



efrei

PARIS PANTHÉON-ASSAS UNIVERSITÉ

Architecture Sécurisé

Par David TEJEDA, Vincent LAGOGUE, Tom THIOULOUSE,
Thomas PEUGNET, Alexis PLESSIAS

Table des matières

| | |
|---|----|
| 1. Répartition des Rôles | 3 |
| 2. Choix du Malware..... | 3 |
| Recherche d'un malware dans les bases proposées : | 3 |
| Critères de sélection : | 3 |
| 3. Analyse Statique..... | 3 |
| Outils proposés (choisir au moins 2) : | 5 |
| Étapes principales : | 5 |
| Résultats observés : | 5 |
| 4. Analyse Dynamique | 11 |
| Configurer un environnement isolé : | 11 |
| Outils recommandés : | 11 |
| Étapes principales : | 11 |
| Comportements observés (exemples concrets, logs). | 11 |
| Conclusion | 12 |
| Résumé des découvertes..... | 12 |
| Apports de l'analyse | 13 |

1. Répartition des Rôles

- Recherche du malware et documentation : Alexis Plessias et Tom Thioulouse
- Analyse statique : Vincent Lagogué
- Analyse dynamique : David Tejeda
- Rédaction du rapport : Thomas Peugnet

2. Choix du Malware

Recherche d'un malware dans les bases proposées :

- [TheZoo](#)
- [Ikarus Security](#)
- [Subreddit Malware Resources](#)

Critères de sélection :

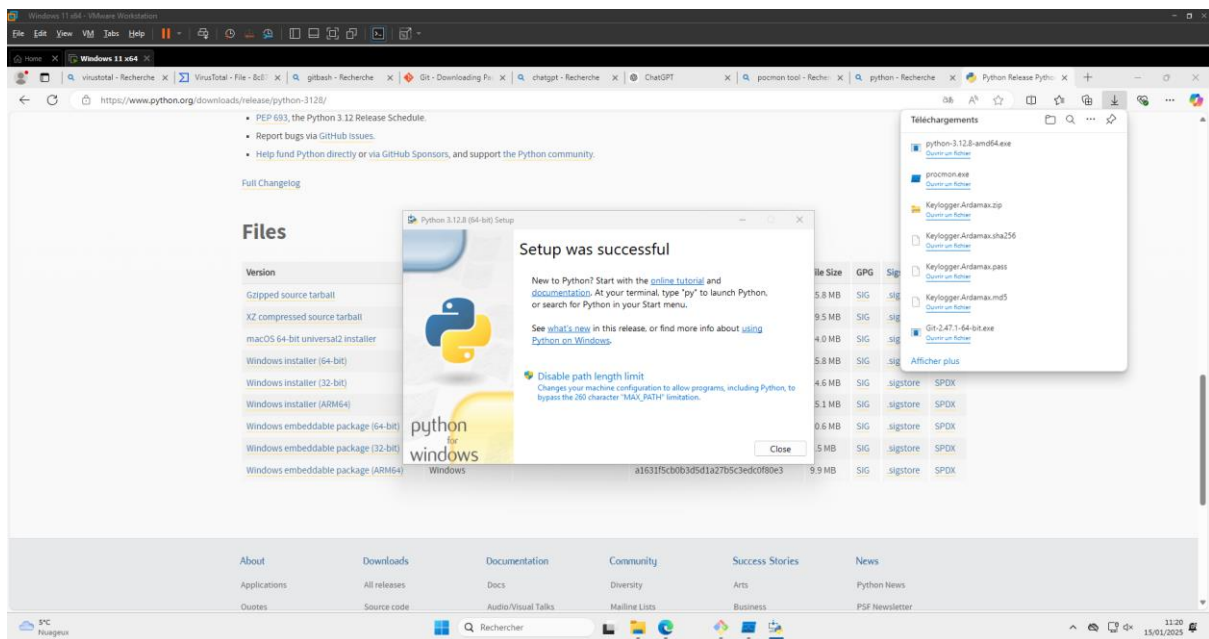
Nous avons sélectionné le keylogger **Ardamax** pour les raisons suivantes :

- Compatibilité avec l'environnement d'analyse, en l'occurrence, Windows.
- Complexité adaptée à notre niveau, comme nous avons-nous même réalisé un keylogger, nous pourrons par la même occasion comparer les différences.
- Limitation des risques de propagation vers la machine physique.
- Variété du type de données récupérées. Dans le cas présent, du texte, des photos de la webcam, le presse-papier et bien d'autres choses.

