A Behind the Scenes Look at Cyber Breaches

Secure the Village
Cybersecurity Roundtable
July 2016

Stan Stahl, Ph.D.
President
Citadel Information Group

From: Facebook [mailto:notification+zrdodp6ihooz@facebookmail.com]
Sent: Saturday, July 23, 2011 4:32 PM
To: Kathrine Hepburn
Subject: See Your Friends at 20th High School Reunion

Facebook

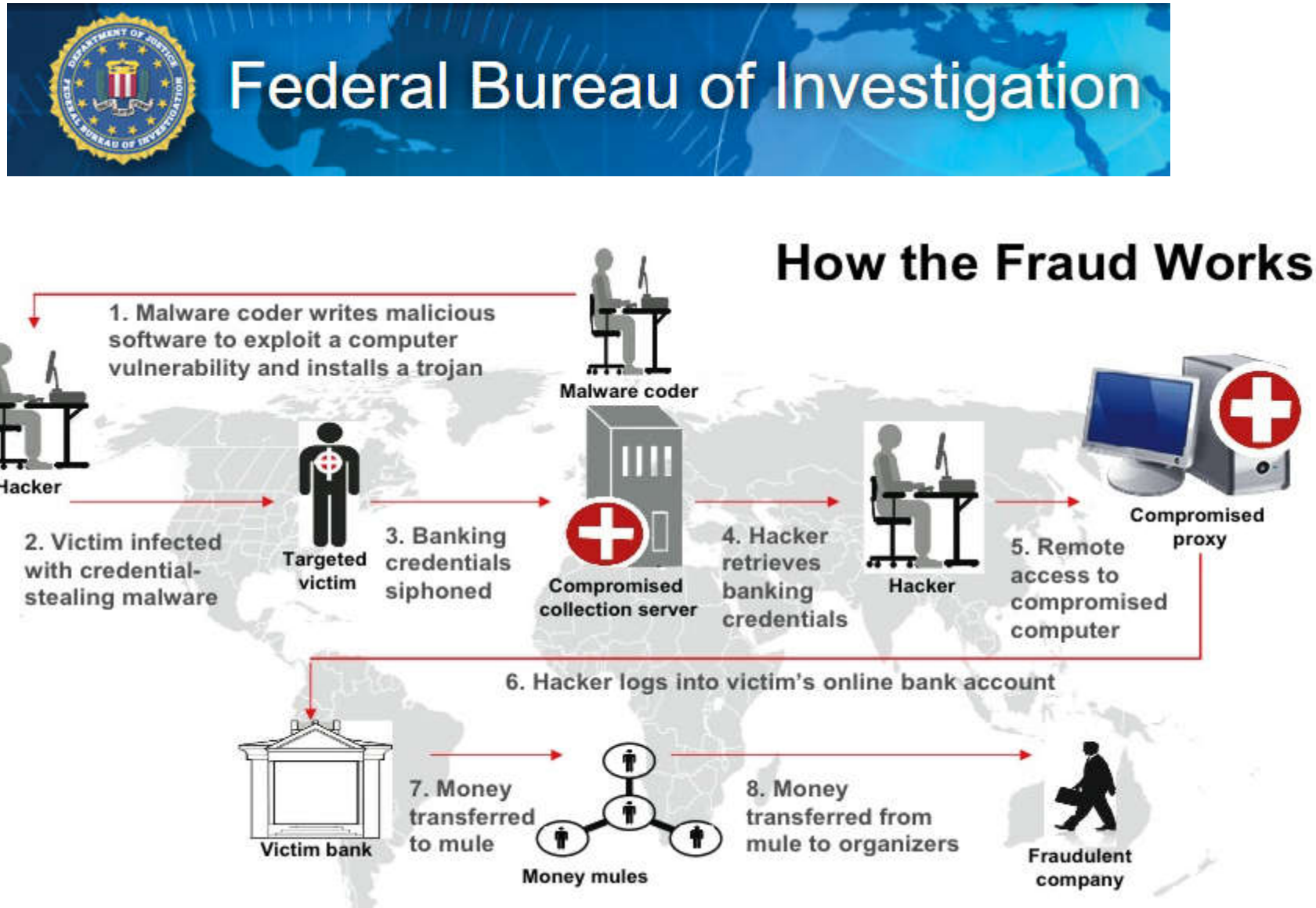
Hi Kate

Mark your calendar.

June 18 is the 20th Anniversary of our graduation from Algonquin High.

Visit Our Facebook Page for More Information.

Visit Page **See All Requests**

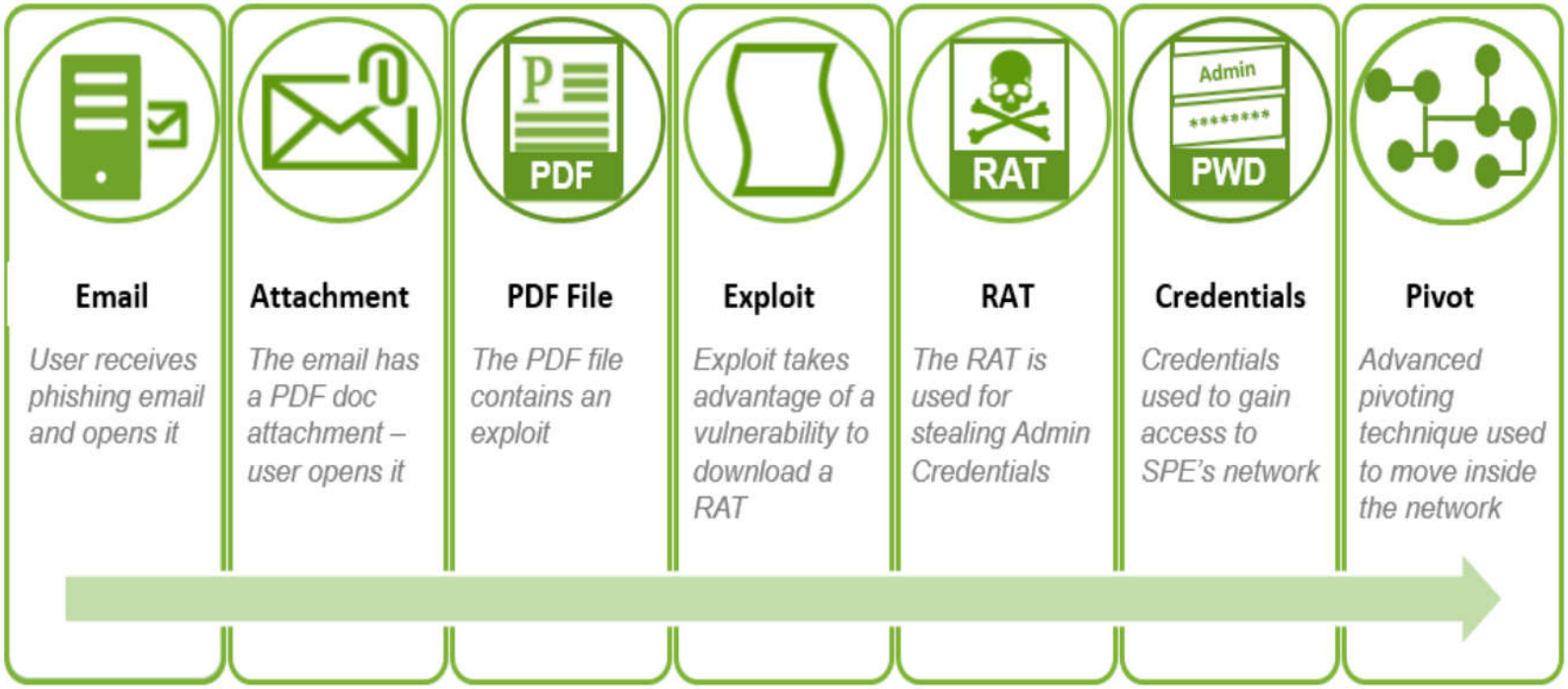


