Network Attacks: Analysis of Department of Justice Prosecutions 1999 - 2006

August 28, 2006

A study by Trusted Strategies, L.L.C. commissioned by Phoenix Technologies, Ltd.

Copyright © 2006 Trusted Strategies, L.L.C. All rights reserved.

Most Damaging Network Attacks Preventable

Until now, data used in most reports regarding computer security crimes was obtained by surveying organizations, many of which refused to share cost figures about their losses. For this report, data about financial losses of computer crimes is improved because the data has been disclosed through and verified by the U.S. legal system.

This study examined all cases of cybercrime related to network intrusion and data theft prosecuted and publicly disclosed by the Department of Justice Computer Crime and Intellectual Property Section that occurred between March 1999 and February 2006. The information collected and analyzed portrays a clearer picture of the attacks and real damages of computer security crimes than has previously been available.

Research Methodology

The cases analyzed involved everything from spreading malicious code such as viruses, Trojans, spyware and worms; to theft of valuable data like intellectual property, credit card or other private financial information; and a host of other crimes such as denial of services, unauthorized access and financial theft. Prior to the analysis of the data, each crime was examined and classified as to:

- type of attack;
- methods used to carry it out;
- attacker's relationship, if any, to penetrated organization;
- location of attacker at time of attack;
- type, location and nature of equipment used in attack.

Key Findings:

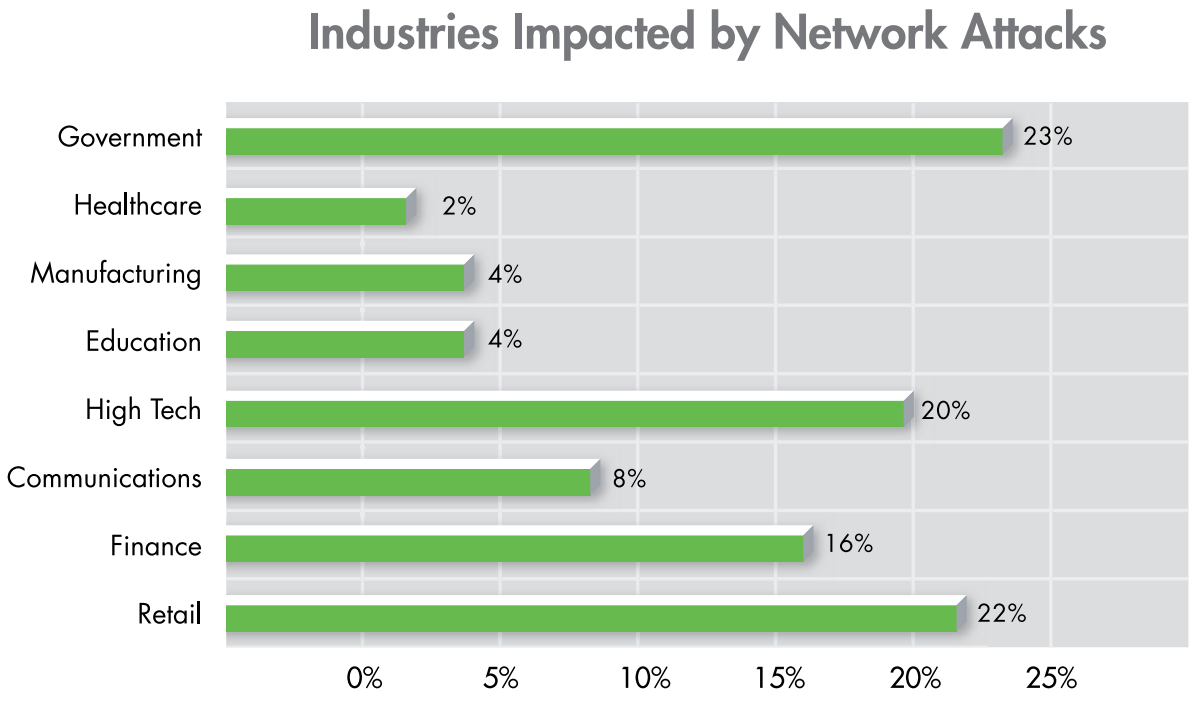
- Average financial loss was more than $3M per case
- Individual attacks caused as much as $10M in damages to individual organizations
- Organizations suffered the greatest financial loss and damage, more than $1.5M per occurrence, when attackers used stolen IDs and passwords
- Largest damages to organizations caused by attackers logging onto privileged user or administrator accounts where a small number of authorized computers were sanctioned to perform work
- Most crimes, 84 percent, could have been prevented if the identity of the computers connecting were checked in addition to user IDs and passwords
- Losses from stolen IDs and passwords far exceeded damages from worms, viruses, and other attack methods not utilizing logon accounts
- Vast majority of attackers, 78 percent, committed crimes from their home computers; most often using unsanctioned computers with no relationship to the penetrated organization

