Advanced Persistent Threat (APT)

Lethal Combination of Social Engineering and Technology

June 6th, 2011
Agenda

Headlines

Data Loss Perspectives

- The Bottom Line of Data Loss
- What is at Risk
- Data at Risk
- Conduits
- Threats
- Those Most Affected
- Professional Hacking

Case Studies

APT Case Studies

- Google
- RSA

APT Explained

- APT Definitions
- How APT works

What can we do?

Key take a ways
From the Headlines

Hackers Targeted Oil Companies for Oil-Location Data
By Kim Zeller | January 26, 2010 | 1:11 pm | Categories: Cybersecurity, Hacks and Cracks

Three U.S. oil companies were targeted in a coordinated hack that sought valuable information about new discoveries of oil deposits and other data, according to a new report in the Christian Science Monitor.

The attacks predated by two years recent intrusions into Google and other companies but shared some similarities with those attacks. Highly targeted malicious e-mails were sent to employees and customized spyware attempted to grab specific data.

The hackers sold the oil deposits at a premium.

Epsilon Data Breach Hits Banks, Retail Giants
By Fahmida Y. Rashid | 2011-04-14

Marketing company Epsilon is reporting a data breach that could affect the email addresses of thousands of customers of major banks, retail and hotel chains.

Epsilon, a large email marketing services company with a roster of A-list clients, reported a data breach that is impacting practically anyone who has ever signed up to receive a retail offer or alert through its email account. The company warned that thieves may use the information to launch a phishing campaign to trick users into disclosing more critical data.

On March 30, Epsilon detected "an unauthorized entry" into its email system. During this time, a subset of clients' customer data was exposed. Epsilon only has the information of people who opted-in to receive marketing emails, and the theft was limited to email addresses and customer names, according to the company.

There are 18 user comments on this IT Security & Network Security News & Reviews story.

'Tricked' RSA Worker Opened Backdoor to APT Attack

By Christopher Crey and John Markoff | Published: May 27, 2011

The New York Times

Business Day

Data Breach at Security Firm Linked to Attack on Lockheed

Lockheed Martin, the nation's largest military contractor, has battled disruptions in its computer networks this week that might be tied to a hacking attack on a vendor that supplies coded security tokens to millions of users, security officials said on Friday.

Go to your Portfolio ▶

RSA acknowledged in March that it had sustained a data breach that could have compromised some of its security products. Executives in the military industry said Friday that Lockheed's problems appeared to stem from that data breach and could be the first public signs of damage from it.

The March intrusion reverberated through the computer security community. The RSA technology is used by most Fortune 500 companies and federal agencies to provide an extra layer of security when employees use their networks from customer offices, hotels or their homes.

Many of RSA's customers have taken extra measures since the intrusion was discovered, either by adding security measures, finding alternative solutions or simply shutting off remote access. Security experts said it was possible that companies other than Lockheed had faced attacks, whether they realized it or not.
The Bottom Line of Data Loss

- 9.5 million consumers were victims of identity theft in 2010\(^1\).
- The total fraud loss amount was $500 Million\(^2\).
- The average loss to organizations in 2010 was nearly $400,000\(^3\).
- The average consumer victim spent 21 hours and $373 to resolve the crime\(^4\).
- More than 84.3% of e-mail is Spam
- 52% of data theft occurred over the Web\(^5\)
- Industry standards, such as PCI compliance, will help reduce the risk.

\(^1\)2011 ITRC Breach Report
\(^2\)The 2010 Verizon Business Data Breach Investigations Report
\(^3\)2010 Cybercrime Security Survey
\(^4\)Javelin Strategy and Research, 2009
\(^5\)Web Sense 2010 Threat Report
What Are The Risks?

The risks are more than just immediate monetary impact:

- Litigation
- Reputation Loss
- Loss of System Availability
- Lost Productivity
- Loss of Intellectual Property
- Regulatory Fines
• In a trend consistent with pre-2009 levels, the food and beverage and retail industries shouldered the brunt of data breaches - accounting for 75% of all investigations.

• As with prior years, the majority of incident response caseload consisted of payment card data breaches.

