

SearchSecurity.com

Cisco: Targeted phishing helped hackers earn \$150 million last month

Mass email attacks designed to target a wide-ranging audience are falling out of favor with attackers, according to research conducted by Cisco Systems Inc.

You've got to ask yourself: In your organization, do you possess data or are you an organization that someone would preselect as a target?

Wade Baker, director of research and risk management, Verizon Business

The study, "Email Attacks: This Time It's Personal," (.pdf) was conducted by Cisco's Security Intelligence Operations, the San Jose, Calif.-based networking giant's threat management unit. It found the success rate declining for mass email campaigns. Mass spam volumes plummeted from 300 billion daily spam messages to just 40 billion between June 2010 and June 2011. The estimate of how much money is being made from traditional mass email-based attacks has declined more than 50%, from \$1.1 billion in June 2010, to \$500 million in June 2011.

To make up for the lack of success, attackers are developing spear phishing campaigns and personalized scams, according to the report. Rather than pushing out thousands of email randomly, attackers use targeted phishing to exploit select groups of people: employees at a defense contractor, bank tellers or college students. Typically the attack has a more deceptive email catered toward the victim's interests or activities.

The Cisco researchers credit the reduction in mass email attacks to law enforcement action, effectively crippling botnets that drive the activity, including Rustock, Bredolab and Mega-D. In addition, Russian police pressed charges against the owner of SpamIt, a large spam-sending affiliate network. "By disrupting the financial and technical business models of key cartels," the report states, "threat volumes have declined in favor of more lucrative activities."

Cybercriminals made an estimated \$150 million in June from spear phishing attacks, according to the report. The figure, derived from what Cisco calls a conservative estimate of a \$400 loss per user, per successful phishing event, and then extrapolated on an annualized basis, has tripped from \$50 million in June 2010, and is expected to continue to increase.

Spear phishing and other targeted attack methods were used in a number of recent high-profile data breaches. A spear phishing email was used in the RSA breach, which led to the loss of sensitive data pertaining to the company's SecurID two-factor authentication product. The Google Aurora attack also contained a spear phishing component. Once a victim clicks on the link, the attacker typically scans for an application vulnerability and sometimes exploits a zero-day flaw to infect and gain control of the victim's machine.

While the costs to the cybercriminal are typically higher for a spear phishing attack, Cisco said, the yield and benefit is greater. A single spear phishing attack targeting 1,000 people has the potential to haul in \$150,000, according to the Cisco report. Meanwhile, a cybercriminal's traditional mass email campaign that targets about 1 million people can potentially bring in \$14,000.

The 2011 Verizon Data Breach Investigations Report also found a moderate increase in targeted attacks. Breaches are not one dimensional, said Wade Baker, director of research and risk management at Verizon Business. Organizations often have a social engineering element, a malware element and a hacking element to an incident, Baker said.

“There are attackers that seek out whatever organizations they can exploit using a particular method because they are there to find easy targets, and then there are attackers who are targeting specific organizations,” Baker said. “You’ve got to ask yourself: In your organization, do you possess data or are you an organization that someone would preselect as a target?”

There are a variety of ways to mitigate the threat of targeted attacks. In addition to security awareness training for end users, organizations need to bolster patch management for applications running on endpoint machines, said Marc Maiffret, chief technology officer at vulnerability management vendor eEye Digital Security, in a recent interview with SearchSecurity.com. Most organizations lack a real process for assessing and remediating vulnerabilities, Maiffret said. For attackers, using a zero-day is simply overkill because a lot of businesses have endpoint machines running software that is not up to date.

“ The reality is there are so many organizations and solo attackers who have a significant number of zero-days,” Maiffret said. “A lot of times when businesses are being compromised these days it’s still through normal, everyday Adobe- and Microsoft-related flaws, and typically they are not even zero-day vulnerabilities.”