

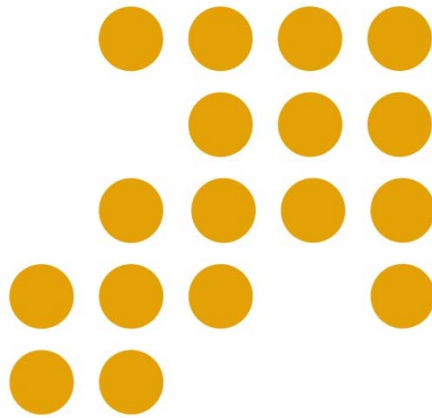


# Cyber Security Policy Research Division

## CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

**Report No. 13 – September 2010**

**1 September 2010**



CyberSecurity Malaysia  
Level 8, Block A,  
Mines Waterfront Business Park  
No 3, Jalan Tasik  
The Mines Resort City  
43300 Seri Kembangan  
Selangor Darul Ehsan

*Securing Our Cyberspace*



An agency under  
**mosti**  
Ministry of Science,  
Technology and Innovation

## TABLE OF CONTENTS

<b>DISCLAIMER .....</b>	<b>iii</b>
<b>1 FRAUD .....</b>	<b>1</b>
<b>1.1 MIAMI MAN PLEADS GUILTY IN ID THEFT CASE.....</b>	<b>1</b>
<b>1.2 MOSCOW PROBES ALLEGED RANSOMWARE GANG.....</b>	<b>1</b>
<b>1.3 TOP SCAMS ON THE WEB .....</b>	<b>1</b>
<b>1.4 ATM CLONING: PROBE TEAM TO CORROBORATE FRAUD DETAILS ...</b>	<b>2</b>
<b>1.5 FACEBOOK SCAM: "10 THINGS ADULTS NEVER TELL THEIR KIDS"....</b>	<b>2</b>
<b>1.6 FRAUD AT SPRINT OFFERS LESSONS FOR ENTERPRISES.....</b>	<b>2</b>
<b>1.7 GOOGLE INSTANT A POTENTIAL BONANZA FOR SEARCH SCAMS .....</b>	<b>3</b>
<b>1.8 HOTEL SYSTEMS BREACHED AND CARD INFO STOLEN ALL OVER         THE U.S.....</b>	<b>3</b>
<b>2 HACK THREAT/INTRUSION .....</b>	<b>3</b>
<b>2.1 CYBER THIEVES STEAL NEARLY \$1,000,000 FROM UNIVERSITY OF         VIRGINIA COLLEGE.....</b>	<b>3</b>
<b>2.2 ALGERIAN HACKERS ATTACK WRONG WEBSITE .....</b>	<b>4</b>
<b>2.3 WIRELESS CAR HACKING DUE TO POOR SECURITY .....</b>	<b>4</b>
<b>2.4 RBS WORLDPAY HACKER GETS FOUR YEARS' PROBATION .....</b>	<b>4</b>
<b>2.5 UK HACKER FINED FOR PERSONNEL DATABASE MISCHIEF.....</b>	<b>5</b>
<b>2.6 EMPLOYEE CHARGED WITH HACKING COMPUTER WITH PORN.....</b>	<b>5</b>
<b>2.7 SIENNA MILLER SET TO SUE 'NEWS OF THE WORLD' OVER PHONE         HACKING .....</b>	<b>5</b>
<b>3 PHISHING ATTACK .....</b>	<b>6</b>
<b>3.1 LABOR DAY PHISHING WARNING .....</b>	<b>6</b>
<b>4 MALWARE.....</b>	<b>6</b>
<b>4.1 RUSSIAN TROJAN BLAMED FOR CREDIT CARD LOSSES AT US         DINER.....</b>	<b>6</b>
<b>4.2 MALWARE HOSTED ON GOOGLE CODE PROJECT SITE.....</b>	<b>6</b>