https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud

IBM Security Intelligence

Sony breach by Russian hackers

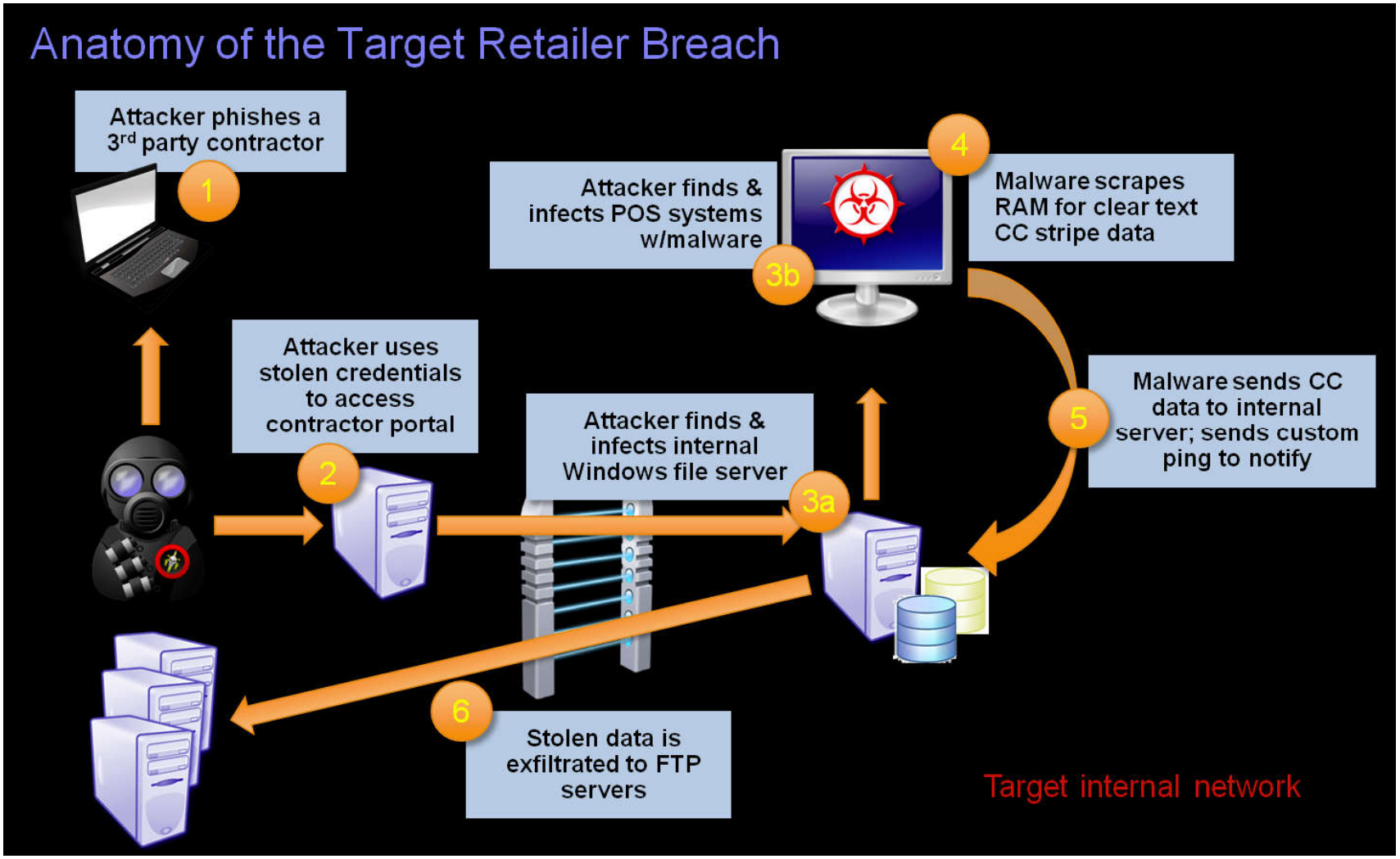
Spear-phishing email sent to employees in Russia, India and other parts of Asia



