Threat Report: In Cyber Wars, Hackers Are Gaining Ground

Posted: 4/20/2015 - 2 comment(s) [Comment] - 0 trackback(s) [Trackback]
Tags: Collaboration, Security

By Drew Doggett

It's not a matter of if you'll get hacked – it's when.

Attackers are evolving faster than the defenses they attack, and conventional threats, such as phishing and watering hole attacks, continue to expand and produce results, according to the 2015 Internet Security Threat Report released last week by Symantec. Among its findings:

- One out of every 965 emails was a phishing attack last year
- Five out of six large companies (those with 2,500 or more employees) in the U.S. were targets, in 2014, a 40 percent jump from 2013
- New attack platforms are emerging: Symantec found that 17 percent of all Android apps available last year –nearly 1 million apps – were actually malware in disguise
- 70 percent of social media attacks rely on the initial victim to spread the threat to others Hackers don't need to break down the walls behind every computer within a network – it only takes one crack to infiltrate an entire system.

But while attackers are gaining sophistication, vendors are falling behind. Symantec found that vendor response times are slowing down.

On average, vendors took 204, 22 and 53 days respectively to release a patch in the three most-exploited zero-day vulnerabilities. That's compared with a four-day average in 2013. And malware is proliferating. More than 317 million malware programs were created last year – nearly 1 million a day.

While spam accounted for 60 percent of all email sent last year (slightly down from 66 percent in 2013), attacks are more dangerous and precise than ever. Attackers used 20 percent fewer emails than last year to successfully breach their targets. They don't need their attacks to be exact to succeed – they just need one employee to be careless.

Fighting Back
So what's an organization to do?

John Carlin, Assistant Attorney General, National Security Division, Department of Justice, said the best defense is one that is so fortified that it fatigues hackers into submission.

"That means upping our game until we change the behavior of our adversaries, but we need to move quickly to do it," Carlin said during the Symantec Symposium in Washington, D.C.

Stepping Up
Former FBI Director Robert Mueller, also speaking at the Symposium, said organizations must get better at responding to cyberattacks and information sharing among government and industry. That's been a challenge, historically, as neither was inclined to let others know of their problems.

"In my mind, there's an incentive to share information," Mueller said.

Call Them Out
Carlin agreed that the U.S. government must be more vocal, as it was following the Sony attack, when President Obama publicly called out North Korea, and the president sanctioned the country. Obama later issued an Executive Order allowing the U.S. to sanction bad actors for their malicious activity.

"We can't be afraid to say who did it, whether it's a nation state or a terrorist group," said Carlin.

New Enemies, Same Threats
The Threat Report profiles the hackers as well as the hacks. Organized criminal gangs took credit for 312 major breaches against companies last year – up 23 percent from the 2014 report.

Carlin sees a growing number of terrorist groups and nation-state attacks in the future.

"It's not enough to detect threats," Carlin said. "We have to find a way to disrupt them and provide deterrents against those who think they can steal with impunity."

Join the conversation. Post a comment below or email me at adoggett@300brand.com.

MeriTalk News

Comments (2)

Write Something...

Allowed HTML Tags: b,img,a,br

Enter the words to the left:

Post Comment

MeriTalk Visitor 4/30/2015 12:59 PM

Training must increase so we can "think" before we act

MeriTalk Visitor 4/21/2015 8:49 AM

I agree, email seems to be vector of choice, phishing attacks are hard to stop, spam is easier to address, and vendor tools don't always work together, again a layer approach, with prevention at the frontend, then detection, with recovery and mitigation the last resort.