



Apocalypse Now?



MSc. Ivica Ostojic CISSP, CISM

Warning – Disclaimer - Upozorenje

Warning – Disclaimer - Upozorenje

Neither Cisco or the presenter encourages the use of any methods and/or tools mentioned within this presentation without the expresses aproval and signed agreement with the owner of the IT infrastructure in question.

Warning – Disclaimer - Upozorenje

Neither Cisco or the presenter encourages the use of any methods and/or tools mentioned within this presentation without the expresses aproval and signed agreement with the owner of the IT infrastructure in question.

The unathorised usage of the aforementioned tools and/or methods could lead to legal prosecution and severe penalties.

First – words of wisdom

SUN TZU

THE ART OF WAR

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.



The Economist

APRIL 25TH - MAY 1ST 2009

Economist.com

Gordon Brown's desperate measures
Sri Lanka: the Tigers' last stand
Could Fiat's boss turn Chrysler around?
Obama, Cheney and torture
The death of a great science writer

A glimmer of hope?

The world economy
and the perils of
optimism



The

Gordon Brown's desperate measures

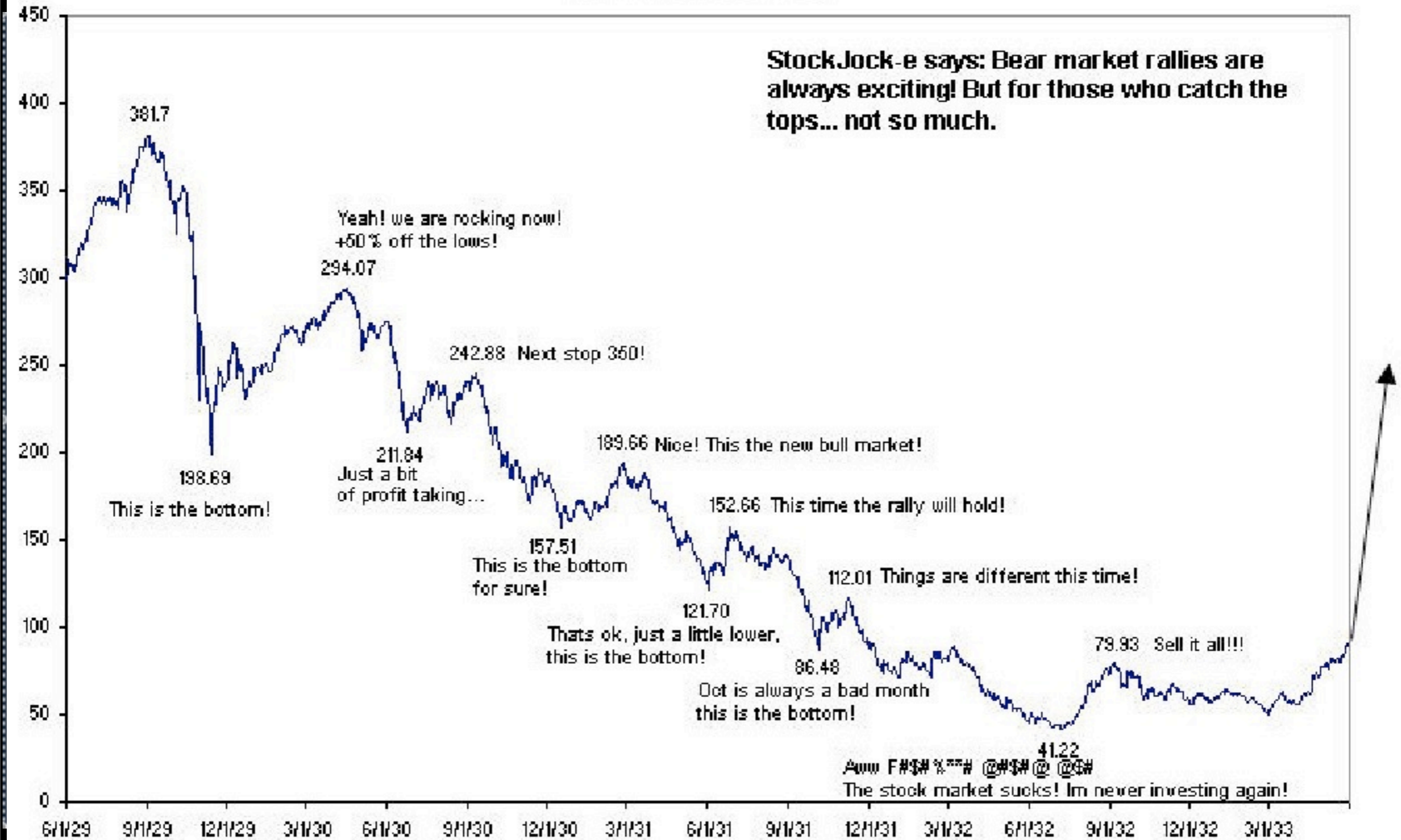
Sri Lanka: the Tigers' last stand

Dow Jones Index: 1929-1940 vs. 2007-today (20/05/09) - www.dickreuter.com



Dow Jones Industrials (June 1929 to May 1933)

StockJock-e says: Bear market rallies are always exciting! But for those who catch the tops... not so much.



Back to IT security ;-)

Infrastructure

IT & the Business

Government & Law

Security

Careers & HR

Online

TECHNOLOGY

Applications

Business Intelligence

Development

Hardware

Mobile & Wireless

Networking

Internet

Operating Systems

Security Products

Servers & Datacentre

Storage

TOOLBOX

Open Source

Green Computing

Quality & Testing

TRAINING

BOOKS

WHITE PAPERS

March 24, 2009

Economic crisis 'could drive IT professionals to cybercrime'

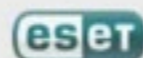
[View the IT & the Business section](#)

Job losses and bonus cuts could push security gurus to the dark side

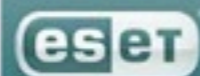
By Jeremy Kirk, IDG News Service [ShareThis](#)

Enterprises feel their employees will be increasingly willing to steal data or sell insider knowledge due to the poor economy, according to an annual security survey conducted by KPMG.

ADVERT



Download a free trial at
www.eset.co.uk



We Protect Your Digital Worlds™

Sixty-six percent of respondents felt that out-of-work IT workers would be tempted to join the criminal underground, driven in part by threats to bonuses, job losses and worthless stock options.

The E-crime Survey 2009, presented at the E-Crime Congress in London on Tuesday, surveyed 307 private companies, government organisations and law enforcement agencies.

