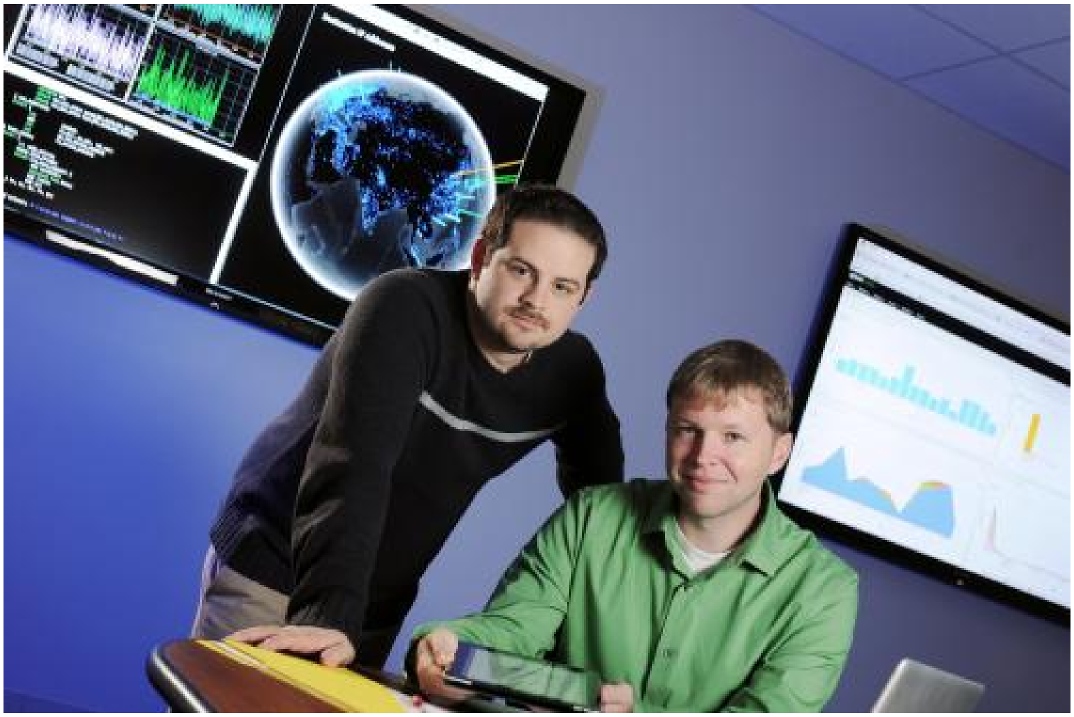
Spear phishing: Researchers work to counter email attacks that gain recipients' trust

January 9 2013, by John Toon



Researchers at the Georgia Tech Research Institute (GTRI) are working to counter threats from spear phishing. The attacks use knowledge of computer users to gain their trust to break into corportate networks. Credit: Gary Meek

(Phys.org)—The email resembled the organization's own employee e-newsletter and asked recipients to visit a website to confirm that they wanted to continue receiving the newsletter. Another email carried an attachment it said contained the marketing plan the recipient had requested at a recent conference. A third email bearing a colleague's name suggested a useful website to visit.

None of these emails were what they pretended to be. The first directed victims to a website that asked for personal information, including the user's password. The second included a virus launched when the "marketing plan" was opened. The third directed users to a website that attempted to install a malicious program.

All three are examples of what information security experts at the Georgia Tech Research Institute (GTRI) say is the most challenging threat facing corporate networks today: "spear phishing."

Generic emails asking employees to open malicious attachments, provide confidential information or follow links to infected websites have been around for a long time. What's new today is that the authors of these emails are now targeting their attacks using specific knowledge about employees and the organizations they work for. The inside knowledge used in these spear phishing attacks gains the trust of recipients.

"Spear phishing is the most popular way to get into a corporate network these days," said Andrew Howard, a GTRI research scientist who heads up the organization's malware unit. "Because the malware authors now have some information about the people they are sending these to, they are more likely to get a response. When they know something about you, they can dramatically increase their odds."

The success of spear phishing attacks depends on finding the weakest link in a corporate network. That weakest link can be just one person who falls for an authentic-looking email.

"Organizations can spend millions and millions of dollars to protect their networks, but all it takes is one carefully-crafted email to let someone into it," Howard said. "It's very difficult to put technical controls into place to prevent humans from making a mistake. To keep these attacks out, email users have to do the right thing every single time."

Howard and other GTRI researchers are now working to help email recipients by taking advantage of the same public information the malware authors use to con their victims. Much of that information comes from social media sites that both companies and malware authors find helpful. Other information may be found in Securities and Exchange Commission (SEC) filings, or even on an organization's own website.

"There are lots of open sources of information that will increase the chances of eliciting a response in spear phishing," Howard said. "We are looking at a way to warn users based on this information. We'd like to see email systems smart enough to let users know that information contained in a suspect message is from an open source and suggest they be cautious."

Other techniques to counter the attacks may come from having access to all the traffic entering a corporate network.

To increase their chance of success, criminals attempting to access a corporate network often target more than one person in an organization. Network security tools could use information about similar spear phishing attempts to warn other members of an organization. And by having access to all email, security systems could learn what's "normal" for each individual – and recognize unusual email that may be suspicious.

"We are looking at building behavioral patterns for users so we'd know what kinds of email they usually receive. When something comes in that's suspicious, we could warn the user," Howard said. "We think the real answer is to keep malicious email from ever getting into a user's inbox, but that is a much more difficult problem."

It's difficult because organizations today depend on receiving, opening and responding to email from customers. Deleting or even delaying emails can have a high business cost.

"What we do requires a careful balance of protecting the user, but allowing the user to get his or her job done," he said. "Like any security challenge we have to balance that."

These and other strategies will be part of Phalanx, a new product being developed by GTRI researchers to protect corporate networks from spear phishing. It will be part of Titan, a dynamic framework for malicious software analysis that GTRI launched last spring.

Among the challenges ahead are developing natural language algorithms that can quickly separate potential spear phishing attacks from harmless emails. That could be done by searching for language indicating a request such as "open this attachment" or "verify your password."

GTRI researchers been gaining experience with corporate networks based on security evaluations they've done, and work with GTRI's own network – which receives millions of emails each day. Fortunately, they say, it's not just the bad guys who are learning more.

"The chief financial officers of companies now understand the financial impacts of spear phishing, and whey they join forces with the chief information officers, there will be an urgency to address this problem," he added. "Until then, users are the front line defense. We need every user to have a little paranoia about email."

Provided by Georgia Institute of Technology

Citation: Spear phishing: Researchers work to counter email attacks that gain recipients' trust (2013, January 9) retrieved 26 April 2024 from https://phys.org/news/2013-01-spear-phishing-counter-email-gain.html