KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

Monitoring techniques for information and network security
(INT1429)

Huỳnh Trọng Thưa
htthua@ptithcm.edu.vn

Aurora Attack

Dec 2009

- In December, 2009, Google discovered that confidential materials were being sent out of their network to China.
- Google hacked into the Chinese server and stole data back, discovering that dozens of other companies had also been exploited, including Adobe and Intel.

Aurora Attack Sequence

- Attacks were customized for each target based on vulnerable software and antivirus protection
  1. A user is tricked into visiting a malicious website
  2. Browser exploited to load malware on target PC
  3. Malware calls home to a control server
  4. Local privilege escalation
  5. Active Directory password database stolen and cracked
  6. Cracked credentials used to gain VPN Access
  7. Valuable data is sent to China.

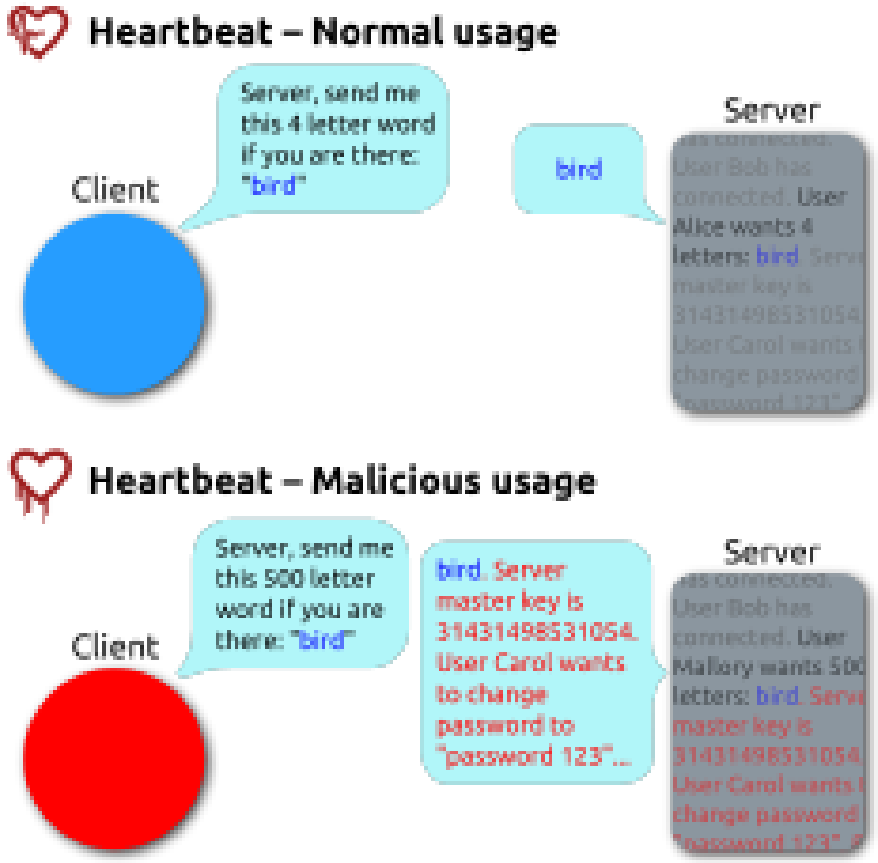
Heartbleed

2012-2014

- Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security(TLS) protocol.
- The bug was named by an engineer at Codenomicon, a Finnish cybersecurity company that also created the bleeding heart logo and launched the domain heartbleed.com to explain the bug to the public
- Both Google and Codenomicon discovered it independently at approximately the same time.

A depiction of Heartbleed

- At the time of disclosure, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords.



