CYBER $\begin{cases} \boldsymbol{ataque} \\ \boldsymbol{explora}\text{çã}\boldsymbol{o} \end{cases}$

Uma visão estratégica

Otávio Cunha

Disclaimer

As opiniões e visões aqui apresentadas são de total responsabilidade do seu autor e não necessariamente representam as da sua organização.

REDIT BANK
519 9860 1535 9007
YOUR NAME HERE

“Choose a job you love, and you will never have to work a day in your life."

- Confucius

Cyber ataque ?

- O ataque cibernético, de acordo com o relatório Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities do Committee on Offensive Information Warfare Computer Science and Telecommunications Board Division on Engineering and Physical Sciences vinculado ao National Research Council, refere-se a ações deliberadas para alterar, interromper, enganar, degradar, ou destruir sistemas de computador ou redes ou as informações em trânsito ou programas residentes em sistemas ou redes.

Cyber exploração

- Refere-se à utilização de ações ofensivas de cyber — talvez durante um longo período de tempo — para apoiar os objetivos e missões da parte que conduz a exploração, geralmente com a finalidade de **obtenção de informação** residente ou em trânsito através de sistemas de informação ou redes de um adversário.
- Procura não perturbar o normal funcionamento de um sistema de computador ou a rede do ponto de vista do usuário — na verdade, a melhor exploração cibernética é aquela executada de modo que o alvo nunca percebe que está sendo vítima de uma ação de coleta.

Cyber ataque ≠ Cyber exploração

- O ataque cibernético deve ser claramente distinguido da exploração cibernética:
  - Um ataque cibernético tem por objetivo indisponibilizar ou tornar as informações e sistemas de informação, a que o adversário necessita ter acesso, não confiáveis.
  - Enquanto que a atividade de exploração cibernética caracteriza-se como uma atividade de coleta de inteligência, em vez de uma atividade destrutiva. A exploração cibernética procura não perturbar o normal funcionamento de um sistema de computador ou a rede do ponto de vista do usuário — na verdade, a melhor exploração cibernética é aquela executada de modo que o alvo nunca perceba.

Condições de Contorno

- Existem, pelo menos, duas razões que uma apresentação sobre ataque cibernético necessariamente toca na exploração cibernética:
  - Primeiro, o ataque cibernético e a exploração cibernética estão intimamente relacionadas do ponto de vista técnico.
  - Em segundo lugar, por causa de tais semelhanças uma nação que é o destino de uma exploração cibernética pode interpretá-la como sendo um ataque cibernético.

Características dos cyber ataques

- Os resultados de um ataque cibernético são muitas vezes altamente incertos;
- Ataques cibernéticos são frequentemente muito complexos para planejar e executar.
- A identidade da origem por trás de um ataque cibernético significativo pode ser escondida com relativa facilidade, comparada com a de um ataque de cinético significativo.

Considerações operacionais

- Muitas das considerações operacionais para exploração cibernética são semelhantes aos do ataque cibernético.
- Como o ataque cibernético, uma exploração cibernética bem sucedida requer uma vulnerabilidade, o acesso a essa vulnerabilidade e um payload a ser executado.
- Essas semelhanças muitas vezes significam que o destino pode não ser capaz de distinguir facilmente entre uma exploração cibernética e um ataque cibernético.
- A principal exigência técnica de uma exploração cibernética é que a entrega e a execução do payload seja realizada o mais indectável possível.
- O segredo é frequentemente muito menos importante quando o ataque cibernético é a missão, porque em muitos casos, os efeitos do ataque vão ser imediatamente aparentes para o destino.

