Top Blogs

A CGNET News Special Edition
November 25, 2019

A Phish Tale:

What a Successful Attack Looks Like

by Dan Callahan

It's instructive to see how a successful phishing attack can happen. Let me share a story with you. I got a text message, then a call last week. Both were from the same customer. "Dan, I think my account has been hacked," was the message. "What do I do now?" The customer went on to say that he figured out his account had been hacked when he began getting calls from people, asking him why he'd sent them a message about an overdue invoice.

I was in the car, so I told the customer to unplug from the Internet and scan his computer right away. Once I got to a computer, I changed his account password. As I continued to work with the customer, I began to see how this successful phishing attacked happened.

First Comes the Phish

Jim (not his real name) told me that he had recently received a message and clicked on the link in the message. He wasn't sure what happened next but thought that maybe he'd given up his username and password by accident.

As we checked the security logs, we determined that someone accessed the account around the time Jim clicked on that link, September 17th. There were first some unsuccessful attempts to access Jim's account from IP addresses in Asia. Seven hours later, there were successful login attempts from Europe. Five hours later, there were other successful logins from Africa. It's possible the IP address locations were spoofed. It's also possible that Jim's account credentials were now on some dark web database and being exploited.

Next Come the Outlook Rules

The next step in this successful phishing attack occurred when the Bad Guy created some Outlook rules designed to hide their activity. Clearly, they were planning to use Jim's account for some time. The Bad Guy created rules to

- Delete sent messages
- Delete any undeliverable messages
- Send any replies to an obscure folder
- Forward all messages to (presumably) that Bad Guy's Gmail account

Jim's account had been hacked for a week before he noticed. And he only noticed when people started asking him why he was sending them a note about a past due invoice (Jim doesn't work in Accounts Receivable). These Inbox rules hid any signs that something was wrong.

Continued on Page 6

How Secure Is Your Attack Surface?

by Tim Haight

Recently, CGNET has begun to offer attack surface assessments in addition to internal and external penetration testing. I thought I'd tell you why.

Conventional penetration tests, such as Nessus or QualysGuard, do a terrific job of detecting vulnerabilities on servers. Regular use of these tools has become a best practice, with good reason.

Unfortunately, in the same way that rust never sleeps, malicious actors are constantly looking for new ways to get into your systems. Now that hacking has become big business, malicious researchers have plenty of resources to devote to discovering new methods.

Continued on Page 7

Take a Look Inside: