



Confidence in a connected world.

Symantec Internet Security Threat Report

September 2007

Financial Services Industry Data Sheet

An important note about these statistics

The statistics discussed in this document are based on attacks against an extensive sample of Symantec customers. The attack activity was detected by the Symantec™ Global Intelligence Network, which includes Symantec™ Managed Security Services and Symantec DeepSight™ Threat Management System, between January 1 and June 30, 2007.

Symantec Managed Security Services and Symantec DeepSight Threat Management System use automated systems to map the IP address of the attacking system to identify the country in which it is located. However, because attackers frequently use compromised systems situated around the world to launch attacks remotely, the location of the attacking system may differ from the location of the attacker. Despite the uncertainty that this creates, this type of data is useful in creating a high-level profile of global attack patterns.

The number of contributing sensors in each industry varies. Combined with different standard security practices, these variations may result in different attack data being recorded in each industry. This may preclude valid comparisons between industries.

Executive Summary

In addition to gathering Internet-wide attack data for the *Internet Security Threat Report*, Symantec also gathers and analyzes attack data that is detected by sensors deployed in specific industries. This industry data sheet will discuss the top attacks, top targeted ports, and top source countries for attack activity targeting organizations in the financial services industry. It will also discuss developments in phishing activity across the Internet, specifically those targeting financial service organizations between January 1 and June 30, 2007.

During this period, the financial services sector was the second most targeted sector, accounting for five percent of all targeted attacks. The financial services sector is often targeted by profit-driven attackers looking to gain access to personal information or financial information such as bank or credit card details. Attackers may also target organizations in the financial services sector in order to disrupt their ability to conduct business.

The most widespread attack carried out against the financial services sector was the Non-SMTP Session Start. Detection of this attack is likely the result of attackers attempting to manipulate email protocols, which may be driven by spammers who are attempting to locate computers that can be used to deliver unsolicited email. Attacks against email services in the financial sector may also be carried out to facilitate email-based phishing attacks.

Financial Services Industry Data Sheet

The most targeted port in the financial services sector in the first half of 2007 was TCP port 25, which provides SMTP email service. High amounts of activity against this port are often the result of automated attack reconnaissance. TCP port 25 is also often scanned for by spammers who are attempting to locate computers that can be used to deliver unsolicited email. These unprotected systems are often called open relays, as they allow anyone to relay mail. Attackers may also target email services to aid in email-based phishing attacks.

China ranked highest for attacks detected by sensors in the financial services industry, accounting for 26 percent of the total. This is significantly higher than the 13 percent of Internet-wide attacks that originated in China during this period, indicating that attacks originating in China are targeting financial service organizations in particular.

Organizations in the financial services sector accounted for 79 percent of the brands that were used for phishing during the first six months of 2007. This is down somewhat from the last six months of 2006, when they accounted for 84 percent. The financial services sector also accounted for 72 percent of all phishing Web sites reported to Symantec, more than any other sector during this period. Financial services made up 64 percent of all phishing Web sites in the last half of 2006.

Financial services as a target

Between January 1 and June 30, 2007, financial services was the sector targeted by the second highest number of targeted attacks, receiving five percent of all targeted attacks. Home users were the top-ranked sector and the health care sector ranked third. Symantec has observed that attack activity is often motivated by the desire for financial gain. With this in mind, it is natural that attackers would target organizations in the financial services sector.

The financial services sector is often targeted by profit-driven attackers looking to gain access to personal information or financial information such as bank or credit card details. Attackers may also target organizations in the financial services sector in order to disrupt their ability to conduct business.

Top Attacks

Sector Rank	Attack	Percentage of Attacks in Sector
1	Non-SMTP Session Start	40%
2	Generic Extra SYN in TCP Connection Event	21%
3	ICMP Error Msg About Unseen Packet	10%
4	Generic SMTP Invalid Domain Name Attack	7%
5	Generic TCP Segment With Invalid Checksum Event	5%
6	Generic UDP Flood DoS Attack	3%
7	Microsoft SQL-Server Buffer Overflow Attack	2%
8	Generic TCP RST-ACK Flood Denial of Service Attack	2%
9	Windows SMTP Overflow	1%
10	Malformed HTTPS TLS Packet Detected	1%

Table 1. Top attacks targeting the financial services sector

Source: Symantec Corporation

Financial Services Industry Data Sheet

For the purposes of this data sheet, top attacks were determined by the percentage of total attackers detected performing each attack. The most widespread attack carried out against the financial services sector in the first six months of 2007 was the Non-SMTP Session Start, which accounted for 40 percent of all attacking IP addresses. SMTP, or simple mail transfer protocol, is the protocol that is used to transfer messages between email servers. Detection of this attack is likely the result of attackers attempting to manipulate email protocols, which may be driven by spammers who are attempting to locate computers that can be used to deliver unsolicited email.

