Magic Lantern. . . reloaded / (Anti) viral psychosis - McAfee Case

Eric Filiol & Alan Zaccardelle

About Author(s)

Eric Filiol is head of research and development at ESIEA and head of the Operational Cryptology and Computer Virology lab at ESIEA Laval. He has spent 22 years in the French Army during which he has conducted operational research in information and system security.

Contact Details : ESIEA – Laval Laboratoire de virologie et de cryptologie opérationnelles 38 rue des Dr Calmette et Guérin 53000 Laval

Email : filiol@esiea.fr,ffiliol@gmail.com

Alan ZACCARDELLE is Security Research Engineer and member of the Operational Cryptology and Virology Laboratory (ESIEA Research). He has participated in the iAWACS 2010 Antivirus challenge and also presented his first Anti-malware conference.

His previous roles included Security log analysis, Anntivirus Architect for Dimension DATA.

He spends his time with his children and searching any ideas in his daytime to bypass or block computer or software security features.

Contact Details : ESIEA – Laval Laboratoire de virologie et de cryptologie opérationnelles 38 rue des Dr Calmette et Guérin 53000 Laval

Email : alan.zaccardelle@gmail.com

Keywords *Security, Analysis, Malwares detection, Virus database signatures, AV detection patterns, Threat statistics, McAfee, FBI, LOPSSI2, Intelligent agencies, Quarantine,*

Magic Lantern. . . reloaded / (Anti)viral psychosis - McAfee Case

Abstract

How far would you trust your antivirus viral database updates? From a security point of view, updates help and continue to enhance your security. Antivirus solutions remain a mandatory component of computer systems as it is updated at least once a day. In this paper we address interesting issue around the confidence we can give to our antivirus. We have chosen to analyze the McAfee antivirus on a technical and reproducible basis. This particular choice is motivated by the fact that this antivirus is widely used and has been suspected of supporting Magic Lantern US intelligence initiative by the press and later by the public opinion.

We intend to address several issues. First we will analyze their protection/detection approach with respect to the 2008 Conficker: even now this threat is not fully detected. Second, we will present McAfee's approach in malware signatures management and updates that could lead to third party access on systems protected by McAfee Antivirus products. We will show on a technical and reproducible basis how the real number of malware is artificially increased thus leading to exaggerated and thus incorrect numbers.

We then show how badly the quarantine process is managed and how to analyze the naming convention in McAfee's Official DAT signature file. This can help users to check new added threats.

Finally, we will explain how your Antivirus and your web browsing can help hackers, Cybercriminals, Organizations, law enforcement, intelligence agencies or even other government entities to gain access in your systems and take what they want.

Introduction

After the 11th of September 2001, the US Government has decided to change its way to fight (Cyber)-terrorism. In the same time, they were facing a major issue: how to bypass authentication mechanisms (password) and encryption, officially of bad guys or citizens living in countries belonging in the Evil axis. How could they access some encrypted data without performing uncertain, time-consuming cryptanalysis attempts? To avoid this time issue, a FBI project code-named "Magic Lantern"[1] has been launched. The Magic Lantern initiative (a part of the CyberKnight Project which is itself a sequel of the former Carnivore/DCS10000 Project) would have been used as a Trojan/Backdoor to circumvent systems and data protections by secretly recording any passphrase and any secret encryption key, then forwarding the confidential data to the feds. There is hitherto no evidence but allegations still exist that McAfee (and other AV vendors) have been contacted by the feds to ensure that the bureau's snooping software is not detected by their products in order not to alert the "culprit".

Since 2001, most Western countries have adopted such approach for national security (fighting against terrorism) or internal security purposes (fight against organized crime). The

[1] http://www.wired.com/politics/law/news/2001/11/48648?currentPage=1 ;
http://www.usatoday.com/news/washington/nov01/2001-11-21-fbi.htm

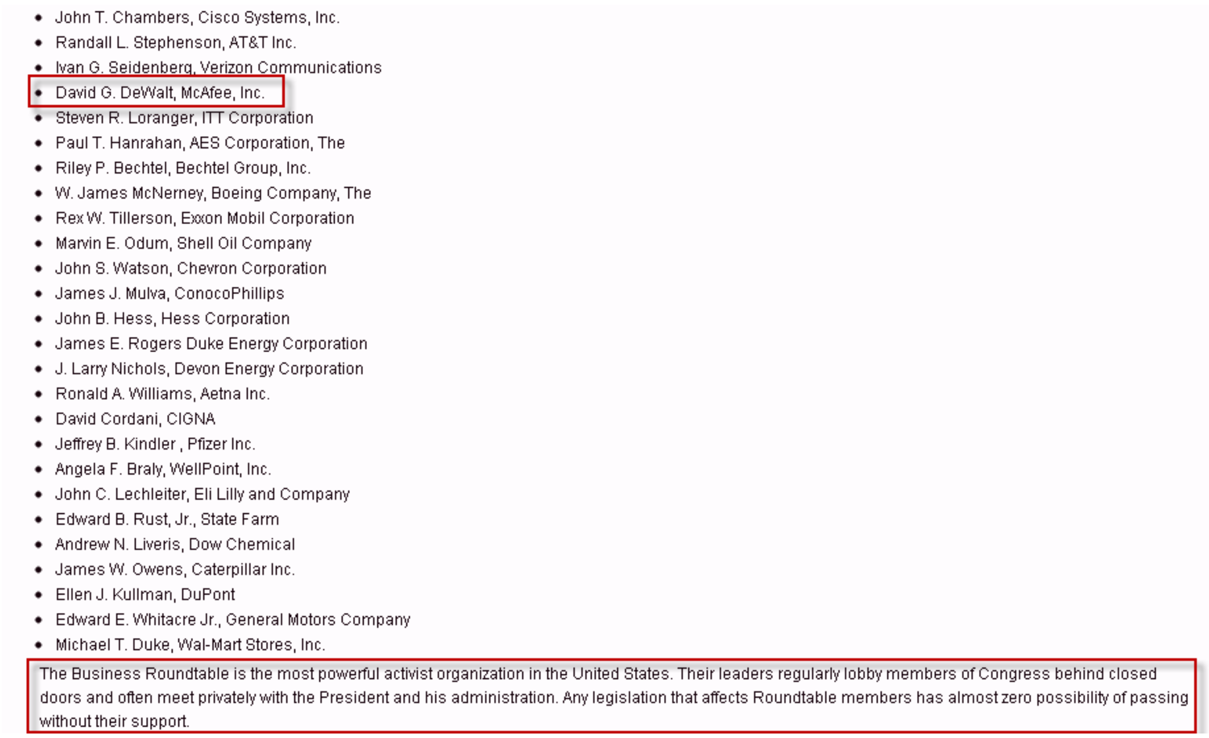
most recent example refers to the LOPPSI2[2] initiative in France. Almost ten years after the Magic Lantern project we are going to add new insights on this fascinating yet worrying topic with our Proof of Concept called “ZouAV” that enabled us to unveil how technically it is possible to enforce Magic Lantern technology.

Another issue arises from the previous one. Why is a well-known, devastating worm like Conficker still not efficiently detected by some prominent antivirus software while a few others have succeeded as soon as the worm has been analyzed?

All those previous issues relate in fact to the following general question: how far would you trust your antivirus viral database updates? From a security point of view, updates help and continue to enhance your security. Antivirus solutions remain a mandatory component of computer systems as it is updated at least once a day.

In this paper we intend to address all those issues technically and operationally. We have chosen the McAfee antivirus software to illustrate our different views. The aim is to not demonize particular software – it is more than likely that a few other products could similarly lead to the same conclusions – but the McAfee case is interesting for many reasons:

- McAfee was one of the two antivirus companies suspected of helping and supporting FBI’s initiative (Magic Lantern, 2001) by modifying their product. In this respect, Figure 0 clearly shows that this AV company is deeply involved in the US and Homeland Security.



