USA TODAY Education

Collegiate Case Study

Homeland Security

STAYSAFEONLINE.org
National Cyber Security Alliance

Cyber Security

Table of Contents

Overview

USA TODAY, The National Cyber Security Alliance and the Department of Homeland Security have partnered to bring you this case study on cyber security. The articles contained in this study discuss how cyber criminals are using increasingly sophisticated tools to attack legitimate Internet sites, search engines, online social networks, browsers, Federal government information systems and databases, bank accounts, and more recently, cell phones. In addition, they look into the very difficult questions of how to protect our Internet use, our data and our Federal government systems. Finally, they consider the potential loss of confidence in legitimate websites and our vulnerability as a nation. The critical inquiry and future implication questions at the end of the study, developed by subject matter expert, Dr. Karen McDowell, challenge you to come to a deeper understanding of the implications and impact of cyber security.

Hackers infiltrate search engines, social networks

By Jon Swartz
USA TODAY
Published April 9, 2008

SAN FRANCISCO – Consumers who use search engines, online social networks, browsers and the like face a gantlet of viruses and malicious software code, according to a cybersecurity report from Symantec, issued Tuesday as security experts gather here for the sprawling RSA Conference on tech security.

The repercussions go beyond the loss of personal data, security experts say. As more consumers are victimized, it could undercut their confidence in legitimate websites, says Billy Hoffman, manager of Hewlett-Packard Security Labs.

Previously, hackers were more likely to use e-mail with attachments to steer victims to virus-tainted websites. Now, they are implanting their links on legitimate websites.

In all, Symantec detected 711,912 threats last year, compared with 125,243 in 2006.

The malicious attacks – including recent exploits of users of Google, Facebook, search engine Mozilla and others -- are designed to steal user credentials or launch bigger attacks through the victim's social network of contacts, says Alfred Huger, vice president of engineering at Symantec.

"Rather than set a bear trap – a porn or get-rich-quick site loaded with malicious code – to entice users, hackers are actively hunting by injecting their bad stuff on trustworthy sites," Hoffman says.

Among the most frequent targets:

▸ **Search engines**. Cybercriminals are using a chink in Google's website to redirect unsuspecting PC users to sites containing malicious software. When someone does a Google search, they are redirected to what appears to be a legitimate website. The site, in fact, is tainted with malware.

Google says it is fixing the problem.

▸ **Browsers**. Mozilla, considered a safer alternative to Microsoft's Internet Explorer, is not immune. In the last six months of 2007, there were 88 vulnerabilities reported in Mozilla browsers, compared with 34 in the first half, says Symantec's report.

▸ **Social networks**. Hackers are intensifying their efforts to compromise social-networking sites using unsecure Web 2.0 technologies to load malware onto the PCs of consumers. Indeed, the number of compromised sites is "slowly outnumbering malicious ones created specifically by cybercriminals," the report says.

In one breach, a widget application on Facebook that promised to tell members who had a secret crush on them instead tried to trick them into downloading spyware. The scam was discovered by security firm Fortinet.

Meanwhile, the latest of three computer worms wriggled into Google's social-networking service, Orkut, in February.
Like a worm in December, this one spreads through comments that are typically posted on a user's profile, says Robert McArdle, an anti-virus specialist at Trend Micro.

▸ **Calendar**. Scammers are sending personalized e-mail as meeting invitations in Google Calendar. Since each e-mail has a different link for each recipient, it is harder for spam filters to detect anything wrong, says Jamz Yaneza, research project manager at Trend Micro.

The e-mail informs victims that they have inherited or are due a large amount of money from an unlikely source. The spammer asks the victim to pay a nominal fee to cover the transfer of the alleged inherited funds.

Google support has been notified by security firms, and it is blocking accounts used in the scam.

USA TODAY Education

Russian cybercrooks target high bank balances online

Coreflood Gang infects PCs at thousands of firms, large and small

By Byron Acohido
USA TODAY
Published July 16, 2008

Call them the Coreflood Gang. A ring of cyber bank robbers from southern Russia has quietly perfected a way to get a beachhead inside company networks.