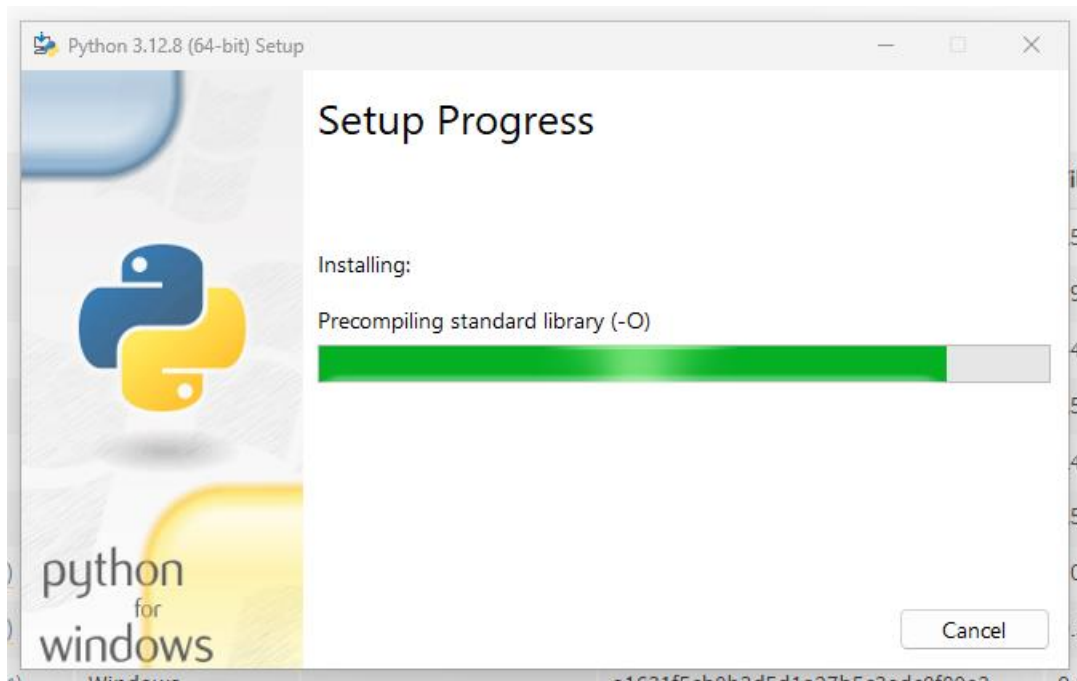
3. Analyse Statique

Création de la VM

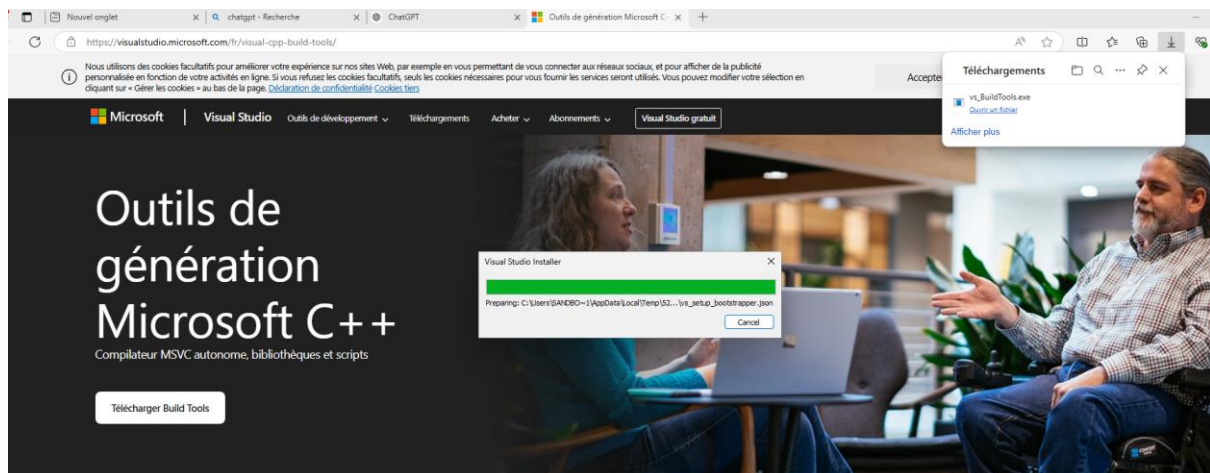
Nous avons commencé par créer une machine virtuelle dans VMWare :



Installation de Python dans la VM :



Installation des outils de génération C++ :



Outils proposés (choisir au moins 2) :

Nous avons choisi deux outils pour réaliser l'analyse statique :

- **VirusTotal** est une plateforme en ligne permettant d'obtenir une analyse immédiate et exhaustive d'un fichier malveillant à l'aide de nombreux moteurs antivirus et outils d'analyse comportementale.
- **IDA Free** est un décompilateur et désassembleur permettant de transformer un fichier binaire en code assembleur ou pseudo-code lisible. Il est particulièrement adapté pour analyser un malware comme Keylogger.Ardamax en profondeur.

