GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

HOW HARD DOES THE HACK HAVE TO HURT?
AN ANALYSIS OF THE DAMAGE REQUIREMENT OF THE COMPUTER FRAUD AND ABUSE ACT,
18 U.S.C. SECTION 1030

Kristine Z. Green March 2000

In the Computer Fraud and Abuse Act, 18 U.S.C. §1030, Congress made its intentions clear that the amount of damage done to a system can be crucial in establishing a violation of Federal criminal law, particularly for felony violations. However, the methods used to calculate damage are unclear and there has been little judicial precedent to provide guidance to prosecutors and victims of computer-related violations on what factors can be considered in a damage assessment. In the past year, the courts have been working to address this deficiency and provide some direction on the issue. An understanding of the CFAA and recent caselaw can assist both victims and prosecutors in accurately assessing damages and the amount of loss.

THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §1030:

The primary federal anti-hacking statute, the Computer Fraud and Abuse Act (CFAA), criminalizes seven forms of activities.

1) Section (a)(1) prohibits the knowing access of computers of the federal government to obtain classified information without authorization or in excess of authorization;

2) Section (a)(2) prohibits the intentional access of a computer to obtain information from a financial institution, the federal government, or any protected computer involved in interstate or foreign communications (essentially any computer connected to the Internet) without authorization or in excess of authorization;

3) Section (a)(3) prohibits the intentional and unauthorized access of computers of the federal government, or computers used by or for the government when the access affects the government's use of that computer;

4) Section (a)(4) prohibits the knowing access of a protected computer without authorization or in excess of authorization with the intent to defraud;

5) Section (a)(5)(A) prohibits anyone from knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer. Section (a)(5)(B) prohibits the intentional unauthorized access of a computer that recklessly causes damage, and Section (a)(5)(C) covers the intentional unauthorized access of a computer that negligently causes damage;

6) Section (a)(6) prohibits the knowing trafficking of computer passwords with the intent to defraud;

7) Section (a)(7) prohibits the transmission of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

communications containing threats to cause damage to a protected computer.

ANALYSIS:

Regardless of the amount of damage caused by an attack, Sections (a)(1) and (a)(7) are felonies. Similarly, sections (a)(3) and (a)(5)(C) are misdemeanors; the amount of damage is irrelevant. Sections (a)(5)(A) and (a)(5)(B) are felonies, but only if damage is caused as is outlined by 18 U.S.C. §1030(e)(8), which defines damage as the impairment to the integrity or availability of data, a program, a system or information that causes loss aggregating at least $5,000 in value during any one year period to one or more individuals; anything that modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; causes physical injury to any person; or threatens public health or safety.

Section (a)(2) has its own damage provision: a violation under this section may be a felony, but only if the offense was committed (1) for purposes of commercial advantage or private financial gain, or (2) in furtherance of any criminal or tortious act in violation of the Constitution, or laws of the U.S. or of any State, or (3) if the value of the information obtained exceeds $5,000. Otherwise, it is a misdemeanor. Finally, the amount of damage is so important to Section (a)(4) that there is no violation at all unless the value of the thing obtained is more than $5,000 in any one-year period.

Although the five thousand dollar requirement appears clear, uncertainties surrounding what can be included in the calculation of damage may preclude many types of activity from rising to a violation of the CFAA. For example, if only the text of a web page is altered in an attack without actual damage to the system, meeting the five thousand dollar threshold may be difficult. Additionally, it may be difficult to determine a fixed amount in damages if an attacker used a victim's computer only to launch attacks.

Moreover, federal authorities may have to wait for a damage assessment to determine if there is federal jurisdiction. Electronic evidence can easily be destroyed, and such a delay can devastate efforts to trace the attacker. Therefore, a quick and reliable determination of the amount of loss can mean the difference between a successful investigation and a languishing one.

Additionally, reliable data on which estimates are based may be lacking because parties may have incentives to distort the costs. Targets might minimize the loss if they fear that the actual damage might scare customers and have an adverse affect on business, or, they might report inflated losses in an effort to ensure that the hacker is punished. Government entities and law enforcement officials may be prone to inflate the costs in hopes of obtaining more resources. Private

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

security consultants may be tempted to maximize damage reports in order to attract business. Hacker sympathizers interested in curtailing the government's reach may find lower costs believing that most hackers have benign motives and are only seeking a challenging learning experience.

Federal courts are finally beginning to provide guidance on this issue. In U.S. v. Middleton, a case decided in the ninth circuit in 2000, the Court held that damage could be calculated based on salaries paid to, and hours worked by, in-house employees who repaired the damage done by an unauthorized intruder. In this case, Nicholas Middleton was employed as the personal computer administrator for Slip.net, an Internet Service Provider. His responsibilities included installing software and hardware on the company's computers and providing technical support to its employees. He had extensive knowledge of Slip.net's internal systems, including employee and computer program passwords.

Dissatisfied with his job, Middleton quit, but Slip.net allowed Middleton to retain an e-mail account as a paying customer. Middleton used this account to commit his first unauthorized act, which was to use the "Switch User" program to switch his account to that of a slip.net receptionist, Valerie Wilson. Using Wilson's account, Middleton took advantage of the benefits and privileges associated with her account, such as creating and deleting accounts and adding features to existing accounts.