**4.3 SLOVENIAN MARIPOSA SUSPECTS' IDENTITIES REVEALED ..... 7**

**5 BOTNET ..... 7**

**5.1 SPAMMERS STAY BUSY DESPITE PUSHDO BOTNET HIT ..... 7**

**5.2 BOTNET TAKEDOWN MAY YIELD VALUABLE DATA ..... 7**

**6 OTHERS ..... 8**

**6.1 CUSTOMER INFORMATION OF DRUGSTORE CHAIN EXPOSED ..... 8**

**6.2 UK CONSUMERS FACE 1 IN 63 CHANCE OF ATTACK ONLINE ..... 8**

**6.3 CAN YOU TRUST YOUR DATA RECOVERY VENDOR? ..... 8**

**6.4 THE EMOTIONAL IMPACT OF CYBERCRIME ..... 8**

**DISCLAIMER**

This document is a non-commercial publication intended to educate and disseminate information about security incidents reported outside Malaysia. Further reproduction or redistribution is subject to original copyright restrictions. CyberSecurity Malaysia provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

CyberSecurity Malaysia did not warrant the completeness or accuracy of the document and neither accepts any liability for losses howsoever incurred. The content on this site, including news, quotes, data and other information, is provided by third party content providers for your personal information only, and neither CyberSecurity Malaysia nor its third party content providers shall be liable for any errors, inaccuracies or delays in content, or for any actions taken in reliance thereon.

## 1 FRAUD

### 1.1 MIAMI MAN PLEADS GUILTY IN ID THEFT CASE

According to the U.S. Department of Justice, a Miami man has pleaded guilty to two identity-theft related charges after federal agents found more than 26,000 credit card numbers stored on his computer. Juan Javier Cardenas, 45, purchased stolen credit card numbers over the Internet between February 2008 and May 2009. He pleaded guilty in U.S. District Court for the Southern District of Florida to one count of conspiracy to traffic in and possess unauthorized credit card numbers with intent to defraud, and one count of trafficking in unauthorized credit card numbers. Between March and May 2009, Cardenas e-mailed more than 1,500 credit card numbers to five co-conspirators, according to a June indictment of Cardenas. Those co-conspirators used the compromised credit card numbers to make fraudulent purchases.

**Source: Computerworld, 1 September 2010**  
[http://www.computerworld.com/s/article/9183262/Miami\\_man\\_pleads\\_guilty\\_in\\_ID\\_theft\\_case?](http://www.computerworld.com/s/article/9183262/Miami_man_pleads_guilty_in_ID_theft_case?)

### 1.2 MOSCOW PROBES ALLEGED RANSOMWARE GANG

Russian police are reportedly investigating a criminal gang that installed malicious "ransomware" programs on thousands of PCs and then forced victims to send SMS messages in order to unlock their PCs. According to reports by Russian news agencies, the scam has been ongoing and may have made Russian criminals millions of dollars. Russian police seized computer equipment and detained a Russian "crime family" in connection with the crime. The criminals reportedly used news sites to spread their malicious software, known as WinLock, which disables certain Windows components, rendering the PC unusable,

and then displays pornographic images. To unlock the code, victims must send SMS messages that cost between 300 rubles (US\$9.72) and 1,000 rubles. The scam may have hit as many as 1 million PCs in the Russian-speaking world, according to Sergey Golovanov, a malware analyst with Russian antivirus vendor Kaspersky Lab. The scam has worked so well, because in many former Soviet-bloc countries telecommunication companies make it very easy for criminals to anonymously register the kind of paid phone numbers used to pay the ransom.

**Source: CSO, 1 September 2010**  
<http://www.csoonline.com/article/608563/moscow-probes-alleged-ransomware-gang?>

### 1.3 TOP SCAMS ON THE WEB

PandaLabs has drawn up a ranking of the most widely used scams over the last few years. These confidence tricks, which are still in wide circulation, all have the same objective: to defraud users of amounts ranging from \$500 to thousands of dollars. Typically, these scams follow a similar pattern: initial contact is made via email or through social networks. The intended victim is then asked to respond, either by email, telephone, fax, etc. Once this initial bait has been taken, criminals will try to gain the trust of the victim, finally asking for a sum of money under one pretext or another. Below are the most frequent scams of the last 10 years, based on their distribution and the frequency with which they are received.

- Nigerian scam
- Lotteries
- Girlfriends
- Job offers
- Facebook / Hotmail
- Compensation

- The mistake

**Source: Help Net Security, 1 September 2010**  
<http://www.net-security.org/secworld.php?id=9808&utm>

#### **1.4 ATM CLONING: PROBE TEAM TO CORROBORATE FRAUD DETAILS**

UT police is still clueless about the identity of those behind the ATM fraud, which came to light few days ago. Even as a criminal case has already been registered, sources in the UT police stated that the investigation team will now call all the complainants to know the exact details. Initially, maximum complainants had approached the State Bank of India and not the police. According to sources in the Chandigarh Police, cops have confirmed some of the ATMs from where huge transactions were made by unknown persons. According to the initial probe, it has been established that huge transactions were made from SBI ATMs situated in sectors 37, 36, 47, 22 and 17 of the city. Police are also corroborating the exact amount withdrawn from these ATM branches and the figures recorded in bank statements of the victims.

