



SPEED MATTERS
It's time to ditch your antivirus

TRY VIPRE ANTIVIRUS BUSINESS

FREE 30-DAY TRIAL

smarter technology

Get info and resources from IT industry experts.

VISIT SMARTER TECH



IT Security & Network Security News

RSA SecurID Breach Is a Lesson in APTs

LinkedIn
 Twitter 14
 Facebook 3
 +1 0
 Share

By: Fahmida Y. Rashid
2011-03-29
Article Rating: ★★★★★ / 1

[There are 0 user comments on this IT Security & Network Security News & Reviews story.](#)

While security researchers have been talking about advanced persistent threats for some time, RSA's SecurID breach has thrust APTs to the forefront as the biggest danger to organizations.

While customers are understandably concerned about the security of their SecurID deployments, the RSA breach is a wake-up call about the recent increase in what security experts call APTs: advanced persistent threats.

Attackers had successfully breached the RSA's networks and stolen information related to the company's SecurID two-factor authentication technology, revealed Art Coviello, the executive chairman of RSA Security, in an open letter to customers posted on the RSA Website on March 17. RSA identified the attack as an APT in its letter.

APTs are ongoing attacks where perpetrators probe the target systems looking for information such as source code and other sensitive intellectual property. APTs are a "new breed of cyber-adversary" and cannot be addressed in the same way as other Web threats, Adam Vincent, CTO of the Public Sector group at Layer 7 Technologies, told eWEEK.

The attackers are well-funded, highly organized and are most likely employing new techniques—ones that are probably not protected by network encryption, firewalls and other security products, Vincent said. Security products can't provide sufficient capabilities to protect an organization from APTs as the lurking attackers are often indistinguishable from legitimate users, he said.

Operation Aurora, which compromised systems at Google and a number of other major companies in 2009, was a type of APT. "If Google and Aurora wasn't enough of a wake-up call, this is another wake-up call," said Peter Schlamm, vice president of product management at Solera Networks, told eWEEK.

The general consensus appears to be that if RSA can fall, then there's little chance for smaller companies. So organizations need to do more than just spend money to block threats, Chris Larsen, head security malware researcher at Blue Coat Systems, told eWEEK. They need to assume they are already infected and invest in security technologies, such as network forensics and log management systems, that will allow them to find the breach, he said.

While RSA has remained silent about what was stolen, when the data breach occurred, how attackers got into the network and how long the breach lasted, the company recommended that customers harden their other security layers in case of a follow-up attack.

"A layered security approach is always best," said Avivah Litan, a distinguished analyst at Gartner. While one-time password [OTP] systems "raise the bar for the criminals," they were vulnerable to compromise even before the RSA breach, she said. "Maybe this incident will wake up companies to the need for more controls than just OTP authentication," she said.

Assuming that the attackers stole the seed values used to generate the one-time passwords on the SecurID tokens, a potential scenario has cyber-criminals leveraging social engineering and spear phishing tactics to obtain the serial number of the SecurID token. With that serial number and seed values in hand, attackers can masquerade as the user to log in to secured networks, such as those in financial institutions.

The scenario isn't all that dire: It just means that RSA customers will need to replace the tokens, according to Kyle Adams, architect and lead developer at Mykonos Software. "The actual two-factor authentication technology remains secure, and it's just some key information that was lost," Adams told eWEEK.

If customers feel that SecurID is compromised, they are likely to replace it with

Rate This Article:

Poor Best

E-mail
 PDF Version
 Print

eWEEK Videos Newsbreak Videos

All Videos

Today's Featured Video

Understanding Hybrid Routing For Managed DNS
03:43
Watch Now>

Newest Videos

03:46
 03:16
 03:06
 02:54
 03:43
 03:04
 06:43
 03:19

Videos sponsored by

Suggested Related Content:

Articles Labs/How-To

Multimedia

Visit the Internet Infrastructure Service Center for resources, videos, blogs and polls. (Sponsor)

