

CERT SOCIETE GENERALE

Computer Security, Incident Response, Forensics, Malware and Cybercrime

13/04/2015

Analyzing Gootkit's persistence mechanism (new ASEP inside!)

Malware authors are quite known for their innovation. A couple of years back, we wouldn't have imagined running into Node.js and JavaScript-based malware, yet that's exactly [what Gootkit does](#). Gootkit is a piece of banking malware that uses web-injects (just like ZeuS and its derivatives) to capture credentials and OTPs from infected users. It has other nifty features such as TLS interception using a local proxy and fake certificates, keylogging, library hooking, UAC bypass... you name it.

A mandatory step in malware's execution process is ensuring persistence, or survival from reboots. The most popular persistence mechanisms include adding an entry to the well-known "Run key" in the user's registry base, or creating a Windows service if the necessary privileges are available. Malware can also use Scheduled Tasks, Winlogon, Applnit, ActiveSetup... That was apparently not enough for the people behind Gootkit, since they use a completely different persistence mechanism.

When running dynamic analysis of recent Gootkit samples (MD5 at the end of the blogpost), we noticed the creation of lots of .sdb files and just as many instances of sdbinst processes. A [blogpost](#) pointed us towards a paper [written in 2014 by Jon Erickson](#), explaining how Microsoft's Fix it patches could be abused to ensure persistence. Gootkit is the first malware we see that uses this persistence mechanism.

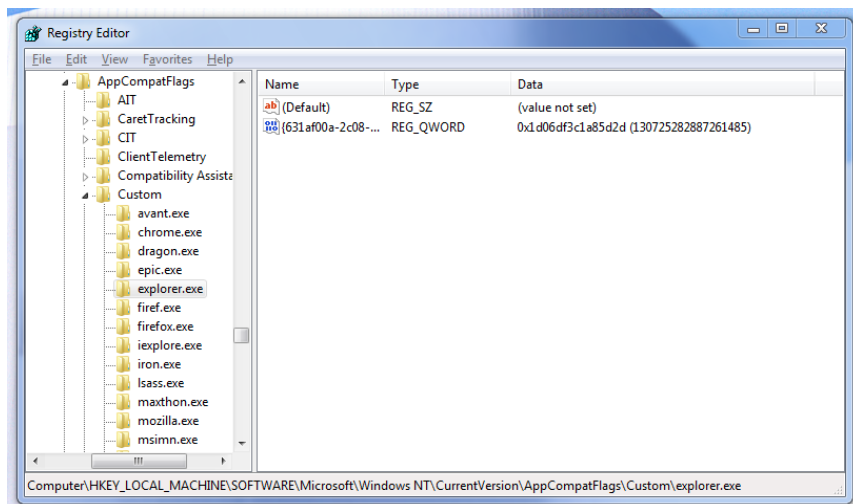
Fix-it patches are used by Microsoft to quickly issue patches without having to release entire binaries. They don't modify the target binary itself but instead provide the Windows loader with information allowing it to patch it once it has been loaded in memory. Patches range from performance improvements to security fixes and can be set on individual programs.

The information concerning these patches is contained in .sdb files. The Windows loader identifies these files through the following registry keys:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB

The Custom key designates the corresponding GUID in the InstalledSDB key. InstalledSDB contains a pointer to the SDB file that will actually define where and how to apply the patch.

Since creating this kind of patches imply writing to the HKLM registry key, administrator rights are required.



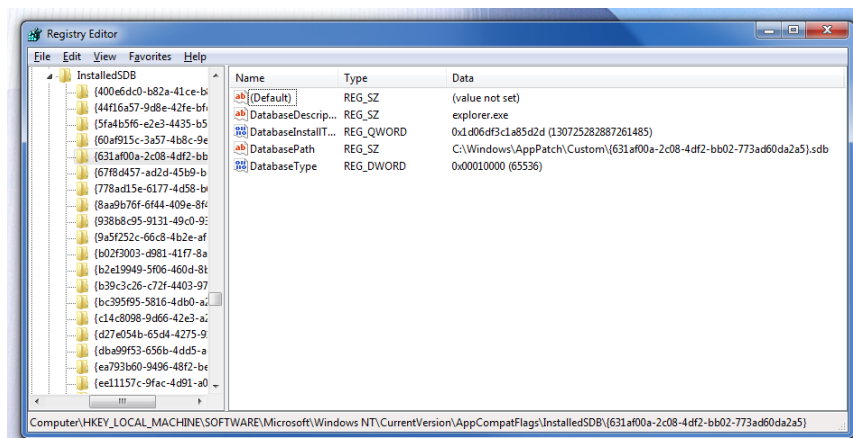
Follow us on Twitter : [@CertSG](#)

Follow by Email

Search

Archives du blog

- ▼ 2015 (3)
 - ▼ 04/12 - 04/19 (1)
 - [Analyzing Gootkit's persistence mechanism \(new ASE...](#)
 - 03/08 - 03/15 (1)
 - 02/01 - 02/08 (1)
- 2013 (3)
- 2012 (4)
- 2011 (4)



The file located at `C:\Windows\AppPatch\Custom\{...}.sdb` is a binary file. It can be read with a tool like [sdb-explorer](#). `sdb-explorer` can be used to manipulate `.sdb` files in many ways, but we'll show how to use it to recover the patch.

`sdb-explorer.exe -t file.sdb` will generate a tree with the information contained in the SDB file. Here's the tree for patching `myie.exe`:

```
c TAG 7802 - INDEXES
12 TAG 7803 - INDEX
 18 TAG 3802 - INDEX_TAG: 28679 (0x7007)
 1c TAG 3803 - INDEX_KEY: 24577 (0x6001)
 20 TAG 4016 - INDEX_FLAGS: 1 (0x1)
 26 TAG 9801 - INDEX_BITS
45 58 45 2e 45 49 59 4d 62 1a 00 00
38 TAG 7001 - DATABASE
 3e TAG 4023 - OS_PLATFORM: 0 (0x0)
 44 TAG 6001 - NAME: myie.exe
 4a TAG 9007 - DATABASE_ID: {5FA4B5F6-E2E3-4435-B56B-70A717FCFA61} NON-STANDARD
 60 TAG 7002 - LIBRARY
 66 TAG 7009 - SHIM_REF
 6c TAG 7005 - PATCH
 72 TAG 6001 - NAME: patchdata0
 78 TAG 9002 - PATCH_BITS

1a62 TAG 7007 - EXE
 1a68 TAG 6001 - NAME: myie.exe
 1a6e TAG 6006 - APP_NAME: myie.exe
 1a74 TAG 9004 - EXE_ID: {7BFBE30-D6BB-4CC1-BD6A-E30E8AE75BDA}
 1a8a TAG 7008 - MATCHING FILE
 1a90 TAG 6001 - NAME: myie.exe
 1a96 TAG 700a - PATCH_REF
 1a9c TAG 6001 - NAME: patchdata0
 1aa2 TAG 4005 - PATCH_TAGID: 108 (0x6c)
1aa8 TAG 7801 - STRINGTABLE
 1aae TAG 8801 - STRINGTABLE_ITEM: myie.exe
 1ac6 TAG 8801 - STRINGTABLE_ITEM: patchdata0
```

