EKANS (SNAKE) RANSOMWARE

Table des matières

EKANS (SNAKE) RANSOMWARE

Avertissement *: L'auteur du document ne peut en aucun cas être tenu responsable de la pertinence, de l'exactitude, de l'intégrité ou de la qualité du document. La responsabilité de l'auteur de ce document ne peut être engagée en cas de dommages matériels ou intellectuels résultant de l'utilisation ou de la non-utilisation des informations contenues dans ce document, d'informations erronées ou incomplètes, dans la mesure où il ne peut pas être établi qu'il s'agit d'un acte délibéré ou d'une négligence de la part de l'auteur.*

Toutes les informations contenues dans ce document sont libres et sans engagement. L'auteur de ce document se réserve expressément le droit de modifier, de compléter ou de supprimer tout ou partie du contenu du document sans préavis ainsi que d'en suspendre la publication à titre temporaire ou définitif.

Introduction

Ce document traite du ransomware EKANS (Snake) découvert par Malware Hunter Team en décembre 2019.

Le rapport réalisé et publié par Dragos le 3 Février 2020 reflète bien la situation actuelle, avec une émergence des menaces sur le secteur industriel, souvent laissé de côté par les attaquants. De nombreuses analyses ont ensuite été publiées par des médias plus traditionnels. Cependant aucune victimologie n'a été rendu public. L'architecture assez simpliste du ransomware a été relevée plusieurs fois. Certaines des analyses montrent un lien avec le ransomware MegaCortex, cependant ce raccourci a été contesté à plusieurs reprises.

Analyse statique

Le fichier analysé

Virustotal :

Type de hash	Hash
MD5	3d1cc4ef33bad0e39c757fce317ef82a
SHA-1	f34e4b7080aa2ee5cfee2dac38ec0c306203b4ac
SHA-256	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60
Vhash	0360475d5d141az1dtz2017z
Authentihash	4f2d723ab4502e05853066268c53dee6b2eebaefde2978002ab18a1df31cf012
Imphash	96c44fa1eee2c4e9b9e77d7bf42d59e6
SSDEEP	49152:QAdGB73ejP3+EMfRdASVaAvrC5Xh602+:QAgR3epMjASHch
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
File size	3.55 MB (3718656 bytes)

Langage : Golang

Première soumission à Virustotal :

2019-12-26 09:21:29

Détail de l'exécutable :

Nom	Adresse virtuel	Taille virtuel	Taille brut	Entropie	MD5
.text	4096	3626760	3627008	5.76	e2fb2d843f5fff39c8f7a5285456e7bb
.data	3633152	173704	89088	5.48	3392592e512a8b3eca9c020bcda01fa6
.idata	3809280	882	1024	4.31	1d0ced8b2d7ad9f05b7c986fb63c6026
.symtab	3813376	4	512	0.02	07b5472d347d42780469fb2654b7fc54

EKANS (SNAKE) RANSOMWARE

Les chaînes de caractères

Les chaînes de caractères du malware ont pu être décodées avec un script python[1]. En effet le créateur du malware a encodé une partie des chaînes de caractères avec un XOR.

Dans les chaînes de caractères (intégralité en annexe), on retrouve la clé publique qui sert à chiffrer les données, le message de rançon ainsi la liste des processus qui, s'ils existent seront arrêtés (détails dans la partie sur les Spécificité industrielles).