• The targeting of payment card data is expected, as payment card fraud is an established business, and this data can be easily sold or laundered through established black market networks to realize financial gain.
Conduits for Data Loss

- Lost Laptop (35%)
- System Failure (33%)
- Other Data Bearing Device (14%)
- Paper Spill (7%)
- Lost Media Backup (5%)
- Cybercrime or Hack (5%)
- Social Engineering (2%)

Ponemon 2010 Annual Study: Cost of a Data Breach

- Access Rights
- Authentication
- Storage
- Transmission
- Backups
- Systems Security
- Network Security
- Information Disposal
- Application Development and Management
Threat Trends

Figure 14. Threat action categories by percent of breaches and records

- Malware: 38% / 54%
- Hacking: 40% / 96%
- Social: 28% / 3%
- Misuse: 48% / 3%
- Physical: 15% / 1%
- Error: 2% / 0%
- Environmental: 0% / 0%

Verizon 2011 Data Breach Investigations Report

What is your biggest security concern for this year?

- Meeting security compliance requirements
- Cloud computing
- Advanced persistent threat
- Web application vulnerabilities
- Smartphones
- Social media
- Virtualization
- VOIP vulnerabilities (Vishing)
- Targeted threat environment

nCircle 2011 - Security & Compliance Trends
Most Affected Business Processes and Functions

Retail follows only hospitality as the industry sector most affected by breaches and loss of information. Good security practices and compliance with security regulations can help plug the holes.

### Industry groups represented by percent of breaches

<table>
<thead>
<tr>
<th>Industry Group</th>
<th>Percent of Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospitality</td>
<td>40%</td>
</tr>
<tr>
<td>Retail</td>
<td>25%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>22%</td>
</tr>
<tr>
<td>Government</td>
<td>1%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2%</td>
</tr>
<tr>
<td>Tech Services</td>
<td>2%</td>
</tr>
<tr>
<td>Business Services</td>
<td>1%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>1%</td>
</tr>
<tr>
<td>Media</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Transportation</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

• *Verizon 2011 Data Breach Investigations Report*
Methods of attack have become more complex. While web applications are the primary vectors of attack, the use of stolen credentials contributes to the highest volume of stolen records – Both points directly impact retail and merchants.

Information is very valuable. Information for fraud, Spam, Phishing against retail and their customers are all highly marketable.

There is a black market for professional hackers in selling stolen data and hacker holes and tools.

Recent Experience

Reported Breach – Professional hacking for profit. UBN sold e-mail lists and user-id passwords for at least $100,000. Backdoors and admin passwords sold at the best price. Federal investigators are trying to shutdown this ring.

Hacker used a SQL Injection on the Web-Server

- SQL command line and guessed a password
- with admin access

- Added local Admin user

- Downloaded and decrypted passwords

- Download database and upload backdoors

<table>
<thead>
<tr>
<th>Hacker Attack Step</th>
<th>Control Which Broke Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Injection</td>
<td>Application input validation was not implemented, further vulnerability assessment/pen tests did not occur</td>
</tr>
<tr>
<td>Command Prompt</td>
<td>SQL user least privilege and logging and monitoring were not employed</td>
</tr>
<tr>
<td>Guest Admin User-ID</td>
<td>Passwords and User ID were identical</td>
</tr>
<tr>
<td>Add Local Admin User</td>
<td>Privileged User Logging and Monitoring</td>
</tr>
<tr>
<td>Crack passwords for two domain accounts</td>
<td>Needed strong encryption – not the LANMAN Password Hashing Algorithm</td>
</tr>
<tr>
<td>Upload Backdoors</td>
<td>Privileged User Activity Logs No Anti-Virus on Servers</td>
</tr>
<tr>
<td>Download Data</td>
<td>Data Leakage Detection Database Logs</td>
</tr>
</tbody>
</table>
Recent Experience

Attackers executed a phishing attack against unsuspecting personnel, resulting in a compromise of Desktop integrity, compromise of credentials and remote access into the corporate environment.