The interesting part is `1aa2 TAG 4005 - PATCH_TAGID: 108 (0x6c)`. You can dump the patch corresponding to `PATCH_TAGID: 108` by issuing the command `sdb-explorer.exe -p {...}.sdb 1aa2 > file.txt`. `file.txt` will have contents similar to this:

```
Trying to process patch by tag type: PATCH_TAGID

00000000: 02 00 00 00 2a 17 00 00 d6 16 00 00 00 80 0c 00
[snip]
000019D0: 00 00 00 00 e8 33 71 07 00 eb f9 00 00 00 00 00
000019E0: 00 00 00

module      : kernel32.dll
opcode      : 2 REPLACE
actionSize  : 5930
patternSize : 5846
RVA         : 0x000c8000
Bytes: 55 8b ec 83 e4 f8 [snip] 5f 5e 5b 8b e5 5d c3

Code:
00000000 55          push ebp
00000001 8bec        mov ebp, esp
00000003 83e4f8      and esp, 0xffffffff
[snip]
000016cf 5f          pop edi
000016d0 5e          pop esi
```

```
000016d1 5b          pop ebx
000016d2 8be5        mov esp, ebp
000016d4 5d          pop ebp
000016d5 c3          ret

module      : kernel32.dll
opcode      : 4 MATCH
actionSize  : 92
patternSize : 8
RVA         : 0x000c5f4b
Bytes: 00 00 00 00 00 00 00 00

Code:
00000000 0000        add [eax], al
00000002 0000        add [eax], al
00000004 0000        add [eax], al
00000006 0000        add [eax], al

module      : kernel32.dll
opcode      : 2 REPLACE
actionSize  : 227
patternSize : 143
RVA         : 0x000c5f4b
Bytes: 55 8b ec 51 51 [snip] 5f 5e 8b e5 5d c3

Code:
00000000 55          push ebp
00000001 8bec        mov ebp, esp
00000003 51          push ecx
00000004 51          push ecx
[snip]
00000089 5f          pop edi
0000008a 5e          pop esi
0000008b 8be5        mov esp, ebp
0000008d 5d          pop ebp
0000008e c3          ret

module      : kernel32.dll
opcode      : 4 MATCH
actionSize  : 92
patternSize : 8
RVA         : 0x000c5f3d
Bytes: 00 00 00 00 00 00 00 00

Code:
00000000 0000        add [eax], al
00000002 0000        add [eax], al
00000004 0000        add [eax], al
00000006 0000        add [eax], al

module      : kernel32.dll
opcode      : 2 REPLACE
actionSize  : 98
patternSize : 14
RVA         : 0x000c5f3d
Bytes: 83 04 24 02 60 9c e8 03 00 00 00 9d 61 c3

Code:
00000000 83042402    add dword [esp], 0x2
00000004 60          pushad
00000005 9c          pushfd
00000006 e803000000  call 0xe
0000000b 9d          popfd
0000000c 61          popad
0000000d c3          ret

module      : kernel32.dll
opcode      : 4 MATCH
actionSize  : 89
patternSize : 5
RVA         : 0x0004ee05
Bytes: 90 90 90 90 90

Code:
00000000 90          nop
00000001 90          nop
00000002 90          nop
00000003 90          nop
00000004 90          nop

module      : kernel32.dll
opcode      : 2 REPLACE
actionSize  : 91
patternSize : 7
RVA         : 0x0004ee05
Bytes: e8 33 71 07 00 eb f9
```

```
Code:
00000000 e833710700 call 0x77138
00000005 ebf9 jmp 0x0
```

The `MATCH` instruction will check that the sequence of bytes are present (e.g. it is the correct version of the PE they are about to patch), and the `REPLACE` instruction will actually do the replacement.

The `90 90 90 90 90 90` snippet allows for code to be inserted right before the entry point (or other function prologues) without breaking everything. The `jmp` instruction in our patch replaces a dummy instruction (`mov edi, edi`) and jumps to the call defined just before it, entering our code. It is then up to the code to jump back to the correct location after the patch.

This process is somewhat similar to "hooking" functions in DLLs, except it is being done systematically by the Windows loader if the conditions match.

In this case, the inserted snippet is responsible for loading Gootkit's main executable from the registry and launching it.

The patch will look for a couple of registry keys in `HKCU\Software\AppDataLow`. They are named according to the system architecture: on a 32-bit Windows 7 system, the studied sample generated keys named `BinaryImage32_[\d]`:

The loader concatenates all the key's values, and proceeds to decrypt the blob using a rotating XOR algorithm and uncompresses it using `RtlDecompressBuffer` (LZNT1). The file itself is Gootkit's bulky ~4,5 MB DLL which contains the Node.js engine to launch the malware. The loader then loads the PE, resolves imports, and `DllMain`, ensuring that the malicious payload is up and running.

Dropper MD5 / SHA-1: a28a620b41f852cf7699a7218fe62c69 / 4095c19435cad4aed7490e2fb59c538b1885407a

Publié par [CERT SG](#) à 14:17  +1 Recommander ce contenu sur Google

12/03/2015

Meet FIR - our cybersecurity incident management platform

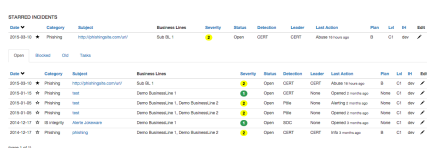
Two years ago we started looking for a tool to help us manage the large number of incidents we have to deal with daily. As most of other CSIRT teams out there, we were left quite disappointed with the tools that were out there (free or not). So we decided to roll our own.

FIR stands for "Fast Incident Response". It's meant to be exactly that - fast and agile - so that we can focus on responding to incidents rather than filling forms. Over the past months, we've been looking behind us and we thought that it would be a good idea to release it to the public.

First and foremost, in hope of helping the community out by providing a simple tool to manage cybersecurity incidents, but also to learn from our fellow responders and give them the opportunity to share their workflows and methods and contribute to this project.

So we're releasing FIR to the public. You'll find everything you need to test it out on our GitHub repo: <https://github.com/certsocietegenerale/FIR>. Everything you need to know to get rolling is on the Wiki. Remember, this is the tool we use daily to manage and keep track of our incidents, so expect lots of new features (and, of course, the inevitable bug or two) and a reasonable amount of reactivity on open issues. We'll be happy to merge your pull requests in exchange.

Sharing is caring!



