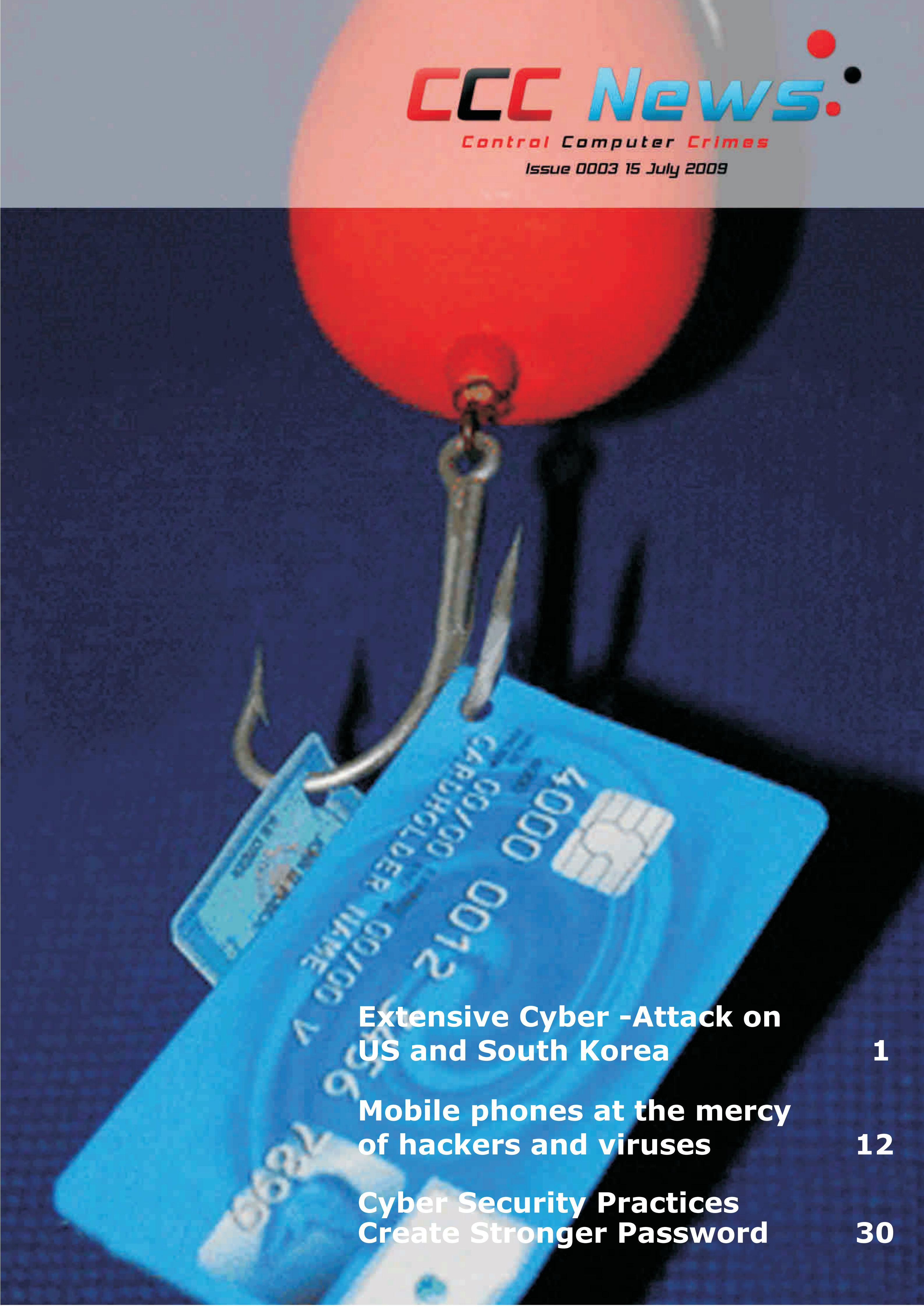
CCC News

Control Computer Crimes

Issue 0003 15 July 2009



Extensive Cyber -Attack on US and South Korea 1

Mobile phones at the mercy of hackers and viruses 12

Cyber Security Practices Create Stronger Password 30

Message from Editor

Welcome to the third issue of CCCNews Magazine.

Like the first issue, over 100,000 downloads have been recorded for the second issue of the CCCNews Magazine, from our website www.cccnews.in. This encourages the whole team of CCCNews, which worked overtime to collate the publication material to make it more and more user friendly.

I again thank all the subscribers and constituents for showing better response to the second issue. I further request the readers to circulate the publication weblink to their friend and colleagues, so that more and more people can take advantage of the CCCNews magazine.

Here is the third issue of the CCCNews Magazine.

This fortnight has again been very cyber attack active. There are reports that 13 major Korean and 26 major US websites have been DDOS attacked. The identities of the attackers could not be established. There are various speculations. Though there has been no conclusive evidence yet, but various reports speculate attackers like North Korea, ethical disturbed China and Russians.

This compels us to think that the attackers are becoming so sophisticated that they could successfully hide the clues leading to their identity. Further, these sites are high security sites including (and not limited to) Korean Government, Parliament, Banks; US government including White House, newspapers like Washington Post, NYSE, NASDAQ. These are all highly secure organisations. If these matured organisations can be attacked, what can be the fate of less secure organisation, data centers and websites.

Further, the tools of attack are available easily. The technology is also available easily. The skill set requirement is not high. This makes the situation more and more scary, as the world is moving very fast towards digital business processes, security is becoming the biggest concern. Thus, in the name of patriotism or challenge or rebellion or revenge, cyber attacks become highly potent and at the same time the cheapest and safest weapon, in the hands of any interested group.

The need of the hour is to develop and offer a path-breaking technology at commercially affordable rates to counter these attacks. This need mobilisation of large number of researchers and lateral thinkers. Marketing savvy commercial interests, closed technologies and patent restrictions hamper wider participation but somehow this cycle need to be broken. The current cycle of half-baked, untested and constantly patched technologies must be channelised into robust, secure and cheaper technologies.

Rakesh Goyal
Editor

CCC News

Issue 0003
15th July 2009

Rakesh Goyal
Editor
editor@cccnews.in

Moiz Mamoowala
Marketing & Sales
moiz@cccnews.in
+919769887077
+919967247000

Published by
CCC Media
Mumbai, India

Contents

News

Extensive Cyber - Attack on US and South Korea 1

List of Korean and US sites attacked 2

U.S. and Europe Join hands to form Cyber-Crime Force 3

China postpones mandatory installation of controversial filtering software 4

Internet Attack Barometer 6

INTERPOL and FIRST to Fight Cyber Crime together 7

E-mail Scammers Focus on Webmail Accounts 9

France creates new national IT security agency 10

2 Jailed for hacking into phone system 11

Mobile phones at the mercy of hackers and viruses 12

Programmer arrested for stealing source code 14

The Hidden Cost of Using Microsoft Software 15

Analysis

US Social Security numbers are predictable 16

Sharing information is the best way to beat cyber crimes 18

Weak security opens door to hackers 20

Cyberspace Shapes Up To Be Next Battleground 23

Contents

Survey

Women More Online Security Conscious than Men 26

Fired employees would take with them password list,
R&D plans and customer database 27

Skype banned by IT departments 29

Around 10 per cent of phishing attacks target India 29

Education

Cyber Security Practices
Create Stronger Password 30

Stealing Data using electrical outlets and cheap lasers 32

Quiz 0003 34

Quiz 0002 Answers 34

Extensive Cyber-Attack on US and South Korea

Massive DDOS attack has been reported on many US governemnt and South Korea government and Banking web-sites.

Researchers are working to break down the malicious code tied to a DDOS attack targeting government and commercial sites in the US and South Korea

More details are surfacing about a massive denial-of-service (DDOS) attack that has hit both government and commercial websites in the US and South Korea in the past few days.

According to security researchers, the attacks are the work of malware that infected users and routed traffic to government and commercial sites starting during the US 4 July holiday weekend.

Just what that Trojan is exactly is the subject of some disagreement, with some researchers contending the malware is an updated version of the infamous MyDoom worm that plagued Windows users in 2004. However, connections between MyDoom and the malware involved in the attack may be overplayed, according to Joe Stewart, director of malware research for SecureWorks' Counter Threat Unit.

"It's definitely not an updated version of MyDoom," he said in an interview. "I'm not really seeing all that many similarities...most of the code seems to be unique."

Stewart could not say how the malware is being spread. But what is clear is the attack is even broader than initially reported. On 5 July, the list of sites to be attacked included only five US government sites. By the following day, however, that featured 21 sites, including some in the private sector. On the 7 July, the list was updated again and had 26 sites, including some in South Korea.

Among the sites hit by the attack were the US Department of Treasury, the White House, the Federal Trade Commission and the Washington Post. Some of the organisations are reported to have fended off the attacks.

