

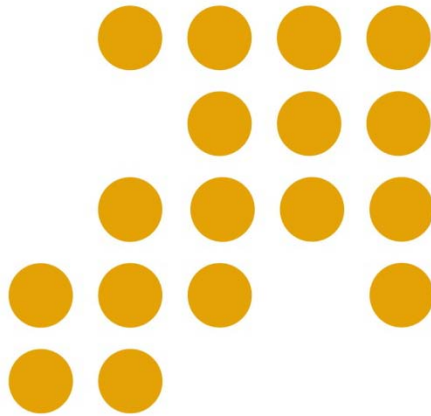


## Cyber Security Policy Research Division

### CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 4 – April 2010

**01 April 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> .....	iii
<b>FRAUD</b> .....	1
1. <b>FAKE GIFT CARD SCAMS ON FACEBOOK</b> .....	1
2. <b>UNDER PROTECTED CORPORATE SECRETS</b> .....	1
3. <b>70 ROMANIAN CYBER CROOKS ARRESTED</b> .....	1
4. <b>BANK EMPLOYEE ACCUSED OF STEALING FROM "INFECTED" ATMS</b> .....	2
5. <b>PLENTY OF CREDIT CARD FRAUD AND IDENTITY THEFT</b> .....	2
6. <b>SCAMMERS' LINK ARCHITECTURES</b> .....	2
<b>MALWARE</b> .....	3
7. <b>1,800 OFFICE BUGS DISCOVERED BY MICROSOFT'S "FUZZING BOTNET"</b> .....	3
8. <b>TROJANS ARE THE MOST CONSTANT INFECTIOUS VECTOR</b> .....	3
9. <b>BOTNETS DRIVE THE RISE OF RANSOMWARE</b> .....	3
10. <b>GLOBAL REPOSE TO CONFICKER THREAT: MODEL FOR FUTURE CYBER THREAT RESPONSE?</b> .....	4
11. <b>CLOSING THE LAST DOOR</b> .....	4
12. <b>GENERIC AND BEHAVIOR-BASED THREATS INCREASING</b> .....	4
13. <b>FIRESHARK: LINKING THE MALICIOUS WEB</b> .....	5
<b>HACK THREAT/INTRUSION</b> .....	5
14. <b>MANY TEENAGERS HACK AND RARELY GET CAUGHT</b> .....	5
15. <b>9-YEAR-OLD BLAMED FOR HACKING SCHOOL SYSTEM</b> .....	5
16. <b>NETWORK SOLUTIONS CUSTOMERS TARGETED BY NEW HACK ATTACK</b> .....	6
17. <b>RUSSIAN HACKER OFFERS 1.5M FACEBOOK CREDENTIALS FOR SALE</b> ..	6
<b>SPAM</b> .....	6
18. <b>GAMES ON SOCIAL NETWORKS INCREASE SPAM AND PHISHING BY 50%</b> .....	6
19. <b>FACEBOOK WILL NOT START CHARGING USERS</b> .....	7
20. <b>SPAMMERS USE THE FAMILIAR TO INSPIRE ACTION</b> .....	7
21. <b>ESCALATION OF PHARMA SPAM FROM GMAIL ACCOUNT</b> .....	7
22. <b>THE US CONTINUES ITS REIGN AS THE KING OF SPAM</b> .....	8

<b>PHISHING ATTACK.....</b>	<b>8</b>
<b>23.HOW TO DETECT A PHISHING WEBSITE, THE GOOGLE WAY .....</b>	<b>8</b>
<b>24.IS PHONE PHISHING MAKING A COMEBACK? .....</b>	<b>8</b>
<b>25.PHISHING STUDENT LOANS' PAGES TARGET STUDENTS .....</b>	<b>9</b>
<b>26.FAKE FAST FOOD SURVEY WITH CASH REWARD LEADS TO PHISHING SITE .....</b>	<b>9</b>
<b>OTHERS.....</b>	<b>9</b>
<b>27. STALKER JAILED FOR PLANTING CHILD PORN ON A COMPUTER .....</b>	<b>9</b>
<b>28.HEALTHCARE INDUSTRY OVERLOOKS CRITICAL GAP IN DATA SECURITY .....</b>	<b>10</b>
<b>29.U.S. INFRASTRUCTURE AT RISK FROM SOPHISTICATED CYBER ATTACKS .....</b>	<b>10</b>
<b>30.DATA BREACHES COST AUSTRALIAN COMPANIES MILLIONS .....</b>	<b>10</b>
<b>31.PREVENT UNAUTHORIZED ELECTRONIC FUND TRANSFER .....</b>	<b>11</b>
<b>32.ENDPOINT DATA LEAK PREVENTION STILLS A MAJOR HEADACHE. ....</b>	<b>11</b>
<b>33.FUTURE AIR TRAVEL SECURITY RISKS, PRIVACY AND SOCIAL IMPLICATIONS .....</b>	<b>11</b>
<b>34.MEDICAL RECORDS SECURED BY CODE-CHANGING ALGORITHM.....</b>	<b>12</b>
<b>35.FACEBOOK BUILDS UP ITS DEFENSES .....</b>	<b>12</b>
<b>36.USER ACCESS CONTINUES TO BE POORLY MANAGED .....</b>	<b>12</b>
<b>37.DATA INTEGRITY ATTACKS A GROWING THREAT .....</b>	<b>13</b>
<b>38.CLOUD COMPUTING AND SOCIAL NETWORKING EXPOSE BUSINESSES TO ATTACKS .....</b>	<b>13</b>
<b>39.SPLUNK.COM PASSWORD LEAK .....</b>	<b>13</b>
<b>40.THE STAGGERING COST OF DATA BREACH .....</b>	<b>13</b>
<b>41.MAJORITY UNWARE OF HOW SENSITIVE DATA IS STORED ONLINE .....</b>	<b>14</b>

