FireEye™

The New Threat Landscape

Andy Sciaroni – FireEye Systems Engineer

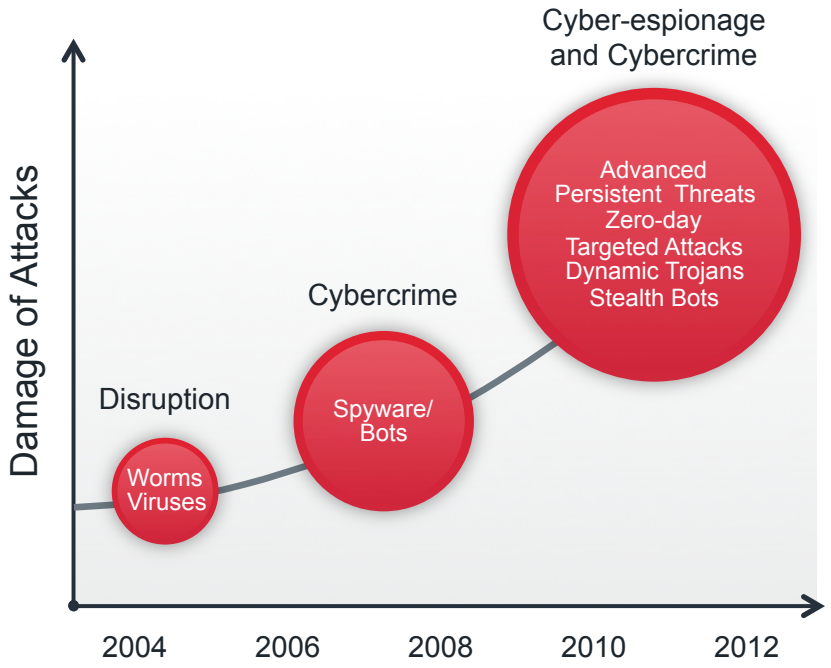
Agenda

- Threat Landscape Defined
- Malware Infection Lifecycle
- FireEye Overview

FireEye

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

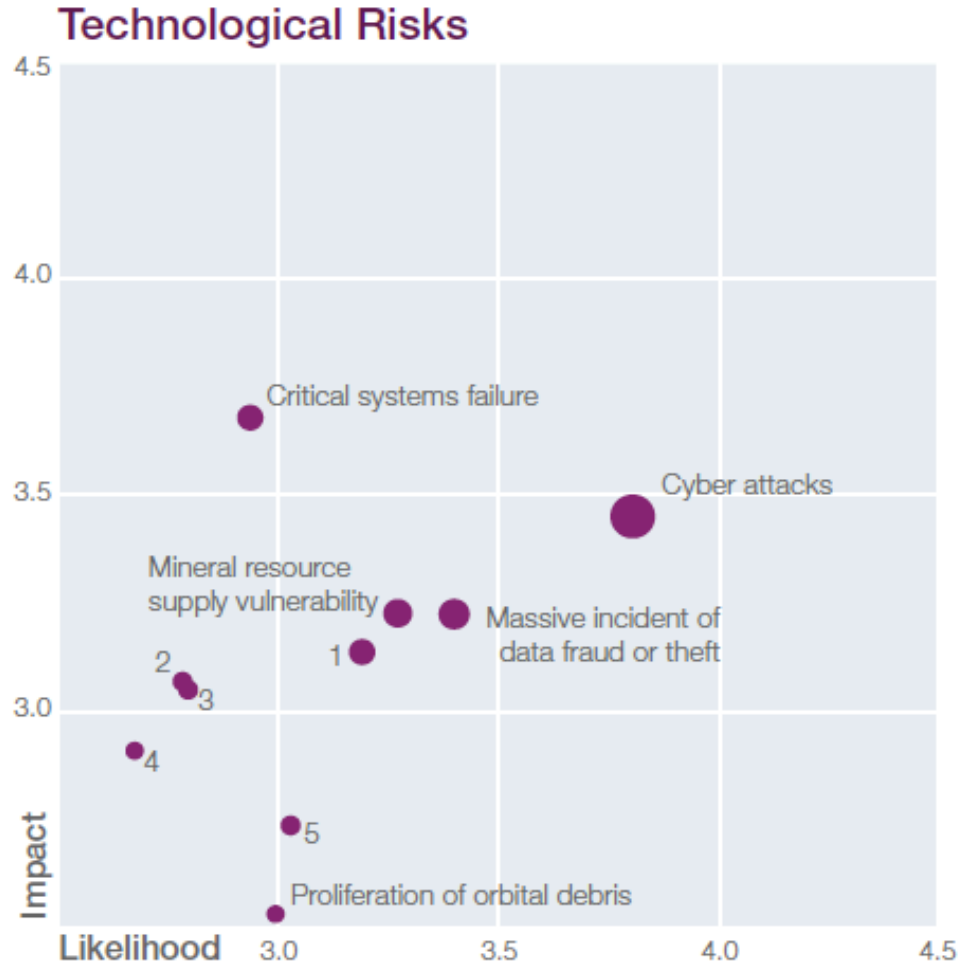


"Organizations face an evolving threat scenario that they are ill-prepared to deal with….advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems."

Gartner, 2012

FireEye

Technological Risks



Source: World Economic Forum

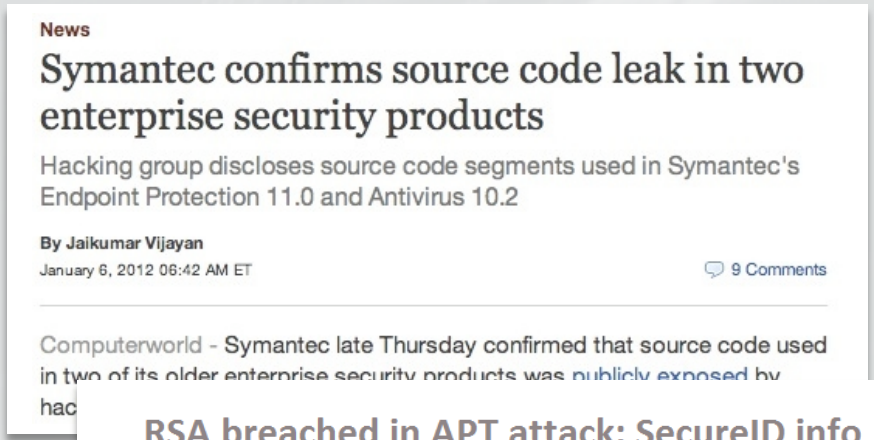
FireEye

Top 5 Global Risks

Source: World Economic Forum

FireEye

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

9 Comments

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

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

SHARE THIS STORY

Like Sign Up to see what your friends like.

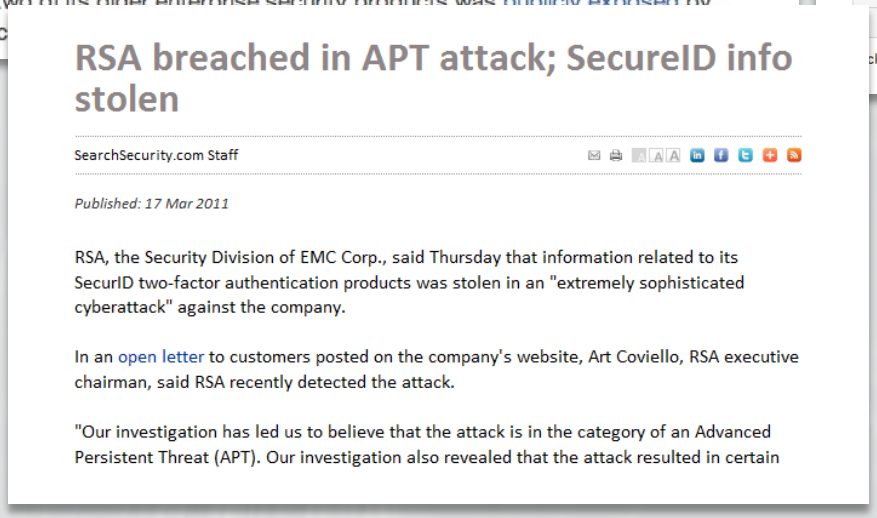
6 share | 11 tweet | 1 email | 20 comment

Get Technology Alerts

Sign Up

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



RSA breached in APT attack; SecureID info stolen

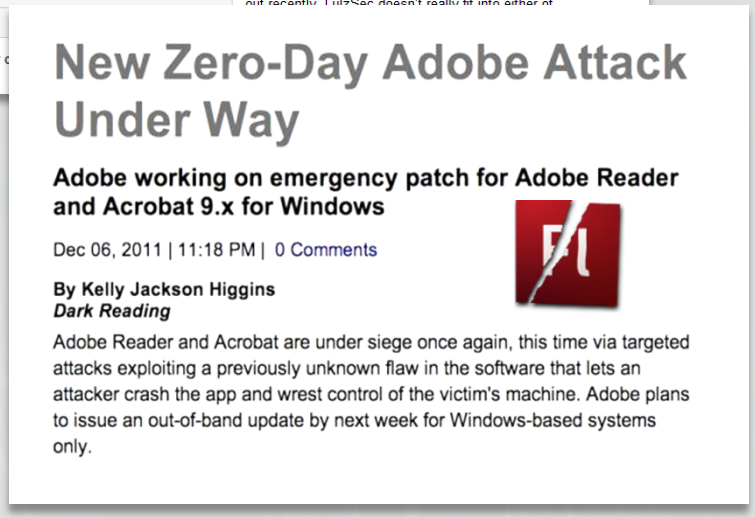
SearchSecurity.com Staff

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



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.

