Tackling Advanced Modern Cyber Malware Advanced Persistent Threats.

E-Crime Congress
Istanbul Turkey
Oct 12th, 2011
The Evolving Threat Landscape

- # of threats are up 10X
- Nature of threats changing
  - From broad, scattershot to focused, targeted
- Pace of advanced attacks accelerating
  - High profile attacks commonplace
  - RSA, Citicorp, Epsilon, Lockheed…

“71% of surveyed IT Security Professionals said the ‘changing/evolving nature of threats’ is a major challenge or challenge.” – Forrester, 2011
High Profile Attacks are Increasingly Common

In latest attack, hackers steal Citibank card data

By PALLAVI GOOI and KELVIN CHAN, AP Business Writers - Thu Jun 9, 1:31 pm ET

NEW YORK – About 200,000 Citibank credit card customers in North America have had their names, account numbers and email addresses stolen by hackers who broke into Citi’s online account site.

CitiGroup Inc. said it discovered that account information for about 1 percent of its credit card customers had been viewed by hackers. Citi has more than 21 million credit card customers in North America, according to its 2010 annual report. The New York-based bank, which discovered the problem during routine monitoring, didn’t say exactly how many accounts were breached. Citi said it was contacting those customers.

Adobe warns of Flash Player zero-day attack

By Ryan Naraine | March 14, 2011, 1:02pm PDT

Summary

Malicious hackers are using rigged Microsoft Excel files to exploit a zero-day flaw in Adobe’s ubiquitous Flash Player software.

Topics


Malicious hackers are using rigged Microsoft Excel files to exploit a zero-day flaw in Adobe’s ubiquitous Flash Player software.

A security advisory from Adobe says the “critical” vulnerability affects the latest versions of Adobe Flash Player for Windows, Mac OS X, Linux, Solaris and Chrome. It also exists in the autoupdate component that ships with Adobe Reader and Acrobat.

“There are reports that this vulnerability is being exploited in the wild in very limited, targeted attacks via a Flash (.swf) file embedded in a Microsoft Excel (.xls) file and delivered as an email attachment,” the company warned.

LulzSec, Sony, And The Rise Of A New Breed Of Hacker

NEW YORK – When a new hacking entity calling itself LulzSec claimed credit for a barrage of recent attacks on Sony and several other companies, many cyber-security experts found themselves grasping for a term to describe the attackers.

Hackers often divide themselves into two groups -- the “black hat” hackers, who exploit the vulnerabilities of their victims for profit, and the “white hat” hackers, who point out those weaknesses so that the vulnerable can take the proper measures to protect themselves. Yet as several experts pointed out recently, LulzSec doesn’t really fit into either of those categories, and that slipperiness, combined with the group’s sudden prominence, speaks to how hacker culture is changing.

RSA breached in APT attack; SecureID info stolen

SecurityWeek.com Staff

Published: 17 Mar 2011

RSA, the Security Division of EMC Corp., said Thursday that information related to its SecurID two-factor authentication products was stolen in an “extremely sophisticated cyberattack” against the company.

In an open letter to customers posted on the company’s website, Art Coviello, RSA executive chairman, said RSA recently detected the attack.

“Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain
We are Only Seeing the Tip of the Iceberg

Headline Grabbing Attacks

Thousands More Below the Surface

- APT Attacks
- Zero-Day Attacks
- Polymorphic Attacks
- Targeted Attacks
Defining Advanced Malware

- Next generation of threats
  - Unknown
  - Targeted
  - Polymorphic
  - Dynamic
  - Personalized
- Leverage zero-day vulnerabilities, commercial quality toolkits, social engineering tactics
- Often targets IP, credentials or other networked assets
World’s Top Malware

