Dangers grow on Web from attacks

July 9 2009, By Elise Ackerman

When people worry about the dangers of the Internet, a Web site built by the producers of "Mister Rogers' Neighborhood" is probably not what they have in mind.

So parents and teachers became highly alarmed when their Google searches earlier this year for the site, Family Communications, turned up dire warnings about a malicious software infection.

"The phone kept ringing and ringing," said Kevin Morrison, the chief operating officer for the Pittsburgh production company founded in 1971 by Fred Rogers, the popular children's television host. "They were saying, 'Google says your site is not safe.'"

It took Morrison some time to figure out that fci.org had been hacked. And it wasn't alone. More than a dozen other sites that share the same hosting provider had been targeted, part of a global and growing wave of malicious activity that is forcing ordinary Internet destinations into the online equivalent of quarantine zones.

"Hackers are breaking into every site they can," said Richard Wang, a manager at SophosLab US, a Boston-based security company. "The old advice about avoiding sites offering free software, illegal downloads or adult content is less relevant now. Any site can be a source for infection."

By the end of last year, Microsoft was finding booby-trapped Web pages at the rate of a million a month. These sites, also known as drive-by

downloads, can infect a computer without a person taking any action except visiting a Web page. A human isn't required to click on an e-mail link or to agree to install any software. Instead, the sites automatically download software onto visitors' computers.

Once that happens, cyber criminals can do several things. They can implant a keystroke logger on the machine to record passwords or other valuable information. Compromised machines also often become part of "botnets," large collections of computers that are rented out for criminal purposes, including sending spam or phishing, an attack that attempts to trick someone into revealing valuable personal information.

While drive-by downloads have plagued the Web for years, security experts say their numbers are spiking because criminals have automated their attacks, and because sites have become more vulnerable as they have become more complex. Sophos said its Web crawler discovers a new infected Web page every 4.5 seconds, a threefold increase over 2007.

"It's one of the biggest trends we are seeing," said Zulfikar Ramzan, a technical director at Symantec.

Infected Web pages still make up only a tiny portion of the Web itself, which has grown to more than a trillion pages. But by piggybacking on popular destinations -- like the Mister Rogers site -- they turn up with increasing frequency in search results.

Last year attackers broke into sites owned by well-known brands like Sony and Adobe, as well as BusinessWeek and Cambridge University Press.

Ordinary people can largely protect themselves by keeping their operating systems, browsers and anti-virus software up to date. Browser

plug-ins from large anti-virus manufacturers such as Symantec and McAfee as well as smaller companies like Web of Trust identify potentially problematic Web sites. And other plug-ins like NoScript for the FireFox browser can cripple malicious code by disabling software scripts, though they can also reduce the "special effects" on some sites.

All major search engines prominently flag risky sites when they show up in search results. For example, Google inserts a link underneath the title of such sites that says "this site may harm your computer."

If someone clicks on the link anyway, Google will take the person to one of its own pages that contains a lengthy warning: "Please be aware that malicious software is often installed without your knowledge or permission when you visit these sites, and can include programs that delete data on your computer, steal personal information such as passwords and credit card numbers, or alter your search results." The Google page does not link to the original URL, or Web address.

At that point, the only way someone can get to the offending site is to type in the URL directly.

The problem with this kind of approach, said Neil Daswani, who worked on the security team at Google for three years, is that a lot of unsuspecting Web site owners are finding themselves blacklisted for reasons they don't understand. There are literally 10,000 ways attackers can break into a Web site. Locating the harmful code they insert and removing it takes specialized skills. Daswani said the average Web site operator can't keep up.

Daswani left Google in October to co-found a company, Dasient, whose goal is to help ease the load at a reasonable price. Basic diagnostic and monitoring services are free. For an additional fee, ?Dasient will automatically remove dangerous code before the problem is spotted by a

search engine without disrupting the operation of the site.

Morrison said he was initially skeptical of Dasient, but after the company quickly found rogue software that was using the Family Communications site to run a phishing scam, he happily signed on as a beta tester. "If you do have a Web site with a lot of pages there is no easy way to know where the bad code is," he said. "Google doesn't tell you."

___

PROTECT YOURSELF FROM A DRIVE-BY DOWNLOAD

1. Make sure you have the most current version of your operating system and browser.

2. Update anti-virus and anti-spyware software.

3. Pay attention to search-engine warnings.

4. Add a browser plug-in that will provide additional information about problem Web pages.

5. Add a browser plug-in that will prevent automatic launching of Web-page software.

___