- RSA Data Breach Highlights Value of Network Forensics Technology (2011-03-19)
- RSA Warns SecurID Customers of Data Breach (2011-03-18)
- Cyber Criminals Nab RSA SecurID Information in Breach (2011-03-19)
- CA Woos RSA SecurID Customers After Data Breach (2011-03-30)
- EMC Acquires Security Automation Vendor NetWitness (2011-04-04)
- EMC Will Roll Security Automation Vendor NetWitness Into RSA (2011-04-04)
- CA Capitalizes on RSA SecurID Breach with a Token Trade-in

SUBSCRIBE TO eWEEK

AdChoices ▶

Free NIST Compliance Info
Whitepaper. Get All the Facts About NIST Compliance. Download Today.
www.LogRhythm.com

Unified Security Anywhere
Adaptive, Predictive Cloud Security for Cloud or Hybrid Environments.
www.globaldataguard.com

10-TB Solid State Disk
eMLC, 320,000 IOPS, 4-GB/s, 1U The World's Fastest Storage® by TMS
RamSan.com/products/R...

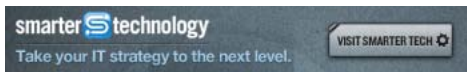
Data Security
New Technologies from Oracle. Learn More. Free Download.
www.quberasolutions.com

Cloud configuration

High volume configuration. Requires a new approach. Download Puppet www.PuppetLabs.com/CL...

competitor products. In fact, CA has announced that SecurID customers can trade in their RSA tokens in a one-for-one swap for CA's own authentication platform, the CA ArcotID Secure Software Credentials.

[LinkedIn](#)
[Twitter](#) 14
 [Facebook](#) 3
 [+1](#) 0
 [Share](#)



Post a new comment

Login [f](#) [t](#) [g](#) ...

Post

0 Comments

[>>> More IT Security & Network Security News & Reviews Articles](#)
[>>> More By Fahmida Y. Rashid](#)

[Email Article To Friend](#) ?
 [Print Version Of Article](#) ?
 [PDF Version Of Article](#)

FEATURED SPONSOR VIDEOS

[Benefits of Workload Optimization](#)

[What Smart Companies MUST Learn from Gaming](#)

[Advances in Authentication](#)

[Vertical Markets Benefit from Workload Optimization](#)

[View More Videos](#)



FEATURED SPONSOR MESSAGE

[Internet Infrastructure Service Center](#)

Visit the Internet Infrastructure Service Center to cast your vote on the infrastructure issues IT professionals face today.

[Click Here](#)

Brought to you by



- NetApp's Mendoza discusses how MLB utilizes data
- Managing Regulatory Change in 2011 and Beyond
- New expert blog about automating and improving business decisions.
- Deliver business data to iPads and iPhones
- Developers—learn how Web apps can win Ultrabooks
- Get 3X Performance with Check Point Appliances
- Keep your business connected between the dots with cyber security from Verisign.
- Colocation Buyer's Guide: Making the right decision
- Secure your mobile enterprise with Zenprise
- Free Whitepaper – Replace Tokens With Phone Authentication
- See how Verisign keeps your business connecting between the dots.
- Start your free trial for VeriSign>> verisign.com/ssl/free-30day-

SUBSCRIBE

APPLY FOR A FREE SUBSCRIPTION BELOW:

First Name: Last Name:

Title: Company:

Address: City:

State: Zip Code:

Email:

SUBSCRIBE



- > Try digital eWEEK
- > Renew today
- > Subscription help
- > MORE FREE SUBSCRIPTIONS

Marketplace (Sponsored Links)

Real-time insights from Google Analytics
 Make better marketing decisions faster. Google Analytics Premium. One flat fee. www.google.com/analytics/premium

Simple, Secure Sharing From Anywhere
 "The cost savings with Box made it a no-brainer." – Balfour Beatty Construction www.box.net

Simple, Secure Sharing From Anywhere
 "Box is the quickest and easiest way to share files, period." – Six Flags www.box.net

Spam & Virus Firewall www.barracudanetworks.com
 Real-Time Protection with Lowest False Positives. Free Eval Units!

AdChoices