Once inside, it infects every PC within reach with a custom-made data-stealing program called Coreflood. The goal: go rip off bank accounts online.

Over the past 16 months, the Coreflood Gang has infected swaths of PCs inside thousands of companies, hospitals, universities and government agencies, says SecureWorks researcher Joe Stewart, who has tracked and documented the spread of Coreflood over that period.

“It’s spying on you, capturing your log-ons, user names, passwords, bank balances, contents of your e-mail,” Stewart says. “It can capture anything.”

Coreflood is part of a class of malicious software, called banking trojans, designed primarily to help crooks break into bank accounts online. The number of banking trojans detected on the Internet this month topped 24,800, up from 3,342 at the start of 2006, security firm F-Secure says.

An infection usually starts when you visit a Web page implanted with a snippet of malicious coding. By simply navigating to the tainted page, your browser gets redirected, unseen, to a hub server that downloads the data-stealing program onto your hard drive.

Dozens of gangs specialize in banking trojans. They have it much easier than phishing scammers, who must lure victims into typing sensitive data on spoofed Web pages, says F-Secure researcher Patrik Runald.

“This is very organized crime,” Runald says. “These gangs are hiring people and making tons of money.”

The Coreflood Gang is among the most sophisticated. Stewart recently analyzed 500 gigabytes of stolen data stored on a rented hub server. He pinpointed 378,758 Coreflood infections inside thousands of organizations, small and large.

A workplace PC can get a new infection each time someone logs on. The most infections: a county school district with 31,425, a hotel chain with 14,093 and a health care company with 6,744. About 230 networks turned up with 50 or more Coreflood infections, while 35 networks each had 500 or more.

Gang members cull the stolen data for log-ons and account statements, especially bank accounts online with high balances. Next, they log into the accounts and make online cash transfers into “drop” accounts they control.

After having two hub servers shut down by the tech security community in May, the Coreflood Gang rented two new hubs and picked up where they left off. Today, they continue operations unimpeded, says Stewart.

Companies infiltrated by the Coreflood Gang need to rethink how they do network security. Employees surfing the Internet on work PCs ought to take pause. “If you don’t understand the threats that are out there, then you probably should not be banking online,” Stewart says.

Cell security seen as profit frontier

As mobile phones become more like PCs, hackers emerge

By Byron Acohido
USA TODAY
Published June 24, 2008

The race is on to get businesses and consumers to pay for security for their cellphone the way they do for their PCs.

Tech security companies see a lucrative emerging market for cellphone security products. Researcher IDC predicts businesses and consumers will spend $958 million by 2011, up from $214 million in 2006 spent mostly by corporations. Symantec, Kaspersky Lab, Trend Micro and others have stepped up consumer marketing of anti-virus subscriptions for mobile devices. Typical annual cost: about $30.

Security firms are also pitching more elaborate protections to corporate buyers. “Mobile devices represent the most porous piece of the IT infrastructure,” says Jeff Aliber, senior director of anti-virus supplier Kaspersky Lab.

Having saturated PCs and networks with data-stealing programs and financial scams, cybercriminals are following people as they e-mail, text message and surf the Internet from their mobile devices. So far, cellphone users have not faced any pervasive threats “because it’s still faster and easier for hackers to earn money in the PC domain,” says Jan Volzke, McAfee’s director of mobile security.

But recent developments suggest an opening for more wide-scale attacks. Verizon and AT&T this year outbid Google for a swath of airwaves. At Google’s urging, the Federal Communications Commission required the telecoms to provide open access to any programmer who develops Web applications designed to run on devices that use those airwaves.

That ruling is expected to spawn a wave of cool applications for mobile browsers at a time when cutting-edge iPhones, Windows Mobile smartphones, RIM BlackBerrys and Palm Treos are gaining in popularity. As use of cellphones that act more like PCs reach critical mass, so will phone hacking.

“It’s going to be like the early days of Web applications, people throwing code together as fast as they can, giving no thought to security,” says Aliber.

