Minerals Management Service

Information Security Newsletter

FRONTLINE

SUMMER 2007

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

INSIDE

It's the Thought that Counts

These days there are a lot of greeting cards flying across the Internet. It's easy to see why: sending an electronic "thinking of you" costs less than sending a traditional card, can be sent for birthday delivery on the day of the recipient's birthday and still arrive on time, and can include animation and music (try that with a paper card).

But all's not well in the world of e-greetings. Cybercriminals have jumped on the "thinking of you" bandwagon and are sending out fake notices telling you a card has just arrived for you. You're supposed to click on a link to see the greeting. In some cases, the mailings are exact duplicates of those sent from real greeting sites such as BlueMountain.com. But if you click on the link in one of these messages, you get more than an affectionate note.

NOTHING NEW?

The truth is, we've seen lots of variations on this basic theme, but it is worth looking at again for two reasons:

- ❏ Some of these messages really are more cleverly designed than ever. The fakes are getting genuinely hard to detect. It's more important than ever to think long and hard before clicking a link.
- ❏ The result of clicking on one of these hacker messages is getting increasingly painful. It's important that you know what's out

[Continued on page 2]

What's a Bot?

Believe it or not, it may be that there are fewer hackers now than there were a few years ago. The current crop of hackers, though, works a lot more efficiently, in part because they use coordinated groups of attack computers, nicknamed "bots" (because the machines carry out their assigned tasks like robots). A group of such computers, working under a single hacker organization's control, is called a "botnet." These botnets have become a huge force in current cybercrime.

Botnets are the compromised machines of ordinary business and home users; and there are a staggering quantity of them. The FBI recently launched a special operation to disrupt bot operators–somewhat amusingly called "Operation Bot Roast"–and identified over a million bot computers connected to the Internet. As a result of its investigations, the Bureau has brought charges against several individuals.

For example, Robert Alan Soloway of Seattle is accused of using botnets to send tens of millions of spam messages touting his Web site. James C. Brewer of Arlington, Texas, is accused of infecting tens of thousands of computers worldwide, including some at Chicago-area hospitals. And Jason Michael Downey of Kentucky is charged with using botnets to attack and disable other systems.

[Continued on page 3]

© 2007 by COMPUTER SECURITY INSTITUTE

there—it'll provide some serious motivation to keep you out of harm's way.

A message made the rounds the other day announcing that a new greeting card was waiting for the recipient at BlueMountain.com. Granted, the overwhelming majority of greeting cards on the authentic Blue Mountain site are perfectly safe. But here's the trick: how can you tell if the link you're about to click is going to take you to the authentic site? The email will look exactly like an authentic Blue Mountain email message, complete with colors and wording; even the link will appear exactly like the authentic. If you were to click on the link, you'd be taken to a hacker Web site that immediately begins downloading software to your system.

WHAT KIND OF SOFTWARE?

You don't want the software that you get from clicking on this link. For the first week and a half that this particular attack circulated, the software that it downloaded went undetected by at least one of the major anti-virus packages. So you could be infected without knowing it.

The software downloaded by the malicious site is definitely bad news. It's what computer security experts call a "keystroke logger" which quietly watches you type, and forwards anything resembling a password entry from your computer, over the Internet, to a hacker waiting on the other end. This kind of malicious software is becoming increasingly common, along with software that secretly uses your machine to send out spam for con artists. With this kind of infection, your computer becomes a "bot," meaning that it's used by someone else without your permission (see page 1, "What's a Bot?").

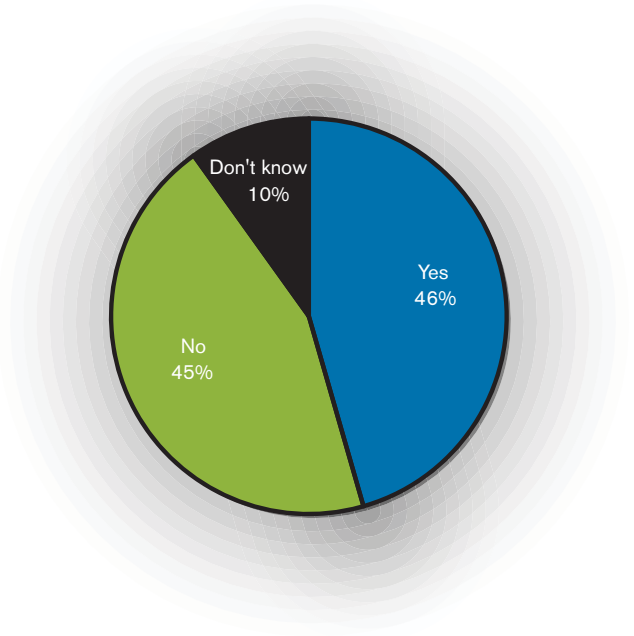
In general, there are a staggering number of Web sites out there that will automatically and secretly download software to your system. A study done by researchers at Google looked at 4.5 million Web addresses and found that 450,000 (one in ten!) attempted to download software without permission.