- John T. Chambers, Cisco Systems, Inc.
- Randall L. Stephenson, AT&T Inc.
- Ivan G. Seidenberg, Verizon Communications
- David G. DeWalt, McAfee, Inc.
- Steven R. Loranger, ITT Corporation
- Paul T. Hanrahan, AES Corporation, The
- Riley P. Bechtel, Bechtel Group, Inc.
- W. James McNerney, Boeing Company, The
- Rex W. Tillerson, Exxon Mobil Corporation
- Marvin E. Odum, Shell Oil Company
- John S. Watson, Chevron Corporation
- James J. Mulva, ConocoPhillips
- John B. Hess, Hess Corporation
- James E. Rogers Duke Energy Corporation
- J. Larry Nichols, Devon Energy Corporation
- Ronald A. Williams, Aetna Inc.
- David Cordani, CIGNA
- Jeffrey B. Kindler , Pfizer Inc.
- Angela F. Braly, WellPoint, Inc.
- John C. Lechleiter, Eli Lilly and Company
- Edward B. Rust, Jr., State Farm
- Andrew N. Liveris, Dow Chemical
- James W. Owens, Caterpillar Inc.
- Ellen J. Kullman, DuPont
- Edward E. Whitacre Jr., General Motors Company
- Michael T. Duke, Wal-Mart Stores, Inc.

The Business Roundtable is the most powerful activist organization in the United States. Their leaders regularly lobby members of Congress behind closed doors and often meet privately with the President and his administration. Any legislation that affects Roundtable members has almost zero possibility of passing without their support.

Figure 0. McAfee as member of the Business Roundtable (source http://www.alternet.org/economy/145996/the_business_roundtable:_the_most_powerful_corporate_business_club_most_americans_have_never_heard_of)

---

[2] http://www.lemonde.fr/technologies/article/2009/05/18/apres-la-dadvsi-et-hadopi-bientot-la-loppsi-2_1187141_651865.html ; http://www.lexpress.fr/actualite/societe/loppsi-2-les-dictateurs-en-ont-reve-sarkozy-l-a-fait_917757.html

- Purely at random, during the iAWACS 2010 PWN2KILL challenge (iAWACS, 2010), we have noticed strange behaviours in McAfee antivirus that triggered alerts, questions and interesting issues. So the choice of McAfee is just a matter of technical opportunity
- MCAfee is one of the most widely used antiviruses and moreover it is installed by default on most Windows computers sold throughout the world. Considering the McAfee products just give an enhanced scope to a worrying situation.

In this paper, we will not talk about malware techniques to bypass Antivirus protection that are used by Cybercriminals or any other bad guys. There are already a lot of topics around it. In this paper, we address different issues. First we will analyze a curious malware protection/detection approach in a few antivirus products. The case of the 2008 Conficker worm will deeply investigated: even now this threat is not fully managed.

Second, we will present strange and weird ways in malware signature management and updates that could let specific organizations (intelligence, terrorism, mafias) to gain access on systems protected by McAfee Antivirus products. We will focus also a little bit more on World Wide threat dashboard that scores the number of malware detected and their evolution within the next months. We will show on a technical and reproducible basis how the real number of malware is artificially increased thus leading to a malware psychosis.

Third we will describe a way to recover your quarantined files and choose a specific location instead of the original one proposed by VirusScan. We will explain another way to list all virus names from an Official DAT signature file to help you to check new added threats.

Finally, we will explain how your Antivirus and your web browsing can help hackers, Cybercriminals, Organizations, law enforcement, intelligence agencies or even other government entities to gain access in your systems and perform any action they may desire. If the 100% security does not exist it is however possible to limit the risk efficiently. We will propose such workarounds and mitigations to reduce the threat.

Disclaimer - To establish all the results presented in this paper, we strictly used legal tools and approaches, thus complying with the existing laws in France and in Europe. No reverse engineering or equivalent, illegal techniques have been used. Moreover, all information used here is public (and thus can be retrieved by anyone) and do not come from the private or confidential sphere. This enables to reproduce all our results and approach.

The Real Conficker detection

A lot of articles[3] around this threat have been detailed by Security Experts[4] on Internet. We are not going to explain how Conficker infected systems or spread it out on networks; we will just list mitigations that have been proposed by Antivirus companies to protect systems against the infection.
Even if some systems continued to be infected by this threat (due to poor security awareness for some users), we can say that all editors worked closely to fix the worldwide worm.

[3] http://en.wikipedia.org/wiki/Conficker
[4] http://download.nai.com/products/mcafee-avert/documents/combating w32 conficker worm.pdf

- Microsoft[5] has issued a security patch (MS08-067).
- Antivirus Companies updated their virus database signatures to detect Conficker and its variants, in a rather efficient way. But some end users' tasks remain to be protected against that threat totally:
    - Applying last security patches from editors.
    - Using strong password and not guessable ones.
    - Adopting a thorough users' right management (restricted and limited user account rights).
    - Keeping antivirus up to date and regularly perform full scans on their systems to find new virus or variants.

Despite the fact Conficker infection made a lot of buzz throughout the world, its spreading behaviour uses basic propagation means:

- Netbios.
- Removable media (USB).
- Web and P2P protocols.

Its infection vectors are based on three actions through:

- MS08-067 exploit.
- Weak and guessable passwords.
- Autorun mechanism.

This is precisely the last point that we wanted to highlight on the McAfee's poor detection. The Conficker's Autorun mechanism detection is not really operational under certain assumptions and conditions for VirusScan.

We decided to analyze how McAfee Antivirus was dealing with a malicious Autorun files that were used by Conficker Autorun spreading mechanisms. Even if some Autorun files are not dangerous without the dll infection file, it does not mean that your system is cleaned and healthy.

Test success conditions

First of all, the sample has been submitted[6] to the McAfee AvertLabs through its portal and support. The McAfee robots are analyzing every submission with their last products version, engine and virus database signatures. You receive an email with an automatic analysis. Three possible answers can be returned to you from McAfee Labs' robots:

- The current available engine and virus database signatures have not detected your samples. They are considered as inconclusive files and in this case all your files will be followed and analyzed by a Technical Malware Expert analyst.
- Their current Antivirus has successfully detected your samples and McAfee informs you that you should be protected with the last available virus signatures.

[5] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[6] http://vil.nai.com/vil/submit-sample.aspx

- Your samples have been successfully detected but with a specific virus signature. McAfee attaches the specific signature in the email and gives you all steps to follow to apply it and confirm the detection and mitigation.

The last point is also applied once a Technical Malware Expert analyst has confirmed the new threat. In any cases, whenever detection occurs and is validated by McAfee Labs, McAfee includes it, as a “new” signature, in the next official updates.

If the processes have proved its efficiency for years now, it is unfortunately no longer the case as soon as you can check and investigate by your own. Our tested platform runs under Microsoft Windows XP with last Security patches and McAfee VirusScan Antivirus evaluation[7] software up to date (DAT6182 - 29th of November 2010).

Our McAfee Antivirus protection software has been installed with default settings (without any exclusion).
Samples used:

- Conficker sample roetvbvl.dll
    - (SHA-256: 125113537783310410A4A4A04961E0649EF4E55108EF86AF3CCFEE4BE5BF6EFA)
    - (MD5: 466B24FEED3C6897B5623B8E694F5792)
- Autorun sample files (01.inf, 02.inf, 03.inf, 04.inf, 05.inf, 06.inf, 07.inf, 08.inf, 09.inf, 10.inf, 11.inf, 12.inf)
    - (SHA-256: 7611738317DABE43DAEEB0B45698C0E37ECFD546D29761A63E57DD779984589B)
    - (MD5: 466B24FEED3C6897B5623B8E694F5792)

Any VirusTotal[8] reports are not validated from Antivirus Editors’ point of view. Their answers and detections belong to them and end users should trust them instead of using such of un-controlled web services based on Antivirus malware detections. For antivirus vendors, VirusTotal’s results cannot be proved and verified but we are going to show some tests that will help and support our point of view.

