AFTERMATH:
CRAFTS AND LESSONS OF INCIDENT RECOVERY
JUNE 28-JULY 3, 2009
HOTEL GRANVIA
KYOTO STATION, KYOTO, JAPAN
21st Annual FIRST Conference KYOTO June 28-July 3, 2009

New Developments on Brazilian Phishing Malware

Jacomo Piccolini
Security Academic Coordinator
Brazilian Research and Academic Network – RNP
Educational Team – ESR
www.esr.rnp.br
jacomo@rnp.br

Escola Superior de Redes RNP

Content removed from public version.

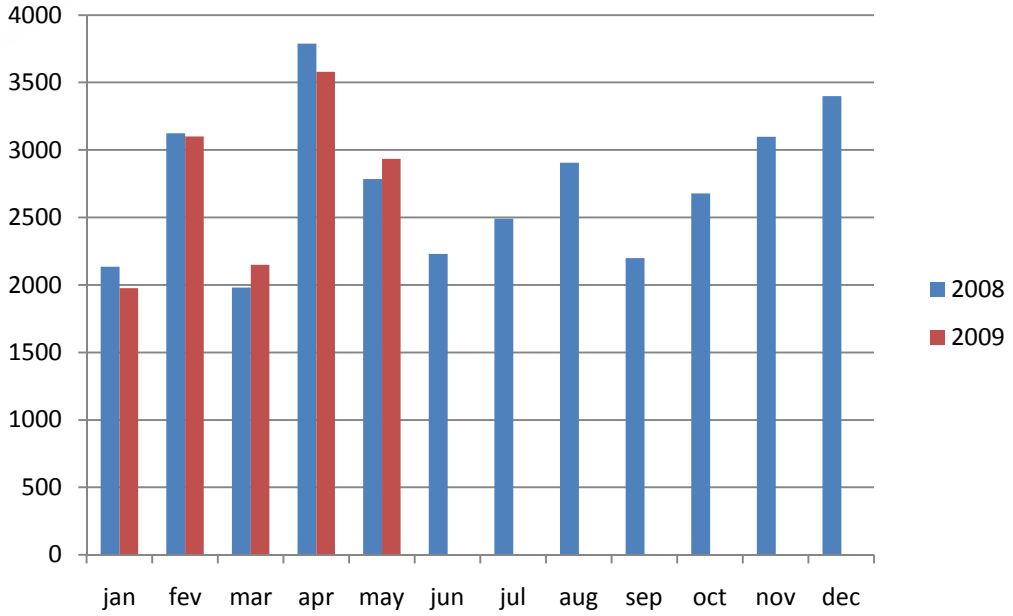
Content removed from public version.

From 2008 to 2009: where do we stand?

Facts:

- same number of malware circulating
- same theme exploration (news)
- same spreading technique (spam)
- same demographic (users)
- carnaval/vacations/taxes cycle

- Big differences from source code with Java, C++ and decrease on usage of Delphi, Visual Basic



- New techniques, we will see some malware cases!

Malware 1 – Simple and efficient and still deadly

Simple malware that add entries on windows host file:

Content removed from public version.

Not a space rocket science malware, but the problem is that Virustotal had this on database on **26-Jan**-2009 and the phishing sites were online on **12-Apr**-2009.

Malware 1 – Simple and efficient and still deadly

This raises some questions:

"Why the sites were on-line for so long?"

"Why no one reported this?"

"Are we relying only on AV detection?"

Malware 2 – Information is **power**

INFOSEG is a Brazilian government database with information of all citizens, and is used by law enforcement, department of justice and miscreants ☺

This is not the web site, it's the malware overlapping the page to collect access information.

This database have all information about citizens, telephone, banking, cars, id's. And a username/password is available for U$ 1,000 (tv report)

Post on AvertLabs blog from Guilherme Vênere

http://www.avertlabs.com/research/blog/index.php/2009/05/01/a-closer-look-at-a-swine-flu-spam/

Malware 2 – Information is **power**

video source: SBT news

Malware 3 – BHO

Malware acting as an Internet Explorer BHO (*Browser Helper Object*)

O2 - BHO: (no name) - {ECB58DB3-53F9-4E39-94E4-122E940F6FDE} - C:\WINDOWS\system32\blbho.dll

Virustotal detection rate was 0

More difficult to detect (user perspective) no process (process explorer you can see the dll loaded on iexplorer.exe)

Proxy to a single IP all banking requests:

Content removed from public version.