Tech analyst Jack Gold, of J. Gold Associates, predicts that in the next few months, profit-minded hackers will take aim at the hottest mobile device on the market. “You’re going to see a lot of malware being written for the iPhone,” says Gold.

The bad guys are certainly ready to pounce. One recent attack spread a program called InfoJack that infected Windows Mobile smartphones. InfoJack disabled the phone’s security settings and connected it to a server in China, giving the intruder a way to install malicious programs.

Cybercrooks are most likely to seek tech-gadget lovers who use cellphones to access corporate networks, or to shop and bank online. “The more sensitive data you store on that device, the more valuable it is to an attacker,” says Mark Kominsky, CEO of Bluefire Security Technologies, a mobile devices security company.

Bush pushes cybersecurity

President wants to raise funding to $7.3 billion

By Richard Wolf
USA TODAY
Published March 14, 2008

WASHINGTON - A sudden spike in the number of successful attacks against federal government information systems and databases has led President Bush to propose a multibillion-dollar response.

The number of incidents reported to the Department of Homeland Security rose by 152% last year, to nearly 13,000, according to a new government report. The security breaches, more than 4,000 of which remain under investigation, ranged from the work of random hackers to organized crime and foreign governments, says Tim Bennett, president of the Cyber Security Industry Alliance.

The increase and severity of data breaches prompted Bush to recommend a 10% increase in cybersecurity funding for the coming fiscal year, to $7.3 billion. That's a 73% increase since 2004.

"The president's put a lot of emphasis on this recently," says Robert Jamison, undersecretary for national protection and programs at the Department of Homeland Security. "We're concerned that the threats are real and growing....We're more vulnerable as a nation."

Members of Congress and experts in the private sector say the government's new initiative is overdue.

"There are more and more bad guys out there," says Sen. Tom Carper, D-Del., who chaired a Senate Homeland Security subcommittee hearing this week on government information security risks. In 31% of the infiltrations, he says, "agencies do not know who took the information or how much information was taken."

Rep. Jim Langevin, D-R.I., who chairs the House Homeland Security subcommittee with jurisdiction over the issue, says the Bush administration "has not paid nearly enough attention to cybersecurity" until this year. Now, he says, "they're at least trying to move in the right direction."

Homeland Security Secretary Michael Chertoff has made improving cybersecurity one of his top four goals for 2008. "It's the one area in which I feel we've been behind where I would like to be," he told reporters here last week.

A focus on China

The Defense Department and federal intelligence agencies are on the warpath against increasing numbers of cyberattacks.

To combat the threat, the government is rolling out a system this year that reduces external connections to the Internet, detects intrusions in and out of federal networks and enables faster patching of holes.

Even so, the Government Accountability Office reported this week that 20 of 24 major federal agencies are deficient in protecting against cyberattacks. Gregory Wilshusen, the GAO's director of information security issues, cited past instances in which the State Department network was breached by a malicious code inside an e-mail; a Transportation Security Administration hard drive with employment records was found missing; and an idled nuclear power plant's private computer network was infected by a virus, disabling a safety monitoring system.

Deputy Defense Secretary Gordon England noted last week that Estonia was victimized by a series of attacks for three weeks in 2007 that forced its largest bank to shut down its online banking network. "Cyberwarfare is already here," England told a Veterans of Foreign Wars conference.

Much of the attention focuses on China, which could be infiltrating U.S. government information technology systems despite denials by Beijing. In its annual report to Congress last week on China's military power, the Pentagon said several cyberspace attacks around the world in 2007 were sourced back to China.

Director of National Intelligence Mike McConnell told the Senate Intelligence Committee last month that several nations, including China and Russia, “have the technical capabilities to target and disrupt elements of the U.S. information infrastructure and for intelligence collection.” He recommended “proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage.”

“The Chinese have a lot of resources, and they’re willing to spend it to break in,” says James Lewis, a cybersecurity expert at the Center for Strategic and International Studies.