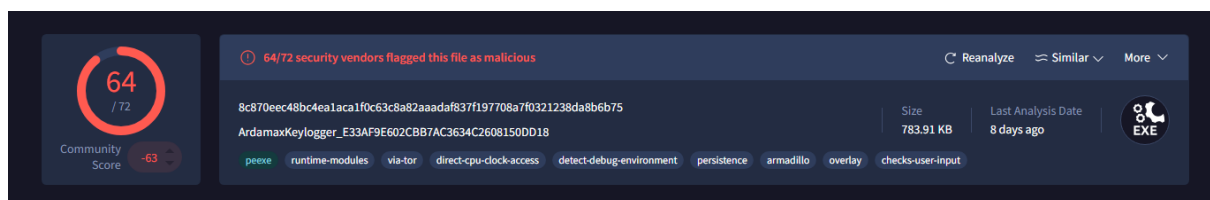
Étapes principales :

1. Examiner les métadonnées du fichier.
2. Identifier les bibliothèques et API utilisées.
3. Repérer des patterns malveillants (par exemple, des connexions réseau ou des mécanismes d'obfuscation).

Virus Total

Résultats observés :

Nous avons obtenu une détection par 64 sur 72 vendeurs dans VirusTotal.



Le méchant logiciel est un cheval de Troie et plus précisément un enregistreur de frappe.

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY24 +

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ⓘ trojan.ardamax/keylogger

Threat categoriestrojan spyware

Family labelsardamax keylogger tsy

Security vendors' analysis ⓘ

Do you want to automate checks?

| | | | |
|--------------------|-------------------------------------|-------------|---|
| AhnLab-V3 | ⓘ Trojan/Win.Ardamax.R424106 | Alibaba | ⓘ Malware:Win32/km_24a2a.None |
| AliCloud | ⓘ Trojan:Win/Keylogger | ALYac | ⓘ Trojan.Keylogger.ArdamaxKey |
| Antiy-AVL | ⓘ Trojan[KeyLogger]/Win32.Ardamax | Arcabit | ⓘ Application.Keylogger.Ardamax.Gen |
| Avast | ⓘ Win32:Ardamax-LV [Spy] | AVG | ⓘ Win32:Ardamax-LV [Spy] |
| Avira (no cloud) | ⓘ TR/Spy.Ardamax.ckp | BitDefender | ⓘ Dropped:Application.Keylogger.Ardama... |
| Bkav Pro | ⓘ W32.AIDetectMalware | ClamAV | ⓘ Win.Packed.Ardamax-6965118-0 |
| CrowdStrike Falcon | ⓘ Win/malicious_confidence_100% (W) | CTX | ⓘ Exe.trojan.ardamax |
| Cylance | ⓘ Unsafe | Cynet | ⓘ Malicious (score: 99) |

Page details

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY

24 +

Join our Community

 and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties

MD5

e33af9e602cbb7ac3634c2608150dd18

SHA-1

8f6ec9bc137822bc1dd439c35fedc3b847ce3fe

SHA-256

8c870eec48bc4ea1aca1f0c63c8a82aaadsf837f197708a7f0321238da8b6b75

Vhash

085046655d151bfz18lz1fz

Authentihash

bd0ef20d5ab6f6ab56355b666d16639d8770b54c003d046799d19491aca168e5

Imphash

86632da30434ccfc050190a47fb559c4

SSDEEP

12288:0E9uQIDT8c/wtocu3HhGSrllDhIPnRq/iITUOvqF8dtbcZl36VBqWPH:FuqD2cYWzBGZohIE/zUD8/bgl2qW/

TLSH

T13D05234816605922FC292B770F0CDA946DAF47A8304D4F1F76622B491E5BB49FF337A8

File type

Win32 EXE

executable

windows

win32

pe

peexe

Magic

PE32 executable (GUI) Intel 80386, for MS Windows

TrID

Win32 Executable (generic) (52.9%) | Generic Win/DOS Executable (23.5%) | DOS Executable Generic (23.5%)

DetectItEasy

PE32 | Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] | Compiler: Microsoft Visual C/C++ (15.00.30729) [C] | Linker: Microsoft Linker (9.00.30729) | Tool: ...

Magika

PEBIN

File size

783.91 KB (802724 bytes)

PEID packer

Microsoft Visual C++

History

Creation Time

2009-03-04 14:29:05 UTC

First Seen In The Wild

2013-06-06 16:22:30 UTC

First Submission

2013-05-31 20:41:36 UTC

Last Submission

2025-01-12 17:13:55 UTC

Last Analysis

2025-01-07 09:24:34 UTC

Nous pouvons observer que ce méchantgiciel a une multitude de noms.

Names

ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18

Muestra4

Muestra4.exe

Week 14.exe

keylogger

suspicious

ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe

Ardamax.exe

Keylogger.exe

8c870eec48bc4ea1aca1f0c63c8a82aada837f197708a7f0321238da8b6b75.exe

Il cible les machines fonctionnant avec des processeurs Intel.