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAyQ+M5ve829umuy9+BSsUX/krgdF83L3m8/uxRvKX5EZbSh1+buON
ZYr5MjfhrdiOGnrbB1j0Fy31U/uzvWcy7VvK/zcsO/5aAhujhHB/qMAVpZ8zT5BB
ujT1Bvsith/BXgtM99MixD8oZ67VDZaRM9TPE89WuAjnaBZORrk48wFcn1DOAAHD
Z9z9komtqIH1fm3Y0Q6P76nUscLsYOme082L217Th/lTMoqqs4cF2rn9O9Vp4V9U
aCs4XVxGSpcuqbIscfpf0cm44P2eOEk+sbZdahO9C6fezt7YF4OCJ4Vz3qqMD6z4
+6d7FRxUu6k3Te2T2bWBZnsDO30pYFi/gwIDAQAB
-----END RSA PUBLIC KEY-----
```

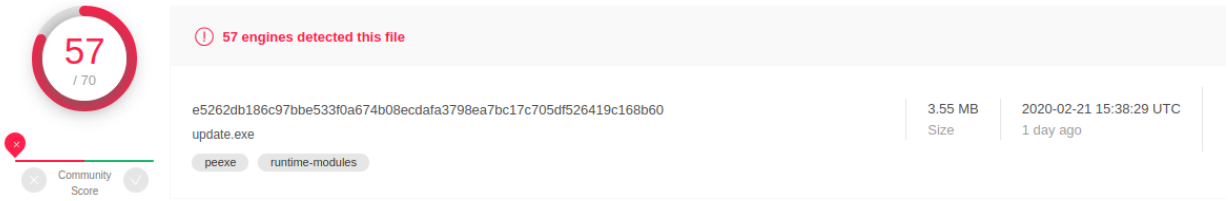
Figure 2: clé RSA publique qui est utilisée pour chiffrer les données

```
windir
SystemDrive
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery
\AppData\
```

Figure 1: Chemin de dossiers

Les antivirus

L'analyse a été réalisée via l'outil en ligne virustotal :



Ad-Aware	Gen:Win32.AV-Killer.ItW@aei5Gqj	AhnLab-V3	Trojan/Win32.FileCoder.C3866073
Alibaba	Trojan:Win32/Antavmu.2b943168	ALYac	Trojan.Ransom.Filecoder
Antiy-AVL	Trojan/Win32.Antavmu	SecureAge APEX	Malicious
Arcabit	Gen:Win32.AV-Killer.E64FB6	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Antavmu.tygqh
BitDefender	Gen:Win32.AV-Killer.ItW@aei5Gqj	BitDefenderTheta	Gen:NN.ZexaF.34090.ItW@aei5Gqj
Bkav	W32.AIDetectVM.malware	CAT-QuickHeal	Worm.vinf
ClamAV	Win.Ransomware.Snake-7546377-0	Comodo	Malware@#3hlbu4qfgaf2f
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/Trojan.AQQM-5188	DrWeb	Trojan.Encoder.30786

[1] Github

Emsisoft	Gen:Win32.AV-Killer.ItW@aei5Gqj (B)	Endgame	Malicious (high Confidence)
eScan	Gen:Win32.AV-Killer.ItW@aei5Gqj	ESET-NOD32	A Variant Of Win32/Filecoder.Snake.A
F-Prot	W32/Ransom.AEY	F-Secure	Trojan.TR/Antavmu.tygqh
FireEye	Gen:Win32.AV-Killer.ItW@aei5Gqj	Fortinet	W32/Filecoder.SNAKE.A!tr.ransom
GData	Gen:Win32.AV-Killer.ItW@aei5Gqj	Ikarus	Trojan-Ransom.Snake
Jiangmin	Trojan.Antavmu.eyp	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Trojan.Win32.Antavmu.asdd
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.74756041.susgen
McAfee	Trojan-Ransom.b	McAfee-GW-Edition	BehavesLike.Win32.Downloader.wm
Microsoft	Ransom:Win32/Killpror!MSR	NANO-Antivirus	Trojan.Win32.Encoder.gvakaa
Palo Alto Networks	Generic.ml	Panda	Trj/CI.A
Qihoo-360	Win32/Trojan.07f	Sangfor Engine Zero	Malware
Sophos AV	Troj/Ransom-FUJ	Sophos ML	Heuristic
Symantec	Downloader	Tencent	Win32.Trojan.Antavmu.Lkee
TrendMicro	Ransom.Win32.EKANS.A	TrendMicro-HouseCall	Ransom.Win32.EKANS.A
VBA32	Trojan.AntiAV	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.S.SnakeRansom.3718656	Webroot	W32.Ransom.Snake
Yandex	Trojan.Antavmu!IkuqQwJ5NMA	Zillya	Trojan.AntiAV.Win32.11788
ZoneAlarm by Check Point	Trojan.Win32.Antavmu.asdd	Dr.Web vxCube	MALWARE
Lastline	MALWARE	NSFOCUS POMA	MALWARE
Acronis	Undetected	Avast-Mobile	Undetected
Baidu	Undetected	CMC	Undetected
Cybereason	Undetected	eGambit	Undetected
Kingsoft	Undetected	Rising	Undetected
SentinelOne (Static ML)	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	Trapmine	Undetected
Zoner	Undetected	Symantec Mobile Insight	Unable to process file type

Les règles Yara

Les règles Yara déclenchées sont les suivantes :

