The New Threat Landscape

Andy Sciaroni – FireEye Systems Engineer
Agenda

• Threat Landscape Defined
• Malware Infection Lifecycle
• FireEye Overview
The Acceleration of Advanced Targeted Attacks

- # of threats are up **5X**
- Nature of **threats changing**
  - From broad, scattershot to advanced, targeted, persistent
- Advanced **attacks accelerating**
  - High profile victims common (e.g., RSA, Symantec, Google)
  - Numerous APT attacks like Operation Aurora, Shady RAT, GhostNet, Night Dragon, Nitro

"Organizations face an evolving threat scenario that they are ill-prepared to deal with....advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems."

Gartner, 2012
Technological Risks

Source: World Economic Forum
Top 5 Global Risks

Source: World Economic Forum
High Profile APT Attacks Are Increasingly Common

News
Symantec confirms source code leak in two enterprise security products
Hacking group discloses source code segments used in Symantec’s Endpoint Protection 11.0 and Antivirus 10.2
By Jaikumar Vijayan
January 6, 2012 06:42 AM ET

Computerworld - Symantec late Thursday confirmed that source code used in two of its older enterprise security products was publicly exposed by hackers.

RSA breached in APT attack; SecureID info stolen

Published: 17 Mar 2011

RSA, the Security Division of EMC Corp, said Thursday that information related to its SecureID 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

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 exactly fit either of...

New Zero-Day Adobe Attack Under Way

Adobe working on emergency patch for Adobe Reader and Acrobat 9.x for Windows
Dec 06, 2011 | 11:18 PM | 0 Comments
By Kelly Jackson Higgins
Dark Reading
Adobe Reader and Acrobat are under siege once again, this time via targeted attacks exploiting a previously unknown flaw in the software that lets an attacker crash the app and wrest control of the victim's machine. Adobe plans to issue an out-of-band update by next week for Windows-based systems only.
Wall Street Journal – Cybersecurity 2.0

FBI Director Robert Mueller last month told a Senate committee that cyber espionage against infrastructure such as power plants will someday surpass terrorism as the “No. 1 threat to the country.” This may be hyperbole, but the violations we know about are the tip of the iceberg. It takes a high level of sophistication to discover breaches of computer systems, which makes it likely that many remain undiscovered. Also, many companies choose not to disclose violations for fear of being sued. For example, news that some 30 high-tech companies had been hacked, including Yahoo, Adobe and Northrop Grumman, came to light only when Google disclosed that the Gmail accounts for Chinese human-rights activists had been compromised.

The Cybersecurity Act of 2012, introduced by Sen. Joe Lieberman, ran into trouble by trying to set new rules on how companies would monitor cyber security. A regulatory approach is flawed because types of cyber attack change faster than regulations can anticipate them. Sen. John McCain’s measure, which will be introduced soon, makes it easier for companies and intelligence agencies to share information about cyber attacks, ending a situation akin to the government pre-9/11, when intelligence was restricted to silos instead of being shared.

Both bills include provisions to encourage disclosure of cyber attacks by limiting companies’ legal liability for monitoring their systems and disclosing information about unauthorized access. Companies would participate in newly created “cybersecurity exchanges” where information would be shared without creating legal risk. The intelligence community would use these exchanges to share classified tips about security breaches.

The debate on cybersecurity has echoes from the recent battle over the Stop Online Piracy Act, because earlier approaches similarly threatened the mechanics of the Web. The cybersecurity bills now in Congress avoid the over-reaching of SOPA, which was withdrawn when it became clear that the government cure of regulation of the Web was worse than the disease.

The U.S. and its allies are also engaged in cyber warfare—the Stuxnet virus apparently developed by the U.S. and Israel slowed down Iran’s nuclear program—but the open nature of the Web makes this a high-stakes game. Today’s world is different from the pre-Internet era when industrial espionage featured spies from France visiting U.S. silicon chip factories wearing shoes with special adhesives to help them pilfer samples.