FireEye

Wall Street Journal – Cybersecurity 2.0

Cybersecurity 2.0

Give Washington some credit: It looks as if politicians have learned it's not a good idea to destroy the Internet in order to save it.

Congress and the White House have considered dozens of bills over the past few years to address cybersecurity, chiefly how countries such as China and Russia are using the Web to access confidential information from companies and U.S. agencies.

INFORMATION AGE

By L. Gordon Crovitz

The original approach was to create a "kill switch" empowering regulators to turn off access to the Web. New legislation would instead break down silos between U.S. companies and intelligence agencies so that cyber attacks can be tracked and reported, raising prospects for identifying cyber spies.

The U.S. is experiencing mind-boggling violations of cyber security. Consider this sample of violations traced to China alone discovered over the past year:

For a decade, hackers accessed the corporate computer network of Nortel, whose digital switches power much of the Web; defense contractor Lockheed Martin suffered a break-in when the SecureID system that provides encrypted authentication was breached; the U.S. Chamber of Commerce had all its systems accessed (one tipoff of a problem was when a printer in its office mysteriously printed pages with Chinese characters); five large oil companies lost information about their operations, including bidding strategies; and hackers accessed details of the Pentagon's costliest weapons program—the $300 billion Joint Strike Fighter project—including aircraft design and electronics.

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 a few years ago only when Google disclosed that the Gmail accounts for Chinese human-rights activists had been compromised.

Gen. Keith Alexander, director of the National Security Agency, told an FBI conference last month that the known attacks are the exception. When big companies are hacked, "people ask, 'What's wrong with these guys?'" Gen. Alexander said. "Actually, they're the gold standard for securing cyber. They're the ones that know they've been hacked."

Two bills in the Senate try to address the problem. Both reject earlier ideas such as giving federal authorities the ability to turn off parts of the Web or licensing cybersecurity workers in industries such as the electricity grid, chemical plants and financial-services computer networks.

> Encouraging companies and intelligence agencies to share information freely is a good first step.

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 overreaching 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.

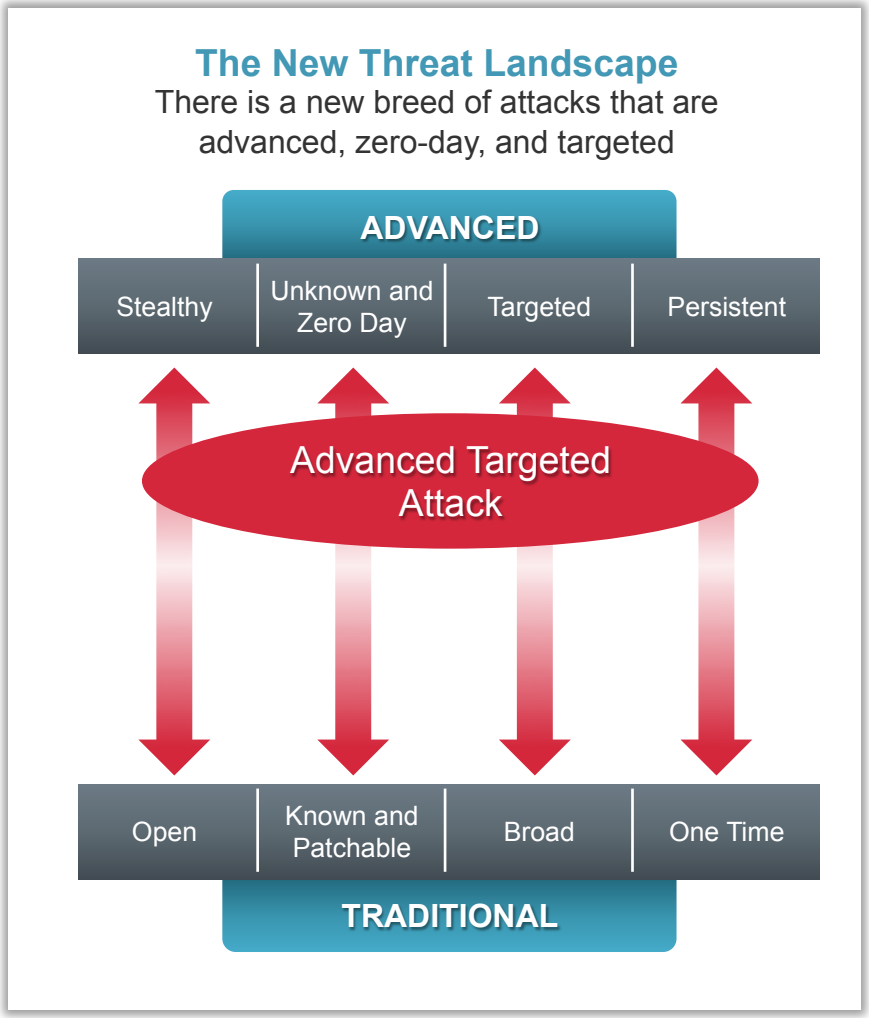
FireEye

We Are Only Seeing the Tip of the Iceberg

FireEye

Defining Advanced Targeted Attacks

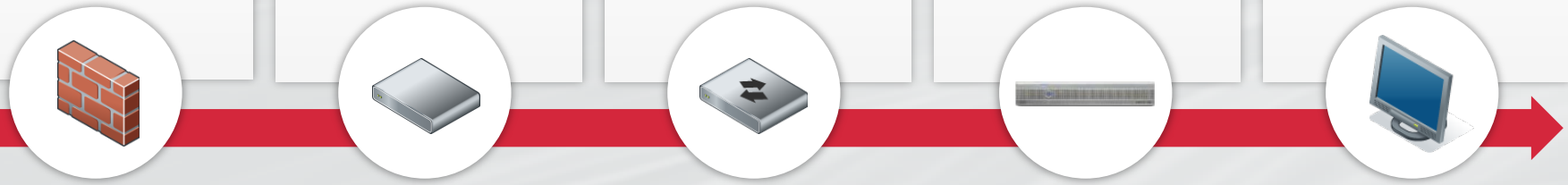
- Utilizes advanced techniques and/or malware
  - Unknown
  - Targeted
  - Polymorphic
  - Dynamic
  - Personalized
- Uses zero-day exploits, commercial quality toolkits, and social engineering
- Often targets IP, credentials and often spreads laterally throughout network
- AKA—Advanced Persistent Threat (APT)