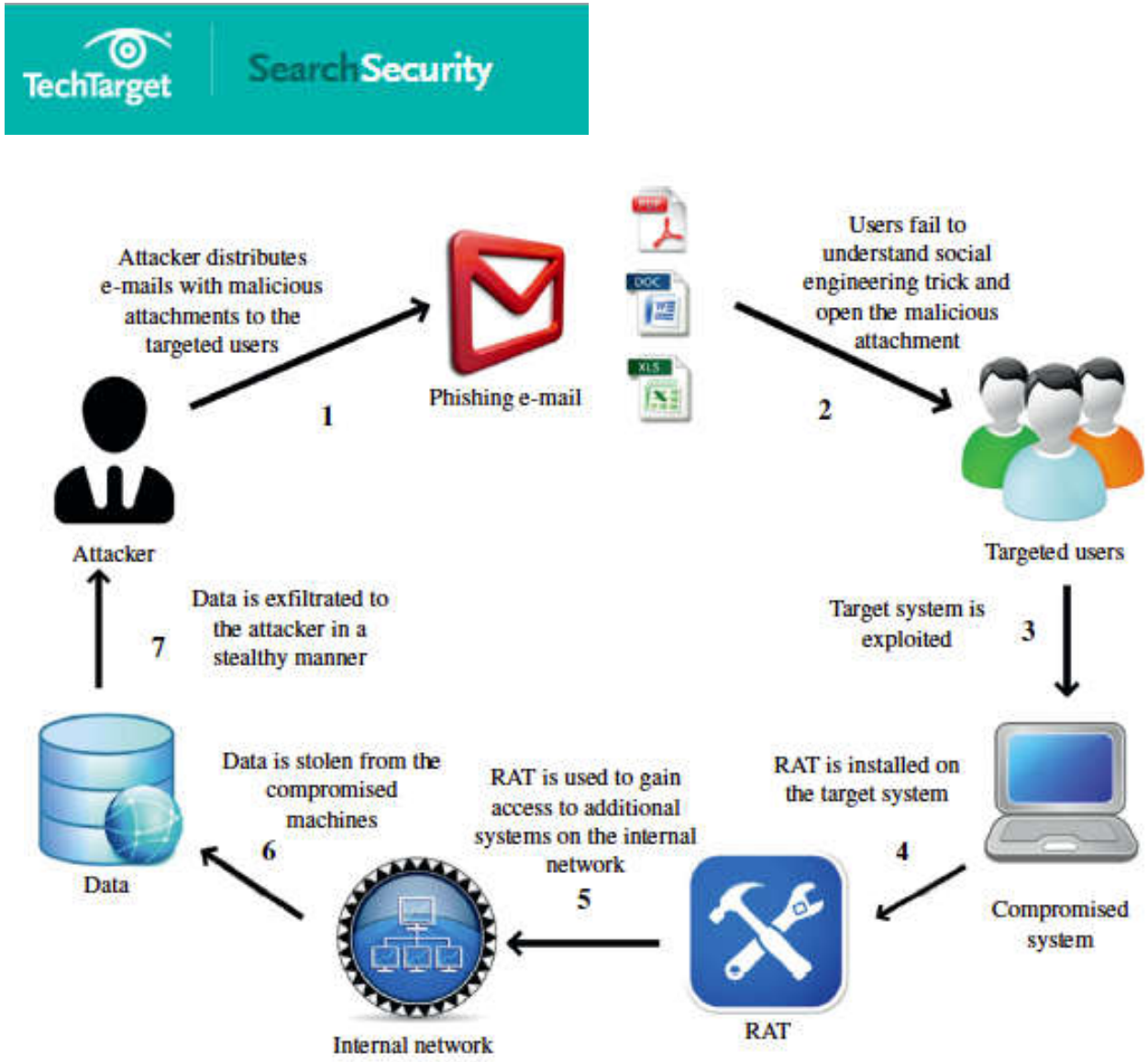
RAT: Remote Access Trojan

https://securityintelligence.com/who-hacked-sony-new-report-raises-more-questions-about-scandalous-breach/