<table>
<thead>
<tr>
<th>Hacker Attack Step</th>
<th>Control Which Broke Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed phishing e-mail and attachment with malicious payload.</td>
<td>Awareness training was not effective, nor were software local to the machine kept current.</td>
</tr>
<tr>
<td>Establishes a connection to compromises accounts.</td>
<td>Desktop administrators had domain level permissions, later leveraged in the attack.</td>
</tr>
<tr>
<td>Authenticated to VPN.</td>
<td>Multifactor controls were not required for remote VPN authentication.</td>
</tr>
<tr>
<td>Further compromise adjacent systems.</td>
<td>Flat network allowed for immediate access to core systems from the DMZ.</td>
</tr>
<tr>
<td>Attempted access to database.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Definition:

Advanced Persistent Threat (APT):

A sophisticated cyber attack against a specifically targeted corporation or individual by a highly organized and well-funded organization or government.

Key pieces of the attack:

Advanced:

Involves the use of multiple attack methodologies and tools. Combines social engineering as well as technical attacks.

Persistent:

Because the company or individual is targeted specifically, attackers will change their attack method when faced with resistance. If they are seeking financial gain, the attackers will not move on to another target.
### Recent Experience

Attackers send phishing e-mails to target that suggest they visit an interesting site. Social engineering is used to entice the target with a website that is of personal interest. Site has malware hidden in an JPG file. Malware opens back-door. Called Operation Aurora. Targets included Adobe, Juniper, Rackspace, Yahoo, Grumman, Dow, Symantec, & Morgan Stanley.

<table>
<thead>
<tr>
<th>Hacker Attack Step</th>
<th>Control Which Broke Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop target information</td>
<td>Policy and training for social networking did not contain adequate provisions for how information can be used for targeting. Information should be nonspecific.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>E-mail sender not filtered</td>
</tr>
<tr>
<td>Phishing e-mail sent to target.</td>
<td>Target visits website with malware</td>
</tr>
<tr>
<td>Develop zero day JPG Malware</td>
<td>No zero day malware software detection</td>
</tr>
<tr>
<td>JPG Malware exposes target to PDF Exploit</td>
<td>No zero day malware software detection</td>
</tr>
<tr>
<td>Malware opens backdoor used to gather passwords, data etc.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Operation Aurora:

On January 10, 2010, Google announced it had been compromised by a sophisticated attack stemming from China.
Recent Experience

Attackers send phishing e-mails to target with compelling attachment. Attachment contains malware that allows remote control. Social engineering is used to develop target. Malware opens remote control. Targets included law firms, federal government agencies, defense contractors, and technology companies, like Google and RSA.

<table>
<thead>
<tr>
<th>Hacker Attack Step</th>
<th>Control Which Broke Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop target information Social Engineering</td>
<td>Policy and training for social networking did not contain adequate provisions for how information can be used for targeting. Information should be nonspecific.</td>
</tr>
<tr>
<td>Phishing e-mail sent to target. Compelling attachment “2011 Recruitment Plan”</td>
<td>E-mail sender not filtered E-mail attachment (.xls) scanned but no malware detected Target opens E-Mail Attachment</td>
</tr>
<tr>
<td>Malware allows remote control to collect passwords etc.</td>
<td>N/A</td>
</tr>
<tr>
<td>RAR files created and FTP Used to send date</td>
<td>FTP not detected No Data Leakage Detection.</td>
</tr>
<tr>
<td>Gather and monitor information gathered</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Human Factor

Social Engineering Specialist

Because there is no patch for human stupidity

I have a new hobby. It’s called phishing.

I send fake banking e-mails to gullible executives. Then I find out their financial information and use it to steal the money they don’t deserve.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don’t you send them to us so we can protect your money.
Sincerely,
I. B. Banker

© Scott Adams, Inc./Dist. by UFS, Inc.
RSA Compromised:

On March 18, 2011, RSA revealed it had been compromised by an APT and that information related to its SecurID authentication products was stolen.
Why is APT Different

APT is a different type of attack because it combines targeted social engineering with technical attacks. The combination is new the attacks are not.

Targeted:

Attackers know where the money is through media reports and annual reports. The attack focuses of key people and key organizations.

Social Engineering:

Protiviti generally has success rates in excess of 89% when executing social engineering tests. If these tests are targeted and specifically tailored and marketed, success rates are even higher.

