



Forensic Services



Revision History			
Issue	Date	Author	Reviewed by
Version 1.0	3/31/2011	Iftach Ian Amit	Yoram Golandsky

Contents

1. Abstract..... 3

2. Methodology 4

 2.1. Identification and scoping..... 5

 2.2. Preparation and Preservation..... 5

 2.3. Collection and Examination 5

 2.4. Analysis 6

 2.5. Presentation and Evidence Release 6

1. Abstract

Digital forensics is an area that organizations tend to shy away from because of the association with an information security breach whose source and/or real impact cannot always be determined. Often, digital forensics spans multiple realms such as computer systems, mobile devices, networks and databases.

The forensics process is often used to satisfy legal requirements, law enforcement evidence collection and archiving requirements. It is expected to provide the raw data for the analytical process of the attacker, the attacker's toolbox and the actual extent of the breach.

As modern information security incidents are rarely limited in impact to a single information asset or system, organizations are faced with the problem of quickly identifying the actual impact of an incident on the business, intellectual property, partners and customers. Such an analysis can often be performed by employing advanced digital forensic capabilities which identify the full timeline of the incident, as well as the actual information being accessed, the tools used to access it and what information has been leaked/modified/deleted.

Security Art's digital forensic services provide organizations the best of both worlds – evidence collection that adheres to law enforcement standards, as well as expert analysis of the forensic data that provides organizations with business insight that can be used to draw conclusions and act upon them.

2. Methodology

Security Art's forensics services focus on several areas of digital forensics. In each area, different expertise is provided. We provide digital forensic services in the following realms:

- i. Computer forensics
 - a. Cross-drive analysis
 - b. Live analysis
 - c. Deleted files
 - d. Log correlation and analysis
- ii. Mobile device forensics
 - a. Physical acquisition
 - b. Logical acquisition
 - c. Manual acquisition
 - d. External memory
 - e. Internal memory
- iii. Network forensics
 - a. Traffic analysis
 - b. Open source intelligence
- iv. Database forensics
- v. Advanced malware analysis (cross-domain expertise)

A general explanation of our methodology of digital forensics follows.

2.1. Identification and Scoping

Every digital forensic examination begins with identifying the incident based on indicators available prior to any thorough analysis of digital equipment. Security Art takes into account the business impact of such an incident in order to “reverse engineer” the threat model or attack tree used by the attacker. A scope of the forensic examination is then defined by mapping out both the business and technological elements related to the incident.

2.2. Preparation and Preservation

Based on the initial identification of the incident, which would indicate what realms the forensic examination should be conducted upon, the required tools, techniques, equipment and monitoring services are set up. Law enforcement coordination is also initiated at this stage.

Additionally, the related physical and digital evidence are isolated and their state is preserved in order to maintain their validity. This process includes properly storing the devices in tamper evident containers where they cannot be physically or digitally modified.

2.3. Collection and Examination

Data collection and examination begins after the evidence has been identified and isolated. All evidence is duplicated in accordance with forensic evidence handling standards (read-only, no modifications to hardware or digital data) and hashed to ensure the validity of the duplicated evidence.

In order to provide a comprehensive picture of the environment, any logs that correspond to peripheral systems are collected and indexed for further analysis and correlation. Secondary and tertiary impact not initially detected can be identified during this stage.

The collection process is immediately followed by an in-depth examination of the data. This examination focuses on finding the relevant evidence within the acquired data and ensuring that hidden or less trivial information (e.g. swap areas, deleted information, slack space, etc.) is identified, documented and analyzed.

2.4. Analysis

The analysis phase builds the complete picture in terms of the incident based on the collected and examined evidence. At this phase, resources that are not necessarily technical are also involved in order to better understand the examined evidence and build a comprehensive timeline of events and activities. The analysis may uncover additional evidence that would need to be collected and examined in order to complete the incident timeline and determine the impact on the organization.

Most of the malware analysis is performed for incidents that involve targeted attacks in which external information on the malware does not provide enough insight on the impact on the organization. In such cases of custom malware analysis, access to additional systems, protocols and equipment may also be required by Security Art forensic experts in order to draw a full conclusion relating to malware capabilities and impact.

2.5. Presentation and Evidence Release

Security Art provides a comprehensive report that describes the process of forensic examination and analysis and lays out the complete timeline of the incident. The report is usually composed of technical elements along with an executive level summary. The technical section describes the incident in terms of security vulnerabilities and attacks that were used to obtain access to the organization. The executive level report focuses on the impact of the incident, the procedures and policies that were affected by it (or that should be amended due to it) and a recommendation for continued handling of the incident – either internally, with law-enforcement or through public relations channels.