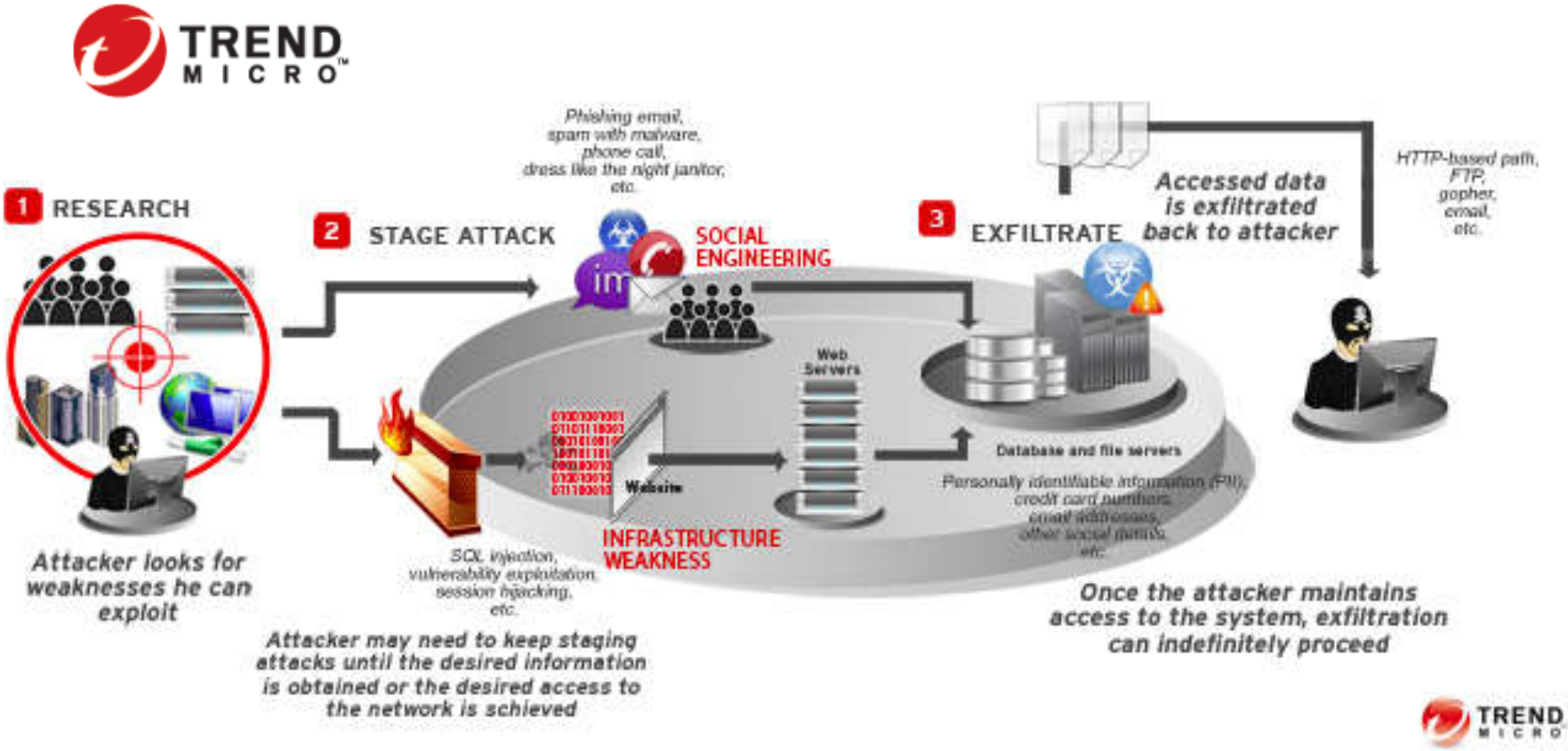
IBM Security Intelligence



https://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/



http://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks

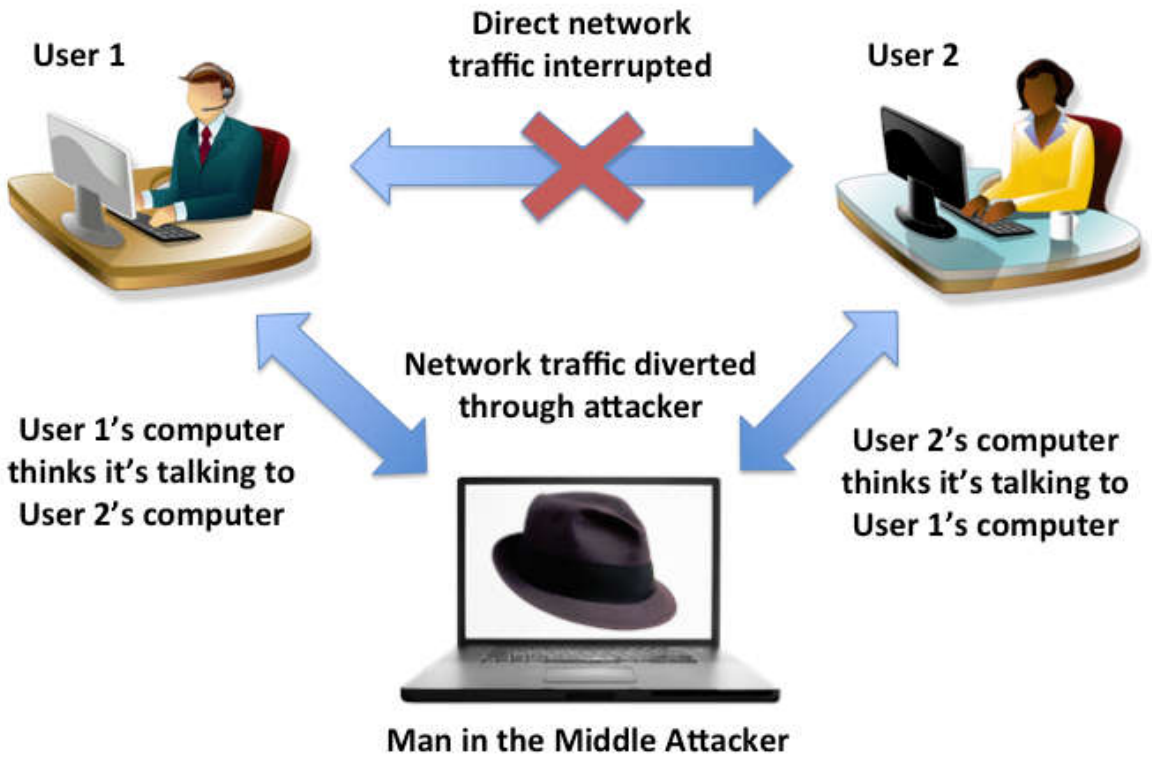


MALICIOUS DATA BREACH DIAGRAM

http://about-threats.trendmicro.com/dumpimages/238201144426.jpeg

CS111 Winter 2013 Lecture 17: Introduction to Security
Scribe notes prepared by Gary Chao and Bryant Khau