Attackers may also target SMTP services in the financial sector to help carry out phishing attacks. As is discussed in the “Phishing Activity by Sector” section below, financial services was the sector involved in the most phishing attacks during this period. In many cases, phishing attacks are carried out using email. An attacker will send an email to an intended target person or group that asks for sensitive information such as online banking credentials. Phishing emails may also contain links to malicious Web pages that masquerade as legitimate financial institution Web pages. If a target user follows the link, he or she may be fooled into entering authentication credentials or other sensitive information into a form on the malicious Web page.

If an attacker can compromise an email server in a financial organization, he or she may be able to use it to send phishing emails from the financial organization’s email accounts. Email phishing attempts that target customers of the compromised organization have a good chance of success because they would originate from legitimate email addresses.

Most phishing activity is conducted for financial gain. A successful phishing attack that mimics the brand of a financial entity is most likely to yield data that can be used for immediate financial gain. It is therefore logical that phishing attacks focus on brands within the financial services sector.

During the first six months of 2007, the second most widespread attack detected by sensors deployed by the financial services sector was the Generic Extra SYN in TCP Connection Event, which was used by 21 percent of attacking IP addresses.

TCP/IP is the protocol that is responsible for routing data between two endpoints. The popularity of this attack indicates that attackers may be attempting to manipulate the TCP/IP connection that underlies most of the other Internet protocols. An attacker who is able to manipulate a TCP/IP connection might be able to create denial of service (DoS) conditions and read or manipulate the data sent over that connection. This may allow an attacker to gain access to or change potentially sensitive information being communicated over the Internet, such as credit card numbers, personal information, or user authentication credentials.

In order to protect against this attack, organizations should ensure that appropriate patch levels are maintained for all systems, including firewalls and routers. Organizations should deploy intrusion detection systems with signatures that can detect TCP/IP and other protocol anomalies, and any alerts should be investigated.

The third most widespread attack targeting this sector during the period was the ICMP Error Msg About Unseen Packet. This attack indicates a response to an Internet control message (a ping, for example) that was never sent. This may be a result of backscatter from a DoS attack that is using spoofed IP addresses against a server connected to the Internet. Attackers often spoof IPs when performing DoS attacks, and when an error occurs, the error message is returned to the spoofed IP, not the IP from which it was originally sent. If the IP of a sensor is spoofed, the sensor will detect an error for a packet it never sent.

Financial Services Industry Data Sheet

A DoS attack can render Web sites or other network services inaccessible to customers and employees. This could result in the disruption of organizational communications, a significant loss of revenue, and/or damage to the organization's reputation.

Organizations should ensure that a documented procedure exists for responding to DoS attacks. One of the best ways to mitigate the effects of a DoS attack is to filter upstream of the target. For most organizations, this filtering would involve contacting their Internet service provider. Symantec also recommends that organizations perform egress filtering on all outbound traffic.¹ Many firewall and operating systems have configuration parameters that can be changed to help mitigate the effect of a net flood attack. Organizations should ensure that all potential DoS targets are appropriately configured to minimize impact should an attack occur.

Top Targeted Ports

Sector Rank	Port	Percentage	Service
1	TCP 25	6%	Email (SMTP)
2	TCP 80	3%	Web (HTTP)
3	TCP 21	3%	FTP
4	UDP 1434	2%	Microsoft SQL Server
5	UDP 53	2%	DNS
6	TCP 443	2%	Secure Web (HTTPS)
7	UDP 8116	2%	Checkpoint clustering
8	UDP 161	2%	SNMP
9	UDP 137	2%	NetBIOS name service
10	TCP 1433	2%	Microsoft SQL Server

Table 2. Top attacked ports, financial services sector

Source: Symantec Corporation

Monitoring ports that are being attacked can give administrators an understanding of which services are being targeted and, thus, which may be most vulnerable to attack.² The top targeted ports are determined by the number of unique incidents of attacks launched against each port.

The most frequently targeted port in the financial services sector in the first half of 2007 was TCP port 25, which provides SMTP email service. High amounts of activity against this port are often the result of automated attack reconnaissance. TCP port 25 is also often scanned for by spammers who are attempting to locate computers that can be used to deliver unsolicited email. These unprotected systems are often called open relays, as they allow anyone to relay mail.

