CCC News

Control Computer Crimes

Issue 0009 - 31 October 2009

Message from the Editor

Welcome to the ninth issue of CCCNews Magazine.

The CCCNews Magazine has become a complete digest to provide value addition to news.

In this edition, we brings you an story on the first internet worm, which was created and released in 1988 in Cornell University in US. The worm had an interesting bug, due to which the author of the worm was caught. What happened to worm and the author, is an interesting story.

Further, we bring 10 stories of havoc created by teenage hackers in over a period of time. Another story covers 10 email blunders of 2009, which is not yet over.

We further discuss, four myths of Cyber Security, where people have fixed mental blocks about, (a) who is responsible for cyber security; (b) why I am protected; (c) do we need cyber security and; (d) security is difficult. The author discusses these four myths and provides interesting insight.

We bring a next report on the experience of Estonia, when they were cyber attacked 2 years back. Nations and organisations can take advantages of their experiences to mould their own policies to suit their specific needs.

Happy reading,

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0009
31 October 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

LAST ISSUE DOWNLOAD COUNT : 155,000+

OPINION

The Four Myths of Cyber Security

Incidents and exploits crafted by an effective and growing menace are threatening the continuity of and confidence in the very core of our commercial and social infrastructure. In just 90 criminal investigations performed in 2008, where data compromise was confirmed, the Verizon Business RISK team reported more than 285 million consumer credit records stolen. This number far exceeds the combined total confirmed for all its investigations from 2004 to 2007.

Organizations around the globe are failing to accept responsibility for their own security. Instead, they are blaming the inherent flaws and insecurity of the Internet and claiming ignorance in the erroneous belief that security is a global problem. Therefore, they say, everyone is to blame with no single company guilty.

It’s time to dispel these myths:

Myth One: World Leaders Are Responsible For Making the Internet Safe

With cyber attacks threatening to bring down an entire country’s digital systems by allowing foreign states to access them, it is clear that there’s no magic wand now, or likely to be anytime soon, for anyone.

Internet fraud is costing billions of pounds a year. Even Whitehall computer systems are facing repeated assaults from abroad, so UK ministers may be deemed either genius, or just desperate, in their decision to hire hackers to protect state secrets. In addition, June saw Prime Minister Gordon Brown appoint the first national cyber security chief, a senior civil servant named Neil Thompson, to protect the country from terrorist computer hackers and electronic espionage. That appointment came amid fears that the computer systems of government and business are vulnerable to online attack from hostile countries and terrorist organizations. Another tactic is that of the Police Central E-Crime Unit, which has asked IT industry workers to volunteer in the fight against cyber crime.

Let’s face it, the primary role of the police is to protect us and keep our property safe. But if we decide to leave our doors and windows wide open, they’d be the first to point out we were inviting trouble.

The UK government doesn’t have the finances, resources or even the remit to make the entire Internet a safe place for everyone that uses it. It’s trying to do the best it can – so should you.

Myth Two: I’ve Got A Firewall, So I’m Safe

A firewall isn’t enough protection due to its very ethos – it provides a gateway for users to explore the outside world and, therefore, is the very doorway by which hackers gain entry. Systems are designed primarily to help users travel through the firewall often with little regard given to what may travel in the opposite direction. Hackers understand the typical code used and will exploit simple mistakes in programming and oversights in security efforts. Verizon’s 2009 Data Breach Investigation Report states “only 17 percent of attacks were designated to be highly difficult.” So the conclusion is that 83 percent were not difficult and therefore avoidable.

In the more successful breaches, attackers will exploit a mistake committed by the victim, such as unauthorized access via default credentials (usually third-party remote access) and SQL injection (against Web applications). This is a phenomenon verified by Verizon, which established that 67 percent of the breaches it investigated in 2008 were “aided by significant errors.”

Myth Three: “A Hacker Wouldn’t Target us - We Don’t Process Financial Transactions.”

Why spend money on research and development if you can steal the product from someone else? Intellectual property theft is an "invisible" type of business theft, meaning it often isn't thought about and can go unnoticed, but it costs organizations billions. Unlike credit card data that can clearly be identified as stolen when fraudulent charges are later incurred, the impact of a company losing proprietary designs, business plans, inventory strategies and so forth may never be visibly traced to a single event. In a survey of 800 chief information officers in Japan, China, India, Brazil, Britain, Dubai, Germany and the United States, the companies surveyed estimated they lost a combined £2.9 billion (US$4.7 billion) worth of intellectual property last year alone, and spent approximately £375 million (US$612 million) repairing damage from data breaches.

Myth Four: "It's Too Difficult to Secure My Systems."

Programmers have a responsibility to test and score the security of their software. By employing secure coding practices earlier in the software development life cycle, errors can be avoided. There are online services available that allow you to upload in-house, and vendor, open source and outsourced software to test the code. An automated turnkey solution will provide both source- and binary-level static analysis for accurate detection of security vulnerabilities, returning accurate and complete findings, with vulnerabilities prioritized based on severity and exploitability. It also empowers in-house and third-party developers to actively manage application security on their own terms, extending limited security resources and reducing total cost of security by replacing more expensive assessment services.

If you are in business today, you have risks — it's that simple. You have something to lose. If you don't, well, then don't worry, because you won't be in business much longer. Your software is probably one of the single largest exposures to risk that your business faces today. At the same time, if it is designed and built correctly, your software could end up being one of your most effective countermeasures against most of the common attacks employed by hackers today. Don't be afraid – you can take control of your own security. The time is now.

Courtesy : Richard Kirk; http://www.itbusinessedge.com
Oct 27, 2009

ANALYSIS

10 Stories of Teenage Hackers Getting into the System

Examining the most famous youthful cybercriminals and their exploits

Much like Lolcats, some überteens are up in the Internet, stealing your ... well, whatever they want. If you envision these kids as harmless nerds who hole themselves up in their rooms clicking away their adolescence, check out this list, which details the costly and frightening toll their computer "games" have exacted throughout recent history.

