Text Size: A A

WIRED NEWS

Home Technology Culture Business Politics Wired Mag

Pharming Out-Scams Phishing

PRINT MAIL RANTS + RAVES REPRINTS

By Michelle Delio | Also by this reporter

02:00 AM Mar. 14, 2005 PT

First came phishing scams, in which con artists hooked unwary internet users one by one into compromising their personal data. Now the latest cyberswindle, pharming, threatens to reel in entire schools of victims.

Pharmers simply redirect as many users as possible from the legitimate commercial websites they'd intended to visit and lead them to malicious ones. The bogus sites, to which victims are redirected without their knowledge or consent, will likely look the same as a genuine site. But when users enter their login name and password, the information is captured by criminals.

"Phishing is to pharming what a guy with a rod and a reel is to a Russian trawler. Phishers have to approach their targets one by one. Pharmers can scoop up many victims in a single pass," said Chris Risley, president and chief executive officer of Nominum, a provider of IP address infrastructure technology for businesses.

E-mailed viruses that rewrite local host files on individual PCs, like the Banker Trojan, have been used to conduct smaller-scale pharming attacks. Host files convert standard URLs into the numeric strings a computer understands. A computer with a compromised host file will go to the wrong website even if a user types in the correct URL.

The most alarming pharming threat is DNS poisoning, which can cause a large group of users to be herded to bogus sites. DNS -- the domain name system -- translates web and e-mail addresses into numerical strings, acting as a sort of telephone directory for the internet. If a DNS directory is "poisoned" -- altered to contain false information regarding which web address is associated with what numeric string -- users can be silently shuttled to a bogus website even if they type in the correct URL.

"DNS poisoning has been around for over a decade now," said Gregg Mastoras, senior security analyst at Sophos. "Many would argue that the DNS system we all depend so heavily on has inherent design vulnerabilities, and because of the initial design flaws there have been a variety of methods used to create successful attacks.

"So while DNS poisoning is not new, the dramatic rise of phishing, and more importantly the complexity of the new pharming attacks, is cause for some concern," Mastoras said.

Phishing is essentially an old con game updated to take advantage of new technology. Similarly, although DNS attack tactics used by pharmers have been around for a while, the rise in internet banking, online shopping and electronic bill paying has created a wide potential profit zone for criminals eager to snag login information and credit card and bank account numbers.

According to information provided by the SANS Internet Storm Center and internet-monitoring firm Netcraft, this past weekend would-be pharmers attempted to exploit a known vulnerability in Symantec's firewall, redirecting some users from eBay, Google and weather.com to three sites that attempted to install spyware on visitors' computers.

Security experts believe the attack was just a trial run; it was limited in scope and few users seem to have been affected.

However, Mastoras says other sophisticated attacks that take advantage of the flaws in DNS protocols are also currently being tested.

In one example, Mastoras said, Barclays Bank was recently targeted. The phishers sent messages that included a link whose first letters were the correct "barclays.co.uk" but then had additional letters that misdirected the user.

Mastoras called this particular method DNS wildcards. A wildcard DNS record is used to manage mistyped e-mail addresses, but has lately been used by spammers and now by phishers, he said.

"DNS just isn't as secure as we'd like to think it is," said Nominum's Risley. "Every internet request has to go through a DNS server, and malicious hackers realized a long time ago the profit potential in hacking DNS records."

Story continued on Page 2 »

refresh all | expand all | collapse all **Rants & Raves**

Want to start a new thread or reply to a post? Login / Register and start talking!

Frequently Asked Questions

Submit

Ads by Google

Spyware Remover Download
PC Magazine Editor's Choice Winner 5 Star Anti-Spyware. Download Now!
www.pctools.com

100% Free Virus Scan
2005 Highly-Rated Virus Remover. Download it Today!
www.Free-Virus-Remover.org

Phishing Scam?
Brief and Straightforward Guide to
Phishing Scams
wisegeek.com

Find DNS Server
A directory of websites offering information on DNS. (aff)
www.eWoss.com

Text Size: A A A

Home | Technology | Culture | Business | Politics | Wired Mag

Pharming Out-Scams Phishing

PRINT | MAIL | RANTS + RAVES | REPRINTS

By Michelle Delio | Also by this reporter

02:00 AM Mar. 14, 2005 PT

Nominum's chief scientist, Paul Mockapetris, helped to pioneer the internet domain name system through the Internet Engineering Task Force in 1983. Mockapetris also designed the DNS architecture that is still in use today, wrote the specifications and coded the first implementation.

Risley said Mockapetris firmly believes it's time to refresh DNS, and that Mockapetris never expected DNS and BIND -- the most widely used DNS software package for Unix/Linux machines -- to be used on today's huge public systems. Nominum now sells commercial alternatives to open-source BIND and other DNS solutions.

Still, some security experts believe pharmers will not widely deploy DNS-poisoning techniques.

"Could DNS poisoning be an issue? Yes. Will it be a major issue? Probably not," said Mikko H. Hypponen, director of antivirus research at security services vendor F-Secure. Hypponen cited the skill level needed to hack a high-level DNS server as a major deterrent.

Others say plenty of computer-savvy criminals lurking on the internet are eager and able to conduct sophisticated large-scale crimes.

"I believe that DNS-poisoning pharmers will become more of a threat this year, as there is money to be made on a large scale here," said Patrick Hinojosa, chief technical officer at Panda Software, a security technology provider.

"If the right domain can be hijacked or the right DNS record poisoned, a group could make off with data that could be used to accomplish huge financial rip-offs. The problem is that the end user sitting at his computer thinks he's at the correct site because he typed the right URL into the browser," Hinojosa said.

Experts say pharming could be combated if browsers would authenticate websites' identities. Web browser toolbars like one offered by Netcraft can alert users by displaying the true physical location of a website's host. U.S. customers, for example, would likely pause before typing in their passwords when a website that looks like their local bank's site is reported to be hosted in Russia.

"What would go a long way to protecting people would be server-side certificates," said Hinojosa. "But any certificate system would have to be widespread to be effective."

Some financial institutions, whose users are the prime targets of phishing and pharming scams, are experimenting with "multi-factor authentication" logins, including things like single-use passwords and automatic telephone call-backs confirming that a transaction is about to take place. Such practices can limit the havoc a malicious hacker can wreak with a collection of stolen logins and passwords.

Rants & Raves

Frequently Asked Questions

Submit

Ads by Google