Exemplos

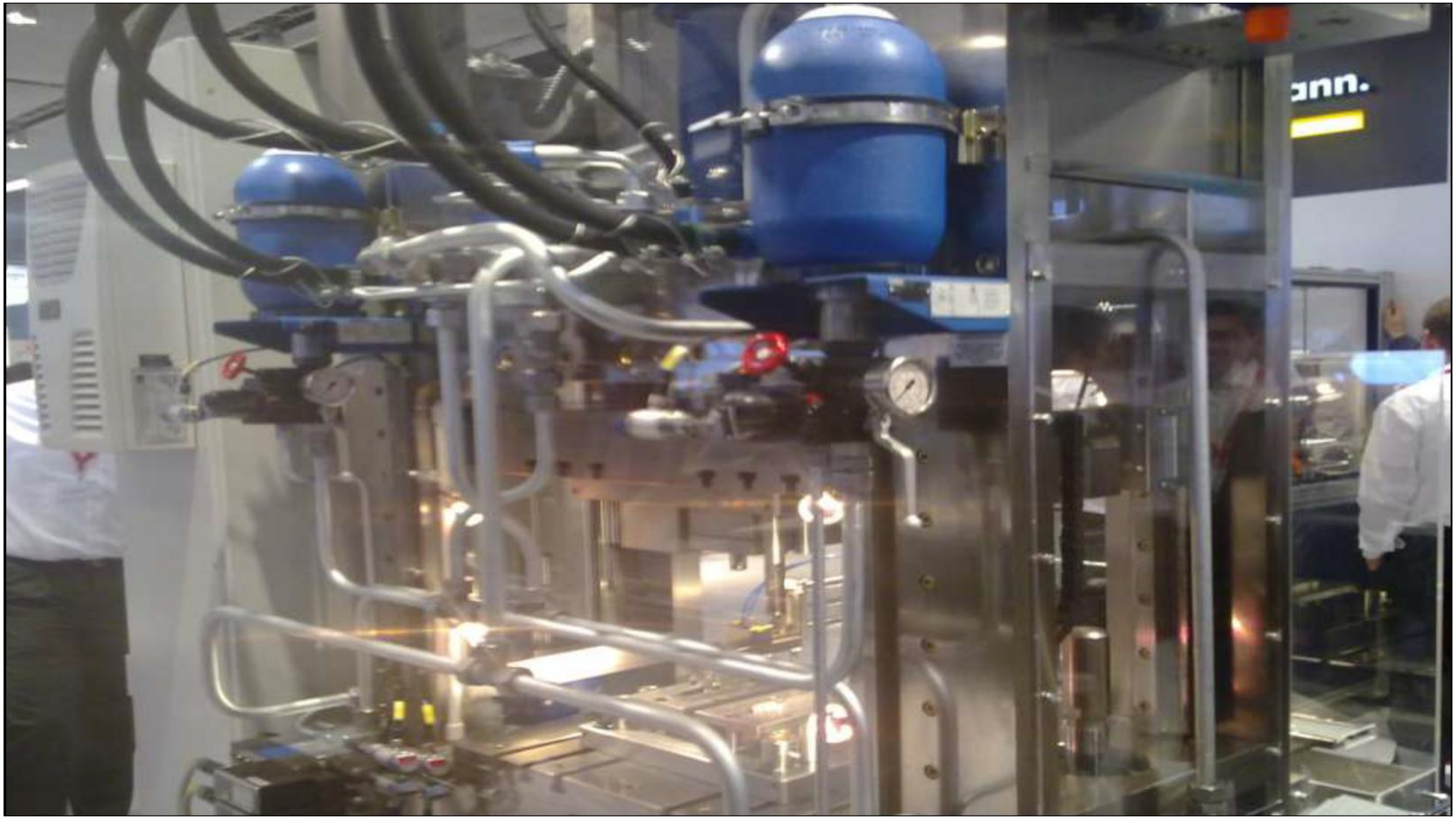
- **Nation state sponsored attacks: the offensive of Governments in cyberspace**
  - by paganinip on November 12th, 2012

  - Publishers of mainstream ICT news are ablaze with articles on the evolution of the “Flame” malware targeting the Middle East region for cyber espionage purposes, and new menaces such as Gauss or Shamoon.
  - No longer the province of deviant black-hat hackers or transnational organised crime groups, malware is now being actively developed and deployed by Nation States.