In the survey, KPMG said that fraud committed by managers,

SEARCH »

Latest blog posts

A Day to Remember: 23 April, 2009

EU on ACTA: "TRIPS Is Floor Not Ceiling"

Should security companies turn a blind eye to FBI's use of spyware?

To GRC or not to GRC, that is the question

IdM anyone? Anyone? Notes from RSA

VMware wants to be your network operating system of choice

CIO Open Source Corner - The Top 5 Tips for getting the most out of Open Source

Richard's last...

What on Earth is the Open Source World Map For?

Outsourcing and the virtualisation boom

[More blogs posts](#)

Most-read news

Hardware fault crashed online tax returns on deadline day

Oracle's Sun merger raises questions over MySQL, antitrust

Mission Critical Centre

Follow the latest trends: with news, features, blogs, podcasts, video and more

[Blades](#)[Virtualisation](#)[Platform Modernisation](#)[Datacentre Transformation](#)

In association with



Hosted by



Enterprise 2.0

d this site from opening a pop-up window.



National World Opinion Business Technology Sport Entertainment Life & Style Travel

You are here: Home » Breaking News Technology » Article

Search here...

smh.com.au

Search

Mobiles

RSS

Text

Newsletters

Low vision

Economic crisis 'to boost cyber crime': Microsoft

Denholm Barnetson
April 17, 2009

The global financial crisis threatens to spark a rise in cyber crime as computer experts lose their jobs and resort to illegal ways to earn a living, a senior official of Microsoft said Thursday.

"Today these (cyber) attacks are not about vandalism any more, today it's about cash," said Roger Halbheer, Microsoft's chief security advisor for Europe, the Middle East and Africa.

"Cyber crime has gone from cool to cash. And this will definitely grow in the future," he told AFP on the sidelines of an international conference on terrorism and cyber security.

It is "one of the things that scares me about the economic downturn because I'm expecting cyber crime will grow."

He said the crisis had meant people with good knowledge of the industry were being laid off. "They then have time and they don't have money," he said.

"At the moment we are still at the cool side. But I'm expecting it to move to the cash side."

He referred to the Conficker worm, believed to have burrowed into millions of computers around the world in the last few

Advertisement

[Ads by Google](#)

[Catch Hackers Red-Handed](#)

with GFI EventsManager! Intrusion detection via event log monitoring
www.gfi.com

Today in Breaking News Technology

Twitter a global sensation: Hitwise

Twitter a global sensation: Hitwise

Lost laptops cost companies dearly: study

Cost-cutting saves Microsoft stock after rough 3Q

Latin American banks look to mobiles to battle crisis

+ [More Breaking News Technology news](#)

Story Tools

Email this story

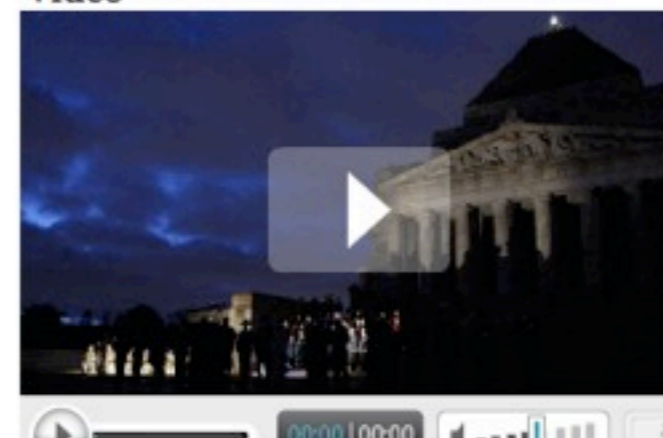
Share / Bookmark story

Print this story

LATEST VIDEO

LATEST

Latest Breaking News Technology Video



- ▶ Asia-Pacific Politics
- ▶ Business
- ▶ Culture and Lifestyle
- ▶ Diplomacy
- ▶ Domestic Policy
- ▶ Economic Crisis
- ▶ Economic Issues
- ▶ Economic Policy
- ▶ Financial Rescue Plans
- ▶ International Relations
- ▶ Islam
- ▶ Islamism
- ▶ Media
- ▶ Middle Eastern Politics
- ▶ National Economy
- ▶ Political Policy
- ▶ Politics
- ▶ Public Finance
- ▶ Science and Technology
- ▶ Terrorism
- ▶ U.S. Government
- ▶ U.S. National Economy
- ▶ U.S. Politics
- ▶ War and Conflict
- ▶ World Politics

WORLD NEWS

POLITICS

BUSINESS

SCIENCE

ENTERTAINMENT

SPORTS

Cyberspies hack into U.S. fighter project: report

Posted 2009/04/21 at 11:15 am EDT

WASHINGTON, Apr. 21, 2009 (Reuters) — Computer spies have repeatedly breached the Pentagon's costliest weapons program, the \$300 billion Joint Strike Fighter project, *The Wall Street Journal* reported on Tuesday.

The newspaper quoted current and former government officials familiar with the matter as saying the intruders were able to copy and siphon data related to design and electronics systems, making it potentially easier to defend against the plane.

The spies could not access the most sensitive material, which is kept on computers that are not connected to the Internet, the paper added.

Citing people briefed on the matter, it said the intruders entered through vulnerabilities in the networks of two or three of the contractors involved in building the fighter jet.

Lockheed Martin Corp is the lead contractor. Northrop Grumman Corp and BAE Systems PLC also have major roles in the project. Lockheed Martin and BAE declined comment and Northrop referred questions to Lockheed, the paper said.

The Journal said Pentagon officials declined to comment



Workers prepare a F-35 joint strike fighter four days before the opening of the 47th Paris Air Show at the Le Bourget airport near Paris, June 14, 2007. REUTERS/Pascal Rossignol

Related Topics

- ▶ Armed Forces
- ▶ Military and Defense Policy
- ▶ Political Policy
- ▶ Science and Technology
- ▶ Technology

Ads by Google

Advertise here

Wonderland Online Game

Modern Life, Item Manufacturing FREE2Play!
Decorate Own House Now

NEWS FROM THE NET

powered by Inform



Related Articles

- ▶ **Lockheed Martin 1Q Net Falls 8.8%, Raises Full-Year EPS View**
Apr. 21, 2009 (Wall Street Journal) — Lockheed Martin Corp.'s (LMT) first-quarter net income fell 8.8% on higher pension-related expenses, though the defense contractor raised its ...
- ▶ **Hackers Break Into Pentagon's Fighter Jet Project**
Apr. 21, 2009 (CIO Magazine) — Hackers broke into U.S. Department of Defense computers and downloaded terabytes of data containing design information about the Joint Strike ...
- ▶ **Lockheed Profit Falls 8.8% on Rising Pension Costs; 2009 Forecast Raised**
Apr. 21, 2009 (Bloomberg) — Lockheed Martin Corp., the world's largest defense company, said first-quarter profit fell 8.8 percent as rising pension costs offset increased ...
- ▶ **Wanted: Nerds to byte into U.S. hacker battle**
Apr. 20, 2009 (Boston Herald) — The feds are

Black Hats



Researchers hack Wi-Fi driver to breach laptop

One of many flaws found allowed them to take over a laptop by exploiting a bug in an 802.11 wireless driver

By Robert McMillan, IDG News Service
June 21, 2006

E-mail Printer Friendly Reprints Slashdot It!