**Source: The Times of India, 2 September 2010**  
<http://timesofindia.indiatimes.com/city/chandigarh/ATM-cloning-Probe-team-to-corroborate-fraud-details/articleshow/6477144.cms>

#### **1.5 FACEBOOK SCAM: "10 THINGS ADULTS NEVER TELL THEIR KIDS"**

Another very effective scam has been spotted coursing through Facebook, aided perhaps by the long Labor Day weekend and people's wish to unwind and abundance of free time. The name of the page is "10 Things Adults Never Tell Their Kids", and you found about it the usual way: a friend of yours has "liked" it and has

shared the link with you. You followed the link, but no immediate fun followed. Instead, you first had to do follow what has become a usual procedure for this kind of scam: "like" the page, share the link, complete a survey. According to Graham Cluley, you just earned some money for the scammers, since they are paid for every filled out questionnaire. You have also practically recommended it to your friends, some of which will go on to perpetuate the scam circle.

**Source: Help net Security, 6 September 2010**  
<http://www.net-security.org/secworld.php?id=9828&utm>

#### **1.6 FRAUD AT SPRINT OFFERS LESSONS FOR ENTERPRISES**

The recently revealed abuse of insiders' system privileges to commit fraud at Sprint could be a wake-up call for other enterprises to implement more stringent security practices. Last week, nine Sprint employees were charged with misusing their access to the telecommunications giant's systems to redirect phone charges to other customers by "cloning" their cell phones -- to the tune of more than \$15 million in fraudulent charges in the first six months of this year. The case highlights the need for enterprises to implement controls that will help them catch insiders who might be focused on fraud, says Dawn Cappelli, technical manager of the threat and incident management team at Carnegie Mellon University's Software Engineering Institute CERT Program.

**Source: DarkReading, 8 September 2010**  
<http://www.darkreading.com/insiderthreat/security/management/showArticle.jhtml?articleID=227300424>

## **1.7 GOOGLE INSTANT A POTENTIAL BONANZA FOR SEARCH SCAMS**

Security watchers are concerned that scareware scammers may quickly adapt to the introduction of real-time search technology from Google to develop even more potent search engine poisoning attacks. Google Instant speeds up search results by working as users' type into the Google search box. The technology predicts what users are trying to type and rapidly makes suggestions on which search term is most relevant, all in real time. Blackhat SEO threats typically seek to make sure links to malicious sites are returned close to the top of searches for topical terms. The problem has bedeviled search engines for years and more recently has become the main tactic in promoting rogue anti-virus (AKA scareware) scam portals. Sean-Paul Correll, a security researcher at Panda Security, warns that this contamination of search results might become even worse with the advent of 'real-time' search.

**Source: The Register, 9 September 2010**  
[http://www.theregister.co.uk/2010/09/09/google\\_instant\\_black\\_hat\\_seo/](http://www.theregister.co.uk/2010/09/09/google_instant_black_hat_seo/)

## **1.8 HOTEL SYSTEMS BREACHED AND CARD INFO STOLEN ALL OVER THE U.S**

The payment system at a number of properties of HEI Hospitality - the hospitality operator that runs over 30 upscale hotels across the U.S. under brand names as Marriott, Hilton, Sheraton and others - has been breached and card data of some 3,400 customers has been compromised. The New Hampshire Attorney General's Office has been notified of the fact, and the customers whose data might have been stolen received a letter earlier this month notifying them of the occurrence. In the letter - sent to a customer who stayed at the Algonquin Hotel in New York - it states that

they believe the electronic point-of sale and the property management system used at check-in was "illegally accessed and credit card transactions processed between March 25, 2010 and April 17, 2010 were potentially subject to illegal interception." So far, they claim, there are no indications that the stolen information was misused, but they urge potential victims to keep an eye on their account statements and their credit reports. They have also provided them a one year free credit card monitoring service, which includes identity theft insurance.

