http://www.computerweekly.com/news/1280095593/RSA-discloses-phishing-attack-data-breach-details

RSA discloses phishing-attack data breach details

RSA, the security division of EMC, has revealed the firm's data breach in mid March was the result of a spear phishing attack. The spear phishing attack exploited an Adobe Flash vulnerability that was unpatched at the time.

RSA quickly reported it had suffered a breach of information related to the firm's SecureID two-factor authentication product, but has since been tight-lipped on details.

The company has faced strong criticism of its approach, but the secrecy was aimed at keeping the attackers in the dark as much as possible while the breach was being investigated, executives told Computer Weekly.

In a conference call with analysts on Friday, however, RSA revealed that a small group of RSA employees was targeted by phishing e-mails.

According to Gartner analyst Avivah Litan, the phishing e-mail displayed the title "2011 Recruitment Plan" in the subject line.

The e-mails landed in the users' junk folders. "At least RSA's SPAM filters were working, even if their social engineering training for employees was not," Avivah Litan wrote in a blog post.

Attached to the e-mail was an Excel spreadsheet with recently discovered Adobe Flash zero day flaw CVE 20110609.

With the trojan downloaded, the attackers harvested credentials and made their way up the RSA food-chain via both IT and non-IT personnel accounts, until they finally obtained privileged access to the targeted system, said Litan.

The targeted data and files were stolen and sent to an external compromised machine at a hosting provider. RSA saw the attack, using its NetWitness, and stopped the attack before more damage could be done.

"RSA came clean and told its customers immediately about the attack (which is something other companies have not done) and should be credited for handling a bad situation as well as it can," said Litan.

But, she said, they relied on yesterday's best of breed tools to prevent and detect the attack, which means RSA was unable to stop the attack in real time.

RSA sells fraud detection systems based on user and account profiling which use statistical Beysian models and rules to spot abnormal behaviour and intervene in real time to re-authenticate users and verify the authenticity of suspect access, behaviour or transactions.

"They should have applied these techniques to their own internal systems. They need to stay innovative and apply the lessons learned from serving their clients to their own internal enterprise systems," said Litan.

RSA needs to make it possible for the innovation to bubble up quickly into products and services they not only sell and implement at customer sites, she said, but that they use themselves internally.

---

http://searchsecurity.techtarget.com/news/1529523/RSA-SecurID-breach-began-with-spear-phishing-attack

RSA SecurID breach began with spear phishing attack

Robert Westervelt, News Director

The assault against RSA, the security division of EMC Corp., began with two waves of spear phishing attacks using an attached Microsoft Excel file, which targeted an Adobe Flash zero-day flaw.

“The bottom line is that these attacks can be stopped and they have been stopped by other companies that are more prepared. Avivah Litan,, Vice PresidentGartner Inc.”

The phishing attacks took place over a two-day period and targeted two small groups of low-profile employees. Attackers were successful in getting at least one employee to retrieve it from their junk mail folder and open the Excel file titled "2011 Recruitment plan.xls." Eventually, attackers gained access to critical systems. A NetWitness early detection system discovered the anomaly, alerting incident response teams while the attack was in progress, but not before attackers could make off with details about the company's SecurID two-factor authentication products.

Uri Rivner, head of new technologies, identity protection and verification at RSA, shared the first details of the RSA SecurID attack since March 22, when the company warned that information related to its SecurID products was stolen.

According to the details released last week, the attackers installed a backdoor and a variant of the Poison Ivy remote administration tool, to reach out to a remote command-and-control server and navigate through RSA's sensitive systems. Once in, the attackers shoulder surfed on the victims, mapped the network and the resources, and started looking for a path to the coveted assets they desired, Rivner said.

"The attackers first harvested access credentials from the compromised users," Rivner said. "They performed privilege escalation on non-administrative users in the targeted systems and then moved on to gain access to key high value targets, which included process experts and IT and Non-IT specific server administrators."

Once the attackers removed data from the servers of interest, they moved it to "internal staging servers where the data was aggregated, compressed and encrypted for extraction," Rivner said.

The data was transferred via FTP using password protected RAR files to an external compromised host. Once there, the attackers removed the files to eliminate any traces of the attack.

More on RSA and SecurID:
RSA SecurID breach fallout should be limited, experts say:
Experts say the risk of an attack that exploits stolen proprietary data on RSA's SecurID products is low, but it can't be completely dismissed until attack details are revealed.

RSA breached in APT attack; SecureID info stolen:
Company warns customers that SecurID product data was stolen in sophisticated attack.

While RSA's NetWitness network monitoring system detected the attack in progress, the company failed to have a process in place to reauthenticate suspicious users, said Avivah Litan, vice president at Gartner Inc. In an interview with SearchSecurity.com, Litan said other companies have been successful in stopping similar attacks by deploying layered defenses. For example, many financial firms use secure browsing technologies to monitor end-user interaction with third-party websites in combination with on-site network monitoring, Litan said.

"The bottom line is that these attacks can be stopped and they have been stopped by other companies that are more prepared," said Litan, who was among several analysts briefed on the attack. "There was abnormal user behavior, which [RSA] did detect, but they didn't have an inline process to stop it."