Source: Brain Prince, www.eweekeurope.co.uk , 09 July 2009

List of Korean and US sites attacked

List of Korean sites

- banking.nonghyup.com - Banking.nonghyup.com (bank, internet banking)
- blog.naver.com - Blog.naver.com (Naver blog)
- ebank.keb.co.kr - Ebank.keb.co.kr (Korea Exchange Bank Internet Banking)
- ezbank.shinhan.com - Ezbank.shinhan.com (Shinhan Bank, Internet Banking)
- mail.naver.com - Mail.naver.com (Naver Mail)
- www.assembly.go.kr - www.assembly.go.kr (Republic of Korea National Assembly)
- www.auction.co.kr - www.auction.co.kr (auction)
- www.chosun.com - www.chosun.com (Chosun Ilbo)
- www.hannara.or.kr - www.hannara.or.kr (GNP)
- www.mnd.go.kr - www.mnd.go.kr (Defense)
- www.mofat.go.kr - www.mofat.go.kr (Foreign Minister)
- www.president.go.kr - www.president.go.kr (Blue House)

List of US sites

- www.usfk.mil - www.usfk.mil (USFK)
- finance.yahoo.com - Finance.yahoo.com
- travel.state.gov - Travel.state.gov
- www.amazon.com - www.amazon.com
- www.dhs.gov - www.dhs.gov
- www.dot.gov - www.dot.gov
- www.faa.gov - www.faa.gov
- www.ftc.gov - www.ftc.gov
- www.nasdaq.com - www.nasdaq.com
- www.nsa.gov - www.nsa.gov
- www.nyse.com - www.nyse.com
- www.state.gov - www.state.gov
- www.usbank.com - www.usbank.com
- www.usps.gov - www.usps.gov
- www.ustreas.gov - www.ustreas.gov
- www.voa.gov - www.voa.gov
- www.voanews.com - www.voanews.com
- www.whitehouse.gov - www.whitehouse.gov
- www.yahoo.com - www.yahoo.com
- www.washingtonpost.com - www.washingtonpost.com
- www.usauctionslive.com - www.usauctionslive.com
- www.defenselink.mil - www.defenselink.mil
- www.marketwatch.com - www.marketwatch.com
- www.site-by-site.com - www.site-by-site.com

U.S. and Europe Join hands to form Cyber-Crime Force

ROME -- The U.S. Secret Service plans to unveil Tuesday plans for a pan-European task force charged with preventing identity theft, computer hacking and other computer-based crime.

The unit will be based in Rome, teaming up with an Italian anti-cyber-crime police unit and the Italian post office Poste Italiane SpA, which has developed software that can track electronic payments as it moves beyond traditional mail delivery.

The European Electronic Crime Task Force's main job will group together the cyber-crime efforts of the European Union nations and the U.S., bolstering defenses against computer attacks on embassies and other government sites that host sensitive computer systems such as air-traffic control. It will also monitor computer networks for threats, as well as deal with attacks once they happen.

"The transnational nature of cyber attacks requires international collaboration and expertise, as exemplified by this joint professional partnership," said Robert Gombar, a special agent in charge of the Secret Service's Rome field office, which coordinates its activities in southern Europe and the Mediterranean.

Under the terms of the agreement, the new task force will monitor computer networks across Europe using software designed by Poste Italiane. The software could comb through money transfers performed over the Internet for suspicious signs, such as an account being opened by the same person in several different places, according to Poste Italiane Chief Executive Massimo Sarmi.

In recent years many Italians, as well as newly arrived immigrants, have begun to use Poste Italiane's 14,000-branch postal system as a bank to deposit their paychecks and pay their bills. Poste Italiane users can also make payments online. Poste Italiane now makes more money from banking and insurance services than it does from sending letters and packages. Of the €50 billion ($70 billion) that crosses Poste Italiane's electronic network each month, total theft amounts to "a few hundred thousand euros" per month, said Mr. Sarmi.

Source: Jennifer Clark, www.nationalcybersecurity.com, 30 June 2009.

China postpones mandatory installation of controversial filtering software

BEIJING: China will delay the mandatory installation of the controversial "Green Dam-Youth Escort" filtering software on new computers, the Ministry of Industry and Information Technology (MIIT) said here Tuesday.

The pre-installation was postponed as some computer producers said such massive installation demanded extra time, said the ministry.

"The ministry would keep on soliciting opinions to perfect the pre-installation plan," a spokesman with MIIT said.

All computers produced or sold in China were scheduled to be installed with such software after July 1, according to MIIT's previous announcement.

The ministry would continue to provide a free download of the software and equip school and Internet bar computers with it after July 1, said the spokesman.

The software is designed to block violence and pornographic contents on the Internet to protect minors. It could also help parents control how much time their children spend online.

However, the ministry did not mention when the pre-installation requirement would resume its effect.

SAFE, LEGAL AND TRUSTWORTHY

Although the pre-installation plan had aroused much controversy, MIIT defended its plan as a safe, legal and trustworthy one.

The pre-installation would not be compulsory, as the software could be easily switched off and uninstalled by computer users, the spokesman reaffirmed.

It would not collect the online activities of users or collect any information about users, he said.

Accusations of the software's privacy invasion and blocking information flow, which had been raised by a few overseas media and institutions, is "groundless" and "irresponsible," he said.

Developers of the "Green Dam," greatly concerned over software security, had also modified the software as technical problems had been revealed during earlier promotion.

They will continue to improve the software with services packs and upgrades, said the spokesman.

The spokesman also mentioned that the government procurement procedure of the software had complied with China's Government Procurement Law, which was open, fair, transparent, non-exclusive, and under strict supervision.

The procurement of such filtering software is "an act for public good", and is in line with regulations of the World Trade Organization (WTO).

POPULAR AMONG PARENTS

The software, however, had already gained much popularity among parents, according to Zhao Huiqin, president of Jinhui Computer System Engineering Co. Ltd., developer of "Green Dam."

"There had been a geometric growth in Green Dam users this month," she said, pointing out that they had seen an average of more than 100,000 users registering the software per day, while the highest daily level had reached over 400,000.

Statistics from MIIT showed that the software had been downloaded 7.17 million times from the company's Web site by the end of last month, and 2.62 million computers in schools across the country, as well as 4.7 million ones in Internet bars, had been protected by "Green Dam".

A business man surnamed Zhou, who lives in China's southeastern Hangzhou City and has a pupil at home, registered for the software a week ago.

“Now I am at ease when my kid surfs on the Internet," he told Xinhua, as "Green Dam" had shut down most of the pornographic and other unpleasant contents in the past week.

The software could prevent 90 percent of improper content from the Internet, according to a third-party evaluation, said MIIT.

"I have read quite some negative reports on the software, but I need to take my child into consideration," Zhou said.

Source: news.xinhuanet.com, 30 June 2009.

Internet Attack Barometer

Interoute has launched a new online Internet Barometer detailing attacks as observed from their 22 monitoring stations across the European portion of the Internet.

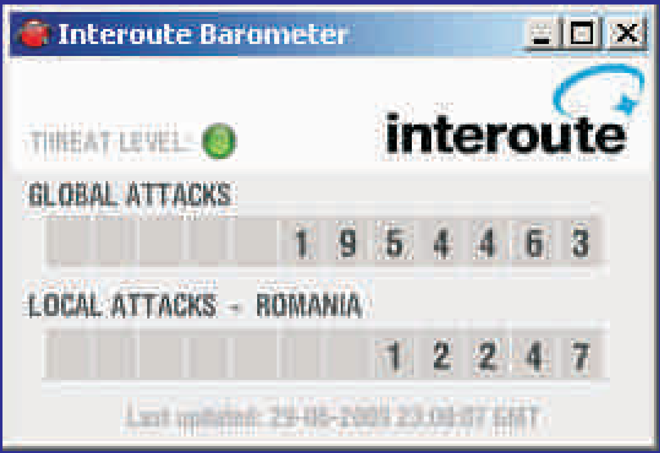
The site provides rich graph and chart interfaces, which are nicely interactive. There are definitely some ideas I want to incorporate form this into my own Network Telescope management console. It is however worth bearing in mind that his is a Eurocentric view and is only based on their observed traffic. As such the "attacking countries" view seems to be a bit skewed.

After digging around with squid and wireshark, its evident that a lot of the data is actually served up as XML files, and as such can potentially be postprocessed. The Adobe AIR Barometer Widget they provide also makes use of these. One issue I had getting this installed is you need Air 1.5.1, and the 1.0.8 version I had wouldn't auto upgrade correctly. A little disappointing in that I was expecting a map view, it provides the basics of a total count and cycles through various country stats.

Where the real value comes form is having another independent source of reporting (even at the highly granular level) that can be used to correlate observations with my own data sets, and those available form places like dShield and ISC. Maybe I should dust off my old Infocon alert plugin for Firefox and integrate some of this data.

Source: lair.moria.org, 30 June 2009.

Interoute Barometer Widget



THREAT LEVEL

GLOBAL ATTACKS
1 9 5 4 4 6 3

LOCAL ATTACKS - ROMANIA
1 2 2 4 7

Last updated: 29-06-2009 23:08:07 GMT

Interoute World view 2009-06-30

INTERPOL and FIRST to Fight Cyber Crime together

A law enforcement loophole through which cyber criminals have been escaping started to close today as international police and the world's leading forum of online security experts forged a new alliance.

