TJX, Heartland, and CERT’s Forensics Analysis Capabilities

Key Message: Complex, distributed, multi-year investigations of computer crimes require sophisticated methods, techniques, and tools.

Executive Summary

The TJX and Heartland cases took place over many years (approximately 2005 to 2010), from the time that networks were initially breached and millions of credit card numbers were compromised, through forensics investigation involving many agencies and organizations, to prosecution and final sentencing. Cases of this type are becoming more the norm, particularly when conducted on the internet. They present daunting challenges in conducting forensics analysis and investigation involving terabytes of information.

In this podcast, Kevin Moore and Cal Waits, members of CERT’s Forensics Team, discuss CERT’s contribution to helping solve the TJX and Heartland data breach cases, the increasing sophistication and organization of the intruder community, and forensics analysis approaches for complex, distributed investigations including CERT’s Clustered Computing Analysis Platform (C-CAP).

PART 1: TJX AND HEARTLAND; THE ROLE OF CERT’S FORENSICS TEAM

TJX

The TJX breach of credit card information belonging to thousands of card holders is estimated to have started sometime in 2005. Albert Gonzalez and his co-conspirators were able to gain illegal access due to a vulnerability in a retail outlet node of the TJX network. They were able to escalate their privileges, allowing them to access stored-in-real-time credit card information used by the retailer.

They were able to maintain access for a number of years, until at least 2008 and possibly into early 2009.

In March 2010, Gonzalez was sentenced to 20 years in prison (see References).

CERT’s Role: Part 1

CERT’s Forensics Team aided the U.S. Secret service in collecting evidence and creating forensic images of the computers used by the attackers. Given the terabytes of data involved, analyzing it required a collaborative effort.

CERT’s Clustered Computing Analysis Platform (C-CAP) aided in this analysis.

The Forensics Team also lent their expertise in dealing with encrypted data and sophisticated configurations used by the attackers.

Introducing CERT’s C-CAP

As the amount of digital evidence increases, the ability to wade through this amount of information and analyze it in a meaningful way becomes more and more difficult.

As part of the SEI, a federally funded research and development center, CERT can be more objective as it is not subject to the pressures faced by law enforcement.
C-CAP provides an environment where digital evidence can be hosted and stored in a central location. Forensics analysts, often from multiple agencies, are provided with secure access and can access C-CAP from anywhere, at any time.

**Heartland**

The Heartland case was very similar to and overlapped with TJX; it extended from approximately 2007 through 2009. Gonzalez and his co-conspirators again gained access to information associated with millions of credit cards by exploiting a network vulnerability.

**The Exploitation of Common Vulnerabilities**

Many successful attacks result from finding a vulnerability on a single node in a network. Vulnerabilities can result from incomplete or improper patching, lack of security patches, out-of-date or missing anti-virus protection, and open firewall ports.

Attackers use automated scanning tools to identify open ports, operating systems being used, current versions of service packs, and the presence of anti-virus software – and then they record the location of the most vulnerable systems for later use.

Once a vulnerability is exploited, attackers are often able to escalate their privileges to gain greater administrative access to the exploited system and those systems with which it communicates.

**CERT’s Role: Part 2**

CERT fulfills a variety of roles based on the case and the needs of the requesting agency (for example, U.S. Department of Justice or U.S. Department of Homeland Security). CERT may be asked to examine a single computer hard drive or a single file.

CERT is often involved in cases from start to finish, from collecting evidence on systems used by attackers, to analysis and reporting, to testifying in court.

---

**PART 2: PROTECT FINANCIAL INFORMATION; UNDERSTAND ATTACK COMMUNITY AND METHODS**

**Increased Responsibility to Protect Financial Information**

Business leaders of organizations that hold credit card numbers, debit card numbers, and bank account information have an added responsibility to protect this information. The practices for doing so are well known, but often are not practiced, particularly across large, distributed organizations with nationwide or global networks. These practices include the following:

- Develop, implement, and enforce a strong security policy.
- Deploy patches in a timely manner.
- Make sure anti-virus software is up-to-date and regularly executed.
- Deploy practices that reflect defense-in-depth. Such practices can limit the extent and impact of a breach when it occurs so it does not spread across the entire organization.