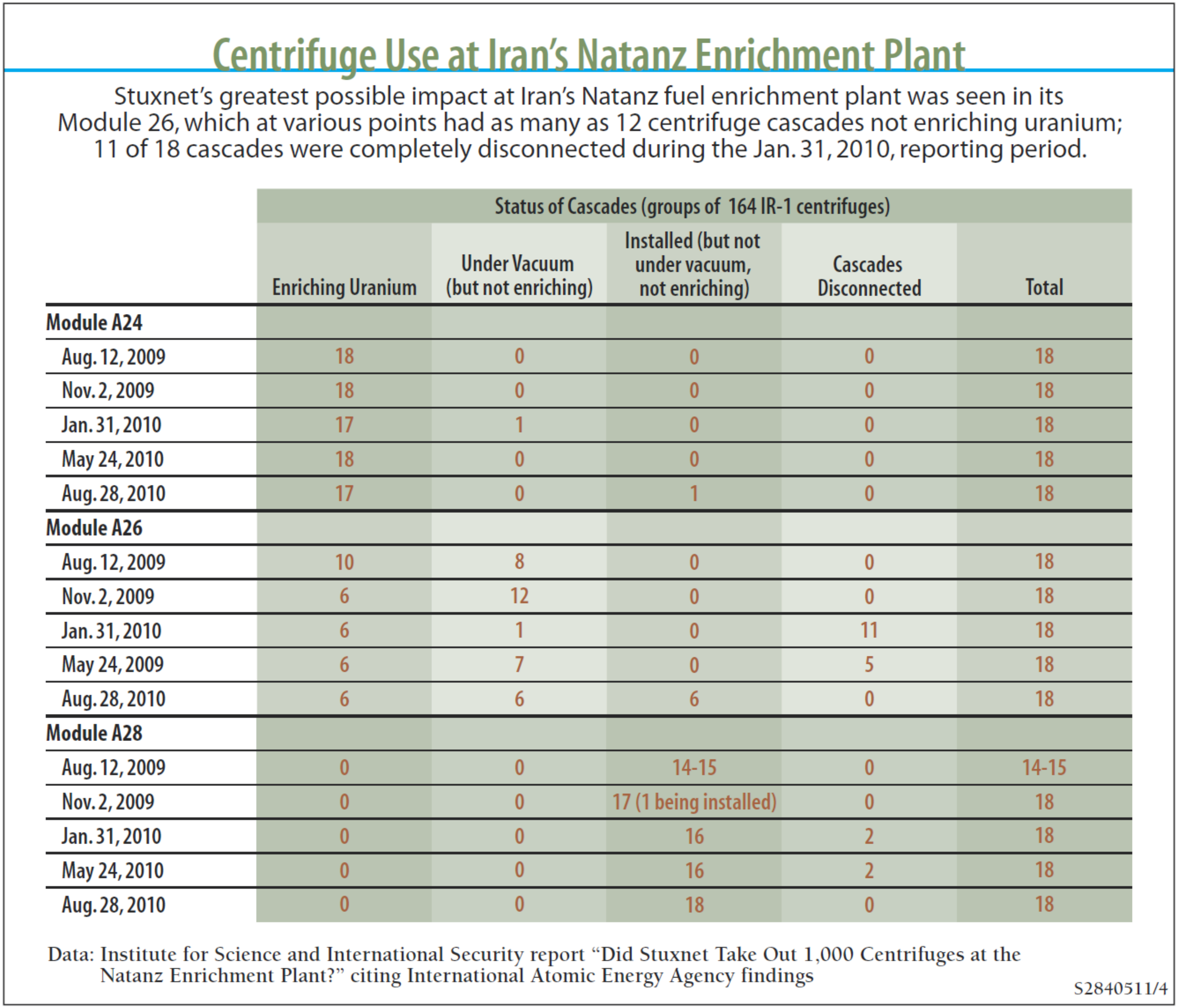
Iran

- **Era of targeted attacks is here to stay**
  - **FINANCIAL TIMES** TUESDAY NOVEMBER 1 2011
- **Iranian nuclear facilities,**
  - zero-day exploits, secret operatives and nation-state government involvement sounds more like the backstory to a spy novel than a piece of malware.
  - Yet Stuxnet, the most researched and analyzed malware ever, is still being studied and discussed in security circles around the world even though it was discovered more than a year ago.