The first file has been detected as Conficker and erased by the McAfee Antivirus. But if we scan those autorun files without any changes, the Conficker detection does not occur. It is this point that we will address and describe.

Conficker Autorun files vs other Antivirus solutions

VirusTotal’s report tells that 36/40 Antivirus detect the threat. It has been detected as Conficker. We will focus on the McAfee detection because it is detecting it but not as it should and this is why VirusTotal’s reports have to be read carefully. In fact McAfee detects the autorun files as W32/Conficker.worm!inf[9] . Let us verify why McAfee does not detect it as it should do.

---

[7] https://secure.nai.com/apps/downloads/free evaluations/
[8] www.virustotal.com
[9] http://vil.nai.com/vil/content/v_153724.htm

Analyzing files with the last available DAT 6188

To conduct a full analysis, the antivirus will start an On-Demand scan, on the directory where those INF files are stored. Those files are real Conficker autorun files but how can we explain that McAfee cannot detect them even with the last available DAT6188. An On-Demand scan will not detect either Conficker threat (see Figures 1, 2 and 3).

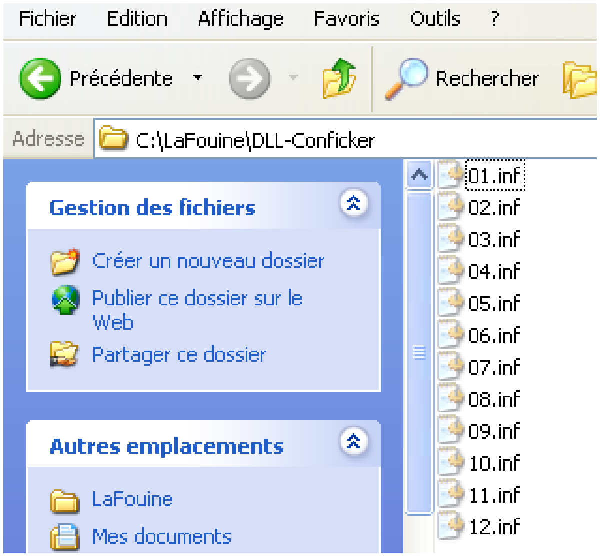


Figure 1 All INF file autorun files

Characteristics -

This is a generic detection for a configuration text file (autorun.inf) used by the W32/Conficker.worm. This file is usually dropped onto the root of all removable drivers and mapped drives in an attempt to autorun an executable when the drive is accesed.

The size for this file varies.

Some copies of this file has the System (S) and Hidden (H) attributes present in attempt to hide the file from certain, default, viewing options within Windows Explorer.

The contents of the file are similar to the following:

....Garbage......

shelLExECUte=RuNdLl32.EXE .\RECYCLER\S-x-x-xx-2819952290-8240758988-879315005-xxxx\jwgkvsq.vmx,ahaezedrn

.....Garbage....

Upon Autorun being initiated the file is executed and infection occurs, because this infection is instigated locally the worm does not need to exploit ms08-067, so having applied the patch will not stop the infection.

Figure 1 Conficker Autorun.inf threat description from McAfee Website

File name: 01.inf
Submission date: 2010-12-05 23:52:26 (UTC)
Current status: finished
Result: 36/ 43 (83.7%)

not
Saf

Compact

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.12.06.00	2010.12.05	Win32/Conficker.worm
AntiVir	7.10.14.191	2010.12.05	Worm/Kido.IX
Antiy-AVL	2.0.3.7	2010.12.05	Worm/Win32.Kido
Avast	4.8.1351.0	2010.12.05	BV:AutoRun-S
Avast5	5.0.677.0	2010.12.05	BV:AutoRun-S
AVG	9.0.0.851	2010.12.05	Worm/Generic_c.ZS
BitDefender	7.2	2010.12.05	Worm.Autorun.VHG
CAT-QuickHeal	11.00	2010.12.04	-
ClamAV	0.96.4.0	2010.12.05	Worm.Autorun-2191
Command	5.2.11.5	2010.12.05	JS/AutoRun
Comodo	6960	2010.12.05	NetWorm.Win32.Kido.~ir
DrWeb	5.0.2.03300	2010.12.06	Win32.HLLW.Autoruner.5601
Emsisoft	5.0.0.50	2010.12.05	Net-Worm.Win32.Kido!IK
eSafe	7.0.17.0	2010.12.05	-
eTrust-Vet	36.1.8018	2010.12.05	INF/Conficker
F-Prot	4.6.2.117	2010.12.05	JS/AutoRun
F-Secure	9.0.16160.0	2010.12.05	Worm:W32/Downaduprun.A
Fortinet	4.2.254.0	2010.12.05	INF/Conficker.EM!worm
GData	21	2010.12.05	Worm.Autorun.VHG
Ikarus	T3.1.1.90.0	2010.12.05	Net-Worm.Win32.Kido
Jiangmin	13.0.900	2010.12.05	Worm/Kido.ahn
K7AntiVirus	9.70.3162	2010.12.04	Trojan
Kaspersky	7.0.0.125	2010.12.05	Net-Worm.Win32.Kido.ir
McAfee	5.400.0.1158	2010.12.06	-
McAfee-GW-Edition	2010.1C	2010.12.05	-

Figure 3 Autorun file detected as Conficker on 2010-12-05: DAT 6188

When McAfee Conficker's Autorun really occurs

In fact, the only way to let VirusScan detecting and removing Conficker autorun is to rename the files. It was written in their Conficker's web page description:

.....Garbage....

Upon Autorun being initiated the file is executed and infection occurs, because this infection is instigated locally the worm does not need to exploit ms08-067, so having applied the patch will not stop the infection.

Figure 2 Autorun description from McAfee Conficker's threat webpage

Here, we can read 'autorun.inf' that means Conficker threat can be activated by an autorun file. But those files are really autorun files but we have just named them differently.

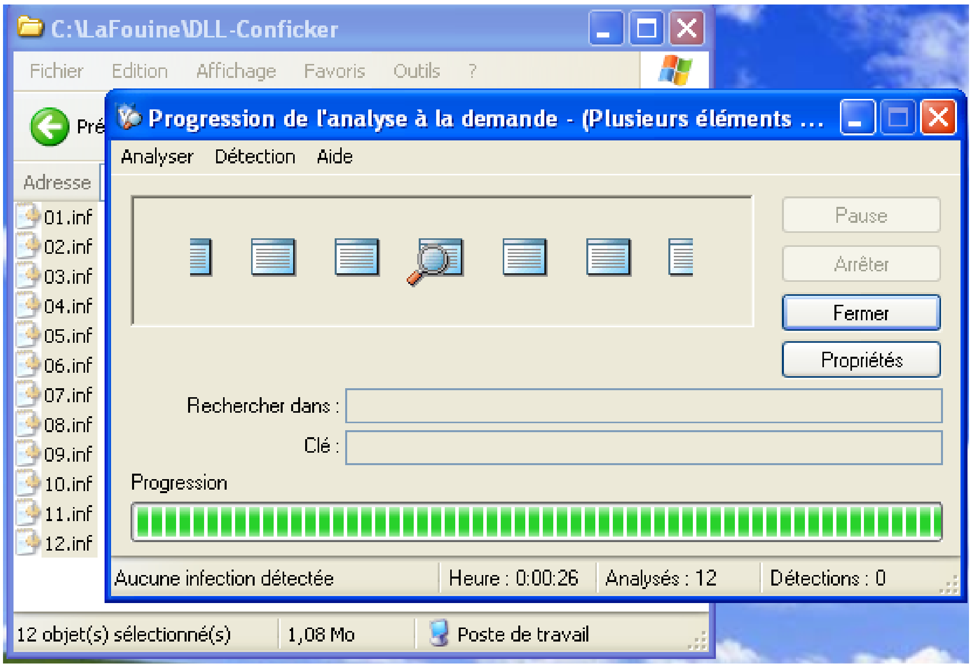


Figure 3 Undetectable conficker INF files

But, if the user renames a file into autorun.inf, McAfee VirusScan will be able to detect it and remove it.