Alan Paller, director of research at the SANS Institute, which specializes in information security research and training, says preventing cyberattacks is as important as preventing physical attacks. “Owning our computers is a powerful weapon in a war,” Paller says. “We need to get them out.”

Practicing for attacks

To test security against about 100 possible attacks, the Department of Homeland Security today is completing a week-long series of simulations called “Cyber Storm II.” The event presumed a coordinated cyberattack on information technology, communication, chemical and transportation systems. Participants from five countries, nine states, 18 federal agencies and more than 40 private companies participated.

“They remarked somewhat sheepishly how much of a stretch this has been for them,” Greg Garcia, assistant secretary for cybersecurity at the Homeland Security Department, said Thursday during a tour of the event at Secret Service headquarters here.

Karen Evans, administrator for electronic government and information technology at the Office of Management and Budget, says part of the 152% increase in security breaches in 2007 was due to more accurate reporting, but she acknowledges that much of it represents a real rise.

Industry officials want a greater government role in preventing cyberattacks. Bennett says, “With global attacks on data networks increasing at an alarming rate, in a more organized and sophisticated manner, and often originating from state-sponsored sources, there is precious little time to lose.”

Critical Inquiry Questions:

1. In the article “Hackers infiltrate search engines, social networks,” SecureWorks researcher Joe Stewart states, “If you don’t understand the threats that are out there, then you probably should not be banking online.” Do you agree or disagree with his statement? Can the average person be expected to understand these threats? If not, should banks require security awareness testing of their account holders?

2. Why are cyber criminals changing their tactics from sending fraudulent email (phishing) to injecting their malware directly onto legitimate sites? What role do ISPs, website owners, website hosting services and government play in preventing the spread of malware?

3. As a nation we have often debated the role of the Federal government in private industry. Now, however, some private “industry officials want a greater government role in preventing cyber attacks,” and Tim Bennett, President of the Cyber Security Industry Alliance, even states “…there is precious little time to lose.” What accounts for this dramatic change? What kind of incentives might improve government and private sector actions? What specifically should the government be able to do? When it comes to cyber security, should the federal government play a different role than state and local governments?

4. What are the advantages for cyber criminals in attacking social networking sites?

5. What are some of the challenges in deciphering cyber attackers and responding to cyber incidents? What are the differences in the risks associated with cyber attacks perpetuated by a nation state, a terrorist group, a non-state sector or a private business?

6. Google recently urged the Federal Communications Commission to provide open access to any programmer who develops Web applications designed to run on smart phones, iPhones, BlackBerrys and Palm Treos, among others that use the airwaves. What are the implications of this? Why do you think Google wanted this? Is there a special advantage for Google?

Future Implication Questions:

1. The increase and severity of cyber attacks is dramatic and alarming. As an example, the number, according to the Department of Homeland Security, rose by 152% in 2007. What should we expect of our government, and what should we do as individuals to try and reduce the number and severity of attacks?

2. What are the implications for software developers and programmers, especially given Aliber’s comment that cell phone development “…is going to be like the early days of Web applications, people throwing code together as fast as they can, giving no thought to security”? There is a movement to require developers and programmers to earn security certification, but there is a lot of resistance, too. Don’t developers and programmers have a responsibility to create very secure products? Is it possible to legislate more and better security in the manufacturing of software products themselves? What do you think about creating legislation that requires software manufacturers to meet rigorous security standards? Would such legislation make any difference in the frequency and kinds of threats?

3. The logical objective of these cyber attacks, if they are not greatly reduced or prevented, is to render the US helpless against them. According to Alan Paller, Director of Research at the SANS Institute, “preventing cyber attacks is as important as preventing physical attacks.” Should we launch an intense national initiative engaging all our citizens in awareness and activities to prevent cyber attacks? What if we do, but more importantly, what if we don’t do anything?

4. As smart phones become more like miniature PCs, they will hold more data and have greater access. They may even supplant PCs. Cyber attacks are expected to become more frequent and more severe, and theft may become a common problem. What kinds of techniques could we develop to reduce electronic attacks and to prevent theft of these small computers?