1. Student at Downingtown High School West — Downingtown, Pa.

A 15-year-old student was arrested and charged with felonies in May 2008 for stealing personal data from the Downingtown School District's computer system and downloading files that contained the names and Social Security numbers of more than 41,000 of district residents (including 15,000 students). The unnamed student allegedly accessed the files, which were located on the district's server, through a school computer during a study period, and officials believe that he copied the files to his home computer. This is the second time in the 2007-2008 academic year that a student has broken into the Downingtown School District's computer system; another student was arrested for hacking into the system in December 2007.

2. Matthew the phone phreak — Boston

In February 2008, the FBI identified the culprit in a 2005 Colorado "swatting" incident — a phone hoax involving hackers who call in fake emergencies and get SWAT teams to barrel into people's homes. The responsible party was a 17-year-old East Boston "phreak," or phone hacker, named Matthew. The remarkable thing about him is that he's blind. Matthew, who's been at the game since he was 14, is considered one of the most skilled phreakers alive.

3. Jeanson James Ancheta — Los Angeles

In 2005, the FBI nabbed 20-year-old Jeanson James Ancheta, a reported member of the "Botmaster Underground," a group of script kiddies known for their bot attacks and spam inundation. His sinister cyberscheme infected computers at the United States Naval Air Warfare Center Weapons Division in China Lake, Calf. and the Defense Information Systems Agency, a component of the United States Department of Defense. In the first prosecution of its kind in the U.S., Ancheta was arrested and indicted on 17 federal charges for profiting from the use of "botnets."

4. Aaron Caffrey — Britain

Aaron Caffrey 19, was accused of almost destroying of North America's biggest ports, the Port of Houston in Texas, by hacking into its computer systems. Computers at the port were hit with a DoS (denial of service) attack on Sept. 20, 2001, which crashed systems at the port that contained data for helping ships navigate the harbor.

The prosecution said that the Brit’s computer contained a list of 11,608 IP addresses of vulnerable servers, along with malicious script. The attack on Houston was apparently tied to a female chat-room user called Bokkie, who had made anti-U.S. comments online. Still, a jury found Caffrey not guilty in October 2003.

5. Raphael Gray — Wales

Raphael Gray, 19, became the subject of an international investigation after he got his hands on 23,000 Internet shoppers' details and posted some of them to Web sites. The scheme, which Gray claimed was an attempt to expose security weaknesses in Internet shopping, cost users hundreds of thousands of pounds. Gray was been sentenced to psychiatric care and told reporters that he felt no regret for what he’d done.

6. c0mrade — Miami

In 2000, a 16-year-old from Miami known on the Internet as "c0mrade" became the first juvenile to go to jail on federal computer-crime charges for hacking into NASA. The boy admitted to attacking a military computer network used by the DTRA (Defense Threat Reduction Agency) from Aug. 23, 1999 to Oct. 27, 1999. The youth installed a backdoor access on a server that intercepted more than 3,300 electronic messages to and from DTRA staff. The backdoor also accessed at least 19 usernames and passwords of DTRA employees, including at least 10 usernames and passwords on military computers. The unnamed juvenile was sentenced to six months in a detention facility.

7. Mafiaboy — Canada

Over a five-day period in February 2000, Yahoo! Inc., CNN, eBay Inc. and Amazon.com Inc. became victims of the largest DoS attack ever to hit the Internet. The attacker? A 14-year-old Canadian named Mike Calce, who went by “Mafiaboy” online. He became the most notorious teenage hacker of all time, causing millions of dollars worth of damage on the Internet.

Calce initially denied responsibility for the assault but later pled guilty to most of the nearly 50 charges against him. On Sept. 12, 2001, the Montreal Youth Court sentenced him to eight months of "open custody," one year of probation, restricted use of the Internet and a small fine. Calce later wrote as a columnist on computer-security topics for the French-language newspaper Le Journal de Montréal.

8. Ehud Tenenbaum — Israel

Computers at the Pentagon were targeted in an attack called "Solar Sunrise" during a tense time in the Persian Gulf in 1998. The attack led to the establishment of round-the-clock, online guards at major military computer sites. At the time, U.S. Deputy Defense Secretary John Hamre called the attack "the most organized and systematic attack" on U.S. military systems.

While officials initially pointed fingers at two American teens, 19-year-old Israeli hacker Ehud Tenenbaum, who was called "The Analyzer," was identified as their leader and arrested. Tenenbaum later became the CTO of a computer-consulting firm.

9. Richard Pryce and Matthew Bevan — Britain

Two teens touched off one of the biggest ever international computer crime investigations in the U.S. when, for several weeks in 1994, they attacked the Pentagon's computer network and tried to get access to a nuclear facility somewhere in Korea. The cyberculprits were identified as 16-year-old music student Richard Pryce (known as "Datastream Cowboy") and Matthew Bevan (known as "Kuji"), who was arrested two years later at age 21. Conspiracy charges against both Pryce and Bevan were later dropped, though Pryce was ordered to pay a small fine.

10. 414s — Milwaukee

They may sound like a cheesy '80s band, but the 414s were actually a band of youthful hackers who broke into dozens of high-profile computer systems, including ones at Los Alamos National Laboratory and Memorial Sloan-Kettering Cancer Center. Later uncovered as six youths ranging in age from 16 to 22, the group met when they were members of a local Explorer Scout troop. These Scouts-turned-cybercriminals were investigated by the FBI in 1983.

The media took to the story of the youths, who met the somewhat sexy profile of early '80s computer hackers as established by Matthew Broderick's character in "WarGames," which was released the same year that the 414s rose to glory. In fact, 17-year-old Neal Patrick got more than his 15 minutes of fame when he appeared on the Sept. 5, 1983 cover of Newsweek. Most of the members of the 414s were not prosecuted, but their cybershenanigans lead to government hearings on hacking, as well as the introduction of six bills concerning computer crime in the U.S. House of Representatives.