INTERPOL today became the latest and biggest law enforcer to join FIRST, the Forum of Incident Response and Security Teams, in the battle against cyber crime.

The global police network's membership of FIRST was announced at the Forum's 21st annual conference in Kyoto.

Noboru Nakatani, INTERPOL's Director of Information Systems and Technology, hailed the move as "one of the most important bridges we've ever built" bringing the chance at last to close a gap between forensic techniques through which criminals have been able to escape justice.

While computer emergency response teams almost always try to disable attacks immediately, without waiting to trace aggressors who can then move on to fresh targets, police forces have preferred to watch crimes develop, hoping to pick up a trail that will lead to detection and a successful prosecution.

But, said Derrick Scholl, chairman of the FIRST steering committee, the problem of that approach is that "probably in no other area of criminal activity is it so easy to lay a false trail."

He explained: "Criminals can remotely hijack innocent users' PCs and deploy them to hack, steal and sabotage while the PCs owners carry on at the keyboard completely oblivious to what's going on behind their screens. So the cops turn up at the wrong door only to find someone who's not guilty, just bewildered.

"Track the incident down finally to the criminals' PCs and they can make it look as if they themselves are the innocent victims of a hijacking by unknown villains in a remote hideaway."

Often the elusive nature of cyber felony and the geographical vagueness of its origins have deterred or prevented police from undertaking investigations.

INTERPOL and FIRST agree that neither approach is working satisfactorily - but meanwhile some sources estimate that the perpetrators of just one version of Internet crime, "phishing" scams which purloin bank details online, are now stealing upwards of US$2-trillion a year.

Welcoming INTERPOL's admission as a member of FIRST, Mr Scholl went on: "This is the best chance we have of closing the gap. Having the biggest law enforcer on the planet on board with us is a great move forward.

"We've been wrestling with this problem now for three years, and at last here's a real opportunity to combine our efforts, set an agenda, and work to find a solution that gets criminals out of the virtual world and into the dock."

Vincent Danjean, INTERPOL Information Security Manager, addressed FIRST members today at their conference in the Hotel Granvia, Kyoto. He said: "INTERPOL provides the secure global police communication system which connects all its 187 member countries virtually with each other: now FIRST will be able to make use of this formidable network."

Meanwhile significant advances in the development of online detection programs were honored at the conference with awards jointly sponsored by FIRST and its affiliate and major conference sponsor CERT (computer emergency response team) Coordination Centre, the Software Engineering Institute CERT program in Pittsburgh, PA.

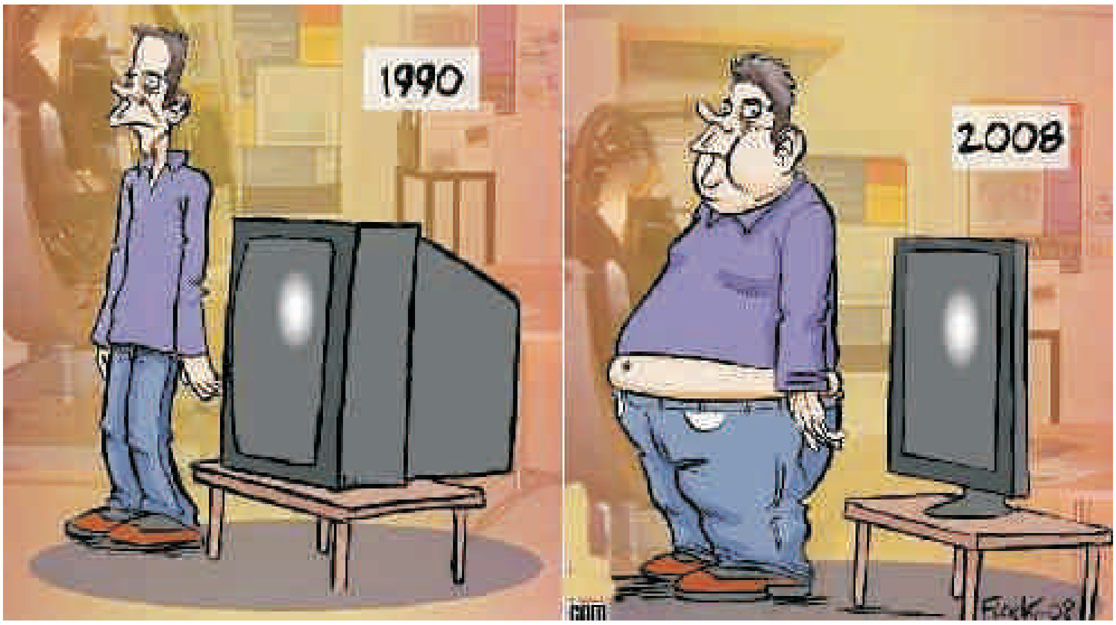
Thomas Grenman and his fellow team-members at CERT-FI (Finland) were awarded US$2500 for their pioneering creation of Autoreporter, which keeps the Finnish network space secure, and US$5000 was presented to Michael Scheck and fellow team members at Cisco CSIRT (computer security incident response team) who devised the groundbreaking Netflow system for incident detection.

Details and reports from both winners can be found at CERT CC's website, http://www.cert.org/csirts/national/contest_2009.html and on the FIRST website at http://www.first.org/global/practices/

Source: www.prweb.com, 30 June 2009.

Humour

How Technology changed our lives?



E-mail Scammers Focus on Webmail Accounts

According to security researchers, spammers are infiltrating users' Webmail accounts and using them to dispatch e-mails to each of the persons on the victim's address book. The e-mails usually advertise websites like electronic business sites alternatively make a direct request for money.

Explain the researchers that Webmail is an e-mail facility that is used through an Internet browser as opposed to a normal e-mail client.

Evidently, the 'Webmail account' hacking dishonorably manipulates a long standing scam. Miscreants down the years have relied on stolen e-mail ids from where they have been spamming mails so that the e-mails appeared authentic. However, with anti-spam solutions constantly improving in preventing such hoax e-mails, the conmen are currently compromising actual accounts to send their malicious e-mails.

Former Certified Public Accountant Maureen Arnold in Apache Junction, Arizona (USA) recently became a target of this kind of attack. One day as she checked her MSN mail, she saw several alert messages related to undelivered e-mails dispatched from her Webmail account which she never wrote.

To Arnold's surprise, the spam mail advertising a website that sold electronic items left her mailbox to reach her friends and family. Other attacks similarly requested recipients to remit cash to a specific bank account, with some even erasing the contact list of the hacked accounts later.

Meanwhile, the attacks highlight a frequently ignored truth that hackers chiefly target Webmail accounts due to the high value attached to them. A newly published report from the APWG (Anti-Phishing Working Group) states that the typical kinds of logins that keylogger malware steal are for e-commerce websites, financial sites as well as Webmail. Along with compromising a user's e-mail account for the dispatch of messages, miscreants could frequently harvest information with which they could break into the financial account(s) of a victim.

Moreover, experts apprehend that as cloud-computing increases along with a want to go online anytime, any place, Gmail as also other Webmail users could be exposed to a "man-in-the-middle" attack, which requires the capturing as also swindling of real cookies related to session browsing, while the intruder could be provided with complete access to an account.

Source: www.spamfighter.com, 04 July 2009.

France creates new national IT security agency

France has created a new national IT systems security agency to better defend its IT networks.

The French Networks and Information Security Agency (FNISA) will conduct a round-the-clock watch on sensitive government networks in order to detect and respond to cyberattacks.

That mission is increasingly important, as U.S. and South Korean government authorities have battled this week with attacks on their information infrastructures.

The French agency will also advise government departments and commercial network operators on best practices, and provide information about information security threats and how to avoid them to the general public.

In addition, FNISA will help develop trusted IT products and services for use by French companies and government networks. The possibility that key network infrastructure purchased from foreign suppliers could contain hidden "back doors" allowing them to spy on communications has become a concern for governments in recent years. A plan by Chinese network equipment manufacturer Huawei Technologies to acquire a stake in U.S. vendor 3Com in 2007 fell apart after U.S. lawmakers raised questions about the potential effect on national security.

FNISA was set up at the request of President Nicolas Sarkozy following a review of defense and national security last year. Its creation was announced in the government's Official Journal on Wednesday.

The agency is recruiting, and the vacancies to be filled give a taste of what concerns it.

For one post, it is looking for an engineer with experience in securing VOIP systems -- on desktop and mobile systems.

Another post will deal with the security of the physical layer of wireless communications systems, including Wi-Fi networks and contactless payment systems.

There are no clues which way the agency leans in the description of a post dealing with operating system security: neither Windows nor Linux gets a mention, although the ideal candidate will have experience of virtualization and compartmentalization of processes.

FNISA will take the place of an existing government agency, the Central Information Systems Security Division, which was set up in 2001 to advise the government and provide information to the general public on information security threats. Both agencies, old and new, fall under the control of the General Secretary for National Defense.