Portable Executable Info

Header

Target Machine

Intel 386 or later processors and compatible processors

Compilation Timestamp

2009-03-04 14:29:05 UTC

Entry Point

13038

Contained Sections

4

Sections

| Name | Virtual Address | Virtual Size | Raw Size | Entropy | MD5 | Chi2 |
|--------|-----------------|--------------|----------|---------|----------------------------------|----------|
| .text | 4096 | 9378 | 9728 | 6.4 | 4ef1264582652a9ec4aad81a3a3a3cab | 59562.13 |
| .rdata | 16384 | 1974 | 2048 | 4.65 | f9d1f664a99225db6972201e8538ffb7 | 64990.25 |
| .data | 20480 | 5216 | 1024 | 2.83 | 10cae41a2555972be498787b5dcf2939 | 115509 |
| .rsrc | 28672 | 928 | 1024 | 3.09 | 52c107d08e7e82d2753ec15d9a73ecde | 79584 |

Imports

+ MSVCRT.dll

+ KERNEL32.dll

+ USER32.dll

Contained Resources By Type

| | |
|---------------|---|
| RT_GROUP_ICON | 1 |
| RT_ICON | 1 |

Contained Resources By Language

| | |
|---------|---|
| NEUTRAL | 2 |
|---------|---|

Relations

DETECTIONDETAILSRELATIONSASSOCIATIONSBEHAVIORCOMMUNITY24+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted URLs4

| Scanned | Detections | Status | URL |
|------------|------------|--------|--|
| 2024-12-31 | 0 / 96 | 200 | http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt |
| 2024-12-31 | 0 / 96 | 200 | http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt |
| 2024-12-31 | 0 / 96 | 200 | http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c |
| 2024-12-31 | 0 / 96 | 200 | http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt |

Contacted Domains13

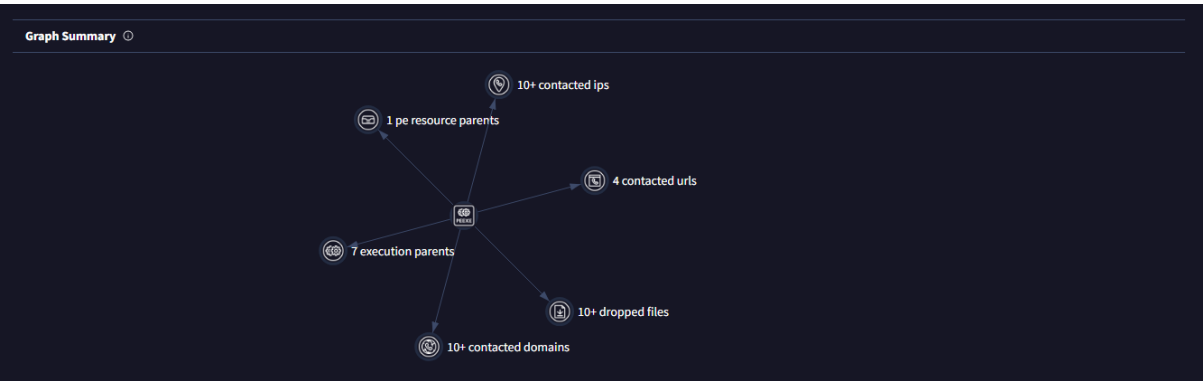
| Domain | Detections | Created | Registrar |
|---|------------|------------|-----------------------------|
| crt.sectigo.com | 0 / 94 | 2018-08-16 | CSC CORPORATE DOMAINS, INC. |
| fp2e7a.wpc.2be4.phicdn.net | 0 / 94 | 2014-11-14 | GoDaddy.com, LLC |
| fp2e7a.wpc.phicdn.net | 0 / 94 | 2014-11-14 | GoDaddy.com, LLC |
| microsoft.com | 0 / 94 | 1991-05-02 | MarkMonitor Inc. |
| query.prod.cms.rt.microsoft.com | 0 / 94 | 1991-05-02 | MarkMonitor Inc. |
| res.public.onecdn.static.microsoft | 0 / 94 | 2023-05-05 | MarkMonitor Inc. |
| sectigo.com | 0 / 94 | 2018-08-16 | CSC CORPORATE DOMAINS, INC. |
| smtp-yahoo.mail-prod1.omega.vip.ir2.yahoo.com | 0 / 94 | 1995-01-18 | MarkMonitor Inc. |
| smtp.mail.global.gm0.yahoodns.net | 0 / 94 | 2009-01-20 | MarkMonitor Inc. |
| smtp.mail.yahoo.com | 0 / 94 | 1995-01-18 | MarkMonitor Inc. |

| Contacted IP addresses (40) | | | |
|-----------------------------|------------|-------------------|---------|
| IP | Detections | Autonomous System | Country |
| 104.18.38.233 | 0 / 94 | 13335 | - |
| 104.71.214.69 | 0 / 94 | 16625 | US |
| 152.195.19.97 | 0 / 94 | 15133 | US |
| 184.25.191.235 | 0 / 94 | 16625 | US |
| 192.168.0.1 | 0 / 94 | - | - |
| 192.168.0.26 | 0 / 94 | - | - |
| 192.168.0.36 | 0 / 94 | - | - |
| 192.168.0.54 | 0 / 94 | - | - |
| 192.229.211.108 | 0 / 94 | 15133 | US |
| 192.229.221.95 | 2 / 94 | 15133 | US |
| ... | | | |