Date ▼	Category	Subject	Business Lines	Severity	Status	Description	Location	Last Action	Plan	Lat	Alt	Map
2015-03-10	Phishing	http://certsocietegenerale.com/	Sub-BL 1	High	Open	GDPR	GDPR	Added to watch list	0	C1	dev	
Open Closed C21 Tools												
Date ▼	Category	Subject	Business Lines	Severity	Status	Description	Location	Last Action	Plan	Lat	Alt	Map
2015-03-10	Phishing	http://certsocietegenerale.com/	Sub-BL 1	High	Open	GDPR	GDPR	Added to watch list	0	C1	dev	
2015-03-10	Phishing	test	Domain BusinessLine 1	High	Open	GDPR	GDPR	Added to watch list	0	C1	dev	
2015-03-10	Phishing	test	Domain BusinessLine 1, Domain BusinessLine 2	High	Open	Phishing	Phishing	Added to watch list	0	C1	dev	
2015-03-10	Phishing	test	Domain BusinessLine 1, Domain BusinessLine 2	High	Open	Phishing	Phishing	Added to watch list	0	C1	dev	
2015-03-10	Phishing	test	Domain BusinessLine 1	High	Open	GDPR	GDPR	Added to watch list	0	C1	dev	
2015-03-10	Phishing	test	Domain BusinessLine 1, Domain BusinessLine 2	High	Open	GDPR	GDPR	Added to watch list	0	C1	dev	

page 1 of 1

Publié par [CERT SG](#) à 10:56  +4 Recommander ce contenu sur Google

03/02/2015

CTB Locker: a new massive crypto-ransomware campaign

A new crypto-ransomware called **CTB-Locker** has been overloading our mailboxes since last week.

Like its infamous "Cryptolocker" counterpart its goal is to encrypt your files (on your computer and also on all the network shares it is connected to) in order to extort a ransom (3 bitcoins or approximately 620 € at the time of this writing).

CTB stands for "Curve-Tor-Bitcoin", the three pillars of this new threat: elliptic curve cryptography to perform the encryption, Tor and Bitcoin to ensure anonymity for the payment.

The common infection vector is via an email containing a fake invoice compressed in a ".zip" or ".cab" archive file. The archives contain a binary (Dalexis dropper, usually in an ".scr" file) which, once

opened, displays a decoy RTF document, waits for 5 minutes and then drops the actual CTB-Locker payload, which in turn performs the encryption routines.

Below are a few malicious email examples:



ctb1.png



ctb2.png



ctb3.png



ctb4.png

Once the computer is infected, an explicit message is displayed explaining how to pay the ransom:



CTB-Locker.png

At the moment, file recovery is impossible once the system is infected (unless you restore the files from backup). The latest version deactivates the shadow copies on the system.

We have collected a list of URLs from where the payloads are dropped. We recommend you to block them on your proxies. Please note these are not actual **.tar.gz** files but encrypted binary blobs.

<https://agatecom.fr/voeux/doom.tar.gz>
<https://aspiroflash.fr/cai/abc.tar.gz>
<https://baselineproduction.fr/Modules/doom.tar.gz>
<https://bikeceuta.com/templates/hello.tar.gz>
<https://bikeceuta.com/templates/nero.tar.gz>
<https://breteau-photographe.com/tmp/pack.tar.gz>
<https://cargol.cat/IESABP/hello.tar.gz>
<https://cargol.cat/IESABP/nero.tar.gz>
<https://cds-chartreuse.fr/locales/sancho.tar.gz>
https://collection-opus.fr/_gfx/cario.tar.gz
<https://compassfx.com/OLD/cario.tar.gz>
https://dariocasati.it/logs/dostanes_do_drzky.tar.gz
<https://dequinnzangersborne.nl/language/upupup.tar.gz>
<https://dieideenwerkstatt.at/css/abc.tar.gz>
<https://evalero.com/img/cario.tar.gz>
<https://fbrugues.com/language/hiser.tar.gz>
<https://firststepbahamas.com/PDF/abc.tar.gz>
<https://fotocb.de/php/upupup.tar.gz>
<https://hotel-mas-saint-joseph.com/css/pack.tar.gz>
<https://integritysites.net/files/nero.tar.gz>
<https://jbmsystem.fr/jb/pack.tar.gz>
<https://joefel.com/easyscripts/sancho.tar.gz>
<https://krzysztofkarpiński.pl/log/hiser.tar.gz>
<https://locamat-antilles.com/memo/sancho.tar.gz>
<https://m-a-metare.fr/media/sancho.tar.gz>
<https://maisondeessources.com/assets/pack.tar.gz>
<https://masterbranditalia.com/downloader/cario.tar.gz>
https://microneedle.com/menu_files/pack.tar.gz
<https://mmadolec.ipower.com/me/cario.tar.gz>
<https://n23.fr/asstempo/doom.tar.gz>
<https://necaps.org/pagestyles/mine.tar.gz>
https://ohayons.com/dostanes_do_drzky.tar.gz
<https://ourtrainingacademy.com/LeadingRE/sancho.tar.gz>
<https://peche-sportive-martinique.com/wp-includes/pack.tar.gz>
<https://pinballpassion.fr/images/mine.tar.gz>
<https://pleiade.asso.fr/piwigotest/pack.tar.gz>
<https://ppc.cba.pl/cache/hello.tar.gz>
<https://ppc.cba.pl/cache/nero.tar.gz>
<https://prevencionprl.com/im/hiser.tar.gz>
<https://pubbliemme.com/plugins/doom.tar.gz>
<https://scolapedia.org/histoiredesarts/pack.tar.gz>
<https://shop-oye.it/XXXinstallXXX/abc.tar.gz>
<https://siestahealthtrack.com/media/pack.tar.gz>
<https://smartoptionsinc.com/data-test/hello.tar.gz>
<https://smartoptionsinc.com/data-test/nero.tar.gz>
https://sp107.home.pl/logs/dostanes_do_drzky.tar.gz

https://springtree.cba.pl/modules/cario.tar.gz
https://stmarys-andover.org.uk/audio_files/upupup.tar.gz
https://telasramacrisna.com.br/ramacrisna/mine.tar.gz
https://telasramacrisna.com.br/site/lightbox/hiser.tar.gz
https://thinkonthis.net/style/dostanes_do_drzky.tar.gz
https://thomasottogalli.com/webtest/sancho.tar.gz
https://voigt-its.de/fit/pack.tar.gz
https://wcicinc.org/flv/dostanes_do_drzky.tar.gz
https://www.cpeconsultores.com/tmp/pack.tar.gz
https://www.lamas.si/picture_library/upupup.tar.gz
https://www.sazlar.de/sazlar/mine.tar.gz
https://wymiana-wsb.cba.pl/pp/abc.tar.gz
https://zysztokarpinski.pl/log/hiser.tar.gz