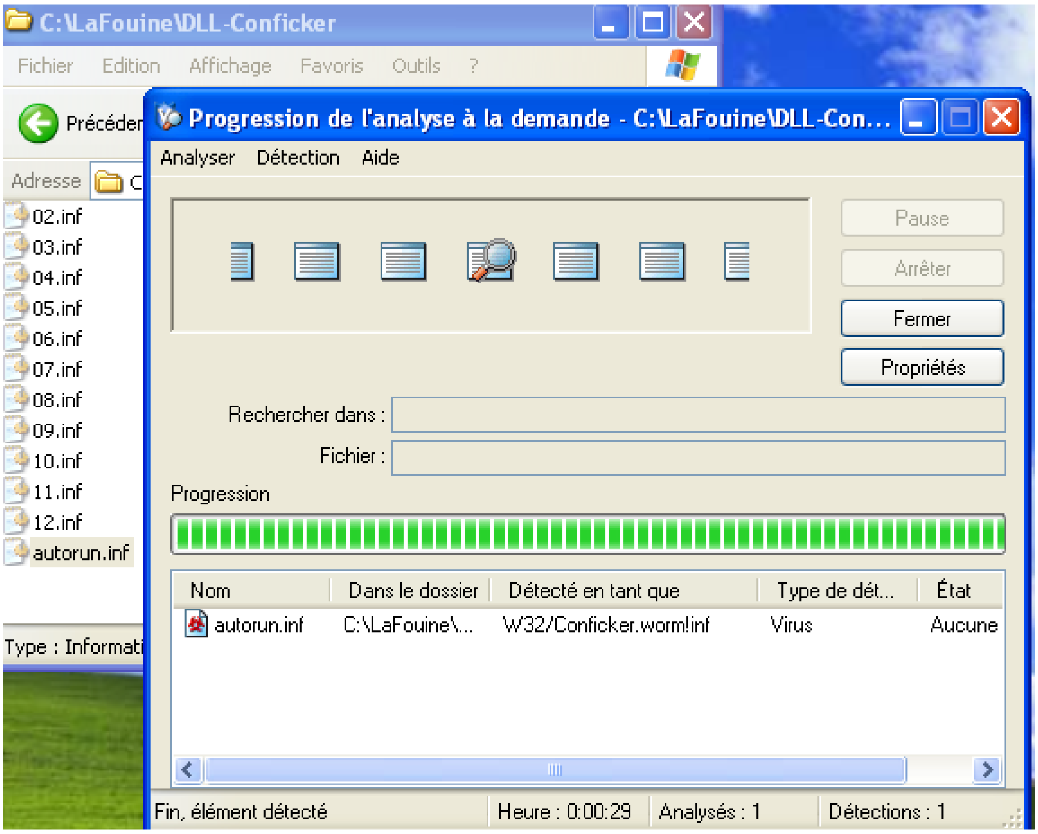


Figure 4 Detection of Conficker in Autorun occuring

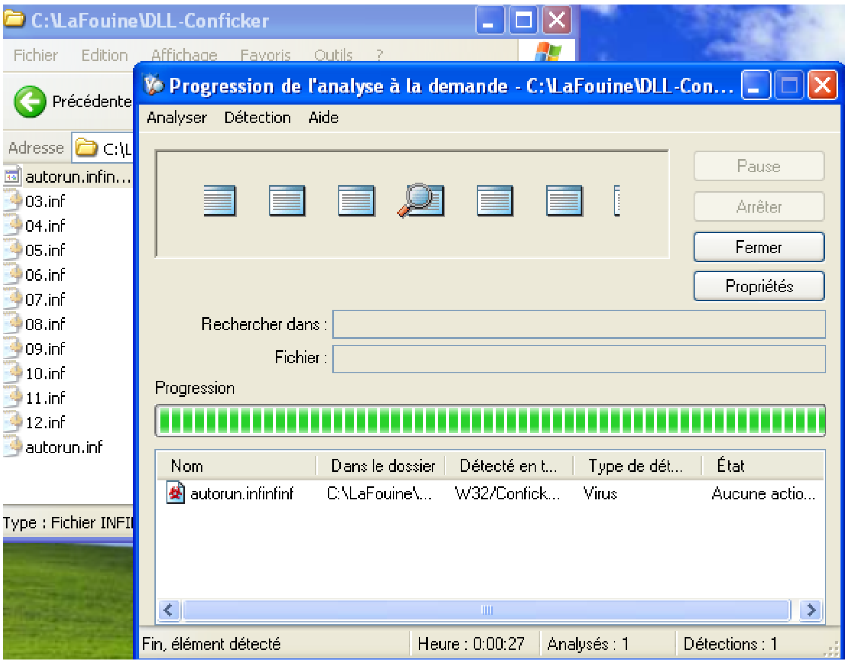


Figure 5 Conficker in autorun file detected in autorun.infinfinf

Even if the file is renamed as 'autorun.infinifinf', McAfee VirusScan still detects Conficker.

Same files from AVG Antivirus Analysis

They were all detected and removed as soon as they copied on a disk.

Figure 6 AVG Detection occurs on an un-conventional autorun.inf file

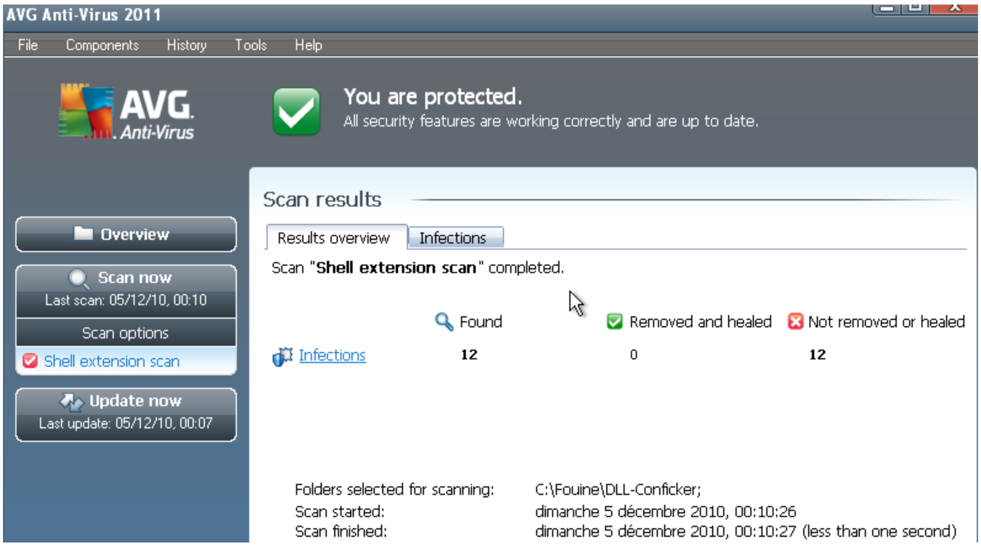


Figure 7 AVG Full detection

McAfee Autorun Parsing errors ?

It seems that McAfee Antivirus software protection makes some heuristics priorities in their autorun analysis. If a malware infection uses the most common autorun.inf file based propagation, it would have chances to be detected by McAfee. But if it uses an un-conventional name for autorun file, it would start successfully if VirusScan is installed on the system ;)

In fact, McAfee scans files and compares it to a pattern [autorun.inf] for autorun files analysis. No matter behind the [inf.] extension, VirusScan will be able to detect the threat. But now, if you rename the same file into autorun.toto or autorun.toto.inf, McAfee's Antivirus software protection won't be able to detect it (to believe that their threats analysis are based only on this [autorun.inf].* pattern]

Conficker Autorun worms and the Worldwide Top 5 Malwares Statistics

If you read McAfee Annual Threats reports[10] (Q1 2010), *(especially 'Malware Growth Remains 'Healthy' on page 11-12)*, McAfee analyzes on one of their most active category of malwares that are described as Autorun worms and belong to the Worldwide Top 5 Malware.