Technical Attacks take advantage of trusting people and networks:

Using techniques like spear-phishing, executives and key may disclose passwords, pick-up malware, go to a attackers web-site. Once in, the attacker moves data out. Security defenses are designed to keep out attacks and normally permit trusted internal traffic to go out. So once in, attackers can go undetected.
Example of How APT Works

HOW APTs WORK

APT attacks are unique and attack processes are custom-tailored to the target. The techniques depicted here are similar to those used in Operation Aurora against private sector corporations.

1. Identifying “the mark”
   Attackers pinpoint individuals with the access privileges they need.

2. Spear-phishing
   Attackers send spoofed emails with malicious links or attachments to infect specific, high-value employees’ machines.

3. Organization mapping
   Once inside, attackers map the organization’s IT environment to identify strategic assets, privileged nodes and employees with more useful privileges.

4. Privilege escalation
   Attackers elevate privileges through additional spear phishing or by decrypting administrative credentials.

5. Stealth fighters
   Attackers install malware to hijack systems, creating backdoors and establishing “back connect” functionality to communicate with command and control servers.

6. D-day
   Attackers activate command-and-control infrastructure to steal, encrypt, compress and transmit information.

Source: RSA Security Brief - February 2011
New Attack Pattern

### Attack Tools

- Blended email threats
- Legitimate websites hosting malware Combination of malware tools
- Infected workstations (bots)
- Command & Control servers
- Attack management console
Levering Malware as a New Attack Pattern

Figure 21. Malware customization over time by percent of breaches within Malware*

Level of malware customization by percent of breaches within Malware*

* Verizon caseload only

Verizon 2011 Data Breach Investigations Report

© 2011 Protiviti Inc.
Risks from APT

Assets:

The old adage is follow the money. APT targets the assets worth stealing and targets worth the attackers time and persistence.

Financial:

Less concern for credit card and financial data theft – for now. Focus of detected APT is national secrets, Intellectual Property and unique company data.

Intellectual Property:

Systems contain IP information that a criminal or government entity would find valuable.
What can you do?

1. Keep applications up to date
   • Most vulnerabilities target outdated browsers and old versions of applications like Adobe Flash and Adobe Reader. Patches to these applications address many of the vulnerabilities.

2. Monitor
   • Monitor outbound and inbound traffic. Look for large data movements. Use Data Leakage tools.

3. Turn Perimeter Defenses Around
   • Use perimeter controls like IDS, Firewalls, content block and monitor traffic.

4. Disable administrative rights for most users
   • It’s been proven that by eliminating user administrative privileges risk is lowered.

5. Educate users
   • Ensure your employees can recognize social engineering, Phishing, Man-in-the-middle malware, etc. And institute a policy regarding external devices such as USB sticks.

6. Governance
   • Engage proactive governance, risk and compliance assessments to produce predictable, scalable environments and prioritize protection of information and strategic assets.

The Bottom Line:
Stopping APT requires a multi-layer approach involving preventative technologies and processes. An in-depth review should be performed to create an effective way to spot possible APT attacks.
- **Open Source Analysis**
  - APT will use all the information you give them against you
  - You can use their analysis to predict their actions

- **Attack Phase**
  - Social Engineered Email and Web Site planting
  - Awareness, Monitoring, Sharing

- **Lateral Movement Phase**
  - They will jump to new systems and establish new footholds
  - Monitor for lateral movement and segregate your networks

- **Command & Control and Exfiltration**
  - They will communicate with your systems and take what they want
  - Block unnecessary outbound traffic, monitor, and share
Key Take A Ways

- Malware attacks are prevalent, effective and damaging;
- Define your response strategy and core objectives to response;
- Have a plan to address malware incidents based on a proven framework and mythology;
- The plan should be flexible enough to address shifting approaches to IT and business operations;
- Keep the plan current and introduce malware scenarios into training exercises;
- Have the tools and resources required to respond to a malware incident;
- Stay current on attack trends and vectors;
- Prepare your defenses accordingly;
- Monitor.
 Powerful Insights.  
 Proven Delivery.™