Publié par [CERT.SG](#) à 17:28



+18 Recommander ce contenu sur Google

24/10/2013

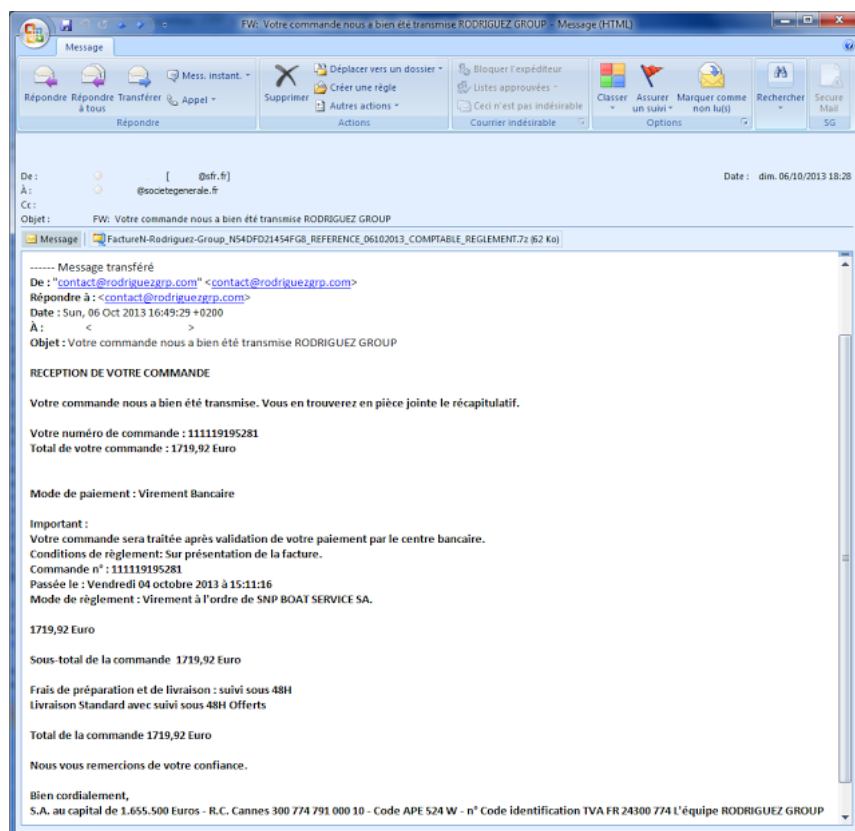
Spamvertizing : du malware dans votre boîte mail

A l'occasion de ce deuxième article du [Cyber Security Awareness Month](#), nous allons présenter une des techniques les plus utilisées par les cybercriminels pour diffuser du malware : le spamvertizing.

Le mot "spamvertizing" est un mot-valise composé de "spam" et "advertising". Autrement dit, c'est une technique qui consiste à diffuser un produit (en l'occurrence un malware) par le biais de spam (des campagnes massives de courriers électroniques non-sollicités). L'objectif du spamvertizing est d'installer un logiciel malveillant, le plus souvent un [cheval de Troie](#), sur le plus grand nombre de postes possibles afin de pouvoir en prendre le contrôle et récupérer des informations bancaires (numéros de carte, codes de connexion à distance) ou personnelles qui y transiteraient.

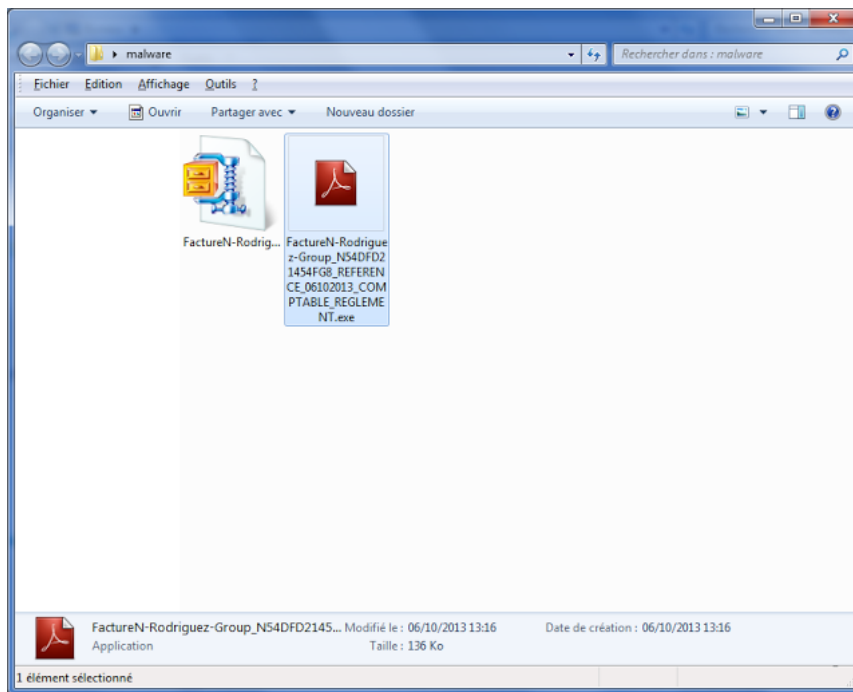
Très souvent ces emails semblent provenir d'une autorité financière reconnue (Ministère des Finances, Paypal, un établissement bancaire) et tentent de persuader le destinataire d'ouvrir la pièce jointe. Plusieurs prétextes sont possibles : un défaut de paiement, un paiement doublonné, ou tout simplement la facture d'un produit (souvent très cher) que l'internaute n'a jamais commandé. Ces arnaques peuvent aussi s'appuyer sur des produits de consommation : de faux envois de colis, de faux billets d'avions, etc.

Voici un exemple typique de cas de malware spamvertisé :



Ici, le prétexte est un faux accusé de réception de commande. L'internaute peu suspicieux s'alarmera du montant qui lui sera, pense-t-il, débité, et voudra en savoir plus en ouvrant la "facture" en pièce jointe. Cette facture n'est rien d'autre que le logiciel malveillant qui s'exécutera sur l'ordinateur de l'internaute et s'y installera.

La pièce jointe est un fichier compressé. Afin de duper les utilisateurs les moins avertis, l'archive contient un fichier exécutable comportant une icône de fichier PDF. Une fois que l'utilisateur ouvre le fichier, le poste est contaminé.



Nous conseillons à tous les internautes de rester vigilants face à ces menaces : n'ouvrez pas les pièces jointes envoyées par des personnes ou entités que vous ne connaissez pas et veillez à maintenir votre antivirus à jour.

Publié par [CERT SG à 12:02](#)  Recommander ce contenu sur Google

Libellés : [Cyber Security Awareness Month](#), [cybercriminalité](#), [fausse facture](#), [malware](#), [modus operandi](#), [spamvertising](#)

17/10/2013

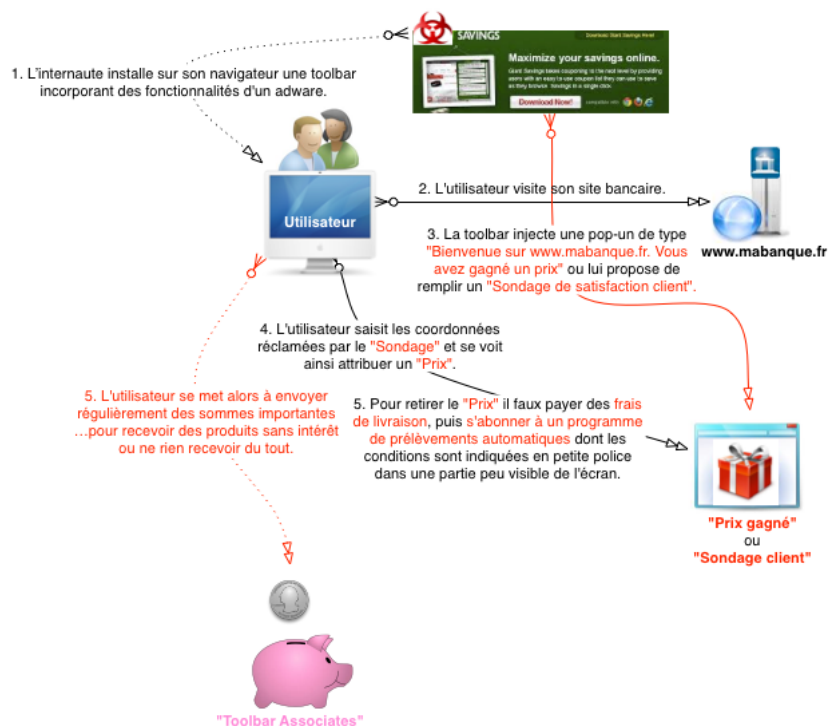
Attention, greyware !

