CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Worms and Social Engineering

Video Summary

- What are worms?
- Examples for well-know worms
- Worm target discovery
- Social Engineering
- Social Engineering Case Study

Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Worm Target Discovery

Scanning (or fingerprinting)

- First function in the propagation phase for a network worm
- Searches for other systems to infect

Random

- Each compromised host probes random addresses in the IP address space using a different seed

Hit-list

- The attacker first compiles a long list of potential vulnerable machines
- Once the list is compiled the attacker begins infecting machines on the list
- Each infected machine is provided with a portion of the list to scan
- This results in a very short scanning period which may make it difficult to detect that infection is taking place

Topological

- This method uses information contained on an infected victim machine to find more hosts to scan

Local subnet

- If a host can be infected behind a firewall that host then looks for targets in its own local network
- The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

Worm Attacks

Melissa	1998	E-mail worm First to include virus, worm and Trojan in one package
Code Red	July 2001	Exploited Microsoft Internet Information Services (IIS) bug Probes random IP addresses Consumes significant Internet capacity when active
Code Red II	August 2001	Also targeted Microsoft IIS Installs a backdoor for access
Nimda	September 2001	Had worm, virus and mobile code characteristics Spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	Exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	Exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	Mass-mailing e-mail worm Installed a backdoor in infected machines
Warezov	2006	Creates executables in system directories Sends itself as an e-mail attachment Can disable security related products
Conficker (Downadup)	November 2008	Exploits a Windows buffer overflow vulnerability Most widespread infection since SQL Slammer
Stuxnet	2010	Restricted rate of spread to reduce chance of detection Targeted industrial control systems

Code Red

- July 16 2001
- Worm aimed at Microsoft Internet Information Server (IIS) web servers (not users)
- Sent to web server as HTTP GET request
  - Bug in IIS allows the code to be stored by the server
  - Worm was stored in RAM; a reboot deleted the worm
- Worm had several states:
  - On first 19 days of month, send HTTP GET requests to random IP addresses, with the intention of infecting other web servers
  - On days 20 to 28, creates a DoS attack on www.whitehourse.gov
  - Dormant for the remaining of the month
- Infected 20,000 servers in 5 hours
- Consumed significant network resources (DoS attack)

Code Red II

- 4 August 2001
- Similar to CodeRed but also installed a Trojan horse on the web server
- Allowed anyone with web browser to send commands to web server:
  - Eg: delete or modify files on server

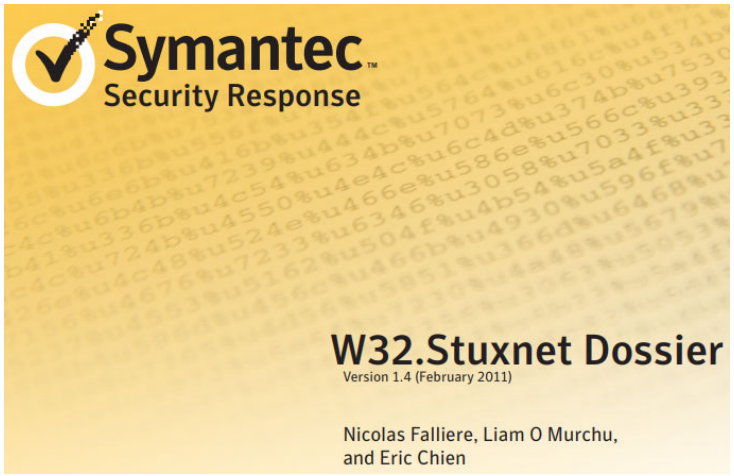
Stuxnet Worm

- **Stuxnet** is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005

- Stuxnet targets PLC and supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran

Stuxnet Worm

- Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart



Mobile Phone Worms

- First discovery was Cabir worm in 2004
- Then Lasco and CommWarrior in 2005
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages
- Recent attacks on Mobile phones: https://www.youtube.com/watch?time_continue=75&v=nZ_56MH_RV4&feature=emb_logo

Mobile Phone Worms

DroidKungFu

This piece of malware is unique in that it is able to avoid detection by antimalware software, according to the Wall Street Journal. It installs a backdoor in the Android OS that allows hackers to gain full control over a user's mobile device.

Mobile Phone Worms

DroidDream

This piece of malware, discovered in March 2011, has packaged itself inside legitimate applications in the official Android market that were released under developers "Kingmall2010," "we20090202," and "Myournet," according to MSNBC. The malware can then send user information to a remote server. A new variant of DroidDream – called DroidDreamLight – was discovered in May 2011.