Courtesy : http://www.itsecurity.com

ANALYSIS

Top 10 E-mail Blunders Of 2009, So Far

Proofpoint's list of the ten biggest e-mail gaffes this year shows that organizations have yet to deal with the risks of e-mail

E-mail, the Internet's first killer app, can injure companies and individuals when not used with care.

In its attempt to document the risks of electronic messaging and to make the case for the value of its services, Proofpoint, a security company, has assembled a list of what it considers are the "Top 10 Terrifying E-mail Blunders of 2009."

Keith Crosley, director of market development at Proofpoint, says the incidents his company has cited demonstrate the ongoing need for user training, for corporate e-mail policies, and for technology to enforce corporate policies. He says that only about a third of enterprises have deployed systems that can identify and block the unauthorized transmission of health or financial data.

The incidents that follow are, according to Proofpoint, in no particular order.

E-mail That Empties Bank Accounts

In September, the URLZone Trojan was reported to be spreading through e-mail and compromised Web sites, and emptying victims' bank accounts. It's even sophisticated enough to create forged balance reports to conceal its looting.

"No More Internet Banking For You!": That's what FBI director Robert Mueller's wife told him after the agency head clicked on a phishing message and nearly surrendered his personal information to a phishing Web site.

White House Spam

A White House effort to set the record straight about its healthcare plans in August led to the sending of unsolicited e-mail. The incident wasn't exactly a disaster. But it was it great public relations either.

Hotmail Accounts Blocked

Earlier this month, Microsoft blocked tens of thousands of Hotmail accounts that the company believed had been compromised as a result of a phishing scam. A security researcher at ScanSafe subsequently argued that exposed account credentials were gathered using a data theft trojan rather than a phishing attack.

Department Of Gaffes

Social media start-up RockYou reportedly managed to mess up its e-mail messaging three times in the past year. In January, it sent a mailing list message using the CC address field rather than BCC, exposing the e-mail addresses of everyone on the list. In November, it reportedly asked contractors for W-8/W-9 information in a message sent to a mailing list, which prompted replies containing personal information to the e-mail list rather than to the company's accounting department. And in September 2008, RockYou reportedly revealed over 200 e-mail addresses in a message it sent out.

Here's The Sensitive Data You Didn't Ask For

An employee of Rocky Mountain Bank in Wyoming inadvertently sent a message containing confidential customer information for 1,325 individual and business accounts to the wrong Gmail account. The Bank sued Google to force it to reveal information about the Gmail user who had accidentally received the information. Fortunately for all concerned, it appears that nothing was done with the exposed information.

Pay Day

Some customers of payroll processor PayChoice reportedly fell victim to a spear-phishing scheme in September when they received an e-mail message advising them to install a browser plug-in to maintain access to the company's online portal. The installed software was malware of course. PayChoice is still investigating the incident.

Tax Warning

Britain's tax authority, HM Revenue & Customs, issued a warning in January about "the most sophisticated and prolific phishing scam that we have encountered." The phishing messages asked for bank or credit card information, ostensibly so the government could provide a tax refund. Those who complied risked "their accounts being emptied and credit cards used to their limit."

Tax Warning Strikes Again

Last month, US-CERT warned about " malicious code circulating via spam e-mail messages related to the IRS." The messages contain links or attachments which attempt to install the dangerous Zeus trojan.

Congratulations! Oops, Never Mind

UC San Diego in April managed to send an acceptance e-mail to its entire pool of freshman applicants -- 46,000 students -- instead of just notifying the 18,000 students who had actually been admitted.

The point of recounting such incidents, says Crosley, is that "even today, users still need education about inbound e-mail security issues." He adds that despite the rise in social media, e-mail remains the number one threat vector. That partly, he says, because so many social media sites send out e-mail notifications. Spammers have realized this, he says, and have taken to sending out spoofed of social media notification messages.

Organizations that didn't make the list shouldn't give up: There are still two months left before the end of the year.

Courtesy : Thomas Claburn, http://www.informationweek.com
Oct. 26, 2009

REPORT

The Story of the First Internet Worm

Robert Tappan Morris was the first person convicted by a jury under the Computer Fraud and Abuse Act of 1986. The story of the worm he created and what happened to him after it was released is a tale of mistakes, infamy, and ultimately the financial and professional success of its author.

Morris was a 23-year-old graduate student at Cornell University in 1988 when he wrote the first Internet worm in 99 lines of C code. According to him, his worm was an experiment to gain access to as many machines as possible. Morris designed the worm to detect the existence of other copies of itself on infected machines and not reinfect those machines. Although he didn't appear to create the worm to be malicious by destroying files or damaging systems, according to comments in his source code he did design it to "break- in" to systems and "steal" passwords. Morris' worm worked by exploiting holes in the debug mode of the Unix sendmail program and in the finger daemon fingered.

On November 2, 1988, Morris released his worm from MIT to disguise the fact that the author was a Cornell student. Unfortunately for Morris, his worm had a bug and the part that was supposed to not reinfect machines that already harbored the worm didn't work. So systems quickly became infested with dozens of copies of the worm, each trying to break into accounts and replicate more worms. With no free processor cycles, infected systems soon crashed or became completely unresponsive. Rebooting infected systems didn't help. Killing the worm processes by hand was futile because they just kept multiplying. The only solution was to disconnect the systems from the Internet and try to figure out how the worm worked.

Programmers at the University of Berkeley, MIT, and Purdue were actively disassembling copies of the worm. Meanwhile, once he realized the worm was out of control, Morris enlisted the help of a friend at Harvard to stop the contagion. Within a day, the Berkeley and Purdue teams had developed and distributed procedures to slow down the spread of the worm. Also, Morris and his friend sent an anonymous message from Harvard describing how to kill the worm and patch vulnerable systems. Of course, few were able to get the information from either the universities or Morris because they were disconnected from the Internet.

