

The New York Times

© 2011 The New York Times

FRIDAY, JUNE 3, 2011

E-Mail Fraud Hides Behind Friendly Face

By **MATT RICHTEL**
and **VERNE G. KOPYTOFF**

SAN FRANCISCO — Most people know to ignore the e-mail overture from a Nigerian prince offering riches in exchange for a bank account number. That is a scam, plain to the eye.

But what if the e-mail appears to come from a colleague down the hall? And all he asks is that you add some personal information to a company database?

This is spear phishing, a rapidly proliferating form of fraud that comes with a familiar face: messages that appear to be from co-workers, friends or family members, customized to trick you into letting your guard down online. And it has turned into a major problem, according to technology companies and computer security experts.

On Wednesday, Google disclosed that it had discovered and disrupted an effort to use such pinpoint tactics to steal hundreds of Gmail passwords and monitor the accounts of prominent people, including senior government officials. Secretary of State Hillary Rodham Clinton said Thurs-

Continued on Page A3

Spreading E-Mail Fraud Hides Behind Friendly Faces

From Page A1

day that the F.B.I. would investigate Google's assertion that the campaign originated in China.

Such tactics were also used in an attack on a company called RSA Security, which security experts say may have given hackers the tools to carry out a serious intrusion last month at Lockheed Martin, the world's largest military contractor.

The security specialists say these efforts are a far cry from more standard phishing attempts, which involve spraying the Internet with millions of e-mails that appear to be from, say, Citibank in the hope of snaring a few unfortunate Citibank customers. Spear phishing entails sending highly targeted pitches that can look authentic because they appear to come from a trusted source and contain plausible messages.

As such, the specialists say, the overtures are becoming very difficult for recipients to detect.

"It's a really nasty tactic because it's so personalized," said Bruce Schneier, the chief security technology officer of the British company BT Group. "It's an e-mail from your mother saying she needs your Social Security number for the will she's doing."

Mr. Schneier said the attacks are more like a traditional con game than a technically sophisticated intrusion. "This is hacking the person," he said. "It's not hacking the computer."

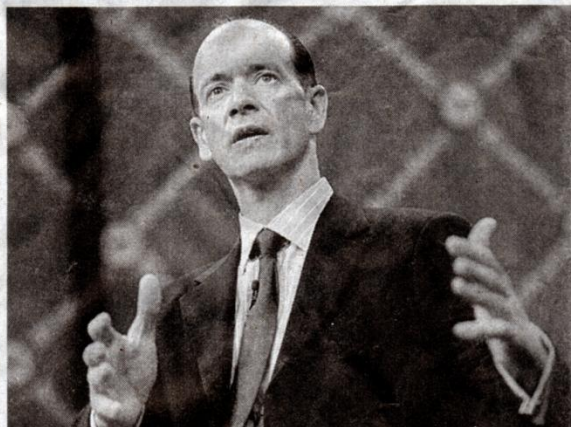
Symantec, the computer security firm, said it intercepted around 85 targeted attacks a day in March, including efforts to steal personal information through phishing or with links to nefarious software that could ultimately expose corporate files. The only month with more attacks was March 2009, when there was a surge that coincided with a G20 summit meeting.

Symantec said the most common targets were government agencies and senior managers and executives; the phishing of such big game is commonly referred to as "whaling." Manufacturing firms were the targets of 15.9 percent of the attacks, compared with 8 percent for the financial sector and 6.1 percent for technology companies, Symantec said. Hackers taking aim at corporations are often seeking new product designs and may focus on engineers at a defense con-

John Markoff contributed reporting.



JOSE LUIS MAGANA/ASSOCIATED PRESS



ANDREW HARRER/BLOOMBERG NEWS

Secretary of State Hillary Rodham Clinton said the F.B.I. would investigate a series of fraudulent e-mails. Enrique Salem, Symantec's chief executive, said hackers personalize messages.

tractor, for example, to get data they can sell on the black market.

Enrique Salem, Symantec's chief executive, gave the example of an e-mail sent to the head of a company that appears to be from the Internal Revenue Service. The message raises questions about the tax implications of an acquisition, and the chief executive passes the message to others inside the company. Someone opens the attachment, giving the attacker access to the company's internal network.

"It's about getting you to do something to compromise the system," Mr. Salem said.

In the case of the Gmail attacks, Google said they appeared to originate from Jinan, China, and were aimed at users like Chinese political activists, military personnel, journalists and South Korean officials.

paign when one of the victims let her examine some suspicious messages.

That led her to discover a fake but convincing Gmail login screen that attackers used to dupe targets into submitting their passwords. She said the messages indicated that the phishing attempts had begun at least a year before she learned of them — early in 2010.

"I thought it was interesting because they did it for so long," Ms. Parkour said. She said she also saw screens that mimicked the login pages for the Web portals of corporate e-mail systems.

Companies and individuals can take steps to head off these attacks. For instance, Google encourages people to use a two-step process that sends a special code to their cellphone when they log into Gmail. The Defense Department asks its personnel to use a "digital signature" on their e-mails that verifies their identity.

The momentum is on the side of the attackers, given that their forgeries can be realistic and thus irresistible, according to Lt. Col. Gregory Conti, a computer security expert at West Point. He said one reason the problem was getting harder to parry was that the people sending the messages use the Internet, specifically social networks like Facebook, to gather so much personal information about potential targets.

"What's 'wrong' with these e-mails is very, very subtle," he said, adding: "They'll come in error-free, often using the appropriate jargon or acronyms for a given office or organization."

The way to stop such efforts is not clear, Mr. Conti said: "It's an open problem."

Victims of spear phishing include people who oversee corporate security, said Larry Ponemon, chairman of the Ponemon Institute, a research company in Traverse City, Mich., that focuses on data security. He gave the example of a security technology executive who received an e-mail from what appeared to be his employer's human resources department that asked for personal information to make a payment.

Mr. Schneier of BT said he did not believe there was an easy and universal fix for the problem, any more than there was for car theft. He said the personal nature of the attacks makes them too seductive.

"Welcome to the world. You cannot stop it," he said. "Live with it."

The Chinese Foreign Ministry said Thursday that the government had no involvement in any such attacks, and that it "consistently opposes any criminal activities that damage the Internet and computer networks including hacking, and cracks down on these activities according to law."

It is not clear how the attackers obtained the Gmail addresses they used, although they could have been found inside other compromised accounts, including corporate or government accounts whose addresses are often easier to guess.

The attackers may have hoped to find some work-related e-mail in their victims' personal Gmail accounts.

Mila Parkour, an independent security researcher who helped alert Google to the attacks, said she was tipped off to the cam-