Stuxnet



Stuxnet



Centrifuge Use at Iran's Natanz Enrichment Plant

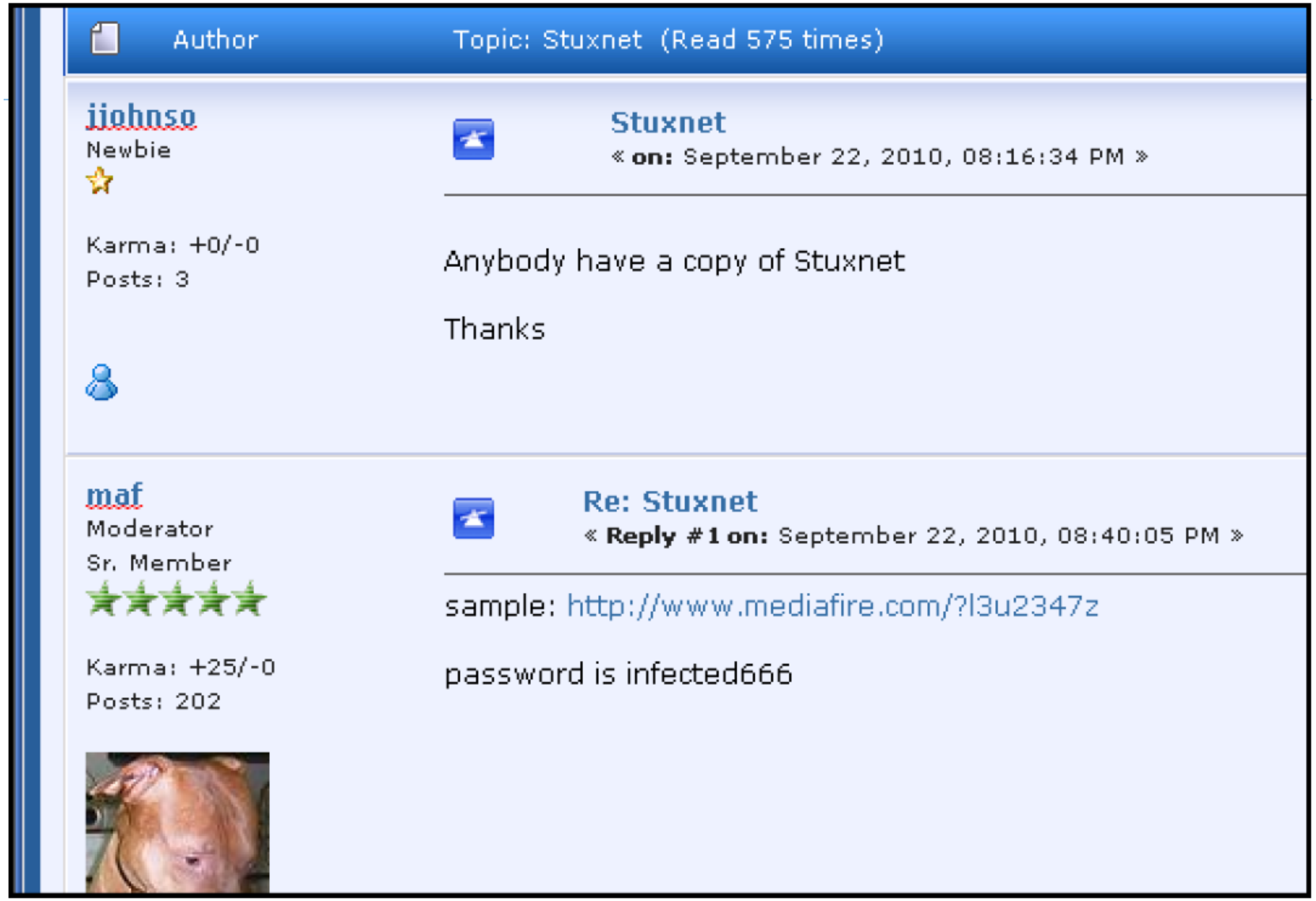
Stuxnet's greatest possible impact at Iran's Natanz fuel enrichment plant was seen in its Module 26, which at various points had as many as 12 centrifuge cascades not enriching uranium; 11 of 18 cascades were completely disconnected during the Jan. 31, 2010, reporting period.

	Status of Cascades (groups of 164 IR-1 centrifuges)				
	Enriching Uranium	Under Vacuum (but not enriching)	Installed (but not under vacuum, not enriching)	Cascades Disconnected	Total
Module A24					
Aug. 12, 2009	18	0	0	0	18
Nov. 2, 2009	18	0	0	0	18
Jan. 31, 2010	17	1	0	0	18
May 24, 2010	18	0	0	0	18
Aug. 28, 2010	17	0	1	0	18
Module A26					
Aug. 12, 2009	10	8	0	0	18
Nov. 2, 2009	6	12	0	0	18
Jan. 31, 2010	6	1	0	11	18
May 24, 2009	6	7	0	5	18
Aug. 28, 2010	6	6	6	0	18
Module A28					
Aug. 12, 2009	0	0	14-15	0	14-15
Nov. 2, 2009	0	0	17 (1 being installed)	0	18
Jan. 31, 2010	0	0	16	2	18
May 24, 2010	0	0	16	2	18
Aug. 28, 2010	0	0	18	0	18

Data: Institute for Science and International Security report "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" citing International Atomic Energy Agency findings

S2840511/4

Stuxnet



Author | Topic: Stuxnet (Read 575 times)

jjohnso
Newbie

Karma: +0/-0
Posts: 3

Stuxnet
« **on:** September 22, 2010, 08:16:34 PM »

Anybody have a copy of Stuxnet

Thanks

maf
Moderator
Sr. Member

Karma: +25/-0
Posts: 202

Re: Stuxnet
« **Reply #1 on:** September 22, 2010, 08:40:05 PM »

sample: http://www.mediafire.com/?l3u2347z

password is infected666

Iran

- **Narilam: A 'New' Destructive Malware Used In the Middle East**
  - Several days ago, our colleagues from Symantec published an analysis of a new destructive malware reported in the Middle East. Dubbed “Narilam”, the malware appears to be designed to corrupt databases. The database structure naming indicates that targets are probably in Iran.
    - http://www.securelist.com/en/blog/208193954/Narilam_A_New_Destructive_Malware_Used_In_the_Middle_East

Israel

- **Cyber espionage attack against Israel is not an isolated event**
    - by paganinip on November 14th, 2012
  - – Once again Middle East area is the scene of a series of cyber attacks, several malware attacks have hit over the last year Israeli and Palestinian systems apparentlyhaving a common origin. A group of experts from Norwegian antivirus and security firm Norman ASA have discovered a new cyber espionage campaign against the countries that used various malware to spy on victims.