Successful compromise of this port may result in spammers using it to relay spam, which will result in unauthorized consumption of network bandwidth. This in turn may result in system slowdowns or, in worst-case scenarios, DoS conditions. Organizations whose systems are identified as being used to send spam risk being placed on a DNS block lists, which could subsequently result in email from the organization's end users being blocked.

¹ Egress traffic refers to traffic that is leaving a network, bound for the Internet or another network.

² Although specific ports are typically identified with specific services, it should be noted that it is possible to configure most services to run over any port. As services can be identified with common ports, however, analysis of large scale port activity such as this typically coincides with its commonly associated service.

Financial Services Industry Data Sheet

As discussed previously in the “Top Attacks” section, attacks targeting email services may also be carried out to facilitate phishing attacks. An attacker will send an email to an intended target that asks for sensitive information, such as online banking credentials. Phishing emails may also contain links to malicious Web pages that masquerade as the legitimate Web page of a financial institution. If a targeted user follows the link, he or she may be fooled into entering authentication credentials or other sensitive information into a form on the malicious Web page.

Attackers who compromise an email server in a financial organization may be able to use it to send phishing emails from the financial organization’s email accounts. These phishing attempts would have a good chance of success because they would originate from legitimate email addresses.

The second most frequently port targeted in attacks detected by sensors deployed in the financial services sector in the first half of 2007 was TCP port 80. This port provides access to Web sites, Web applications, and Web services. It is widely scanned for by attackers looking for Web applications that may be vulnerable or old, unpatched Web servers.

The prominence of this port illustrates a trend outlined in previous volumes of the Symantec *Internet Security Threat Report*.³ Attackers are moving away from targeting network-based operating system services due to patching and the wide implementation of perimeter security defenses such as firewalls. TCP port 80 has thus become a more common target because it is often not blocked by firewalls. Furthermore, attackers interested in fraud may also target this port in order to carry out phishing attacks using cross-site scripting.⁴

Organizations should audit all external connections to ensure that only known and valid servers are accessible. They should also audit all systems to ensure that patch levels and configurations are secure.

The third most frequently targeted port between January 1 and June 30, 2007 was TCP port 21, which provides FTP file-sharing service. Attack traffic on this port often indicates the use of brute-force attacks targeting weak passwords. Attackers targeting FTP are likely looking for potentially sensitive information that is stored there. They may also be looking for a convenient place to store pirated software for distribution.

A successful compromise of an FTP server could allow an attacker to gain access to sensitive information, or to use the compromised server to distribute pirated software or other malicious executables. Organizations should implement a password policy that ensures that strong passwords are being used to protect user accounts from brute-force attacks. Organizations should also ensure that their FTP software security patches are up-to-date.

³ Symantec *Internet Security Threat Report*, Volume IX (March 2006): http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf : p. 29

⁴ A successful cross-site scripting attack would allow an attacker to place arbitrary text, HTML, or script code onto a vulnerable Web page, potentially allowing phishers to carry out more successful attacks.

Top countries of attack origin

Sector Rank	Country	Percentage of Attacks in Sector	Percentage of Worldwide Attacks
1	China	26%	13%
2	United States	20%	25%
3	Germany	7%	8%
4	Spain	6%	5%
5	France	4%	6%
6	Italy	3%	3%
7	United Kingdom	3%	5%
8	Poland	3%	2%
9	Taiwan	2%	2%
10	Canada	2%	4%

Table 3. Top countries of origin for attacks targeting financial services sector
 Source: Symantec Corporation

In the first half of 2007, China was the country of origin of the highest number of attacks detected by sensors in the financial services industry, accounting for 26 percent of the total. This is significantly higher than the 13 percent of Internet-wide attacks that originated in China during this period. This indicates that attacks originating in China are targeting financial service organizations in particular.

Over the past two reporting periods, Symantec has observed that the number of bot-infected computers in China has risen. During the first half of 2007, China hosted about 29 percent of the world's bot-infected computers, up from 26 percent during the previous six months. However, this does not mean the attackers were situated in China. Bot network owners use command-and-control servers to control their networks. During the current reporting period, only about three percent of bot command-and-control servers were located in China. Because China has a significantly lower percentage of command-and-control servers than bot-infected computers, it is likely that bot-infected computers in China—and the attack activity originating from them—are being controlled by attackers in other countries. Attackers likely proxy their attacks in this manner because of the potential consequences of getting caught. It is common for an attack to be relayed through compromised computers before attacking a high-profile target in order to obscure the attacker's location and avoid prosecution.

