

PHISHING SPECIAL REPORT: WHAT WE CAN EXPECT FOR 2007

White Paper



EACH MONTH, RSA'S ANTI-FRAUD COMMAND CENTER (AFCC) ISSUES ITS *ONLINE FRAUD REPORT* WITH KEY STATISTICS FROM ITS GLOBAL PHISHING REPOSITORY.

THE AFCC IS A 24X7 WAR-ROOM THAT DETECTS, MONITORS, TRACKS AND SHUTS DOWN PHISHING AND OTHER TYPES OF ONLINE ATTACKS AGAINST OVER 180 INSTITUTIONS WORLDWIDE. THE AFCC HAS SHUT DOWN OVER 30,000 PHISHING ATTACKS AND IS A KEY INDUSTRY SOURCE FOR INFORMATION ON PHISHING AND EMERGING ONLINE THREATS.

LOOKING BACK AT THE PAST YEAR OF PHISHING-FIGHTING ACTIVITY, MANY TRENDS CAN BE OBSERVED.



The Security Division of EMC

Key Findings

• Phishing incidents level continues to grow

- Number of attacks has grown by 41% in the past 12 months
- Number of distinct brands attacked per month has grown by 135%

• Phishing targets are more varied than ever

- While most phishing attacks target the financial industry, there are more phishing incidents targeting other sectors such as retailers, online game operators and large ISPs.
- As phishers have advanced their local language capabilities, attacks have expanded geographically to many European and Asian countries. The most targeted countries in Europe are Spain, Italy and Germany.
- National banks are no longer the primary target of phishing. In the U.S., most phishing attacks now target regional banks and credit unions.





- **Phishing has become a mainstream fraud.** No longer the realm of sophisticated fraudsters who build their own tools and use the credentials they've stolen, phishing now has a structured "supply chain" that facilitates trades between "suppliers" (phishers) and "buyers" (typically local criminals who can 'cash out' compromised accounts).
- **Fraudsters are becoming more creative.** New forms of phishing attacks emerge, as well as more advanced attacks in the form of Trojans and Man-in-the-middle attacks, that are able to penetrate login-level two-factor authentication.

Phishing Incidents

Phishing activity is on the rise. While the number of monthly attacks tends to fluctuate—some months have a drop in phishing activities and some months have an increase—there's a clear growth over time. The number of phishing attacks increased by 41% in the last 12 months.

Brands Attacked by Phishing

More and more organizations are targeted by phishing. The number of distinct brands attacked increased by 135% in the past year, from 83 in July 2005 to 195 in July 2006.

Additional facts:

- In July 2006, 15% of the attacked brands (30 out of 195) accounted for 80% of total attacks.
- The average number of monthly attacks per brand dropped from 30 in 2005 to about 18 in 2006.
- Much of the growth is outside the 'traditional' target countries (i.e. US, Canada, UK and Australia).

April 2006 had a sharp decline in the number of attacked brands, but the overall number of attacks increased that month. This can be attributed to the strong demand for the credentials of a major US bank, diverting fraudster's attention away from other targets. That bank was heavily attacked for a few weeks, at times suffering hundreds of attacks per day.

Number of Phishing Attacks per Month

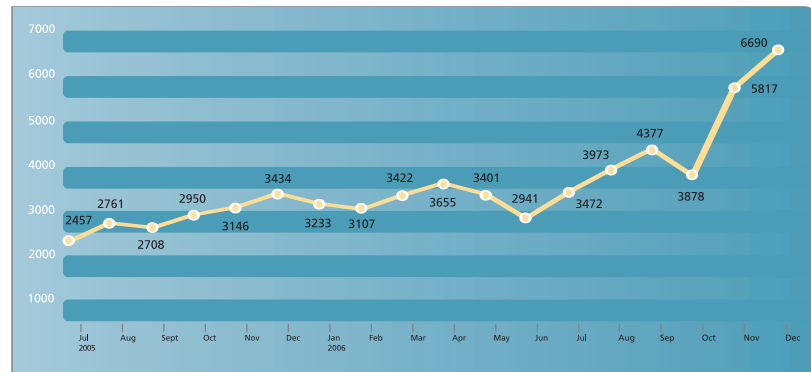


Figure 1: Phishing attacks per month—Worldwide (Note: The figure relates to distinct attacks spotted by the AFCC. Some industry sources use other methods, such as total number of reports on phishing attacks.)

