

“Pharmers” Plant A New Crop Of Online Fraud

By Michelle Delio

But most financial institutions are old hands at dealing with phishing scams. One of the most effective methods for spoiling the attacks has become practically routine: educating customers not to respond to those now-familiar e-mails demanding they update their account information.

But now cybercriminals are upping the ante with a new spoofing specialty called pharming, a tactic that could potentially be far more potent than phishing because it is executed on a larger scale. Plus, it does not rely on end-user naiveté to work. With the Internet security watchdog group, SANS Internet Storm Center having recently raised its threat level for the scam, alarm over pharming is justifiably on the rise.

While phishers reel in victims one at a time via e-mails soliciting personal information, pharmers attempt to cut right to the chase by automatically redirecting large numbers of unsuspecting users from legitimate commercial Web sites to malicious ones. Pharmers use a number of techniques to accomplish this, including viruses that change settings on end-user's computers. But the most frightening method is DNS poisoning, because it's difficult for even the most computer-savvy user to spot.

DNS, the Domain Name System, translates Web or e-mail addresses into numerical strings, acting as a sort of telephone directory for the Internet. It makes it possible for end users to type in mybank.com rather than a string of numbers to reach their banks' Web sites. But if a DNS directory — a file that resides on most corporate networks and ISP's servers — is “poisoned” or altered to contain false information

regarding which Web address is associated with which numeric string, users can be silently shuttled to a bogus Web site even if they typed in the correct address. If the criminals manage to put together a decent-looking fake Web page, even security-savvy users may never know they have landed on a scam site.

How Big A Threat?

Security experts are divided over whether DNS poisoning is likely to become a major threat. It takes a moderate level of skill to carry out a DNS poisoning attack, so some experts like F-Secure's Mikko Hypponen believe that most scammers will stick to easier methods of prying financial data from unwary users. But security monitoring consortiums such as SANS and Netcraft have been reporting a rise in proof of concept pharming attacks — essentially trial runs — using DNS poisoning.

During March and April 2005 security experts at SANS reported three instances of DNS poisoning. According to a report by SANS researcher Kyle Haugsness, one of these attacks affected only a small group of Internet users and was a rather clumsy attempt by a known spammer to steer visitors to a Web site offering pharmaceuticals.

The other two incidents affected a wider group of users (SANS doesn't know exactly how many). The larger attacks redirected users from well-known Web sites like Google and eBay to three phishing sites, which then attempted to install onto visitors'

machines spyware — software that collects data on users' browsing habits, which is then transmitted back to the spyware's owners.

According to Haugsness' report, log files from two machines used to carry out both of the larger attacks indicated that 1,304 domain names were poisoned. On a third system, which had been compromised during the third attack, a review by SANS revealed that 665 host names were poisoned.

If users of networks relying on these poisoned DNS servers tried to reach a

number of well-traveled sites, including americanexpress.com and citicards.com, or well-known business and news sites such as fedex.com, walmart.com, or espn.com, among hundreds of other Web sites, they would have been redirected to a site that attempted to install a slew of spyware on their machines.

