



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





Forum of Incident Response and Security Teams



Content removed from public version.



Forum of Incident Response and Security Teams



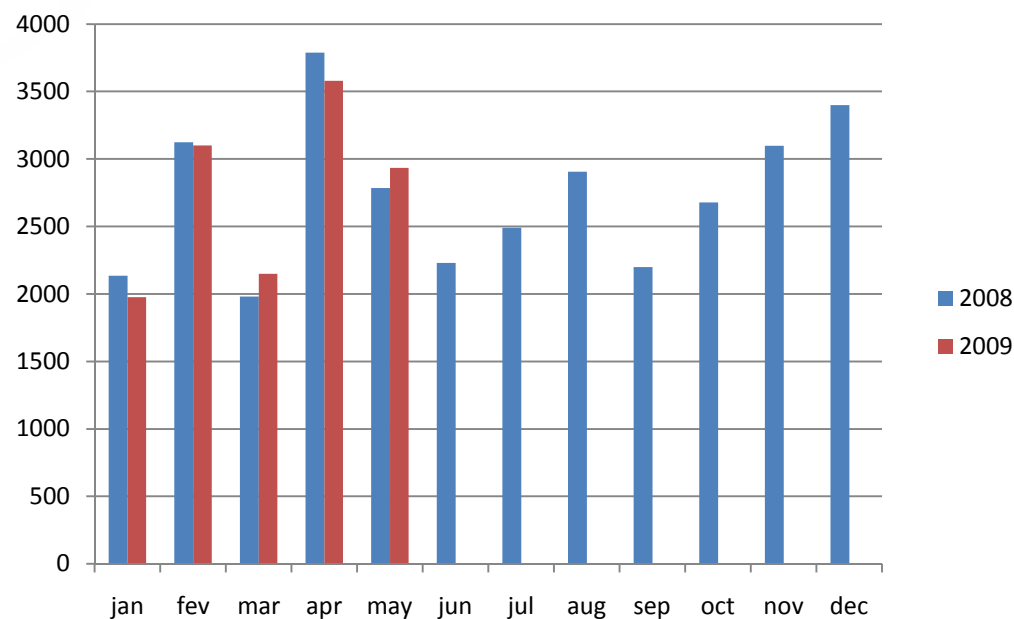
Content removed from public version.

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!



Forum of Incident Response and Security Teams



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 😊



© 2004 - REDE INFOSEG - Esplanada dos Ministérios Edifício Anexo II, Andar Térreo, Infoseg, CEP - 70.064-900, Brasília - DF, Fone (61) 3429-9393

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 Vêner

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



Forum of Incident Response and Security Teams



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”

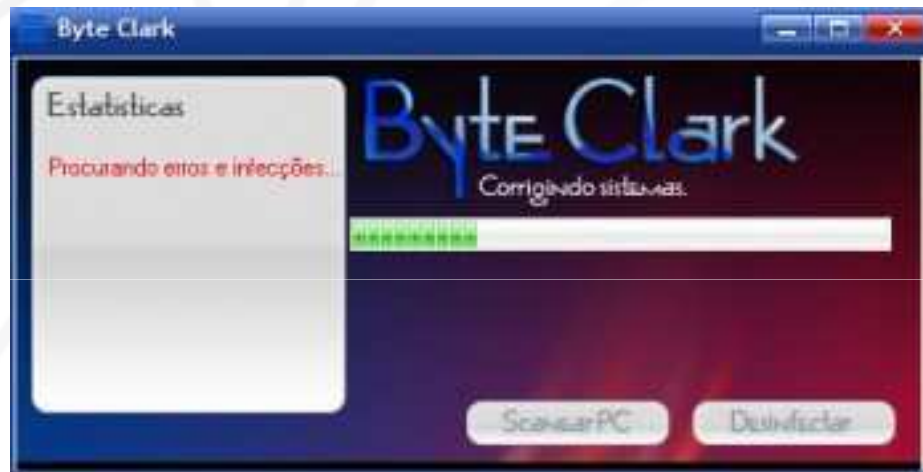
Malware 4 – Ransomware is all about Money



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.



Forum of Incident Response and Security Teams



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!