| Execution Parents (7) | | | |
|-----------------------|------------|-----------|--|
| Scanned | Detections | Type | Name |
| 2024-07-18 | 46 / 73 | Win32 EXE | mtk.exe |
| 2024-08-28 | 42 / 75 | Win32 EXE | mtk.exe |
| 2024-07-19 | 31 / 59 | ZIP | NEAS.542ace4d7932e2a9f7c0f27cf0b13cb7f50546c2256d4eca213ed337b4f544fezip.zip |
| 2024-12-07 | 48 / 72 | Win32 EXE | mtk.exe |
| 2024-04-30 | 40 / 68 | ZIP | NEAS.c619e92d516921b48efdddfc63bc752b1f920ebd005a0335a5e8bba56c8b7d16zip.zip |
| 2020-11-23 | 34 / 71 | Win32 EXE | CryptedFile.exe |
| 2020-08-14 | 59 / 68 | Win32 EXE | Urbina.exe |

| PE Resource Parents (1) | | | |
|-------------------------|------------|-----------|------------|
| Scanned | Detections | Type | Name |
| 2020-08-14 | 59 / 68 | Win32 EXE | Urbina.exe |

| Dropped Files (28) | | | |
|--------------------|------------|-----------|--|
| Scanned | Detections | File type | Name |
| ? | ? | file | 0a4ab4cf9a5fcc5c2c1837588203b4ab2f2c2386e1364d05a2ecc83e24bc42a |
| 2024-12-05 | 58 / 72 | Win32 EXE | DPBJ.exe |
| ? | ? | file | 15b543536c7b3a2c87e97e7d3edddd1e8dec151a3aec08d86568a8d9613e666 |
| ? | ? | file | 1bfae4260cfe42e1b74b56038b7fb0ea3dba01cf9bf9de190b954e3f28c68610 |
| ? | ? | file | 23149f4b9c00552f4ce86a6ce4912b25457a957e59933d14017fbc33cf5347ab |
| ? | ? | file | 2951de054de976b61023921aa018c925cad833d361b2d625a44199d6992ef700 |
| ? | ? | file | 29acbf9380cbcf455705b96a727ed1486bdad97a20cd9b8f0e7cfab70f08ad14 |
| 2024-12-05 | 54 / 72 | Win32 EXE | AKV.exe |
| 2024-04-28 | 51 / 70 | Win32 DLL | DPBJ.007 |
| ? | ? | file | 41fb5e040b0d53312114c03d50528b15886682c0410c45a113ef82a51ff263c5 |
| ... | | | |



Associations

DETECTION
DETAILS
RELATIONS
ASSOCIATIONS
BEHAVIOR
COMMUNITY
24+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Threats

Filters
Clear All

| Threats - 4 Known Threats | Activity |
|---|-------------------------------------|
| ArdaMax Malware Updated 5 hours ago bA collection of files, url's, ip's and domains related to the malware ArdaMax/b blf you want to request for something to b... IoCs 2.2 K | By JaffaCakes... (Crowdsourced) |
| ArdaMax Updated 1 day ago According to f-secure, Ardamax is a commercial keylogger program that can be installed onto the system from the product... IoCs 1.7 K | By CarlosCabal (Partner) |
| malware_sha256_7days Updated 1 year ago malwaresha2567days IoCs 1.4 K | By AlvdX (Crowdsourced) |

HexEd.it

Le format MZ, également connu sous le nom de format DOS executable, est un format de fichier exécutable utilisé par le système d'exploitation MS-DOS et les premières versions de Microsoft Windows.