During the first six months of 2007, the United States was the country of origin of the second most attacks detected by sensors in the financial sector (table 3). Twenty percent of the attacks targeting this industry originated there. The proportion of attacks against the financial sector originating in the United States is significantly lower than the percentage of worldwide attacks originating in the United States. This indicates that attacks originating in the United States are not targeting financial service organizations in particular. If they are doing so, they are likely using bots situated in other countries.

Financial Services Industry Data Sheet

Germany was the third highest country of origin for attacks targeting the financial sector, with seven percent. The proportion of attacks originating in Germany wasn't significantly different from those noted for attacks against the Internet as a whole, which was eight percent. This would indicate that attacks originating in Germany were not specifically targeting organizations in the financial services sector.

Phishing

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, usually for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to commit fraudulent acts. This section of the *Financial Services Industry Data Sheet* looks at phishing attacks that have been conducted across the Internet and, where possible, specifically against financial service organizations between January 1 and June 30, 2007.

Phishing is assessed according to two indicators: phishing messages and phishing attempts. A phishing message is a single, unique message that is sent to targets with the intent of gaining confidential and/or personal information from computer users. Each phishing message has different content and each one will represent a different way of trying to fool a user into disclosing information. A phishing message can be considered the "lure" with which a phisher attempts to entice a phishing target to disclose confidential information. A single message, or lure, can be used many times in different phishing attacks.

A phishing attempt, on the other hand, can be defined as an instance of a phishing message being sent to a single user. A single phishing message can be used in numerous distinct phishing attempts, usually targeting different end users. Extending the fishing analogy, a phishing attempt can be considered a single cast of the lure (the phishing message) to try to ensnare a target.

The volume of phishing messages is determined by tracking the number of unique messages that appear in each batch of messages that the Symantec Probe Network classifies as a phishing attempt. Over the first six months of 2007, the Symantec Probe Network detected 196,860 unique phishing messages across all industry sectors. This is an 18 percent increase over the 166,248 unique phishing messages that were detected in the last half of 2006. This is a greater increase than in the previous six-month period, during which the number of unique phishing messages increased by six percent.

The continued increase is likely influenced in part by the strategy of varying the content in phishing messages to bypass filtering techniques. These messages may attempt to phish the same brands, but include slight variations in the message to evade detection by common antiphishing methods. Furthermore, more widespread adoption of this technique may indicate a rise in targeted attacks on particular groups, in which phishing messages are modified to be more suitable and convincing for the targeted group.

Phishing Activity Targeting the Financial Service Sector

Of the 198,860 unique phishing messages detected during this reporting period, 107,451, or 54 percent, targeted the financial services sector (figure 1). This shows that attackers were not only focused on this sector, but possibly attempted to target a wider variety of brands within the industry.