Security researchers have found a way to seize control of a laptop computer by manipulating buggy code in the system's wireless device driver.

Free IT resource

Free White Papers, Trialware and more

Sponsored by Symantec

Free IT resource

InfoWorld Podcast: Interview with log management expert Dominique Levin.

Sponsored by LogLogic

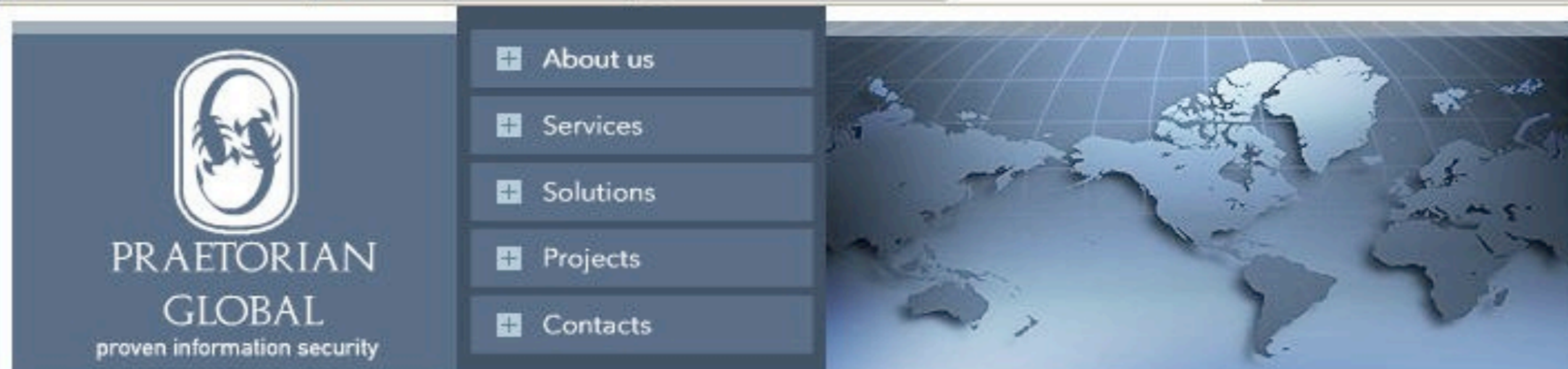
The hack will be demonstrated at the upcoming Black Hat USA 2006 conference during a presentation by David Maynor, a research engineer with Internet Security Systems and Jon Ellch, a student at the U.S. Naval postgraduate school in Monterey, California.

Device driver hacking is technically challenging, but the field has become more appealing in recent years, thanks in part to new software tools that make it easier for less technically savvy hackers, known as script kiddies, to attack wireless cards, Maynor said in

an interview.

The two researchers used an open-source 802.11 hacking tool called LORCON (Loss of Radio Connectivity) to throw an extremely large number of wireless packets at different wireless cards. Hackers use this technique, called fuzzing, to see if they can cause programs to fail, or perhaps even run unauthorized software when they are bombarded with unexpected data.

Using tools like LORCON, Maynor and Ellch were able to discover many examples of wireless device driver flaws, including one that allowed them to take over a laptop by exploiting a bug in an 802.11 wireless driver. They also examined other networking technologies including Bluetooth, Ev-Do (Evolution-Data Only), and HSDPA (High Speed Downlink Packet Access).



Blackjacking - Owning the Enterprise via the Blackberry

Presented at Defcon 14 - Las Vegas, NV 2006

Jesse D'Aguanno
jesse [at] praetoriang.net

Abstract:

Research in Motion's Blackberry technology has quickly become the defacto standard for executives and technical personnel alike to maintain unteathered remote access to critical data. Often regarded as inherently secure, most administrators deploy this solution without a full understanding of the technology or risks involved.

This presentation will demonstrate how an attacker could utilize many typical corporate blackberry deployments to directly attack machines on the internal network—behind your perimeter defenses! The tools and source code presented will be available for attendees. Techniques for reducing the risks associated with this technology will also be presented.

Materials:

Presentation Slides

[Download](#)

Blackberry Attack Toolkit (Including BBProxy)

[Download](#)

NOTE: This link is now active!

Blackjacking – Owning the Enterprise via Blackberry



Jesse 'x30n' D'Aguanno
•x30n@digrev.org
•jesse@praetoriang.net

| Folder | New | Total | | | | From | To | Subject |
|-----------|-----|-------|--|--|--|------|----|---------|
| + @ Ivica | | 240 | | | | | | |
| | 310 | 13711 | | | | | | |
| Inbox | 310 | 314 | | | | | | |
| Outbox | | 0 | | | | | | |
| Sent | | 0 | | | | | | |
| Trash | | 5 | | | | | | |
| Prebaceno | | 4502 | | | | | | |
| Vazno | | 270 | | | | | | |
| Arhiva | | 8620 | | | | | | |
| + @ | 347 | 14221 | | | | | | |

From
Reply-To
To
Subject

Apache Proof of Concept Exploit

4,256 b



apache.c

Summary

This is a proof of concept exploit for Apache,
This
code exploit multipart/form-data POST requests bug. This code only
crash
 apache daemon, not open any shell or execute code in the
remote server.
PHP supports multipart/form-data POST requests (as described in
RFC1867)

apache.c

Attack by web sites

Attack by web sites

IndiaTimes website 'attacks visitors' | The Register - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.theregister.co.uk/2007/11/10/india_times_under_attack/

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When security becomes ... Zone-H.org - War 2.0 FT.com / World - Computer misuse act... The Register: Security News and View... IndiaTimes

Search

Reg Hardware
Reg Developer
Channel Register
Whitepapers

News Tools
Newsletters & Feeds
Reg Mobile
Reg Desktop News Alerts

Reg Shops
Reg Merchandise
Books/Online Learning

Top Stories Top Rated

- MS patch system poses 'significant risk', say researchers
- YouTube has a little local difficulty in Arabia
- Standalone security industry dying, says guru
- Hidden card fraud taxes UK.biz
- Smut blocking? We're more bothered about

IndiaTimes website 'attacks visitors'

Targets multiple vulns, some new

By [Dan Goodin in San Francisco](#) → [More by this author](#)

Published Saturday 10th November 2007 01:47 GMT

[See what the experts have to say on attracting, retaining and developing IT talent](#)

Visitors to the *IndiaTimes* website are being bombarded by malware, some of which appear to target previously unknown vulnerabilities in Windows, a security researcher warns.

In all, the English-language Indian news site is directly or indirectly serving up at least 434 malicious files, many of which are not detected by antivirus software, according to Mary Landesman, a senior security researcher at ScanSafe. She said at least 18 different IP addresses are involved in the attack.

"The end result of the compromise is that the user, going through their normal course of activities, is subject to a really massive installation of malicious files," she told us. "Coupled with the low detection by antivirus vendors, it does put the end user in a very vulnerable position."

Visitors can be infected even if they have up-to-date systems and they don't fall victim to tricks to install software or browser add-ons, she said. She urged people to avoid the site until it's been cleaned up.

[Diwali](#), the Hindu festival of lights, is in full swing in India and Landesman is concerned webmasters for the site may be hard to reach over this holiday weekend.

"Our hope is they'll cut their holiday short and take care of this before Monday," she said.

She said most pages on the IndiaTimes site are clean. Those that are infected, however, contain a potent cocktail of downloader and dropper Trojans and other binaries. They contain a script that points to remote sites, some of which link to still other sites. The malicious files exploit multiple vulnerabilities, and some appear to be previously unknown flaws in Windows, according to Landesman, who used to be a security researcher for Microsoft.

Attack by web sites

Attackers turn Bank of India site into malware bazaar | The Register - Mozilla Firefox

Edit View History Bookmarks Tools Help

http://www.theregister.co.uk/2007/09/01/bank_of_india_website_takeover/

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When sec... Zone-H.org - War 2.0 FT.com / World - Comp... The Register: Security ... IndiaTimes website 'att... Attackers turn Bank...

Attackers turn Bank of India site into malware bazaar

31 unique exploits served

By [Dan Goodin in San Francisco](#) → [More by this author](#)

Published Saturday 1st September 2007 00:11 GMT

[Test Drive Sun's Quad-Core Intel Xeon systems today](#)

Bank of India IT staff are mopping up the mess left by attackers who rigged the firm's website to feed malware to customers trying to access online services.

The bank managed to pry loose the rogue iframe responsible for the malware sometime early Friday morning California time. At time of writing, though, Bank of India's website was effectively cordoned off, bearing a terse notification saying: "This site is under temporary maintenance and will be available after 09:00 IST on 1.09.07."

The shuttering came a day after employees for security provider Sunbelt Software discovered someone had planted an iframe in the site that caused unpatched Windows machines to be infected with some of the most destructive pieces of malware currently in circulation. Sunbelt counted 31 separate pieces in all, including Pinch, a [powerful and easy-to-use Trojan](#) that siphons personal information from a user's PC. Other malware included Trojan.Netview, Trojan-Spy.Win32.Agent.ql, various rootkits and several spam bots.

Executives and IT administrators at US offices of Bank of India who were contacted Friday morning by IDG were initially unaware of the attack. A spokesman [later told the news service](#) that officials were aware of the problem and were working to correct it, but had no information concerning its severity or duration.

Some of the servers used to install the malware belonged to the notorious Russian Business Network, a group Spamhaus [says](#) is involved in child porn, phishing and other misdeeds. According to Verisign's iDefense unit, the RBN also played a hand in bringing us MPack, a powerful Trojan downloader that [infect edmore than 10,000 websites](#) in just three days.

In this case, the attackers appeared to use an exploit kit dubbed n404, according to [this post](#) by Dancho Danchev. It relies on a

Attack by web sites

Hackers load malware onto Mercury music award site | The Register - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.theregister.co.uk/2007/06/07/dreamhost_hack/

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When security b... Zone-H.org - War 2.0 FT.com / World - Computer mi... The Register: Security News ... IndiaTimes website 'attacks vi... Hacking

Search

Reg Hardware
Reg Developer
Channel Register
Whitepapers

News Tools
Newsletters & Feeds
Reg Mobile
Reg Desktop News Alerts

Reg Shops
Reg Merchandise
Books/Online Learning

Top Stories Top Rated

- MS patch system poses 'significant risk', say researchers
- Modern 'primitive' could ease the pain of encrypting massive amounts of data
- Prime yourself for security on the web
- Microsoft: Finding flaws on our website is OK
- Apple gets into

Hackers load malware onto Mercury music award site

Security nightmare for DreamHost

By [John Leyden](#) → [More by this author](#)
Published Thursday 7th June 2007 15:04 GMT

[Find out how to eradicate 99.7% of spam](#)

Hackers have been able to load malware onto the official Mercury music awards site, as well as hundreds of other sites, after breaking into the systems of US-based hosting firm DreamHost.

DreamHost blamed a security flaw in its web control panel software for an attack that allowed hackers to compromise a "very small subset" of user accounts. Affected customers have been notified by email. DreamHost said only web content - not credit card or billing information - was compromised.

In a [statement](#) published Wednesday, DreamHost said: "The security flaw allowed the attackers to log into our customer web control panel with the access privileges of another user. From our web panel they were able to access individual user password information. The attackers also attempted to gain access to our central database and billing information but were ultimately thwarted in that attempt. No credit card information or customer personal information was obtained."

DreamHost takes care of more than 500,000 domains, according to the firm. An email sent by DreamHost to its customers on 5 June, said approximately 3,500 separate FTP accounts were compromised by the hack. DreamHost has advised its customers to change their FTP account passwords immediately. The firm has promised to update concerned punters about the steps it is taking to prevent a repetition.

News of the attack followed just hours after DreamHost said it had upgraded its WebFTP systems. The timing of this announcement suggests this was more likely to have been part of DreamHost's efforts to put its house in order rather than the cause of its problems.

