Lesson 2

Cracking the code

How cybercriminals unleash Internet worms to infiltrate networking sites

By Byron Acohido
USA TODAY
April 23, 2009

It's become the new front in cybercrime: scams and identity-theft programs that attack e-mail accounts and users of social-networking sites such as Facebook and MySpace.

To carry out many of these automated attacks, cybercriminals first must overcome "captchas," the distorted letters and characters that users of an e-mail or social-networking account are required to type to complete certain online forms. For years, captchas have helped to stop or bog down automated programs aimed at creating, among other things, e-mail accounts that promote scams such as fake computer virus protection and bogus accounts on social websites that can be used to collect personal information on legitimate users.

Now, security specialists say, a growing number of captcha-breaking groups are using real people to type in captcha responses for cybergangs around the world. This is allowing the gangs to create fake e-mail and social-network accounts by the tens of thousands — and use them as the starting point for a variety of cyberscams spread by e-mail and instant messages.

MySpace and Facebook say that, so far, they have kept such attacks largely in check. But security researchers say that as long as captchas are a key security feature on networking websites, cyberattacks on such sites are likely to intensify.

"We shouldn't have any illusions about captchas," says Sergei Shevchenko, a virus hunter at Internet security firm PC Tools. "If the professionals want to break in, they'll do it."

For social-networking sites that have exploded in popularity during the past two years — Facebook now claims more than 200 million members — the stakes are enormous.

The social networks, scrambling to build audiences and ad revenue, want to avoid e-mail's fate: Today, 90% of all e-mail traffic is spam, and companies across the nation pour vast resources into keeping legitimate e-mail viable by filtering away spam.

Meanwhile, cybergangs recognize the opportunity to get fresh mileage from tried-and-true scams. They are repurposing ruses perfected in e-mail spamming to try to fool members of social networks into accepting — or even spreading — ads for fake products, data-stealing programs and other harmful computer bugs.

"Social-networking sites are a viral marketer's dream," says Paul Wood, analyst at Message Labs-Symantec, an Internet security firm. "The potential to tap into a huge community of like-minded individuals is enormous."

A penny at a time

Captchas first appeared in 2001. They are based on the idea that humans — and not automated programs used by cybercriminals — can distinguish a word or group of characters shown as a warped graphical representation and then type them on an online form to gain access to a protected Web page.

Social networks typically require captchas for creating accounts and sending private messages that include Web links.

Captchas represent the first line of deterrence against automated programs, called bots, which typically are assembled in large groups known as botnets.

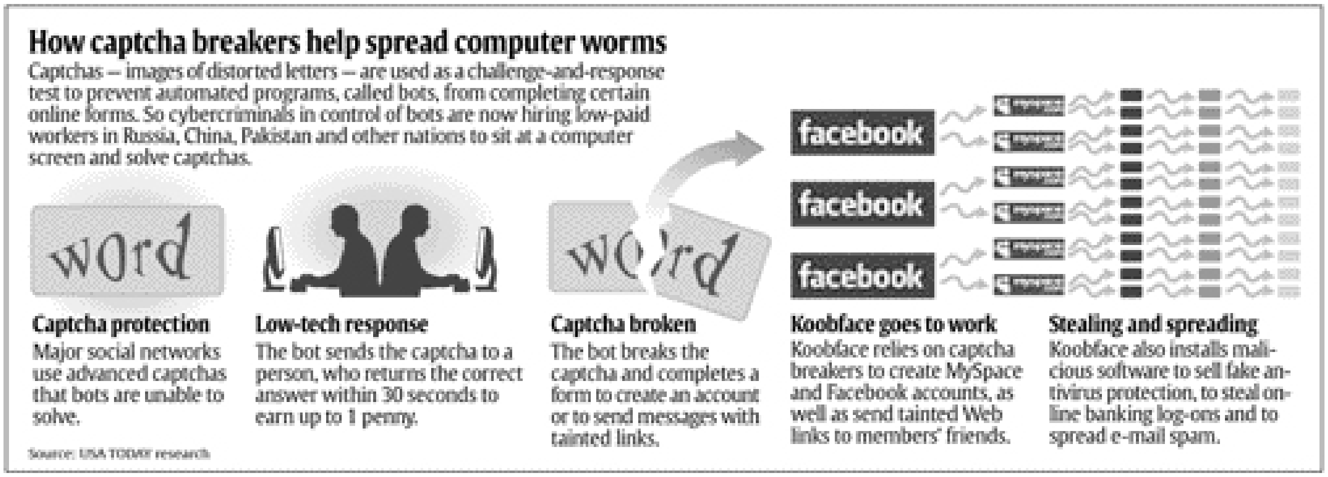
Bots are the little engines that propel online criminal activities. Bots, for example, are efficient at creating bogus Gmail, Hotmail, Yahoo and AOL messaging accounts, as well as memberships on MySpace, Facebook, Twitter and YouTube. These bogus accounts can serve as launching points to spread spam, steal data, pitch fake antivirus subscriptions — and scoop more PCs into the botnet.