```
  - Crypto
Big_Numbers0 EKANS.exe
Big_Numbers1 EKANS.exe
Big_Numbers3 EKANS.exe
MD5_Constants EKANS.exe
RIPEMD160_Constants EKANS.exe
SHA1_Constants EKANS.exe
SHA512_Constants EKANS.exe
SHA2_BLAKE2_IVs EKANS.exe
RijnDael_AES EKANS.exe
RijnDael_AES_CHAR EKANS.exe
RijnDael_AES_LONG EKANS.exe
BASE64_table EKANS.exe
  - CVE rules
  - Maldocs
  - WebShells
  - Malware
  - Anti debug AntiVM
DebuggerException__SetConsoleCtrl EKANS.exe
SEH__vectored EKANS.exe
  - Email
  - Packers
IsPE32 EKANS.exe
IsConsole EKANS.exe
```

Figure 3 : Règles YARA déclenchées par le fichier

Analyse dynamique

Comportement

Au lancement du ransomware, une fenêtre du cmd.exe se lance. EKANS va commencer à supprimer les « Shadow Volumes ». Ensuite il va « kill » les 64 processus[2] et va parcourir les dossiers dans l'ordre alphabétique (anglais) pour en chiffrer le contenu. Comme vu précédemment, certains chemins de dossier sont spécifiés en claire dans le code, selon l'étude de Bleeping Computer les dossiers listés ci-dessous sont ignorés :

- windir
- SystemDrive
- :\$Recycle.Bin
- :\ProgramData
- :\Users\All Users
- :\Program Files
- :\Local Settings
- :\Boot
- :\System Volume Information
- :\Recovery
- \AppData\

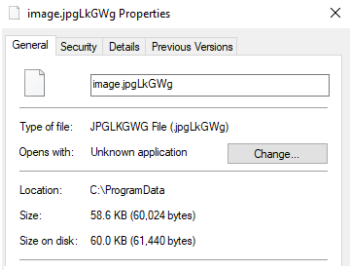


Figure 4: Image situé dans ProgramData chiffré par le ransomware

Cependant durant l'analyse, certains fichiers placés intentionnellement dans « ProgramData » ont bien été chiffrés. Les fichiers situés dans les dossiers enfants n'ont pas été impactés.

Figure 6: Lancement du PE malveillant

Figure 5: Figure 6: Le processus lancé par EKANS dans le gestionnaire des tâches

21:44:09,5688973	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla\Firefox\Profiles\pjqhhag3.default	NO MORE FILES
21:44:09,5689103	EKANS.exe	4396	CloseFile	C:\Users\root\AppData\Roaming\Mozilla\Firefox\Profiles\pjqhhag3.default	SUCCESS
21:44:09,5689300	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla\Firefox\Profiles	NO MORE FILES
21:44:09,5689396	EKANS.exe	4396	CloseFile	C:\Users\root\AppData\Roaming\Mozilla\Firefox\Profiles	SUCCESS
21:44:09,5689649	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla\Firefox	NO MORE FILES
21:44:09,5689743	EKANS.exe	4396	CloseFile	C:\Users\root\AppData\Roaming\Mozilla\Firefox	SUCCESS
21:44:09,5690788	EKANS.exe	4396	CreateFile	C:\Users\root\AppData\Roaming\Mozilla\SystemExtensionsDev	IS DIRECTORY
21:44:09,5691765	EKANS.exe	4396	CreateFile	C:\Users\root\AppData\Roaming\Mozilla\SystemExtensionsDev	SUCCESS
21:44:09,5692077	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla\SystemExtensionsDev*	SUCCESS
21:44:09,5692295	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla\SystemExtensionsDev	SUCCESS
21:44:09,5692444	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla\SystemExtensionsDev	NO MORE FILES
21:44:09,5692541	EKANS.exe	4396	CloseFile	C:\Users\root\AppData\Roaming\Mozilla\SystemExtensionsDev	SUCCESS
21:44:09,5692729	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming\Mozilla	NO MORE FILES
21:44:09,5692822	EKANS.exe	4396	CloseFile	C:\Users\root\AppData\Roaming\Mozilla	SUCCESS
21:44:09,5693012	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData\Roaming	NO MORE FILES
21:44:09,5693105	EKANS.exe	4396	CloseFile	C:\Users\root\AppData\Roaming	SUCCESS
21:44:09,5693287	EKANS.exe	4396	QueryDirectory	C:\Users\root\AppData	NO MORE FILES