Two of them *(Malware Generic.dx and W32/Conficker.worm !inf)* are on the Top 3 of their list. Is it a surprise? Well, it should not as long as systems still infected with no antivirus protection, but from our point of view, it is a particular strange report. Generic.dx *(Generic downloaders and Trojans)* and W32/Conficker.worm!inf *(Removable-device Conficker worm detection)* have both been analyzed in our paper. Even if the Conficker autorun threat is not really detected as it should *(parsing error)*, it would have taken at least the first or the second position of this Worldwide Top 5 list.
For the *Generic.dx* threat, we have proved that for *ZouAV* example, McAfee detected it in three different categories. This means from our first analysis, 2/5 of the worldwide malwares

[10] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2010.pdf

are wrong or not ordered.

It could be subjected to discussions if McAfee had just reported this threat for the first Quarter of 2010, but our analysis still works for Second [11]and Third[12] Quarter of 2010

Traditional and "McAfee's Smart removal of autorun.inf"

After detailing some weakness or error detection files Autorun.inf Conficker we fall accidentally on an article at least a little more interesting that could explain the error. Indeed, a recent article[13] summarizes well the proliferation of viruses via removable media and the fact that Microsoft still has not corrected the default disabling autorun (Autorun.inf). *(last update from Microsoft Patch Tuesday 8th of February 2011) ; Microsoft decided[14] to disable the autorun feature in its Operating systems*

But what attracts our attention is when McAfee praised on its so-called *Intelligent* detection of Conficker infection with respect to Autorun.inf files. Indeed McAfee exposes the very simple techniques introduced by some antivirus companies that fail to detect the strain with checksum or simple logic-based string detection. Indeed, the example is very well explained and it is understandable that hackers have also implemented more sophisticated algorithms to counteract this type of analysis.

But the most interesting is when McAfee starts to present its own implementation on the detection of Conficker and its autorun file. Whether at the standalone host antivirus level or at it cloud version level, the problem seems to persist despite the famous flowchart. The autorun.inf file should be a mandatory autorun resource to be dangerous? It is a question that our results do not seem to have been treated.

Let us now explore the "performance vs security" issue. McAfee had made the announcement several months ago. It is now official: the new version of McAfee (VirusScan 8.8) is available[15] since January 22, 2011 for corporate uses. McAfee has mainly concentrated on optimizing the performance with respect to the on-demand scanning but also with respect to its the real-time analysis. If you believe in this marketing ploy, it should actually change our lives with the analysis of hard disks that never ended, the loading time of the engine and signatures to scan a file. In short, a significant advance according to McAfee and to AV benchmarks between that will appear in the coming weeks.

Despite all these new developments, we again see that basic security is still not here. We have done tests with our Conficker autorun.inf files. Even if the files are scanned and while they are not detected -- when they are not named autorun.inf -- McAfee has chosen not to analyze them from the moment they had been "tagged" as being healthy and sound.

Just copy the infected file under a different name (e.g. toto.inf), perform a scan or just wait

---

[11] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2010.pdf
[12] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2010.pdf
[13] http://www.mcafee.com/us/resources/white-papers/wp-rise-of-autorun-based-malware.pdf
[14] http://blogs.technet.com/b/mmpc/archive/2011/02/08/breaking-up-the-romance-between-malware-and-autorun.aspx
[15] https: / / kc.mcafee.com / resources / sites / MCAFEE / content / live / PRODUCT_DOCUMENTATION/22000/PD22973/en_US/VSE% 208.8% 20 -% 20What's% 20New.pdf

until it is scanned in real time and then rename it to autorun.inf, it will no longer be analyzed until the next update of the signature database. This can pose serious security problem from users’ perspective. We have performance but no longer security! Our example is a particular case of what can be called the``autorun.inf detection bug’’ but it may happen that other people can find a way to play with the McAfee Antivirus cache as we have done with MITM attacks and cache poisoning attacks.

Wake up! Wake up!

In this section we are now explaining how an attack against McAfee protected systems could easily consists in waking up sleeping virus from their quarantine. The reason lies in the fact that the quarantine algorithm is surprisingly weak and lame.

Depending on the end user’s Antivirus configuration, an infected file may be blocked or deleted when the infection occurs or when the antivirus detects the threat during an On-Demand Scan. To avoid any fault detection issues (false positive), McAfee as other Editors move infected files into a quarantine directory. As soon as they are moved, the original file is ”encrypted” by McAfee Antivirus product and stored in an undocumented way in order to be used only by Avert Labs for analysis through dedicated McAfee users’ support or to avoid any threat infection from quarantine files. A user may choose between:

- Restoring the infected file (to its original location).
- Rescanning the file with new DAT signatures.
- Deleting infected file from the Quarantine.
- Sending the file to the McAfee Labs for further analysis.

Quarantine algorithm

Whenever a suspected threat occurs, McAfee VirusScan product ’encrypts/encodes’ the original source and creates also a report file ’details file’ with all information that are needed for:

- The Antivirus Quarantine Management (to display threat infection to the user).
- For user in case of restoration.
- Or for McAfee Labs internal analysis whenever it is submitted.

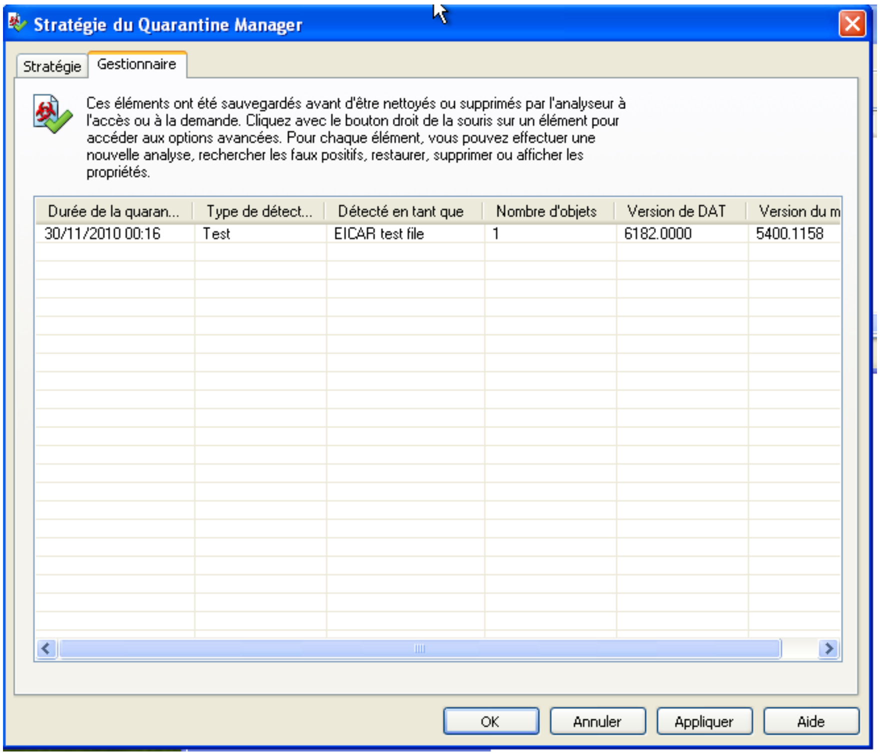


Figure 8 Quarantine GUI from VirusScan

Two files are created on threat occurence:

- Details (Detection time, engine and virus signature, product ID, file. . .
- File0 (the virus)

Information available in the Details file with an EICAR test file

```
[Details]
DetectionName=EICAR test file
DetectionType=6
EngineMajor=5400
EngineMinor=1158
DATMajor=6182
DATMinor=0
DATType=2
ProductID=12072
CreationYear=2010
CreationMonth=11
CreationDay=30
CreationHour=0
CreationMinute=16
CreationSecond=43
TimeZoneName=Paris, Madrid
TimeZoneOffset=-60
NumberOfFiles=1
NumberOfValues=0

[File_0]
ObjectType=5
OriginalName=\\?\C:\LaFouine\eicar.com
WasAdded=0
```

Figure 9 Details file from a BUP Quarantine file

Those two files are not available, as it is been described above. McAfee has chosen to hide them by encoding and compressing them. We are going to explain how it is possible to recover all quarantine files and restore them to a chosen directory and not the original location as VirusScan proposes to you. It is precisely what a malware could do easily, of course for malicious purposes (e.g. DoS through massive quarantined files reactivation).