Captcha designers have made their work increasingly distorted and camouflaged to defeat improved character-recognition programs carried by bots. Today, most major websites use advanced captchas that bots can't resolve.

Enter captcha-breaking groups, bearing a new weapon that combines cheap labor with the Internet's capacity for quick, anonymous global transactions.

Spawned in the online underground, these groups are difficult to pin down, security specialists say. But based on recruitment ads, discussions on hackers' forums and the rising volume of bogus accounts being created, there appear to be dozens of captcha-breaking gangs employing hundreds of people in several countries, tech security researchers say.

Human captcha-solvers work piecemeal. They have shown up in Internet cafes or in sweatshops filled with Internet-connected PCs in China, India, Russia, Brazil, Argentina and Nigeria, working long shifts deciphering streams of characters forwarded by an unseen coordinator, researchers say.



How captcha breakers help spread computer worms

Captchas — images of distorted letters — are used as a challenge-and-response test to prevent automated programs, called bots, from completing certain online forms. So cybercriminals in control of bots are now hiring low-paid workers in Russia, China, Pakistan and other nations to sit at a computer screen and solve captchas.

Captcha protection Major social networks use advanced captchas that bots are unable to solve.

Low-tech response The bot sends the captcha to a person, who returns the correct answer within 30 seconds to earn up to 1 penny.

Captcha broken The bot breaks the captcha and completes a form to create an account or to send messages with tainted links.

Koobface goes to work Koobface relies on captcha breakers to create MySpace and Facebook accounts, as well as send tainted Web links to members' friends.

Stealing and spreading Koobface also installs malicious software to sell fake antivirus protection, to steal online banking log-ons and to spread e-mail spam.

Source: USA TODAY research

By Alejandro Gonzalez, USA TODAY

"At least one major operation is being run out of Pakistan," says Adam O'Donnell, director of emerging technologies at messaging security firm Cloudmark. "I suspect similar operations are being run anywhere that has bandwidth and cheap labor."

Cybergangs typically pay captcha-solvers a half-cent to a penny for every captcha they complete, according to online recruitment ads on hackers' forums that reflect how captcha-solving has become a growing underground business.

"You can pay a business for captcha-breaking services, and they'll make it happen," says Patrick Peterson, chief security researcher at Cisco. "You can have the captchas solved in the Internet cloud as you create each new account."

Networks fight back

Without the emergence of for-hire captcha-breakers, a particularly destructive worm that plagued the Internet in May — known as Koobface — would not have been possible. A worm is a program designed to self-replicate across the Internet.

Koobface — a cockeyed spelling of Facebook — targeted MySpace and Facebook. It initiated messages that duped victims into clicking on a Web link to view a funny YouTube video.

Clicking on the link led to instructions to download a Flash Player update required to view the video. Clicking on the video player update downloaded a copy of the worm, which instantly searched out the victim's friend lists on Facebook and MySpace and sent copies of itself to everyone on the list. So, subsequent victims received a message that actually arrived from the account of a trusted friend.

"This certainly represented the sullying of what began as a clear, worry-free place to interact with peers," says Joel Smith, chief technology officer at messaging security firm AppRiver.

MySpace and Facebook scrambled to warn users about Koobface, block suspicious Web links and take other defensive measures.