**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.

## **FRAUD**

### **1. FAKE GIFT CARD SCAMS ON FACEBOOK**

Whole Foods Market, a Texas supermarket chain, has been fighting the latest gift card scam that takes advantage of the company well-known brand by offering a \$500 gift card to lure Facebook users to part with their personal and credit card information. According to CNet, the scam artists have set up a couple of "fan pages" with names that misuse the company name to gain an aura of legitimacy ("Whole Foods FREE \$500 Gift Card! Only Available for 36 hours!", "Whole Foods Market Free \$500 Gift Card Limited - first 12,000 fans only") and entice the users to become a "fan". To get the gift card, they are asked to fill out a credit assessment and to give up other personal information. While the users are doing it, the crooks use malware to crash their computers and leave the information vulnerable.

**Source: Help Net Security, April 05, 2010**

[http://www.net-](http://www.net-security.org/secworld.php?id=9099&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

[security.org/secworld.php?id=9099&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9099&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

### **2. UNDER PROTECTED CORPORATE SECRETS**

Enterprises are investing heavily in compliance and protection against accidental leaks of custodial data (such as customer information), but under-investing in protection against theft of far more valuable corporate secrets, according to a global survey by Forrester Consulting. Nearly 90% of surveyed enterprises agreed that compliance with PCI-DSS, data privacy laws, data breach regulations, and existing data security policies is the primary driver of their data security programs. Significant percentages of enterprise budgets (39%) are devoted to compliance-related data security programs. But secrets comprise 62% of the overall information portfolio's total value while compliance-related custodial data comprises just 38%, a much smaller proportion. This strongly suggests that investments are over weighed toward compliance.

**Source: Help Net Security, April 06, 2010**

[http://www.net-](http://www.net-security.org/secworld.php?id=9104&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

[security.org/secworld.php?id=9104&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9104&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

### **3. 70 ROMANIAN CYBER CROOKS ARRESTED**

70 people belonging to 3 unconnected cybercrime gangs were arrested yesterday during raids performed by the Romanian police. The gangs m.o. was apparently as follows: they phished eBay account credentials and used those accounts to sell fake or non-existent goods such as laptops, Rolex watches, luxury cars, yachts, and - can you believe it? - aeroplanes. Romanian DIICOT (Directorate for Investigating Organised Crime and Terrorism) has worked together with the FBI to identify over 800 victims of the gangs and to track down the criminals. The arrests were executed with the help of

the FBI and members of the US Secret Service that are stationed at the US Embassy in Bucharest, the Romanian capital.

**Source: Help Net Security, April 07, 2010**

<http://www.net->

[security.org/secworld.php?id=9114&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9114&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

#### **4. BANK EMPLOYEE ACCUSED OF STEALING FROM "INFECTED" ATMS**

An employee of the Bank of America that was in charge of designing and maintaining the bank's computer system and its ATMs, was charged of committing computer fraud. The accused - Rodney Reed Caverly, of North Carolina - allegedly designed a piece of malicious software and infected the system with it so that he could withdraw money from the ATMs without them recording that the transaction occurred.