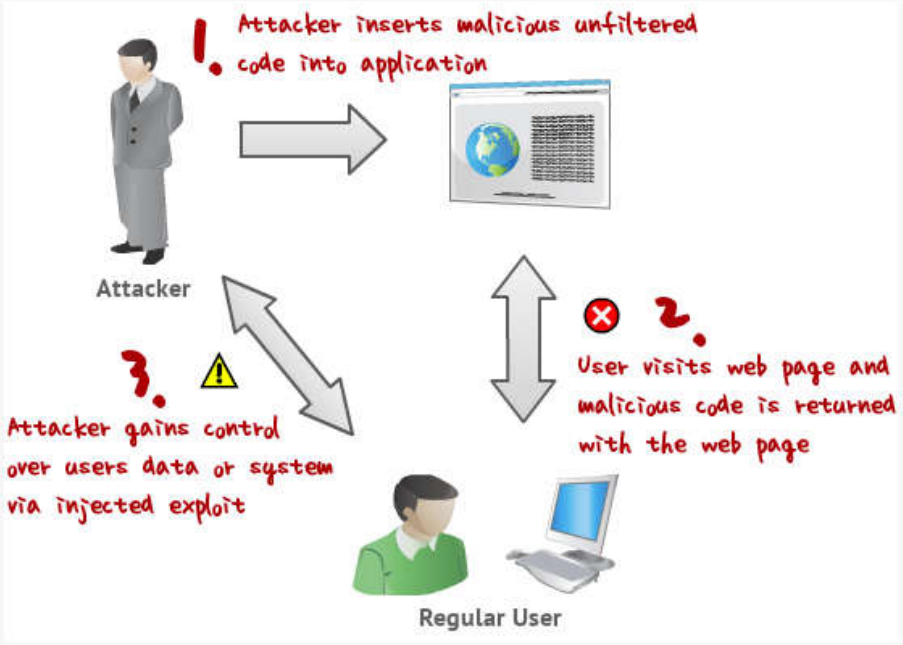
Man-in-the-Middle Attack



http://web.cs.ucla.edu/classes/winter13/cs111/scribe/17b/

Attacking a User by Attacking a Web Site They Visit

Attacker -> exploits web application -> web application delivers a malicious script to a normal users browser -> attacker now has the ability to control the users browser. This is bad for the user and bad for you if you manage the web application.



Some examples of the damage an XSS attack can cause:

- Redirect page to phishing sites, or fake login pages
- Steal the users cookies, allowing them access to other web applications with authenticated sessions
- Insert links to remotely hosted client side exploits within a html body; with the goal of installing malware on the system (key loggers, remote access tools)

https://hackertarget.com/xss-tutorial/

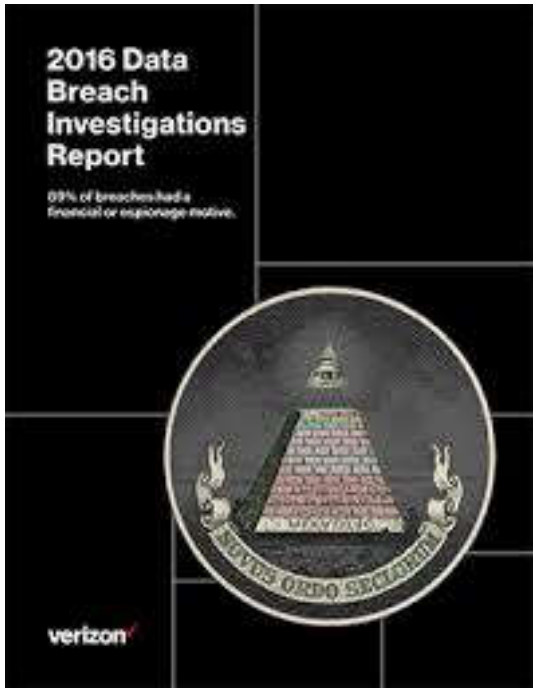
CITADEL INFORMATION GROUP, INC.

