



J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294

RSA- Hacked but not un-Witnessed

It's now been about 3 weeks since the famed two factor authentication end user token system, SecureID was hacked. It had long been assumed that this system was hack proof given its record of security enablement at some of the largest corporations and government agencies. Yet in the end, like most security breaches, it was compromised as a result of human error and not holes in the technology. Its important to note exactly what happened, as it indicates why current end user security models are flawed and why I recommend implementing new comprehensive models just emerging that will enable the next generation of protection in an increasingly sophisticated world of cyber attacks on companies and individuals.

While all the details are not yet public (RSA rightly wants to keep some of the lower level details private to prevent copy cat attacks), enough of the details have surfaced that companies can learn from and hopefully prevent similar attacks. In a nutshell, a "phishing" email was sent to some lower level personnel entitled 2011 Recruitment Plan that included an Excel spreadsheet with a zero-day exploit Flash file. One or more of the recipients opened the file, thinking it was legitimate. The exploit then retrieved the user ID and password and established a connection on the SecureID server, where it gathered a number of data files, and transferred them to a compromised staging server at a hosting provider. From there, the data was transferred to a remote server.

What is important to note is that RSA was able to catch this breach in process, and halt it in near real time (although it was not able to prevent at least some sensitive information from escaping). This extraordinary defense was mounted because RSA was not just looking at log-in authorization and credentials, but was monitoring and analyzing all traffic exiting its network. As a result, RSA was able to determine that this connection was making unauthorized use of sensitive data, and was able to rapidly cut off access. This real time monitoring and analysis is the key to ensuring future security against new-age data breaches, but which very few companies currently have in place. It's nearly impossible to prevent human error created invasions like this one where a user opened an infected file. No traditional PC-installed AV or anti-malware solution (e.g., McAfee, Symantec) prevents this. And as these so called Advanced Persistent Threat (APT) attacks become more sophisticated (often through sponsorship of state funded actors or other well financed hackers), the types and amount of data loss will grow,

I believe that data protection must dramatically and fundamentally change if enterprises want to protect their most valuable assets (also see our research brief entitled *Dramatic Changes Coming in Endpoint Security*, January 2011). It is no longer safe to protect only your endpoint. It is now mandatory to encompass a fresh approach where all data be monitored and checked before exiting the corporate firewall as to whether or not it should be made available to the outside world, including to “trusted” remote users. This requires high speed packet interception, examination and evaluation, and must be done in real time if protection is to be effective. It’s why many of the security companies like McAfee and Symantec are moving to more cloud-based interactions, and it’s why companies like Cisco, Juniper, etc. are becoming security companies as well as network infrastructure companies.

Employing this changing landscape of security technologies is even more critical as companies adopt a cloud-centric position. Companies that provide cloud-based access, whether through internal servers or via a service provider, must have a network based “watch-dog” service or face an increasing amount of escaped data and undetected exploits. To provide such services RSA has announced it is purchasing NetWitness, a company that monitors all data packets over the network, deconstructs the packet, and evaluates the contents based on pre-determined rules. It then prevents or allows the data to exit the corporate network, all in real time. In fact, RSA used this technology to discover and stop the attack on Secure-ID in near real time.

Data monitoring and remediation in real time is what is required to secure data in our hyper-connected world by scrutinizing data content and behavior and stopping any breaches before they escape, regardless of the human or technology errors that allow it to happen. Other Cloud services based providers (e.g., Cisco, Microsoft, Amazon) must have a similar solution or face a competitive disadvantage and expose a huge security hole. And of course, RSA which is owned by EMC, will no doubt make this capability a key component of EMC’s cloud-based offerings. Organizations concerned with security must demand such services if they are to protect their data from loss. And private clouds (i.e., behind the corporate firewall) must include a real time data monitoring component to provide next generation security and data leakage prevention.

Bottom Line: Enterprises will have to migrate to newer models of security in the never ending fight against increasingly sophisticated hackers and growing data loss which may even go undetected. While traditional endpoint solutions will not go away, they can not prevent the phishing/human error APT and zero-day attacks becoming more common. Real time packet monitoring to evaluate and control data on the network is the next important step in securing corporate assets, and must become a component of all enterprise security operations and especially in cloud-based systems. This is the only way to discover and stop the increasingly sophisticated attacks emerging from well funded expert hackers.

For more in-depth comments or analysis on this or other subjects, feel free to contact us.

Copyright 2011 J.Gold Associates, LLC. All right reserved.