Many of the sites contain the sort of material that you shouldn't be visiting using your organization's computers or networks, so one good way to keep keystroke loggers off your system is to stay in "safe network neighborhoods." It is possible, though, to be tricked, perhaps by a phishing message announcing that a greeting card has arrived for you.

Let's say it's your birthday and you get a message about a greeting card. You click a link to retrieve the card, but then you notice your browser is spending a lot of time loading what appears to be a blank or irrelevant Web page. It's possible that a new attack won't yet be detected by your organization's anti-virus software, so there may not be any warning signals. This is the moment to ask for help! Even if an attack is so new that anti-virus systems don't yet detect it, a look at the list of running software on your system will uncover warning signs.

And a word to the wise: instead of clicking on a link in an email message, open your Web browser and type in the address of the company or service in question. Then once at the real site, enter the information required to identify yourself. FL

Proof Positive: What Percentage of Organizations Suffer Computer Security Incidents?



2007 Computer Crime and Security Survey
Source: Computer Security Institute

Asked whether they'd suffered an incident of some kind (other than minor "scans," which are the cyber equivalent of rattling doorknobs to see if they're locked) during the prior year, 487 respondents said that almost half of their organizations had in fact suffered some kind of attack.

SPECIAL TACTICS

Picture This: A Tracking Device on Your Face

Polar Rose, a new service on the Web, is nothing fancy. It is software that studies pictures of faces, determines their unique features, and then attempts to recognize whose faces are shown. This is nothing new, but Polar Rose claims to be more accurate than previously existing facial recognition technology and it's been turned loose on all the pictures stored on the Web. Polar Rose issued a launch announcement promising that the online service will enable people to:

- ❏ Search for more photos of the same person on specific sites or across the whole Internet.
- ❏ Collectively add information and tag people in online photos.
- ❏ Automatically sort online photos by the people appearing in them.
- ❏ Be alerted when new photos matching visual search criteria appear.

If you put family photos on the Web (perhaps you post them on a picture-sharing service like Flickr), Polar Rose should be able to figure out the people in the photographs (the service is able to do this in part because its users collectively fine-tune the recognition and identify new faces).

Therefore, if you're in the pictures you post, it will be possible for others to use the service in the future to identify you in other pictures. These may or may not be pictures you've decided to post. Perhaps it's a picture of you at a political protest, or a visual record of your attendance at a party that you would prefer to be discreet about.

Polar Rose, which hasn't yet made its service publicly available as this issue of *FrontLine* goes to press, recognizes that the service poses some privacy issues. From their Web site: "We'll end up finding photos that the publisher never really thought of as being public. The trick, however, is not to turn off the technology, just like Altavista or any of the subsequent search engines weren't shut down or otherwise censored. The challenge is to facilitate a way to make sure that photos that shouldn't be in our database, aren't. This can be by restricting access or by telling us not to pick them up."

Polar Rose doesn't say they'll let you opt out from being identified in pictures that appear on other people's Web sites.

It's hard to say just how intrusive Polar Rose will be, but the larger point is that there will certainly be more tracking of online photography. Just as you're careful about what you say online, you should be careful about protecting your "photographic privacy" as well. FL

What's a Bot?

[Continued from page 1]

Botnet operators are known as "bot herders" and there are relatively few of them. The number of compromised computers has been increasing, but the number of networks of these bots has become relatively stable. The hackers who create the software for botnets create elaborate systems for communicating with their "herds," adding enough re-routing and encrypted messaging that finding the source of the commands and tracking it back to the individual criminal commanding the botnet is a difficult job.

The herders hire out their networks to other criminals and the number of cyber attacks carried out by hackers who are not using botnets appears to be dropping, according to research by computer security company Symantec. Interestingly, the largest number of bot herders in the world is located in the U.S.

Keeping your computer from becoming a bot (also sometimes called a zombie) involves taking the usual precautions. Be sure your computers have anti-virus software, that it receives regular updates and runs at all times so that it can detect the latest threats. Don't click on Web links in email messages if you aren't absolutely sure the sender can be trusted. Never open email attachments unless you expected the attachment to be sent to you and it's coming from someone you know.

As you'd expect, the increasing use of organized networks of computers to carry out cybercrime is a significant and dangerous development on the Internet. The more that we and the organizations we work for can keep bot software from reaching our computers, the better we'll be able to keep the problem under control. FL

UNDER THE MICROSCOPE

HACKER JUGGLING

How do hackers keep especially sensitive (or legally incriminating) data from being discovered by police if their computers are seized and searched? In some cases, they simply store the information in transit between their computer and other computers on the Internet. One technique, called "juggling," sends encrypted pieces of the information to multiple slow, reliable mail servers.