21:44:09,5693381	EKANS.exe	4396	CloseFile	C:\Users\root\AppData	SUCCESS
21:44:09,5694728	EKANS.exe	4396	CreateFile	C:\Users\root\Contacts	IS DIRECTORY
21:44:09,5695698	EKANS.exe	4396	CreateFile	C:\Users\root\Contacts	SUCCESS

Figure 7: Parcours systématique des dossiers dans l'ordre alphabétique

[2] Cf Annexes

Chiffrement

Le ransomware est peu rapide, il met plusieurs minutes à chiffrer l'environnement des tests constitués de quelques fichiers de tests. Chaque fichier chiffré est renommé sous la forme : *{nom_original}.{extension_original}{5_cacarcéres_aléatoire}*

Figure 8: Exemple de fichiers chiffrés par EKANS

La clé publique qui a permis de chiffrer les fichiers[3] a été générée avec l'algorithme RSA au format X.509. Les fichiers chiffrés possèdent, à la fin, la chaîne de caractère « EKANS » qui permet d'identifier les fichiers déjà chiffrés :

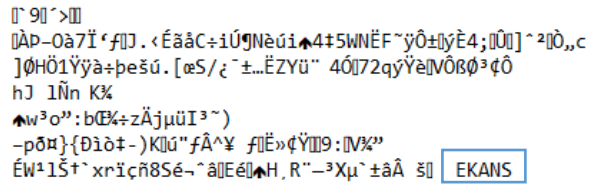


Figure 9: "Tag" placé en fin de fichier pour ne pas chiffrer deux fois le même fichier

Paiement

Selon l'analyse réalisée, un fichier nommé « Fix-Your-Files » est créé, plusieurs tentatives ont été nécessaires au malware avant de trouver un endroit où placer le fichier :

5664	CreateFile	C:\Users\Public\Desktop\Fix-Your-Files.txt	ACCESS DENIED
5664	CreateFile	C:\Users\Public\Desktop\Fix-Your-Files.txt	NAME NOT FOUND
5664	CreateFile	C:\Fix-Your-Files.txt	REPARSE
5664	CreateFile	C:\Users\root\AppData\Local\VirtualStore\Fix-Your-Files.txt	SUCCESS
5664	WriteFile	C:\Users\root\AppData\Local\VirtualStore\Fix-Your-Files.txt	SUCCESS
5664	CloseFile	C:\Users\root\AppData\Local\VirtualStore\Fix-Your-Files.txt	SUCCESS

Figure 10: Logs de l'outil ProcessMonitor

Le fichier spécifie l'adresse mail « bapcocrypt@ctemplar.com » pour contacter l'attaquant. Cet hébergeur situé en Islande garantit un anonymat total et un chiffrement avancé.

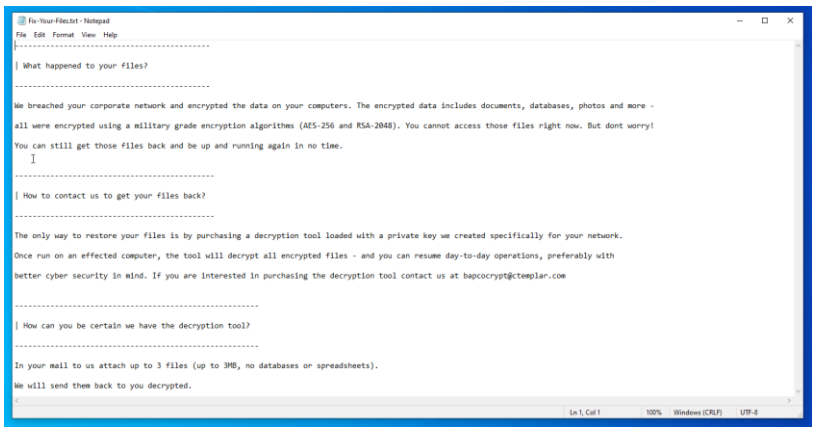


Figure 11: Contenu du fichier de rançon

[3] La clé est dans les chaînes de caractères présentes en Annexe

Spécificité industrielle

Le ransomware présente certaines spécificités concernant le milieu industriel, habituellement peu ciblé par les malwares. EKANS va tenter de couper 64 processus avant de commencer à chiffrer. Cette liste concerne des équipements SCADA, et autres outils utilisés dans le domaine industriel :

Nom du processus	Outil visé
ccflic0.exe	Processus appartenant au Proficy Licensing de GE Fanuc Automation
ccflic4.exe	Processus appartenant au Proficy Licensing de GE Fanuc Automation
healthservice.exe	Processus Windows
ilicensesvc.exe	Processus appartenant au iFIX® de GE Fanuc Automation
nimbus.exe	Processus appartenant à Broadcom
prlicensemgr.exe	Processus appartenant à Proficy Server License Manager in GE Intelligent
certificateprovider.exe	Ambigu
proficypublisherservice.exe	Proficy Related
proficysts.exe	Proficy Related
erlsrv.exe	Erlang
vmtoolsd.exe	VMWare Tools
managementagenthost.exe	VMWare
vgauthservice.exe	VMWare Guest Authentication Service
epmd.exe	RabbitMQ
hasplmv.exe	Sentinel LDK
spooler.exe	Ambigu
hdb.exe	Honeywell HMIWeb
ntservices.exe	360 Total Security
n.exe	Ambigu
monitoringhost.exe	Microsoft SCCM
win32sysinfo.exe	RabbitMQ
inet_gethost.exe	Ambigu
taskhostw.exe	Windows
proficy administrator.exe	Proficy Plant Application
ntevl.exe	Nimsoft