UK-based web security firm ScanSafe, which has been monitoring the attack, said attackers used the insecure web controls at DreamHost to load Trojan downloader malware onto well known and trusted sites. Confirmed targets of the attack include [nationwidemercury.com](#), the Mercury music awards site (which is sponsored by building society Nationwide), and UK law firm

WELCOME TO DARK MARKET

The Bazaar - DarkMarket - Mozilla Firefox

File Edit View Go Bookmarks Yahoo! Tools Help

http://www.darkmarket.ws/forumdisplay.php?f=20

Now: Sunny, 17° C Thu: 7° C Fri: 21° C Fri: 12° C Sat: 17° C Sat: 13° C Sun: 22° C Sun: 12° C Mon: 21° C

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Administration (Administrator) 10-03-2006

| | | Thread / Thread Starter | Rating | Last Post | Replies | Views |
|--|--|---|--------|--------------------------------------|---------|-------|
| | | Sticky: e-gold exchange still available JiLsi | | Yesterday 10:50 PM by JiLsi | 5 | 126 |
| | | rbc logins (1 2) toss | | Today 01:19 AM by toss | 12 | 190 |
| | | Tipper And Embosser For Sale.. wozney | | Yesterday 06:46 PM by soufly | 4 | 158 |
| | | Couple of hacked unix servers for SCAM Fake | | 10-17-2006 03:37 PM by Fake | 5 | 106 |
| | | 100 usa valid fullz for sale crimepays | | 10-17-2006 01:07 PM by ZDEVIL19 | 7 | 215 |
| | | Full infos with Bank account numbers Iceburg | | 10-17-2006 06:45 AM by underown | 1 | 79 |
| | | Halifax UK Logins (1 2) qlegit | | 10-17-2006 06:01 AM by qlegit | 10 | 177 |
| | | Zombie Computers DarkPimp | | 10-15-2006 06:14 PM by soufly | 5 | 258 |
| | | Need JCB cards,any country ibatistuta | | 10-15-2006 02:14 AM by ibatistuta | 2 | 42 |
| | | Need CVV2'S of this county Meki | | 10-14-2006 12:47 PM by Meki | 6 | 81 |
| | | canada banks workerbee | | 10-14-2006 01:15 AM by workerbee | 0 | 26 |
| | | Need Bank logins of this county esc | | 10-12-2006 07:39 AM by esc | 2 | 57 |
| | | Selling comcast and optonline accounts esc | | 10-12-2006 07:39 AM by esc | 4 | 81 |

DarkPimp offline
Member

Join Date: Jul 2006
Posts: 11

 **HIRING: Hacker, need to keylog someone**

I will supply you with IP, you will then get yourself in and install a keylogger.

Paying through egold and paypal.

PM me for full details and if you're willing to do this.

QUOTE

Latvian M, 18 Passport For Sale

09-04-2006, 05:55 PM

#1



Brady offline
Member

Join Date: Apr 2006
Posts: 1

Latvian M, 18 Passport For Sale

Agree to use escrow service, buyer pay fees.
The passport expires in 2010 year.

Anyone interested PM woth offers.
Will send a scan too.

QUOTE

3 European Amex Centurion Dumps

08-07-2006, 12:48 PM

#1



matrix001 Offline

Reviewed Vendor (CC Templates & Custom Graphics)

Join Date: Feb 200

Posts: 163



3 European Amex Centurion Dumps

dumps sold.

Last edited by matrix001 : 08-14-2006 at 03:20 PM.

QUOTE

08-13-2006, 09:17 AM

#1

glegit offline
Member *Use Escrow*

Join Date: Mar 200

Posts: 35



Hacked hosts

hi ppl
I am selling hacked hosts, available for scams and mailers etc.
PHP is supported
CPanel is supported
SSH is supported.

price is : 20 \$ per host.

(if u need more hosts i can give you discount)

icq : 251-611-896
yahoo: azuraza001

[i accept escrow]

C ya

QUOTE

DDos SERVICE

04-18-2006, 06:34 PM

#1

1s Offline

Trial Vendor (ddos service)

Join Date: Mar 200

Posts: 4

DDos SERVICE

I offer services DDos'a.
The prices: from 30 \$ up to 50 \$.

Preliminary check of service is possible. Anonymity of the order
It is completely guaranteed.

Contact icq: 112221111,
Write in offline on all your questions
There will be answers.

QUOTE

I have all this logins from UK.

Comes with DOB/SecurityNumber/ID

These are the accounts and prices, prices are negociable and if you're buying more than one i can make better deals. Escrow is ofcourse always accepted.

Have any questions you can email me at draxdrax@safe-mail.net

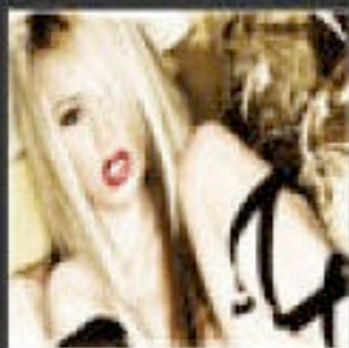
- 1 - Personal - 15 000 - 250GBP
- 2 - Personal - 3 000 - 50GBP
- 3 - Personal - 4 000 - 60GBP
- 4 - Personal - 1 000 - 20GBP
- 5 - Personal - 2 800 - 40GBP
- 6 - Personal - 2 000 - 30GBP
- 7 - Personal - 30 000 - 300GBP
- 8 - Personal - 1 000 - 20GBP
- 9 - Personal - 1 000 - 20GBP
- 10 - Personal - 800 - 10GBP
- 11 - Personal - 700 - 10GBP
- 12 - Personal - 3 600 - 55GBP
- 13 - Personal - 11 000 - SOLD
- 14 - Personal - 1 110 - 10GBP
- 15 - Personal - 500 - 10GBP
- 16 - Personal - 70 000 - 300GBP
- 17 - Personal - 13 000 - 250GBP
- 18 - Personal - 1 500 - 10GBP
- 19 - Personal - 1 200 - 10GBP
- 20 - Personal - 5 000 - 125GBP
- 21 - Personal - 6 000 - 135GBP
- 22 - Business - 2 700 - 50GBP
- 23 - Personal - 9 000 - SOLD
- 24 - Personal - 5 500 - 130GBP
- 25 - Personal - 2 700 - 40GBP

10-05-2006, 11:40 AM

#1



Join Date: Jul 2006
Posts: 118



Drax Offline
Verified Vendor (BANK LOGIN)
DM Reviewer
Canadian Moderator
Donator

Uk Logins

have some of this bank.
In this format

Customer Number:
Memorable Data:
Pass Number:
IP:

I have 3 accs with 10k+ , 11k, 50k, 220k. buy all for 750gbp or each for 300gbp

also have many accs with 1k - 20gbp each acc

QUOTE

19 - Personal - 1 200 - 10GBP
20 - Personal - 5 000 - 125GBP
21 - Personal - 6 000 - 135GBP
22 - Business - 2 700 - 50GBP
23 - Personal - 9 000 - SOLD
24 - Personal - 5 500 - 130GBP
25 - Personal - 2 700 - 40GBP

 **UK logins**

hi ppl
i have ~~bank~~ and other UK logins
msg me for deal
price is 3 - 5 % from balance ..
c ya 😊

QUOTE

 **Uk Logins**

have some of this bank.
In this format

Customer Number:
Memorable Data:
Pass Number:
IP:

I have 3 accs with 10k+ , 11k, 50k, 220k. buy all for 750gbp or each for 300gbp
also have many accs with 1k - 20gbp each acc

QUOTE

19 - Personal - 1 200 - 10GBP
20 - Personal - 5 000 - 125GBP
21 - Personal - 6 000 - 135GBP
22 - Business - 2 700 - 50GBP
23 - Personal - 9 000 - SOLD
24 - Personal - 5 500 - 130GBP
25 - Personal - 2 700 - 40GBP

various usa logs

09-14-2006, 03:06 PM

#1



Drax Offline
Verified Vendor (BANK LOGIN)
DM Reviewer
Canadian Moderator
Donator

Join Date: Jul 2006
Posts: 118

various usa logs

hi i have various amounts of usa logs, only login/pass.

banks such as ~~american express~~ etc.,

pm me if u need anythin

IP:

QUOTE

I have 3 accs with 10k+ , 11k, 50k, 220k. buy all for 750gbp or each for 300gbp

also have many accs with 1k - 20gbp each acc

QUOTE

19 - Personal - 1 200 - 10GBP
20 - Personal - 5 000 - 125GBP
21 - Personal - 6 000 - 135GBP
22 - Business - 2 700 - 50GBP
23 - Personal - 9 000 - SOLD
24 - Personal - 5 500 - 130GBP
25 - Personal - 2 700 - 40GBP

Bluetooth

New antenna ups Bluetooth range to 30 Kilometers

Posted by [Joshua Karp](#) on Jul 2, 2007 10:11 am

[2 Comments](#)

Filed in [News](#)



Yeah, you read that right. The newly announced AIRcable Host XR [Bluetooth USB Adapter](#) extends your average 3 meter Bluetooth range to just over 30 Kilometers. How far is that is America, you might ask? Roughly 19 miles. Whoa. Before you all get too excited, you should know that some level of "professional installation" is required to achieve the increased length. Without the pro-level tweaking you'll get 2 kilometers out of the box, which is still pretty impressive. Bluetooth range has been pushed to these lengths before, but the \$129 price point of this particular box makes it one of the first to be in range of the average consumer. Let the games begin!

[Read](#)

AIRCABLE

BLUETOOTH WITH RANGE!

PROGRAMMABLE, WIRELESS
SENSOR INTERFACES &
DATA LOGGERS WITH RANGE!

Bluetooth® WITH RANGE AS FAR
AS THE EYE CAN SEE...

UP TO
30 KM!

**AIRCable
Host XR**
LONG-RANGE
BLUETOOTH
"DONGLE"

**AIRCable
Industrial XR**
LONG-RANGE
PROGRAMMABLE
SENSOR INTERFACE

AIRCable SMD
THE WIRELESS, PROGRAMMABLE
MICRO-CONTROLLER (W-PLC)

COMPANY PRODUCTS TECHNOLOGIES SUPPORT APPLICATIONS CONTACT US

All

Device Oriented Tree View

| Device | Type | Address | Manufacturer | # o... | Note | First Seen | Last Seen | F | C | Auth |
|----------------|---------------------|-------------------|------------------------|--------|------|---------------------|---------------------|---|---|------|
| All Devices | | | | | | | | | | |
| Computer | | | | | | | | | | |
| (Local) | Desktop Workstation | 00:02:72:C0:6B:49 | CC&C Technologie... | 2 | | 09:58:00 05/20/2008 | 09:58:00 05/20/2008 | | | |
| Phone | | | | | | | | | | |
| N/A | Mobile phone | 00:15:DE:93:EC:BA | Sage Instruments I... | 0 | | 09:58:06 05/20/2008 | 09:58:06 05/20/2008 | | | |
| Fuzik SAMSU... | Mobile phone | 00:17:D5:1B:E7:91 | | 8 | | 09:58:43 05/20/2008 | 10:04:13 05/20/2008 | | | |
| K800i (Anomet) | Mobile phone | 00:19:63:9D:AD:D6 | | 14 | | 10:02:51 05/20/2008 | 10:05:06 05/20/2008 | | | |
| N/A | Mobile phone | 00:1C:D6:7C:4B:89 | | 0 | | 10:00:35 05/20/2008 | 10:02:51 05/20/2008 | | | |
| N/A | Mobile phone | 00:1D:98:56:2A:7F | | 0 | | 09:59:41 05/20/2008 | 10:05:06 05/20/2008 | | | |
| N/A | Mobile phone | 00:1E:45:2D:CD:54 | | 0 | | 10:04:13 05/20/2008 | 10:04:13 05/20/2008 | | | |
| DuKe E60 | Smart phone | 00:12:D2:35:8D:99 | Perception Digital ... | 12 | | 09:58:06 05/20/2008 | 10:05:06 05/20/2008 | | | |
| Kuralkan e61i | Smart phone | 00:12:D2:9E:AB:BE | Perception Digital ... | 13 | | 09:58:06 05/20/2008 | 10:05:06 05/20/2008 | | | |
| Milan | Smart phone | 00:19:2D:42:EA:01 | | 11 | | 09:58:06 05/20/2008 | 09:59:41 05/20/2008 | | | |
| Pawel W/ | Smart phone | 00:1A:89:0D:1C:14 | | 9 | | 09:58:06 05/20/2008 | 10:01:17 05/20/2008 | | | |
| Dodo N73 | Smart phone | 00:1C:35:66:E3:91 | | 13 | | 10:00:35 05/20/2008 | 10:01:50 05/20/2008 | | | |
| Nokia N73 | Smart phone | 00:1C:35:6A:6A:3A | | 12 | | 09:58:06 05/20/2008 | 10:05:06 05/20/2008 | | | |