Then redirect to another site where the phishing site was (for 6 weeks)!!

Malware 4 – Ransomware is all about Money

Like everything it starts with a simple message:

Assunto: Olá, estou te enviando meu convite de formatura com local, data e hora

CONVITE

Olá, estou te enviando meu convite de formatura com local, data e hora.

Conto com sua presença.

Nos encontramos lá,

Abraços...

Anexo:

ConviteFormatura.pps (52KB)

Once the malware runs on the user system it start to block the following files and applications:

Microsoft Word Microsoft Excel Notepad Visualizador de imagens e fax
Photo_Lightweight_Viewer Galeria de Fotos Meus Documentos Editor do Registro
PowerPoint Minhas imagens Calculadora Configurações do sistema
Gerenciador de tarefas Paint Minhas músicas Windows Media Player
Windows Live Messenger Adobe Reader/Acrobat

Malware 4 – Ransomware is all about Money

Once the user tries to open a “blocked” file it will be shown the following popup:

“error on windows module version 4817.3812 (32 bytes)”

Once you click on the “click me” button you were sent to an “Antivirus Company”

Malware 4 – Ransomware is all about Money

www.byteclark.com.br

This company offers the “solution” to the infection at U$ 10,00 . You can download a vaccine to clean your infected computer.

Malware 4 – Ransomware is all about Money

"The antivirus" running…

According with ARIS-LD the site was registered in Brazil on 12-April-2009 and this fraud was reported by LinhaDefensiva on 05-May-2009 and two days latter it was canceled by Brazilian registrar Nic.br

The name used to register the domain ? "Luiz Trojahn" yeah, right! ☺

Malware 4 – Ransomware is all about Money

The malware locks the files and applications through a "*GetActiveWindow"* call; it does not encrypt the files.

One curious fact, to pay for the vaccine the site provided a real account on a Brazilian bank. How hard it was to the law enforcement do find the guy? ☺

Content removed from public version.

Malware 5 – Not a malware but we need to mention (dns poisoning)

On 11-April-2009 (Sunday) one of the biggest ISP in Brazil suffered a dns poisoning and all traffic to a single bank was diverted to a phishing site.

Content removed from public version.

This issue was solved in 7 hours!

Brazilian initiatives – Linha Defensiva (defensive line)

www.linhadefensiva.org

Linha Defensiva is a community blog that deals with end-users infections, acts as a CSIRT team (ARIS-LD) and also provide a anti-malware tool (bankerfix)

Fabio Assolini
fabio @ linhadefensiva.org

Brazilian initiatives – Malware Patrol

www.malwarepatrol.net

Site managed by Andre Correa provides blocking lists to many applications, like mta, proxy and dns.

andre @ malware.com.br

Brazilian initiatives – Malware Patrol

Great information from Andre Correa, those malware are still on-line after 4 years:

Content removed from public version.

Brazilian initiatives – Malware Patrol
Block List examples – 29 formats

0519qq.cn/zzx/
1000millasargentina.com.ar/
12.10.157.6/ 12.24.238.229/images/
12.25.151.68/images/
121.15.220.71/
122.153.17.35/kjboard/images/
122.224.9.221/
125.211.197.75/fuckq1q1q1q1q1q1q1/
13opd.com/xrbv/
140.117.120.161/n/
148.208.196.2/.../
148.243.214.204/beta1/prevencao/

Brazilian initiatives – Federal Police

Operation Trilha (Operation Trail):

691 law enforcement agents
139 arrest warrants
136 search warrants
12 brazilian states (**28** cities)
01 person arrested in USA

Brazilian initiatives – Federal Police

Brazilian initiatives – Federal Police

Brazilian initiatives – Federal Police

Content removed from public version.

Brazilian initiatives – Federal Police

Content removed from public version.

Some thoughts

• Malware is becoming more sophisticated, no surprise here, but the issue is the speed of the change. Are we ready for this change??

• We still have 30,000 to 40,000 new malware files per year that relies on keylogging and screenlogging

• Malware is a alternative source of income and for some “just a job” – social issue

• Packer? What about 140? When we will break the 200 barrier? Are we there yet?

• Do we have persistent malware or too many trash to deal with?