prproficymgr.exe	Proficy
prrds.exe	Proficy Remote Data Service de GE Intelligent Platforms
prrouter.exe	Proficy Related
prconfigmgr.exe	Proficy Related
prgateway.exe	Proficy Server Gateway
premailengine.exe	Proficy Related
pralarmmgr.exe	Proficy Related
prftpengine.exe	Proficy Related
prcalculationmgr.exe	Time Based Historian Data
prprintserver.exe	Proficy Related
prdatabasemgr.exe	Proficy Related
preventmgr.exe	Proficy Related
prreader.exe	Proficy Historian Data
prwriter.exe	Proficy Historian Data
prsummarymgr.exe	Proficy Related
prstubber.exe	Proficy Related
prschedulemgr.exe	Proficy Related
cdm.exe	Nimsoft
musnotificationux.exe	Microsoft update
npmdagent.exe	Microsoft Operations Management Suite
client64.exe	client64.exe
keysvc.exe	Ambigu
server_eventlog.exe	Ambigu
proficyserver.exe	Proficy
server_runtime.exe	Proficy Related
config_api_service.exe	Ambigu (Thingworx)
fnplicensingservice.exe	Activation Licensing Service de FLEXNet
workflowresttest.exe	Ambigu
proficyclient.exe	Proficy Client
vmacthlp.exe	VMware
msdtssrvr.exe	Microsoft SQL server
sqlservr.exe	Microsoft SQL server
msmdsrv.exe	Microsoft SQL Server
reportingservicesservice.exe	Microsoft SQL Server

dsmcsvc.exe	BM Tivoli Storage Manager
winvnc4.exe	WinVNC4
client.exe	Ambigu
collwrap.exe	BlueStripe Collector
bluestripecollector.exe	BlueStripe Collector

Annexes

IOCs

Le message de rançon	---------- | What happened to your files? ---------- We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more- all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry! You can still get those files back and be up and running again in no time. ---------- | How to contact us to get your files back? ---------- The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network. Once run on an effected computer, the tool will decrypt all encrypted files- and you can resume day-to-day operations, preferably with better cyber security in mind. If you are interested in purchasing the decryption tool contact us at %s ---------- | How can you be certain we have the decryption tool? ---------- In your mail to us attach up to 3 files (up to 3MB, no databases or spreadsheets). We will send them back to you decrypted.
Adresse email	bapcocrypt@ctemplar.com
Clé RSA utilisé pour le chiffrement	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAyQ+M5ve829umuy9+BSsUX/krgdF83L3m8/uxRvKX5EZbSh1+buON ZYr5MjfhrdiOGnrbB1j0Fy31U/uzvWcy7VvK/zcsO/5aAhujhHB/qMAVpZ8zT5BB ujT1Bvsith/BXgtM99MixD8oZ67VDZaRM9TPE89WuAjnaBZORrk48wFcn1DOAAHD Z9z9komtqIH1fm3Y0Q6P76nUscLsYOme082L217Th/lTMoqqs4cF2rn9O9Vp4V9U aCs4XVxGSpcuqbIscfpf0cm44P2eOEk+sbZdahO9C6fezt7YF4OCJ4Vz3qqMD6z4 +6d7FRxUu6k3Te2T2bWBZnsDO30pYFi/gwIDAQAB -----END RSA PUBLIC KEY-----

Les hash :

MD5	3d1cc4ef33bad0e39c757fce317ef82a
SHA-1	f34e4b7080aa2ee5cfee2dac38ec0c306203b4ac
SHA-256	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60

EKANS (SNAKE) RANSOMWARE

DLL

Name	Description	Company Name	Path
advapi32.dll	API avancées Windows 32	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcryptprimitives.dll	Windows Cryptographic Primitives Library	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
combase.dll	Microsoft COM pour Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	Bibliothèque de contrôles de l'expérience utilisateur	Microsoft Corporation	C:\Windows\WinSxS\x86_microsoft.windows.common-cont...