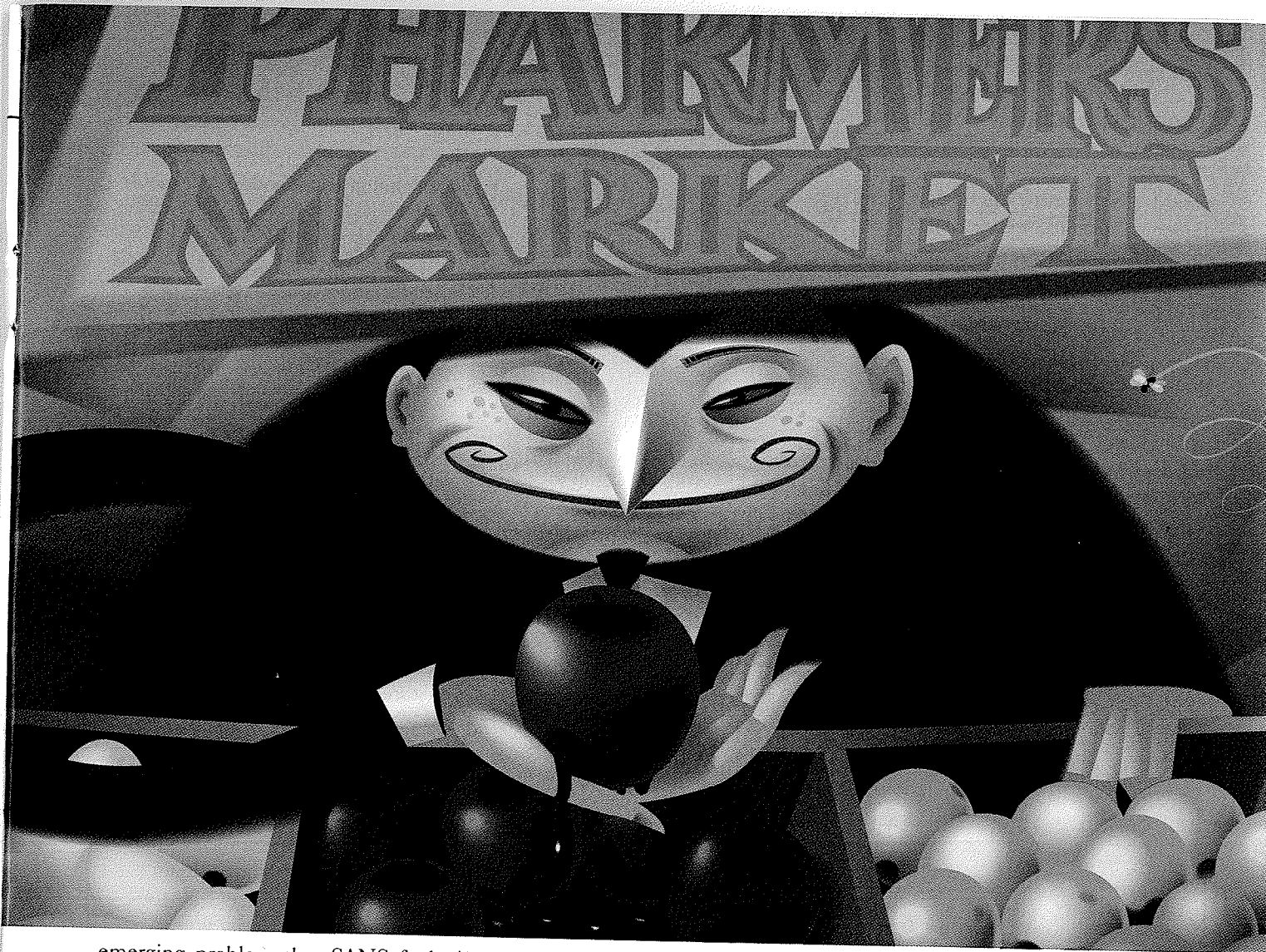
Attempts to install the spyware would most likely have been successful if users were browsing with

Microsoft's Internet Explorer browser and hadn't kept up with security patches from Microsoft. Once this spyware was active on a computer it would enable other malicious software to be easily installed on the affected machine without its owner's knowledge or consent.

In response to these attacks SANS raised its threat rating for DNS poisoning to “yellow” in early April, indicating the emergence of what SANS deems a “significant new threat.” SANS uses a four-color scale to indicate the severity of threats. Green indicates all is well on the Internet; yellow indicates an

Takeaway

“Pharming” is even more insidious than “phishing” because even savvy Internet users can fall victim and the attack takes place beyond the boundaries of the targeted financial services company.



emerging problem that SANS feels bears careful watching; orange indicates a major attack is in process (the Code Red worm earned this designation in the summer of 2001), and the never-yet-seen red indicates large sections of the Internet have lost connectivity.