FireEye

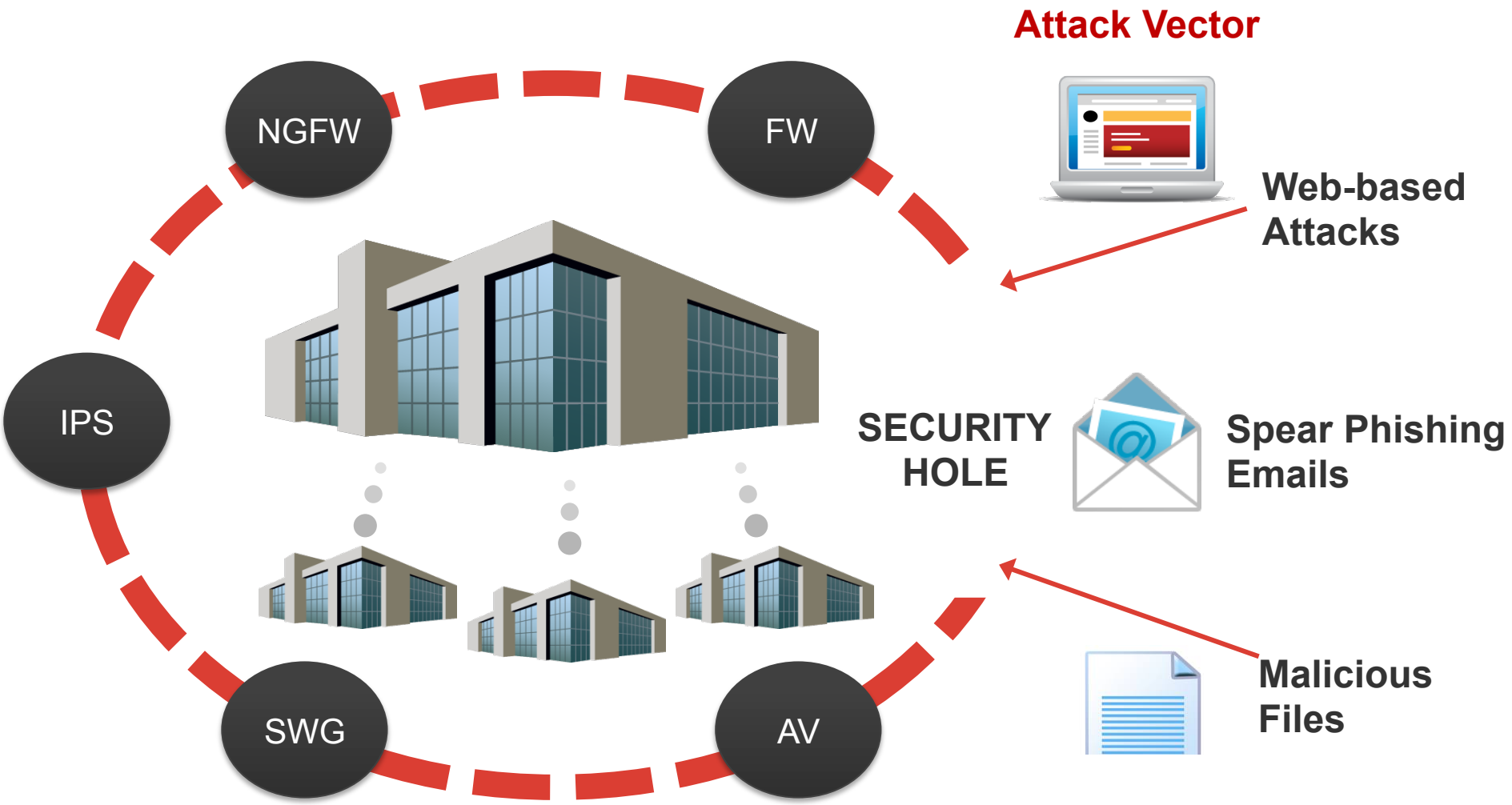
Typical Enterprise Security Architecture

Firewalls/ NGFW	IPS	Secure Web Gateways	Anti-Spam Gateways	Desktop AV
Block IP/port connections, application-level control, no visibility into exploits and ineffective vs. advanced targeted attacks	Attack-signature based detection, shallow application analysis, high-false positives, no visibility into advanced attack lifecycle	Some analysis of script-based malware, AV, IP/ URL filtering; ineffective vs. advanced targeted attacks	Relies largely on antivirus, signature-based detection (some behavioral); no true spear phishing protection	Signature-based detection (some behavioral); ineffective vs. advanced targeted attacks