**Source: Help Net Security, April 09, 2010**

<http://www.net-security.org/secworld.php?id=9119>

#### **5. PLENTY OF CREDIT CARD FRAUD AND IDENTITY THEFT**

A survey of 1000 commuters in London has found that a tidal wave of credit card fraud and identity theft is sweeping the UK as 44 % of people said they have suffered from bank/credit card fraud and 42% have had their identity stolen. According to researchers from Infosecurity Europe, the average amount stolen was £1448 per person, and 37% overall did not get their money back from the bank. People that lost a small amount of money were far less likely to get their money back from their bank than people who lost a large amount of money with 91% of people who lost more than £5000 getting their money back compared to only 41% of people who lost less than £100. The type of organization that most people blame for making them vulnerable to fraud were retailers at 60%, whilst only 12% blamed the banks, and 28% said it was their own fault that they had lost money or had their identity stolen. The researchers also asked if a partner or family member had suffered from bank/credit card fraud and 45% said that they had, whilst 41% said that their family had their Identity stolen.

**Source: Help Net Security, April 26, 2010**

<http://www.net-security.org/secworld.php?id=9191>

#### **6. SCAMMERS' LINK ARCHITECTURES**

As much as it hurts us to admit, online scamming shares many of the characteristics of a legal business. Why? Because, in the end, they have the same goal - revenue. To achieve that goal, businesses are forced to evolve and develop: their strategies, their plans, their modus operandi. Over time, online scammers have developed a series of "link architectures" that are aimed at increasing their pages' Google ranking and, consequently, bringing more traffic their way.

**Source: Help Net Security, April 27, 2010**

<http://www.net-security.org/secworld.php?id=9203>

## **MALWARE**

### **7. 1,800 OFFICE BUGS DISCOVERED BY MICROSOFT'S "FUZZING BOTNET"**

Mariposa botnet has been shut down and three suspected criminals accused of operating it have been arrested by Spanish law enforcement. Mariposa stole account information for social media sites and other online email services, usernames and passwords, banking credentials, and credit card data through infiltrating an estimated 12.7 million compromised personal, corporate, government and university IP addresses in more than 190 countries. The botnet was shutdown and rendered inactive on December 23rd, 2009 thanks to the collaborative effort of different security experts and law enforcement, including Panda Security, Defence Intelligence, the FBI and Spanish Guardia Civil.

**Source: Help Net Security, April 01, 2010**

<http://www.net->

[security.org/secworld.php?id=9092&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9092&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

### **8. TROJANS ARE THE MOST CONSTANT INFECTIOUS VECTOR**

The generic mechanism that spreads using removable devices - Trojan.AutorunInf.Gen – is the top e-threat for March with 13.40 percent of the total amount of global malware. This is a position very frequently occupied by this particular piece of malware. With a percentage of 6.19, also known as the infamous Kido or Conficker, Win32.Worm.Downadup.Gen, ranks second, as it has been for the past three months. "This worm exploits a well-known Windows vulnerability. In order to get rid of this people simply have to update both the operating system and their locally-installed antimalware solution," said Catalin Cosoi, BitDefender's senior researcher. The third e-threat for March is Exploit.PDF-JS.Gen with 5.30 percent. Adobe PDF Reader's Javascript engine is being manipulated by this threat with the sole purpose of executing malicious code on the users' computer.

**Source: Help Net Security, April 02, 2010**

[http://www.net-security.org/malware\\_news.php?id=1284&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/malware_news.php?id=1284&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

### **9. BOTNETS DRIVE THE RISE OF RANSOMWARE**

Ransomware is the dominating threat with nine of the detections in the malware top ten lists resulting in either scareware or ransomware infesting the victim's PC. Fortinet observed the primary drivers behind these threats to be two of the most notorious botnet "loaders" - Bredolab and Pushdo. Another important finding is the aggressive entrance of a new zero-day threat in FortiGuard's top ten attack list, MS.IE.Userdata.Behavior.Code.Execution, which accounted for 25 percent of the detected activity last month.

**Source: Help Net Security, April 02, 2010**

[http://www.net-security.org/secworld.php?id=9095&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9095&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **10. GLOBAL RESPONSE TO CONFICKER THREAT: MODEL FOR FUTURE CYBER THREAT RESPONSE?**

The problem with Conficker is that we still don't know what it's for. Yes, an estimated 7 million computers are infected worldwide, but they don't show signs of any expected type of malicious activity. Basically, we are all waiting for something to happen so that we are able to react or, at least, be able to say "A-ha! So that's the grand plan!" In the meantime, there is one positive aspect of this whole situation. To respond to and mitigate the threat, the Conficker Working Group was created and proved to everybody that security researchers and Internet infrastructure providers around the world and working for many different companies can work together towards a common goal.

