

Scob Attack: A Sign of Bad Things to Come?

Neal Leavitt

A recent Internet attack that exploited a powerful new assault technique has computer security officials worried that it could be a harbinger of worse things to come.

The attack was based on a Trojan horse—a nonreplicating program that hides malicious code inside apparently harmless programming, data, or Web pages—dubbed JS.Scob.Trojan by antivirus experts.

“We have validated a minimum of 630 different Web servers compromised in this attack,” said Ken Dunham, director of malicious code for iDefense, a computer security company. “These servers hosted millions of infected pages during the attack. And ongoing attacks related to this continue to emerge.”

Scob affected Web sites for such well-known organizations as the Kelley Blue Book car pricing service and MinervaHealth, which provides online financial services for the health-care industry.

The Trojan loaded software that captured victims’ keystrokes—which could have included valuable information such as passwords and credit card numbers—and sent them back to the hackers. “Once completed, credit card and identity theft could occur,” explained Dunham.

The attack was particularly effective because it targeted the most common



operating system (all Windows versions) and Web browser (all Internet Explorer versions), as well as the popular Microsoft Internet Information Server (IIS) 5.0, which functions as both a Web and FTP server.

The Scob attack was significant for several reasons. Scob’s dangerous new aspect was that rather than opening e-mail attachments, victims didn’t have to do anything but visit a contaminated Web site to become infected. “By using Web servers and Web sites to install the malicious code, hackers were able to install the Trojan,” explained Dunham.

In the past, hackers have used Web sites to spread adware, spyware, or browser-hijacker software. However, the Scob assault went considerably further by attacking IIS servers so that they would serve infected pages to unsuspecting visitors to popular Web sites.

“Now that the exploit is out, it won’t be long before others adapt it for spamming and for launching broad attacks to cripple the Internet,” predicted Alfred Huger, senior director of engineering at security vendor Symantec.

Scob’s code is readily available on the Internet. “A simple search allows any malicious-code author to retrieve it and use it,” noted Jaime Lyndon Yaneza, a researcher for antivirus software vendor Trend Micro. “This is the danger of such simple script-based viruses. It doesn’t take a rocket scientist to modify the code and rerelease it.”

ORIGINS OF THE ATTACK

On 20 June, the Internet Storm Center—part of the SANS Institute, a computer security research and education organization—got its first inkling of the Scob attack when it began receiving reports that Microsoft IIS servers were being infected.

Law enforcement officials say a group of Russian virus writers called the HangUP Team (hangup.da.ru) probably initiated the attack. “They are a well-organized group that has several years of experience stealing millions of credit cards and online accounts for criminal gain,” noted Dunham.

Scob involved considerable planning, coordination, and sophistication. According to Dan Frasnelli, technical assistance center manager for NetSec, a computer security company, the attack demonstrated the same skills required to design an entire software application. He said careful planning allowed the hackers to target fairly recent or unpatched vulnerabilities in Microsoft’s Web browser, Web server, and Windows platforms.

Several major law enforcement agencies, including the US FBI and the UK’s Scotland Yard, are investigating the incident but hadn’t arrested any suspects at the time this article went to press.

Scob’s authors designed the Trojan so that current antivirus products wouldn’t detect it. “Hackers have an advantage because they get access to our tools,” said Bruce Hughes, director of malicious code research for TruSecure, a computer security company. “They can usually download AV software for 30-day trial periods and

play around with it. They keep modifying their virus until it's undetectable without an update."

On 25 June, officials finally blunted the attack by shutting down the Web site that launched it. For more information, see the "Responding to the Scob Attack" sidebar.

VULNERABILITIES

The Scob attack took advantage of vulnerabilities in Microsoft's IE and IIS, and its Outlook Express e-mail application. Microsoft had already released patches for some of the vulnerabilities when Scob struck, but many users had not installed them. Microsoft has since released patches for all of the security holes.

IE vulnerabilities

According to Sam Curry, vice president for technology vendor Computer Associates International's eTrust security program, Scob exploited unpatched IE vulnerabilities in components such as the Active Data Objects Database, a database class library for the PHP and Python languages. ADODB abstracts the operations so that users can easily switch databases without having to rewrite code.

Active data stream objects contain methods for reading and writing binary and text files. Hackers could thus write executables to the local disk using the ADODB.Stream ActiveX control.

The Scob attack took advantage of this capability, as well as the way that IE handles security by dividing content into five zones, based on its source (and thus its potential risk). IE generally handles Web pages in the Internet zone, which provides medium levels of security by default. Users can adjust security settings for each zone, but most use IE's default settings.

By using active data stream objects to write its executables to the local drive, Scob got IE to handle the Web page-based code in its local zone, explained John S. Quarterman, CEO of InternetPerils, an Internet risk man-

Responding to the Scob Attack

Once major Internet service providers became aware of the Scob attack, they blocked their customers' access to the Russian Web site that launched the assault. The site's address was found in Scob's JavaScript code.

ISP engineers configured routers to discard packets with the site's address as their destination. ISPs also implemented *null routing*, which sent packets destined for the Russian site to a nonexistent address, effectively dropping them.

"[Scob's] reliance on a single, central server as a repository for the malware component was ultimately the downfall of the method," said Dan Frasnelli, technical assistance center manager for NetSec, a computer security company. "Once the addresses associated with the attack were identified, restrictions were implemented at network egress points."

The system administrators of many infected Web sites manually audited their servers for the malicious JavaScript, removed it, turned off IIS's footer feature, and installed patches. In some cases, victims rebuilt their servers, reinstalling all of the software.