**Source: Help Net Security, 8 September 2010**  
<http://www.net-security.org/secworld.php?id=9853&utm>

## **2 HACK THREAT / INTRUSION**

### **2.1 CYBER THIEVES STEAL NEARLY \$1,000,000 FROM UNIVERSITY OF VIRGINIA COLLEGE**

Cyber crooks stole just shy of \$1 million from a satellite campus of The University of Virginia last week. Kathy Still, director of news and media relations at UVA Wise, declined to offer specifics on the theft, saying only that the school was investigating a hacking incident. According to several sources familiar with the case, thieves stole the funds after compromising a computer belonging to the university's comptroller. The attackers used a computer virus to steal the online banking credentials for the University's accounts at BB&T Bank, and initiated a single fraudulent wire transfer in the amount of \$996,000 to the Agricultural Bank of China. BB&T declined to comment for this story. Sources said the FBI is investigating and has possession of the hard drive from the controller's PC. A spokeswoman at FBI headquarters in Washington, D.C. said that as a matter of policy the FBI does not confirm or deny the existence of investigations.

**Source: KrebsOnSecurity, 1 September 2010**

<http://krebsonsecurity.com/2010/09/cyber-thieves-steal-nearly-1000000-from-university-of-virginia-college/>

## **2.2 ALGERIAN HACKERS ATTACK WRONG WEBSITE**

A group of misinformed Algerian 'cyber-pirates' attacked the official website of the Belvoir Castle, mistaking it for the Belvoir Fortress in Israel. The pirate group, known as Dz-SeC, hijacked the website and displayed anti-Jewish slogans in Arabic on the homepage, along with a picture of the Algerian national flag. The Belvoir Fortress on the other hand, was initially a Christian military stronghold used for fending-off attacks from Muslim forces on the city of Jerusalem. However, the fortress fell under Muslim control, which they later had to relinquish following a brutal attack by Israeli forces. The hacker group claims that the attack on the website was due to Israel's presence and thanked other Algerian pirates for contributing to the attack.

Source: ITPortal, 1 September 2010\  
<http://www.itportal.com/portal/news/article/2010/9/1/algerian-hackers-attack-wrong-website/>

## **2.3 WIRELESS CAR HACKING DUE TO POOR SECURITY**

Research from the University of California San Diego and the University of Washington - and which concludes that modern cars are susceptible to wireless hacking - is the result of a security issues being ignored at the car electronics software design stage. With the latest cars now coming with as many as 50 or more interconnected computer systems - controlling everything from the brakes to the door locks and ignition system - now that the vehicles are becoming wirelessly-enabled, they are a lot easier to electronically hack into. "It's interesting to see that the researchers have identified that most cars built since the late 1990s have a computer diagnostic port, since this port needs direct physical access

to operate and therefore hack. But now these systems are being wirelessly enabled and held together with several tens of megabytes of code, it's a relatively small step to modify the code and allow hackers an easy - and wireless - back door into a car's computer system," said Barmak Meftah, CPO at Fortify Software. This was no theoretical exercise, as the researchers were able to load new firmware onto their own circuit board and, by plugging the board into the car's internal network, translate the data flowing between the vehicle and a laptop. This reverse engineering process allowed the researchers to develop a customized vehicle network interface and effectively take control of the car's electronic nervous system.

**Source: Help Net Security, 9 August 2010**  
<http://www.net-security.org/secworld.php?id=9826&utm>

## **2.4 RBS WORLDPAY HACKER GETS FOUR YEARS' PROBATION**

The mastermind behind one of the biggest hacking paydays in history has been sentenced to four years' probation and an US\$8.9 million fine. According to Bloomberg News, Victor Pleshchuk, 28, was sentenced to four years' probation. He is considered the leader of a group of criminals who organized a 2008 precision strike on RBS WorldPay, the payment processing division of the Royal Bank of Scotland. In addition to the reduced sentence of probation, Pleshchuk must also pay back more than 275 million rubles (\$8.9 million) to RBS WorldPay. In the RBS WorldPay hack, the criminals broke into the company's back-end system and downloaded enough data to make duplicate corporate debit cards, which are typically used by employees to withdraw money on payday. Then, using an international network, they took money out of victims' bank accounts using their phony cards. Prosecutors say Pleshchuk and his

gang took \$9.4 million by hitting more than 2,100 ATMs in at least 280 cities around the world during the 12-hour window of their November 2008 attack. It remains one of the most successful computer crimes ever.