**Source: Help Net Security, April 02, 2010**

[http://www.net-security.org/malware\\_news.php?id=1286&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/malware_news.php?id=1286&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **11. CLOSING THE LAST DOOR**

There's always a risk of viruses lurking behind links on a website. Even well-known sites can contain dangerous links, especially those with a high level of public interaction – forums, message boards, social networks and so on. Small and midsized businesses (SMBs) usually protect their data assets and staff with firewalls that include an integrated Web proxy and antivirus solution, known as Unified Threat Management (UTM) appliances. These are reliable at blocking viruses transmitted via ordinary HTTP. However, if the link URL starts with https:// instead of http:// the virus can be transferred via an encrypted connection, so it gets round the firewall and Web proxy without being detected. HTTPS proxies are the only way to ensure these viruses are blocked at the gateway.

**Source: Help Net Security, April 06, 2010**

[http://www.net-security.org/article.php?id=1420&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/article.php?id=1420&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **12. GENERIC AND BEHAVIOR-BASED THREATS INCREASING**

Sunbelt Software announced the top 10 most prevalent malware threats for the month of March 2010. The list shows the continued prevalence of Trojan horse programs circulating on the Internet and the growing trend of generic and behavior-based detections in antivirus detections. Generic and behavior-based detections by the antivirus industry have improved thanks to the massive increase in new malcode, which number thousands per day. The top two detections for the month remained in the same positions as last month. Both Trojan.Win32.Generic!BT (31.07 percent) and Trojan-

Spy.Win32.Zbot.gen (4.97 percent) maintained approximately the same pervasiveness in the overall malware tracked.

**Source: Help Net Security, April 06, 2010**

[http://www.net-](http://www.net-security.org/malware_news.php?id=1288&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

[security.org/malware\\_news.php?id=1288&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/malware_news.php?id=1288&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

### **13. FIRESHARK: LINKING THE MALICIOUS WEB**

Freshark is a tool, made up of a Firefox plugin and a set of post processing scripts that allows you to capture web traffic from the core of your web browser, enabling you to log events and download content to disk for post-process analysis.

**Source: Help Net Security, April 15, 2010**

<http://www.net-security.org/secworld.php?id=9144>

## **HACK THREAT/INTRUSION**

### **14. MANY TEENAGERS HACK AND RARELY GET CAUGHT**

A survey revealed the hacking habits of 1000 New York City teenagers. Exactly half (50%) of kids sampled revealed they'd had their Facebook or email account hacked, which may explain why 75% feel hacking is wrong and 70% think it should be considered a criminal offense. However, 39% of the teens surveyed think hacking is "cool" and 16%, or roughly one in six, admitted to trying their hand at it. Only 15% of the entire sample has either been caught or knows someone who has - particularly disturbing considering 7% of young hackers reported they did so for money and 6% view it as a viable career path. A potentially surprising finding is that it's not just the boys - of the sample, 29% of those who admitted to hacking were girls. The most common reason cited for hacking was for fun (54%) followed by curiosity (30%). 14% that hack aimed to cause disruption and a resourceful 7% of US kids thought they could generate an income from the activity, with 6% viewing it as a viable career path! 34% had already hacked by age 13 and 52% hacked between the ages of 14-16.

**Source: Help Net Security, April 14, 2010**

<http://www.net-security.org/secworld.php?id=9139>

### **15. 9-YEAR-OLD BLAMED FOR HACKING SCHOOL SYSTEM**

Searching for the hacker who broke into the computer system of Spring Hill Elementary in Virginia, the police was more than little surprised when the investigation revealed that the culprit is a precocious 9 year-old student of the school. According to Computerworld, the first sign that something was amiss was the teachers' and staff members' inability to access their accounts because their passwords had been changed. This was followed by the discovery that some courses' content and enrollment information was changed or deleted. The investigation also discovered that the student didn't actually hack the Blackboard system used by the school. "It was actually not a hack, unless you consider

the fact that the 9-year-old took the teacher's username and password from the desk a hack," says a Blackboard vice president.

**Source: Help Net Security, April 19, 2010**

<http://www.net-security.org/secworld.php?id=9154>

## **16. NETWORK SOLUTIONS CUSTOMERS TARGETED BY NEW HACK ATTACK**

Only a week after a number of blogs hosted on Network Solutions have been compromised thanks to a WordPress hack, the company has been thrust back into the spotlight by a massive hacking attack that may or may not be coming from a single source. According to StopMalvertising, a huge number of sites were hacked with a malware script that injects an iframe into the site that points to *corpadsinc.com*, where Adobe PDF exploits are delivered to victims. Also, this time the customers using WordPress are not the only victims - sites using Joomla and just plain-old HTML are also targeted.