FireEye

The Enterprise Security Hole



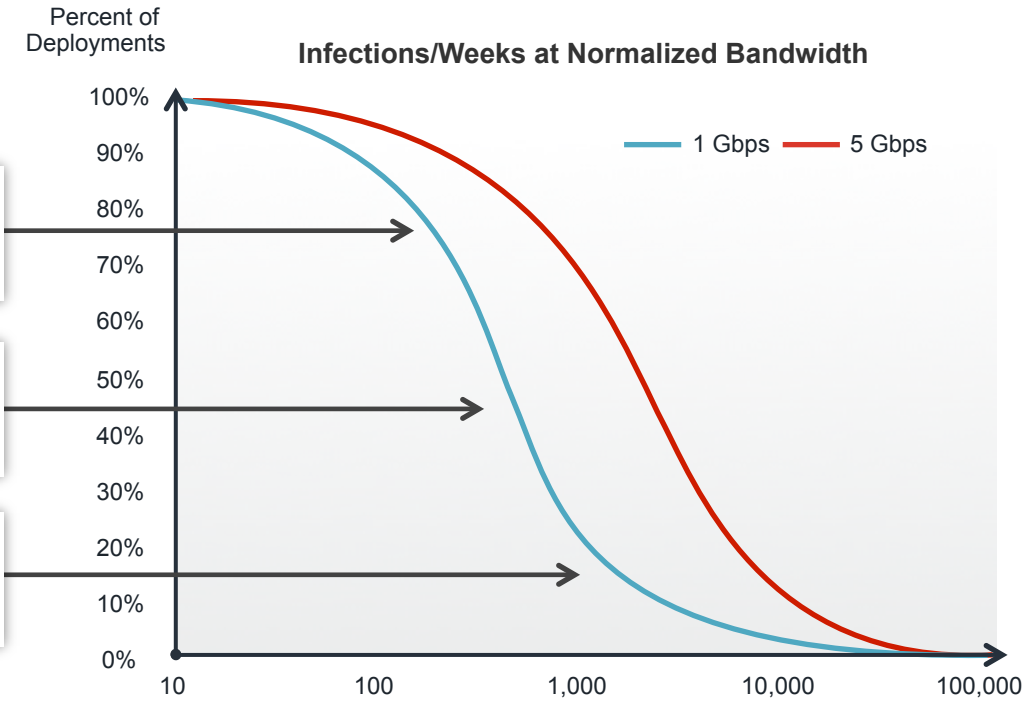
FireEye

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



Source: FireEye Advanced Threat Report, Feb. 2012

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

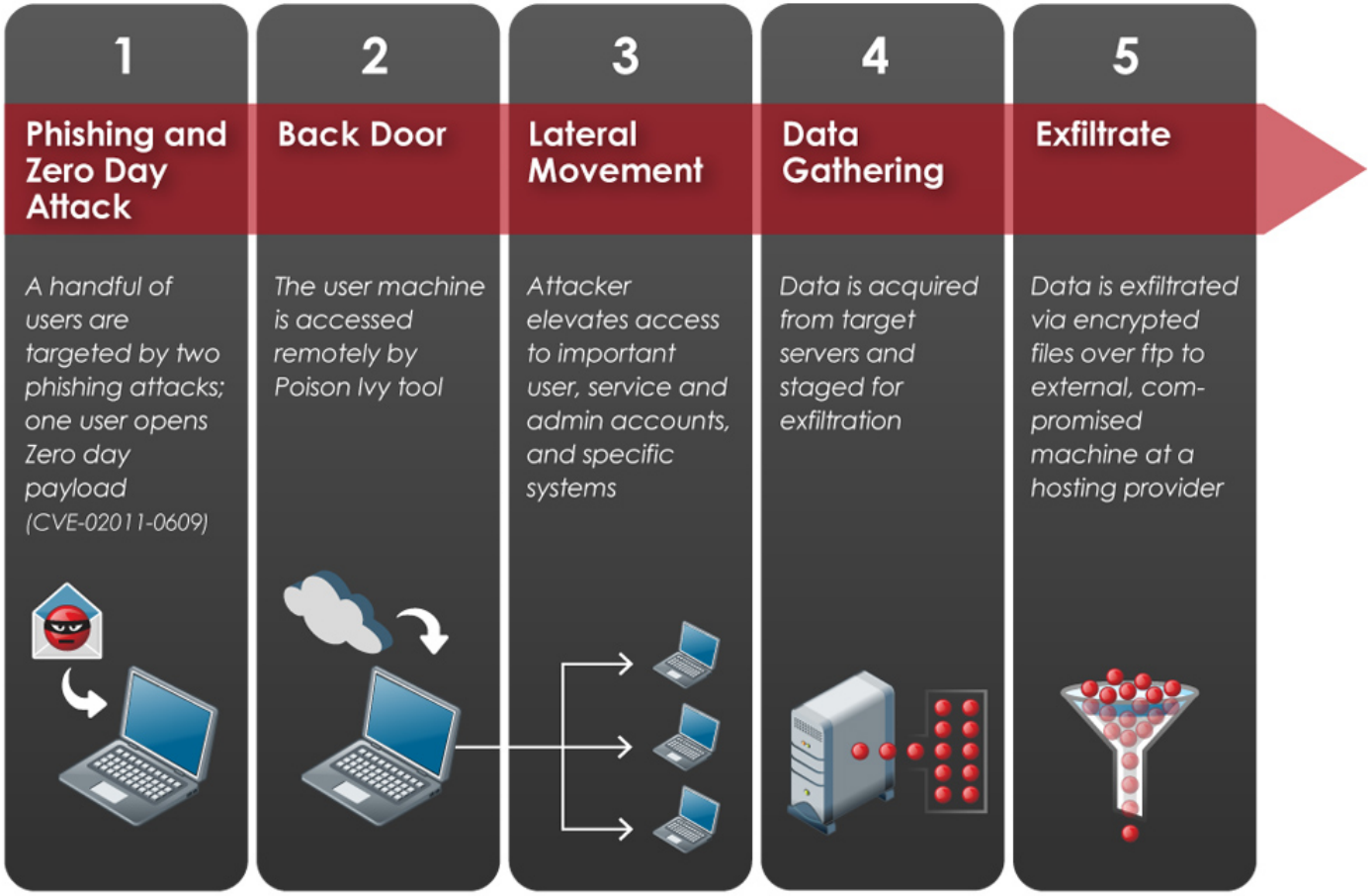
FireEye

FireEye™

Malware Infection Lifecycle

FireEye - Modern Malware Protection System

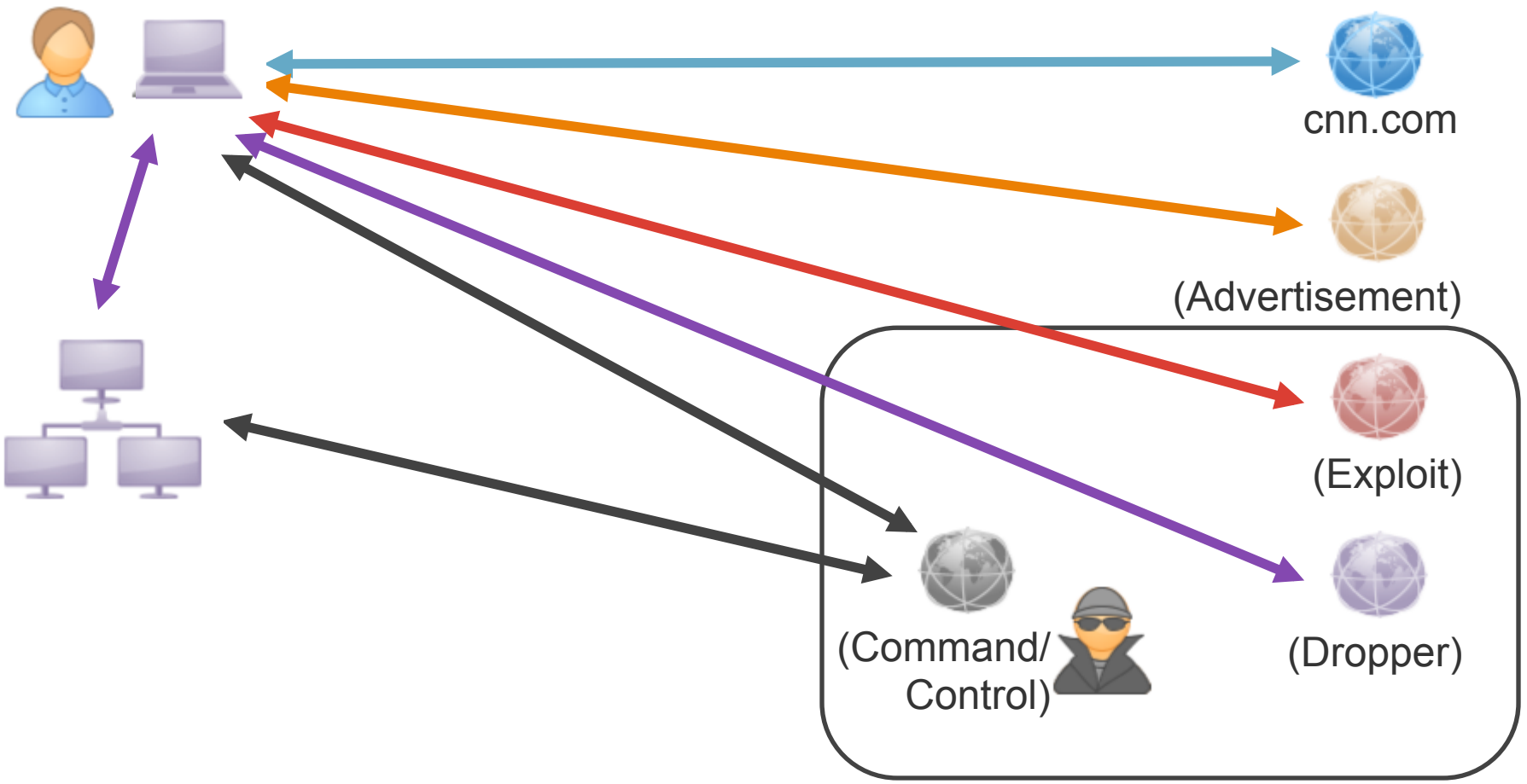
Example Playbook



Next-generation threats like the RSA attack use successive inbound and outbound stages