**Source: Computerworld, 8 September 2010**  
[http://www.computerworld.com/s/article/9184179/Report\\_RBS\\_WorldPay\\_hacker\\_gets\\_four\\_years\\_probation](http://www.computerworld.com/s/article/9184179/Report_RBS_WorldPay_hacker_gets_four_years_probation)

## **2.5 UK HACKER FINED FOR PERSONNEL DATABASE MISCHIEF**

A court has ordered a UK hacker to pay compensation after he used a purloined laptop to hack into his ex-employer's personnel database. Colin Parker, 31, gained unauthorized access to staff contracts containing salary details and emailed this to around 400 workers at his ex-employer, CHI and Partners. Parker's attempt to create bad feeling among workers at the firm was foiled by an alert system admin, who intercepted and deleted the potentially incendiary emails. Parker, who was found responsible for the theft of a laptop and given a conditional discharge, agreed to pay his ex employer CHI and Partners £4,000 in compensation and £3,000 in prosecution costs to settle the case during a hearing at Southwark Crown Court on Monday. He is liable for 12 months' imprisonment if he fails to satisfy these conditions, a spokesman for Southwark Crown Court confirmed.

**Source: The Register, 8 September 2010**  
[http://www.theregister.co.uk/2010/09/08/salary\\_database\\_hack/](http://www.theregister.co.uk/2010/09/08/salary_database_hack/)

## **2.6 EMPLOYEE CHARGED WITH HACKING COMPUTER WITH PORN**

It happened one day last year, as more than a dozen board members of a Baltimore substance abuse center had gathered around a conference room. The CEO was

giving a PowerPoint presentation on his accomplishments. Suddenly, his computer shut down, then restarted, replacing the latest slide with an image of a naked woman onto a 64-inch screen. The board members include city officials and foundation heads and are chaired by Baltimore's health commissioner. Today, Baltimore's State's Attorney's Office announced a grand jury had indicted Walter Powell, 51, with hacking into the computer system. They described him as a disgruntled worker who allegedly used his home computer to access the system, distribute confidential emails from his boss and break into the presentation. The CEO of the Baltimore Substance Abuse System Inc., which distributes public funds to more than 50 substance abuse programs helping thousands of people, told the attack cost \$80,000 mostly to rebuild the system, replace software and upgrade security measures.

**Source: The Baltimore Sun, 8 September 2010**  
[http://weblogs.baltimoresun.com/news/crime/blog/2010/09/employee\\_charged\\_with\\_hacking.html](http://weblogs.baltimoresun.com/news/crime/blog/2010/09/employee_charged_with_hacking.html)

## **2.7 SIENNA MILLER SET TO SUE 'NEWS OF THE WORLD' OVER PHONE HACKING**

The actress Sienna Miller is poised to become the latest litigant to join a growing queue of high-profile figures seeking damages from the publishers of the News of the World newspaper over the illegal hacking of voicemail messages. It also emerged last night that Sean Hoare, the reporter whose testimony was central to The New York Times's article that reignited the phone-hacking controversy, has been interviewed by police under caution. Her mobile phone was targeted by Glenn Mulcaire, a private investigator hired by the News of the World at a cost of £100,000-a-year. Mulcaire was jailed for six months in January 2007 for phone hacking. Mulcaire admitted hacking into the voicemail

messages of aides to the royal family as well as several high-profile figures including Gordon Taylor, the chief executive of the Professional Footballers' Association and Max Clifford, the publicist. Both Mr Taylor and Mr Clifford have taken action against Rupert Murdoch's News Group, the publishers of the News of the World, and both claims were settled out of court for around £1m each.

**Source: *The Independent*, 15 September 2010**

<http://www.independent.co.uk/news/media/press/sienna-miller-set-to-sue-news-of-the-world-over-phone-hacking-2079555.html>

### **3 PHISHING ATTACK**

#### **3.1 LABOR DAY PHISHING WARNING**

Due to the upcoming Labor Day holiday, consumers are at high risk for targeted phishing attacks due to the preponderance of online retail sales events over the holiday weekend. Amidst the flurry of emails promoting holiday sales are fraudulent messages that include bogus links to sites that download malicious software or phishing sites soliciting personal information. While research from companies like IBM have suggested that phishing attacks were on the decline last year, GFI warns that customers should not be lulled into a false sense of security. According to Phishtank.com, there are over 2,900 active phishing web sites currently verified on the internet. Furthermore, the popularity of social media sites such as Facebook and Twitter has made them attractive platforms for holiday-themed attacks.