**Source: Help Net Security, April 19, 2010**

<http://www.net-security.org/secworld.php?id=9158>

## **17. RUSSIAN HACKER OFFERS 1.5M FACEBOOK CREDENTIALS FOR SALE**

What will Facebook do if the Russian hacker Kirillos' claim that he has in his possession login credentials for 1.5 million Facebook accounts proves to be true? The hacker was spotted offering the credentials for sale on an underground forum. Kirillos asks from \$25 to \$45 per 1,000 accounts (that's \$0.025/\$0.045 per account), and according to VeriSign's Director of Cyber Intelligence Rick Howard, he has already been able to sell almost half of the total number.

**Source: Help Net Security, April 23, 2010**

<http://www.net-security.org/secworld.php?id=9186>

## **SPAM**

## **18. GAMES ON SOCIAL NETWORKS INCREASE SPAM AND PHISHING BY 50%**

In order to reach high scores, social entertainment applications require users to gather a considerable number of friends and supporters to play the same game, leading to player-development of social gaming channels, groups and fan pages to facilitate player interaction. Spammers and phishers exploit the increasing trend of social gaming with fake profiles and bots that send spam messages to groups, as a BitDefender case study shows. Unlike the regular social networking spam, when the users are enticed to add the spammer in their circle of friends, the social gaming-related phony profiles are willingly added by the users as an immediate consequence of their interest in enlarging the supportive players' community. This makes it almost impossible for the bogus accounts to be automatically suspended, since the spammers' action does not constitute an abuse.

**Source: Help Net Security, April 01, 2010**

[http://www.net-security.org/malware\\_news.php?id=1283&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/malware_news.php?id=1283&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **19. FACEBOOK WILL NOT START CHARGING USERS**

"News" of Facebook's plan to charge for the use of its network is once again surfacing and being propagated by users and Facebook groups set up (as it seems) for the purpose of collecting a "fan" base will probably be spammed every once in a while. I noticed today that some of my Facebook "friends" have joined a group that professes to be something like a public petition against paying for Facebook use. I am aware that occasionally such groups spring up - this has been going on for a while now - but I'm always surprised when people who have been using the social network for a long time turn out to have bad memory when it comes to stuff like this.

**Source: Help Net Security, April 07, 2010**

[http://www.net-security.org/secworld.php?id=9110&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9110&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **20. SPAMMERS USE THE FAMILIAR TO INSPIRE ACTION**

Spammers have become adept at using the most familiar Internet names to give deceptive legitimacy to the billions of emails that they send. For example, between five to ten percent of all spam appears to originate from Gmail accounts, according to a Commtouch report. Gmail's message style, as well as those of PayPal and Facebook, is frequently used by spammers and phishers as standard templates to prompt action by targets of spam or phishing. This quarter, a phishing attack directed at Blogger and Google users was based on a template using techniques effectively downplaying the "phishy" nature of the email.

**Source: Help Net Security, April 15, 2010**

<http://www.net-security.org/secworld.php?id=9143>

## **21. ESCALATION OF PHARMA SPAM FROM GMAIL ACCOUNT**

A recent noticeable upsurge of spam messages coming from compromised Gmail accounts has led the unfortunate victims to speculate that there is a bug in the Gmail mobile interface. The base for this hypothesis can be found in the fact that the great majority of the victims noticed - by checking out the details of account activity that can be accessed by clicking on a "Details" link at the bottom of the Gmail page - that the hackers accessed the accounts through a mobile interface.

**Source: Help Net Security, April 21, 2010**

<http://www.net-security.org/secworld.php?id=9174>

## **22. THE US CONTINUES ITS REIGN AS THE KING OF SPAM**

The United States continues its reign as the king of spam, relaying more than 13% of global spam, accounting for hundreds of millions of junk messages every day, according to a report by Sophos. However, most dramatically, China – often blamed for cybercrime by other countries – has disappeared from the “dirty dozen,” coming in at 15th place with responsibility for relaying just 1.9% of the world’s spam.

**Source: Help Net Security, April 28, 2010**

<http://www.net-security.org/secworld.php?id=9210>

## **PHISHING ATTACK**

## **23. HOW TO DETECT A PHISHING WEBSITE, THE GOOGLE WAY**

Google analyzes millions of pages per day when searching for phishing behavior. This kind of activity is, of course, not done by people but by computers. The computers are programmed to look for certain things that will identify the page as a phishing site. Those things are actually the same things that users should check when evaluating if a page is legitimate or not. According to a post on Google's official online security blog, the first step is looking at the URL- Does it contain words like "login" or "banking" or trademarks of the phishing target? Does it use an IP address for its hostname? Does it have a large number of host components, making the address unusually long? If the answer is yes to all of these questions, the page could be a phishing one.