Source: Peter Sayer, www.itworld.com, 09 July 2009.

2 Jailed for hacking into phone system

A teenager and a 23-year-old man from Massachusetts are headed to prison after being sentenced in Dallas on conspiracy charges related to a phone hacking case.

Nineteen-year-old Matthew Weigman of Revere, Mass., was sentenced to more than 11 years in prison Friday after pleading guilty to one count of conspiracy to retaliate against a witness, victim or an informant and one count of conspiracy to commit access device fraud. Twenty-3-year-old Sean Paul Benton of Malden, Mass., received an 18-month sentence after pleading guilty to one count of conspiring to obstruct justice.

Prosecutors say Weigman hacked into Verizon computers to obtain identifying information on customers and change or discontinue their service. He and Benton then harassed a Verizon investigator who was cooperating with authorities in the case.

Source: www.kten.com, 29 June 2009.

Humour

Tips to protect your password

... Tip 1

.....next tip Page 15

Mobile phones at the mercy of hackers and viruses

Increased access to the internet via mobile phones has increased the risk of being targeted by the viruses and hackers that prowl the internet. Security experts today all concur that mobile phones are the least-protected devices in the entire computing arena, leaving them at the mercy of internet evils.

The need for mobile phone protection has jolted security software companies such as Moscow-based Kaspersky Lab into action to focus aggressively on mobile security development for both consumers and businesses using mobile phones as an internet source.

Smartphones have become essential devices, with many people relying on them to run their businesses and lives. That being the case, we keep loads of personal and importantly, company, information on our smart phones, creating a variety of security risks.

Smartphones are now essentially mini-computers with hefty processing power and ample storage capacity; business applications; as well as email and network capabilities - meaning that many of us rely on these devices for business communications, but have the potential to leave users open to security vulnerabilities.

In theory, the threats we currently face on personal computers can potentially be exposed on mobile phones if malicious code is unsuspectingly downloaded via the Web; through email or a Wi-Fi connection; or beamed via active Bluetooth and infrared ports.

Victor Dronov, Product Manager of Mobile solutions at Kaspersky Lab, says that over and above the threat of viruses, worms and malware that are doing the rounds on mobile phones today; the most common form of company data leakage is mobile phone theft.

"The regulation of Interceptions of Communications Act states that whenever a mobile phone or SIM card is lost; stolen; or destroyed, the owner of that mobile phone or SIM card must, within a reasonable time after having become aware of the loss, report it to a police official at any police station.

"However, this doesn't protect the content on the mobile device. Anyone who has access to your device potentially has access to your confidential information, be it private- or business-related," he says.

While this can have very serious implications, Dronov says that globally, companies are implementing measures to counter this, but few South African companies have mobile phone security measures in place with strong encryption and authentication policies to ensure the data remains secure.

"Every device needs to have an up-to-date antivirus scanner; anti-spam protection; and a firewall, together with an anti-theft solution that can track the stolen device even after the SIM card has been changed," Dronov says.

Research firm, IDC, reports that the mobile software industry is steadily moving towards providing standard features found on all desktop administration solutions, such as maintaining PC hardware and software inventories; performing software distribution; managing anti-virus scan files; and enabling remote control for systems diagnostics.

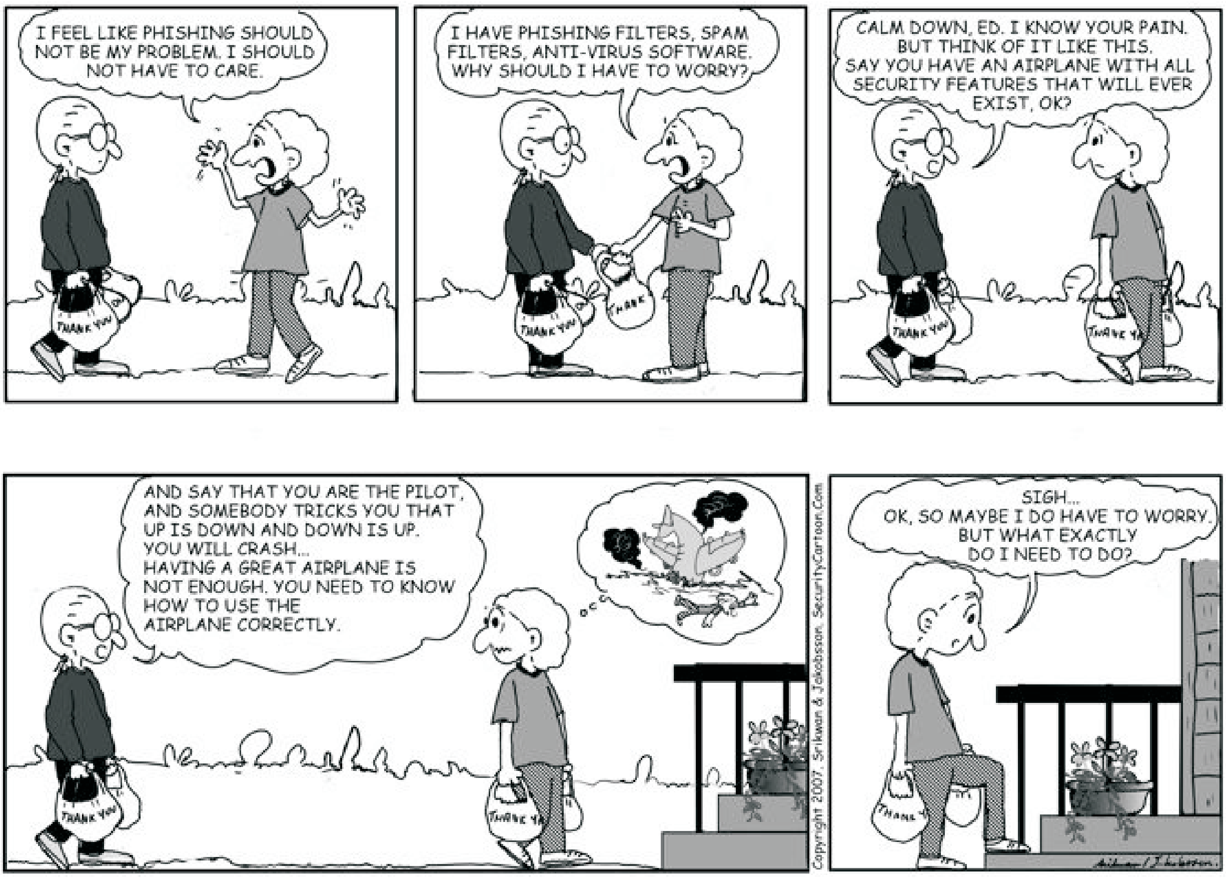
Kaspersky's Dronov says this trend will continue as more and more applications make their way onto mobile devices.

"Fortunately, while these risks are very real, they aren't insurmountable.
It"s just a case of using your common sense, just like you would against threats in the real world," he concludes.

Source: www.mediaupdate.co.za, 02 July 2009,

Humour

By Sukamol Srikwan & Markus Jakobsson


I FEEL LIKE PHISHING SHOULD NOT BE MY PROBLEM. I SHOULD NOT HAVE TO CARE.
I HAVE PHISHING FILTERS, SPAM FILTERS, ANTI-VIRUS SOFTWARE. WHY SHOULD I HAVE TO WORRY?
CALM DOWN, ED. I KNOW YOUR PAIN. BUT THINK OF IT LIKE THIS. SAY YOU HAVE AN AIRPLANE WITH ALL SECURITY FEATURES THAT WILL EVER EXIST, OK?
AND SAY THAT YOU ARE THE PILOT, AND SOMEBODY TRICKS YOU THAT UP IS DOWN AND DOWN IS UP. YOU WILL CRASH... HAVING A GREAT AIRPLANE IS NOT ENOUGH. YOU NEED TO KNOW HOW TO USE THE AIRPLANE CORRECTLY.
SIGH... OK, SO MAYBE I DO HAVE TO WORRY. BUT WHAT EXACTLY DO I NEED TO DO?
THANK YOU
Copyright 2007, Srikwan & Jakobsson, SecurityCartoon.Com

Reproduced with permission www.SecurityCartoon.com

Programmer arrested for stealing source code

Missing code may be hidden on German server

A Russian programmer has been arrested on charges that he illegally copied proprietary source code from his employer.

Sergey Aleynikov, a former computer programmer at Goldman Sachs, is accused of stealing the company's computer trading software shortly before leaving for a job with a rival firm.

The code was described in the affidavit as: "A computer platform that allows the financial institution to engage in sophisticated, high-speed, and high-volume trades on various stock and commodities markets.

"Among other things, the platform is capable of quickly obtaining and processing information regarding rapid developments in these markets. The financial institution believes that certain features of the platform, such as the speed and efficiency by which it obtains and processes market data, give the financial institution a competitive advantage among other firms that also engage in high-volume automated trading."

Aleynikov is accused of uploading the 32MB of code to a remote server in Germany. He has reportedly claimed that the upload was a mistake, and that he thought they were open-source files.