Device Note:

| Service Name | Description | Service UUID | First Seen | Last Seen |
|---------------------------|-------------------------------|--------------|---------------------|---------------------|
| Limited Service Discovery | SDP Server | 0x1000 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| AV Remote Control Target | AVRCP TargetAudio Video ... | 0x110C | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Dial up Networking | Dial-Up Networking | 0x1103 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| OBEX Object Push | OBEX Object Push | 0x1105 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Handsfree Audio Gateway | Hands-Free Audio Gateway | 0x111F | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Headset Audio Gateway | Headset Audio Gateway | 0x1112 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Audio Source | Audio Source | 0x110A | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Imaging Repsonder | Imaging | 0x111B | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Unknown | SyncMLClient | 0x2 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| OBEX File Transfer | OBEX File Transfer | 0x1106 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Unknown | Nokia OBEX PC Suite Servic... | 0x5005 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Unknown | Nokia SyncML Server | 0x5601 | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |
| Unknown | SIM Access | 0x112D | 10:00:51 05/20/2008 | 10:01:59 05/20/2008 |

Security Posture Assessment



- About SPA
- Things We've Found

About SPA

- SPA is a 'snap shot' of the current state of a network, identifying and detailing how the network can be compromised and so highlighting risk factors

A hybrid **penetration test** and **vulnerability assessment**

- Delivered using a combination of **commercial and proprietary tools**

The proprietary tools are developed and maintained in house with capabilities that extend beyond standard commercial tools, both in terms of efficiency and robustness

- SPA is available in two 'families':

Vector-defined: how unauthorised access is gained to a network

Functional: testing an aspect of network functionality

About SPA

External SPA

Assessment Description

- Conducted from Cisco SOC
- Identify Internet visible vulnerabilities

Value Proposition

- Mature service offering
- Proprietary tools
- Industry leading expertise

Impact

- Protect intellectual capital
- Harden Internet perimeter



Wireless SPA

Assessment Description

- Locate rogue access points
- Review 802.11 security

Value Proposition

- Joint NAR offering with WWWP
- Proprietary tools
- Industry leading expertise

Impact

- Protect intellectual capital
- Locate and disable backdoors



Internal SPA

Assessment Description

- On-site inspection
- Trusted insider perspective

Value Proposition

- Mature service offering
- Proprietary tools
- Industry leading expertise

Impact

- Protect intellectual capital
- Meet compliance requirements
- Mergers and acquisitions



About SPA

Unified Communications SPA

Assessment Description

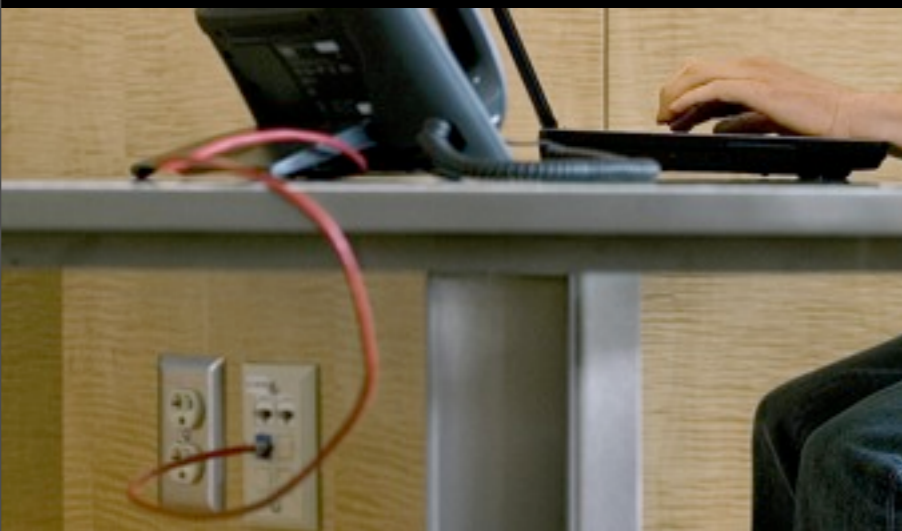
- On-site assessment
- Trusted insider perspective
- Identify VoIP / IPT vulnerabilities

Value Proposition

- Proprietary tools
- Industry leading expertise

Impact

- Protect intellectual capital
- Meet compliance requirements
- Mergers and acquisitions



Web Application SPA

Assessment Description

- In-depth review of web app(s)
- Black-box and white-box testing
- Integrate into development lifecycle

Value Proposition

- Proprietary tools
- Industry leading expertise

Impact

- Protect intellectual capital
- Meet compliance requirements
- Harden web applications



“Leak Test”

Assessment Description

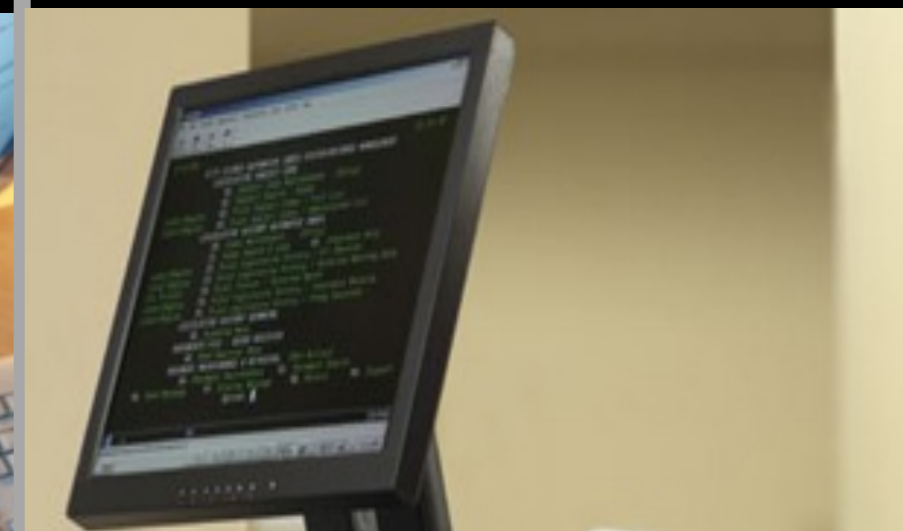
- Locate unauthorized Internet access
- Collector - injector architecture
- On-site assessment

Value Proposition

- Proprietary tools
- Industry leading expertise

Impact

- Protect intellectual capital
- Meet compliance requirements
- Mergers and acquisitions



