Anatomy of an Attack

Lessons Learned From the RSA Breach

Kevin Flanagan, CISSP, CISA
Director, North American Technical Consulting
RSA, The Security Division of EMC
Open Letter to RSA SecurID Customers

To Our Customers:

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems, and that certain information related to the RSA SecurID product had been extracted. We immediately published best practices and our prioritized remediation steps, and proactively reached out to thousands of customers to help them implement those steps. We remain convinced that customers who implement these steps can be confident in their continued security, and customers in all industries have given us positive feedback on our remediation steps.

Certain characteristics of the attack on RSA indicated that the perpetrator’s most likely motive was to obtain an element of security information that
• An Overview: What Happened?
• What We Learned
• How You Can Help
2 phishing emails
launch zero-day
lateral movement from low value to higher value targets with a focus on VPN compromise
attacker initiates separate network using obtained credentials
demonstrated knowledge of internal architecture
encrypt and transfer
resilient and resourceful

exploited people, switched connection techniques, changed tools, and disguised origin
What makes you a target? What kind of information? What about partners and supply chain? How vulnerable are you?

Reconsider your risk. What you can do.
What makes you a target?

What kind of information?

What about partners and supply chain?

How vulnerable are you?

Reconsider your risk
Anti-Virus is Ineffective

Don’t rely solely on signature-based detection
Set realistic goals
People are the weakness
The Kill Chain

Attack Begins
Exploitation

Exfiltration
Actions on Objectives

Compromise (Days)

Detection (Weeks)

Add Friction
(Preventative Controls)

Increase Visibility
(Detective Controls)

Time

AFP® Annual Conference
Solution Is Simple
Balance Detective and Preventative Controls

- Attack Begins
- Exploitation
- Compromise (Weeks)
- Detection (Days)
- Increase Visibility (Detective Controls)
- Attack Identified
- Add Friction (Preventative Controls)
- Exfiltration Actions on Objectives
Resource Shift: Budgets and People

Today’s Priorities

- Monitoring: 15%
- Response: 5%
- Prevention: 80%

Intelligence-Driven Security

- Monitoring: 33%
- Response: 33%
- Prevention: 33%
Get into board-level conversations

End-user awareness

Limit social media

Block high-risk sites
4 Guiding Principles

Security is not black and white
“Can you get some security on my PC?”

Security needs to balance business requirements
“The best firewall is a pair of wire cutters”

Understanding the threat is the best defense
“If you know the enemy and know yourself, you need not fear…”

Don’t underestimate the power of people
This is not computers attacking computers, it’s people attacking people
trust in the digital world

Kevin Flanagan, CISSP, CISA
Director, North American Presales
kflanagan@rsa.com
## Security Practices – Critical Checklist

<table>
<thead>
<tr>
<th>Business Risk Assessment – Critical Asset Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify most critical systems; ensure they are given the highest priorities for all hardening and monitoring activities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Directory and Exchange Hardening</th>
<th>Infrastructure &amp; Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize number of admins</td>
<td>Full and detailed logging &amp; analysis</td>
</tr>
<tr>
<td>Monitoring and alerting (Windows Event ID #566)</td>
<td>Tighten VPN controls</td>
</tr>
<tr>
<td>Two factor admin access from hardened VDI platform</td>
<td>Increase controls on crypto keys</td>
</tr>
<tr>
<td>Executable whitelisting on hardened DCs</td>
<td>Full packet capture at strategic network locations</td>
</tr>
<tr>
<td>Disable default account and rename key accounts</td>
<td>Network segmentation</td>
</tr>
<tr>
<td>Complex passwords (9 &amp; 15 Char)</td>
<td>Team trained and focused on APT activity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Accounts</th>
<th>Web Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review accounts for privilege creep</td>
<td>Block access to high risk and web filter categories</td>
</tr>
<tr>
<td>Change passwords frequently</td>
<td>Click through on medium risk websites</td>
</tr>
<tr>
<td>Do not embed credentials into scripts</td>
<td>Black hole dynamic DNS domains</td>
</tr>
<tr>
<td>Minimize interactive login</td>
<td>Authenticated internet access</td>
</tr>
<tr>
<td>Restrict login only from required hosts</td>
<td>DNS traffic analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Education</th>
<th>User Machine Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase security training for IT</td>
<td>Limit local admin and randomize PW- change often</td>
</tr>
<tr>
<td>Launch security improvement initiative</td>
<td>Increase patching regime</td>
</tr>
<tr>
<td>Regular education of users on phishing attacks</td>
<td>Enable security controls in applications</td>
</tr>
<tr>
<td>Regular education on social engineering</td>
<td>Deep visibility to identify lateral movement</td>
</tr>
<tr>
<td>Increase mail filtering controls</td>
<td>Limit use of non-authorized and unapproved software</td>
</tr>
</tbody>
</table>