Slip.net's president, Ted Glenwright, discovered this unauthorized action while reviewing the Switch User log, which recorded all attempts to use the Switch User program. Glenwright cross-checked the information with the company's "Radius Log" which recorded an outside user's attempt to dial into the company's modem banks. These logs revealed Middleton's actions.

Glenwright immediately terminated Middleton's e-mail account, but Middleton was able to continue his activities. Three days later, Middleton obtained access to Slip.net's computers by logging in to a computer that contained a test account. He used that test account to gain access to the company's main computers. Once in Slip.net's main system, Middleton accessed the account of a sales representative and created two new accounts, "Terpid" and "Santos." Middleton used the "Terpid" and "Santos" accounts to obtain access to a different computer named "Lemming," which Slip.net used to perform internal administrative functions and to host customer's websites. Lemming also contained the software for a new billing system. After gaining access to Lemming, Middleton changed all the administrative passwords, altered the computer's registry, deleted the entire billing system (including programs that ran the billing software) and deleted two internal databases.

Glenwright discovered the damage the next morning. He

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

immediately contacted the company's system administrator, Bruno Connelly. Glenwright and Connelly spent an entire weekend repairing the damage that Middleton had caused to Slip.net's computers, including restoring access to the computer system, assigning new passwords, reloading the billing software, and recreating the deleted databases. They spent many hours investigating the source and the extent of the damage. Glenwright estimated that he spent 93 hours repairing the damage; Connelly estimated that he spent 28 hours and other employees estimated that they spent a total of 33 hours. Additionally, Slip.net bought new software to replace software that Middleton deleted, and the company hired an outside consultant for technical support.

The amount of damage that occurred was computed by multiplying the number of hours that each employee spent in fixing the computer problems by their respective hourly rates (calculated using their annual salaries), then adding the cost of the consultant and the new software. The total amount of damage was estimated to be $10,092. Glenwright estimated that his time alone was worth $90 per hour, based on his salary of $180,000 per year. He testified that he did not hire an outside contractor to repair the damage because he believed that he, as a computer expert with a pre-existing knowledge of the customized features of his company's computers, could fix the problems more efficiently.

Middleton was arrested and charged with a violation of 18 U.S.C. §1030 (a)(5)(A). The Court decided that damages were properly defined as any impairment to Slip.net's computer system that caused a loss of at least $5,000. The Court determined that "Loss" was properly defined as any monetary loss that Slip.net sustained as a result of any damage to Slip.net's computer data, program, system or information. Additionally, it was proper to consider any loss that was a natural and foreseeable result of any damage and any measures that were reasonably necessary to restore or resecure the data, program, system, or information that was damaged.

Furthermore, another recent Court case decided in the ninth circuit established that the data does not have to be physically changed or erased for its integrity to be damaged. In Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., the Court stated that impairment can include the alleged access and disclosure of trade secrets when the data was copied rather than modified. Shurgard Storage Centers, the plaintiff in this case, was the industry leader in full and self-service storage facilities in both the United States and Europe. Shurgard's growth was primarily due to the development and construction of top-quality storage centers in "high barrier to entry" markets.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Pursuant to this strategy, Shurgard developed a sophisticated system of creating market plans, identifying appropriate development sites, and evaluating whether a site would provide a high return on an investment.

Shurgard's competing company, Safeguard Self Storage, Inc., was a newer company that developed self-storage facilities in the United States and abroad. Shurgard alleged that Safegard engaged in a systematic scheme to hire away key employees from Shurgard for the purpose of obtaining the plaintiff's trade secrets. Additionally, a Shurgard employee, while still working for Shurgard and prior to his employment with Safegard, used Shurgard's computers to send trade secrets to Safegard via e-mail.

The Court stated that the damage and thus violation to the "integrity" was caused by the alleged infiltration of Shurgard's computer network and the collection and dissemination of confidential information. The Court found that an impairment of the data's integrity occurred even though no data was physically changed or erased. The Court stated that although there may be no damage to data in such a situation, there is still a "loss."

CONCLUSION

Damage under 18 U.S.C. §1030 (e)(8) is any impairment to a victim's computer system that caused a loss of at least $5,000. "Loss" can include any monetary loss that the victim sustained as a result of any damage to computer data, a program, a system or information. Additionally, loss includes the costs that were a natural and foreseeable result of any damage, and any measures that were reasonably necessary to restore or resecure the data, the program, the system, or information. An impairment of the data's integrity may occur even though no data was physically changed or erased if the victim suffered a "loss." Therefore, a victim of a computer compromise would be advised to calculate the amount of damage based on these and similar factors. Should the victim decide to involve federal law enforcement, a timely estimate of the amount of loss may assist in swiftly tracing the attacker.

SOURCES

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121 (9th Cir. 2000); website http://www.privacysecuritynetwork.com/Library/docs/Shurguard.htm

U.S. v. Middleton, 231 F.3d 1207 (9th Cir. 2000); website http://caselaw.lp.findlaw.com/scripts/getcase.pl?Court=9th&navby=case&no=9910518;

Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Geo.L.J. 171, (2000).

Eric J. Sinrod and William P. Reilly, *Cyber-crimes: A Practical Approach to the Applications of Federal Computer Crime Laws*, 16 Santa Clara Computer & High Tech. L.J. 177 (2000).

Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?*, 6 RICH. J.L. & TECH. 23 (Spring 2000); website <http://www.richmond.edu/jolt/v6i5/article2.html>.

© SANS Institute 2000 - 2002, Author retains full rights.