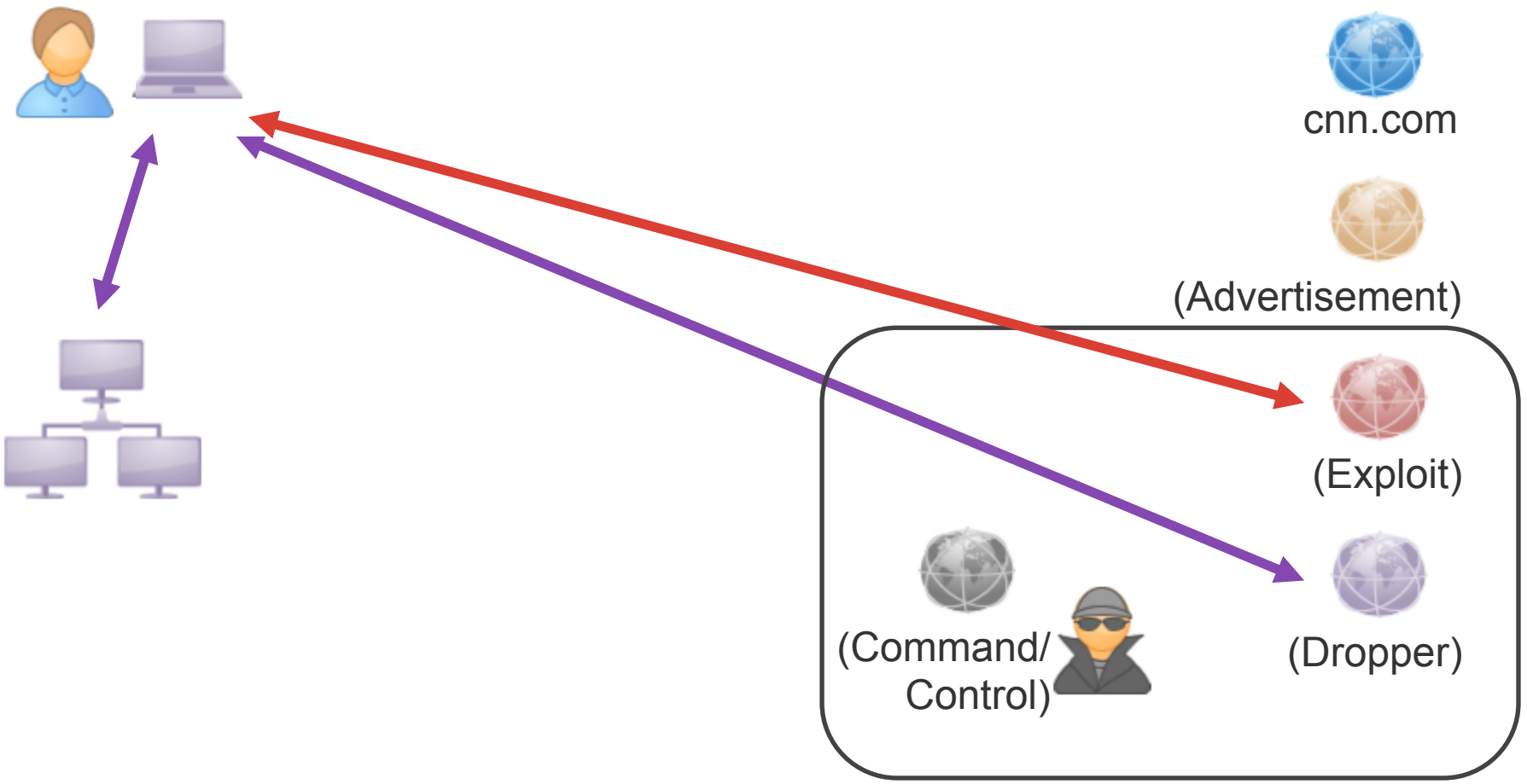
FireEye

Malware Infection Lifecycle



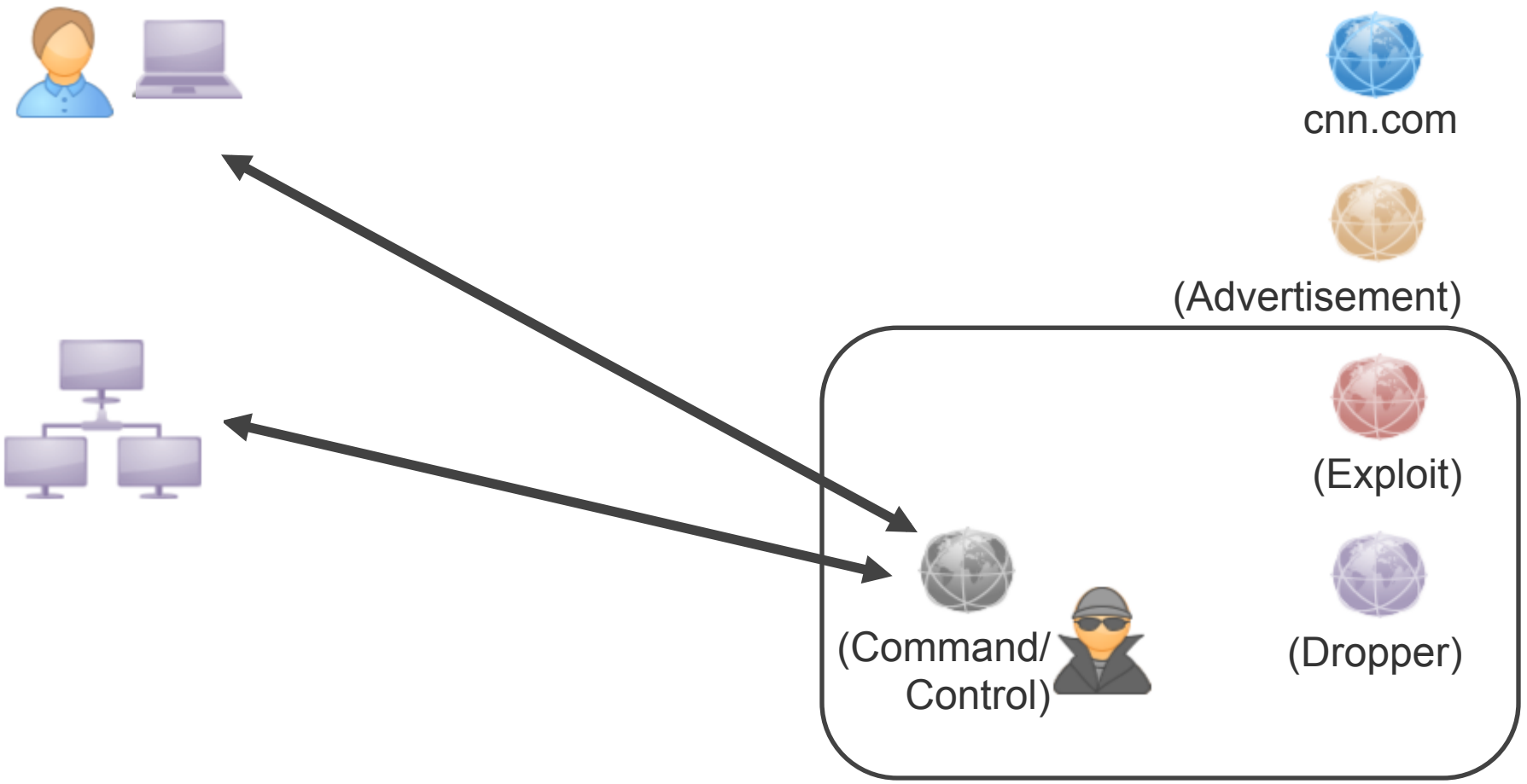
FireEye

Infection Phase



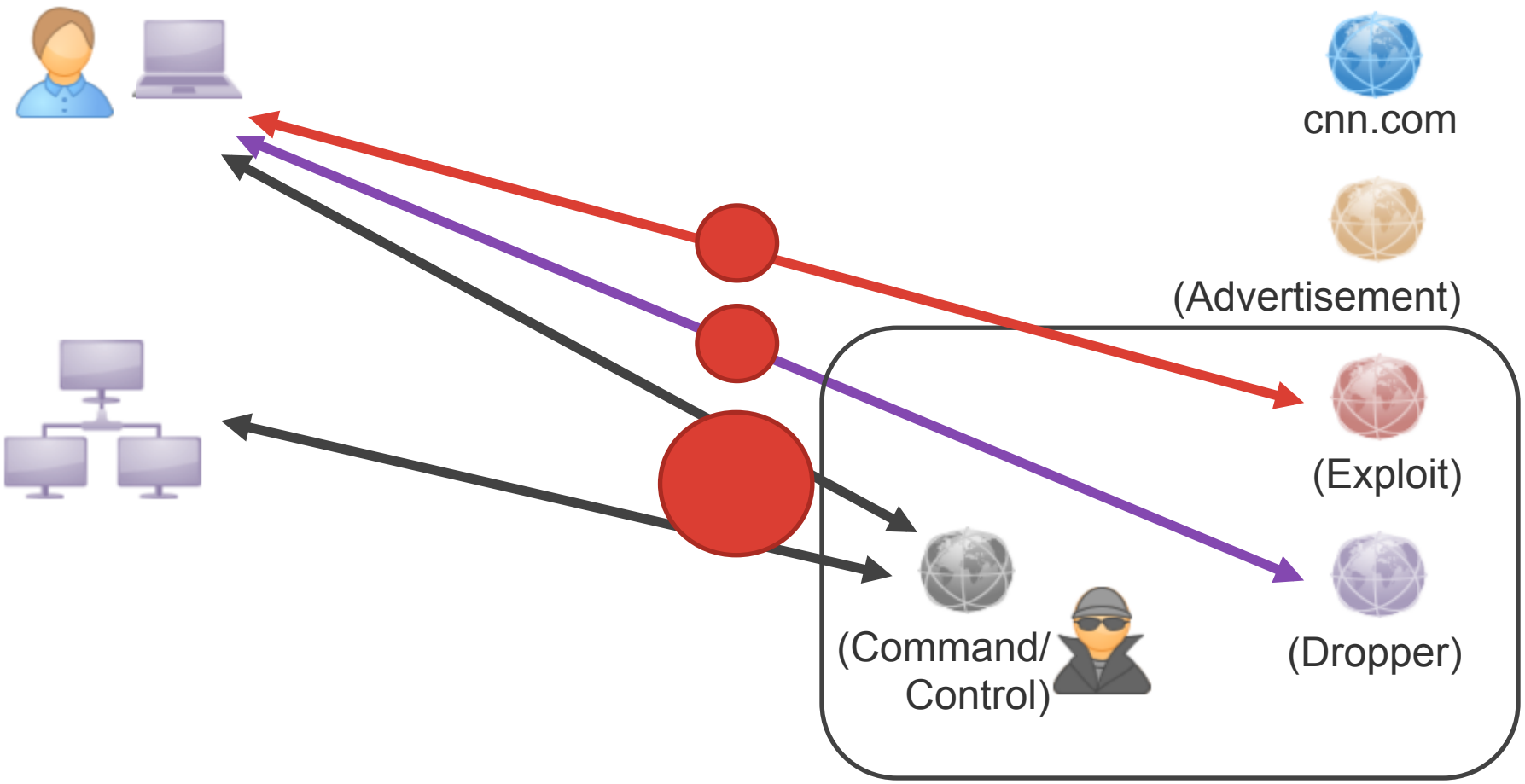
FireEye

Callback Phase



FireEye

Three Independent Detections…Correlated



FireEye

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!