Aleynikov was caught because of the IT security procedures followed by his employer. While he allegedly made every effort to cover his tracks by deleting records of the upload, he was not aware that his employer ran a secret backup program that recorded every action of its employees.

These kinds of software backups are becoming increasingly common, particularly at companies in high value areas like the financial industry.

The majority of data theft is carried out from within companies rather than by outside hackers, and organisations are focusing less on building impenetrable firewalls and more on monitoring data flows.

Source: Iain Thomson, www.V3.co.uk, 07 July 2009.

Opinion

The Hidden Cost of Using Microsoft Software

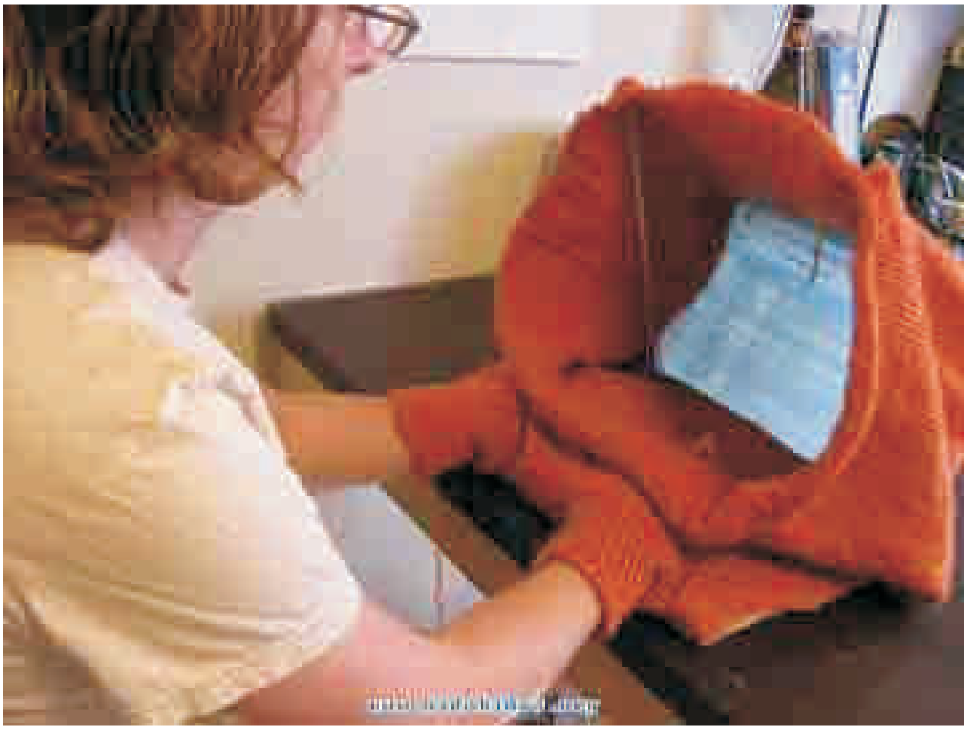
Glyn Moody writes "Detractors of free software like to point out it's not really 'free,' and claim that its Total Cost of Ownership is often comparable with closed-source solutions if you take everything into account. And yet, despite their enthusiasm for including all the costs, they never include a very real extra that users of Microsoft's products frequently have to pay: the cost of cleaning up malware infections.

For example, the UK city of Manchester has just paid out nearly $2.5 million to clean up the Conficker worm, most of which was 'a £1.2m [$2million] bill in the IT department, including £600,000 [$1 million] getting "consultancy support" to fix the problems, which including drafting in experts from Microsoft.' To make the comparisons fair, isn't it about time these often massive costs were included in TCO calculations?”

Source: news.slashdot.org, 30 June 2009

Humour

Tips to protect your password ... Tip 2



.....next tip on Page 22

US Social Security numbers are predictable

US Social Security numbers (SSNs) may not be as random as believed, as a new study contends that powerful mathematical techniques combined with open-source research can, in some cases, reveal a person's secret number.

The study, published on Monday in the journal Proceedings of the National Academy of Sciences, serves as a stark warning that SSNs are increasingly vulnerable, putting more people at risk of identity theft.

"Unless mitigating strategies are implemented, the predictability of SSNs exposes them to risks of identity theft on mass scales," the study said.

The study comes from Carnegie Mellon University's Alessandro Acquisti, an assistant professor of information technology and public policy, and Ralph Gross, a postdoctoral researcher.

The Social Security Administration responded on Tuesday, saying the public should not be alarmed since there is no foolproof method for predicting an SSN. However, the agency said it is developing a new system to randomly assign SSNs that will be in place next year, although those efforts are unrelated to the study.

"The method by which Social Security assigns numbers has been a matter of public record for years," the statement said. "The suggestion that Mr. Acquisti has cracked a code for predicting an SSN is a dramatic exaggeration."

Gross and Acquisti developed an algorithm that analyzed data from the Social Security Administration's Death Master File, a public database of some 65 million Americans who have died and their SSNs, which is used for antifraud purposes.

They looked for numerical patterns in the deceased's SSNs, drawing correlations between where a person was born and their birth date and how that data relates to their SSN.

"Our prediction algorithm exploits the observation that individuals with close birth dates and identical state of SSN assignment are likely to share similar SSNs," they wrote.

The first three digits of an SSN is an area number, which is based on the Zip code of the mailing address provided when a card was applied for. The next two digits is a group number, which assigned in a "precise but nonconsecutive order between one and 99." The last four digits is a serial number.

The algorithm, which the authors did not detail, successfully ascertained the first five digits for 44% of the records in the Death Master File for people born between 1989 to 2003. The complete SSN could be picked out for 8.5% of those people in under 1,000 attempts. For people born between 1973 and 1988, the algorithm could predict the first five digits for 7% of those in the Death Master File.

"SSNs were designed as identifiers at a time when personal computers and identity theft were unthinkable," the study said.

Other changes in how the Social Security Administration assigns numbers have made guessing even easier. In 1989, the agency stated a program called Enumeration at Birth, assigning SSNs to newborns as part of the birth certification process.

The changes, however, increased the correlation between a person's birth date and all nine digits of a SSN, especially for people in less populated states, making SSNs easier to discover, the researchers wrote.

DID YOU KNOW YOUR SOCIAL SECURITY NUMBER IS ALMOST THE SAME AS SOME RICH GUY?
GIVE

Additionally, the proliferation of information on social-networking profiles, such as a person's hometown and birth date, puts people at greater risk, since that information could be used to infer SSNs.

"Such findings highlight the hidden privacy costs of widespread information dissemination and the complex interactions among multiple data sources in modern information economies," the researchers wrote.

Attackers could then take the SSNs they think are accurate and run them through credit approval services. Even though many of those services will limit the number of attempts to verify data, botnets could be employed to test vast numbers of SSNs to ensure they're valid, they wrote.

The Social Security Administration also said that it has cautioned the private sector against using SSNs as a personal identifier.

Source: Jeremy Kirk, www.computerworld.com, 7 July 2009,

Sharing information is the best way to beat cyber crimes

Police need to focus on ways of sharing information to improve chances in fight against cyber crime

As Lord Carter's Digital Britain report tries to promote an all-digital world, there is also a darker opportunity for less-than-honest people to enrich themselves through the digital economy. To combat the growing threat of cyber crime, new approaches are needed. So exactly how will the police address the thorny problem of internet crime and cyber criminals in the future?

At a roundtable hosted by business and technology consultants Unisys, six of the UK's leading experts from academia and the front line of public law enforcement agencies debated the problem of cyber crime, and how and where the UK needs to deploy resources to address the threat.

David Wall, professor of criminal justice and IT at Leeds University, outlined the historical path to the current cyber crime epidemic. First, discrete mainframe systems created an opportunity for insider hacking and fraud; the move to dial-in modems created opportunities for hacking out of so-called " phone freaking". Finally, broadband development led to the creation of botnets. The next phase of cyber crime, said Wall, "will come out of the ambient technologies, and we need to look at the convergences and the knock-on effects that could happen when these technologies mature."

National Police Improvement Agency (NPIA) detective superintendent John Mooney insisted that police must be attuned to the next generation of threats before it is too late. "From a policing perspective, we always seem to be playing catch-up," he said.

One of the major successes in fighting cyber crime was Operation Cathedral, which targeted an international child pornography ring, the so-called Wonderland Group. But that success highlights one of the difficulties facing the crime fighter: success encourages criminals to modify their behaviour. As Birmingham City University's professor of criminology David Wilson noted: cyber criminals are "already using net-enabled mobile phones and peer-to-peer systems, and won't leave the kind of trace they used to leave on their systems."

A further difficulty for police is that traditional forces were set up to deal with local crime, where incidents took place in the real world. "The vast majority of police forces are still mainly dealing with crimes such as car robberies and simple theft," said John Vine, independent chief inspector at the UK Border Agency.

This creates a problem for forces to "get a proper balance which acknowledges the need for delivery of local policing services, while addressing cyber crime, " said Ian Readhead, director of information at the Association of Chief Police Officers (Acpo).

