CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Building a Malware Analysis Capability

Key Message: Analyzing malware is essential to assess the damage and reduce the impact associated with ongoing infection.

Executive Summary

Malicious code (often referred to as malware) is on the rise in terms of occurrences and sophistication, motivated by financial gain. Malware includes viruses, Trojan horses, worms, rootkits, backdoors, spyware, and adware. It is important to have criteria for prioritizing malware for analysis, focusing on malware that is the most invasive with the largest impact (disclosure of sensitive information including personal credentials). Malware can be analyzed using three techniques: surface analysis, runtime analysis, and static analysis.

In this podcast, Jeff Gennari, a member of CERT's Malicious Code Analysis team, discusses techniques involved in analyzing malicious code and why business leaders should consider building an organizational capability to do this. Jeff also describes CERT's hands-on, lab-oriented Malware Apprenticeship Program Course.

PART 1: THE MALWARE ARMS RACE

Defining Malware

Malware is software that runs without the user's explicit consent, often without the user's knowledge. Malware is typically used to conduct illicit and criminal activities.

Malware includes viruses, Trojan horses, rootkits, backdoors, spyware, and adware. It is typically an executable file or an exploit of some type.

Uses of Malware

Malware can be used to steal identities, take control of computers, and send spam. It harvests information and can steal credentials that are used for personal banking and credit card transactions.

The primary motivation for the development and use of malware is financial gain. There is an entire underground economy that sells malicious code and the services it provides, like a commodity.

An Arms Race

As defenders against malware improve their methods, so do the adversaries. Malware continues to increase in sophistication, to evade detection and removal. The rise of online banking is a major catalyst for this escalation.

Botnets as One Example

A botnet is a collection of computers that are all running the same piece of malware. The person or group who controls the botnet and installs malware on target computers is called a bot herder. Botnets can include tens of thousands of computers.

With centralized commands, botnets can be used to send spam and to launch denial of service attacks. Botnet services are available for purchase.

PART 2: PRIORITIZING MALWARE; ANALYSIS TECHNIQUES

Given the growth and proliferation of malware, most organizations cannot analyze all of the malware that may be resident on their systems. In CERT's Malware Analysis Apprenticeship Course, the following criteria are discussed as a means to prioritize malware for analysis:

- The extent of the infection: higher priority (number of reported incidents, antivirus hits, etc.)
- The way in which the malware spreads: more prolific or automated infection is higher priority
- The impact of the malware: malware that steals sensitive information is higher priority than nuisance malware (window popups). It is worth analyzing higher priority malware to better understand the motive of the attacker, what they are looking for, and the malware's capabilities
- The effort required to remove the malware including reimaging the machine, wiping it clean, deleting specific files, and rebooting

Tagging, Categorizing, and Archiving Malware

When conducting malware analysis, it is important to have a historical understanding of malware that you have seen before.

Categorizing malware into families can greatly expedite the analysis process, allowing analysts to compare new malware to previous malware.

Malware Analysis Techniques

Malware analysis is typically of three types, from most straightforward and least resource-intensive to techniques requiring the most time and skill. Techniques include:

1. Surface analysis: used to characterize the malware. Surface analysis may include capturing an MD5 hash and the malware's file size and file name. Surface analysis helps determine if you have seen this exact file before.

   Surface analysis, while straightforward, does not convey much information about what the file actually does.

2. Runtime analysis: the malware is executed in a controlled environment and its behavior and impact are observed.

   The runtime environment needs to be properly instrumented to gain insights on what the malware does. More sophisticated malware can often detect that it is running in a controlled environment so it may not behave in any interesting way – or it may just terminate or delete itself.

3. Static analysis: also referred to as reverse engineering. The malware code is broken down into its machine instructions (disassembling) and the instructions are analyzed. This is the most effective technique for determining what the malware actually does. This requires more skill and expertise than the other analysis techniques.

All malware that CERT analyzes is subject to surface analysis. Most malware is subject to runtime analysis. Only the highest priority malware is subject to static analysis due to the expense of doing this type of analysis and the skills required.

The criteria described above help inform which type of analysis is performed.

PART 3: WHY INVEST IN A MALWARE ANALYSIS CAPABILITY; FIRST STEPS

Why Perform Malware Analysis?

Some organizations don’t particularly care what malware does, just that it is detected and removed. That said, wiping machines clean and restoring from backups every time malware is detected can be impractical and expensive.

Without some level of analysis, you cannot perform a meaningful damage assessment to estimate and report what data has been lost. And cleaning up one machine may not stop the malware from spreading to others or reinfecting the recently cleaned machine.

Understanding how malware propagates and detecting infections can aid in developing a strategy to prevent new infections based on the infection vector.

Getting Started

The first steps for building a malware analysis capability include:

- building some type of repository infrastructure to store and preserve a historical record of past malware
- conduct surface analysis on newly detected malware

Resources

CERT’s Malware Analysis Apprenticeship Course is offered 3 times per year in the Washington, D.C. area. The course is hands-on and lab-oriented. It covers the 3 stages of analysis and introduces students to specific tools that they use to analyze actual malware.

"One of the 'worst' quarters ever for security" (describes a recent PandaLabs report noting the significant increase in malware), CSO online.com, July 7, 2011.