conhost.exe	Hôte de la fenêtre de la console	Microsoft Corporation	C:\Windows\System32\conhost.exe
Conhost.exe.mui	Hôte de la fenêtre de la console	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.LanguageExperie...
CoreMessaging.dll	Microsoft CoreMessaging Dll	Microsoft Corporation	C:\Windows\System32\CoreMessaging.dll
CoreUIComponents.dll	Microsoft Core UI Components Dll	Microsoft Corporation	C:\Windows\System32\CoreUIComponents.dll
cryptsp.dll	Cryptographic Service Provider API	Microsoft Corporation	C:\Windows\System32\cryptsp.dll
dwmapi.dll	API du Gestionnaire de fenêtres du Bureau Microsoft	Microsoft Corporation	C:\Windows\System32\dwmapi.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll
iertutil.dll	Utilitaire à l'exécution pour Internet Explorer	Microsoft Corporation	C:\Windows\System32\iertutil.dll
imm32.dll	Multi-User Windows IMM32 API Client DLL	Microsoft Corporation	C:\Windows\System32\imm32.dll
kernel.appcore.dll	AppModel API Host	Microsoft Corporation	C:\Windows\System32\kernel.appcore.dll
kernel32.dll	DLL du client API BASE Windows NT	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	DLL du client API BASE Windows NT	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
msctf.dll	DLL de MSCTF Server	Microsoft Corporation	C:\Windows\System32\msctf.dll
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcrt.dll
ntdll.dll	DLL Couche NT	Microsoft Corporation	C:\Windows\System32\ntdll.dll
ntmarta.dll	Fournisseur MARTA Windows NT	Microsoft Corporation	C:\Windows\System32\ntmarta.dll
oleaut32.dll	OLEAUT32.DLL	Microsoft Corporation	C:\Windows\System32\oleaut32.dll
powrprof.dll	DLL d'assistance du profil d'alimentation	Microsoft Corporation	C:\Windows\System32\powrprof.dll
profapi.dll	User Profile Basic API	Microsoft Corporation	C:\Windows\System32\profapi.dll
rpcrt4.dll	Runtime d'appel de procédure distante	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup APIs	Microsoft Corporation	C:\Windows\System32\sechost.dll
SHCore.dll	SHCORE	Microsoft Corporation	C:\Windows\System32\SHCore.dll
shell32.dll	DLL commune du shell Windows	Microsoft Corporation	C:\Windows\System32\shell32.dll
shlwapi.dll	Bibliothèque d'utilitaires légers du Shell	Microsoft Corporation	C:\Windows\System32\shlwapi.dll
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls
StaticCache.dat			C:\Windows\Fonts\StaticCache.dat
TextInputFramework.dll	"TextInputFramework.DYNLINK"	Microsoft Corporation	C:\Windows\System32\TextInputFramework.dll
ucrtbase.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\ucrtbase.dll
umpdc.dll			C:\Windows\System32\umpdc.dll
user32.dll	DLL client de l'API utilisateur de Windows multi-utilisateurs	Microsoft Corporation	C:\Windows\System32\user32.dll
user32.dll.mui	DLL client de l'API utilisateur de Windows multi-utilisateurs	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.LanguageExperie...
uxtheme.dll	Bibliothèque de thèmes Ux Microsoft	Microsoft Corporation	C:\Windows\System32\uxtheme.dll
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\System32\win32u.dll
windows.storage.dll	API de stockage Microsoft WinRT	Microsoft Corporation	C:\Windows\System32\windows.storage.dll
WinTypes.dll	DLL de types de base Windows	Microsoft Corporation	C:\Windows\System32\WinTypes.dll

Figure 12: DLL chargé par EKANS

Strings