Furthermore, the fight against cyber crime was being hamstrung by a failure to collect proper data on its prevalence, said Peter Sommer, visiting professor at the London

School of Economics. The Crown Prosecution Service rarely charges under the Computer Misuse Act, preferring to use other fraud-related laws, or child protection legislation.

Better information collection and sharing would also help improve the effectiveness of policing cyber crime, said NPIA's Mooney. "We need a much better ability to share information with each other. We've got to the first stages of that with the police national database, and there's the Information Systems Improvement Strategy programme," he said.

Another problem highlighted by the UK Border Agency's Vine was that the debate on cyber crime needs to be concentrated on more than just "intra-police boundaries ". "There are 9,000 warranted officers working for the UK Border Agency now, and there is a much higher need for organisations to share intelligence," said Vine.

"We need to get away from bespoke applications, which would help people share information. We keep talking about this, but we need to make greater progress in dealing with it," he added.

ACPO's Read said that because of the pressure on finance, developing bespoke applications through which information will be shared wouldn't happen as much. "We'll be developing proven, commercial ones off the shelf."

"We need to see how we can converge and have open systems, perhaps building first on regional and then national applications, which are coherent and financially affordable," he added.

Source: Dave Bailey, www.computing.co.uk, 29 June 2009.

Weak security opens door to hackers

Every time you swipe your credit card and wait for the transaction to be approved, sensitive data including your name and account number are ferried from store to bank through computer networks, each step a potential opening for hackers.

And while you may take steps to protect yourself against identity theft, an Associated Press investigation has found the banks and other companies that handle your information are not being nearly as cautious as they could.

The government leaves it to card companies to design security rules that protect the nation's 50 billion annual transactions. Yet an examination of those industry requirements explains why so many breaches occur: The rules are cursory at best and all but meaningless at worst, according to the analysis of data breaches dating to 2005.

It means every time you pay with plastic, companies are gambling with your personal data. If hackers intercept your numbers, you'll spend weeks straightening your mangled credit, though you can't be held liable for unauthorized charges. Even if your transaction isn't hacked, you still lose: Merchants pass to all their customers the costs they incur from fraud.

More than 70 retailers and payment processors have disclosed breaches since 2006, involving tens of millions of credit and debit card numbers, according to the Privacy Rights Clearinghouse. Meanwhile, many others likely have been breached and didn't detect it. Even the companies that had the payment industry's top rating for computer security, a seal of approval known as PCI compliance, have fallen victim to huge heists.

Companies that are not compliant with the PCI standards—including one in 10 of the medium-sized and large retailers in the United States—face fines but are left free to process credit and debit card payments. Most retailers don't have to endure security audits, but can evaluate themselves.

Credit card providers don't appear to be in a rush to tighten the rules. They see fraud as a cost of doing business and say stricter security would throw sand into the gears of the payment system, which is built on speed, convenience and low cost.

That is of little consolation to consumers who bet on the industry's payment security and lost.

It took four months for Pamela LaMotte, 46, of Colchester, Vt., to fix the damage after two of her credit card accounts were tapped by hack-ers in a breach traced to a Hannaford

Bros. grocery store.

LaMotte, who was unemployed at the time, says she had to borrow money from her mother and boyfriend to pay $500 in overdraft and late fees—which were eventually refunded— while the banks investigated.

“Maybe somebody who doesn't live paycheck to paycheck, it wouldn't matter to them too much, but for me it screwed me up in a major way,” she said. LaMotte says she pays more by cash and check now.

It all happened at a supermarket chain that met the PCI standards. Someone installed malicious software on Hannaford's servers that snatched customer data while it was being sent to the banks for approval.

Since then, hackers plundered two companies that process payments and had PCI certification. Heartland Payment Systems lost card numbers, expiration dates and other data for potentially hundreds of millions of shoppers. RBS World- Pay Inc. got taken for more than 1 million Social Security numbers—a golden ticket to hackers that enables all kinds of fraud.

In the past, each credit card company had its own security rules, a system that was chaotic for stores.

In 2006, the big card brands—Visa, MasterCard, American Express, Discover and JCB International— formed the Payment Card Industry Security Standards Council and created uniform security rules for merchants.

Avivah Litan, a Gartner Inc. analyst, says retailers and payment processors have spent more than $2 billion on security upgrades to comply with PCI. And the payment industry touts the fact that 93 percent of big retailers in the U. S., and 88 percent of medium-sized ones, are compliant with the PCI rules.

Computer security experts say the PCI guidelines are superficial, including requirements that stores run antivirus software and install computer firewalls. Those steps are designed to keep hackers out and customer data in. Yet tests that simulate hacker attacks are required just once a year, and businesses can run the tests themselves.

“It's like going to a doctor and getting your blood pressure read, and if your blood pressure's good you get a clean bill of health,” said Tom Kellermann, a former senior member of the World Bank's Treasury security team and now vice president of security awareness for Core Security Technologies, which audited Google's Internet payment processing system.

“PCI compliance can cost just a couple hundred bucks,” said Jeremiah Grossman, founder of WhiteHat Security Inc., a Web security firm. “If that's the case, all the incentives are in the wrong direction. The merchants are inclined to go with the cheapest certification they need.” For some inspectors, the certification course takes just one weekend and ends in an open-book exam.

Security experts say there are several steps the payment industry could take to make sure customer information doesn't leak out of networks. Banks could scramble the data that travels over payment networks, so it would be meaningless to anyone not authorized to see it.

Another possibility: Some security professionals think the banks and credit card companies should start their own PCI inspection arms to make sure the audits are done properly. Banks say they have stepped up oversight of the inspections, doing their own checks of questionable PCI assessment jobs. But taking control of the whole process is far-fetched: nobody wants the liability.

Source: Jordan Robertson ,www.buffalownews.com, July 06, 2009,

Humour

Tips to protect your password

... Tip 3

...next tip on Page 25

Cyberspace Shapes Up To Be Next Battleground

Government and private computers are attacked millions of times a day. Many of these attacks are easy to identify and stop. The most sophisticated ones are not, and we must establish patterns of close cooperation and information-sharing among public and private experts to give ourselves the best chance to mitigate a substantial attack on vital systems.

Congressional computers have been penetrated, probably by the Chinese. The avionics system of the F-22 fighter may be compromised. Computers of our presidential candidates were hacked into --- and probably not by teenagers on a lark.

Last year's advance of Russian tanks into Georgia was accompanied by the disruption of Georgian government computer systems.

These are only public manifestations of a new reality: Attacks on computer systems will be an integral element of future conflict, and the United States is more dependent on computer networks than any other nation.

Both policy-makers and the military are in the early stages of coming to grips with this threat. We need to take some important first steps to strengthen our national capability to defend ourselves in cyberspace.

First, we must abandon the notion that static defenses will help us against sophisticated threats.

One bipartisan Senate bill proposes to establish a government committee to set standards for all computer systems and software.

This is the electronic equivalent of building a Maginot Line of concrete fortifications against a mobile enemy.

It may keep common criminals at bay, but it will be no defense against a mobile and adaptable top-tier adversary.

American government and private computer systems operate on an interconnected global network that is constantly changing like a biological organism.

It operates at light speed, and both friends and adversaries are connected to the same network.

We must anticipate that the most dangerous players will stay quiet until a time of national tension.

Our cyber-defense capabilities must be inherently dynamic, with a close connection between system operators, intelligence analysts, and the researchers who can rapidly build and deploy tools to protect or restore vital capabilities.

Second, our intelligence on other countries' cyber capabilities must be strengthened.

We have scores of trained experts who know the ins and outs of foreign radars and missile systems and almost none who are daily tracking cyber threats in all their manifestations.

What new tools are under development and how do they work? How do other countries and non-state actors train their people? What do they value and what, if anything, can deter them? How do the entities that pose a threat communicate and who commands them? Who are these guys, anyway?

We need to know more about our sophisticated adversaries before they strike so that we can defeat them.

Third, while there are national security Relevant Products/Services systems we certainly need to protect, our greatest vulnerability as a nation is outside the government.

Our banking system, our telephone communications Relevant Products/Services and our electricity grid are all owned and run by private companies and are interconnected to the global computer network.

We must anticipate that an adversary determined to cause economic damage or enhance the fog of war will exploit these vulnerabilities.

Currently, there is a strong disincentive for private entities to reveal that their computer systems have been compromised.

For example, a bank that lets people know that its computers have been penetrated will see business move elsewhere and stock prices drop even if its competitors are dealing with the same problems.

Yet an important part of protecting ourselves is sharing information about what probes and compromises are found before a period of crisis or heightened tension.

While the government could mandate reporting of certain threats, some problems are so difficult to identify that failure to report would be easily justified.

And a compliance-oriented reporting system will not encourage the learning needed or expand the capacity of critical private-sector systems to protect themselves.

A better approach is to align the interests of stockholders with the interests of national security by establishing a trusted safe harbor where private entities can confidentially share information and get help from cyber experts in and out of government.