Eventually the word got out and the systems came back online. Within a few days things were mostly back to normal. It is estimated that the Morris worm infected more than 6,000 computers, which in 1988 represented one-tenth of the Internet. Although none of the infected systems were actually damaged and no data was lost, the costs in system downtime and man-hours were estimated at $15 million. Victims of the worm included computers at NASA, some military facilities, several major universities, and medical research facilities.

Writing a buggy worm and releasing it was Morris' second mistake. His first mistake was talking about his worm for months before he released it. The police found him without much effort, especially after he was named in the New York Times as the author.

The fact that his worm had gained unauthorized access to computers of "federal interest" sealed his fate, and in 1990 he was convicted of violating the Computer Fraud and Abuse Act (Title 18). He was sentenced to three years probation, 400 hours of community service, a fine of $10,500, and the costs of his supervision. Ironically, Morris' father, Robert Morris Sr., was a computer security expert with the National Security Agency at the time.

As a direct result of the Morris worm, the CERT Coordination Center (CERT/CC) was established by the Defense Advanced Research Projects Agency (DARPA) in November 1988 to "prevent and respond to such incidents in the future". The CERT/CC is now a major reporting center for Internet security problems.

After the incident, Morris was suspended from Cornell for acting irresponsibly according to a university board of inquiry. Later, Morris would obtain his Ph.D. from Harvard University for his work on modeling and controlling networks with large numbers of competing connections.

In 1995, Morris co-founded a startup called Viaweb with fellow Harvard Ph.D. Paul Graham. Viaweb was a web-based program that allowed users to build stores online. Interestingly, they wrote their code primarily in Lisp, an artificial intelligence language most commonly used at universities. Viaweb was a success, and in 1998, ten years after Morris released his infamous worm, Viaweb was bought by Yahoo! for $49 million. You can still see the application Morris and Graham developed in action as Yahoo! Shopping.

Robert Morris is currently an assistant professor at MIT (apparently they forgave him for launching his worm from their network) and a member of their Laboratory of Computer Science in the Parallel and Distributed Operating Systems group. He teaches a course on

Operating System Engineering and has published numerous papers on advanced concepts in computer networking.

Courtesy : Marc Menninger; http://transmeet.com
October 27th, 2009

OPINION

Carelessness Is The Biggest Security Threat

As a security professional, the essential disciplines associated with operating in cyberspace, such as using the right security tools, installing the latest updates and encrypting data, come pretty naturally to me.

However, of late it has become obvious that it is not just the technical practices and the whizz-bang technologies that make us secure. It is more about a state of mind, and continued application of best - – or at least good –- security practices as we use our chosen technology.

Most mobile professionals need at some time to access a PC in a public place –- a PC which has been, and will continue to be, used by large numbers of unknown people. Recently, when I was using such a computer, after my session I carried out all the usual best practice tasks, and cleared down the browser history, cookies, and other digital footprints. However, when I looked at the previous history of use, it was possible to see the type of person, and in some cases the company, that had used this resource.

In this case, the previous users had clearly been working on business-related topics, and had downloaded files to the local disk. Under Windows, where such data will be written to by default, sure enough in the My Pictures and My Documents folders, information was located that would be considered pretty sensitive by many.

Without exception, the users of the system in question were all considered to be computer literate, and as such, would have been expected to be aware of the threats, and the necessary steps and countermeasures to protect their identities.

Security tools, applications, and other related technological methodologies employed to defend user systems go a long way to mitigating against cyber attacks. But only when they are combined with user best security practices will they fulfil their potential to secure the system. It is good to be careful, but possibly, much better to be paranoid.

Courtesy : John Walker; http://www.itnews.com.au

LESSONS

Lessons From The Estonian Cyber-Attacks

Terrorist groups and rogue states are moving their battle to the Internet.

The cyber attacks carried out against Estonia in the spring of 2007 served as a wake-up call about the potential damage that a large scale cyber attack can have on a highly wired country.

Estonia is a small nation that can't afford a large, complex government. Instead, we use IT to run our affairs. Ninety-eight percent of all bank transactions here are made electronically via the Internet. Estonians can vote online in local and national elections. More than 90% of taxes are filed electronically. And the Estonian government is paperless. All official documents are produced, adopted and published electronically.

Unfortunately, the more technologically advanced a country is, the more vulnerable it is to cyber attacks. But because the Estonian government kept the potential for cyber attackers in mind when we developed our e-services, we were able to repel the 2007 attacks without suffering any serious threat to our national security, while the private sector in Estonia suffered significant economic losses.

We also learned some important lessons. In response to the attacks, Estonia adopted a National Cyber Defense Strategy together with an Implementation Plan. One of the main principles is the importance of protecting the civilian critical information infrastructure. Since most of the infrastructure serving our basic daily needs is run by the private sector, it is the easiest target for attackers hoping to cause significant loss and affect our way of life.

The state has, therefore, partnered with the main IT actors in Estonia who are involved in both producing cyber defense policies and managing the cyber defense efforts. Our approach is aiming to bring together security analysts, technical experts, lawyers, diplomats and regulators in order to take into account all aspects of cyber security. This approach also helps us bridge the gap between cyber experts and policy makers.

Another important goal is increasing awareness and educating computer users. More than 60% of our population uses the Internet every day so we must start at the grass roots. We have launched targeted campaigns, used social marketing and implemented special programs. Priority target groups are home users, small- and mediumsized businesses and system administrators. At the same time, we are offering training and education to policy makers and business executives. We have increased IT education in our universities as well as included computer safety classes in primary and secondary school curricula.

There is a lot of work to be done internationally. We have had some success in raising awareness among global policy makers, but we still need to work on that in order to be able to collectively address cyber threats without waiting for an inevitable cyber catastrophe to jolt us into action. And we should not limit ourselves to the club of technically well-developed Western states. Our aim should also be to help some of the less developed countries where cyber attacks are not part of the criminal code and where there is no cyber attack response capability.