Defensive Tactics

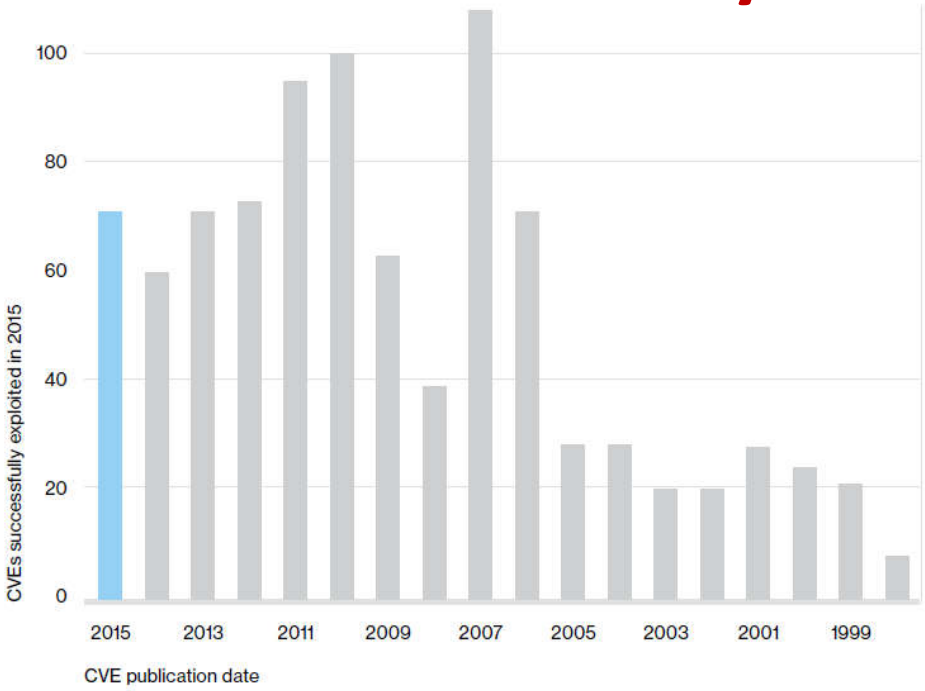
To warn of an evil is justified only if, along with the warning, there is a way of escape.

Cicero, On Divination, Book II, 44 BCE

There Are Significant Opportunities to Level the Playing Field



80% of breaches preventable with basic security



The Vast Majority of Breaches Exploit Vulnerabilities for Which Upgrades Have Been Available for Well-Over a Year

CITADEL INFORMATION GROUP, INC.

The Seven Key Defense Strategies

Implement Formal <u>Information Security Management System</u>

1. Information Security Manager / Chief Information Security Officer
   a. C-Suite and Board Governance
   b. Independent Perspective from CIO or Technology Director
   c. Supported by Cross-Functional Leadership Team
   d. Supported with Subject-Matter Expertise
2. Implement Formal Risk-Driven Information Security Policies and Standards
3. Identify, Document and Control Sensitive Information
4. Train and Educate Personnel. Change Culture.
5. Manage Vendor Security
6. Manage IT Infrastructure from “information security point of view”
7. Be prepared. Incident Response and Business Continuity Planning.

CITADEL
INFORMATION GROUP, INC.


Information Peace of Mind ®
Information Security Proactively Managed
Commercially Reasonable Information Security Practices
Lower Total Cost of Information Security SM

Citadel Information Group: Who We Are

Stan Stahl, Ph.D
Co-Founder & President

35+ Years Experience
Reagan White House
Nuclear Missile Control

Kimberly Pease, CISSP
Co-Founder & VP

Former CIO
15+ Years Information Security Experience

David Lam, CISSP, CPP
VP Technology Management Services

LABJ CIO of Year
20+ Years Information Security Experience

CITADEL
INFORMATION GROUP, INC.

Citadel Information Group: What We Do

Deliver *Information Peace of Mind* SM
to Business and the Not-for-Profit Community

Cyber Security Management Services

Information Security Leadership

Information Security Management Consulting & Coaching

Assessments & Reviews … Executive Management …Technical Management

Secure Network Engineering … Secure Software Engineering

Incident Response / Business Continuity Planning

Adverse Termination

CITADEL
INFORMATION GROUP, INC.

For More Information

Stan Stahl Stan@citadel-information.com 323-428-0441
LinkedIn: Stan Stahl Twitter: @StanStahl

Citadel Information Group: www.citadel-information.com
Information Security Resource Library

Free: Cyber Security News of the Week
Free: Weekend Vulnerability and Patch Report

CITADEL
INFORMATION GROUP, INC.

A Behind the Scenes Look at Cyber Breaches

Thank You!

Secure the Village

Cybersecurity Roundtable

July 2016

Stan Stahl, Ph.D.
President
Citadel Information Group