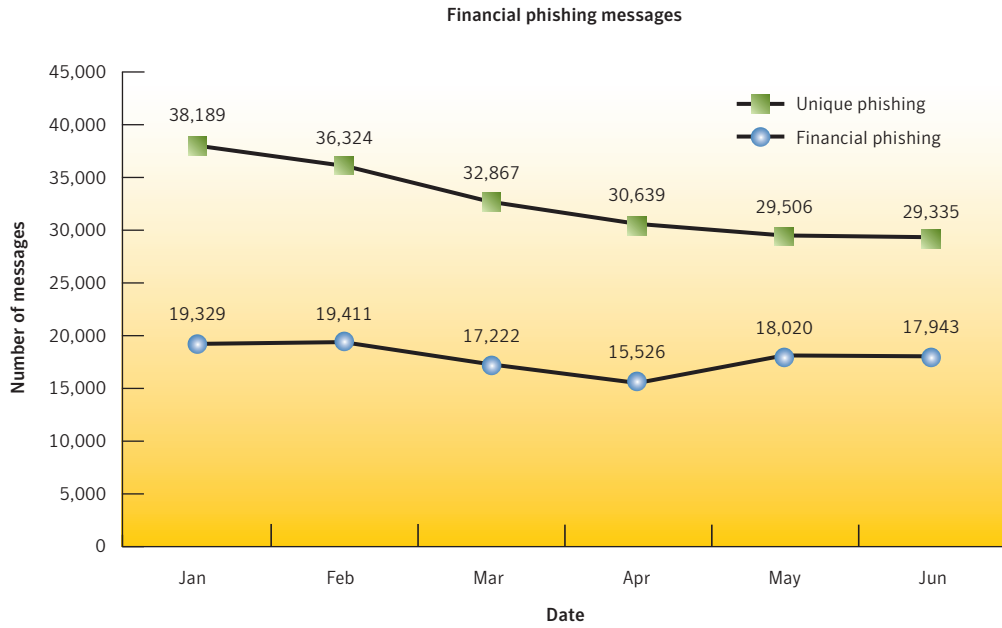


Figure 1. Unique phishing messages per month
 Source: Symantec Corporation

This metric will assess phishing activity that targeted organizations in the financial services sector. This means that the organization’s brand was used in phishing attacks. This is important for enterprises because the use of an organization’s brand in phishing activity can have significant negative consequences. It can undermine consumer confidence and damage the organization’s reputation. Furthermore, the company may be required to compensate victims of any phishing scams that use the company’s brand.

Organizations in the financial services sector accounted for 79 percent of the brands that were used for phishing during the first six months of 2007 (figure 2). This is down somewhat from the last six months of 2006, when they accounted for 84 percent. The financial services sector also accounted for 72 percent of all phishing Web sites reported to Symantec, more than any other sector during this period. Financial services made up 64 percent of all phishing Web sites in the last half of 2006.

Most phishing activity is conducted for financial gain. A successful phishing attack that mimics the brand of a financial entity is most likely to yield data that can be used for immediate financial gain. It is therefore logical that phishing attacks focus on brands within the financial services sector.

Financial Services Industry Data Sheet

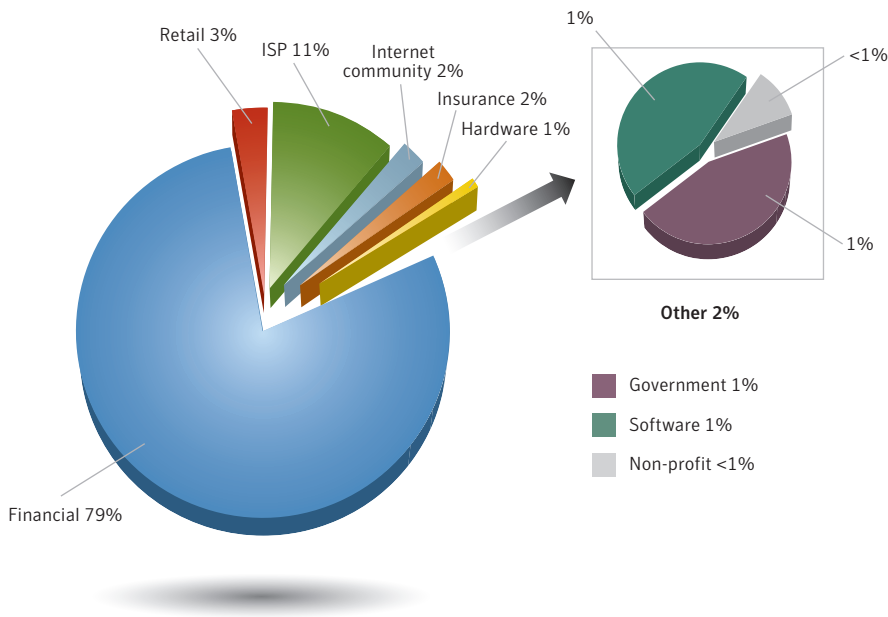


Figure 2. Brands phished by sector

Source: Symantec Corporation

Eight of the top ten organizations whose brands were spoofed by attackers in phishing attacks during first six months of 2007 belong to the financial services sector. Interestingly, one of the most frequently spoofed brands this period was a social networking site. While there is no immediate financial gain to be obtained by attackers who steal a user's account information, it may provide other returns. The attacker could use a social networking account to gather information from the hijacked account's friends, such as email addresses, by sending messages that appear to come from the legitimate user, who would likely be implicitly trusted by the message recipient.⁵ Additionally, the attacker can send messages containing links to Web sites that are designed to download malicious code on visitors' computers.⁶ Since the link comes from a user's friend, they may be more likely to trust the link and visit the site.⁷

⁵ http://www.symantec.com/enterprise/security_response/weblog/2006/11/an_imaginative_phishing_attack_1.html

⁶ http://blog.washingtonpost.com/securityfix/2007/06/web_2pointuhoh_worm_whacks_mys.html

⁷ For more on phishing attacks that target social networking sites, please see:
http://www.symantec.com/enterprise/security_response/weblog/2006/09/contextaware_phishing_realized.html

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
09/07 12755156