Peter the Great Versus Sun Tzu

- "While East Asian hackers dominate cybersecurity-related headlines around the world with high-profile intrusions and advanced persistent threats (APTs), it would be a mistake to conclude that these attackers are the sole or greatest criminal threat to the global Internet today. After conducting extensive research into the nature of the East Asian and East European underground, Trend Micro has concluded that hackers from the former Soviet Bloc are a more sophisticated and clandestine threat than their more well-known East Asian counterparts.
- Peter the Great is now manifesting himself in cyberspace.

- Tom Kellermann - Vice President of Cybersecurity Trend Micro

China?

- **Cyber espionage on energy sector, Chinese hackers are not the only**
    - by paganinip on September 27th, 2012
  - Since last month a new campaign of cyber attacks have hit the Energy sector, all is started with the incidents to Saudi Aramco and RasGas companies, in both cases a malware infected internal networks without impacting on the production systems. Due the nature of the targets, the mode of attack and the specific malware behavior cyber security experts believe that the incidents were caused by cyber warfare operations but it wasn’t possible to discover the real origin of the offensive.

Advanced Persistent Threats
APT

- **A huge challenge from China, Russia and organised crime**
  - ‘ What can security companies do to prevent governments and large corporations being attacked by **“advanced persistent threats”** in cyberspace?’
  - ‘The Chinese are notable for the sheer volume of what they do. The Russians are less active but very sophisticated’

FLAME

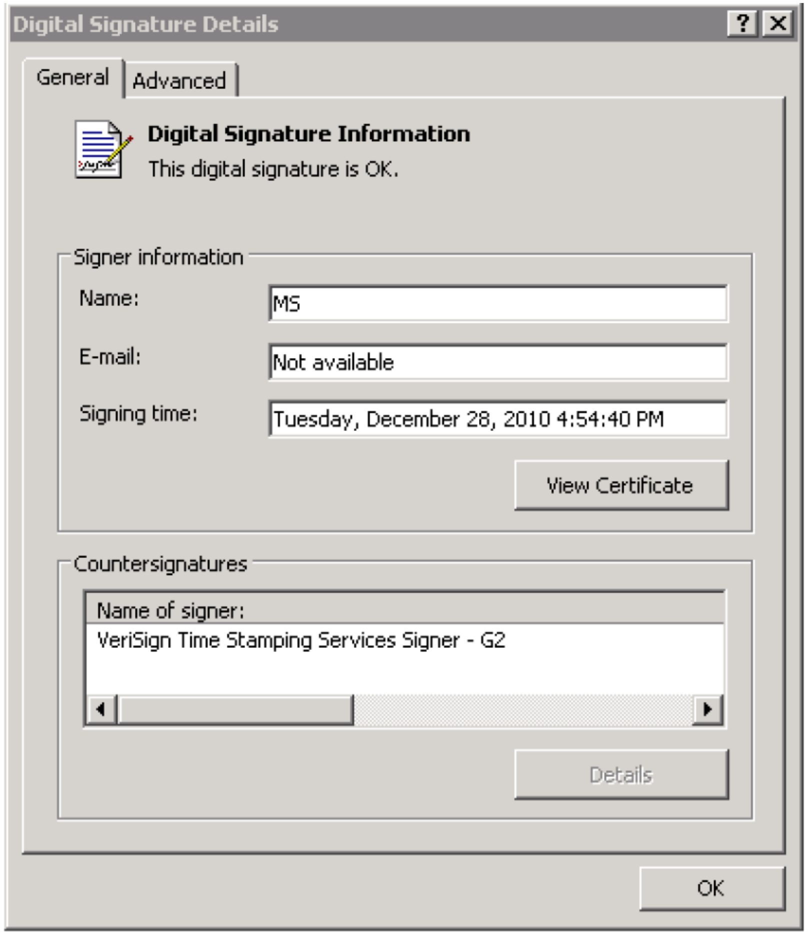
Flame

- Código enorme
- Contém keylogger e um capturador de tela
- Tem bibliotecas SSH e LUA
- Coleta partes de documentos
- Coleta coordenadas de arquivos de imagens
- Checa por dispositivos conectados por bluetooth

- Envia as informações roubadas para fora das organizações mesmo sem conexão de rede
- É relacionado com o Stuxnet
- Se dissemina por intermédio de updates da Microsoft
- É assinado pela Microsoft e os certificados foram tratados por força-bruta por supercomputadores

Fonte: F-Secure

Flame



Digital Signature Information

This digital signature is OK.