5. What part does trust play in the Internet? How do you determine whether a website is trustworthy (i.e. what is your own calculation)? Do you trust social networking sites? What about youTube and MySpace? Do you trust that using these sites will not harm your computer and/or steal your identity? What if no one trusted the Internet any more? What would happen? Is there a relationship in terms of trust between the stock market and social networking sites?

6. At what age should we begin educating kids about cyber security? What specifically do they need to know? What outcome do we want to achieve through education? Should we begin teaching Internet safety at the elementary school level, if we want a safe and well-educated Internet population? Are there other ways of teaching people about these threats, and what they can do to protect themselves?

7. What recommendations would you offer the president about cyber security?

Links to Additional Research:

Organizations

- **United States Computer Emergency Readiness Team (US-CERT)**: www.us-cert.gov
- **The National Cyber Security Alliance**: www.staysafeonline.org
- **Federal Trade Commission**: www.onguardonline.gov
- **Multi-State Information Sharing and Analysis Center**: www.msisac.org
- **SANS Institute, Computer Security Newsletters and Digests**: www.sans.org/newsletters

Reports

- **Multi-State Information Sharing and Analysis Center**: “Emerging Cyber Threats Report for 2008,” www.gtisc.gatech.edu/pdf/GTISC%20Cyber%20Threats%20Report.pdf
- **Symantec**: “The Symantec Internet Security Threat Report,” www.symantec.com/business/theme_jsp?themeid=threatreport
- **TippingPoint.com**: “SANS Top 20 Internet Security Risks of 2007 Point to Two Major Transformations in Attacker Targets,” www.tippingpoint.com/pdf/press/2007/SANSTop20-2007_112707.pdf
- **Pew Internet and American Life Project, Trust and Privacy Online**: “Why Americans Want to Rewrite the Rules,” www.pewinternet.org/report_display.asp?r=19

News Stories

- **SD Times**: “Expert backs new security certification for coders,” www.sdtimes.com/EXPERT_BACKS_NEW_SECURITY_CERTIFICATION_FOR_CODERS/About_SECURITY_and_SOFTWAREDEVELOPMENT_and_ISC2/32912
- **SD Times**: “Seven Steps To Reducing Software Security Risks,” www.sdtimes.com/SearchResult/29108
- **Times Online**: “China’s cyber army is preparing to march on America, says Pentagon,” http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece
- **TechNewsWorld**: “The Winds of Cyber War,” www.technewsworld.com/story/64494.html?wlc=1224261178
- **InformationWeek**: “CIA Admits Cyberattacks Blacked Out Cities,” www.informationweek.com/news/internet/showArticle.jhtml?articleID=205901631
- **ConsumerReports.org**: “RSA 2008: Only you can prevent cyber-attacks,” blogs.consumerreports.org/electronics/2008/04/only-you-can-pr.html
- **Silicon.com**: “Criminal IT: Should you trust the internet?” software.silicon.com/security/0,39024655,39127375,00.htm

About the Expert: Karen McDowell, Ph.D. University of Virginia

While Karen McDowell was earning a Ph.D. from the University of Virginia (1996), she became fascinated by the burgeoning field of information technology and the Internet. She began studying hardware, software, and network problems. She worked on early Windows NT systems and earned Microsoft Certified Professional Certification in NT Server and Workstation and Exchange 5.5. Karen then became proficient in troubleshooting all kinds of Windows and third-party software problems. In due course, she noticed the rapidly growing threats to computers and networks and began to study them. She also worked on learning how to keep computers safe and how to fix infected computers. In 2003, Karen began writing about these problems to reach a broader audience in the interest of helping people learn how to keep their data, identity, and computers safe. She has presented at numerous conferences, including an international conference held in Canada in 2006, and has published articles about IT security.

In 2006 she earned a GIAC Security Essentials Certification from the SANS Institute. She is now pursuing CISSP Certification, while she works for the IT Security and Policy Office at the University of Virginia in Charlottesville, VA.