E-Crime Congress
Istanbul Turkey
Oct 12th, 2011

Copyright (c) 2011, FireEye, Inc. All rights reserved. | CONFIDENTIAL

<table>
<thead>
<tr>
<th>Modern Malware</th>
<th>% Infected hosts</th>
<th>Payload</th>
<th>Single Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Butterfly/Palevo</td>
<td>7.5</td>
<td>DDoS, Info stealer</td>
<td>NO</td>
</tr>
<tr>
<td>2 Hilotti</td>
<td>4.69</td>
<td>Downloader/PPI</td>
<td>YES</td>
</tr>
<tr>
<td>3 Zbot/Zeus</td>
<td>3.62</td>
<td>Info stealer</td>
<td>NO</td>
</tr>
<tr>
<td>4 FakeRean</td>
<td>3.47</td>
<td>Rogue AV(s)</td>
<td>YES</td>
</tr>
<tr>
<td>5 Onlinegames</td>
<td>2.94</td>
<td>Info stealer</td>
<td>YES</td>
</tr>
<tr>
<td>6 Rustock</td>
<td>2.66</td>
<td>Spam</td>
<td>YES</td>
</tr>
<tr>
<td>7 Ldpinch</td>
<td>2.64</td>
<td>Info stealer</td>
<td>NO</td>
</tr>
<tr>
<td>8 Renos</td>
<td>2.58</td>
<td>Rogue AV(s)</td>
<td>YES</td>
</tr>
<tr>
<td>9 Zlob</td>
<td>2.54</td>
<td>Rogue software</td>
<td>YES</td>
</tr>
<tr>
<td>10 Autoit</td>
<td>2.53</td>
<td>Downloader/PPI</td>
<td>YES</td>
</tr>
<tr>
<td>11 Conficker</td>
<td>2.48</td>
<td>Worm</td>
<td>YES</td>
</tr>
<tr>
<td>12 Opachki</td>
<td>1.95</td>
<td>Click Fraud</td>
<td>YES</td>
</tr>
<tr>
<td>13 Buzus</td>
<td>1.91</td>
<td>Info stealer</td>
<td>YES</td>
</tr>
<tr>
<td>14 Koobface</td>
<td>1.17</td>
<td>Downloader</td>
<td>YES</td>
</tr>
<tr>
<td>15 Alureon</td>
<td>1.16</td>
<td>Downloader</td>
<td>NO</td>
</tr>
</tbody>
</table>

Source: FireEye Malware Intelligence Lab, Q3/2010
Today’s Typical Enterprise Malware Defense

<table>
<thead>
<tr>
<th>Secure web gateways</th>
<th>Some analysis of script-based malware, AV, IP/URL filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop AV</td>
<td>Signature-based detection (some behavioral detection)</td>
</tr>
<tr>
<td>IPS</td>
<td>Attack-signature based detection, shallow application-level analysis</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Block IP/port connections, pure network-level logic</td>
</tr>
</tbody>
</table>
Malware Detection Rates for Leading AV Solutions (August 2010)

<table>
<thead>
<tr>
<th>Trend Micro</th>
<th>Sophos</th>
<th>McAfee</th>
<th>Kaspersky</th>
<th>F-Secure</th>
<th>Dr Web</th>
<th>AVG</th>
<th>Nod32</th>
<th>F-Prot</th>
<th>Virus Buster</th>
<th>Norman</th>
<th>eTrust Vet</th>
<th>Symantec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>17%</td>
<td>20%</td>
<td>22%</td>
<td>22%</td>
<td>27%</td>
<td>7%</td>
<td>13%</td>
<td>37%</td>
<td>17%</td>
<td>10%</td>
<td>17%</td>
<td>16%</td>
</tr>
<tr>
<td>Day 8</td>
<td>29%</td>
<td>36%</td>
<td>53%</td>
<td>87%</td>
<td>50%</td>
<td>29%</td>
<td>85%</td>
<td>86%</td>
<td>23%</td>
<td>30%</td>
<td>29%</td>
<td>21%</td>
</tr>
<tr>
<td>Day 15</td>
<td>32%</td>
<td>75%</td>
<td>95%</td>
<td>91%</td>
<td>59%</td>
<td>33%</td>
<td>92%</td>
<td>88%</td>
<td>34%</td>
<td>46%</td>
<td>31%</td>
<td>27%</td>
</tr>
<tr>
<td>Day 22</td>
<td>32%</td>
<td>81%</td>
<td>86%</td>
<td>92%</td>
<td>62%</td>
<td>33%</td>
<td>92%</td>
<td>88%</td>
<td>37%</td>
<td>74%</td>
<td>32%</td>
<td>29%</td>
</tr>
<tr>
<td>Day 30</td>
<td>38%</td>
<td>85%</td>
<td>86%</td>
<td>92%</td>
<td>64%</td>
<td>33%</td>
<td>93%</td>
<td>89%</td>
<td>39%</td>
<td>74%</td>
<td>32%</td>
<td>30%</td>
</tr>
</tbody>
</table>