A l'occasion du [Cyber Security Awareness Month](#), le CERT Société Générale inaugure une nouvelle rubrique, « *Modus Operandi* ». Cette rubrique a pour but de sensibiliser le grand public aux différents modes opératoires frauduleux ou autres pièges existants.

Dans ce premier billet, nous présentons un schéma récent, à mi-chemin entre malware et marketing malintentionné qui vise à abonner l'internaute à des services dont il n'a pas forcément besoin ou à lui vendre des produits ayant a priori peu d'intérêt. Tout cela se fait de manière tout à fait automatisée, au travers d'un logiciel se rapprochant des [publiciels](#) (adware).

Même si le [greyware](#) utilisé n'est pas un malware bancaire, les clients des banques françaises peuvent être une cible privilégiée.

Selon notre analyse, le processus se déroule de la manière décrite dans le schéma ci-dessous :



Le CERT Société Générale recommande de toujours rester vigilant quant à l'origine des logiciels téléchargés (ici, le vecteur "d'infection" est la barre d'outils installée en 1.) et d'utiliser un anti-virus à jour.

Une très grande partie des barres d'outils pour navigateur rencontrées sur Internet a pour but plus ou moins dissimulé d'installer des agents publicitaires sur l'ordinateur de l'internaute ayant téléchargé l'application.

Publié par [CERT SG](#) à 17:48



Recommander ce contenu sur Google

03/07/2013

event2timeline - a Windows security event log visualization tool

event2timeline has its own [Github repo](#).

A recurring task in DFIR is to scour through hundreds of megabytes of Microsoft Windows event logs, searching for suspicious session establishments. Even with great tools such as [log2timeline](#) (or its newer version, [plaso](#)) and an unlimited amount of coffee, singling out "strange" session establishments can be a daunting task, especially on a busy server used by people from all over the world. It's like looking for a black cat in a dark basement, while blindfolded.

We had to come up with a solution that would avoid us the hassle of nitpicking through lines and lines of log entries. A tool that would take those hefty log files, extract every single session out of them, associate them to their username, and display the result on an easy-to-read timeline. That's exactly what event2timeline does.

event2timeline can parse EVTX Security log files (the ones from Windows Vista and onwards - Windows 7 and Windows 8), as well as CSV extracts from tools such as [Event Log Explorer](#) (free for personal, non-commercial use) or Microsoft's [Log Parser 2.2](#). It parses through the logs and generate an HTML based timeline, using the [D3.js](#) Javascript visualization library. You can zoom and scroll through the timeline, and mouseover any session to get more information, such as Event ID, domain/username, source IP (if applicable), etc.

Below is a screenshot of the final result, based on demo material from the [SANS Advanced computer forensic analysis incident response](#) course.



Feel free to use event2timeline during your daily DFIR routine. Let us know of any improvements you would like to make through [pull requests on github](#) or via our Twitter account [@CertSG](#).

Publié par [CERT SG](#) à 13:21

+1 Recommander ce contenu sur Google

Libellés : [dfr](#), [event log](#), [session](#), [tools](#), [windows](#)

22/10/2012

Le « domain slamming »

1. Définition et variantes
2. Caractéristiques communes
3. Recommandations

Définition et variantes

Le domain slamming, ou « écrasement de domaine » peut être défini comme une pratique illicite visant à tromper des clients afin de les inciter à acheter des services non sollicités. Bien que ce genre de pratiques existe ailleurs, notamment dans le monde des télécommunications, le slamming s'entend ici dans l'univers des noms de domaine. La plupart du temps, les entités se livrant à cette activité utilisent les bases WHOIS des registres pour contacter leurs victimes.

Nous présentons ici trois grandes familles de slamming. Toutefois, cette liste ne peut pas être considérée comme étant exhaustive dans la mesure où elle dépend de l'imagination des auteurs de ces pratiques illicites.

La fausse facture de renouvellement

Cette variante de slamming consiste à envoyer au titulaire d'un nom de domaine un « Avis d'expiration » de celui-ci, le document se présentant comme une facture de renouvellement.

Un client peu familiarisé avec les procédures de gestion des noms de domaine et avec la terminologie employée pourra considérer qu'il doit honorer cette « facture » pour renouveler son nom de domaine. En réalité, il signera une demande de transfert de son nom vers l'émetteur de « l'Avis d'expiration », c'est-à-dire vers un prestataire qu'il ne connaît pas.

Les retours que nous avons eu de victimes de cette pratique indiquent que le nouveau prestataire ne répond généralement pas aux sollicitations dont il est ensuite l'objet. Les divers procès intentés contre les auteurs de cette pratique illicite ne paraissent pas les avoir contraints à cesser leurs activités.

En 2010, la Federal Trade Commission américaine a [réussi à mettre fin](#) à une vaste opération de renouvellements frauduleux.

Le cas de faux cyber-squatting

Cette variante du slamming consiste pour un prestataire à prendre contact avec une entreprise en lui indiquant « que l'un de ses clients » lui a demandé de déposer un ou plusieurs noms de domaine identiques ou proches du nom de l'entreprise ou de l'une de ses marques. Le prestataire propose alors à l'entreprise de déposer ces noms pour elle afin de les protéger contre les intentions visiblement illicites de son « client ». Les noms de domaine proposés sont souvent assez éloignés de la marque originale, et ont des TLD peu communs (comme par exemple .asia). Par ailleurs, les prix proposés pour une telle prestation dépassent largement ceux qui peuvent être obtenus en utilisant des canaux conventionnels. Dans l'exemple ci-dessous, un slammer propose un domaine finissant en .asia à 55 € par an, alors que le prix de marché pour le même domaine est à 1,99 € par an.