**Source: Help Net Security, April 02, 2010**

<http://www.net->

[security.org/secworld.php?id=9096&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9096&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **24. IS PHONE PHISHING MAKING A COMEBACK?**

By now, pretty much everyone knows that when one receives an email purportedly coming from a bank or a financial institution, extreme caution and distrust is in order. We have been warned time and again that banks would never send an email demanding you to send them back your personal or account information, let alone your PIN number. The repeated warnings have obviously brought results, and scammers have started reverting to good old phone phishing. The phishers call the victim up and deliver the usual spiel of how the victim's account/credit card might have been compromised and would they mind confirming their account number, PIN or password to make sure that it hasn't? According to [ConsumerAffairs.com](http://www.ConsumerAffairs.com), the Pennsylvania Attorney General Tom Corbett is warning the state residents that the number of phishing calls of this kind has increased recently, and that the scammers are using live operators and automated calls to create an aura of legitimacy.

**Source: Help Net Security, April 07, 2010**

<http://www.net->

[security.org/secworld.php?id=9115&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9115&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **25. PHISHING STUDENT LOANS' PAGES TARGET STUDENTS**

University students in the UK that have taken out a loan with the Student Loans Company have lately been targeted by a phishing scam that presents to them a page that is supposedly a login page for "Student Finance". According to Sunbelt, users are asked to enter their Customer Reference Number and then to enter a large amount of personal information: name, date of birth, National insurance number, address, email address, password, bank sort code, bank account number, and more.

**Source: Help Net Security, April 20, 2010**

<http://www.net-security.org/secworld.php?id=9160>

## **26. FAKE FAST FOOD SURVEY WITH CASH REWARD LEADS TO PHISHING SITE**

Scammers often use the familiarity of a brand as a means of lessening the victims' tendency to be cautious when perusing unsolicited emails. In this latest email scam, this method is coupled with the offer of \$80 to whoever takes a short survey. The email supposedly comes from a globally well-known fast food chain, and claims that the company is planning major changes to the establishments in order to improve the quality of service. In order to do so, they are asking the customers to fill out a survey and they offer the cash as incentive. Symantec reports that to access the survey, the victims are encouraged to follow the link in the email, which will then take them to a bogus page ostensibly belonging to the company.

**Source: Help Net Security, April 23, 2010**

<http://www.net-security.org/secworld.php?id=9182>

## **OTHERS**

## **27. STALKER JAILED FOR PLANTING CHILD PORN ON A COMPUTER**

An elaborate scheme to get the husband of a co-worker he was obsessed with locked up in jail, backfired on Ilkka Karttunen, a 48-year from Essex. His plan was to get the husband arrested so that he could have a go at a relationship with the woman, and to do this he broke into the couple's home while they were sleeping, used their family computer to download child pornography and then removed the hard drive and mailed it anonymously to the police, along with a note that identified the owner. The whole family received a shock when the police came and arrested the husband on suspicion of possession of indecent images of children. He was banned from seeing his own children and from returning to his home while he was under investigation.

**Source: Help Net Security, April 01, 2010**

<http://www.net->

[security.org/secworld.php?id=9090&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9090&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **28. HEALTHCARE INDUSTRY OVERLOOKS CRITICAL GAP IN DATA SECURITY**

As the healthcare industry prepares for a major shift to electronic health records (EHRs) over the next several years, a new bi-annual report provides data that shows that providers are still having difficulty adequately securing patient data in a rapidly changing landscape. The 2010 HIMSS Analytics Report: Security of Patient Data indicates that healthcare organizations are actively taking steps to ensure that patient data is secure. However, these efforts appear to be more reactive than proactive, as hospitals dedicate more resources toward breach response vs. breach prevention through risk management activities.

**Source: Help Net Security, April 06, 2010**

[http://www.net-security.org/secworld.php?id=9102&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9102&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **29. U.S. INFRASTRUCTURE AT RISK FROM SOPHISTICATED CYBER ATTACKS**

Nearly three-quarters of federal IT decision-makers who work in national defense and security departments or agencies say the possibility is “high” for a cyber attack by a foreign nation in the next year, according to a Clarus Research Group survey. Additionally, a third of these respondents say they have already experienced such a cyber attack within the last year. The survey of 201 federal IT decision-makers and influencers also identifies the growing volume and sophistication of cyber attacks as the top IT security risks facing federal IT in the coming year. Yet, more than half of those surveyed expect only minor policy changes as a result of the recently created federal cyber security coordinator position. Of federal IT personnel surveyed, 41 percent said they spent less than 10 percent of their time over the past year working on the Comprehensive National Cyber Security Initiative - and a solid majority, 62 percent, said they spent less than 25 percent of their time on it.

