Lecture 7: Viruses and Worms

Summary

We look at viruses and worms in more detail

Viruses in Depth

Reference: P&P, Section 3.3

Virus Lifecycle

Dormant phase

Propagation phase

Triggering phase

Action phase

Virus Types

File viruses

Example: Sality (http://www.f-secure.com/v-descs/virus_w32_sality_aa.shtml)

Macro viruses

Example: Melissa (http://www.f-secure.com/v-descs/melissa.shtml)

Boot sector viruses

Example: Parity Boot (http://www.f-secure.com/v-descs/parboo.shtml)

Virus Signatures

What is a virus signature?

How are they used to defend against viruses?

Example: ClamAV Open Source signatures

Clever virus writers make efforts to evade signature recognition

Encrypted, Polymorphic, and Metamorphic Viruses

Why would a virus writer encrypt the virus code?

What limitations are there on encryption of the code?

What is a *Polymorphic Virus*?

Example: Sality.Q (http://www.f-secure.com/v-descs/sality_q.shtml)

A *Metamorphic Virus* attempt to defeat signature recognition by re-writing its own code.

Garbage code insertion

Register Use Exchange

Code Block Permutation / Jump Insertion

Code Integration

Worms

Much of what we've said about viruses applies to worms as well; the main difference is that worms can spread without user action.

Example: The Morris Worm, 1988 (http://en.wikipedia.org/wiki/Morris_worm)

Exploited three vulnerabilities to gain access to systems (fingerd, SMTP, password); did not require user action to spread

What design flaw turned this "experiment" into a denial-of-service?

Example: Stuxnet, 2010 (http://en.wikipedia.org/wiki/Stuxnet)

A *zero-day vulnerability* is a vulnerability that was previously unknown to the general public. What was special about Stuxnet with regard to zero-days?

Stuxnet targeted a Siemens Programmable Logic Control (PLC). Why is this a concern? Recall the TED video.

How was Stuxnet able to install device drivers that were trusted by Windows?

Was Stuxnet harmful?

Exercises

Read about the Flame worm (*http://en.wikipedia.org/wiki/Flame_(malware)*). What was its purpose? How were the authors able to make Windows trust the worm code? What types of information was Flame able to gather?