| File Information | | -Untitled- x ArdakamKeylogger_E... x | |
|--------------------------------|--------------------------------|--------------------------------------|---|
| File Name | ArdakamKeylogger_E33AF9E602... | 00000000 | 00000000 |
| File Size | 802,724 bytes (784 KiB) | 00000010 | 40 5A 45 00 01 00 00 00 04 00 00 00 FF FF 00 00 |
| Data Inspector (Little-endian) | | 00000020 | 00 3A 00 00 00 00 00 00 2A 00 56 62 04 3C 00 00 |
| | | 00000030 | 91 00 00 00 A1 40 1C 30 00 00 00 C0 00 00 00 00 |
| | | 00000040 | 08 08 4C CD 21 00 00 00 05 F8 FF 62 C1 99 91 31 |
| | | 00000050 | C1 99 91 31 C1 99 91 31 E6 5A 01 C5 99 91 31 |
| Type | Unsigned (+) Signed (t) | 00000060 | C1 99 90 31 E8 99 91 31 29 86 95 C1 C2 99 91 31 |
| 8-bit Integer | 77 77 | 00000070 | 42 85 9F 31 C8 99 91 31 29 86 9A C1 C8 99 91 31 |
| 16-bit Integer | 23177 23117 | 00000080 | 29 86 9B 31 CA 99 91 31 C8 E1 15 31 CA 99 91 31 |
| 24-bit Integer | 4545101 4545101 | 00000090 | C8 E1 12 31 C9 99 91 31 DF C8 65 C1 C8 99 91 31 |
| 32-bit Integer | 4545101 4545101 | 000000A0 | C8 E1 00 31 C8 99 91 31 52 09 63 68 C1 99 91 31 |
| 64-bit Integer (+) | 4299512397 | 000000B0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| 64-bit Integer (t) | 4299512397 | 000000C0 | 58 45 00 00 4C 01 84 00 31 90 AE 49 00 00 00 00 |
| 16-bit Float: P | 201.625 | 000000D0 | 00 00 00 00 E8 00 63 01 00 01 00 00 26 00 00 |
| 32-bit Float: P | 6.3690431e-39 | 000000E0 | 00 22 00 00 00 00 00 00 EF 32 00 00 00 00 00 |
| 64-bit Float: P | 2.124241369226251e-314 | 000000F0 | 00 48 00 00 00 00 00 00 00 18 00 00 00 00 00 |
| LEB128 (+) | 77 | 00000100 | 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 |
| LEB128 (t) | -51 | 00000110 | 00 80 00 00 00 04 00 00 00 00 00 00 00 00 00 |
| Rational (+) | 4545101 | 00000120 | 00 00 10 00 00 10 00 00 00 00 10 00 00 00 00 |
| Rational (t) | 4545101 | 00000130 | 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 |
| Strational (t) | 4545101 | 00000140 | 4C 44 00 00 50 00 00 00 00 70 00 00 A0 03 00 00 |
| MS-DOS Date/Time | 1980-02-05 11:18:25 Local | 00000150 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| UNIX 2.0 Date/Time | 1979-12-30 00:00:00.000 UTC | 00000160 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| OLEX 32-bit Date/Time | 1890-02-22 14:31:41 UTC | 00000170 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| Macintosh HFS Date/Time | 1904-02-22 14:41:02 Local | 00000180 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| Macintosh HFS+ Date/Time | 1904-02-22 14:41:02 Local | 00000190 | 00 00 00 00 00 00 00 00 00 40 00 00 AC 00 00 00 |
| Macintosh HFS+ Date/Time | 1904-02-22 14:41:02 Local | 000001A0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| Macintosh HFS+ Date/Time | 1904-02-22 14:41:02 Local | 000001B0 | 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 |
| Macintosh HFS+ Date/Time | 1904-02-22 14:41:02 Local | 000001C0 | A2 24 00 00 00 10 00 00 00 26 00 00 00 04 00 00 |

PE Studio

Analyse des strings

Voici notre analyse des strings du méchantgiciel :

WriteFile : Écriture de données dans un fichier (indique potentiellement une tentative de journalisation des frappes ou des informations capturées).

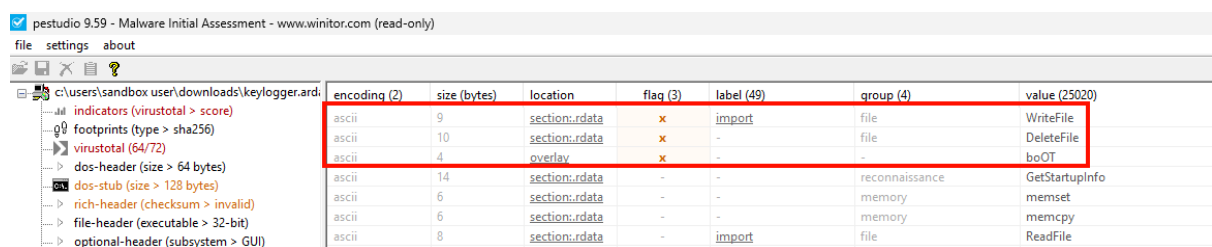
DeleteFile : Suppression de fichiers, ce qui peut suggérer que le malware nettoie ses traces après avoir exécuté certaines tâches.

GetStartupInfo : Récupération d'informations sur le processus (indique un comportement de reconnaissance, potentiellement pour déterminer le contexte d'exécution).

Les appels à WriteFile et DeleteFile sont caractéristiques de logiciels malveillants qui collectent et manipulent des données locales avant de les exfiltrer ou de supprimer les traces.

La combinaison d'appels comme ReadFile et GetStartupInfo laisse fortement supposer que le méchant logiciel effectue des activités de collecte d'informations.

Ces informations permettent de comprendre les capacités principales du malware : il est capable de lire, écrire et supprimer des fichiers, un comportement typique des keyloggers ou logiciels espions. De plus, il effectue une reconnaissance de l'environnement local, une pratique courante pour adapter son comportement à la machine cible. Les chaînes identifiées peuvent également être utilisées comme indicateurs de compromission (IoCs) dans une recherche de menaces.