Internationally, we should focus on sharing best practices on protecting critical information infrastructure. We can all learn from each other. On the practical level, we should facilitate international incidence response and information sharing between our national agencies. We should also promote international enforcement mechanisms for adopting legal instruments to fight cyber crime. The best existing tool for that is the Council of Europe Convention on Cybercrime, which Canada has also signed.

I firmly believe that cyber threats should not be allowed to overshadow the positive aspects of using information technology and the Internet. However, as open and pioneering societies, we must act together to bolster our cyber defenses against those who are intent on challenging our modern way of life.

Courtesy : Vaino Reinart; http://network.nationalpost.com
October 22, 2009

EDUCATION

How to Protect Your Business Against Cyber Fraud

Like the flu virus, cyber-crime never vanishes, it merely evolves. According to the Internet Crime Complaint Center (IC3) — a partnership between the FBI and The National White Collar Crime Center — the U.S. lost $239 million to Internet fraud in 2008. This represents a 33 percent one-year rise, with the recession leading to an increase in fraud both on and off the Internet.

Most online fraud goes unreported — as little as one cyber-crime in seven, according to Justin Yurek, president of ID Watchdog, Inc. As the recession continues, we can expect the problem of cyber fraud to remain with us.

For certain scammers an economic downturn is manna from the gods. In a money crunch people can grow desperate and succumb to even well-publicized e-mail scams — they believe that the Nigerian gentleman who wants to split $8 million with them really exists, or that they *did* win the Spanish lottery, even though they never bought a ticket.

Even if you're not gullible or desperate, you still risk falling into an online scam. Among the latest cyber fraud mutations are "typo squatting," "fast flux" sites and social networking site scams — which contribute to the nine million annual *reported* cases of identity theft in the U.S., according to the Federal Trade Commission. Here's a look at the latest concerns.

Typo Squatting: Mind Your Ps & Qs

For years savvy eBay buyers have been purposely misspelling product names in eBay searches, counting on seller typos to keep potential buyers away and to score a bargain. Now a sinister offshoot of this concept — called typo squatting — targets both companies and individuals.

A typo squatter typically registers a domain name that is within a keystroke of a legitimate business (such as Compac for Compaq). The practice is prevalent: in 2008 McAfee Security found 80,000 domains that were typo squatting on the top 2,000 Web sites. Criminals do this to perpetrate click fraud; they cash in on paid ads being sponsored by legitimate Web sites. Worse yet are sites with misspelled bank names intended to lure bank customers to a bogus site set up to harvest the customer's account numbers and other sensitive information.

Fast Flux and the Botnets

The term “fast flux” refers to scammers who first create “botnets” by hacking into third-party computers via spy ware, virus-bearing e-mails, or browser activity such as compromised banner ads. Without the original owners knowledge, the criminals turn the infected computers into software-infested (ro)bots to do the bidding of the botnet “herder.”

Botnet herders continuously move the location of a Web site, e-mail source or DNS server from one zombie computer to the next, never staying in one place more than several minutes. This makes it extremely difficult to locate and shut down illegal activities and sites.

Social Networking Scams

According to Reuters, Facebook with its 200 million customers has become one of the most dangerous places on the Internet, replacing MySpace as the favorite social networking target for cyber-predators.

Scammers break into Facebook accounts posing as friends, and then direct them to Web sites that harvest personal information and spread viruses. Facebook has an advantage over e-mail systems in that once it detects a spam message they can delete it from all inboxes on the site. Still, Facebook issues this caveat among its terms of use: “We do our best to keep Facebook safe, but we can’t guarantee it.”

Romanian Ruse

Online auction fraud has become a cottage industry in tech-savvy Romania. In November 2006 the FBI declared most eBay fraud traceable to “Romania or Romanians.” More than a year later eBay sent detectives to Romania — to no avail as Internet fraud still ranks with human trafficking and drug smuggling as the main crimes in Romania. The fraudsters tend to work out of small towns away from the increased police scrutiny in Budapest.

The above is just one depiction of the many fraud perils lurking on the Internet. Here are a few precautions you can take to minimize your exposure:

- Never pay for anything online by Western Union, money gram, or bank wire transfers as the money is virtually unrecoverable with no recourse for the victim. eBay will not even allow sellers to put the words “western union” in an item description.

- While many legitimate buyers use free e-mail services that do not require a credit card to open the account, so do scammers. Be wary as the free accounts show a higher percentage of Internet fraud than do paid Internet server accounts or a company e-mail address.

- Laws in other countries may be quite different than those in the U.S. Refuse U.S. buyers or sellers who claim they're out of the country and request goods or money sent overseas.

- Always try to obtain a seller's physical address rather than just a phone number or post office box. Call the seller to make sure the phone number works.

- Google Maps' Street View can help accurately assess the risk of fulfilling a suspicious cc order. If the address looks like an abandoned building, call to determine if the cardholder actually made the purchase.

- To fight click fraud, businesses should monitor order velocity for multiple orders placed within the same day, hour or even minute, typically appearing from one device, address, credit card or user ID.

- "Friendly fraud" involves a buyer claiming he never purchased or received an item. A delivery confirmation form will establish that an item is delivered for PayPal transactions, but insurance or registration on international orders can be prohibitively expensive. Cast a wary eye on orders from known fraud hotbeds such as Eastern Europe, Russia and China, to name a few, but be aware that fraud gangs now operate out of most everywhere.

- Careful spelling is the first step in avoiding typo-squatting scams. Businesses victimized by typo-squatters can seek recourse with the Federal courts, which have increasingly ruled against the cyber squatters for domain name infringement.

By Frank Fortunato; http://www.ecommerce-guide.com
October 20, 2009

DEVELOPMENT

Human behavior: the key to future tech developments

Professor Michael Wesch is a cultural anthropologist at Kansas State University, over the past few years he's received a hundred-plus requests from people around the world eager to enroll in the school's graduate program for "digital ethnography," a subject that he's known for. One problem: no such program exists.