“Even after 30 days, many AV vendors cannot detect known attacks, making it critical for enterprises to take a more proactive approach to online security in order to minimize the potential for infection,” said Panos Anastassiadis, COO of Cyveillance.
Traditional Defenses Don’t Work

- Current defenses are no match for the new breed of sophisticated attacks
- Advanced threats bypass both signature and heuristics-based technologies
STOPPING ALL THE ATTACKS
STOPPING ALL THE ATTACKS
STOPPING ALL THE ATTACKS
STOPPING ALL THE ATTACKS
What the Analysts are Saying

E-Crime Congress
Istanbul Turkey
Oct 12th, 2011

“The widening gap between hacker capabilities and security defenses has security organizations struggling to keep up with the changing nature, complexity, and scale of attacks.”
– Forrester, 2011

“Incumbent defenses fall short…existing antimalware initiatives are no longer enough.”
– Forrester, 2011

“Some IPS/IDS/NGFW vendors are no better at handling evasions today than they were when they released their original products.”
– Gartner Group, 2011

“Organizations that rely on desktop AV and secure web gateways as their primary antimalware technologies may very well find themselves falling victim to malware-based attacks.”
- Forrester, 2011

“Being online grows more dangerous by the day, and, for many exploits, the browser is the target of choice. In the last few years, enterprises have seen a parade of vulnerabilities through Adobe Acrobat, Microsoft Internet Explorer, and browser plug-ins. Often, the browser exploit is only the first stage of a more insidious attack, as in Operation Aurora.”
- Gartner Group, 2011
The Security Gap is Broad

Over 95% of Companies are Compromised
Toxic Data Spills and Thefts are Frequent...

Number of breached records per year (millions)

- Base: 1,605 data breach incidents
- Source: DataLossDB, with Forrester Research analysis

- Toxic data spilled includes PII-, PHI-, PCI-related data
- Many spills accidental, but most are malicious - 60% of exposures due to hacking

Source: Forrester
Anatomy of an Attack

1. Phishing and Zero Day Attack
   A handful of users are targeted by two phishing attacks: one user opens Zero day payload (CVE-2011-0609)

2. Back Door
   The user machine is accessed remotely by Poison Ivy tool

3. Lateral Movement
   Attacker elevates access to important user, service and admin accounts, and specific systems

4. Data Gathering
   Data is acquired from target servers and staged for exfiltration

5. Exfiltrate
   Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

Next-generation threats like the RSA attack use successive inbound and outbound stages
Tactics of a Targeted Attack

E-Crime Congress
Istanbul Turkey
Oct 12th, 2011

Step 1: Victim receives a specially crafted email message

Step 2: Victim opens an attachment or visits a link to a site hosting a one-off malicious exploit

Step 3: The exploit executes on victim’s machine, creates backdoor

Step 4: Attacker moves around in the system and grabs users credentials and install backdoors as they go

Step 5: The malware can now pose as a user and access critical system assets

Source: Forrester
Current Defense Technologies All Fall Short

E-Crime Congress
Istanbul Turkey
Oct 12th, 2011

Facebook message: “Hi Jack, this material is getting a lot of attention. Let me know if we can leverage its functionality. http://bitly/aw4yl. - Dan”.

Spear-Phishing eludes anti-spam technology
Vulnerability scanning is ill equipped to find zero-day vulns
Desktop AV often do not pick up zero-day exploits
Secure Web Gateway is far from fool-proof

Firewalls and IPS will let this message go straight through.

Source: Forrester
Next Generation Threat Protection

- Must be proactive, real-time and signature-less
- Complete security combines signature-based with signature-less
- Plugs hole left open by NGFW, IPS, AV and SWG
- Focuses on unknown threats
Company Overview

• The world leader in combating advanced malware, zero-day and targeted APT attacks

• Marquee customers across every industry in every region

• One of the fastest growing technology companies in US

• Silicon Valley-based, backed by top investors in the world
  – Sequoia Capital, NorWest, In-Q-Tel (CIA) and Juniper Networks
Summary

• Pace of advanced threats accelerating, targeting all verticals and all segments

• Traditional defenses (NGFW, IPS, AV, and Web gateways) no longer combat these attacks

• Real-time, proactive signature-less solution is required across Web and Email to solve issue

• FireEye has engineered the best threat protection solution to supplement traditional defenses and combat advanced attacks