Forum of Incident Response and Security Teams



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](mailto:fabio@linhadefensiva.org)

Notícias: Beta de antivírus grátis da Microsoft deve chegar em breve | RSS | BankerFix | Twitter | IRC | ARIS | geral@linhadefensiva.com.br

Linha Defensiva

defendendo seu PC contra os perigos da Internet

Google™ Pesquisa Personalizada

Linha Defensiva | Boletim | Blog da Redação | Downloads | Fórum

Antivirus Avq Gratis - AVG
Precisa Detectar Vírus no seu PC? Proteja-se com o iG AntiVírus.
CentraldeSeguranca.iG.com.br

Antivirus Bom e Barato
Assine agora o PC Seguro e tenha um antivírus rápido e eficiente. Veja!
www.PCSeguro.com.br

ANÚNCIOS Google

LINHA DEFENSIVA | SEGURANÇA DA INFORMAÇÃO

Antivirus fraudulento brasileiro "sequestra" sistema
Malware brasileiro impede acesso aos documentos na máquina infectada, exigindo a compra de um programa "antivirus" para consertar o problema

Beta de antivírus grátis da Microsoft deve chegar em breve
Software será disponibilizado gratuitamente para quem possuir Windows XP, Windows Vista ou Windows 7, e oferecerá proteção contra vírus, spywares e trojans

Governo dos EUA derruba provedor que colaborava com criminosos
Empresa hospedava cavalos de troia, pornografia infantil e sites farmacêuticos falsos, segundo investigação do FTC

Criminosos criam golpe usando voo AF 447

90% dos emails enviados são spam, diz Symantec

SITE SEGURO
SITE SEGURO! NÃO DUVIDE.

PUBLICIDADE
Anúncios Google
AntiVirus - iG AntiVirus
Seu Computador Pode Estar em Risco! iG AntiVirus a partir de R\$3,95/mês
iG.com.br/Antivirus
Computador pelo

Principais
Notícias
Boatos & Fraudes
Reportagens Especiais
Dúvidas
Entrevistas
Editoriais
Dicionário
Reviews
Guias/Tutoriais
Textos Técnicos
Descrições de Vírus
Biblioteca de Arquivos
Provas/Quizzes



Brazilian initiatives – Malware Patrol

The screenshot shows the MalwarePatrol website. At the top, there is a navigation bar with links for Home, Stats, Block Lists, News/Blog, Contribute, ToDo, FAQ, and Terms. Below the navigation bar is a search bar with the text "Search MBL:#" and a "Search" button. The main content area is divided into several sections:

- Conficker Alert!**: A red alert icon with a spiky virus. Text: "As **Conficker** continues to evolve as a series of variants and downloads other worms and 'scareware', we prepared a special block list to help you protect your network. Visit our [Conficker](#) page for more information on how to block **Conficker** from downloading **Malware** using the Waledac botnet."
- Welcome**: A section with a blue background and a gold padlock. Text: "Malware Patrol is a free, automated and user contributed system for verifying URLs for the presence of Viruses, Trojans, Worms, or any other software considered **Malware**. Our main tasks are:
 - Collect**: Our crawling system automatically collects URLs pointing to dangerous extensions.
 - Analyze**: Every URL is analyzed for the presence of **Malware**
 - Block**: We provide block lists in [29 formats](#). With than, administrators can block access to infected URLs and Phishing Scams
 - Alert**: Owners of domains and servers hosting **Malware** receive our e-mail alerts. Some security groups and CSIRTs are also alerted
 - Monitor**: Infected URLs are monitored to assure our block lists are fresh and trustworthy. Every URL in our database is verified daily
- Current URL Stats**: A box showing "Blocked: 4,080" and "Dangerous: 110,961".
- Recent Malware detected**: A list of URLs including [Tri_Dwnldr.Doldow.dq](#), [Tri_Dwnldr.Agent.cfmq](#), [W32.Dwnldr_disq...](#), [Tri_Banker.Banker.aikz](#), and [Tri_Dwnldr.Banload.bfn](#).
- News**: A section with a date "18 May 09" and text: "Today we faced two problems that adversely impacted our users: an unexpected reboot of a database server caused some URLs to change status to 'new'; later we had DNS problems in the malware.com.br zone. We sincerely apologize for the trouble this may have caused and assure users that we are working to provide the best"

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/fuckq1q1q1q1q1q1q1q1/
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





Forum of Incident Response and Security Teams



Brazilian initiatives – Federal Police

Content removed from public version.



Forum of Incident Response and Security Teams



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?