Such an information clearinghouse could, without attribution, share information with other private entities so that everyone benefits.

The motivation to share information would be immunity from liability when private entities report problems.

Government and private computers in this country are attacked millions of times a day. Many of these attacks are easy to identify and stop.

The most sophisticated ones are not, and we must establish patterns of close cooperation and information-sharing among public and private experts to give ourselves the best chance to mitigate a substantial attack on vital systems.

Cyber warfare is a realm where technology is fast outpacing policy, doctrine and law. We must start closing the gap.

Source: Heather Wilson, www.enterprise-security-today.com, July 3, 2009.

Humour

Tips to protect your password

... Tip 4

Courtesy - Kamal Singh

Women More Online Security Conscious than Men

According to a new survey conducted by security vendor 'PC Tools', more than one third of computer users do not update their security applications that include spam filters, antivirus and other security products. Besides, more than 50% of computer users neglect security alerts they receive, as reported by watchdog on June 18, 2009.

The survey also discloses that men are less savvy than women in terms of online security, which means when a man is using a computer, the chances of malware infiltration in the system increases.

PC Tools has discovered that around 47% of men using online banking services use the same passwords for online facilities whereas only 26% of women do the same. Men show more causal attitude towards e-mail attachment as 60% of them admitted of opening them instantly without checking their legitimacy while just 48% of women opened the attachments without complete scan. Moreover, men do not bother to check whether the website he is transacting on is legitimate or fake which implies that the possibilities of men falling to phishing scams are more compared to women.

However, PC Tools has revealed in its study that nearly 85% of men understand various types of security threats like social networking scams, dodgy e-mail attachments and website attacks. On the other hand, around 50% of women are unaware of the threats emanating from social networks. This implies that women are ignorant of the fact that they could be caught by phishing, e-mail scams and other kinds of malicious traps.

Dr. Michael Greene, Vice President of PC Tools, said that the study showed the gravity of problem on part of men who were quite complacent with regard to online security. If computer users applied commonsense and behavior-based protection apart from the existing antivirus while surfing online, they would effectively protect their personal and financial information, as reported by findmysoft on June 22, 2009.

After evaluating the study and its critical findings, PC Tools has advised users to change their attitude and become more abreast of online threats and the potential risks while using the Internet.

Source: www.spamfighter.com, 26 June 2009.

Fired employees would take with them password list, R&D plans and customer database

Despite a sharp rise in data breaches and increased media awareness on the subject, the third annual Cyber-Ark survey reveals that 35 percent of IT workers now admit to accessing corporate information without authorisation, while 74 percent of respondents stated that they could circumvent the controls currently in place to prevent access to internal information.

Twelve months after the Cyber-Ark "Trust, Security & Passwords" survey discovered that 33 percent of IT staff used their IT administration rights to snoop around networks to access privileged, corporate information such as HR records, redundancy lists, customer databases and M&A plans, a repeat of the survey has discovered that the situation has escalated.

One of the most revealing aspects of the survey was found in the types and quantity of information employees would take with them if they were fired. As the economic climate has worsened, the survey found a sharp increase in the number of respondents who say they would take proprietary data and information that is critical to maintaining competitive advantage and corporate security.

When asked this year "What would you take with you," the survey found a six-fold increase in staff who said they would take financial reports or merger and acquisition plans, and a four-fold increase in those who would take CEO passwords and research and development plans.

Of the information targeted, respondents indicated they would be most likely to steal the following types of information:

Ominously, 1 in 5 companies admit having experienced cases of insider sabotage or IT security fraud. Of those companies, 36 percent suspect that their competitors have received their company's highly sensitive information or intellectual property.

Organizations are increasingly aware of the need to monitor privileged account access and activity, with 71 percent of respondents indicating that privileged accounts are partially monitored, while 91 percent of those who are monitored admitting they are "okay with their employer's monitoring activities." Despite these efforts, 74 percent of respondents revealed that even with the controls being put in place to monitor them, they could still get around them, making current controls ineffectual.

Highlighting the ineffectiveness of current controls and access policies, 35 percent of IT administrators admitted they were using their administration rights to snoop around the network to access confidential or sensitive information. The most common areas respondents indicated they access are HR records, followed by customer databases, M&A plans, redundancy lists and lastly, marketing information.

“This survey shows that while most employees claim that access to privileged accounts is currently monitored and an overwhelming majority support additional monitoring practices, employee snooping on sensitive information continues unabated. Unauthorised access to information such as customer credit card data, private personnel information, internal financial reports and R&D plans leaves a company vulnerable to a severe data leak with the risk of financial or regulatory exposure and damage to its brand, or competitors obtaining critically important competitive information,” said Udi Mokady, CEO of Cyber-Ark.

“Cyber-Ark is committed to raising awareness around the risk of unmanaged privileged accounts. While seemingly innocuous, these accounts provide workers with the 'keys to the kingdom,' allowing them to access critically sensitive information, no matter where it resides. Businesses must wake up and realize that trust is not a security policy; they have an organizational responsibility to lock down sensitive data and systems, while monitoring all activity even when legitimate access is granted,” Mokady added.

Source: www.securitypark.co.uk, 03 July 2009.

Skype banned by IT departments

Skype has joined Facebook and Hotmail on IT department blacklists as organisations limit avenues for information leaks, an Integ survey found.

Four in 10 of the 233 respondents surveyed at the recent AusCERT conference said they were blocking the popular internet telephone service, while a third blocked Facebook and Hotmail.

Hosted audio conferencing was also blocked by 13 percent of those surveyed.

It found organisations were finding other, more easily managed ways to communicate.

Nearly half said they provided workers with an internal instant messaging tool, half provided collaboration tools such as Microsoft Sharepoint, and more than a quarter had their own blogging software.

"Organisations are keen to keep the elements of [popular social networking] tools that have business use in their internal environments," said Integ chief Ian Poole.

Source: www.itnews.com.au, 08 July 2009.

Around 10 per cent of phishing attacks target India

Around 10 per cent of all global phishing activities are being targeted at India. RSA, the security division of EMC, points out that the evidence of this trend lies in the fact that several Indian banks came under attack in 2008, and there have been over 400 phishing scams in the last few months.

However, more alarming is the fact that these attacks are likely to increase in future. “The convenience and ease of conducting financial transactions with a single click is increasingly witnessing online banking coming of age in India and many other parts of Asia. As a result, these geographies represent a ripe new market for cyber criminals who look to launch online attacks,” said Arthur W Coviello, Jr, president RSA, the Security Division of EMC .

Source: Kritika Suneja, www.business-standard.com, 09 July 2009,

Cyber Security Practices

Create stronger passwords

Here's how to make your personal data harder to hack

An attacker who wants to break into one of your accounts manually might first try likely passwords such as your pet's name, your anniversary, or other terms that are significant to you. If that doesn't produce results quickly, a hacker might turn to a program that rapidly tries each of the thousands or even millions of words in a big list—a procedure known as a dictionary attack. Some dictionary attacks are quite clever, checking not only common English terms but also foreign words, common misspellings, words in which letters have been replaced by numbers or symbols (such as @ppl3 for Apple), and easy-to-type sequences of characters, such as poiuytre.

If that doesn't work, and if someone has the time and motivation, the next step would be a brute-force attack. In this type of attack, a computer program tries every possible combination of characters until the password is found, although current technology puts practical limits on the extent of such attacks.

When you create a new password, the trick is to come up with something that a dictionary attack could never discover, and to make the password long enough and complex enough that even a brute-force attack couldn't succeed because it would require too much time and processing power. Here's how:

Make them long

Passwords become exponentially harder to crack with each character you add, so longer passwords are much better than shorter ones. A brute-force attack can easily defeat a password with seven or fewer characters. Your mandatory minimum should be eight characters. Even then, you need to make those eight characters count: a randomly generated eight-character password using letters, numbers, and symbols (for example, h7%R9#jA) is vastly more secure than an ordinary eight-letter word such as licenses. You'll get the best protection from a random password of at least 11 characters or a non-random password of at least 17 characters (make sure that the password is not discoverable in any dictionary).

Start with a sentence

True mathematical randomness is hard to come by, but for a run-of-the-mill password, what counts is that a computer couldn't discern obvious or personal patterns in it. One common way to create a random password is to turn a sentence that you can easily remember into a password by using the first letter of each word, perhaps substituting some numbers as appropriate. The string ZTwt12potUS, as it follows no apparent pattern, might be a good choice. But it's still quite memorable because I derived it from the sentence "Zachary Taylor was the twelfth president of the United States."

Spell out a sentence

Systems vary as to the maximum password length they permit, but in cases where you have a large maximum, such as 32 or more characters, you can use an entire sentence. Because spaces, apostrophes, and quotation marks sometimes confuse computers when used in passwords, leave out those items—but keep other punctuation (such as a period), and include at least one digit for extra security. For example, Mymotherwas30yearsoldwhenIwasborn. and IwasinNewYorkonDecember31,2000. are splendid passwords.