**Source: Help Net Security, April 07, 2010**

[http://www.net-security.org/secworld.php?id=9108&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9108&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

## **30. DATA BREACHES COST AUSTRALIAN COMPANIES MILLIONS**

Australian organizations experience costly data breaches with the average organizational cost of a data breach, including activities intended to prevent a loss of customer or consumer trust, at AUS\$1.97 million and the average cost per compromised record at AUS\$123. The most expensive data breach cost one organization surveyed more than AUS\$4 million to resolve, according to a data breach report by the Ponemon Institute, the first of its kind to quantify the costs associated with both public and private sector data breaches in Australia. The research analyzed the actual data breach experiences of 16 Australian companies from nine different industry sectors taking into account a wide range of business costs including expensive outlays for detection, escalation, notification and after-the-fact responses. It also analyzed the

economic impact of lost or diminished customer trust and confidence as measured by customer turnover (churn) rates.

**Source: Help Net Security, April 08, 2010**

<http://www.net->

[security.org/secworld.php?id=9117&utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29](http://www.net-security.org/secworld.php?id=9117&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29)

### **31. PREVENT UNAUTHORIZED ELECTRONIC FUND TRANSFER**

Authentify released the ETF Verifier application which enables financial applications and payment platforms to alert legitimate account owners via phone whenever a new payee or funds transfer destination account is added to the user's financial account. This verification process permits the account owners to authorize a transaction or, more importantly, cancel a transaction if they are not behind the activity themselves. Adding new destination accounts has been the point of attack for the organized criminals behind Zeus and its variants for getting cash from compromised accounts.

**Source: Help Net Security, April 09, 2010**

<http://www.net-security.org/secworld.php?id=9120>

### **32. ENDPOINT DATA LEAK PREVENTION STILL A MAJOR HEADACHE**

More than one in three (38%) of respondents are still failing to deploy any form of data leak prevention, whether that be device control, endpoint DLP or DLP appliances. Amongst small to medium sized business this figure increases to over half of organizations (54%), according to a survey by DeviceLock. The survey also revealed that even those managers that are deploying technology solutions to prevent data leakage from within their organizations the majority are failing to protect all the possible channels where data leakage can occur.

**Source: Help Net Security, April 12, 2010**

<http://www.net-security.org/secworld.php?id=9125>

### **33. FUTURE AIR TRAVEL SECURITY RISKS, PRIVACY AND SOCIAL IMPLICATIONS**

The European Network and Information Security Agency (ENISA) has analyzed the risks associated with a future air travel scenario, enabled with "Internet of things", IoT / RFID technology. The report identifies major security risks, as well as privacy, social and legal implications and also makes concrete policy and research and legal, recommendations. IoT is a vision where all manufactured things are connected to each other via wireless or wired communication networks. The movement of travelers, airport staff, and luggage creates an increasing, continuous interaction between smart devices. It also implies sharing of significant amounts of sensitive information. Every day 28.000 flights occur in Europe, (i.e. 10 Mn/year), so the importance of air travel is easily understandable.

**Source: Help Net Security, April 13, 2010**

<http://www.net-security.org/secworld.php?id=9126>

### **34. MEDICAL RECORDS SECURED BY CODE-CHANGING ALGORITHM**

Medical records databases are a treasure trove for researchers - mapping trends in diseases and studying them to discover better treatment methods has never been easier. Information that was previously available to a restricted number of researchers is now digital and accessible to many, making the issue of patient privacy prominent in discussions regarding the handling of these records. Electronic medical records consist of very detailed patient data, where every disease, symptom or injury has its own code, which makes analysis easier and faster. But, the problem is that these codes are available through public databases and electronic medical records, and with this knowledge, this anonymized data can be still tied to the persons to whom it belongs. To prove that this is a realistic problem, a research team from the Vanderbilt University in Nashville has conducted an experiment which resulted in 96 percent of the 2,762 patients belonging to the test group identified through diagnosis codes.

**Source: Help Net Security, April 13, 2010**

<http://www.net-security.org/secworld.php?id=9128>

### **35. FACEBOOK BUILDS UP ITS DEFENSES**

The redesign of its Safety Center is just one of the steps Facebook is lately taking to tackle the security issues that have been steadily rising along with the number of users. As Max Kelly, Facebook's Director of Security, explained during his keynote presentation at the Black Hat security conference in Barcelona on Tuesday, circa 10% of the 1,200 company's employees are engaged in security-related tasks. 20 people form the core security team, 15 constitute the site integrity team, and around 200 people altogether monitor illegal activity on the social network. Facebook has also put in place an automated detection system that identifies aberrant user behavior and initiates defensive maneuvers such as forcing the user to pass through CAPTCHAs to prove it is human and not a bot, limiting the number of messages that can be sent from the account and, finally, disabling accounts if the situation demands it.