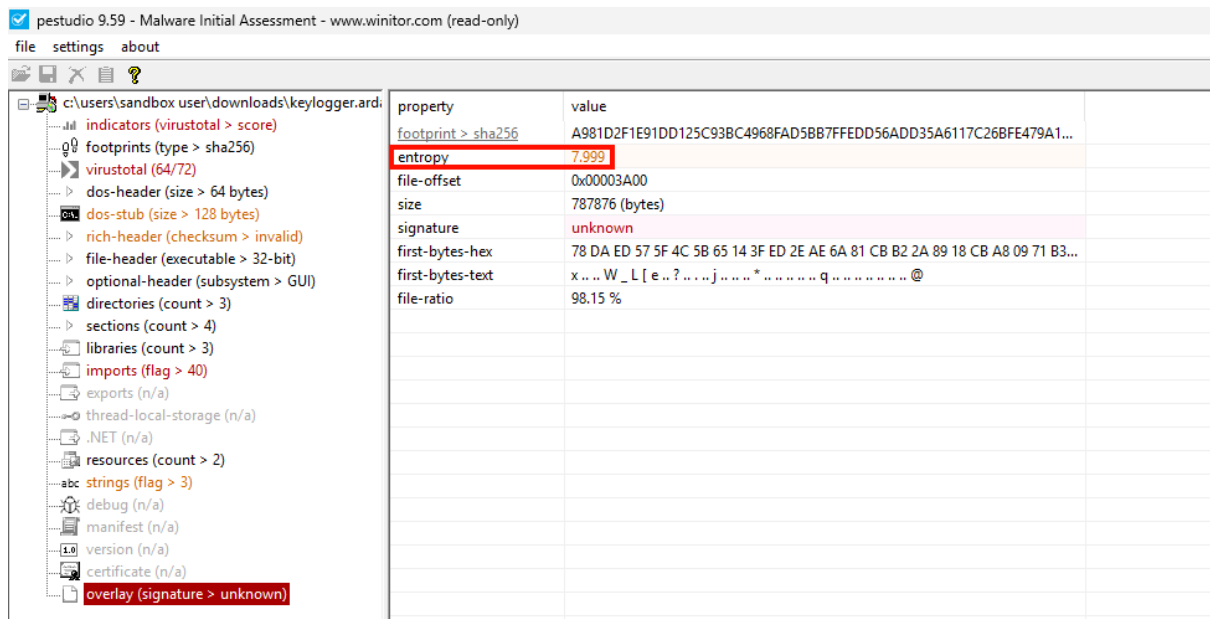


| encoding (2) | size (bytes) | location | flag (3) | label (49) | group (4) | value (25020) |
|--------------|--------------|----------------|----------|------------|----------------|----------------|
| ascii | 9 | section: rdata | x | import | file | WriteFile |
| ascii | 10 | section: rdata | x | - | file | DeleteFile |
| ascii | 4 | overlay | x | - | - | boOT |
| ascii | 14 | section: rdata | - | - | reconnaissance | GetStartupInfo |
| ascii | 6 | section: rdata | - | - | memory | memset |
| ascii | 6 | section: rdata | - | - | memory | memcpy |
| ascii | 8 | section: rdata | - | import | file | ReadFile |

Overlay

Une entropie élevée (proche de 8) indique que le fichier est probablement compressé ou chiffré. Cela indique que le malware peut être packé pour dissimuler son contenu et éviter l'analyse.

La section "overlay" correspond à des données supplémentaires situées en dehors des sections normales d'un fichier exécutable PE (Portable Executable). Lorsqu'une signature est inconnue, cela peut indiquer la présence de données cachées ou malveillantes, telles qu'une configuration ou un payload secondaire, souvent utilisées par les malwares pour exécuter des actions nuisibles. Cela peut également révéler une tentative d'obfuscation visant à contourner les outils de détection et à masquer les véritables intentions du fichier.



4. Analyse Dynamique

Configurer un environnement isolé :

- Machine virtuelle (VM) avec VirtualBox.

On installe une machine virtuelle sous Windows 10 ainsi que plusieurs outils de monitoring (Process Explorer, regShot, SpyShelter)

- Utiliser un environnement spécialisé comme FLARE VM ou REMnux.
- On vérifie que l'environnement est totalement isolé (pas de connexion réseau active ou via un réseau virtuel contrôlé).

Outils:

- Process Monitor (ProcMon) : suivi des processus et des interactions.
- Wireshark : analyse du trafic réseau.
- Regshot : capture des modifications du registre.

Étapes principales :

- Lancer le malware dans l'environnement isolé.
- Observer les comportements : processus créés, fichiers modifiés, connexions établies.
- Documenter chaque observation (captures d'écran, logs).