Signer information

Name: MS

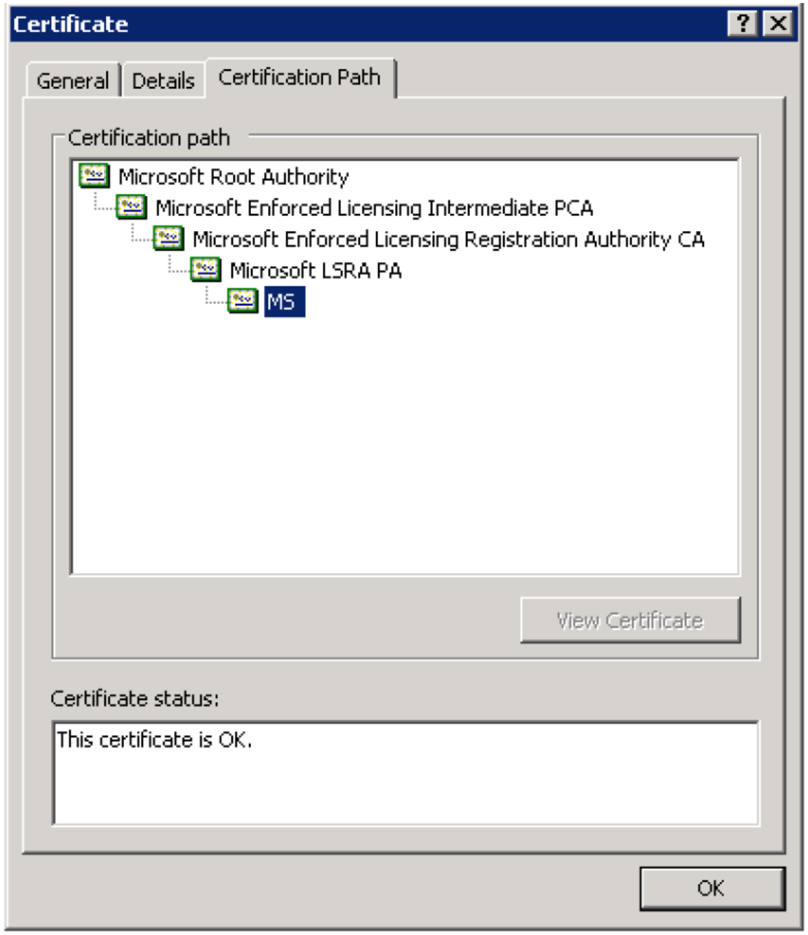
E-mail: Not available

Signing time: Tuesday, December 28, 2010 4:54:40 PM

Countersignatures

Name of signer:

VeriSign Time Stamping Services Signer - G2



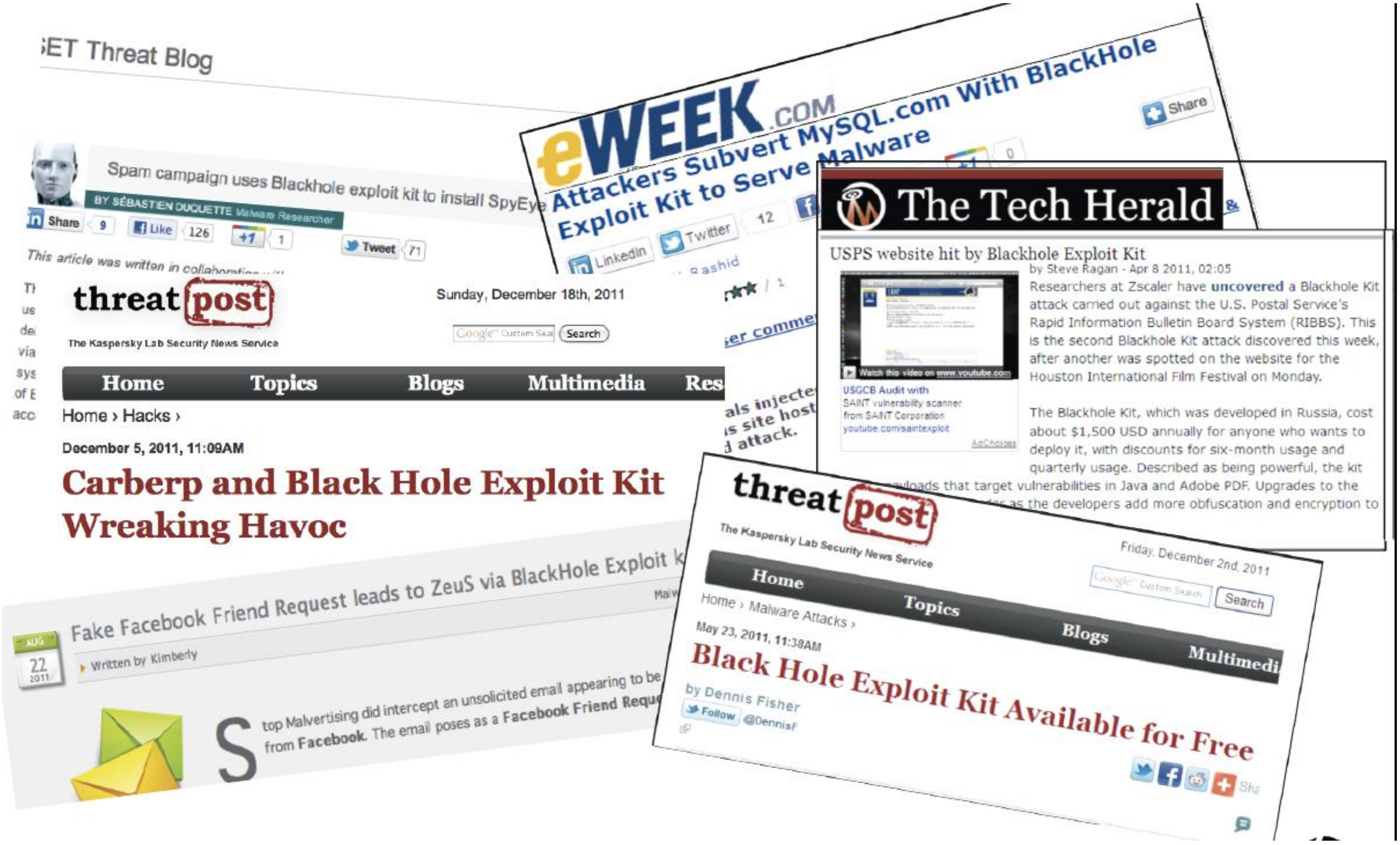
Certification path

- Microsoft Root Authority
  - Microsoft Enforced Licensing Intermediate PCA
    - Microsoft Enforced Licensing Registration Authority CA
      - Microsoft LSRA PA
        - MS

Certificate status:

This certificate is OK.

Blackhole 2.0



ET Threat Blog

Spam campaign uses Blackhole exploit kit to install SpyEye

BY SÉBASTIEN DUQUETTE Malware Researcher

This article was written in collaboration wit

eWEEK.COM

Attackers Subvert MySQL.com With BlackHole Exploit Kit to Serve Malware

als injecte
s site host
d attack.

The Tech Herald

USPS website hit by Blackhole Exploit Kit

by Steve Ragan - Apr 8 2011, 02:05

Researchers at Zscaler have **uncovered** a Blackhole Kit attack carried out against the U.S. Postal Service's Rapid Information Bulletin Board System (RIBBS). This is the second Blackhole Kit attack discovered this week, after another was spotted on the website for the Houston International Film Festival on Monday.

The Blackhole Kit, which was developed in Russia, cost about $1,500 USD annually for anyone who wants to deploy it, with discounts for six-month usage and quarterly usage. Described as being powerful, the kit …yloads that target vulnerabilities in Java and Adobe PDF. Upgrades to the …der as the developers add more obfuscation and encryption to

USGCB Audit with
SAINT vulnerability scanner
from SAINT Corporation
youtube.com/saintexploit

threatpost

The Kaspersky Lab Security News Service

Sunday, December 18th, 2011

Home › Hacks ›

December 5, 2011, 11:09AM

Carberp and Black Hole Exploit Kit Wreaking Havoc

Fake Facebook Friend Request leads to ZeuS via BlackHole Exploit k

Written by Kimberly

AUG 22 2011

Stop Malvertising did intercept an unsolicited email appearing to be from **Facebook**. The email poses as a **Facebook Friend Reque**