Quarantine’s encryptions

Despite of some advanced detection features from McAfee’s point of view, they have implemented a very simple and basic encryption algorithm to secure virus sample in its quarantine process. The encryption is based on a single XOR with a ’6A’ key.
But before ’Xoring’ Details or file 0 files, we need to extract all files from the BUP file use 7Zip[16] to uncompress the quarantine BUP file.

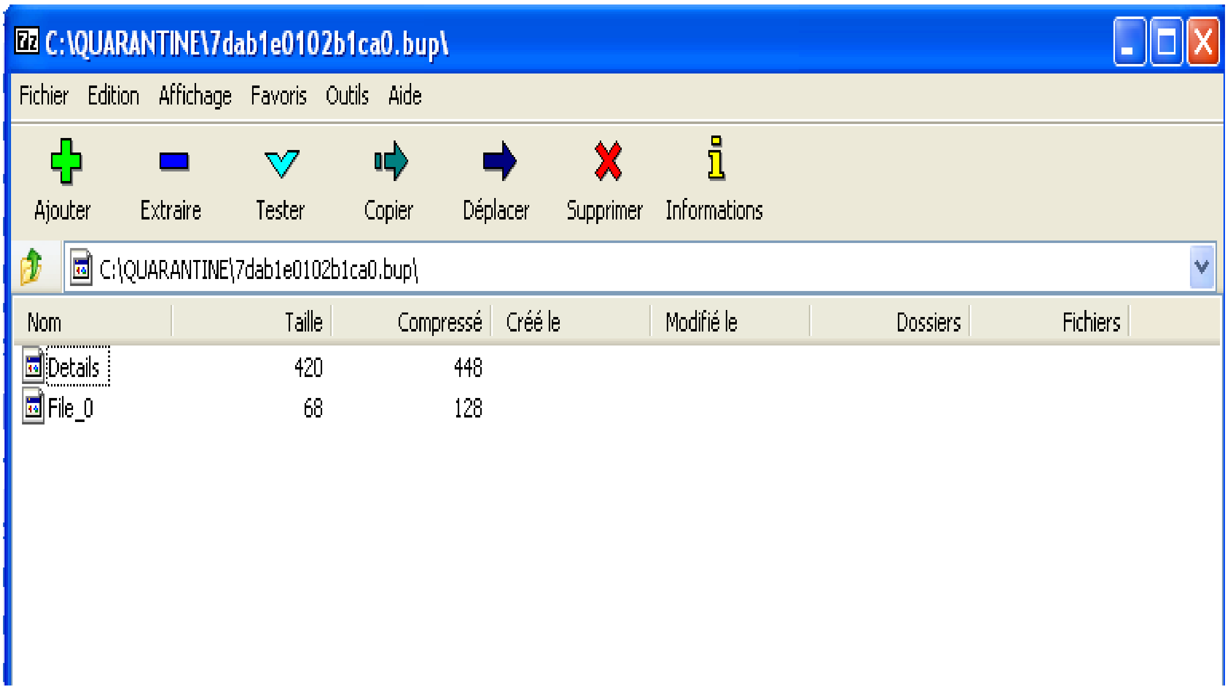


Figure 10 BUP file contents

In our example, the BUP file is composed of two files (Details & file 0). In a case of multiple threat detections, we can have more than two files (File 0, File 1, File *). It usually applies whenever a specific threat modifies the registry base, in this case VirusScan will put the registry key in a file. Recovering the key is more than easy: just xor the original file and the ”encrypted” one and you get the McAfee VirusScan Quarantine Key.

Decrypting BUP contents

We’ve used the Hexadecimal editor to manipulate the original file Details and modifying it by xoring each byte with the recovered 6A key.

[16] www.7-zip.org

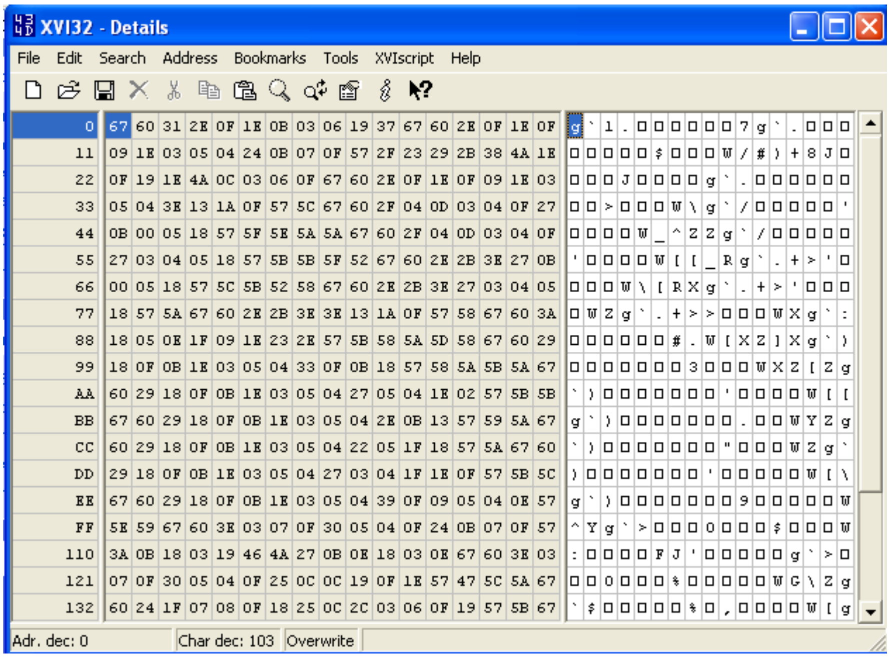


Figure 11 Original Details file

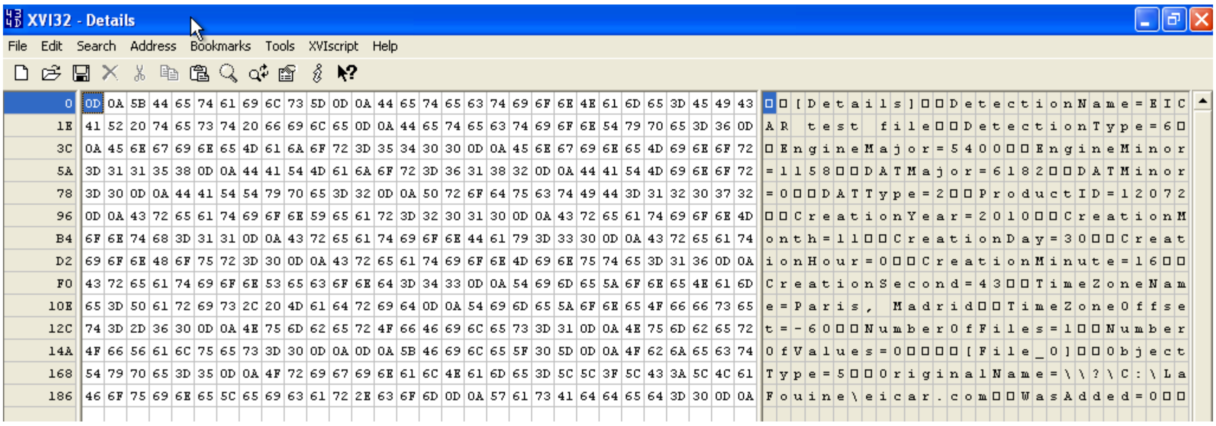


Figure 12 Decrypted Details file

The decrypted file gives all information that is used by McAfee in its Quarantine VirusScan interface (File's name, Database virus signature that has detected the threat, detection time,). Let us see now if the decryption Key works with the File 0 and restore the virus with a different name.

