RSA Breach: Not the First, Not the Last

By Terry Cutler on April 01, 2011

Go ahead and click on the Viagra emails you've been warned about. Hackers don't need to appeal to your libido to break into the company computer system. They have other compelling ways. These days they've been hanging around inside the network, building up profiles on company employees. By the time they have enough information and let loose their malware, you won't even know that you were an unwilling accomplice in an advanced persistent threat.

Very recently, **RSA revealed that it had been victimized by an APT**. Company investigators said the attack resulted in sensitive customer information extracted from RSA's systems, in particular critical information related to its SecurID, two-factor authentication products which are used by approximately 30,000 customers worldwide. The two-factor authentication uses an online password and a second form of authentication, such as an access card for online security.

How do hackers do it? Hackers get access into companies like RSA through **APTs** by acquiring sufficient information about a particular user. Once the hacker feels there is enough information, the hacker sends out a compelling email with an attachment or link. You would never think it was a fake, as it is something the user would expect, and appears to be from someone they know.

So, it could say, "John, here is the information about the Ottawa office and here are some details. Click on the link." The email appears to have come from inside the company. So, a user clicks on it and malware is downloaded to the computer.

At this point, the hacker has access to your computer.

The technology has been unbreakable for many years, but if the attackers have access to the source code, they'll have all the time in the world to reverse engineer and study how the system works.

Eventually, they will figure out the algorithm and break into the rest of the company. What we need to remember is that most firewalls are configured for what is called state full inspection. This means everything coming to the company network is blocked, but internet traffic going out is not. Once you open up that compelling email, it becomes a case of you called me and invited me into your house. Because I am using an encrypted channel like SSL, the technology inside most companies cannot locate me. I am a ghost and I can use your computer to search other company computers.

Let's say the hacker wants access to specific information and the computer he hijacked doesn't have the proper rights. He'll have to find someone else in the company, like a CEO or someone in IT, with access. From there, he can craft another compelling email and the victim will also open the link to the attachment, thereby inviting the malware. Now the hacker can hop from computer to computer.

Gone are the days of enticing people with Viagra or Cialis. Now it is about building up enough information about a

Most Read | Most Recent

- Hacker Uses XSS and Google Street View Data to Determine Physical Location
- The Rise of the Small Botnet
- An Inside Look at Hacker Business Models
- Defense Department's Cyberwar Credibility Gap
- ATM Hacking Video - Barnaby Jack Demonstrates ATM Hacking at Black Hat USA 2010
- Are Nigerian Scams From Nigeria?
- The Top Five Worst DNS Security Incidents
- The Three Providers Who Decide Whether You Will Be Hacked
- The Root is Signed with DNSSEC - Now What?
- China's Cyber Threat Growing
- Reports: Eugene Kaspersky's Son Returned After Ransom Paid
- Verizon Helps Boost iPhone Enterprise Adoption, According to Report
- Working Compliance - Use Every Advantage You Can Get
- Enterprise Attacks by Mobile Devices Not Fully Realized

target to make emails look real and compelling. Someone wanting to get inside your network can send you a convincing email saying, “It was great meeting you at a certain event,” an event you actually attended. Most of the time they'll offer you a link to photographs. Or they get in through Twitter with a shortened URL, which are very hard to detect.

Are hackers more advanced? No, but they have found easier ways to hit their targets. The only way around this is to train company employees in security awareness and educate them on the different types of hacking. This isn't happening as much as it should, with overworked employees and high turnover.

This knowledge is important outside of the office, when employees go home. For example, an employee downloads a bit torrent client on the corporate laptop. The next morning he returns to work and connects. Now the company system is running bit torrent software and hackers can get into the company and identify weak spots. Even with training, employees are still the number one threat to a company, even after they are terminated. A disgruntled former employee could collaborate with a talented hacker for revenge. There is no way to stop a hacker, we can only make it harder. They always go for the lowest hanging fruit. If a new authentication mechanism is hard to break, they are going to bypass the security by trying to locate a weakness somewhere else in the system.

In the next few years we can expect to see three-factor authenticity. We will see more biometrics technology. For example, let’s say an iPhone user wants to login to the corporate network via his phone through the built-in camera. Three-way authentication could mean facial recognition, fingerprint recognition and a password. You will need all three to match before the authentication will authorize you. This could be part of a company’s new defense strategy, for as long as it keeps hackers away.

For companies, the way around this is to constantly test and assess, have some type of 24/7 alarm system, and security information and event management.

The danger is getting worse, and most breaches are detected 3 months later, even though traces of the attack have been in the logs the entire time. Hackers have penetrated the Nasdaq, the government, and hacked into the U.S.A watch dog company, HB Gary. It is only a matter of time before these hacktivist groups say enough is enough and shut down the U.S government, the financial systems or the electricity grid. This is the future terrorist attack. With so many companies being violated, hacking has become a harsh reality. I tend to agree with Doug Kass, the well respected hedge fund manager who predicted that a successful **cyber attack on financial systems** is inevitable, and could potentially lead to significant losses for many as a result.

To coin a phrase from Diehard 4, “The future is holding a fire sale.”

Terry Cutler is a co-founder of Digital Locksmiths, Inc., an IT security and data defense firm based in Montreal and serves as the company's Chief Security Evangelist and Certified Ethical Hacker. Prior to joining Digital Locksmiths, he was a Premium Support Engineer for Novell in Canada where he analyzed network vulnerabilities and transitioned security technologies into production. In addition to being a licensed private investigator in Canada, Terry is an internationally known author, trainer, speaker, and security consultant, Terry has appeared in numerous national television and radio programs and is very active on the conference circuit. Follow Terry on Twitter at @TerryPCutler

Previous Columns by Terry Cutler:

- RSA Breach: Not the First, Not the Last
- Did Patriot Hackers Attack the Canadian Government?
- A Compliance with a Complex Problem
- Beating Back the Botnets
- Enterprise Security Priorities for 2011

Tags:

INDUSTRY INSIGHTS

Cybercrime

- Trustwave Files for IPO, Reveals Finances
- Hacker That Possessed 675k Stolen Credit Cards Pleads Guilty
- The TLA World of Information Security
- Deploying DKIM for Increased Email Deliverability
- Woman Pleads Guilty to Selling Counterfeit Software With a Street Value of $2M
- Raytheon Launches Mobile Cross Domain Access Solution to Support Remote Workers