**Source: *Help net Security*, 3 September 2010**

<http://www.net-security.org/secworld.php?id=9819&utm>

### **4 MALWARE**

#### **4.1 RUSSIAN TROJAN BLAMED FOR CREDIT CARD LOSSES AT US DINER**

Hundreds of lunchtime customers of a diner in the US city of Memphis are believed to have had funds stolen from their debit and credit cards after PCs at the venue became infected with malware. Large numbers of customers reported having had funds taken after using Jason's Deli in recent weeks, which prompted an investigation by the US Secret Service, part of the Department of Homeland Security. After establishing that staff were not involved, police discovered that a computer system used to verify credit cards had been infected with new variant malware, which intercepted and forwarded the details to criminals believed to be in Russia. "The computers received a virus that was unknown before this event. No antivirus program that we ran against it found it," said Special Agent Rick Harlow of the US Secret Service in a news conference. The sums involved are thought to be significant. One local report cited an unnamed individual as having lost \$793.

**Source: *Network World*, 1 September 2010**

<http://www.networkworld.com/news/2010/09/0110-russian-trojan-blamed-for-credit.html>

#### **4.2 MALWARE HOSTED ON GOOGLE CODE PROJECT SITE**

According to researchers at Zscaler, malicious hackers are using the Google Code repository to host Trojans horses, backdoors and password stealing key loggers. The researchers found a malicious project hosted on the free Google Code site with about 50+ malware executables stored in the download section of the project. According to Zscaler's Umesh Wanve, most of the files are executable files along with zipped ".rar" files. Wanve said the first malicious file was uploaded on June 24, 2010 and was still active at the end of

August this year, proving that Google is slow to find and remove malicious projects.

**Source: Zero Day, 1 September 2010**  
<http://www.zdnet.com/blog/security/malware-hosted-on-google-code-project-site/7247?tag=nl.e019>

### **4.3 SLOVENIAN MARIPOSA SUSPECTS' IDENTITIES REVEALED**

A month has passed since the Mariposa malware author was arrested in Slovenia, and more details about the case have surfaced in the meantime. The Slovenian police say that they have performed several house searches and confiscated 75 pieces of computer equipment. They detained two suspects (aged 23 and 24), who are facing charges for creation of tools that enable computer crime and money laundering. According to Panda Security, that's all the information that the police has shared with the public. But, the media mounted its own investigation and unearthed the identities of the two suspects.

**Source: Help Net Security, 1 September 2010**  
<http://www.net-security.org/secworld.php?id=9814>

## **5 BOTNET**

### **5.1 SPAMMERS STAY BUSY DESPITE PUSHDO BOTNET HIT**

The disruption of the Pushdo botnet has not stopped spammers, despite nearly two-thirds of the botnet's command and control servers being taken out of commission. From the shutdown of McColo to last week's disruption of the Pushdo botnet, spammers have continually found ways to stay in business. Nearly 20 of the 30 command and control (CnC) servers associated with Pushdo were taken offline last week due to efforts by security vendor LastLine. The servers were supported by eight hosting

providers, some of which did not respond to the vendor's requests for action. According to Thorsten Holz, senior threat analyst with LastLine, the goal of the company's research was not to completely take down the botnet, but to gain insight into Pushdo's CnC infrastructure. At full strength, the botnet was believed to be responsible for between 7 and 10 percent of all spam.

**Source: eWEEK.com 1 September 2010**  
<http://www.eweek.com/c/a/Security/Spammers-Stay-Busy-Despite-Pushdo-Botnet-Hit-176895/>

### **5.2 BOTNET TAKEDOWN MAY YIELD VALUABLE DATA**

Researchers are hoping to get a better insight on botnets after taking down part of Pushdo, one of the top five networks of hacked computers responsible for most of the world's spam. Thorsten Holz, an assistant professor of computer science at Ruhr-University in Bochum, Germany, said his group is working on an academic paper focused on methods to figure out what type of malicious spamming software is on a computer that sent a particular spam e-mail. They looked at several of the major spamming botnets, including Mega-D, Lethic, Rustock as well as Pushdo and Cutwail, two kinds of malware that appear to sometimes work together as part of the same botnet. About 15 of Pushdo's 30 servers were with that one hosting provider, which has now taken those servers offline and shared the data contained within them with Holz and his team. Their analysis is still ongoing, but they uncovered some 78 GB of plain text e-mail addresses, and that up to 40% of the infected computers were in India.