**Organized Attack Community**

Today’s attacker community is organized, with specialized skills. This includes those who develop the code used to exploit vulnerabilities and those who conduct the exploits.

The predominant motivation in today’s attacks is to make money by harvesting credit card information and other
Personally Identifiable Information (PII). This information is then offered for sale or provided to those who have the means to monetize this information (for example, using it to purchase goods and services).

Attack Methods

Fraud has been with us for a long time. The difference in fraud conducted on the internet is the high degree of automation (and thus, vaster scale and lightening speed) of attacks. Automation is accomplished by scanning thousands of computers to identify vulnerabilities.

The class or type of vulnerability (such as SQL injection) is not particularly important. As the technology changes, the vulnerabilities change. What is important are the security measures an organization puts in place, such as defense-in-depth. It is also important to identify your most critical assets and protect them commensurate with their value, regardless of where they reside.

PART 3: DISTRIBUTED FORENSICS ANALYSIS; PROTECT SENSITIVE DATA DURING INVESTIGATIONS

CERT’S C-CAP; More Details

C-CAP is an environment for forensics analysts. It is used to examine and analyze digital evidence in a manner that supports today’s more complex, distributed investigations.

Many of today’s standard computer forensics labs include examiners with powerful desktop computers and tools for analyzing digital images. These images are collected during the execution of warrants and subpoenas.

Conducting analysis (such as indexing a hard drive or creating a duplicate image) using a single desktop computer is very resource intensive. Executing analysis tools can take a long time; this can create a backlog as analysts wait for the results.

C-CAP provides greater access to a wider pool of examiner resources (tools and more powerful machines) at a reduced cost. C-CAP supports collaboration between examiners that may reside in different geographic locations. C-CAP’s remote access capability includes two-factor authentication and other security measures.

C-CAP provides an environment within which to manage massive amounts of information, data, and evidence that needs to be accessed by multiple examiners throughout the investigation, for different purposes. Having this all in one place is very effective.

Allaying Business Leaders Concerns by Using C-CAP

When a breach occurs, business leaders are often concerned that they will lose control over sensitive business information by involving law enforcement. C-CAP provides control via a central repository; there is only one copy of the organization’s information. Access controls can be deployed based on the level of data sensitivity.

Protecting information during discovery is also a big concern. During the TJX and Heartland cases, sensitive information included

- millions of credit card numbers
- means and access vectors of attack
- command and control data for computers that were used to compromise networks

Access to all of this information needed to be carefully controlled.

During discovery, examiners can create a separate instance of C-CAP (called C-CAP-light), which can then be used to support discovery, and can be used during other aspects of investigation and prosecution. Access and leaks are
controlled much more rigorously than traditional approaches.

Business leaders can request use of and access to C-CAP through their law enforcement agencies.

**A Few More Lessons Learned**

Business leaders should recognize that the same tools that criminals use to identify and exploit weaknesses (such as automated scanning) can be used by organizations to identify and harden those same weaknesses.

As soon as any indicator of a compromise is detected, the organization should move aggressively to begin their investigation. Access to advanced tools and techniques such as C-CAP can be gained by involving law enforcement early on.

In addition, working with law enforcement can help identify the problem more quickly and reduce its spread. Your organization may not be the first to have been attacked and you can benefit from knowledge gained in similar investigations.

**Resources**


Heartland: “[Hacker Sentenced to 20 Years for Breach of Credit Card Processor](#).” Wired, March 26, 2010. Includes links to associated articles.

TJX and Heartland investigation and sentencing: [U.S. Department of Justice](#)

CERT’s Forensics Team [website](#)

CERT’s [Clustered Computing Analysis Platform](#) (C-CAP)

[US-CERT](#) for information on current vulnerabilities and ways to mitigate these

Forensics Companies

[Guidance Software](#)

[Access Data](#)

Copyright 2010 by Carnegie Mellon University