Number of Brands Attacks per Month

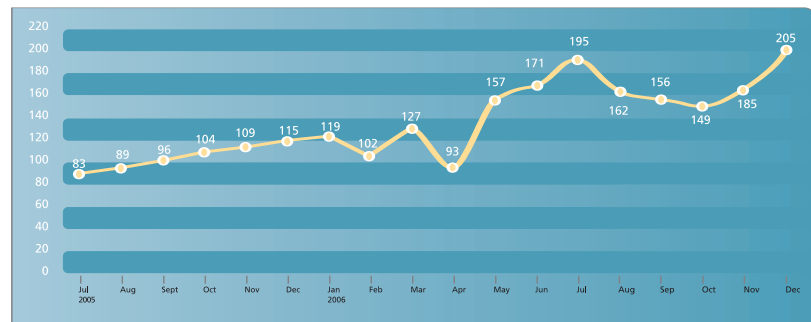


Figure 2: Brands attacked per month—Worldwide

Size of Target

National banks no longer account for the majority of attacks. In the US, the distribution of phishing attacks during July 2006 was as follows:

- National banks: 12%
- Regional banks: 41%
- Credit Unions: 47%

This trend isn't new: it started mid-2005, when fraudsters realized that the large banks were taking measures to reduce the effectiveness of attacks. They also discovered that attacks on national banks have exhausted a lot of their potential to fool unsuspecting customers. The focus shifted first to regional banks, and then in early 2006, to

credit unions and other small financial institutions. We anticipate the trend to continue.

As mentioned above, April was an exception: 35% of attacks focused on national banks, and specifically on a large US financial institution.

Hosting Countries

The United States continues to be the dominant hosting country for phishing attacks. This is triggered by a combination of several factors:

- The U.S. has the largest number of broadband connections, and as a result, the largest number of botnet-hijacked

Distribution of attacks according to FI size
January - December 2006

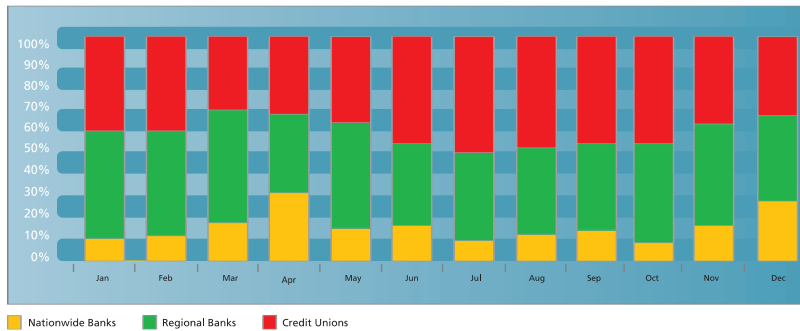


Figure 3: Distribution of attacks per FI size—U.S. only

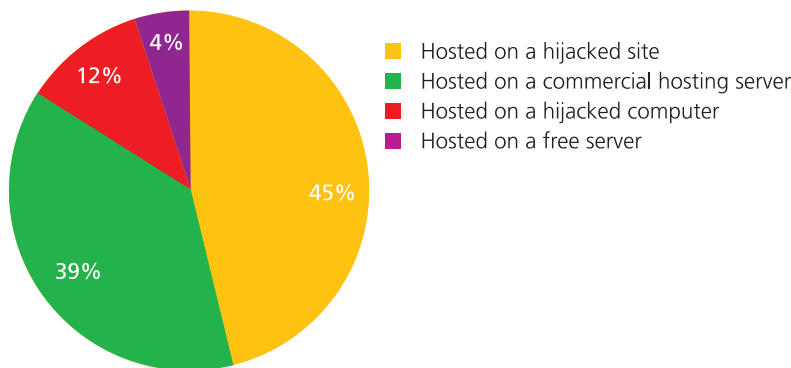


Figure 4: Hosting methods for phishing attacks

computers. Most phishing attacks are hosted in a compromised PC which is part of a botnet. Owners are typically unaware of the fact that their PC is being used as a vehicle in the service of fraudsters.

- The U.S. is also the largest target country. To maximize exposure, phishers prefer to launch attacks early morning in the target country so victims will get the email when they open their inbox in the morning. If the attack is hosted in the U.S., and is launched very early morning within a U.S. time zone, it is more difficult to reach the ISP. However, if the attack is hosted in Russia, for example, [7 hours ahead of the U.S.'s east coast], it's already business hours for the ISP and it can be quickly contacted.

- Since many of the attacks reside on private customer's PCs, shutting down the attack means disconnecting a customer. ISPs in the United States are more concerned with privacy issues and need to balance them against the responsibility of terminating fraud attacks.

In Europe, Germany is the largest host of phishing attacks. In Asia, Korea is the largest hosting country, followed by China.