Greatest losses from unauthorized user logon

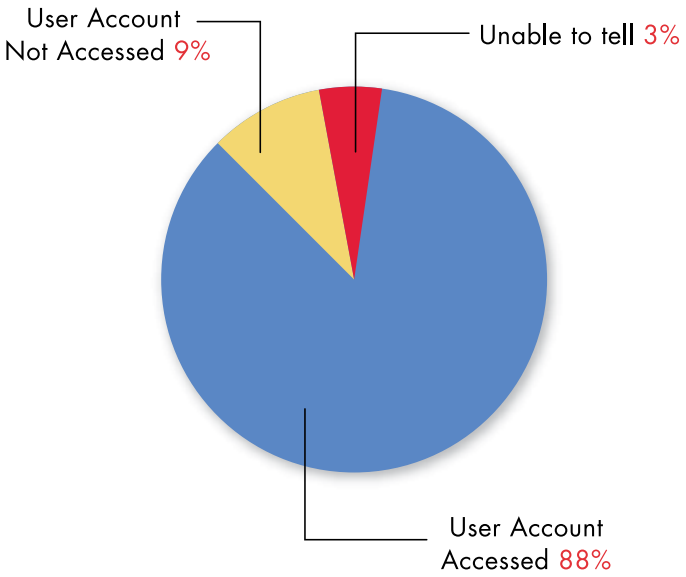
Unauthorized access of privileged logon accounts caused by far the greatest financial losses to individual companies of all crimes analyzed. These were not sophisticated hacks; they were relatively simple crimes committed by attackers obtaining valid user IDs and passwords and using that information to logon to protected resources. Damages from these attacks were significant, ranging from thousands to tens of millions of dollars. The average costs to individual organizations when privileged accounts were penetrated was more than $1.5M.

In one case the attacker was convicted of using stolen IDs and passwords to logon to his victim's administrative accounts and deleting all of the company's sophisticated manufacturing software programs. His acts caused $10M in damages at that company alone.

Damages to individual organizations from unauthorized access far exceeded those damages done by viruses or other malware, which is in contrast to conventional belief. Although viruses and worms did cause the largest amount of total damage, on an aggregated basis, damage was spread across many organizations and countries. The average cost to an individual company from any single virus attack analyzed in this study was surprisingly low, at $2.4K.



Percentage of Logon to Privileged Accounts



Cybercriminals who accessed privileged accounts obtained IDs and passwords through many means, including network sniffing, use of password cracking programs and collusion with insiders. It was also common for employees to share their IDs and passwords with coworkers who later left the organization and used that knowledge to gain access.

In the majority of the cases, the attacker logged onto one or more privileged user accounts, indicating that the intruder had familiarity with the network.

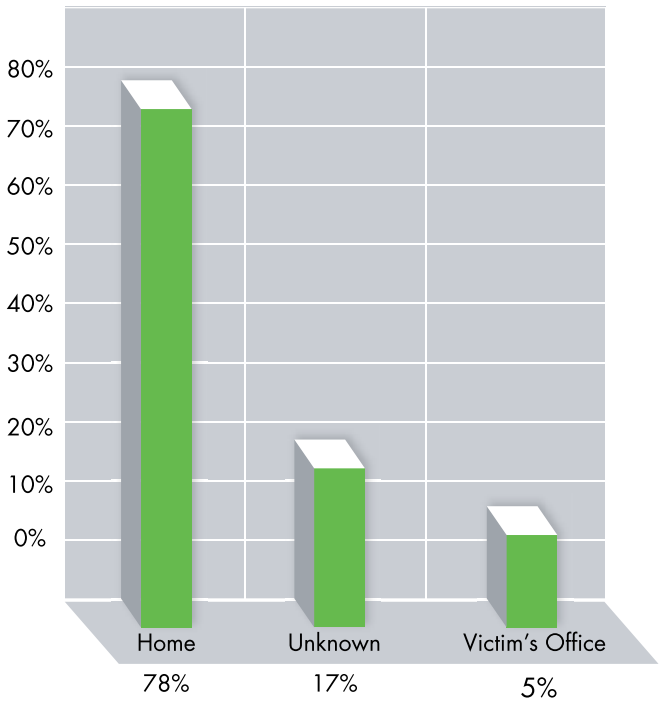
Device authentication would prevent most crimes