**Source: Computerworld, 2 September 2010**  
[http://www.computerworld.com/s/article/9183299/Botnet\\_takedown\\_may\\_yield\\_valuable\\_data](http://www.computerworld.com/s/article/9183299/Botnet_takedown_may_yield_valuable_data)

## 6 OTHERS

### 6.1 CUSTOMER INFORMATION OF DRUGSTORE CHAIN EXPOSED

Personal information of 150,000 online customers of the German drugstore chain Schlecker was available online for everyone to access due to an error of the chain's service provider. The situation has been rectified and the information is now safe, but for an unspecified period of time names, addresses and profiles of the customers, and some 7.1 million email addresses of the customers who are on the list for receiving the company newsletter, were available for anyone to harvest. Schlecker's spokesman made sure to mention that account numbers and passwords were not compromised in any way, but the information that was accessible could be enough for criminals to effectively impersonate the company and contact the customers through the publicly available mail server. The victims could then be persuaded to make their purchases and, thus, hand over their bank account details to the criminals.

**Source: Help Net Security, 1 September 2010**  
<http://www.net-security.org/secworld.php?id=9813&utm>

### 6.2 UK CONSUMERS FACE 1 IN 63 CHANCE OF ATTACK ONLINE

A new survey by antivirus vendor AVG has found that the chances of a UK internet user having the security of their computers compromised by malware or other hacking techniques are one in 64, which is significantly higher than the global average. The UK was ranked 30th in a list that analysed the world's most dangerous locations in which to browse the internet. AVG has analysed data from over one hundred million computers located in 144 different countries to come to this conclusion. The average risk of attack is said to be one in 73, which marks out the UK as being riskier than Africa and China

when it comes to safe shopping online. AVG's Roger Thomson pointed out that under the right conditions it is possible for consumers to greatly reduce their chances of being infected with malware or duped by online scams, as long as proper precautions are taken.

**Source: shopsafe.co.uk, 2 September 2010**  
<http://www.shopsafe.co.uk/news/uk-consumers-face-1-in-63-chance-of-attack-online/10138>

### 6.3 CAN YOU TRUST YOUR DATA RECOVERY VENDOR?

Many government and private-sector organizations consider recovering data from damaged laptop PC hard drives to be a minor budget item that third-party vendors can best handle. But a seemingly inexpensive fix could lead to compromised or stolen data, network breaches and other security nightmares because organizations typically do not vet data recovery vendors. The National Institute of Standards and Technology has issued new guidelines to resolve that problem, but it will be at least a year before agencies are required to fully comply with it. When recovering intellectual property or sensitive documents stored in damaged equipment, major security problems can arise if agencies or companies have not paid attention to vetting data recovery vendors.

**Source: Government Computer News, 3 September 2010**  
<http://gcn.com/articles/2010/09/06/data-recovery-vetting.aspx>

### 6.4 THE EMOTIONAL IMPACT OF CYBERCRIME

A new study by Norton reveals the staggering prevalence of cybercrime: 65% of Internet users globally, and 73% of U.S. Web surfers have fallen victim to cybercrimes, including computer viruses, online credit card fraud and identity theft. As the most victimized nations, America ranks third, after China (83%), Brazil and

India (76%). The first study to examine the emotional impact of cybercrime, it shows that victims' strongest reactions are feeling angry (58%), annoyed (51%) and cheated (40%), and in many cases, they blame themselves for being attacked. Only 3% don't think it will happen to them, and nearly 80% do not expect cybercriminals to be brought to justice— resulting in an ironic reluctance to take action and a sense of helplessness. Despite the emotional burden, the universal threat, and incidents of cybercrime, people still aren't changing their behaviors - with only half (51%) of adults saying they would change their behavior if they became a victim. Even scarier, fewer than half (44%) reported the crime to the police.

**Source: Help Net Security, 8 September 2010**  
<http://www.net-security.org/secworld.php?id=9837&utm>