REGISTRATION DISCOUNT PRICES

Country	Dispute Domain Name & Brand Name	Price(EUR/per year)
China	www.■■■■.cn	35 EUR /per year
China	www.■■■■.com.cn	35 EUR /per year
China	www.■■■■.org.cn	35 EUR /per year
China	www.■■■■.net.cn	35 EUR /per year
HongKong	www.■■■■.com.hk	58 EUR /per year
HongKong	www.■■■■.hk	58 EUR /per year
Taiwan	www.■■■■.com.tw	58 EUR /per year
Taiwan	www.■■■■.tw	58 EUR /per year
India	www.■■■■.in	55 EUR /per year
Asia	www.■■■■.asia	55 EUR /per year
Brand Name	■■■■	200 EUR /per year

Tarifs "domain slamming"

Rubrique Noms de domaine				
CREATION	Domaine	Quantité	Prix unitaire	Prix HT
Création d'un .asia - 1 an	■■■■.asia	1	1,99 €	1,99 €
Création d'un .cn - 1 an	■■■■.cn	1	8,99 €	8,99 €
Création d'un .tw - 1 an	■■■■.com.tw	1	19,99 €	19,99 €
Création d'un .hk - 1 an	■■■■.hk	1	19,99 €	19,99 €
Création d'un .in - 1 an	■■■■.in	1	6,99 €	6,99 €
Création d'un .tw - 1 an	■■■■.tw	1	19,99 €	19,99 €
			Sous total	77,94 €

Tarifs conventionnels pour le même domaine

La démarche est généralement présentée comme découlant d'un souci éthique de protéger l'entreprise ciblée contre les abus de tiers. Quoique fondée dans l'absolu, cette démarche peut pourtant être considérée comme illicite par le caractère systématique du démarchage réalisé par ces types de slammers, les tarifs exceptionnellement élevés pratiqués, ainsi que la création d'une certaine pression psychologique, renforcée par la nécessité de prendre une décision rapidement.

Là encore, nous n'avons pas eu connaissance d'actions juridiques ayant contraint ce type d'acteurs à cesser leurs activités. Les victimes sont vulnérables en ce que pris isolément, chaque cas peut être considéré comme relativement licite. C'est le caractère systématique et « industriel » de la pratique qui peut démontrer l'intention frauduleuse. Pour cette raison, cette approche au domain slamming est extrêmement courante, surtout auprès des petites et moyennes entreprises ayant une image à défendre sur Internet.

Le faux « registre »

Une troisième variante identifiée consiste pour le fraudeur à contacter des entreprises ou organismes français présents sur l'Internet, en leur laissant entendre qu'ils doivent s'inscrire dans l'annuaire réalisé par le fraudeur. Le texte laisse planer un doute sur le caractère obligatoire de ce « référencement » mais les victimes ayant signé la proposition reçoivent un véritable annuaire accompagné d'une facture de plusieurs centaines d'euros – un montant excessif si l'on considère la diffusion « confidentielle » de l'annuaire.

La tromperie résiderait ici dans l'utilisation de référentiels visuels et textuels associés à des acteurs légitimes du marché des annuaires et/ou de l'Internet en France, pouvant induire en erreur les personnes peu familiarisées avec ces acteurs ou faisant preuve de crédulité à l'égard de documents « semi-officiels ».

Cette pratique existe déjà depuis assez longtemps dans le monde des marques, des sociétés étrangères proposant de « finaliser » l'enregistrement international de leur marque à des déposants récents. Si les grandes structures et les professionnels sont bien armés contre ce genre de pratiques, les PME peuvent en être assez facilement victimes.

Ainsi, en 2011, Ostrolenk Faber LLP a [mis en garde](#) contre des types d'arnaques où leurs clients recevaient des notices de la part de faux registrars ou de personnes se faisant passer pour la "United States Trademark Agency"

Caractéristiques communes

Ces différentes approches au "domain slamming" présentent tout de même certaines caractéristiques communes :

- La prestation offerte n'est jamais sollicitée au préalable par la victime mais émane d'un tiers qui lui est inconnu.
- Le mécanisme de l'opération de slamming repose le plus souvent sur un élément de confusion ou de tromperie, visant à profiter de la crédulité de la victime ou de sa méconnaissance des règles.
- Dans la plupart des cas, un élément de pression psychologique existe au travers d'une menace latente à l'encontre de la victime si elle ne répond pas positivement à la proposition qui lui est faite : perte d'un nom, cybersquatting, etc.
- Les tarifs proposés sont généralement sensiblement plus élevés que la normale, ceci afin de permettre au slammer de gagner de l'argent en maximisant son profit sur le pourcentage limité de « prospects » qui se laisseront « convaincre ».

Recommandations

De cette analyse des caractéristiques communes des opérations de slamming découlent quelques recommandations de base :

- Pour toute opération sur un nom de domaine, et notamment les renouvellements, ne passez uniquement par le bureau d'enregistrement auquel vous avez confié la gestion de ce nom de domaine. Tout autre acteur peut être potentiellement suspect dès lors que vous ne l'avez pas préalablement mandaté pour effectuer l'opération projetée.
- Désignez une personne de votre entreprise clairement habilitée à prendre les décisions concernant vos noms de domaine, et faites savoir auprès de vos collaborateurs et de vos bureaux d'enregistrement que toute demande portant sur les noms de domaine doit au minimum être validée par cette personne.
- Assurez-vous que votre bureau d'enregistrement ne répondra à aucune sollicitation venant d'un tiers sans que la personne habilitée ne l'y ait préalablement autorisé, et qu'il vous alertera sur toute sollicitation suspecte.
- Ne prenez aucune décision dans l'urgence ; si vous avez un doute, demandez à votre prestataire de vous expliquer les tenants et aboutissants de la décision à prendre.
- Faites une veille régulière sur l'actualité des noms de domaine ; de telles pratiques sont identifiées par les experts et leurs articles pourront vous tenir informés.

Publié par [CERT.SG](#) à 15:00

+1 Recommander ce contenu sur Google

09/08/2012

Sensibilisation : le typosquatting et le cybersquatting

Nous allons évoquer dans ce billet le *typosquatting* et le *cybersquatting*, deux techniques qui peuvent être utilisées pour tromper un internaute à des fins frauduleuses en manipulant les noms de domaine.

Rappel sur les noms de domaine

Tout ordinateur connecté à Internet possède une adresse dite « IP » (*Internet Protocol*) constituée d'une série de chiffres telle que 213.182.38.47. Cette adresse est utilisée pour joindre un autre équipement informatique sur Internet.

Le nommage Internet consiste à associer un nom tel que *www.google.fr* à une adresse IP : 173.194.67.94. Il est en effet plus simple pour un humain de retenir puis saisir un nom qu'une série de chiffres. Toutefois, votre navigateur va traduire le nom saisi en adresse IP. Pour cela, il utilise le service DNS (*Domain Name Service*). Ce dernier fait automatiquement l'association entre un nom et une adresse IP.

L'erreur étant humaine, il peut arriver qu'un internaute fasse une faute de frappe en entrant le nom d'un site dans son navigateur. Ainsi, il peut taper « *www.socetiegenerale.fr* » au lieu de « *www.societegenerale.fr* ».

Dans certains cas, cette erreur aboutit à l'affichage d'un message d'erreur informant l'internaute que le nom saisi n'existe pas. Dans d'autres, le nom mal orthographié existe et un site est chargé par le navigateur.