Penetrated systems checked the authenticity of the logon user ID and password, but there was virtually no effort to validate that the computer connecting was an authorized device. This was true even though the vast majority of cases involved logons to privileged and administrative accounts that should have been coming from a relatively small number of sanctioned computers.

Unsanctioned computers were used to commit 84 percent of the crimes. Of those, 78 percent used their personal computers to carry out the crimes from their homes, 5 percent were launched from within the victim's own facilities, and in 17 percent of the cases the attacker's location was not specified.

These crimes could have been prevented if penetrated systems had checked the computer's identification as well as the individual's identification during logon.

Location of Attacker



In 16 percent of the cases, device identification would not have stopped the crimes because either the attackers were authorized users at sanctioned computers who were abusing their power, or the attacks resulted from denial of service, viruses, worms or other methods that did not require logging in.

According to research analysis firm IDC, the combined spending for virus control, firewall protection and other security software, including threat management software, security management software, vulnerability assessment software and intrusion detection software, is predicted to be approximately $6.6B in 2007. Yet, worldwide identity and access management software spending is expected to be less than half that, in the range of $3.2B next year. Since device identification and authentication technologies, which are part of identity and access management software, could have prevented 84 percent of the crimes studied in this report, it is surprising that spending for this type of software is predicted to be less than half the amount spent on virus control, firewall protection and other security software.

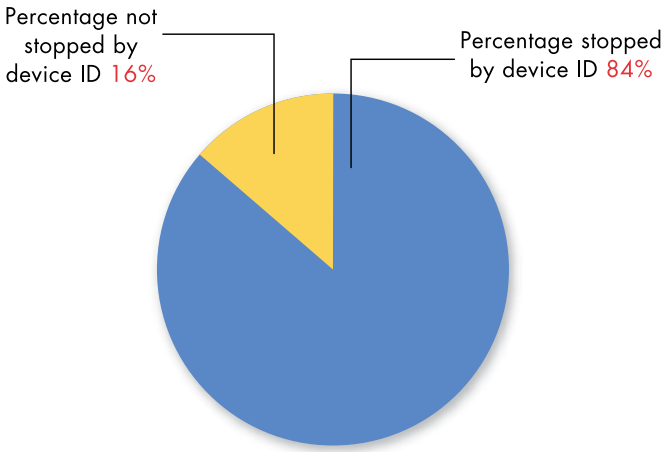
Outsiders committed most of the crimes

While outsiders accounted for 79 percent of the crimes where logon accounts were penetrated, insider crimes demonstrated similar patterns. Most unauthorized logon crimes that could be considered an inside job were perpetrated by former employees or contractors using former coworker's IDs and passwords to gain access. Former employees committed 21 percent of crimes where a logon occurred. In 93 percent of those cases, they used IDs and passwords that were stolen without the victim's knowledge. In 7 percent of the cases involving former employees, insiders intentionally provided IDs and passwords to outside accomplices who performed the attack, usually from their own personal computer.