Jon Oltsik, principal analyst at Milford, Mass.-based consulting firm Enterprise Strategy Group, who was also briefed by RSA on Friday, said the attack raises concern that current security technologies are failing to protect against savvy social engineering attacks. "Pretty much anyone can be breached at any time," Oltsik said, adding that it will likely take a major event, like a lengthy power outage before any progress is made.

"We definitely need to improve our technologies, but this is not a technology problem," Oltsik said. "This is a con. Cybercriminals are preying upon human behavior to trust other people. You can deploy all the technology available, but this shows that it's easy to dupe people and overcome that technology."

RSA said response teams were called in to isolate the attack and investigate the breach and within nine hours the company's crisis response plan was thrown into full gear. Support staff and engineering teams were conducting briefings with affected customers, many of those briefings under non-disclosure agreements, based on the customer's specific exposure.

RSA continues to be tight lipped about exactly what part of its two-factor authentication technology was stolen.

In the RSA SecurID system, users are given a keyfob with a token code that changes randomly. Users also set their own four- to eight-digit PIN number. The PIN number and token code is combined into a password to access a secure server. In a worst case scenario, explained Rob VanderBrink, writing about the RSA attack in the Sans Institute's Storm Center diary, cybercriminals could have "obtained a complete or partial customer list, complete with seeds and serial numbers." Serial numbers are assigned to users of SecurID by the customer's RSA SecurID ACE management server. The seed is the encryption key, assigned by RSA. Sources close to the

investigation also wouldn't disclose specifics, but said the NetWitness early detection system enabled the company to ensure the attackers "didn't empty the coffers of RSA or SecurID."

---

http://searchsecurity.techtarget.com/news/2240036563/RSA-responds-to-SecurID-attack-plans-security-token-replacement

RSA responds to SecurID attack, plans security token replacement

Robert Westervelt, News Director

RSA, The Security Division of EMC Corp. will replace SecurID tokens for some of its largest customers following several attacks against government contractors believed to involve weaknesses with the two-factor authentication mechanism.

Tokens created by RSA after the attack should not be vulnerable, assuming that RSA's new precautions are effective.

Mark Diodati, authentication expert and research vice president, Gartner Inc.

In an open letter to RSA SecurID customers issued Monday, RSA President Art Coviello confirmed that the attack on Lockheed Martin used an element of SecurID. Coviello said RSA has already replaced tokens at government agencies and companies in the defense sector "as an additional precautionary measure." Bethesda, Md.-based Lockheed thwarted the SecurID attack before cybercriminals could access its sensitive systems. The company told the *New York Times* that it was replacing 45,000 SecurID tokens.

Coviello said RSA would extend its replacement program, offering to provide SecurID tokens for customers with "concentrated user bases." The company is also offering monitoring services to its financial industry customers, typically large banks and brokerage firms. RSA said those firms, using SecurID for consumers, would receive "risk-based authentication strategies" to protect web-based financial transactions.

More on the RSA breach:

Contractor attacks via SecurID tokens fuel call for data security reassessment:
Security pros advocate a reassessment of security processes and technologies in the wake of breaches that may be tied to RSA SecurID weaknesses.

Survey finds users re-evaluating two-factor authentication options:
In the wake of the RSA SecurID breach, a vendor survey finds a reduced level of confidence in the security provided by tokens.

RSA SecurID breach began with spear phishing attack:
Two waves of email attacks targeted small groups of RSA employees, the company said in a blog post revealing details of the attack.

“We remain highly confident in the RSA SecurID product as the leading multi-factor authentication solution and we also feel strongly that the specific remediations we have provided to customers will help to deliver the highest levels of customer protection,” Coviello said. “However, we recognize that the increasing frequency and sophistication of cyber attacks generally, and the recent announcements by Lockheed Martin, may reduce some customers' overall risk tolerance.”

RSA has been notably quiet since it acknowledged a breach of its systems in March that exposed its SecurID authentication technology to cybercriminals. In an earlier interview with SearchSecurity.com, a source close to RSA, confirmed that the company would replace security tokens for “high risk customers.” The company also retooled its SecurID manufacturing processes and supply chain management practices.

The recent contractor breaches show that the tokens associated with the stolen information should now be considered compromised, wrote Mark Diodati, an authentication expert and research vice president at Gartner Inc. In a June 2 blog entry, Diodati urged customers to demand new SecurID tokens. “The delivered tokens must be manufactured after implementation of RSA’s post-attack security procedures,” he wrote.

“The reputation of the RSA SecurID OTP technology may be badly tarnished due to this attack. However, the real damage is limited to the token information that was stolen. In other words, tokens created by RSA after the attack should not be vulnerable, assuming that RSA’s new precautions are effective,” Diodati wrote.

Security experts recommend firms using SecurID reassess user access rights within their organization. Remote access to an organization’s most sensitive systems could be denied until further controls are put in place. A third-factor authentication measure can also be used for employees that must access sensitive data, said Nils, a prominent white hat hacker and head of security research at U.K.-based MWR InfoSecurity.