CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 4: Malware - Worms

Worm - Definition

- A worm is self-replicating malware that travels through a network without the assistance of a host application or user interaction.
- A worm resides in memory and can use different transport protocols to travel over a network

Remember: A virus is malicious code that attaches itself to an application and runs when the application is started.

Worms - Overview

- Compromising tens of thousands of computers one-by-one would be a time-consuming task.
- Worms are attack tools that spread across a network, moving from system to system, exploiting weaknesses.
- Worms automate the process of compromising systems. They take over one system and then use that to scan for other vulnerable systems. From here is can self-replicate by using one set of systems to find and conquer new systems. This allows the worms to propagate at an exponential rate.

Worms - Overview

- Worms have been around for decades.
- Robert Tappen Jr released a worm that took down major components of the internet in 1988.
- The difference between viruses and worms is that by definition a virus infects executable host file, programs or operating system and a worm replicates or spreads across a network on its own. These days a large majority of malware is both a virus and a worm.
    - Both of them have malicious payload to carry out its targeted goal.

Worms - Overview

Here are some examples of worms:

- 2001- Ramen, Sadmind/IIS, Code Red I/II, Nimda
- 2002 – Klez, SQLSnake
- 2003 – SQLSlammer, Blaster, Nachia/Welchia
- 2004 – Witty, Bagel, Netsky, MyDoom and Sasser
- 2005 – Zotob and bot-bundling
- 2006 & 2007 saw worms build bot-nets of hundreds of thousands of machines. One of the biggest bot-nets ever detected was discovered in the Netherlands. It had 1.5 million bots which had been taken over by worms.
- 2008 – Conficker Worm
- 2010 – Stuxnet (Severely damaged Iran nuclear plant)
- 2011 – Duqu
- 2012 – Flame, Shamoon

Worms - Overview

Examples of worms:

- 2013 – Cryptolocker (Ransomware)
- 2014 – Regin
- 2015 – SMiShing (A new way of hacking using SMS)
- 2016 – Tiny Banker Trojan

- Some details from

http://techtwisted.com/10-dangerous-computer-viruses-decade-2007-2016/

Worms - Overview

- Malicious Worms are quickly evolving, increasing their capabilities to spread and cause damage.
- There is significant attacker research focusing on creating a new breed of super worm.
- Every two-four months, someone unleashes a new worm with an extra evolutionary twist to confound our defenses.
- We need to ready ourselves for this worm evolution
  - Multi-exploit, multi-platform, zero-day, fast-spreading, polymorphic, metamorphic worms

Multi-Exploit Worms

- A worm will use its exploit warhead to exploit a computer.
- Starting out, most worms had only one or two exploits built in – Witty, Sasser, etc
- Nimda had 12 (buffer overflows, browser vulnerabilities, email problems etc)
- New Worms will look to replicate the Nimda model with dozens of ways to penetrate systems.
- If you have patched against N-1 vulnerabilities, the worm will still get in to your system through hole N.

Multi-Platform Worms

- Most Worms to date have only attacked one type of OS per worm
  - Nimda – Windows
  - Ramen – Linux
  - Sasser – Windows
- A very small number have been cross-platform
  - Sadmind/IIS – Windows and Solaris
- In the future, a single worm will attack many different operating systems at once.
- Instead of just patching your Windows machines, you will have to patch all of your systems.

Zero-Day Exploit Worm

- The worms that we have seen to date have used vulnerabilities that we already know about. Patches were already available and we just download them for protection.
- We might not be so lucky in the future. We'll see worms with zero-day exploits which means that they are brand new and have been available for zero days.
- Unfortunately, no patches will be available and researchers will need time to understand how these worms work.
- Widespread prevention will become very difficult or in some cases impossible.

Fast Spreading Worms

- Typically as a worm spreads through a network, it has an exponential rise in the number of victims.
- In August 2001, a white paper described a mathematical model for the development of hyper-efficient worm distribution techniques. It was known as the Flash technique.

Flash Technique

- An attacker pre-scans the Internet for machines which would be vulnerable to the exploit code that will later be loaded into the worm.
  - The attacker will locate thousands or tens of thousands of vulnerable systems.
  - Then using a list of the addresses of these machines, the attacker will pre-program the worm with its first set of victims.
  - The worm is then unleashed on those known victims with high bandwidth closest to the Internet backbone.
  - It will immediately populate the systems already pre-scanned for the vulnerability.

Flash Technique

- The worm infects the first set of victims, then splits up the remaining list of thousands of pre-scanned victims.
- Various segments of the original worm then attack their share of the remaining pre-scanned targets.
- Once these initial targets are compromised, the worm starts to scan and spread to the general population.

Polymorphic Worms

- Polymorphic programs dynamically change their appearance each time they run, by scrambling their code.
- The attackers use different code instructions that perform the same function.
- The code morphs into different mutations so that it no longer matches detection signatures.
- The worm will have a different appearance on each victim, making it more difficult to detect and analyse.

Metamorphic Worms

- In addition to changing their appearance, new worms will also change their behaviour dynamically.
- Worms will contain encrypted/obfuscated payloads.
- After a given event occurs (time duration, infection rate or some other trigger), the worm will morph by decoding the hidden functionality. It will hide it's real purpose.

  (Backdoor, information stealing, DDoS).
- If we catch the original worm we won't be able to determine its true purpose and this makes reverse engineering very difficult.

Worm Defenses – Ethical Worms

- Some have proposed developing "Ethical Worms"
  - We could harness the breeding power of worms to spread software patches rapidly through the world. We could use digital signatures to ensure that the worm is ethical.
- Problems
  - Liability – legal liability for an ethical worm gone wrong
  - Ethical Worms could use up network capacity when it's needed most.
  - Even with a fast ethical worm, you cannot outrun a Warhol/Flash worm.
  - What happens if attackers ever compromised the ethical worm distribution?

Real Worm Defenses - Preparation

- Buffer overflow defences help a lot here. Non-executable system stack prevents 80% of buffer overflow attacks – Windows, Solaris and Linux
- Having a process for rapidly testing and deploying patches when they become available.
- Anti-virus solutions updated daily
- Linking your incident response capabilities with network management in case you need to cut off segments of your network in real time.
- Encrypt data on your hard drives. At least then if it is stolen it can not be read by the attacker.

Worms, Viruses, Trojan Horses