The Web has transformed many areas of life, now including a new cyber cold war. America’s enemies need to be discovered and deterred. Making it possible for companies and intelligence agencies to share information more freely is a good first step, increasing transparency as a way of using the strength of the open Web as a tool in its own defense.
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 Targeted Attacks

• Utilizes advanced techniques and/or malware
  – Unknown
  – Targeted
  – Polymorphic
  – Dynamic
  – Personalized

• Uses zero-day exploits, commercial quality toolkits, and social engineering

• Often targets IP, credentials and often spreads laterally throughout network

• AKA—Advanced Persistent Threat (APT)
Typical Enterprise Security Architecture

**Firewalls/NGFW**
Block IP/port connections, application-level control, no visibility into exploits and ineffective vs. advanced targeted attacks

**IPS**
Attack-signature based detection, shallow application analysis, high-false positives, no visibility into advanced attack lifecycle

**Secure Web Gateways**
Some analysis of script-based malware, AV, IP/URL filtering; ineffective vs. advanced targeted attacks

**Anti-Spam Gateways**
Relies largely on antivirus, signature-based detection (some behavioral); no true spear phishing protection

**Desktop AV**
Signature-based detection (some behavioral); ineffective vs. advanced targeted attacks
The Enterprise Security Hole

Web-based Attacks
Spear Phishing Emails
Malicious Files

SECURITY HOLE

Attack Vector

NGFW
FW
IPS
SWG
AV
The Degree of Compromise is Significant

98.5% of deployments see at least 10 incidents/week/Gbps

Median is about 450 incidents/week/Gbps

20% of deployments have thousands of incidents/week/Gbps

450 Median Net New Infections Per Week at Only 1 Gbps!

Malware Infection Lifecycle
Example Playbook

1. Phishing and Zero Day Attack
   - A handful of users are targeted by two phishing attacks: one user opens Zero day payload (CVE-02011-0609)

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
Malware Infection Lifecycle

- User
- Malware download
- Exploit
- Dropper
- Command/Control
- Malware
- CNN.com
- Advertisement
- Exploit
- Dropper
- Command/Control
Callback Phase

- CNN.com
- Advertisement
- Exploit
- Dropper
- Command/Control
Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independent Detections...Correlated

Three Independen...
What does a Phish email look like?

- Omaha’s Cyber Security Forum welcomes you! August’s meeting is at 7:30 a.m. on Wednesday the 15th and regular meetings will continue to be held on the third Wednesday of each month. Details are as follows:
  - Note #1: If you need a CPE form please let us know when you RSVP.
  - TOPIC: The New Threat Landscape
  - BY: Andy Sciaroni
  - FireEye
  - WHO: All Nebraska/Iowa Information Security Professionals
  - WHEN: Wednesday - August 15, 7:30 am - 9:00 am
  - WHERE: Bellevue Public Schools Support Center - Room A
    2820 Arboretum Drive, Bellevue NE
    (behind Computer Cable Connection)
  - WHY: To share information with like-minded professionals (and to share a FREE breakfast)
  - HOW: Please RSVP to csfrsvp@nebraskacert.org, and provide your name, company, phone and email address by Close Of Business Monday, 13 August.
  - DESCRIPTION: Traditional protections, like traditional and next-generation firewalls, intrusion prevention systems, anti-virus and Web gateways, only scan for the first move, the inbound attack. These systems rely heavily on signatures and known patterns of misbehavior to identify and block threats. This leaves a gaping hole in network defenses that remain vulnerable to zero-day and targeted advanced persistent threat (APT) attacks.
  - Find out how Malware Protection Systems (MPS) can help stop attacks that traditional and next-generation firewalls, IPS, AV, and Web and email gateways miss
  - If those of you who have access to lists of interested individuals would pass this message along, it would be appreciated!
RSA two-factor tokens

Securing Your Future with Two-Factor Authentication

Do you really know who’s accessing your most sensitive networked information assets? Unfortunately, security built on static, reusable passwords has proven easy for hackers to beat.