"We've been working for months to limit the distribution of Koobface over Facebook," says Facebook spokesman Barry Schnitt. "We take the security of our users very seriously and have invested significant resources in protecting them."

MySpace Chief Security Officer Hemanshu Nigam says improved security has reduced spam that reaches the network's members by 73% since Koobface first appeared. MySpace beefed up its message-filtering systems and developed a tool to warn members about suspicious links.

"We have put in a lot of features to cleanse things like Koobface," Nigam says.

Researchers don't know who created or controls Koobface, which continues to morph on the Web. In mid-March, Microsoft added Koobface detection to its Malicious Software Removal Tool (MSRT), which automatically checks PCs running non-pirated copies of Windows Vista, Windows XP, Windows 2000 and Windows Server 2003 for more than 100 viruses.

In the ensuing two weeks, MSRT removed Koobface nearly 200,000 times from 133,677 PCs.

"Koobface is constantly changing to avoid detection, with over 20,000 variations to date," Jeff Williams, Microsoft Malware Protection Center program manager, said in a blog post. "We're also working to detect new variants of the Koobface virus as they're discovered, so we can provide ongoing protection from this threat."

A 'shark' in 'warm waters'

Early versions of Koobface focused on spreading the worm far and wide.

Besides copying itself to everyone on victims' friend lists, the worm stole cookies — small pieces of text, stored in the users' Web browsers. But it stole only those cookies that contained user IDs and passwords for members of social-networking sites Friendster, BlackPlanet, Bebo, Hi5, Live Journal and MyYearbook. That gave the attackers starting points to launch the worm in the more popular social networks, says Kurt Baumgartner, chief threat officer at PC Tools.

As Koobface steadily added capabilities, Baumgartner observed it begin to incorporate malicious programs widely used by other criminal groups:

- Adware for a $50 fake antivirus program, called Security Protect 2009, that's now also being spread by the Conficker worm.

- Coding that turns an infected PC into a spam-spreading bot, the same coding used by the huge Waledac e-mail virus.

- A program called ZeuS that steals user IDs and passwords from a customizable list of banks.

"Koobface is like a shark that has found itself in warm waters with plenty of prey," Baumgartner says.

Monitoring Koobface with Baumgartner has been colleague Shevchenko, a Russian expatriate. Shevchenko made some startling discoveries about captcha breakers. Monitoring Russian-language forums, he found an ad headlined "Kolotibablo," which means "make easy money."

The job description as translated by Shevchenko: "Your new job is printing English text that you see in the pictures. (Images of captchas were shown.) All you need is to know English alphabet and know where the keys are located on a keyboard. For every correctly entered word you will receive up to 1 cent, depending on the level that you have achieved. Your only limit is your typing speed. Every minute, you'll be able to correctly type the text from 10 pictures on average. Thus, with an average price of 0.5 cent per one correctly typed text from a picture, your salary will be 3 US dollars per hour."

Shevchenko conducted an experiment. First, he reverse-engineered Koobface to discover where the worm sent captchas to be resolved. Next, he generated and saved 100 captchas issued by Facebook, MySpace, Gmail, Yahoo Mail and Hotmail. And finally he built a tool that could submit the 100 captchas to Koobface's resolvers.

Shevchenko's findings, widely cited in tech security circles, astounded many of his peers, a band of about 200 or so elite virus hunters around the world. Two-thirds of the captchas came back resolved in less than 30 seconds. The unresolved words or characters were more highly distorted and thus more difficult to solve.

Some rejects came back with letters typed from one side of the keyboard, such as "asdfg," indicating a human resolver was typing gibberish to quickly get to an easier puzzle. Shevchenko resubmitted the rejects, and eventually all 100 sample captchas were successfully resolved.

"I was just amazed with the effectiveness of the system," Shevchenko says.

As a parting shot, Shevchenko submitted a captcha of his own composition to let the captcha-solvers know someone was on to them: "Don't be a monkey respect yourself."

The message came back solved in 23 seconds.