Deux techniques sont couramment utilisées pour exploiter les erreurs de frappe : le typosquatting et le cybersquatting.

Qu'est-ce que le typosquatting ?

Le typosquatting est une technique consistant à acheter un nom de domaine dont l'orthographe est très proche d'un domaine existant afin de profiter des fautes de frappe des internautes pour détourner le trafic destiné au site légitime vers un autre site.

On distingue 3 grandes catégories de typosquatting :

- l'utilisation du nom du site « squatté » en l'écrivant différemment : *www.societesgenerales.fr*, *www.societe--generale.fr...* ;
- l'utilisation d'une faute d'orthographe dans le nom : *www.sossietegenerale.fr*, *www.societegennerale.fr...* ;
- l'exploitation des fautes de frappe prévisibles dans le nom : *www.societegenerake.fr*, *www.soicetegenerale.fr...*

Qu'est-ce que le cybersquatting ?

Le cybersquatting est une technique qui consiste à déposer un nom Internet correspondant à une marque déposée en lieu et place de son propriétaire. Cela s'apparente à une usurpation d'identité.

On peut distinguer plusieurs cas de figure.

Si le nom n'existe pas encore, le cybersquatteur peut le déposer avant que le propriétaire légitime de la marque ne le fasse. Très souvent, le cybersquatteur va tenter de prendre de vitesse le dépositaire d'un nom de domaine avec une certaine extension (« .com » par exemple) en achetant avant lui le nom de la marque avec une extension différente : « .fr », « .org », et ainsi de suite.

Ont ainsi été victimes de ce type de cybersquatting :

- le site *eBay.com* : en 1999, une société française a déposé le nom *ebay.fr* (<http://www.iuriscom.net/txt/iurisfr/ndm/resum.htm#ebay>)
- France Télévisions : en 2001, les noms *france3.com* et *france2.com* ont été déposés par une société éditant du contenu pour adulte. Ces deux noms dirigeaient les internautes vers des sites pornographiques. (<http://pro.01net.com/editorial/504042/porn-squatting-des-litiges-sur-les-noms-de-domaine-les-plus-hot/>).
- La Présidence américaine et son domaine *whitehouse.gov* : le nom *whitehouse.com* redirigeait vers du contenu pornographique alors que site *whitehouse.org*, redirigeait vers une page promouvant la candidature du républicain Ron Paul aux élections de 2012. (<http://en.wikipedia.org/wiki/Whitehouse.com> et <http://en.wikipedia.org/wiki/Whitehouse.org>)

Quels sont les buts de ces deux techniques ?

Les buts de ces deux techniques sont multiples et ne sont pas tous illégaux.

Le détournement de trafic est une des principales motivations du typosquatting : le site de typosquatting présente alors une simple liste de liens publicitaires. Chaque « clic » d'un internaute sur un de ces liens rapporte quelques centimes au typosquatteur. Le typosquatteur parie sur le fait que quelques internautes cliqueront sur un lien. Quand le site typosquatté est très fréquenté, cela peut s'avérer payant à moindre coût et à moindres efforts.

Le typosquatteur peut aussi proposer des biens et services proches ou concurrents de ceux du site typosquatté, en espérant que les internautes arrivés sur son site par erreur y resteront et effectueront des transactions. Cela représente cependant des risques pour le typosquatteur car son site peut être assimilé à de la contrefaçon ou de la concurrence déloyale.

De manière plus insidieuse, le typosquatteur tout comme le cybersquatteur peuvent espérer négocier le rachat de leur

domaine par le propriétaire légitime d'une marque ou d'un site. En effet, il existe de grandes disparités juridiques entre les pays. Une procédure judiciaire visant, pour une entreprise victime de cybersquatting ou de typosquatting, à récupérer par voie de justice un domaine usurpant une de ses marques, peut se révéler longue, coûteuse, et, parfois, inefficace.

Les squatteurs espèrent alors que l'entreprise va privilégier un mauvais accord (c'est-à-dire que l'entreprise paiera très cher le rachat du domaine) à un procès. Cela peut s'apparenter à une « prise d'otage » numérique ou à du racket.

Mais le typosquatting et le cybersquatting peuvent aussi avoir des objectifs nettement plus frauduleux.

Un pirate peut ainsi typosquatter le nom ou la marque d'une banque, d'un site d'e-commerce ou d'un opérateur Internet, et héberger sous ce nom une copie du site original. En résumé, le pirate peut utiliser le typosquatting et le cybersquatting pour des opérations de [phishing](#), dans le but de rendre celui-ci plus crédible.

Beaucoup d'internautes ne vérifient malheureusement pas l'adresse d'un site de phishing. Quelques-uns, plus avertis que d'autres, prennent le temps de lire l'adresse Internet réelle vers laquelle le phishing renvoie.

Une adresse Internet (ou URL) trop « exotique » (utilisation d'une adresse IP, d'un site d'hébergement de pages personnelles, etc.) éveillera la méfiance de l'internaute et réduira le taux d'efficacité de l'attaque. Mais si cette URL est [www.mabanque.com](#) au lieu de [www.mabanque.com](#), une lecture trop peu attentive ne permettra pas à l'internaute de déceler le subterfuge. Le nom ressemblant à celui du site légitime, il sera plus enclin à entrer des informations sur la page de phishing.

Que faire face à ces deux techniques ?

Au-delà des conseils qui figurent dans notre billet intitulé « [Sensibilisation : le "phishing" ou hameçonnage](#) » et qui restent entièrement applicables, la vigilance reste la meilleure façon de déceler l'emploi de typosquatting ou de cybersquatting à des fins frauduleuses.

Lorsque vous saisissez une adresse Internet dans votre navigateur, nous vous conseillons de la relire pour vous assurer qu'elle ne comporte pas d'erreur avant de taper la touche Entrée.

Les sites que vous visitez fréquemment devraient faire partie de votre liste de favoris. Cette fonctionnalité, offerte par tous les navigateurs grand public, vous permet d'organiser ces sites par rubriques et d'y accéder à chaque fois que vous le désirez par simple clic. Veuillez consulter la documentation de votre navigateur pour savoir comment utiliser cette fonctionnalité.

Lorsque vous recevez un courriel qui vous demande de cliquer sur un lien Internet, assurez-vous que le corps et le sujet du message ne comportent pas d'erreurs d'orthographe ou de grammaire flagrantes. S'il vous semble correctement rédigé, positionnez le pointeur de votre souris sur le lien proposé afin de voir l'adresse vers laquelle il mène. Celle-ci peut avoir été subrepticement définie à des fins de typosquatting et de cybersquatting.



En cas de doute, ne répondez pas au courriel et ne cliquez pas sur les liens qui peuvent vous être proposés. Ne faites pas confiance aux adresses ou numéros de téléphone de contact proposés dans le corps du message. Rendez-vous directement sur le site dont se prétend le courriel afin d'obtenir l'adresse électronique ou le numéro de téléphone du support ou du conseiller qui saura vous indiquer si le courriel est légitime ou non. S'il s'agit d'un courriel relatif à Société Générale, nous disposons d'une [page](#) à cet effet.