**Source: Help Net Security, April 15, 2010**

<http://www.net-security.org/secworld.php?id=9147>

### **36. USER ACCESS CONTINUES TO BE POORLY MANAGED**

Findings gathered from a Ponemon Institute and Aveksa survey of 728 experienced IT practitioners at multinational corporations and government organizations show that ineffective access governance processes expose enterprises to serious noncompliance and business risks. The 2010 Access Governance Trends Survey tracks the perspectives of IT security and compliance practitioners on access governance, measuring how well organizations control user access and prevent misuse that could negatively impact their business. Survey results indicate that many organizations face significant information security risks because of a lack of resources, budget and IT staff - heightened by ad hoc or inconsistent approaches to access management activities across the enterprise. According to 2010 results, cloud computing has emerged as a key factor affecting organizations' access governance processes, with respondents

reporting that its adoption enables business and end users to circumvent existing access governance processes.

**Source: Help Net Security, April 19, 2010**

<http://www.net-security.org/secworld.php?id=9156>

### **37. DATA INTEGRITY ATTACKS A GROWING THREAT**

A survey by Infosecurity Europe of 420 organizations has found that a quarter (28%) have been subject to a data integrity attacks. Of those that think that data integrity attacks could be a problem 14% are not sure they would be able to detect an attack and half of organizations think that attacks could be a problem but have not detected any. Worryingly only 3% thought that data integrity attacks are not a problem with 6% acknowledging that data integrity attacks are a problem and that they were adequately protected.

**Source: Help Net Security, April 20, 2010**

<http://www.net-security.org/secworld.php?id=9159>

### **38. CLOUD COMPUTING AND SOCIAL NETWORKING EXPOSE BUSINESSES TO ATTACKS**

Business use of technology is evolving faster now than at any point in the last decade. Internet use has moved way beyond email and websites and into the realms of social networks and cloud computing. These changes have increased the vulnerability of UK companies and public sector organizations to new cyber attacks. Hacking and DoS attacks have doubled in the last two years. As a result, security remains high on management's list of priorities. These are among the findings a survey by PricewaterhouseCoopers.

**Source: Help Net Security, April 21, 2010**

<http://www.net-security.org/secworld.php?id=9172>

### **39. SPLUNK.COM PASSWORD LEAK**

Splunk announced on their blog that they discovered the logging of users' passwords in clear text. The culprit is debug code that found its way onto the www.splunk.com production web servers. The problem was quickly identified and action was taken to prevent any future logins being recorded in the open. Splunk says that they have no reason to believe any information was exposed in the wild, the only ones with possible access to the data were a few Splunk employees with access to internal deployments.

**Source: Help Net Security, April 26, 2010**

<http://www.net-security.org/secworld.php?id=9189>

### **40. THE STAGGERING COST OF DATA BREACH**

The average cost of a data breach globally stood at USD 3.43 million last year, the equivalent of USD 142 per compromised customer record, according to research from

the Ponemon Institute. Costs varied dramatically between regions, from USD 204 per lost record in the U.S., down to USD 98 per record in the UK. A total of 133 organizations, located in five countries – Australia, France, Germany, UK and U.S. – participated in the research, which was undertaken during 2009. The report shows that costs incurred in countries with data breach notification laws were significantly higher than in countries where no such legislation exists. For example, in the U.S., where 46 states have now introduced laws forcing organizations to publicly disclose the details of breach incidents, the cost per lost record was 43 percent higher than the global average.

**Source: Help Net Security, April 29, 2010**  
<http://www.net-security.org/secworld.php?id=9215>

#### **41. MAJORITY UNWARE OF HOW SENSITIVE DATA IS STORED ONLINE**

The majority of U.S. citizens are unaware of how their online data is stored and who secures it, according to a Business Software Alliance (BSA) survey. Approximately one in five U.S. citizens said they were unaware of whether their personal or corporate data is being held “in the cloud,” and 60 percent said they did not know what “in the cloud” means. In addition, BSA’s findings show U.S. citizens are unsure who should be responsible for protecting sensitive, online data. “As more information is stored in the cloud, coordination between the public and private sectors is more important than ever to protect personal and corporate data,” said Robert Holleyman, President & CEO of BSA. “What this survey tells us is that there is a lag in the general public’s understanding of the emerging cloud environment and how it impacts their data – and a lack of consensus on who is responsible for securing the cloud.”

**Source: Help Net Security, April 30, 2010**  
<http://www.net-security.org/secworld.php?id=9223>