Comportements observés

On remarque que le programme lance plusieurs processus via notre outil

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|--|--------|---------------|-------------|------|----------------------------------|----------------------------|
| Registry | | 6 536 K | 74 812 K | 116 | | |
| System Idle Process | 100.00 | 60 K | 8 K | 0 | | |
| System | < 0.01 | 196 K | 144 K | 4 | | |
| Interrupts | 0.71 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 1 080 K | 1 260 K | 388 | | |
| Memory Compression | | 68 K | 12 K | 1892 | | |
| csrss.exe | | 1 772 K | 5 584 K | 492 | | |
| wininit.exe | | 1 364 K | 7 200 K | 600 | | |
| services.exe | | 4 680 K | 10 012 K | 740 | | |
| lsass.exe | < 0.01 | 6 712 K | 19 632 K | 756 | Local Security Authority Proc... | Microsoft Corporation |
| fontdrvhost.exe | | 1 500 K | 4 156 K | 900 | | |
| csrss.exe | 1.78 | 1 920 K | 5 652 K | 608 | | |
| winlogon.exe | | 3 636 K | 11 700 K | 668 | | |
| fontdrvhost.exe | | 3 632 K | 8 460 K | 908 | | |
| dwm.exe | 0.71 | 108 684 K | 152 656 K | 1096 | | |
| explorer.exe | < 0.01 | 43 700 K | 147 988 K | 4780 | Explorateur Windows | Microsoft Corporation |
| cmd.exe | | 3 272 K | 4 824 K | 4856 | Interpréteur de commandes ... | Microsoft Corporation |
| conhost.exe | | 7 468 K | 21 204 K | 1324 | Hôte de la fenêtre de la cons... | Microsoft Corporation |
| SecurityHealthSystray.exe | | 1 928 K | 9 552 K | 1240 | Windows Security notificatio... | Microsoft Corporation |
| VBxTray.exe | < 0.01 | 2 420 K | 10 828 K | 7228 | VirtualBox Guest Additions Tr... | Oracle Corporation |
| b4064449279669d4cfbc4dd0c5272405b61ab8d3bb7a7a457dcc6afc5394b39d.exe | < 0.01 | 1 332 K | 8 024 K | 6140 | Adobe Download Manager | Adobe Systems Incorporated |
| 1.exe | < 0.01 | 24 088 K | 37 596 K | 5140 | Phull | |
| firefox.exe | | 224 164 K | 319 700 K | 2520 | Firefox | Mozilla Corporation |
| PPI.exe | 4.63 | 9 112 K | 21 832 K | 5804 | | |

Sur la partie réseau on ne détecte rien concernant notre programme.

Keys added: 4

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\7436

HKU\S-1-5-21-712455944-2136033329-2312432185-1002\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplcationViewManagement\W32:00000000000306A6

HKU\S-1-5-21-712455944-2136033329-2312432185-1002\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\21\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

HKU\S-1-5-21-712455944-2136033329-2312432185-1002_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\21\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

Pour la partie registre, comme indiqué au-dessus on a de nouvelles clés qui sont ajoutés au registre. De même, Ardamax ajoute 31 valeurs dans le registre principalement dans le HKU et HKLM. Enfin, il y a 23 valeurs modifiées dans le registre.

Conclusion

Résumé des découvertes

1. Analyse Statique : Compréhension des Capacités et Structure du Malware

L'analyse statique du Keylogger Ardamax a permis d'identifier ses capacités et son comportement. Les chaînes extraites, comme WriteFile, DeleteFile, et GetStartupInfo, indiquent des fonctionnalités caractéristiques des keyloggers ou logiciels espions. Ces fonctions permettent au malware de lire, écrire et supprimer

des fichiers, de collecter des informations sensibles et d'effacer ses traces. La combinaison de ces appels API indique également une reconnaissance de l'environnement local pour adapter le fonctionnement du malware à la machine cible.

L'examen des métadonnées a révélé que le fichier possède une entropie élevée (7.99), indiquant qu'il est probablement compressé ou chiffré, ce qui est une technique commune pour masquer son contenu et rendre l'analyse plus difficile. De plus, la présence d'une section "overlay" avec une signature inconnue peut contenir des données supplémentaires, comme un payload secondaire ou des configurations, et témoigne de tentatives d'obfuscation pour éviter la détection.

2. Analyse Dynamique : Observation des Comportements en Environnement Isolé

L'exécution du malware dans un environnement isolé a permis de mettre en évidence plusieurs comportements malveillants. Le programme a initié la création de plusieurs processus tout en effectuant des modifications dans le registre. Par exemple, il a ajouté 4 nouvelles clés dans des emplacements sensibles du registre, tels que :

HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting

HKU\S-1-5-21-...\Explorer\SessionInfo

En tout, 31 nouvelles valeurs ont été ajoutées et 23 valeurs modifiées, principalement dans les branches HKU et HKLM du registre. Ces modifications permettent de constater la persistance du malware, une technique souvent utilisée pour garantir son exécution continue après le redémarrage de la machine infectée.

Sur la partie réseau, aucune communication n'a été détectée pendant l'exécution, probablement en raison de l'environnement contrôlé ou d'un mécanisme de lazy loading du malware.

3. Apports de l'analyse

Cette analyse a permis d'identifier des indicateurs de compromission (IoCs), comme par exemple des chaînes caractéristiques, des comportements au niveau des processus et des modifications dans le registre.