```
EKANS
kernel32.dll
CreateMutexW
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
already encrypted!

worker %s started job %s

error encrypting %v : %v

There can be only one

-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAyQ+M5ve829umuy9+BSsUX/krgdF83L3m8/uxRvKX5EZbSh1+buON
ZYr5MjfhrdiOGnrbB1j0Fy31U/uzvWcy7VvK/zcsO/5aAhujhHB/qMAVpZ8zT5BB
ujT1Bvsith/BXgtM99MixD8oZ67VDZaRM9TPE89WuAjnaBZORrk48wFcn1DOAAHD
Z9z9komtqIH1fm3Y0Q6P76nUscLsYOme082L217Th/lTMoqqs4cF2rn9O9Vp4V9U
aCs4XVxGSpcuqbIscfpf0cm44P2eOEk+sbZdahO9C6fezt7YF4OCJ4Vz3qqMD6z4
+6d7FRxUu6k3Te2T2bWBZnsDO30pYFi/gwIDAQAB
-----END RSA PUBLIC KEY-----
bad pem
WbemScripting.SWbemLocator
ConnectServer
ExecQuery
SELECT * FROM Win32_ShadowCopy
Count
ItemIndex
ID
Delete_
\temp
total lengt: %v
.docx
.dll
.exe
.sys
.mui
.tmp
.lnk
.config
.manifest
```