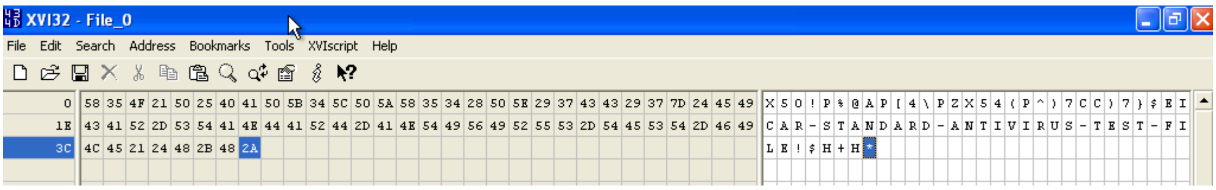


Figure 13 Decrypted File_0

Now, it is possible to save the file and restore it to a directory other than its original. During our test, we kept our Antivirus activated to see if it will be able to detect it.

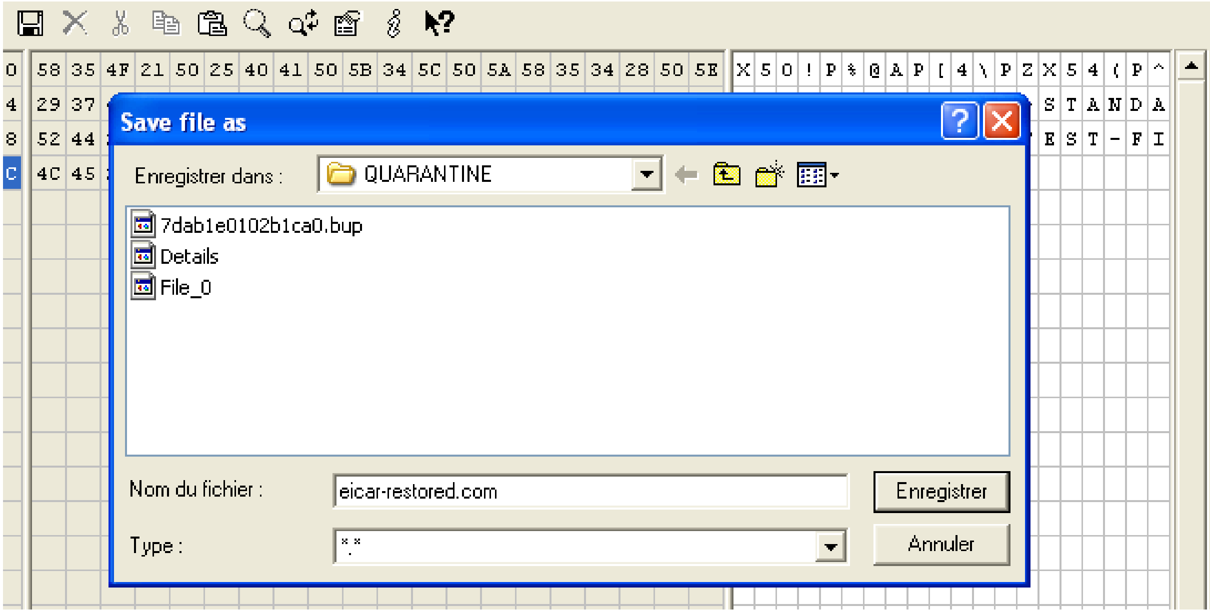


Figure 14 Restoring Quarantined threat

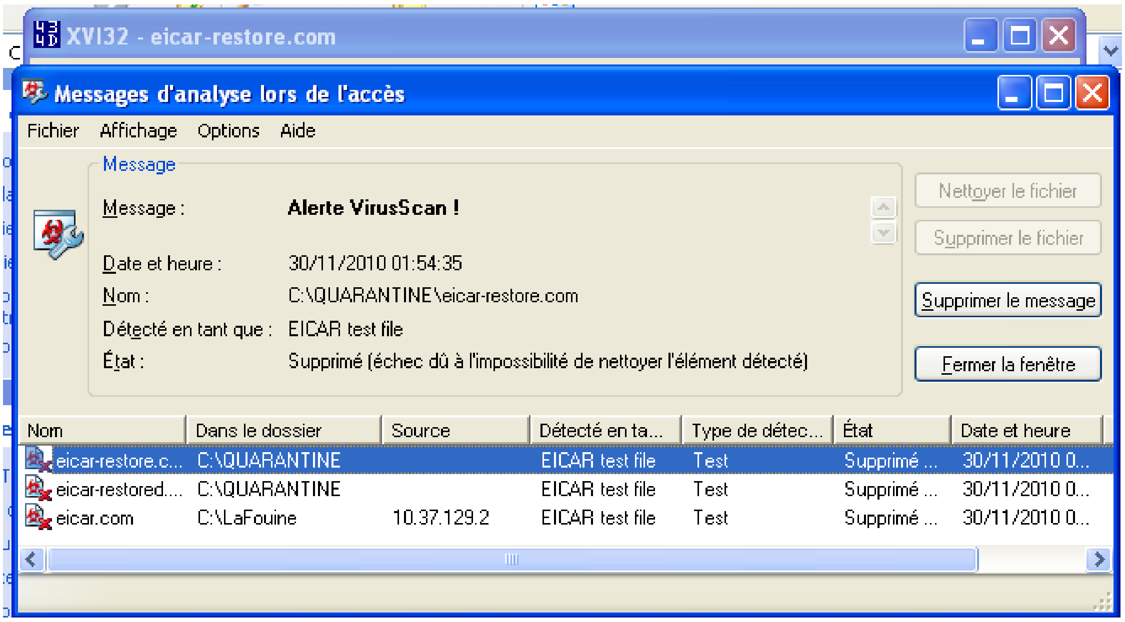


Figure 15 Restored Eicar file / VirusScan detection

Our restored/saved Eicar sample is detected again by VirusScan, it is a normal result but we could make a Denial of Service Attack by looping our script to fill the whole user's local drive (usually the system drive). In the other side, what happens if the system is managed by McAfee ePolicy Orchestrator? The Antivirus database will be filled by threat events and Administrators will detect alerts as if they were under virus attacks. Finally, a new threat could wake up all local malware by exploiting this attack in order to complicate its detection itself (masquerading its own behaviours).

Magic Lantern reloaded or McAfee's Fascinating Virus Database signature management

We are now going to investigate the way McAfee manage its malware databases and the malware detection patterns. Everything started from a PoC used during the iAWACS 2010 PWN2KILL challenge (iAWACS, 2010) and from the strange recurring behaviour of McAfee detection. This PoC is named ZouAV. Its purpose was intially to demonstrate that it was possible to design Microsoft Office macro viruses that are able to infect mis-configured VirusScan-protected computers (too permissive exclusions).

ZouAV is in fact a Trojan horse generated from the Metasploit framework. ZouAV code has been never released before the challenge (which occurred on May 8th, 2010 in Paris). After it, the code has just been communicated to the French CERT-A (which is part of the Prime Minister Office dedicated to the National Computer Security). The first detection[17] by McAfee occurred in February 2nd, 2010 with the DAT5849 under the malware name "Downloader-CCK".

We then submitted the same binary file of ZouAV to McAfee's detection for different DAT files. We obtained the following and surprising results:

- ZouAV code is no longer detected in DAT5980 (May 3rd, 2010).
- From DAT5980 to DAT6002, no détection
- Detection again with DAT6003 but under the new name "Generic.dx!swz"[18]
- When submitting the same code to VirusTotal analysis, McAfee detect it immediately but under a third name "Swrort.a"[19]. This detection is confirmed with DAT6035.