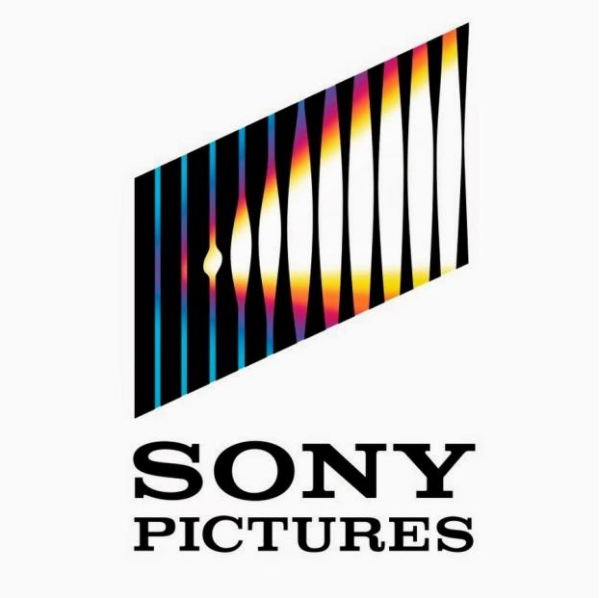
Play Station Network Outage

2011

- The **2011 PlayStation Network outage** was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 and PlayStation Portable consoles from accessing the service.

Sony Picture Entertainment Hack

2014



- On November 24, 2014, a hacker group which identified itself by the name "Guardians of Peace" (GOP) leaked a release of confidential data from the film studio Sony Pictures.
- The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information.

Yahoo! data breaches

2013-2016

- The Internet service company Yahoo! reported two major data breaches of user account data to hackers during the second half of 2016.
- The first announced breach, reported in September 2016, had occurred sometime in late 2014, and affected over 500 million Yahoo! user accounts.
- A separate data breach, occurring earlier around August 2013, was reported in December 2016. Initially believed to have affected over 1 billion user accounts,Yahoo! later affirmed in October 2017 that all 3 billion of its user accounts were impacted.

Yahoo! data breaches

2013-2016

- Both breaches are considered the largest discovered in the history of the Internet.
- Specific details of material taken include names, email addresses, telephone numbers, encrypted or unencrypted security questions and answers, dates of birth, and hashed passwords.
- Further, Yahoo! reported that the late 2014 breach likely used manufactured web cookies to falsify login credentials, allowing hackers to gain access to any account without a password.

WannaCry ransomware attack

May 2017

The **WannaCry ransomware attack** was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

WannaCry ransomware attack

May 2017

- It propagated through EternalBlue, an exploit in older Windows systems released a few months prior to the attack.
- While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems.
- WannaCry also took advantage of installing backdoors onto infected systems.
- The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further.
- The attack was estimated to have affected more than 300,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.
- Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.
- In Dec 2017, the United States and the United Kingdom formally asserted that North Korea was behind the attack.

New Recommendations

Here is a few short-term recommendations, as given by iSEC:

1. Log and inspect DNS traffic
2. Establish internal network surveillance capability
3. Control inbound and outbound network traffic
4. Expand log aggregation
5. Expand Windows endpoint control
6. Audit VPN access and enrollment.
7. Test malware scanning against known rootkits.

As regards long-term goals, companies should:

1. Build a security operations team
2. Secure your overseas offices
3. Classify and catalog sensitive data
4. Secure their Active Directory network (smartcard logins, steering clear of shared local accounts, using read-only domain controllers in overseas offices, and more).

The main lesson to be learned from these attacks is that times have changed. Anti-virus solutions and patching are no longer enough

Grading

- Class participation: 10%
- Lab: 10%
- Mid-Term: 10%
- Project (Final exam): 70%

Tentative Schedule

- Week 1 *Network Security Monitoring Rationale*
  Week 2 *Collecting Network Traffic: Access, Storage, and Management*
- Week 3 *Standalone NSM Deployment and Installation*
- Week 4 *Command Line Packet Analysis Tools*
- Week 5 *Graphical Packet Analysis Tools*
- Week 6 *NSM Consoles*
- Week 7 *NSM Operations*
- **LAB (10%)**
- Lab 1 *NSM with Security Opinion*
- Lab 2 *Using Packet Analysis Tools : NetworkMiner, Sguil, Squert*
- **FINAL EXAM** *Project*

References

1. Richard Bejtlich, The Practice Of Network Security Monitoring, No Starch Press, 2013.
2. Slides of Sam Bowne on Network Security Monitoring, https://samsclass.info/50//50_WinterWWC17.shtml
3. Chris Sanders and Jason Smith, Applied Network Security Monitoring, Syngress, 2014.
4. Richard Bejtlich, The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley, 2004.