34 624 09:0 2:59 -04 0080 30 20 0d 6a 56 20 69 72 69 6f 72 69 74 79 3a 20 00-X-Pri ority: 0090 33 6d 6a 56 2d 4c 69 62 72 61 72 79 3a 26 4b 6a 3-X-Lib rary: In 00a0 64 79 20 39 2e 30 30 2e 31 30 6d 6a 6d 6a 59 61 dy 9:00.10---P 00b0 73 72 77 6f 72 64 3a 20 79 61 73 73 77 6f 72 64 assword: password 00c0 66 6a </pre>
---	--

Capture des paquets pendant que l'on essaie de se connecter avec le mail « kali@linux.com » et mot de passe « password »

On observe que le malware envoie un mail depuis l'adresse « yourpassword@password.com » à « isi_lab16@gmail.com » contenant l'adresse email entrée comme sujet et le mot de passe comme contenu du mail

QUESTION 5.21

Terminé

Noté sur 1,00

Après toutes ces analyses comportementales, pouvez-vous identifier à quel(s) type(s) de maliciels « Windows Live Messenger » appartient ? Pourquoi ?

Il s'agit d'un Trojan car le malware se fait passer pour Windows Live Messenger qui est une vraie application. Il en émule le fonctionnement (en tout cas le login). De ce que l'on n'a pu observer, le malware ne met aucun service en place et ne tente pas de se propager. Il attend juste que l'utilisateur l'utilise en pensant qu'il s'agisse d'une application légitime et il n'exfiltre des informations qu'au moment où l'utilisateur tente de se connecter.

DESCRIPTION

Scène 7 : analyse statique

QUESTION 5.22

Terminé

Noté sur 1,00

Que pouvez-vous en déduire ?

On peut voir que le malware a plusieurs modes de fonctionnement et paramètres possibles. Dans tous les cas, la configuration est sauvée dans le fichier msnsettings.dat et n'est donc pas « portable ». On peut imaginer que ce menu est présent pour déboguer lors du développement ou alors pour installer et configurer le trojan manuellement.

DESCRIPTION

Analyse à l'aide d'outils en ligne

QUESTION 5.23

Terminé

Noté sur 1,00

À quelle(s) catégorie(s) de codes malveillants appartient ce code malveillant ? (virus, ver, spyware, etc.)

Il s'agit d'un Trojan

QUESTION 5.24

Terminé

Noté sur 1,00

Quelle est l'utilité d'un tel code malveillant ?

De se faire passer pour un logiciel légitime.

QUESTION 5.25

Terminé

Noté sur 1,00

Comment se propage ce code malveillant ?

Il n'est pas autonome, il faut que l'utilisateur le télécharge et l'exécute. Généralement, on va trouver ce genre de malwares sur des sites de téléchargements ou sur les réseaux sociaux.

QUESTION 5.26

Terminé

Noté sur 1,00

Comment l'infection par ce code malveillant est-elle réalisée ?

L'utilisateur doit exécuter le malware.

Aller à...