Introduction

Websites have had so many cybercriminal-created computer programs make multiple, bogus accounts that companies are constantly enhancing their cybersecurity. One of these security features is a "captcha," which was designed to make sure an actual human was creating the account and not a software program. However, cybercriminals are finding inexpensive ways to get around some of these security features quickly, so they can still exploit these websites. Read the article and then answer the following questions.

Discussion

1. What is a "captcha"?
2. Why do some websites use these?
3. How are cybercrime rings getting around captchas?
4. What information are cybercriminals able to access with the combination of technology and cheap labor?
5. Why do cybercriminals want to gain that information? What is their endgame?
6. Do you have a MySpace or Facebook account? What kind of danger might you be in from these cybercriminals?

Activity

1. With a partner, create a short, 8-question survey designed to discover the dangerous online behaviors of your peers and how cybercriminals may exploit them. Consider selecting some of the following questions:
    - On what websites have you created personal accounts?
    - Do you use the same password for more than one of these accounts?
    - Have you ever had any of your online accounts hacked? If so, which ones?
    - How did you resolve the situation?
    - What damage was done?
    - What did you do to repair the damage?
    - Was there damage done you couldn't fix? If so, what?
    - Have you ever had a computer virus?
    - How did your computer get the virus?
    - How did you know it was infected?
    - What damage did the virus do? How much did that cost in time and money?
    - Do you think your computer is at-risk right now for being hacked or getting a virus?
2. Give the survey to at least 10 students.
3. Analyze the results. For example: What percent of students engage in potentially dangerous online behavior that cybercriminals can exploit? What percent of peers have had their computers hacked? What kind of damage have viruses caused your peers?
4. Share your most surprising or compelling survey result with your classmates.

Lesson 2

TEACHER'S GUIDE

Overview:

In this lesson, students will:

- Read the article and answer discussion questions.
- Self-evaluate their own risk for getting online accounts hacked or getting a virus on their computer.
- Identify tips on how to avoid these online problems in the future.

Grade level:

6-12

Subject areas:

career and technical education, language arts, social studies, advisory classes

Time requirements:

Step 1: Read the article (20 minutes).
Step 2: Discuss the article using the questions provided (5 minutes).
Step 3: Draft a survey, survey at least 10 students and evaluate the results (40 minutes in class; 40 minutes out of class).
Step 4: Share some of the results and discuss tips for staying safe (10 minutes).
Total: 75 minutes in class; 40 minutes out of class

Notes:

1. You may want to preteach the following concepts and vocabulary words: viable, ruses, viral marketing, piecemeal, sweatshops, self-replicate, duped, sullying, ensuing, variants, expatriate and reverse-engineering.
2. After students have completed their surveys, ask some to share their most interesting or compelling results.
3. Lead a general discussion by asking the following questions:
    a. What accounts were hacked most often?
    b. How many students use the same password for more than one account? Does this put you more at-risk for getting hacked?
    c. What are some tips you can offer to help others avoid these same problems?

Here are tips offered by OnGuardOnline.gov:

- Protect your personal information. It's valuable.
- Know who you're dealing with.
- Use security software that updates automatically.
- Keep your operating system and Web browser up-to-date and learn about their security features.
- Keep your passwords safe, secure and strong.
- Use passwords that have at least eight characters and include numbers or symbols. The longer the password,

the tougher it is to crack. A 12-character password is stronger than one with eight characters.

- Avoid common words: Some hackers use programs that can try every word in the dictionary.
- Don't use your personal information, your login name or adjacent keys on the keyboard as passwords
- Change your passwords regularly (at a minimum, every 90 days).
- Don't use the same password for each online account you access.
- Back up important files.
- Learn what to do in an e-mergency

Additional information can be found at www.onguardonline.gov/topics/computer-security.aspx.

Links:

- National Cyber Security Alliance: www.staysafeonline.org
- Department of Homeland Security: www.DHS.gov/cyber
- i-SAFE: www.isafe.org
- Wired Safety Organization: www.wiredsafety.org
- Federal Trade Commission: www.onguardonline.gov
- Multi-State Information Sharing and Analysis Center: www.msisac.org/awareness
- ConnectSafely: www.connectsafely.org/safety-tips-and-advice.html
- iKeepSafe: http://tools.ikeepsafe.org/older-students