"The most recent incidents of pharming and DNS poisoning pose difficult challenges for the IT departments in financial institutions," says Patrick Hinojosa, chief technical officer at Panda Software, a security technology provider. "The DNS poisoning scenario is difficult to prevent as it happens outside of the direct control of the institution itself."

How To Stop It

Obviously, stopping pharming will take much more than customer education. It could require the industry to make major investments in new types of security. But where exactly that money should go is not yet clear.

Hinojosa says the first preventative

action that should be taken by the industry is deploying server-side certificates. When users visit a legitimate Web site that employs server-side certificates they'll see a pop-up window or a clickable link telling them exactly who owns the site. Financial firms would obtain a certificate from a trusted authority such as VeriSign.

"This may well be the surest method of defense," Hinojosa says.

"Multifactor authentication" logins, including single-use passwords (see cover story in this issue) can limit the havoc a malicious hacker can wreak with a collection of stolen logins and passwords. But in a recent blog post, Bruce Schneier, chief technology officer of Counterpane Internet Security, warned that multifactor systems would not put an end to fraud. Financial institutions risk spending millions of dollars to outfit their users with two-factor authentication tokens, and getting only a negligible drop in the amount of fraud

and identity theft, he says.

"Two-factor authentication isn't our savior," Schneier wrote. Schneier says criminals will always find a way to steal identity information, so sinking money into user-authentication systems isn't the best use of funds. Instead Schneier urges financial firms to focus on making it harder to use the stolen data.

"Banks need to treat this as a problem of fraudulent transactions," Schneier says. "Whether it's two-factor authentication, ID cards, biometrics, or whatever, there's a widespread myth that authenticating the person is the way to prevent these crimes. But once you understand that the problem is fraudulent transactions, you quickly realize that authenticating the person isn't the way to proceed."

Financial institutions should take a cue from credit card companies, which offer a leading example of how to shut down fraudulent transactions, Schneier says. Like card companies, banks

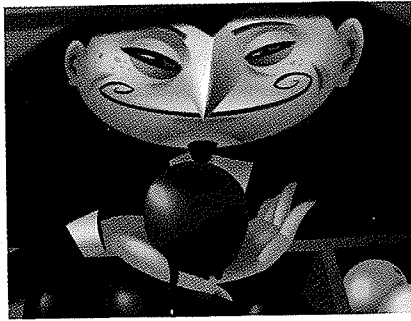
should use pattern-analysis tools to detect suspicious transactions and confirm them with account holders

Echoing Schneier, Elazar Katz, director of the active risk monitoring practice in the global financial services group at Unisys, also says banks should expand their use of pattern-analysis tools. Beyond using them to detect evidence of fraudulent transactions, banks should also use them to better understand criminals' intelligence-gathering activities.

"Financial firms must be able to better detect when hackers try to gain unauthorized access to consumers' personal information, such as address, spouse's name or check images with customer signature," Katz says.

Schneier also believes that banks should put limits on what people can do online with their accounts.

That last proposal may be a tough pill for bankers to swallow. The industry has



been working for years to expand the functionality of online banking. Even potentially risky features like immediate funding of online accounts are starting to creep into the landscape.

Many Defenses

Figuring out how to best fortify your defenses against pharming — through multifactor authentication or pattern recognition — is a murky issue. Avivah Litan, a research director at Gartner, says she believes enterprises shouldn't choose

one solution over another but instead employ a wide range of fraud-protection and detection techniques.

"There is no magic bullet or single remedy," says Litan.

Stronger authentication of customers makes life tougher for crooks, especially if the enterprise re-authenticates the customer before executing a sensitive transaction like a money transfer, Litan says. But she adds that she urges clients to put their highest priority on back-end fraud-detection services that can spot suspicious transactions before they are executed. Once the money moves out of the account, it may be too late.

"An enterprise needs to erect as many walls as possible to keep out the crooks — both on the front end where customers are authenticated and on the back end, where suspect transactions are stopped in their tracks," Litan says.