www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1 800.652.4020

Fidelis Threat Advisory #1001

THE RSA HACK

September 9, 2011

Document Status: FINAL
Last Revised: 2011-09-28

Executive Summary

In March of 2011, a spear-phishing email containing an Excel spreadsheet with an embedded malicious Adobe Flash payload led to a serious security breach at security firm RSA. This breach allowed attackers to compromise the integrity of the RSA SecurID authentication system. Attackers subsequently used information obtained via this breach in attacks against military contractors such as Lockheed Martin, Northrup Grumman and L-3 Communications.

The phishing email originated from a spoofed email address that bypassed reputation-based email filtering, contained a Flash zero-day exploit for which no patch or IPS/AV signature existed and thus was able to penetrate all network perimeter and system-level defenses. Given that Adobe Flash has a history of serious security vulnerabilities and that client applications are notoriously difficult for companies to patch, it is highly likely that other zero-day Flash vulnerabilities will be discovered and used in attempts to penetrate other organizations. Because malicious payloads can be deeply embedded, traditional signature-based network methods are generally ineffective against this type of threat. Given that it serves virtually no business purpose to embed Adobe Flash content inside Microsoft Office documents, detecting and/or excising such content from payloads is recommended.

Threat Overview

The RSA hack consisted of three stages. The first stage was a spear-fishing email containing an Excel spreadsheet with an embedded, malicious Flash object. The second stage was the establishment of remote access via a Poison Ivy reverse tunnel. The third stage involved an unspecified series of internal privilege escalations and the eventual compromise of the RSA SecurID system. (Poison Ivy will be covered in a separate Fidelis Threat Advisory; few specifics are known about the methods used by the attackers to penetrate RSA's network after the initial breach, so this FTA describes only the initial exploitation.)

The malicious Flash object contained a zero-day exploit for which no patch existed and for which there were no AV/IPS signatures. The vulnerability was later assigned CVE number CVE-2011-0609. The email came from a spoofed email address that bypassed email security gateway appliances. Once on the system, the malware downloaded a specialized Poison Ivy toolkit and established a reverse tunnel. Attackers then used this reverse tunnel to mount further attacks.

Risk Assessment

Microsoft Office and Adobe Flash are ubiquitous, and while Office is relatively easy for most organizations to patch, Adobe Flash is far more challenging. Even if an organization were perfect with their patches, the exploit used in this case was a zero-day: it exploited an unknown and unpatched vulnerability. Given the ease by which the malware was able to evade traditional network defenses and given that it led to a serious enough breach of RSA's SecurID system that they were forced to reissue millions of tokens, the threat of a similar type of attack is extremely serious.

Indicators & Mitigation Strategies

Given the relatively high number of recently discovered Flash vulnerabilities and Adobe's poor application security track record, it is likely that another zero-day vulnerability will be utilized in this type of attack. Signature-based defenses will thus be of negligible use against cutting-edge threats. The unusual packaging of the threat is its greatest weakness: there exist few legitimate uses for a Microsoft Office document with embedded Flash and thus we recommend detecting and/or excising such an uncommon file when it appears in network streams.

The Fidelis Take

Fidelis has made a rule available to customers that detects and/or blocks Adobe Flash content in Microsoft Office documents when transmitted over the network. This rule is effective regardless of protocol, the degree of embedding, the vulnerability used, the delivery method chosen by the attackers, or the level of sophistication behind the social engineering attempts.

Further Reading

- Dark Reading, "Researchers Uncover The Email That Led To The RSA Hack", Tim Wilson, 8/26/11. http://goo.gl/Zujdi
- Channel Insider, "RSA to Reissue SecurID Tokens", Ericka Chickowski, 6/7/11. http://goo.gl/aXvWV
- Microsoft Technet, "A Technical Analysis on the CVE-2011-0609 Adobe Flash Player Vulnerability", 3/17/11. http://goo.gl/uhBpf
- Fidelis Security Systems, "Fidelis XPS Policy Pack (May 2011)." http://fidelissecurity.com/support