Publié par [CERT SG](#) à [16:32](#) +1 Recommander ce contenu sur Google

Libellés : [cybercriminalité](#), [dns](#), [sensibilisation](#)

20/03/2012

Lutte contre les chevaux de Troie : Logiciel Trusteer « Rapport »

Nous avons évoqué dans notre [billet](#) de blog précédent ce qu'était un logiciel malveillant de type cheval de Troie. Ce type de logiciel malveillant infecte les ordinateurs pour y dérober des données personnelles et bancaires pouvant être monétisées par les fraudeurs : numéros de cartes bancaires, identifiants et mots de passe de sites bancaires (ou de sites d'e-commerce), comptes de réseaux sociaux, comptes e-mails, etc.

Les antivirus traditionnels sont spécialisés pour lutter contre les infections par ces logiciels malveillants, mais ils doivent être constamment mis à jour pour être efficaces et leur mode de fonctionnement est limité. En effet, un nouveau virus diffusé sur Internet a de bonnes chances de ne pas être détecté par un antivirus pendant plusieurs heures voire plusieurs jours.

Pour comprendre pourquoi ces antivirus ne sont pas efficaces à 100%, il faut se pencher sur les modes de fonctionnement et de diffusion d'un cheval de Troie.

Mode de diffusion des chevaux de Troie

Comme nous l'avions déjà évoqué dans notre [billet](#) précédent, les cybercriminels infectent principalement les ordinateurs par :

- Téléchargement : les chevaux de Troie se trouvent dans des fichiers téléchargés sur Internet, souvent des logiciels piratés ;
- Navigation (drive-by-download) : les cybercriminels infectent des sites Internet qui, à leur tour, infectent les utilisateurs non protégés ;
- E-mail : les cybercriminels envoient des e-mails que les utilisateurs ouvrent, infectant ainsi leur propre ordinateur ;
- Réseaux sociaux et logiciels de messagerie : des messages contenant des liens malveillants sont transmis par Twitter, Facebook, MSN, Yahoo Messenger, etc. vers les utilisateurs, qui les suivent et se font infecter.

Deux choix stratégiques foncièrement différents s'offrent aux cybercriminels : soit ils infectent un maximum de personnes (des dizaines ou des centaines de milliers de personnes) et privilégient la masse pour rentabiliser leur fraude, soit ils décident d'infecter moins de personnes (quelques milliers) afin de rester inaperçus le plus longtemps possible.

Cette décision influence fortement la capacité de détection par les anti-virus. En effet, **plus un cheval de Troie est diffusé sur Internet, plus sa probabilité de détection par les logiciels de sécurité augmente.**

En revanche, comme certains cybercriminels envoient plusieurs variantes d'un même cheval de Troie tous les jours, il est impossible pour un antivirus d'être à jour « dès la diffusion du virus ».

Mode de fonctionnement des chevaux de Troie

Nous allons être très synthétiques ici. Le but n'est pas d'être exhaustif dans les détails techniques, mais plutôt de comprendre ce que fait un cheval de Troie sur un ordinateur.

Le cheval de Troie, une fois qu'il a infecté un ordinateur, reste « en écoute » sur le navigateur et parfois sur d'autres logiciels, tels que l'antivirus, le logiciel de messagerie, les jeux vidéos, etc. On dit que le cheval de Troie s'est « injecté » dans les logiciels importants de l'ordinateur, dont le navigateur Internet.

Il surveille ensuite tout ce qui est fait dans le navigateur, à la recherche d'informations intéressantes. Il examine les navigations, que ce soit en suivant un lien ou en tapant directement une adresse dans la barre de navigation, ou encore en choisissant un marque-page. Il peut également surveiller les communications pour les sites « sécurisés » https.

Que faire contre ces chevaux de Troie ?

Pour éviter l'infection il est nécessaire d'installer dès que possible les mises à jour du système d'exploitation (Microsoft Windows, Apple Mac OS-X, ou autre), celles du navigateur Internet ainsi que celles des logiciels tiers (Sun Java, Adobe Reader ou Acrobat, etc). Les mises à jour à installer en priorité sont celles relatives à la sécurité. Il est également nécessaire de mettre à jour l'antivirus. Ces bonnes pratiques ne sont pas toujours suffisantes pour contrecarrer les chevaux de Troie. Comment pousser alors plus loin la protection et augmenter ainsi les chances de ne pas se faire infecter et voler des données importantes ?

Plusieurs solutions innovantes existent pour tenter de détecter différemment les codes malveillants.

Parmi ces solutions, l'une consiste à placer la solution antivirus directement dans le navigateur Internet et dans certains processus du système d'exploitation, comme le ferait un cheval de Troie. Le logiciel contrôle alors tout ce qui se passe et peut détecter des comportements suspects dans la navigation de l'utilisateur.

Certaines solutions vont encore plus loin, puisqu'elles se concentrent sur la protection de la navigation entre le site Internet de banque en ligne et vous.

Trusteer Rapport

Société Générale a testé longuement plusieurs de ces solutions innovantes et a pu apprécier l'efficacité du logiciel « Rapport », édité par la société Trusteer.

Ce logiciel s'utilise en complément de votre antivirus habituel pour protéger vos navigations, notamment sur l'Espace Internet des Particuliers. De façon très simple, il permet d'augmenter la protection sur votre ordinateur lorsque vous vous connectez à l'Espace Internet des Particuliers.

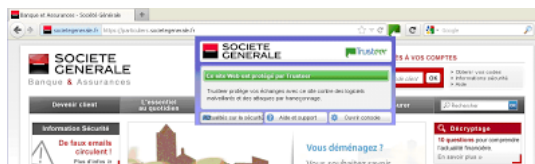
« Rapport » protège les communications Internet grâce à différentes fonctionnalités :

- Désactivation des injections de code malveillant.
- Protection des achats effectués avec des cartes bancaires émises par Société Générale.
- Protection de la navigation sur l'Espace Internet des Particuliers (<https://particuliers.societegenerale.fr>)

Société Générale met à disposition de tous ses clients particuliers le logiciel Rapport à l'adresse suivante :

https://particuliers.societegenerale.fr/votre_site/configuration_securite/les_bonnes_pratiques.html

Une fois installé, il est visible à côté de la barre de navigation. Il est compatible avec les navigateurs Microsoft Internet Explorer, Mozilla Firefox, et Google Chrome sous Microsoft Windows ainsi que Mozilla Firefox et Apple Safari sous Mac OS X.



Société Générale n'est pas la seule banque à avoir choisi Rapport. Environ [80 autres confrères](#) se sont déjà associés à Trusteer pour augmenter la protection de leurs clients.

Publié par [CERT SG à 10:25](#)  Recommander ce contenu sur Google

Libellés : [antivirus](#), [malware](#), [rapport](#), [trusteer](#)

[Accueil](#)

[Articles plus anciens](#)

Inscription à : [Articles \(Atom\)](#)

Le contenu de ce blog est la propriété de Société Générale. Modèle Awesome Inc.. Fourni par [Blogger](#).