These servers receive the information with a command that causes them to echo back the information to the sender. By delaying the sending of the command, the data can be left in limbo on the mail server for an indeterminate amount of time. When the information is finally returned, it's immediately forwarded to another server. It's not a highly reliable storage system. If the hacker's computer freezes or is powered down, the data is lost.

The same problem occurs if a mail server fails while pieces of the file are being sent. Since hackers are able to divide an incriminating file onto several different computers, it's almost impossible for other hackers to steal the information. Perhaps more importantly for hackers, pulling the plug as the police arrive means there's no trace left of the file to serve as evidence for future trials. Furthermore, given the design of Internet services such as email, there's no immediately obvious way to prevent hackers from using juggling to hide their secrets.

© 2007 by COMPUTER SECURITY INSTITUTE

Horror Stories

If you find yourself wondering why today's business managers and security departments are concerned about employee security behaviors, take a look at today's headlines. These selected stories from around the globe make it clear that there are lots of good reasons to be careful.

CREDIT CARD FRAUD FEARS CLOUD OPERATION ORE

Many of the child abuse download suspects snared in Operation Ore may have been innocent victims of credit card fraud, according to a BBC investigation. Operation Ore, the U.K.'s biggest ever child pornography investigation, involved the prosecution of 2,000 suspects among 7,000 Brits whose credit cards were used to pay for access to images of child abuse via a US-based portal run by Landslide Inc.

–The Register, 5/10

MONTH OF SEARCH ENGINE BUGS

A Ukranian security researcher is planning to run a 'Month of Bugs' project that will target vulnerabilities within Search Engines. The project is set to run during June and the researchers stated purpose is exposing the security problems in search engines, which have become some of the most popular sites on the Internet.

–Virus.org, 5/17

TARGETED ATTACKS ON THE RISE

It's the other end of the threat spectrum: Instead of a massive attack on hundreds of your users, it's one message, sent to a single user, containing a backdoor Trojan–or worse. Such narrowly targeted attacks are becoming more popular than ever, according to a new report issued today by MessageLabs. The messaging security company says it identified 716 emails in 249 targeted attacks last month. The attacks targeted 263 different domains, belonging to 216 different customers.

–DarkReading, 4/18

PHISHER 'VLADUZ' DODGES EBAY'S DEFENSES

For at least the third time in as many months, a malicious hacker has gained unauthorized access to parts of eBay's network despite the best efforts of the company's security team to fortify its system against the embarrassing breaches.

–SecurityFocus, 3/1

SPAMMERS STYMIE U.K. EMAIL

More than 200,000 users of a popular British Internet service are without the ability to access email over the Web, thanks to a spam attack that the ISP is still struggling to resolve. The ISP says the attack exploited a vulnerability that "cannot be patched," and therefore it is building new servers for its @ Mail system.

–DarkReading, 5/17

EIGHTIES THROWBACK WORM SPREADS VIA MEMORY STICKS

Miscreants have created a strain of malware that uses memory sticks as a vector for infection. The SillyFD-AA worm spreads by copying itself from infected machines onto removable drives such as USB memory sticks before automatically running when the device is connected to a computer.

–The Register, 5/11

USDA ADMITS EXPOSING 26 YEARS OF SOCIAL SECURITY NUMBERS

The Social Security numbers of about 150,000 people may be at risk for identity theft after it was discovered that a government agency has exposed the personal identifying information on farmers and others for the last 26 years. The U.S. Department of Agriculture announced Friday that it had inadvertently exposed online sensitive information, such as names and Social Security numbers, in a publicly available database.

–InformationWeek, 4/20

SOCIAL SECURITY ADMINISTRATION WORKER CHARGED IN IDENTITY THEFT SCHEME

A former Social Security Administration employee surrendered to federal authorities Wednesday to face charges of illegally disclosing personal information she took off a government computer that was then used in an identity theft scheme that racked up $2.5 million in credit card charges.

–InformationWeek, 4/13

GOOGLE TO ANONYMIZE USER DATA

Google is to discard some information it stores about user search requests in an effort to address concerns by privacy watchdogs and defend itself against government demands for data.

–The Register, 3/15

'YOU'RE NOW FREE TO MOVE ABOUT THE COMPANY'

Personal information–including Social Security numbers of more than 300 pilots and other employees at American Airlines, such as the chief executive–was exposed on a company Web site, according to the pilots union, the Allied Pilots Association.

–DarkReading, 6/27

LAX SECURITY LED TO TJX BREACH

A wireless network that employed less protection than many people use on their home systems appears to be the weak link that led TJX Companies, the U.S.-based retailing empire, to preside over the world's biggest known theft of credit card numbers.

–The Register, 5/4