Fraudsters Improve Their Methods

RSA's fraud intelligence specialists are monitoring fraudster communication channels such as fraud forums and chat rooms on an ongoing basis; they use various Human

EXAMPLE: CASHING OUT VIA POKER ROOMS

RSA identified a recent trend of using online poker rooms to cash out credit cards and other payment mechanisms. The fraudster opens an account in an online poker room, funds it with the stolen account, then plays a few hands in a poker room and intentionally loses all the funds to a collaborator. Money changes hands, the collaborator shares the profit with the fraudster, and the supplier of the stolen account gets his share as well.

Intelligence [HumInt] techniques to gain fraudsters' trust and deepen our understanding of eCrime methods.

Some insights from the fraud intelligence activity:

- Fraudsters have developed an elaborate model of supply and demand. Phishers specialize in collecting credentials from unsuspecting victims, and supply them to local crime rings that have a method of "cashing out" the account. Other links of the supply chain include developers of kits and tools, email collectors and providers of compromised host servers.
- The supply and demand model is built on trust. Similar to auction site trust models, "untrustworthy" fraudsters are publicly deployed.
- The "cash out" mechanisms are becoming more streamlined and creative, as fraudsters discover new exploits and vulnerabilities.

Emerging Threats

The monthly *Phishing Intelligence Report* published by RSA covers a variety of emerging threats¹. A very visible trend of technological advancement can be traced:

¹ Note: The date does not necessarily indicate the first-ever attack of a certain kind, but rather the first streamlined usage of such a method.



November 2005: Fraudsters start using a port-redirection attack commonly referred to as Rock Phishing Kit. In this method, the phishing email points to a proxy [TCP port re-director] that gets its content from a central spoofed website. Since multiple proxies are used—essentially tapping a botnet—it is very difficult to shut down the attack until the central spoofed site is located and the attack can be decapitated.

April 2006: The Torpig-family Trojan, a particularly damaging and technologically advanced session hijacking Trojan, is rapidly spreading. The Trojan monitors major banks' websites worldwide and, after the user logs in, displays a spoofed page while maintaining the original SSL session, thus being very difficult to detect. The Trojan spreads through operating system vulnerabilities.

July 2006: The world's first Man-in-the-middle-type attack targets a major US financial institution. The attack is designed to bypass two-factor authentication during the login.

January 2007: RSA unveils the discovery of a new threat—a "universal" Man-in-the-middle (MITM) phishing kit which can be configured by target, with very little effort required from the attacker. The MITM kit consists of a PHP file which is installed on a compromised server. The server acts as a proxy between the victims of the phishing attack and the genuine website of the bank. Victims of such an attack receive a regular phishing email. Once they click on the link within the email, they are directed to the compromised server (the proxy) which runs the phishing site. The compromised server communicates with the genuine bank site "on behalf" of the victim. Even the most savvy online users can be fooled as the proxy displays the genuine bank website to the victims, including all the various elements within the site.

The Outlook

RSA expects the evolution of online threats to continue in 2007. Here are some projections of trends we expect to see next year:

- Shifts in phishing demographics, driven by a greater focus on very small financial institutions, geographic expansion to new regions, targeting financial organizations that are not banks or lenders, and targeting non-financial organizations.
- Simple attacks and basic social engineering will still be used to attack targets that do not challenge the fraudsters with advanced layers of defense.
- A rapid evolution of real time, Man-in-the-middle Trojans designed to breach new authentication measures that banks deploy in the login stage.
- Integrated attacks on Phone banking and Internet banking using elaborate social engineering.
- An increase in identity theft and use of synthetic identities to funnel money from real accounts to fake accounts.
- Growth of fraud targeting European banks as inter-bank money transfers become faster and more prevalent.

What does all of this mean? As financial institutions raise the bar and continue to adopt new security measures, crimeware will proliferate in an attempt to circumvent the security mechanisms in place. In addition, fraud will likely migrate to new, less-protected markets such as retail, insurance, healthcare and telecommunications.

HOW TO STAY AHEAD OF EVOLVING THREATS

- Monitor the online space and **proactively disable known phishing sites** to protect your customers
- **Reduce fraudsters' interest in your customers' credentials** by enhancing consumer security:
 - Implement strong authentication, which can be transparent, visible or tangible
 - Deploy fraud detection software in the online / phone channel
- **Establish multiple layers of defense.** A single defense mechanism can always be bypassed by a combination of technical skills and social engineering
- **Equip yourself with adaptive, flexible defense mechanisms** that can quickly respond to emerging threats
- **Hook into an international fraud network** that tracks global resources used by fraudsters



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2007 RSA Security Inc. All rights reserved. RSA, and RSA Security are trademarks or registered trademarks of RSA Security in the U.S. and/or other countries. All other products and/or services are trademarks of their respective companies.