RSA SecurID® two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)—providing a much more reliable level of user authentication than reusable passwords.

- The only solution that automatically changes your password every 60 seconds
- 20-year history of outstanding performance and innovation
Kevin Brisson
E-Discovery Litigation Support Engineer
Greater Boston Area | Security and Investigations

Current
Sr E-Discovery Internal Litigation Support Engineer at

Past
Principal Exchange Systems Administrator at

Connections
83 connections

Public Profile
http://www.linkedin.com/in/kevinmbrisson

Experience

Sr E-Discovery Internal Litigation Support Engineer
Information Technology and Services industry
January 2008 – Present (3 years 10 months)

Principal Exchange Systems Administrator
Information Technology and Services industry
January 1999 – January 2008 (9 years 1 month)
Actual spearphish (H/T, @mikko)

From: web master <webmaster@beyond.com>
To: gilbert_david@
Cc: Patonai, Peter; Brisson, Kevin; Kuehne, Paul (SAL BlueBell)
Subject: 2011 Recruitment plan

Message

2011 Recruitment plan.xls

I forward this file to you for review. Please open and view it.
RSA hack targeted Flash vulnerability

By Jack Clark, 2 April, 2011 14:11  Follow @mappingbabel

The mid-March hack that affected RSA was made possible by an Adobe Flash vulnerability, the computer security company has disclosed.

On Friday, Uri Rivner, RSA’s head of new technologies for consumer identity protection, detailed the methods used to penetrate RSA. The attack, which RSA disclosed on March, saw hackers steal information about RSA’s SecureID authentication tokens, which are used to perform two-factor authentication for users of various networks.

Three URLs were associated with the attack. These were Good.mincesur.com, up82573.hopto.org and www.cz88.net.

malware=# select checksum, received from samples where checksum in (select checksum malware(# from fgc where server_dns_name = 'good.mincesur.com') order by received desc;

checksum | received
--------- +------------

b773532d59e313138954f68612f01d1c1 | 2011-05-05 18:19:57.942539
687a92132c7b539661173ded4026005 | 2011-04-13 17:14:15.372646
401f9e862dd9e222bb2038273a50108 | 2011-01-07 23:52:48.748555
f44b51cb037e4141087d96dd067bc6 | 2010-12-18 09:43:17.613809
c3b26ffca03310e1f2fa95b02b2f756 | 2010-11-13 01:41:24.197700
401f9e862dd9e222bb2038273a50108 | 2010-11-13 01:41:24.197700
401f9e862dd9e222bb2038273a50108 | 2010-11-13 01:41:24.197700
401f9e862dd9e222bb2038273a50108 | 2010-11-13 01:41:24.197700
401f9e862dd9e222bb2038273a50108 | 2010-11-13 01:41:24.197700
188ed479857cc58a95033b87949b4c0 | 2010-11-08 09:07:44.752825
401f9e862dd9e222bb2038273a50108 | 2010-11-08 08:42:35.156099
cd83c46857cc58a95033b87949b4c0 | 2010-10-16 02:06:36.093003
b79a92132c7b539661173ded4026005 | 2010-09-22 17:30:10.200994
188ed479857cc58a95033b87949b4c0 | 2010-09-22 17:30:10.200994
188ed479857cc58a95033b87949b4c0 | 2010-09-22 17:30:10.200994
cf92541173413052a657842de825d22 | 2010-09-22 16:42:29.706815
cd83c46857cc58a95033b87949b4c0 | 2010-09-22 16:42:29.688181
b773532d59e313138954f68612f01d1c1 | 2010-09-10 20:39:39.339465
abedf0d5f0599055d6e05325fa7fd | 2010-09-10 19:47:07.255989
b773532d59e313138954f68612f01d1c1 | 2010-09-08 15:35:15.336999
177a9e09f13a9cb6a832454338f46ee | 2010-09-08 14:46:24.924165
abedf0d5f0599055d6e05325fa7fd | 2010-08-21 00:42:51.354382
bf292541173413052a657842de825d22 | 2010-08-21 00:28.552255
abedf0d5f0599055d6e05325fa7fd | 2010-08-09 15:35:56.810414
b773532d59e313138954f68612f01d1c1 | 2010-07-08 15:38:11.369401