Wesch teaches anthropology to undergrads and heads up a working group on digital ethnography. The demand for his non-existent grad program is perhaps indicative, though, of a rising interest in the subject -- and in the skill.

As trained observers of how people in a society live, ethnographers can help companies figure out what people need and then work with designers to meet those needs with new (or more often tweaked) products and services. In a world in which ever more people are using technology products on a daily basis, such skills are increasingly in demand.

For ethnographers, anthropologists, and other social scientists, the upshot can be intriguing work around the globe.

Take Olga Morawczynski, a 20-something University of Edinburgh doctorate student who recently spent over a year in Kenya, where she studied the use of M-Pesa, a system for transferring money by cell phones.

Her research, which shows how M-Pesa is affecting family relationships and other aspects of daily life, was funded by a joint scholarship from the university and Microsoft Research.

The latter has also offered her an internship in Bangalore that will begin in a few months. If she enjoys the work and being in India, notes Morawczynski, "then an offer for something more permanent would be great." But otherwise she'll likely have plenty more opportunities from which to choose.

"Microsoft and many other companies realize that since it is, after all, people who use technology, it's critical for the company to understand how people adapt to technology," notes Kentaro Toyama, who leads the Technology for Emerging Markets research group at Microsoft Research India.

That helps explain why, as Wesch notes, digital ethnography is increasingly being integrated into other majors at universities.

From local to mass market

Toyama recalls a previous intern named Joyojeet Pal, who was then working on a doctorate in city and regional planning at the University of California at Berkeley but was also versed in ethnography.

During his internship Pal helped Toyama and others at Microsoft realize the significance of a practice commonly seen in rural India. He showed how students at overcrowded poor schools usually shared a PC, the result being that the oldest or pushiest often controlled the mouse while others lost interest.

Microsoft responded a few years later with a technology called MultiPoint, which allows for the use of multiple mice on one machine.

It's since steadily increased its investment in MultiPoint, notes Toyama, and today in India, Vietnam, Chile, and elsewhere the dominant use of it is as a way to quiz primary school students in multiple-choice questions.

The social component of interaction might actually be better than having students each with their own PC, notes Toyama. Even in the developed world, this might prove beneficial in classrooms.

Where MultiPoint will go in the future is anyone's guess, but something that started with ethnographic observations in rural India four or five years ago has already gone international.

Bright ideas

Something similar happened with Nokia's 1100 handset model, but on a much bigger scale. Its features make it ideal for the developing world, among them a long battery life, a rugged dust-proof construction, and a built-in flashlight. Once marketed as being "made for India," the handset quickly proved widely popular in the developing world and beyond.

It now ranks as one of the top all-time sellers in consumer electronics history. A feature like a built-in flashlight might hold little appeal to someone living in Tokyo or London. But in places where electricity is hard to access, it can be tremendously useful.

Ken Banks, an anthropologist and tech expert who developed the mass messaging program FrontlineSMS, points to a sign in Uganda he photographed advertising the Nokia 1200. Its main focus? The "ka-torchi," or flashlight.

In much of the developed world, notes Banks, the market for cell phones has been saturated. That means manufacturers must figure out what people in the developing world -- where growth will be strongest -- really need from a phone.

"It's not just a financial thing for them," says Banks. "People are only going to invest in a phone if they see real value in owning it." So observations made in India -- that people hold up their phones at home to see their keys and such at night -- helped Nokia create a global blockbuster.

The success of M-Pesa in Kenya has prompted similar mobile money offerings around the world -- there are now over 120 -- and could eventually have a significant impact on the enormous global remittances industry.

Little wonder, then, that Nokia and other tech companies employ anthropologists to travel around the world observing how people interact with technology.

For her part, Morawczynski is eager to escape academia and get more involved in the development and launch of mobile services.

"I have spent a significant amount of time studying the people, the technology, and the interactions between the two," she notes. "I have loads of ideas as a result."

Courtesy : By Steve Mollman; http://edition.cnn.com
October 22, 2009

ANALYSIS

In the Cybersecurity War, Collaboration Is Key

The evolving threat landscape means government must work more closely with commercial industry players, analysts say.

The landscape is volatile, the rules of the game are fluid, and the adversaries remain cloaked in anonymity. In this ambiguous war, the actual threat is unpredictable, sometimes indecipherable, and it's difficult to tell whether either side is gaining ground.

The location of this battlefield is not a desert road in Iraq or a terrorist redoubt in Afghanistan. It's what has emerged as the forefront of modern warfare: the cyber theater, where traditional rules of engagement don't always apply.

In cyberspace, enemy combatants can pry, spy, implant, extract and dismantle more quickly and more secretly than in the physical terrain of traditional warfare. In some cases, the threat is mundane, involving nothing more complex than defaced Web sites or denial-of-service attacks, such as those inflicted on the nation of Georgia in August 2008 by someone, perhaps the government, across the Russian border. But the potential for more damaging attacks is significant.

"The fact that physically destructive cyberattacks were not carried out against Georgian critical infrastructure industries suggests that someone on the Russian side was exercising considerable restraint," states a report recently published by the U.S. Cyber Consequences Unit (CCU). The independent organization assesses the likelihood and possible consequences of cyberattacks and cyber-assisted physical attacks.

One important result of the emerging cyber threat is a new way of thinking about national security and defense.

"Every day I wake up and say, 'Welcome to the 21st century. We fight in terms of nanoseconds,'" said Army Brig. Gen. LaWarren Patterson, deputy commanding general at the Network Enterprise Technology Command.

To meet the threat, the Department of Defense (DOD) recently created a high-level cyber command charged with spearheading the development of cyber warfare strategies, both defensive and offensive. However, DOD is not alone in this battle, and so creating the command is only the first step. Experts say the military cannot fight this battle without non-military allies. Many stakeholders exist outside the Pentagon.