What to think from these strange results: one malware and three different alerts? Let us now perform detection pattern extraction for each of this database. We use the black-box technique presented in (Filiol, 2006). Here are the results (ZouAV code size is 37887 bytes):

- DAT5902. Detection pattern size 28. Pattern byte indices (in ZouAV code) 0, 1, 60, 224, 225, 228, 229, 230, 244, 246, 257, 305, 309, 489, 493, 508, 511, 512, 513, 514, 515, 516, 517, 529, 569, 605, 628, 631. Detection name: Downloader-CCK
- From DAT5980 to DAT 6002. No détection
- DAT6003. Detection pattern size: 29,013 bytes. Detection name: 'Generic.dx!swz'.
- DAT6035. Detection pattern size: 6,300 bytes. Detection name : 'Swrort.a'.
- DAT6176. No detection while the three previous detection names are still recorded in the DAT as shown in Figures below (except Downloader.CCK which has been renamed as 'Downloader-CCK!a'). Let us note that the name extraction from DATs has been performed by McAfee tools: it consists in using the VirusScan Command line tool with the /VIRLIST argument. Very strangely, if we perform a command-line detection (not very easy for end-users with technical background) with default arguments, then the ZouAV file is detected as 'Swort.a'

[17] http://vil.nai.com/vil/content/v 251957.htm
[18] http://vil.nai.com/vil/content/v 267642.htm
[19] http://vil.nai.com/vil/content/v 267753.htm

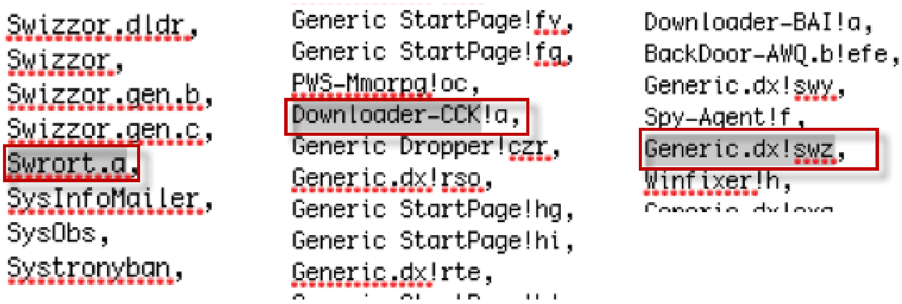


Figure 16 Virus name extraction from McAfee DAT6176 (extract)

- McAfee Antivirus 2011 (full version) does no longer detect the ZouAV binary

The black box extraction clearly confirms that the same code has been produced in McAfee viral database, three different entries with three different signatures (detection patterns).

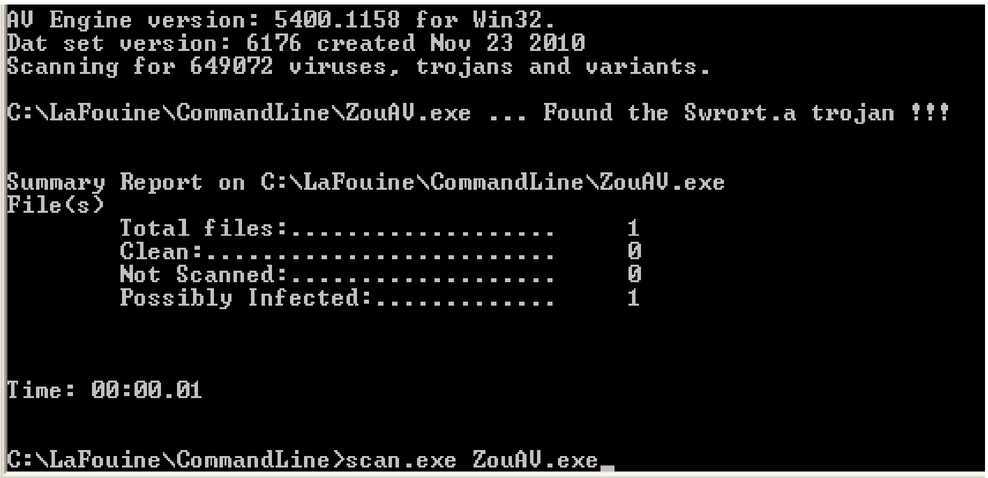


Figure 17 ZouAV detection by McAfee command line scanner

Results' Discussion

For fairness purposes, we have performed the same detection experiments using VirusTotal. Our file has been successfully detected by most of the antivirus products (except McAfee and a few famous other ones).

Then we have contacted and sent the ZouAV file to McAfee technical support. They did not wish to confirm and explain those issues and these strange results. Except that a few days later, the next McAfee's DAT (DAT 6003) released worldwide was indeed able to detect the ZouAV file (but still undetectable with their last antivirus version – Corporate and public)
From a more general point of view, how many malware are concerned with the same situation (one file detected as many names and patterns)? Is it an intended situation and management or just a bug and a worrying inability to manage things thoroughly and seriously? It is clear that

the marketing message hammered to users by McAfee and others about ’60 000’[20] new malware per day must be tampered. But how many in reality?

Magic Lantern reloaded and other avatars (e.g. LOPPSI2)

When considering this intended or not issues, it sheds a new light on the way security or police forces – or worse, bad guys – could exploit them. Instead of using and installing real bugs or spying software – which could betray police actions and thus incriminate their implications – it is far more interesting to use the fact that a given Trojan horse is temporarily removed from a series of viral databases. Somehow it would be like using ’Malware off-the-shelf’ (MOTS).

It is a well-known fact that cybercriminals are very well organized and that they are able to adapt very quickly. Let us imagine that a mafia group intends to seize control over a target company. Using a – modified or not – Trojan horse which is out-of-scope of the antivirus for a few weeks, enable to mount an economic intelligence operation very easily. It is also possible to spy any personality with power: company CEOs, journalists, union leaders, decision-makers . . . without forensics capability who is really behind the attack – contrary to the potential risk with respect to an on-purpose, homemade malware.
The question is: how easy it is possible to identify companies or targets which uses McAfee (or any particular AV software)? Very easy indeed! Even if antivirus vendors guarantee the confidentiality of their clients, it is nonetheless very easy to get that information. Aside our “friend” Google and any classical intelligence tool and trick, using the simple customers’ support webpage can provide a lot of information about a possible target. To do that it just suffices to look for the way McAfee’s clients (from simple home users to big companies) are sending collected data during any malware incident. A simple search on Google (’Upload McAfee file’) enables to get a lot of data and information[21]

For example, in the following example:

/incoming/jdoe/1-212345678

It shows that jdoe is the user name. During a few minutes search, we managed to find a lot of McAfee’s clients through simple Google requests: Dell, Generali, Logica, PWC, UBS, Adobe, Laposte, HSBC, IBM, HP, Renault, Thales, Total. . .

Conclusion

In this paper we have shown that we must be very careful with McAfee’s marketing arguments and probably a few other AV vendors. Antivirus software is a huge world market place with a lot of money to make. If the threat is indeed real, we must maybe ask ourselves whether it is not exaggerated. Building a security policy with respect to malware attacks is difficult and requires a lot of confidence in the actors who are supposed to protect us. Users to their broadest definition are not just blind and mute consumers that have just to pay. It is

[20] http://blogs.mcafee.com/mcafee-labs/malware-at-midyear-a-summary; http://blogs.mcafee.com/mcafee-labs/i-say-we-are-detecting-between-400-000-and-10-000-000-malware
[21] https://kc.mcafee.com/corporate/index?page=content&id=KB50534

probably time to create an independent (European) agency whose role would be to record any different malware and verify some of the marketing claims.

The second point is that any weakness and attempt ’to play’ with security will be inevitably exploited by bad guys. When considering Magic Lantern-like projects, the only problem is now to have a good definition of what is a bad guy.

Bibliography

Filiol E. (2006), Malware Pattern Scanning Schemes Secure against Black-box Analysis. In: *Proceedings of the 15th EICAR Conference*. The extended version has been published in *Journal in Computer Virology*, EICAR 2006 Special Issue, Vol. 2, Nr. 1, pp. 35-50.