FireEye

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

Special Offer

- Evaluate RSA Secur

Weekly Webinar

RSA invites you to cor
SecurID technical exp

FireEye

LinkedIn Account Type: Basic

Home Profile Contacts Groups Jobs Inbox 32 Companies News More

« Go back to Search Results

Kevin Brisson

3rd

E-Discovery Litigation Support Engineer

Greater Boston Area | Security and Investigations

Current	**Sr E-Discovery Internal Litigation Support Engineer** at [redacted]
Past	Principal Exchange Systems Administrator at [redacted]
Connections	**83** connections
Public Profile	http://www.linkedin.com/in/kevinmbrisson

Share PDF Print

Experience

Sr E-Discovery Internal Litigation Support Engineer

[redacted]

nformation Technology and Services industry

January 2008 – Present (3 years 10 months)

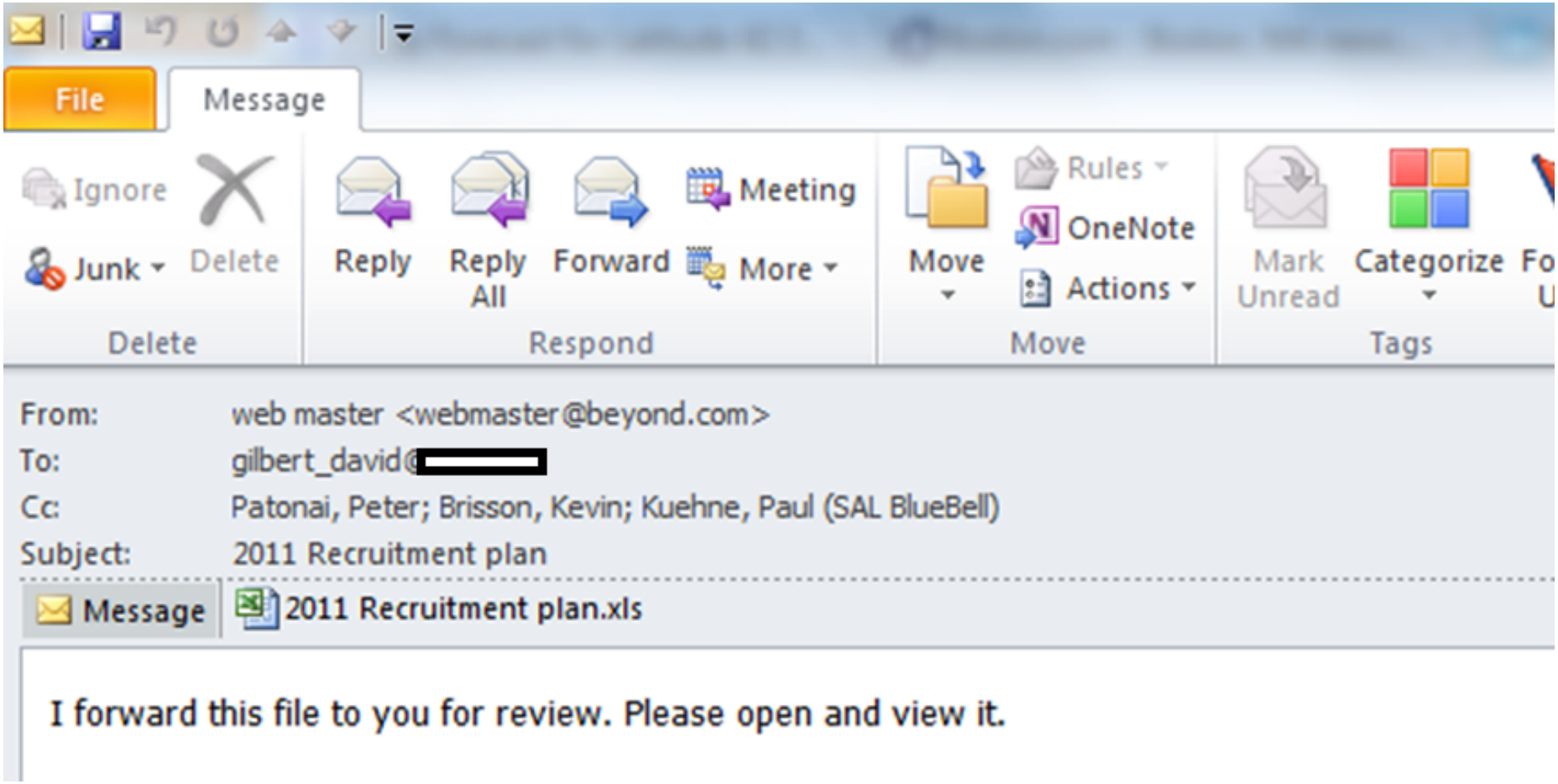
Principal Exchange Systems Administrator

[redacted]

Information Technology and Services industry

January 1999 – January 2008 (9 years 1 month)

Actual spearphish (H/T, @mikko)



FireEye

RSA hack targeted Flash vulnerability

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

About this blog

STAFF

Mapping Babel

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, up82673.hopto.org and www.cz88.net.

RSA malware found
9 months before hand!

```
malware=# select checksum,received from samples where checksum in (select checksum
malware(# from fqc where server_dns_name = 'good.mincesur.com') order by received desc;
             checksum             |          received
----------------------------------+----------------------------
 b773532d91e3f1389954fb612f0d1cff | 2011-05-05 18:19:57.942634
 687a892132c7b539661173ded4026005 | 2011-04-13 17:14:15.372646
 d21fa7722b22734bd0fe84d533814daa | 2011-03-17 01:15:48.76623
 401fd9e862dd92e22bb2038273a50108 | 2011-01-07 23:52:48.74855
 f44b251bdb374a1e41087d96dd067be6 | 2010-12-18 08:43:17.618809
 e3b26ffca3310e11f2fa9518b2ebe756 | 2010-11-13 01:41:24.197708
 401fd9e862dd92e22bb2038273a50108 | 2010-11-12 16:15:16.85705
 401fd9e862dd92e22bb2038273a50108 | 2010-11-09 14:08:05.284567
 188ed479857cc58a1a50533b8749b4c0 | 2010-11-08 09:07:44.752825
 401fd9e862dd92e22bb2038273a50108 | 2010-11-08 08:42:35.165699
 cd03a6c6857cc15af10d8be4107c7f89 | 2010-10-16 02:06:36.098503
 687a892132c7b539661173ded4026005 | 2010-09-22 17:38:10.200891
 188ed479857cc58a1a50533b8749b4c0 | 2010-09-22 17:38:09.83623
 188ed479857cc58a1a50533b8749b4c0 | 2010-09-22 16:42:29.706815
 687a892132c7b539661173ded4026005 | 2010-09-22 16:42:29.638815
 cf92541173413c52a657842deb2c5d22 | 2010-09-22 16:42:29.582547
 cd03a6c6857cc15af10d8be4107c7f89 | 2010-09-22 16:01:31.461162
 b773532d91e3f1389954fb612f0d1cff | 2010-09-10 20:39:39.339465
 a1bedd0dc4f5099055dd8e05328fa7fd | 2010-09-10 19:47:07.255989
 b773532d91e3f1389954fb612f0d1cff | 2010-09-08 15:35:15.336999
 177af09e1fd3a9c6a324545388fd46ce | 2010-09-08 14:46:24.924165
 cf92541173413c52a657842deb2c5d22 | 2010-08-21 00:42:51.354382
 a1bedd0dc4f5099055dd8e05328fa7fd | 2010-08-21 00:00:28.555255
 241566ba80274ce270e13a04cddd4d0d | 2010-08-20 23:41:37.080018
 a1bedd0dc4f5099055dd8e05328fa7fd | 2010-08-09 15:39:56.810414
 cf92541173413c52a657842deb2c5d22 | 2010-07-08 15:38:11.360401
(26 rows)
```

Simple Website Review: www.same.org

Home | About SAME | Events | Membership | Publications | Committees & Councils | SAME Operations | Contact Us

- Home
- + About SAME
- + Events
- + Membership
- + Publications
- + Committees & Councils
- + SAME Operations
- Contact Us

Home >> Contact Us

ShareThis

Contact SAME

607 Prince St.
Alexandria, VA 22314-3117 (view Google Map)
Main Telephone Number: 703-549-3800
Executive Office Fax: 703-684-0231
Membership & Conferences Fax: 703-548-1463
Communications & Finance Fax: 703-548-6153

Executive Office

Executive Director Robert D. Wolff, Ph.D., P.E., F.SAME	Ext. 110	rwolff@same.org
Office Manager Desyreé Jones	Ext. 111	djones@same.org
Administrative Assistant Danielle Tigue	Ext. 112	dtigue@same.org
Logistics & Administrative Services Specialist Otis Carter	Ext. 114	ocarter@same.org