Now, said Jaime Lyndon Yaneza, a researcher for antivirus software vendor Trend Micro, "Any up-to-date antivirus software should detect Scob."

agement company. "The local zone provides access to everything on the computer and typically has little or no security [by default]," Quarterman said. Thus, the Scob hackers uploaded malicious code from an untrusted Internet site but had the system execute it as trusted code in the local zone.

IIS vulnerabilities

"We're still not sure how the attackers got onto the IIS servers to install the hostile JavaScript," said Internet Storm Center director Marcus Sachs. "The SSL/PCT vulnerability is the most likely culprit."

This buffer overflow vulnerability, since patched, affects machines that use Microsoft's Private Communications Transport Protocol, which Windows uses to implement Secure Sockets Layer encryption.

Hackers took advantage of the flaw to install a Trojan that opened communications ports through which they could remotely communicate with victims' machines. This also let the machines send information back to the attackers.

"Hackers might also have first gained access to poorly protected Windows workstations of Web masters,

from which they gained access to servers," said Mikko H. Hypponen, director of antivirus research for vendor F-Secure.

According to the Internet Storm Center's Sachs, not all of the attacked Web sites were from companies in the same economic sector. This suggested that the hackers used Internet scanning to locate unpatched IIS servers, rather than targeting only servers that belonged to certain types of companies.

Outlook Express vulnerabilities

Outlook Express created a vulnerability in the way it handled files based on MHTML (MIME encapsulation of aggregate HTML), a standard that defines the MIME structure used to send HTML content in the body of an e-mail message.

Windows' MHTML URL handler is part of Outlook Express and provides a URL type (MHTML://) that lets applications such as IE render MHTML-encoded documents. IE uses Outlook Express, even if it isn't the default e-mail client, to process MHTML documents. This created an opening for the Scob attack.

Scob's authors exploited the vulnerability in visitors' Windows systems

used to open an MHTML URL specially constructed by the hackers. The URL specified a Web site that would make the victim's URL handler force the browser to inadvertently access a page that would load a malicious embedded object. The victim's systems would then execute the attacker-supplied code within IE's local zone.

HOW THE ATTACK WORKED

In the first stage of the attack, hackers installed the executable agent.exe on compromised IIS servers, which then downloaded the ads.vbs administration utility, used to manipulate IIS configurations. This changed the IIS settings that append footers to every file that IIS servers handle. Thus, every HTTP object sent by the Web server back to a victim's browser contained a JavaScript footer with malicious code, which was the Scob Trojan itself.

"The way Scob used the IIS servers to serve infected files to clients was something that hasn't been used very often," said F-Secure's Hypponen. "The JavaScript contained instructions that pointed the victim to the Russian site from which the Trojan was downloaded," he explained.

The Trojan contained additional instructions to download and execute mists.exe, which retrieved still more malware—Backdoor.Berbew.F—from yet another Russian server. Backdoor.Berbew.F had two parts: a keystroke logger that recorded what users typed and a second component that sent the captured information, via the Web, to one of several servers identified in its source code.

In addition to capturing keystrokes, Scob made accessing infected IIS servers difficult and made affected PCs sluggish because of the file uploading and downloading that the attack entailed.

SCOB'S RAMIFICATIONS

The Scob attack showed that hackers could use the Web to spread malicious code effectively. In addition, it demonstrated that exploits could infect

unsuspecting users who didn't run any programs, noted Dan Hubbard, director of technology and research at Websense, an Internet security company.

The attack showed that the Web could spread malicious code effectively.

"It also proves that traditional perimeter and antivirus security methodologies ... have not evolved enough to cover these new types of attacks," Hubbard said. "But on a positive note, this has prompted Microsoft to patch some vulnerabilities that have been lingering for some time."

In Scob's aftermath, computer security experts have encouraged the use of browsers other than IE, such as Mozilla, Netscape, or Opera.

"IE has certain technologies and design features not found in other browsers, like ActiveX, security zones, [and] proprietary DHTML," noted Art Manion, an Internet security analyst with the US Computer Emergency Readiness Team. US-CERT, the key federal agency for cybersecurity coordination and preparedness, is the operational arm of the Department of Homeland Security's National Cyber Security Division.

"Vulnerabilities related to these technologies and design decisions typically don't affect other browsers since they don't implement these technologies or use the same design choices," Manion explained.

Kevin Beaver, president of computer security firm Principle Logic, said Scob could encourage a small percentage of users who care about information security to change their Web browsers and security-related practices. However, he added, "Most people will just ignore this attack and others like it, until their keystrokes are logged somewhere down the line."

Hubbard said he expects Scob-like attacks to become more targeted and sophisticated because hackers can use them to make money. For example, hackers could use stolen credit card numbers, account passwords, or personal identification numbers for their own gain or they could sell the information to others.

Eventually, hackers could readily adapt Scob to target vulnerabilities in applications with shared Microsoft foundation components or other types of weaknesses. Future attacks could also be more ingenious, added NetSec's Frasnelli. For example, he said, the attacks could embed Trojans deeply into shared system libraries without detection, enabling the future compromise of multiple applications.

The best proactive steps involve educating users, system administrators, and software manufacturers. Software diversity is also important, according to InternetPerils' Quarterman, who said, "The more that people use several Web browsers, the less likely it is that a given exploit can compromise all of them. Plus, if more browsers can compete on security, it will generally improve security for all of them."

If users don't do all of these things, Quarterman said, "the problem will get worse, and it will do so faster. Scob is a wake-up call." ■

Neal Leavitt is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Paris; Hamburg, Germany; London; Hong Kong; Bangalore, India; and Sao Paulo, Brazil. He writes frequently on technology-related topics. Contact him at neal@leavcom.com.

Editor: Lee Garber, *Computer*,
l.garber@computer.org