Hacking Firestorm Rages Through Internet

Doug Bernard

April 13, 2015

First came reports that Lenovo's "Superfish" software was designed to intentionally break secure connections and steal users' private data.

Then, Gemalto – the world's largest SIM card manufacturer – announced it had "reasonable grounds" to conclude British and American intelligence services stole the firm's encryption keys for billions of mobile phones.

Next, the cyber security firm Kaspersky Labs revealed that cyber-criminals, using a new bit of malware dubbed "Carbanak." quietly stole upward of $1 billion from dozens of European banks before anyone caught on. And then came "Fanny," a newly discovered package of crypto-worms and viruses with close similarities to Stuxnet that began turning up on thousands of computers, permanently destroying their hard drives.

These reports came out in the span of just one week recently. And the news may get progressively worse.

A recent poll of Internet security professionals at a major cyber security conference found that 93 percent of respondents said hacking will only get worse in the coming year, with 44 percent believing the U.S. is losing the battle against hack attacks.

There's an emerging consensus among analysts about what needs to be done about it and how individuals can defend themselves.

Digital 'Wild West'

"Twenty five years ago, I could never have imagined all this (hacking)," said cyber security expert Bhavani Thuraisingham. "It's almost like we're being attacked from every direction and everyone is attacking everyone else."

Now a professor at the University of Texas – Dallas, and director of the school's Cyber Security Research Center, Thuraisingham spent many years working in the field of cyber-security before anyone knew what to call it.

She said that hack attacks have been on an upswing lately, and is quick to caution that the situation is likely to get "much worse" before it starts getting better.

“The bad actors, they only have to get one thing right once, whereas we have to be correct 100 percent of the time.” Thuraisingham said. “It’s almost like terrorism. We need to focus much more on the prevention methods because that’s really what we need if we want to stop this.”

Top on her list of prevention methods are hacking prediction models. Thuraisingham said the models, still under development, would allow security professionals not just to plug security holes once they’ve developed but also to predict attacks before they happen.

“We’re always dealing with the immediate problems right in front of us, much like cleaning up the broken china once it’s hit the floor,” she said. “If we’re going to really defend ourselves, we have to get out in front of the problem.”

The explosion of hacking attacks is something that’s not likely to go away any time soon, analysts say.

“We’re kind of living in what amounts to a digital wild west. This is something that folks are going to have to adapt to,” said Patrick Eddington, a policy analyst at the libertarian-leaning Cato Institute.

Eddington said these attacks come from a wide array of sources including organized crime, crypto-anarchist groups, corporate spies and state-sponsored groups, such as “Unit 61398,” a hacking operation allegedly run by China’s People’s Liberation Army.

“If you look at the polling, you do find a tremendous amount of concern over what’s going on,” Eddington said. “But it hasn’t as yet translated into a sustained level of pressure on lawmakers. That may stem from the fact that, in people’s daily lives, they’re much more concerned about keeping a roof over their head, keeping their job, getting their kids through school.”

The encryption debate

One tool both Eddington and Thuraisingham say can help stop, or at least slow many hacks, is encryption.

“If you’re not encrypting, it’s like not locking your door when you go to sleep,” Thuraisingham said. “It’s a protection but it’s not fool-proof. A lock-pick could still get in. But a lock, like encryption, deters most people.”

That may be, but elements in the U.S. government, most notably the FBI, have issued a series of warnings about the spreading use of encryption, and the potential for misuse by criminals or terrorists.

Last fall, FBI Director James Comey compared encrypted devices to safes that could never be opened, putting a wealth of potential helpful information for law enforcement permanently out of reach.

“If the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place,” he said.

More recently, Rep. John Carter (R-TX), chair of the House Homeland Security Appropriates Subcommittee, echoed Comey’s concerns.

“I don’t know anything about this stuff,” he admitted at a recent hearing, adding that “invaders from around the world (are) trying to get in here. If that gets to be the wall, and even the law can’t penetrate it, then aren’t we creating an instrument that’s the perfect tool for lawlessness?” he said.

But analysts say U.S. officials are sending mixed messages.

“The FBI was for encryption before they were against it,” cyber security expert Eddington said. “If you go back to fall 2012 when different malware attacks – like Finfisher – were going on, the FBI was *encouraging*people to use encryption to help protect themselves. These hacking attacks are helping to bring this fundamental conflict to the surface.”

The encryption debate is unlikely to be settled anytime soon, and it will likely be years before hacking prediction models will be robust enough to defend against potential attacks.

So what can be done?

Analysts Eddington and Thuraisingham – as well as many other cyber security analysts – say it’s critical for everyone online to practice “good Internet hygiene.”

“Change your passwords,” Thuraisingham said. “Update your software. Don’t click on links or attachments that people you don’t know send you. Stop putting too much stuff on Facebook. That’s clean hygiene.

“And use encryption as much as possible, so at least if you’re hacked,” he said. “It’s still encrypted.”