Mix and match

Even though words, names, and dates someone might associate with you make poor passwords, you can produce much stronger passwords by combining several terms in unexpected ways. For example, if you combined your first pet's name, the last four digits of your phone number when you were growing up, and your high-school mascot, you might get something like Fluffy3057Bears. Any one of those terms alone might be guessable, but the combination probably won't be if it's long enough.

Try a password generator

If you have trouble coming up with good passwords, and especially if you have to create a large number of them or want them to be as random as possible, you can use one of many programs that generate passwords for you.

Password Assistant

You don't have to come up with strong passwords on your own. Password Assistant, an easy-to-use tool built into OS X, can automatically create passwords to your specifications.

Password Assistant is an excellent password generator built into OS X. To use it, click on the key icon next to the password field in places such as Keychain Access (/Applications/Utilities), the Accounts pane of System Preferences, or the Set Master Password dialog box in the Security preference pane's FileVault tab. If you'd rather access Password Assistant like an ordinary program, download Code Poetry's free Password Assistant utility.

Once you access Password Assistant, you can choose a password type (such as Memorable or Letters & Numbers) from the Type pop-up menu, move the slider to determine how long the password will be, and then choose any of ten suggested passwords from the Suggestion pop-up list.

Stealing data using electrical outlets and cheap lasers

Researches plan to demonstrate security weaknesses of keyboards at Black Hat.

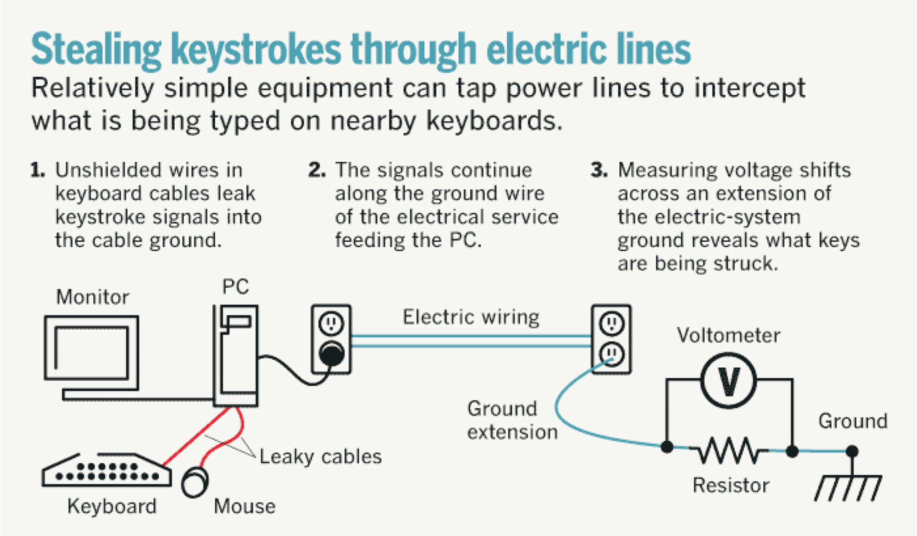
If attackers intent on data theft can tap into an electrical socket near a computer or if they can draw a bead on the machine with a laser, they can steal whatever is being typed into it.

How to execute these attacks will be demonstrated at the Black Hat USA 2009 security conference in Las Vegas later this month by Andrea Barisani and Daniele Bianco, a pair of researchers for network security consultancy Inverse Path.

"The only thing you need for successful attacks are either the electrical grid or a distant line of sight, no expensive piece of equipment is required," Barisani and Bianco say in a paper describing the hacks.

The equipment to carry out the power-line attack could cost as little as $500, and the laser attack gear costs about $100 if the attacker already owns a laptop with a sound card, says Barisani. Carrying out the attacks took about a week, he says.

"We think it is important to raise the awareness about these unconventional attacks and we hope to see more work on this topic in the future," Barisani and Bianco say in their paper. Others with more time and money could doubtless create better spying tools using the same concepts, they say.


Stealing keystrokes through electric lines

Relatively simple equipment can tap power lines to intercept what is being typed on nearby keyboards.

1. Unshielded wires in keyboard cables leak keystroke signals into the cable ground.
2. The signals continue along the ground wire of the electrical service feeding the PC.
3. Measuring voltage shifts across an extension of the electric-system ground reveals what keys are being struck.
Monitor
PC
Electric wiring
Voltometer
V
Ground extension
Ground
Leaky cables
Resistor
Keyboard
Mouse

In the power-line exploit, the attacker grabs the keyboard signals that are generated by hitting keys. Because the data wire within the keyboard cable is unshielded, the signals leak into the ground wire in the cable, and from there into the ground wire of the electrical system feeding the computer. Bit streams generated by the keyboards that indicate what keys have been struck create voltage fluctuations in the grounds, they say.

Attackers extend the ground of a nearby power socket and attach to it two probes separated by a resistor. The voltage difference and the fluctuations in that difference – the keyboard signals – are captured from both ends of the resistor and converted to letters.

To pull the signal out of the ground noise, a reference ground is needed, they say. "A "reference" ground is any piece of metal with a direct physical connection to the Earth, a sink or toilet pipe is perfect for this purpose (while albeit not very classy) and easily reachable (especially if you are performing the attack from [a] hotel room," they say in their paper.

Since keyboards and mice signals are in the 1 to 20 kHz range, a filter can isolate that range for listening, they say.

Variations in individual keyboards and mice result in each keyboard signaling in a slightly different frequency range. With careful filtering, that makes it possible to zero in on a particular keyboard in an environment where many keyboards are in use, the researchers say.

The attack proved successful when tapping electric sockets located up to 15 meters from where the target computer was plugged in the researchers say.

This method would not work if the computer were unplugged from the wall, such as a laptop running on its battery. The second attack can prove effective in this case, Bianco's and Barisani's paper says.

Attackers point a cheap laser, slightly better than what is used in laser pointers, at a shiny part of a laptop or even an object on the table with the laptop. A receiver is aligned to capture the reflected light beam and the modulations that are caused by the vibrations resulting from striking the keys.

This modulation is converted to an electrical signal that is fed into a computer soundcard. "The vibration patterns received by the device clearly show the separate keystrokes," the researchers' paper says. Each key has a unique vibration pattern that distinguishes it from the rest. The spacebar creates a significantly different set of vibrations, so the breaks between words are readily apparent.

Analyzing the sequences of individual keys that are struck and the spacing between words, the attacker can figure out what message has been typed. Knowing what language is being typed is a big help, they say.

Laptop lids, especially shiny logos and areas close to the hinges, provide the most easily read vibrations.

Anyone worried about this type of attack can make sure there is no line of sight to the laptop, move position frequently while typing and polluting the signal by striking random keys and later deleting them with the backspace key.

While they admit their hacking tools are rudimentary, they believe they could be improved upon with a little time, effort and backing.

"If our small research was able to accomplish acceptable results in a brief development time (approximately a week of work) and with cheap hardware," they say. "Consider what a dedicated team or government agency can accomplish with more expensive equipment and effort,"

Source: Tim Greene , Network World , 09 July 2009.

Quiz 0003

1. If you receive an email from a Bank saying that you need to authenticate yourself and thus asking to click a weblink, specified in the email. On clicking the weblink, the Bank website opens and asks your login, password and other details. This type of fraud is called __________.

2. ________ is the agency created by the amended Indian Information Technology Act-2000 to address all issues related to Cyber Crimes

3. If you copy your data in a CDROM / Pen drive / Tape, the process is called ________.

4. France has created a new national IT systems security agency, called ________.

5. To keep your anti-virus up-to-date to fight all known virus, you need to download latest anti virus __________ daily

Terms & Conditions

- One Grand Prize winner will be awarded a cash prize of INR 1000.00.
- Three consolation prizes will be gift hamper of 3 books published by CRPCC/Sysman.
- Winners having all correct entries will be selected by lottery.
- If there is no "all corrrect" entries no prize will be awarded.
- Decision of CCCNews will be final and can not be challenged.
- Gift hampers will be collectable from CCC News office in Mumbai.
- Last date to send entries is 22 July 2009 IST 24:00 hrs.
- Winners will be declared in next issue of CCC News Magazine.
- Please send email with correct answers of all 4 questions to quiz@cccnews.in with your name, age, designation (if any), company (if any), Postal address, Phone no. & email address, please write "Quiz 0002 answers" in subject.
- Ambiguous answers may be out right rejected

Answers to Quiz 0002

a. Which programming languages are associated with buffer overrun?
Ans: C, C++

b. Which is a secure replacement for telnet?
Ans: SSH, MD5

c. What is a DoS attack?
Ans: Denial of Service Attack

d. Which network topology is often used to separate public services such as Web and mail servers from the internal network?
Ans: DMZ

e. Which algorithms are used to compute digital signatures?
Ans: Asymmetric Algorithms

Winners of Quiz 0002

Grand Prize winner
Mr. Arzan Dastoor
Mumbai

Consolation Prize
Mr. Yashwant Chavhan
Delhi

Mr. Durgesh Saqcena
Mumbai

Ms. Sharmila Ghosh
Kolkatta

Hackers are dead.