Digital Investigation (2005) 2, 169–170

ELSEVIER

Digital Investigation

www.elsevier.com/locate/diin

EDITORIAL

Investigating security breaches

Growing public concern about the devastating impact of identity theft has been accompanied by increased public attention on security breaches that result in the exposure of sensitive consumer information (Krim, 2005). Intruders gained unauthorized access to 40 million credit card numbers from CardSystems (Sahadi, 2005). Other affected organizations have been concerned with the exposure of medical records and classified information. Despite the severity of this problem, our community is ill-equipped to conduct the associated digital investigations.

Victims of security breaches immediately want answers to two crucial questions: who is responsible and what valuable information, if any, has been lost? Were insiders involved and are they still pilfering? Were customer's credit card numbers stolen? Without answers to these questions, how can victims determine how much damage was done and mitigate the ramifications?

The stakes on the outcome of an investigation of an intrusion can be high, with potentially adverse consequences for the organization's reputation, bottom line, and compliance with mandatory reporting regulations, as well as risks to individual privacy and even public safety and national security interests. Once the breach becomes public, failure to announce the apprehension of the culprits bolsters the conventional wisdom that criminal hackers and cyber-thieves face little risk of being caught, reducing disincentives and consumer confidence (Levy and Stone, 2005).

An unhealthy divide between computer security and digital forensics is making it more difficult not only to apprehend the perpetrators of these massive breaches, but also to determine whether sensitive data were exposed. Forensic best practices are not being developed with industry in mind. For example, many digital investigators are not equipped to remotely analyze live systems, memory contents, or network logs. The approach of shutting down and examining all systems is not suitable for an enterprise environment that depends on computers distributed over a wide geographic area. If the compromised system is an MSSQL databases server, shutting down the system disrupts operations, loses the memory contents, and updates the last accessed dates of all database files to the current time, obliterating some of the most useful sources of information for determining whether the database files were accessed by the intruders.

To complicate matters, many computer security professionals are unfamiliar with forensic principles. Organizations that do not train their IT security staff to preserve digital evidence, and do not design their logging architecture with investigations in mind are raising the risks associated with security breaches by reducing the chance that digital investigators will be able to solve the case. Even some well-known security consulting firms do not have forensic capabilities, which can create significant problems when they compromise their clients' evidence, or worse, cause damage by attempting to perform forensic examinations without the proper tools and training.

Software vendors are attempting to bridge the gap between computer security and digital forensics with programs such as EnCase Enterprise but they are not yet in widespread use. Physical memory dumps are becoming larger and more common, but the tools and techniques for extracting information from this source are limited, particularly for Microsoft Windows systems. To address this shortcoming, the Digital Forensics Research Workshop (DFRWS) has created the Forensic ''Memory Challenge,'' providing memory captures from a computer intrusion that resulted in theft of intellectual

1742-2876/$ - see front matter
doi:10.1016/j.diin.2005.07.006

property (www.dfrws.org). A snapshot of memory can reveal what an intruder was doing on the compromised system, and better tools for interpreting this information may help investigators determine whether data was stolen and who was responsible.

Although some organizations are preparing for critical incidents by developing logging architectures, they are not applying the fundamental forensic principles that will make the logs useful (Rowlingson, 2004; Forte, 2004). Incomplete or inaccurate logging can be harmful rather than helpful. Network logs that are not maintained with evidentiary value in mind create weak sources of evidence, and rather than aiding an investigation, they can divert the attention of digital investigators without holding any relevant information. Such diversions increase the duration and raise the cost of such investigations.

The gap between computer security and digital forensic practices is resulting in loss of the kinds of evidence that could be most useful for apprehending culprits, and puts these two sets of professionals working at cross-purposes. Security professionals understandably want to plug the breach; digital forensic experts want to capture evidence useful in identifying the culprit and prove the illegal activity in court. Inconsistencies in practice are becoming increasingly problematic as more evidence is found in volatile memory and on connected networks. To enhance our ability to investigate information theft, we must expand forensic best practices to include live systems and network logs. We must also teach computer security professionals how to prepare their systems as sources of evidence, and what to do with that digital evidence when an incident occurs. By improving our abilities to appraise the damage caused by security breaches and apprehend the offenders, we can help allay public concern and discourage criminal activities.

References

Forte D. The art of log correlation. HTCIA Worldwide Conference; 2004. Available from: http://www.dflabs.com/images/Art_of_correlation_Dario_Forte.pdf.

Krim J. LexisNexis data breach bigger than estimated: 310,000 consumers may be affected, Firm says. Washington Post April 13, 2005.

Levy S, Stone B. Grand theft identity. Newsweek July 4, 2005.

Rowlingson R. A ten step process for forensic readiness. International Journal of Digital Evidence 2004;2(3). Available from: http://www.ijde.org/docs/04_winter_v2i3_art2.pdf.

Sahadi J. 40M credit cards hacked: breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards. CNN June 20, 2005.

Eoghan Casey
1150 Connecticut Avenue, Suite 200, Washington, DC 20036, United States
E-mail address: eoghan@digital-evidence.net