Indeed, the Pentagon must ultimately change its culture, say independent analysts and military personnel alike. It must create a collaborative environment in which military, civilian government and, yes, even the commercial players can work together to determine and shape a battle plan against cyber threats.

Assessing the Threats

Although most experts agree that DOD faces evolving threats, not everyone agrees on how serious those threats are. Are would-be cyberattackers a scattered group of individuals looking for easy hits, or are they a well-organized, well-funded cadre that is biding time before striking hard?

Sami Saydjari, president and founder of the nonprofit Cyber Defense Agency, believes it's the latter.

Before a congressional committee two years ago, Saydjari painted a grim picture of the country after a cyber disaster: Think digital Hurricane Katrina on a national scale. He urged the government to provide for the defense of a U.S. cyber territory that is as legitimate as physical land.

He recently said the country's vulnerability to cyberattacks is worse and cites the continued integration of and dependence on information systems.

Military officials think in terms of network centricity, in which the goal is to ensure that warfighters always have access to the data they need. But that approach makes those systems a big target, Saydjari said.

"Net-centricity is great, but it creates huge levels of risk that [are] not well-calculated or well-thought-out by the government," he said.

The concerns are real, but the concept of a digital Hurricane Katrina and similar doomsday theories might be embellished, said Jim Lewis, director and senior fellow at the Technology and Public Policy Program at the Center for Strategic and International Studies. "It's really hard to derail a large country that has a lot of infrastructure," he said. "People tend to exaggerate. I love the Bruce Willis movies, but that's just not the truth."

Lewis said less dramatic but equally dangerous espionage and crime represent the true perils.

"How would you feel about China getting our designs for the F-35" stealth fighter jet? he asked. "What about those who rob U.S. banks over the Internet from Russia, with no chance of prosecution? [Hackers] that are breaking into our systems to steal military secrets or prepare for potential sabotage...these are the real threats."

Those threats are emerging as a priority after high-profile cyberattacks on government sites in Lithuania, Kazakhstan, Georgia and Estonia in recent years. The attacks were widely believed to have originated in Russia.

The attacks included graffiti on Web sites and total shutdowns of banks and media outlets. Although they were not catastrophic, they undermined national morale and raised an unnerving red flag to the rest of the world.

The CCU's report on the Georgia campaign details the preparation, planning, execution, targets, effects and key lessons learned.

Also, according to those researchers, Russia and other would-be cyberattackers are capable of worse damage than they have unleashed so far.

Scott Borg, who co-wrote the CCU report, said specific targets and methods were limited and carried out in a disciplined manner. Denial-of-service attacks, which overload servers and thereby incapacitate Web sites, were the primary weapons.

"It could have been disastrous," Borg said. "The capabilities of carrying out a devastating attack are there...but this was a more humane system of attack. We don't know who it was -- civilian organizers, possibly the Russian government. We do know there was a lot of exchange of information between the Russian military and the attackers on message boards."

In Georgia, the targets of the attacks were primarily the Web sites of media outlets and government entities. "The government now has to start worrying about a wider range of attackers, all kinds of entities that are informal, dispersed and communicating indirectly," Borg said. "As expertise is diffused and more people get these capabilities, the threat grows bigger over time."

The Need To Collaborate

The impending launch of the Cyber Command marks a turning point for the arming of official information networks. But the success of the command depends largely on cultural factors that do not show up in any organizational chart.

Gen. Carter Ham, commanding general of U.S. Army Europe and Seventh Army, called the command's establishment a historic moment. But he also advised DOD officials to ensure that their plans for the command heed the lessons of history and a more traditional era of warfare.

The key is information sharing. During the Cold War, the Soviet Union kept tight control of information and blocked people from easily communicating, while the United States let information flow more freely. The Berlin Wall fell because those firewalls collapsed under their own weight, he said.

"We are at a crossroads," Ham said. "Do we want to build and sustain firewalls between our organizations? Or can we look for an approach that constructs an infrastructure that mirrors the environment in which we find ourselves, which is much more collaborative."

Borg also sees danger in bringing a Cold War mindset to the cyber theater. The concept of deterrence based on mutually assured destruction does not work in cyberspace because we do not know who we are dealing with or how to reach them, he said.

"We have a lot to rethink," Borg said. "We're moving into a world where deterrence and retaliation are only used on occasion. We need alliances."

Others agree that a collaborative approach will be integral to the success of cyber defense, and DOD seems to be taking the idea seriously as it prepares to launch the Cyber Command.

"It's a matter of how we take several global commands under a single" contiguous U.S. command, said Maj. Timothy O'Bryant, a staff officer at the Office of the Army Chief Information Officer. "We need to synchronize our efforts and figure out the lanes [of communication] and eliminate redundancies."

"Joint and coalition warfare is not a natural state, especially in command and control," said Gen. James Mattis, NATO supreme allied commander for transformation and commander of U.S. Joint Forces. "But going without joint efforts is obsolete. No nation on its own can keep its people safe. We need to learn to work together."

Unlikely Bedfellows?

In the era of cyber warfare, any coalition must include industry.

Experts say DOD and the government as a whole still have not fully capitalized on their ability to influence the development of commercial cybersecurity solutions. Industry vendors have the expertise, but government has the money.

"Government may be a late adopter, but we should be exploiting its procurement power," said Melissa Hathaway, former acting senior director for cyberspace for the Obama administration, at the ArcSight conference in Washington last month.

"A public-private partnership is necessary to protect the national infrastructure," she said. "It's the cornerstone of cybersecurity, and cybersecurity is the cornerstone of the global economy."

Such a partnership reflects the blurred boundaries between the defense and civilian domains in cyberspace. Cybersecurity threats are common to everyone.

"We need a new relationship between the military and the critical infrastructure industries if we want to protect our critical infrastructure," Borg said. "We all operate in cyberspace now. It's not a separate region or command."