threatpost

The Kaspersky Lab Security News Service

Friday, December 2nd, 2011

Home › Malware Attacks ›

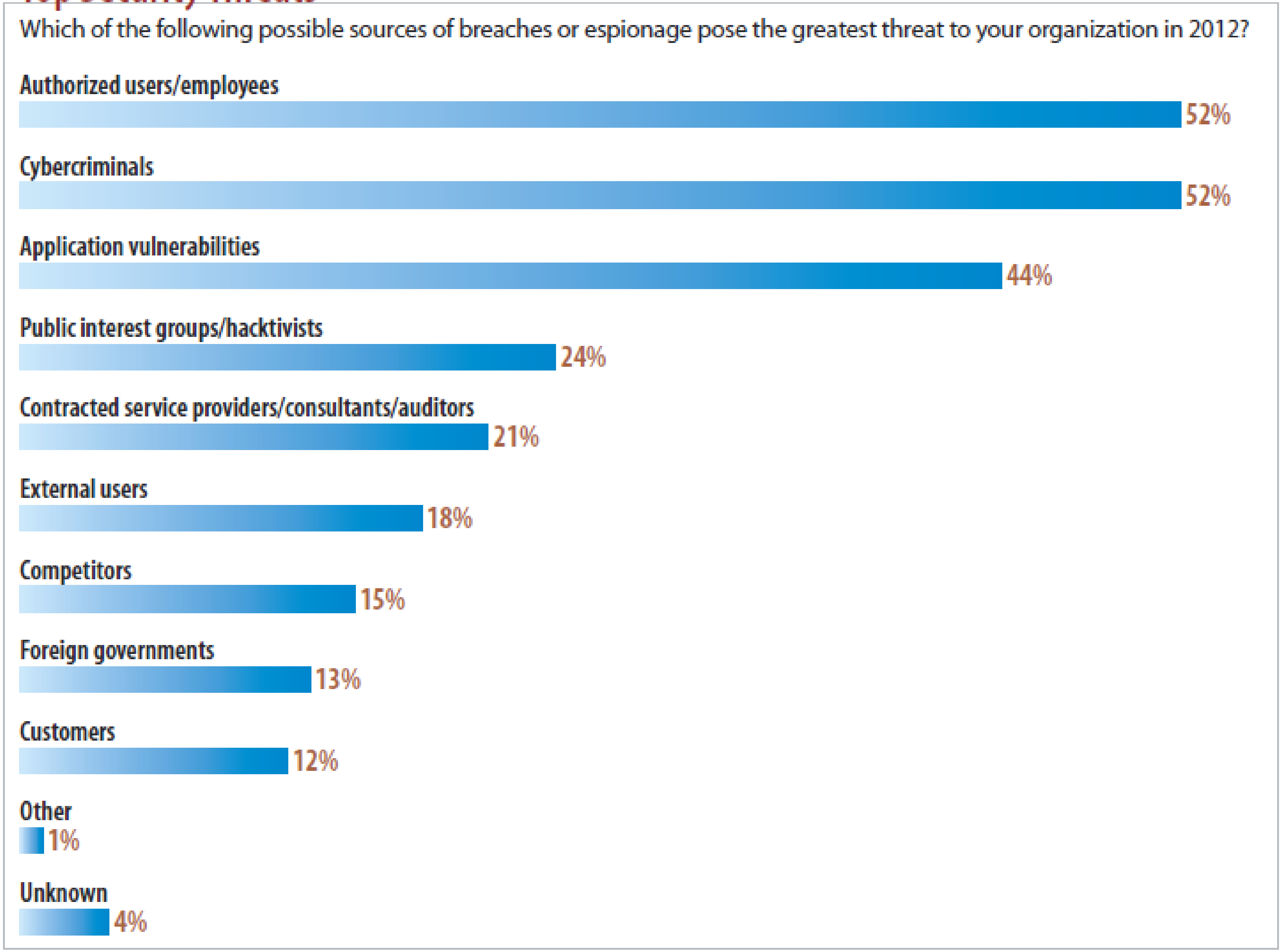
May 23, 2011, 11:38AM

Black Hole Exploit Kit Available for Free

by Dennis Fisher

@DennisF

Top Security Threats



Note: Three responses allowed

R4670512/12

Data: *InformationWeek* Strategic Security Survey of business technology and security professionals at organizations with 100 or more employees

Previsões (sic)

Fonte: Websense 2013

- **1 Attacks will continue to exploit legitimate web platforms.**
  - This includes hundreds of new content management systems and service platforms, in addition to the IIS and Apache exploits of the past.
- **2 More cross-platform threats will involve mobile devices.**
  - More than mobile-threat hype, there are specific emerging desktop, cloud and other technologies that will add to this growth.
- **3 Legitimate mobile app stores will host more malware.**
  - The success of mobile devices, the mobile app sales model and the pure volume of apps are creating a new area of risk.
- **4 Successful "hacktivism" incidents will decrease.**
  - Increased awareness, and the resulting improvements in defensive measures, will result in fewer successful hacktivism incidents, although attacks will increase in sophistication.

Previsões (sic)

Fonte: Websense 2013

- **5 Government-sponsored attacks will increase.**
  - In the wake of several public cyberwarfare events, a number of contributing factors will drive more countries toward cyberwarfare strategies and tactics.
- **6 Threats will become more “virtual aware.”**
  - As network and security vendors apply virtual machines for applications, servers and sandboxing, cybercriminals will customize their threats accordingly.
- **7 Email threats will evolve to new levels.**
  - Domain generation algorithms and other emerging techniques bypass current security, and professionals are becoming the preferred targets. And malicious email attachments are making a comeback.

Futuro?

Otávio Cunha

otavicunha@gmail.com