Continuing Education

Director of Continuing Education Robert D. Wolff, Ph.D., P.E., F.SAME	Ext. 110	rwolff@same.org
Webinar and Course Manager Belle Febbraro	703-924-2616	bfebbraro@same.org

UPCOMING EVENTS

Post Leaders Workshop
August 6-8, 2012

SAME Executive Forum
August 21-22, 2012
View all events

CONNECT WITH SAME

View all social media

In this issue of The Military Engineer

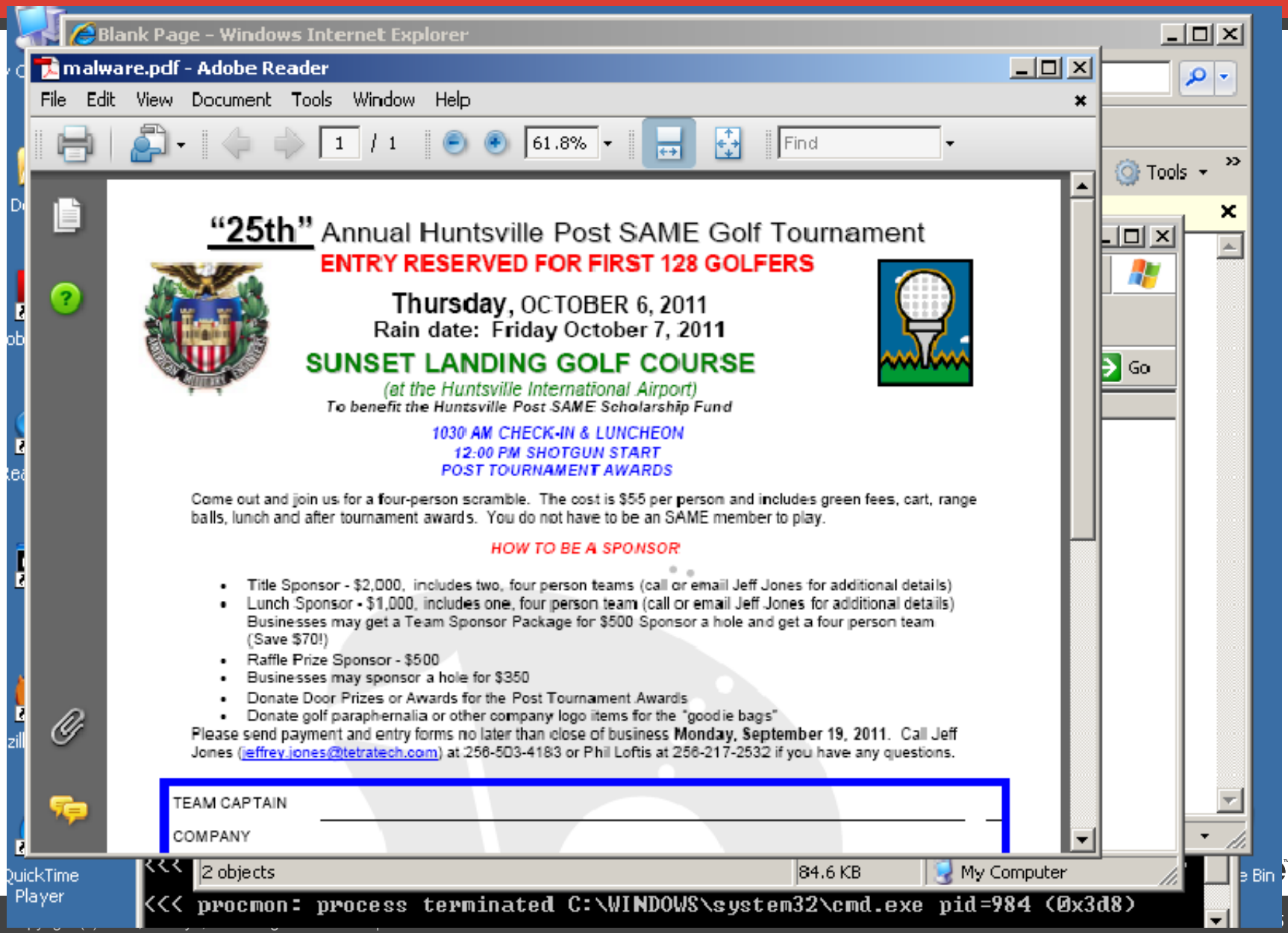
Sustainable Installations
July August 2012