```
.tlb
.olb
.blf
.ico
.regtrans-ms
.devicemetadata-ms
.settingcontent-ms
.bat
.cmd
.ps1
desktop.ini
iconcache.db
ntuser.dat
ntuser.ini
ntuser.dat.log1
ntuser.dat.log2
usrclass.dat
usrclass.dat.log1
usrclass.dat.log2
bootmgr
bootnxt
windir
SystemDrive
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery
\AppData\
ntldr
NTDETECT.COM
boot.ini
bootfont.bin
bootsect.bak
desktop.ini
ctfmon.exe
iconcache.db
ntuser.dat
ntuser.dat.log
ntuser.ini
thumbs.db
.+\\Microsoft\\(User Account Pictures|Windows\\(Explorer|Caches)|Device
Stage\\Device|Windows)\\
files: %v
priority files: %v
priorityFiles: %v
Toatal files: %v
-----------------------------------------
| What happened to your files?
-----------------------------------------
We breached your corporate network and encrypted the data on your computers. The encrypted
data includes documents, databases, photos and more -
all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You
cannot access those files right now. But dont worry!
You can still get those files back and be up and running again in no time.
-----------------------------------------
| How to contact us to get your files back?
-----------------------------------------
The only way to restore your files is by purchasing a decryption tool loaded with a private
key we created specifically for your network.
Once run on an effected computer, the tool will decrypt all encrypted files - and you can
resume day-to-day operations, preferably with
better cyber security in mind. If you are interested in purchasing the decryption tool contact
us at %s
-------------------------------------------------------
| How can you be certain we have the decryption tool?
-------------------------------------------------------
In your mail to us attach up to 3 files (up to 3MB, no databases or spreadsheets).
We will send them back to you decrypted.
Fix-Your-Files.txt
public
systemdrive
```

EKANS (SNAKE) RANSOMWARE

```
pub: %v
root: %v
\Desktop\
\
Global\
ccflic0.exe
ccflic4.exe
healthservice.exe
ilicensesvc.exe
nimbus.exe
prlicensemgr.exe
certificateprovider.exe
proficypublisherservice.exe
proficysts.exe
erlsrv.exe
vmtoolsd.exe
managementagenthost.exe
vgauthservice.exe
epmd.exe
hasplmv.exe
spooler.exe
hdb.exe
ntservices.exe
n.exe
monitoringhost.exe
win32sysinfo.exe
inet_gethost.exe
taskhostw.exe
proficy administrator.exe
ntevl.exe
prproficymgr.exe
prrds.exe
prrouter.exe
prconfigmgr.exe
prgateway.exe
premailengine.exe
pralarmmgr.exe
prftpengine.exe
prcalculationmgr.exe
prprintserver.exe
prdatabasemgr.exe
preventmgr.exe
prreader.exe
prwriter.exe
prsummarymgr.exe
prstubber.exe
prschedulemgr.exe
cdm.exe
musnotificationux.exe
npmdagent.exe
client64.exe
keysvc.exe
server_eventlog.exe
proficyserver.exe
server_runtime.exe
config_api_service.exe
fnplicensingservice.exe
workflowresttest.exe
proficyclient.exe
vmacthlp.exe
msdtssrvr.exe
sqlservr.exe
msmdsrv.exe
reportingservicesservice.exe
dsmcsvc.exe
winvnc4.exe
client.exe
collwrap.exe
bluestripecollector.exe
```