Google Phishing Attack ‘Slight New Twist’ on Increasingly Prevalent Trend, Say Experts

The recent phishing attack on Gmail users was unique because it tried to scam a high-profile company and to exploit a weakness through the newer OAuth standard, said experts in interviews Monday. Beyond that, it’s a “slight new twist on a very old story,” said Luke Beals, senior director-cybersecurity at heath IT firm CNSI. The problem is only getting worse, and experts said awareness, education and training are the best answers, and one cited artificial intelligence as a way to address the issue.

Google said the spoofing campaign, which affected fewer than 0.1 percent of users, was stopped within an hour of being discovered (see 1705050048 and 1705040025). The company said some users were tricked into granting access to contact information after receiving an email that invited them to view a shared file in Google Docs. The company said it is updating policies and enforcement of OAuth apps and anti-spam systems and expanding monitoring of “suspicious” third-party apps that seek information from users.

Exploiting Google was “a bit of a surprise,” said Beals, since the company left a vulnerability in place. He said the attackers may have been a victim of their own success. “It started spreading so fast that it was just blatantly obvious,” he said. “If they slowed it down a bit and maybe taken a little more caution to go under the radar, Google may not have even known about it right away.”

Robert Lord, CEO of healthcare privacy and data security firm

Protenus, said the tactics are much the same across all industries since phishing attacks go after the weakest link: people. “Trends are getting more and more dangerous. It’s getting harder and harder to determine what is a legitimate email and what is not and this is a great example of that,” he said, referring to the Gmail attack. Another concern is that Gmail is also used within some companies, which means if attackers can get into a centralized system, they could potentially gain access, for example, to electronic health records that may be accessible by employees within a hospital, he said.

Citing studies, Paige Schaffer, president of Generali Global Assistance’s identity and digital protection services global unit, said more than 90 percent of cyberattacks start with phishing emails, and 30 percent of those emails get opened. “The numbers are astoundingly high,” she said. “While it is a high-tech problem, the solution is really … more low tech. It’s really about common sense.” If users are suspicious about a link with an email, they should directly go to the purported source’s website and get authenticated through there, she said.

Beals said the best defense against phishing attacks is to prepare, educate and train employees and consumers in recognizing such scams. “There’s no single way to stop it,” he said, other than through education. “It’ll always happen and we’ll just find new twists.” Jay Majmudar, CNSI senior vice president-IT, said many companies seek education and training typically after they’ve been victimized but in this case he said it went to consumers who “would be much more susceptible to hitting that link.”

Lord said technology allows organizations to audit their workforce by testing different groups of employees to see who may need the training. He said AI and machine learning also is being deployed to deal with these typically asymmetric threats and expand capabilities of security teams. Such technologies

can understand in great detail appropriate and inappropriate actions and what a particular user should or shouldn't be doing and identify bad actors, he said. Even if the credentials of a legitimate employee are stolen, such a system could determine if the employee using those credentials in an "odd" manner, he added.

Phishing attacks are increasingly becoming a bigger problem, Schaffer said, but Americans and U.S. companies are more aware and doing something more like using monitoring – such as software tools and/or services that provide consumers with notifications and alerts – though they're not enough. The Center for Identity at the University of Texas-Austin tracks ID theft issues and is like an "Amber Alert" for such trends like phishing, but it's difficult to keep up, she said. "It's just the pace this is going. It's going very quickly."

Original article was published by Communications Daily on Tuesday, May 9, 2017.