Mobile Phone Worms

Android.Pjapps

Some Trojans can disguise themselves as legitimate applications. One example is Android.Pjapps, which hijacked the Steamy Windows app on Android, according to Symantec. The malicious app is similar to the legitimate one and even works – fogging up the screen – but it works in the background to send text messages to premium rate numbers, which in turn pays the creators of the Trojan.

What is Social Engineering

Social Engineer is someone who is a master of asking seemingly non-invasive or unimportant questions to gather information over time

- Gain trust
- Reduce defenses

Can be combined with a number of techniques to gather sensitive information

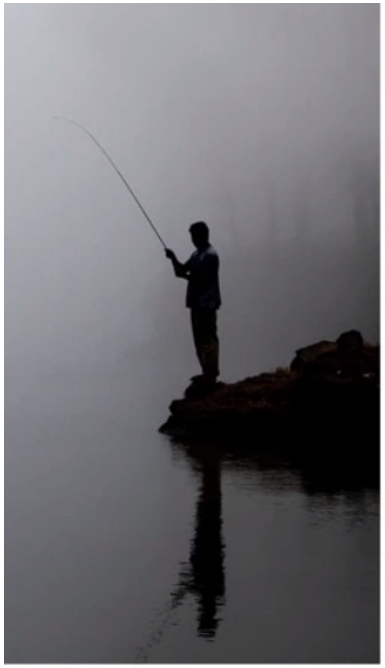
Social Engineering Attacks

Phishing
Attack via electronic communication (i.e. email) posing as someone trustworthy

Spear Phishing
Targeted attack appearing to come from a trusted source, often within the victim's own company, from someone in a position of authority

Whaling
Specific attack targeting high-profile business executives, upper management, etc.

Social Engineering Attacks (Fishing)



Very common

Impersonation (spoofing) of legitimate person or organization

Identity theft, credential theft

Delivery vehicles:

- E-mail
- Instant messaging
- Websites
- Phone calls

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you.

Social Engineering Attacks (Spear Fishing)

Highly targeted phishing attack

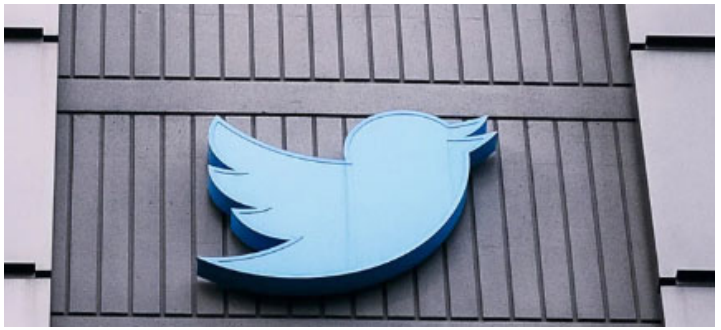
Limited distribution

More likely to use personalized information

May use impersonation of insiders

Users more likely to ascribe authenticity when they see personal details

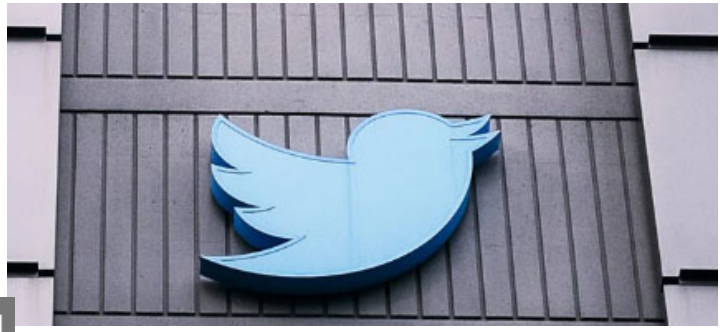
Social Engineering Case Study



- Summer 2020

- **AN** unprecedented Twitter hack saw the accounts of Elon Musk, Barack Obama, Joe Biden, Jeff Bezos, Bill Gates, Apple, Uber, and more fall into the hands of attackers who used that access to push a bitcoin scam?

Social Engineering Case Study



- Scammers received

around $100,000!!

2-3 hours

Video Summary

- What are worms?
- Examples for well-know worms
- Worm target discovery
- Social Engineering
- Social Engineering Case Study