Support to Wounded Warriors

JOB CENTER

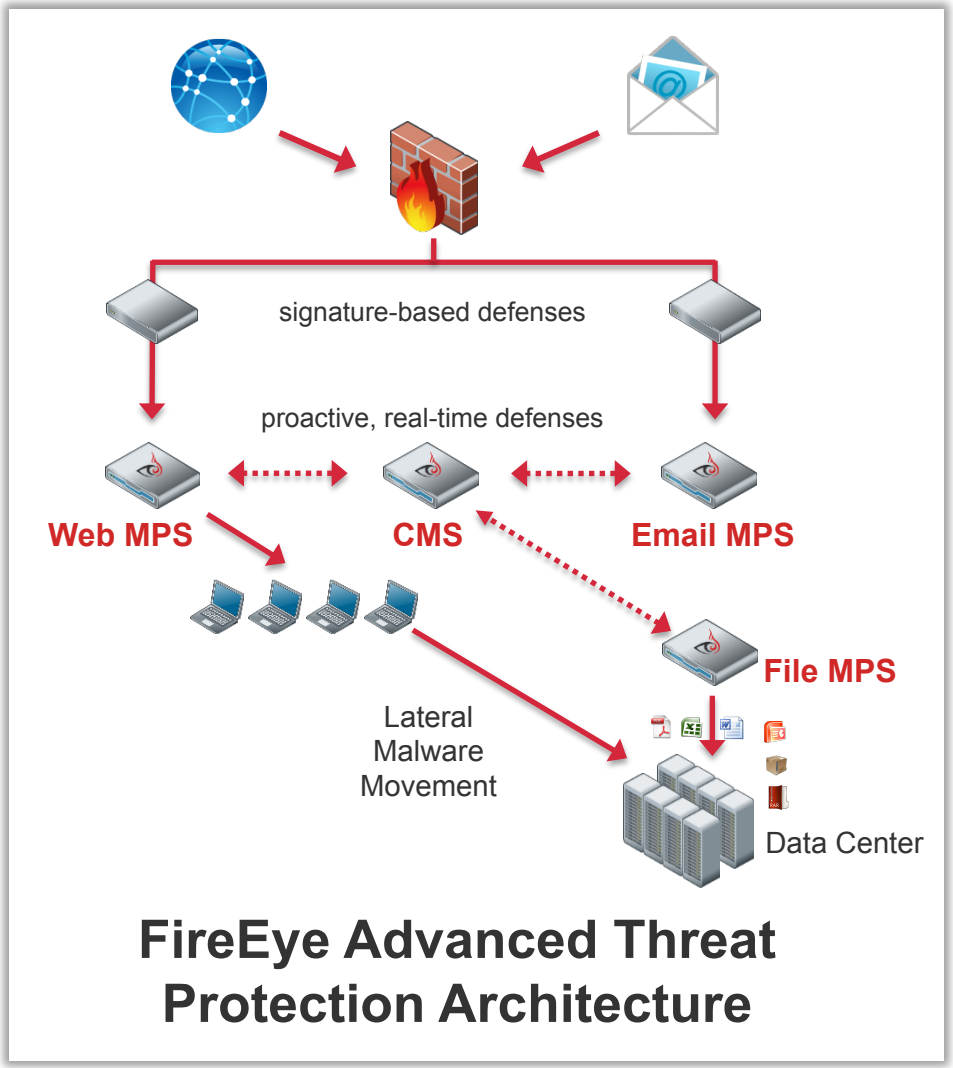
FireEye

Upcoming Golf Tournament




FireEye Overview

Protecting Against Advanced Targeted Attacks

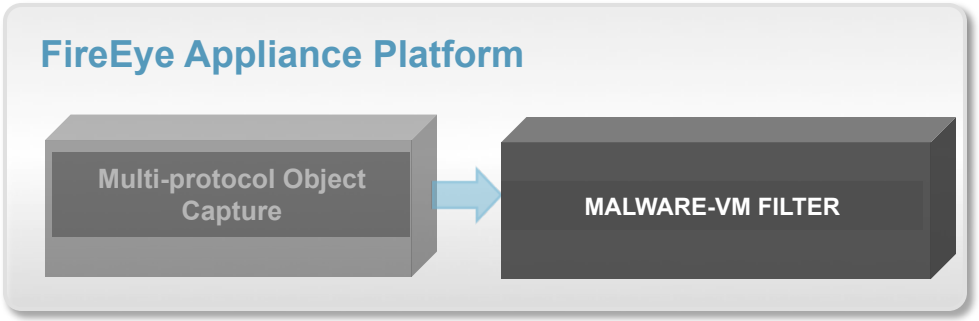


FireEye Advanced Threat Protection Architecture

- 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

FireEye

Multi-Protocol, Real-Time VX Engine



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

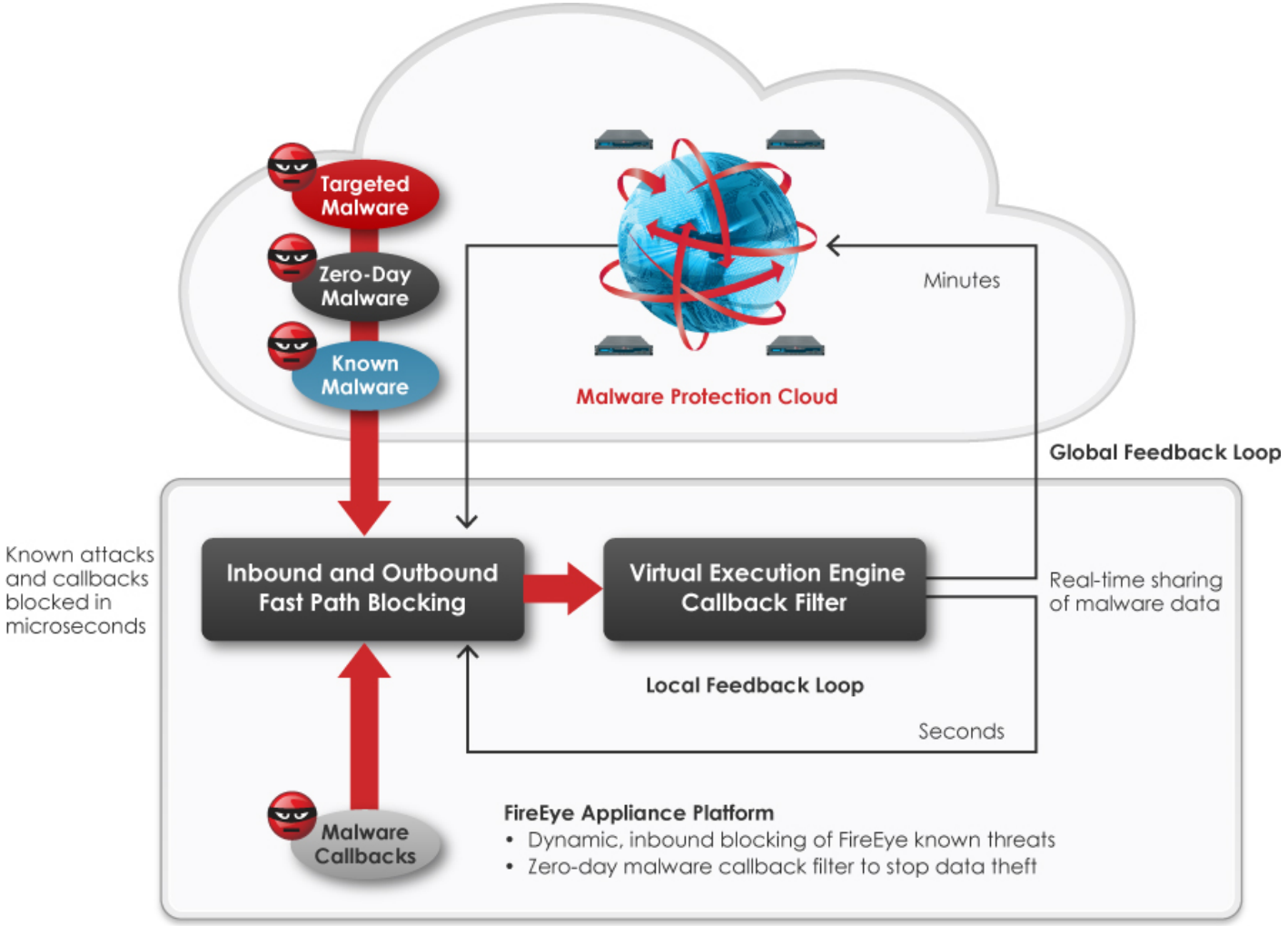
Map To Target OS&Apps

Virtual Execution Environments Phase 2

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

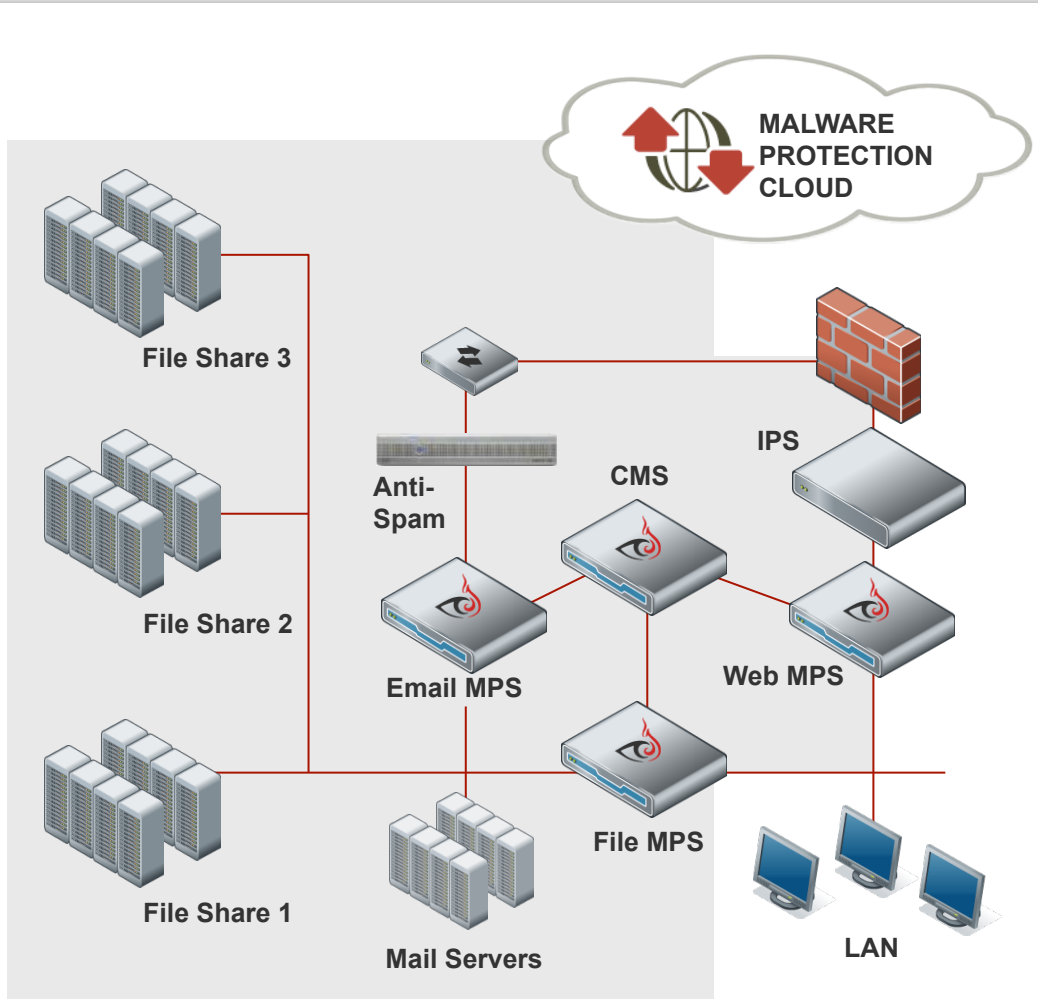
FireEye

Global Intelligence to Protect Local Network



FireEye

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

FireEye

FireEye making a difference

THE CYBERCRIME ECONOMY

Grum takedown: '50% of worldwide spam is gone'

CNNMoney

164 comments

By Stacy Cowley @CNNMoneyTech July 19, 2012: 1:09 PM

Recommend 4.7k Tweet 553 Share

Security researchers estimate that 50% of worldwide spam ha

Third largest Botnet Grum Turn Off: Fire Eye

22 days ago by ankur 0

Tweet 11 +1 1 Share Pin it 1

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

FireEye™

Q&A