(26 rows)
Simple Website Review: www.same.org
Upcoming Golf Tournament

“25th” Annual Huntsville Post SAME Golf Tournament
ENTRY RESERVED FOR FIRST 128 GOLFERS
Thursday, OCTOBER 6, 2011
Rain date: Friday October 7, 2011
SUNSET LANDING GOLF COURSE
(at the Huntsville International Airport)
To benefit the Huntsville Post SAME Scholarship Fund

1030 AM CHECK-IN & LUNCHEON
12:00 PM SHOTSUN START
POST TOURNAMENT AWARDS

Come out and join us for a four-person scramble. The cost is $55 per person and includes green fees, cart, range balls, lunch and after tournament awards. You do not have to be an SAME member to play.

HOW TO BE A SPONSOR

- Title Sponsor - $2,000, includes two, four person teams (call or email Jeff Jones for additional details)
- Lunch Sponsor - $1,000, includes one, four person team (call or email Jeff Jones for additional details)
- Businesses may get a Team Sponsor Package for $500 Sponsor a hole and get a four person team (Save $701)
- Raffle Prize Sponsor - $500
- Businesses may sponsor a hole for $350
- Donate Door Prizes or Awards for the Post Tournament Awards
- Donate golf paraphernalia or other company logo items for the “goodie bags”

Please send payment and entry forms no later than close of business Monday, September 19, 2011. Call Jeff Jones (jeffrey.jones@itecitech.com) at 256-503-4183 or Phil Lofts at 256-217-2532 if you have any questions.

TEAM CAPTAIN

COMPANY
Protecting Against Advanced Targeted Attacks

FireEye Advanced Threat Protection Architecture

- Inline blocking and quarantine available across MPS portfolio
  - Block inbound zero-day Web attacks
  - Multi-protocol blocking of callbacks
  - Quarantine of malicious zero-day emails
  - Quarantine of malicious zero-day files
- Mitigates risk of data exfiltration
- Provides highly actionable information for timely incident response
Multi-Protocol, Real-Time VX Engine

**FireEye Appliance Platform**

- Multi-protocol Object Capture
- MALWARE-VM FILTER

**Phase 1 – Web MPS**
- Aggressive Capture
- Web Object Filter

**Phase 1 – Email MPS**
- Email Attachments
- URL Submission

**Phase 1 – MAS appliance**
- File directories
- Batch mode processing

Dynamic, real-time analysis
- Exploit detection
- Malware Binary analysis
- Cross-matrix of OS/apps
- Originating URL
- Subsequent URLs
- OS Modification Report
- C&C Protocol descriptors
- Generic heap spray
- Shellcode detection

Virtual Execution Environments
Phase 2
Global Intelligence to Protect Local Network

Inbound and Outbound Fast Path Blocking

Virtual Execution Engine Callback Filter

FireEye Appliance Platform
- Dynamic, inbound blocking of FireEye known threats
- Zero-day malware callback filter to stop data theft

Known attacks and callbacks blocked in microseconds

Malware Callbacks

Malware Protection Cloud

Minutes

Global Feedback Loop

Real-time sharing of malware data

Local Feedback Loop

Seconds
Enterprise Malware Protection Deployment

- Real-time Web, email, and file security to stop advanced targeted attacks
- Centralized reporting and management
- Integration into cyber incident response system
Third largest Botnet Grum Turn Off: Fire Eye

The security experts of FireEye destroyed Grum, the third largest botnet in the world, responsible for 18% of global spam
Q&A