Although one analyst praised the efforts to make organizational changes at DOD, he also stressed the need to give industry more freedom. "The real issue is a lack of preparedness and defensive posture at DOD," said Richard Stiennon, chief research analyst at independent research firm IT-Harvest and author of the forthcoming book "Surviving Cyber War."

"Private industry figured this all out 10 years ago," he added. "We could have a rock-solid defense in place if we could quickly acquisition through industry. Industry doesn't need government help -- government should be partnering with industry."

Industry insiders say they are ready to meet the challenge and have the resources to attract the top-notch talent that agencies often cannot afford to hire.

Industry vendors also have the advantage of not working under the political and legal constraints faced by military and civilian agencies. They can develop technology as needed rather than in response to congressional or regulatory requirements or limitations.

"This is a complicated threat with a lot of money at stake," said Steve Hawkins, vice president of information security solutions at Raytheon. "Policies always take longer than technology. We have these large volumes of data, and contractors and private industry can act within milliseconds."

Many experts fear it will take an attack or some form of disaster to spur the government into faster action. Some say more money is needed, while others say a cultural shift is necessary even beyond the military. Too often, cybersecurity solutions have been developed in pieces, with each technology reacting to a specific need, they say. But such an approach means that industry is always one step behind.

"What will it take to drive innovation and spur a game-changing technology?" Hathaway asked. "Our speed, scale and solutions must outpace our opponents, and we need to move from point solutions to enterprise solutions."

Saydjari said it will take a significant change in how the United States invests in research efforts because the government must align its investment in cybersecurity with its reliance on technology.

"The U.S. needs an attitude change," he said. "We don't hesitate in the physical world to invest lots of money to protect ourselves, but in cyberspace, that burden is placed on industry and the commercial sector. Cyberspace is more valuable than we reflect in investment. Our leadership and the public don't understand the degree to which we rely on computers and the Internet."

Meanwhile, some observers worry that people will not realize the seriousness of the threat until it's too late.

"It's not a real theater until something bad happens and people wake up," said Col. Quill Ferguson, chief information management officer at U.S. Army North. Until then, "the back door is open."

Courtesy : Amber Corrin; http://redmondmag.com
26/10/2009

ANALYSIS

Six Years of Microsoft Monthly Patches, Many More to Come

It has been pointed out by a some commentators that this month marks the sixth year of Patch Tuesday, the day that Microsoft releases their Security Bulletins (the second Tuesday of every month). In that period there have been around 400 individual bulletins released, with more than half attracting Microsoft's highest security rating, of Critical. Over the years, the number of vulnerabilities fixed each year continues to grow, with no sign that things will be slowing any time soon.

Microsoft's move to a routine monthly release cycle was seen as a good thing by Information Technology specialists and system administrators. For the first time, it gave end users and administrators a known, routine point in time that security patches would be delivered and allowed people to more effectively develop patch testing and rollout plans and procedures. This was a vast improvement over the ad-hoc release cycle that Microsoft had been following until October 2003. Microsoft still releases adhoc patches, though they are now referred to as out-of-cycle patches and are most often seen when a serious threat is posed to systems, normally in response to a widely attacked vulnerability.

Perhaps the greatest overall benefit with the monthly release cycle is in reducing the exploitability window, the time between when a vulnerability is discovered and the first exploits arise and when the vulnerability is patched and the patch applied to vulnerable systems. Unfortunately, it doesn't work so well when the vulnerabilities have been publicly discussed and freely available well ahead of the patch release, but for those that haven't been disclosed in this manner, the approach severely limits their usefulness as widespread exploits. This benefit is offset by administrators who are struggling with the increasing numbers of patches and vulnerabilities addressed, delaying the eventual implementation of the patches on their systems. Some Information Security companies provide services to help administrators in this situation rapidly identify what the patches are going to do and what can be done in the interim to protect vulnerable systems before the patches can be applied.

Since Microsoft has moved to a monthly release cycle, other major software vendors have also moved away from ad-hoc patch release cycles, with the most notable cyclical patch release being Oracle's quarterly security patch releases. Some might argue that quarterly is too infrequent for patching, especially when many of the flaws being patched allow for complete remote control of various Oracle database and software platforms. Others would argue that quarterly is an appropriate release timeframe, as database and enterprise software administrators are not going to be likely to take their platforms offline monthly in order to apply patches, and even quarterly might be too frequent for that purpose (although there are some ways to mitigate that). Adobe has also moved to a quarterly patching cycle for its range of software products.

Not all vendors stick to such a reliable cycle. Linux distros are quite often the most fluid when it comes to frequency of patch release, there isn't always a defined timeframe when patches are released, only when they are needed. Other large software vendors, such as Apple, continue to release patches on an adhoc cycle.

There are commentators who consider the whole procedural, rigid patch release cycle a fundamentally broken system. That is certainly one way to look at it, however given the current state of deployed software and operating systems, it is one of the better solutions available. Not everyone is going to be able to manage their systems in an environment where patches are provided on an adhoc basis (Apple or the frequent adhoc approach of many Linux distributions). It's not a perfect system by any stretch of the imagination, but it is an improvement over what has come before. The addition of an Advance Notification release on the Thursday before patching gives just that little bit of extra awareness about what might be released and allow the testing and deployment of the patches to be shortened if needs be to address a higher threat.

Microsoft's big push for improved security over the last few years hasn't always been successful, and the newly released Windows 7 has already had Critical patches released for it, even before it hit the retail shelves.

In coming years Windows 2000, then Windows XP will stop being supported by Microsoft and the focus will then be increasingly on systems that were developed following Microsoft's massive shift towards secure development practices. The number of patches released each year is still expected to keep growing and the second Tuesday of every month is going to be a busy one for Information Security staff and system administrators for a very long time to come.

Courtesy : http://www.beskerming.com
22 October 2009