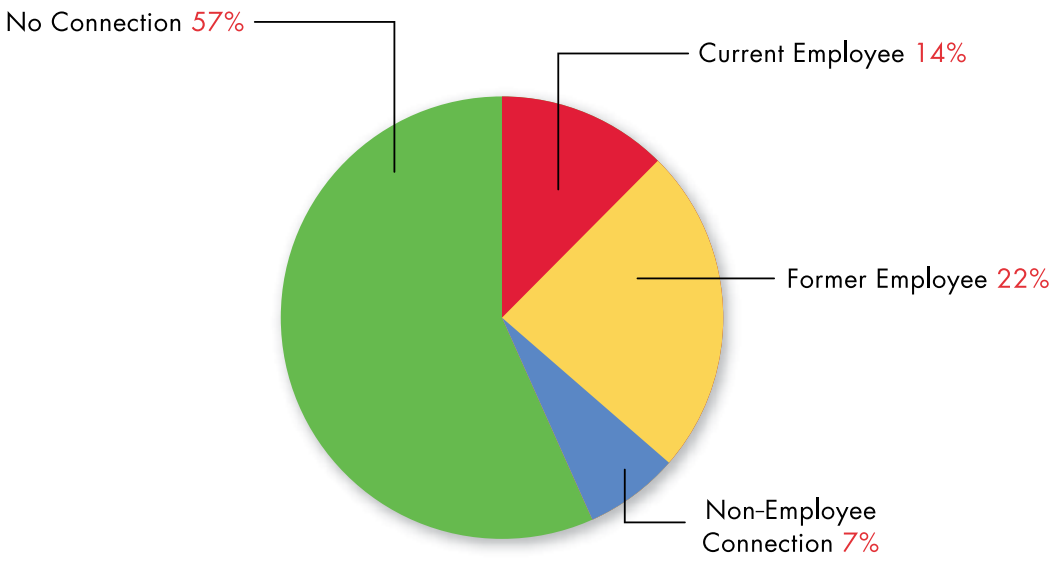
For example, Laurent Chavet of Kirkland, Washington was convicted of using the user ID and password of an unknowing former coworker to gain unauthorized access to his former employer's system from his home in San Mateo, California. Chavet's actions destroyed company systems and caused critical data loss.

In another scenario, an employee of one financial institution provided sensitive customer information to a friend outside the organization. The data included user names and passwords that were later used by yet another person to gain access to the system and steal credit card data.

Crimes Device ID Could Have Prevented



Attacker's Relationship to Victim



Consistent with the findings on crimes committed by outsiders, these insider crimes would have been prevented if the penetrated systems had checked the device identification of the connecting computer as well as the individual's ID and password. This is true even if more robust security procedures had been in place, such as a one-time password system. In some of the crimes studied, insiders supplied accomplises a current one-time password by phone, email or instant message.

In about 5 percent of the cases, attackers penetrating privileged accounts used computers owned by the organization. These attackers were all authorized individuals, usually employees and in some cases contractors, who exceeded the authorized use of their IDs and passwords or used stolen IDs and passwords from coworkers.

For example, in one case an employee at a large debt collection company was advised of adverse employment issues and placed on a specific performance improvement plan. While on the plan, the employee used his account privileges to login to the organization's systems and plant malicious computer code on the network. His actions caused the deletion and modification of financial records that impacted more than 50,000 accounts, disrupted the proper functioning of the computer network and caused the company more than $100,000 in losses.

When all attacks are analyzed: 57 percent of attackers had no relationship to the victim organization, 22 percent were former employees, 14 percent were current employees, and 7 percent were not employees, but did have a connection to the victim organization, such as a customer or supplier.

Summary Conclusions

This study identifies a number of points that should be of critical importance to all organizations.

First, organizations faced much greater risks per attack from unauthorized access to internal networks and resources, about $1.5M on average, than they faced from individual worms and viruses, about $2.4K on average.

Second, it is not always sophisticated hackers conducting devastating network attacks. The vast majority, 88 percent, of those crimes were committed from a home PC using stolen IDs and passwords and following normal logon procedures.

Finally, network attacks could have been prevented in 84 percent of all cases if the organization had implemented device identification and authentication in addition to user ID and password protections. In other words, only requiring user IDs and passwords for network access to high-value information assets should no longer be considered adequate network security.

Trusted Strategies

Copyright © 2006 Trusted Strategies, L.L.C. All rights reserved. This document is furnished to you for your internal use only, and may not be copied or distributed outside the company receiving this document without the prior written permission of Trusted Strategies.

THIS DOCUMENT IS PROVIDED "AS IS" FOR INFORMATIONAL PURPOSES ONLY. TRUSTED STRATEGIES MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT, AND EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

Trusted Strategies™ is a registered trademark of Trusted Strategies protected by the laws of the United States or other countries. This document may contain some references to trademarks owned by entities other than Trusted Strategies, and such trademarks are the property of their respective owners.

For additional information, please contact:

Trusted Strategies, L.L.C.
239 Main Street Suite E
Pleasanton, CA 94566
(925) 229-9919
www.trustedstrategies.com

Or email the author, Bill Bosen, at:
Bill_Bosen@trustedstrategies.com