About SPA

| Features | Managed vulnerability scan (e.g. Qualys) | Traditional penetration test | Cisco SPA (vector-defined) |
|--|---|------------------------------|-------------------------------|
| Automated ICMP (ping) scan | ✓ | ✓ | ✓ |
| Full TCP and UDP scans for asset fingerprinting | ✓ | ✗ | ✓ |
| In-depth vulnerability scan | ✓ | ✗ | ✓ |
| Manual confirmation of vulnerabilities through secondary exploitation, so removing false positives | ✗ | ✗ | ✓ |
| Wireless Access Point configuration review, rogue AP detection and wireless authentication analysis | ✗ | ✗ | ✓ |
| Understand and prove how vulnerabilities on one system can be exploited to provide access to another | ✗ | ✗ | ✓ |
| Prove and report unauthorised system access | ✗ | ✓ | ✓ |
| Validate compliance against relevant parts of ISO27001 framework and industry best practices | ✗ | ✗ | ✓ |
| Formal report, including in-depth analysis specific to your network, by security experts | ✗ | ✗ | ✓ |
| Onsite report presentation / workshop | ✗ | ? | ✓ |

About SPA

- Why is a vector-defined SPA different from a penetration test or vulnerability assessment service?

Comprehensive approach – we look for all ways into the network, not just a sampling of some IPs, attack vectors, etc.

Confirm the presence of vulnerabilities on network – leverage non-destructive exploits to gain root access, prove the risk

Prioritize vulnerabilities – all vulnerabilities are rated (low, medium or high) to help prioritise remediation efforts

Perform secondary exploitation – skilled security experts undertake a detailed analysis of how vulnerabilities can be used in combination to gain unauthorized access

CONCLUSION – GINSBERG THEOREM

CONCLUSION – GINSBERG THEOREM

- **You can't win!**

CONCLUSION – GINSBERG THEOREM

- **You can't win!**
- **You can't break even!**

CONCLUSION – GINSBERG THEOREM

- You can't win!
- You can't break even!
- You can't even quit the game!

Ehrmans Corollary to Ginsberg's Theorem

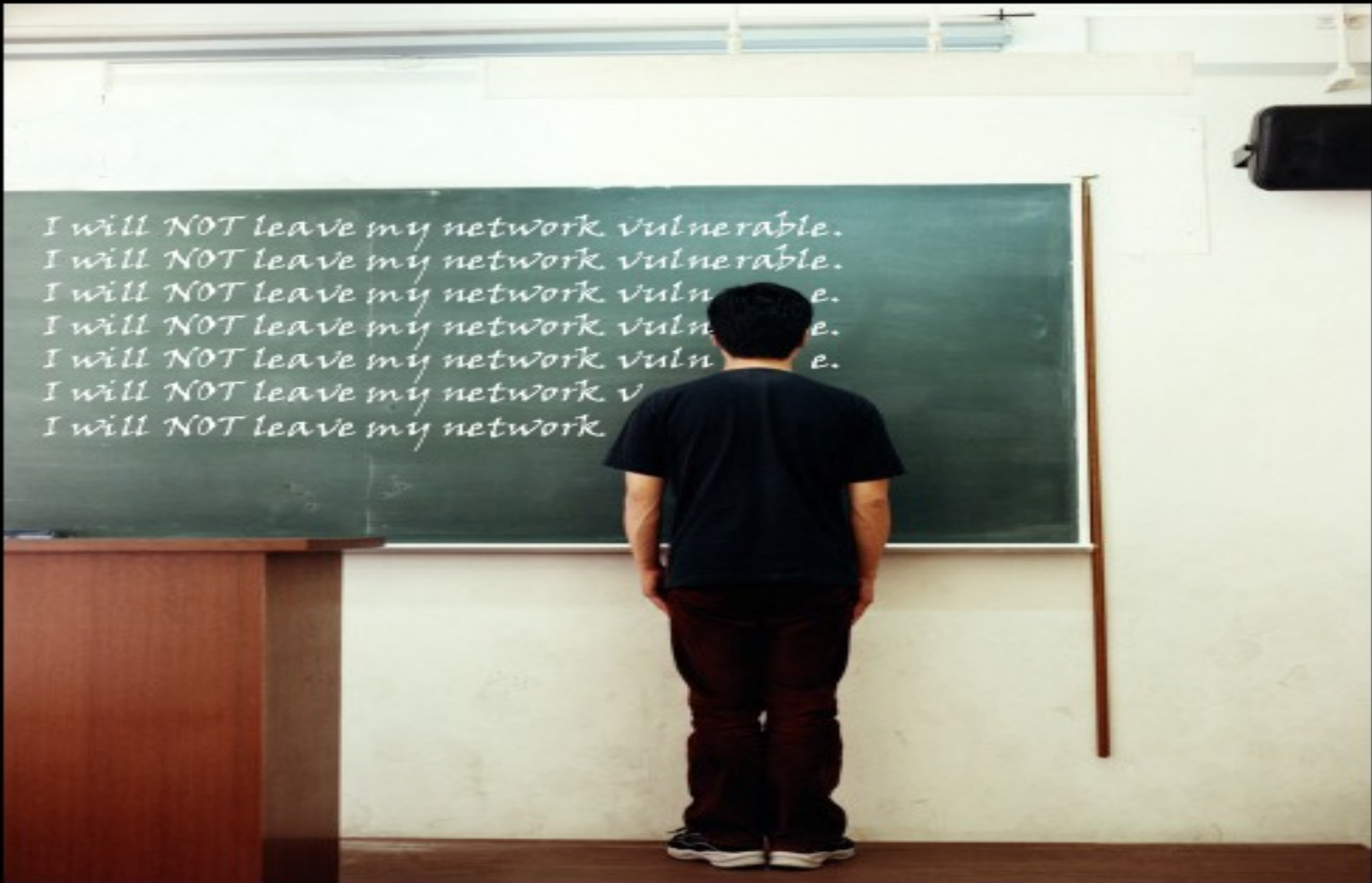
- Things will get worse before they get better!
- Who said things would get better??



Ehrmans Corollary to Ginsberg's Theorem



Conclusion...

A person with short dark hair, wearing a black t-shirt and dark pants, stands with their back to the camera, looking at a green chalkboard. The chalkboard is mounted on a white wall and contains seven lines of text written in white chalk. The text is a repetitive phrase: "I will NOT leave my network vulnerable." The first two lines are complete, and the subsequent five lines are progressively truncated from the right side. To the left of the person is a wooden podium. A black rectangular object, possibly a projector or a bag, is mounted on the wall to the right of the chalkboard.

I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulner e.
I will NOT leave my network vulner e.
I will NOT leave my network vulner e.
I will NOT leave my network v
I will NOT leave my network

