

RSA Online Fraud Report

July, 2008

A Monthly Report from the RSA Anti-Fraud Command Center Phishing Repository

Online fraud is evolving. Phishing and pharming represent one of the most sophisticated, organized and innovative technological crime waves faced by online businesses. Fraudsters have new tools at their disposal; and are able to adapt more rapidly than ever.

The RSA Anti-Fraud Command Center (AFCC) is a 24x7 war room that detects, monitors, tracks and shuts down phishing, pharming and Trojan attacks against almost 300 institutions worldwide. The AFCC has shut down over 97,000 phishing attacks to date and is a key industry source for information on phishing and emerging online threats.

The following statistics have been gathered from the RSA Anti-Fraud Command Center phishing repository. Each statistic includes a short trend analysis based on the expertise of the fraud analysts within the RSA Anti-Fraud Command Center.

This Month: The End of Neosploit?

The first and most important step when working to grow a pool of malware-infected PCs is the infection stage. The goal of the fraudster is to infect as many users as possible, as quickly as possible – and remain undetected for as long as possible.

Neosploit is a brand that could be relied upon to solve that problem rather well. Designed to ease the infection stage, Neosploit is an infection kit which exploits numerous system vulnerabilities and infects PCs worldwide with any type of malware. Neosploit checks “candidate” PCs in order to find vulnerabilities, and once these are found the PC will be infected with the malware of the criminal’s choice.

However, the RSA Anti-Fraud Command Center received information in July indicating that we may soon see the last of this “Neosplitation”.

Background: the Growth of Neosploit

Neosploit is currently the most advanced infection kit used by online criminals, the successor of well-known infection kits such as MPack, Icepack and others. Like all its predecessors, it is sold on the Internet “underground” to online criminals. Neosploit is not new; it has already gained much attention from the media and blogger communities. Neosploit began acquiring its popularity with version 2.0.xx, when it made its first mark as a highly-scalable infection kit. Its reliability, scalability and efficiency all contributed to the growth and adoption of Neosploit. In April 2008, the Neosploit development team launched Neosploit version 3.0.0, introducing numerous new and improved features. Among the noticeable improvements were an improved statistical engine, enhanced configurability, and an improved exploitation package. See “Neosploit infection rate statistics” next page.



The Security Division of EMC

Main Menu
[Total Stats](#)
[Log-Out](#)

Version: 3.0.7 (build 1087)
 Built: Jun 27 2008 23:59:41
 Modules:
 • Standart Pack
 • Multiple File Uploading

Total Stats

Username	Traffic						Loads					Action	Stats	
	MSIE	Gecko	Safari	Opera	Other	Total	MSIE	Gecko	Safari	Opera	Other			Total
admin	2	0	0	0	0	2	1 (50%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (50%)	Reset	D C B S E V M
	36657	6210	39	206	749	42861	2244 (6.2932%)	75 (1.2077%)	0 (0%)	0 (0%)	0 (0%)	2319 (5.4109%)	Reset	D C B S E V M
	19848	2327	4	83	303	22565	916 (4.6160%)	20 (0.8984%)	0 (0%)	0 (0%)	0 (0%)	936 (4.1480%)	Reset	D C B S E V M
	22041	4922	64	86	2037	29140	1451 (6.5831%)	1 (0.0203%)	0 (0%)	0 (0%)	0 (0%)	1452 (4.9828%)	Reset	D C B S E V M
	19025	4241	30	943	1044	25283	2521 (13.250%)	297 (7.0030%)	0 (0%)	0 (0%)	0 (0%)	2818 (11.145%)	Reset	D C B S E V M
	477	179	0	16	29	701	43 (9.0146%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	43 (6.1340%)	Reset	D C B S E V M

Neosploit infection rate statistics

06-06-2008 - вышла бета версия 3.0.6. кому не продлил лицензию стукните еще раз в асю.
 23-05-2008 - вышла бета версия 3.0.5
 18-05-2008 - вышла бета версия 3.0.4
 28-04-2008 - вышла бета версия 3.0.3
 21-04-2008 - вышла бета версия 3.0.2
 18-04-2008 - вышла бета версия 3.0.1

Neosploit's release notes

Neosploit's software versions

Since April's major release, the Neosploit development team continued its work, releasing minor versions and supporting their customers in order to rapidly improve the product. The release cycle was accelerated and new versions started arriving approximately twice per month complete with new and improved features, enhanced support, and the creation of an online forum for customers. Customer demand increased in tandem. Truly, this displayed all the signs of a fully-functional and customer-centric business. See "Neosploit's release notes" above.

Financial problems

In mid-July, however, evidence showed that Neosploit's successful business was running into problems. It is likely that Neosploit was finding it difficult to sustain its new customer acquisition rate, and that its existing customers were not generating enough revenue to sustain the prior rate of development. These problems appear to have been too much of a burden, and we now believe that the Neosploit development team has been forced to abandon its product.

Mimicking the practices of legitimate businesses in similar situations, RSA's sources reported that the organization posted an "out of business" announcement. (see sidebar). Whether or not Neosploit will actually cease its business, and whether or not it will return, is a question that only time can answer. However, there's no doubt that when the demand is high enough someone will step up to the plate and fulfill the need for a professional malware infection kit – Neosploit or not.

Neosploit's "out of business" announcement

"Unfortunately, supporting our product is no longer possible. We apologize for any inconvenience, but business is business since the amount of time spent on this project does not justify itself.

We tried hard to satisfy our clients' needs during the last few months, but the support had to end at some point. We were 1.5 years with you and hope that this was a good time for your business.

Now we will not be with you, but nevertheless we wish that your businesses will prosper for a long time! Good luck all, The Neosploit Team!"

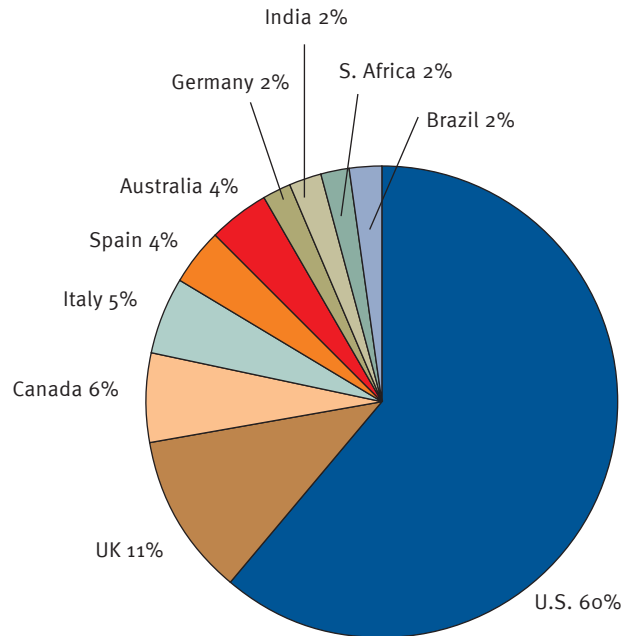
(translated from Russian)



1. Breakdown of Global Banking Brands Attacked by Phishing

Trend Analysis

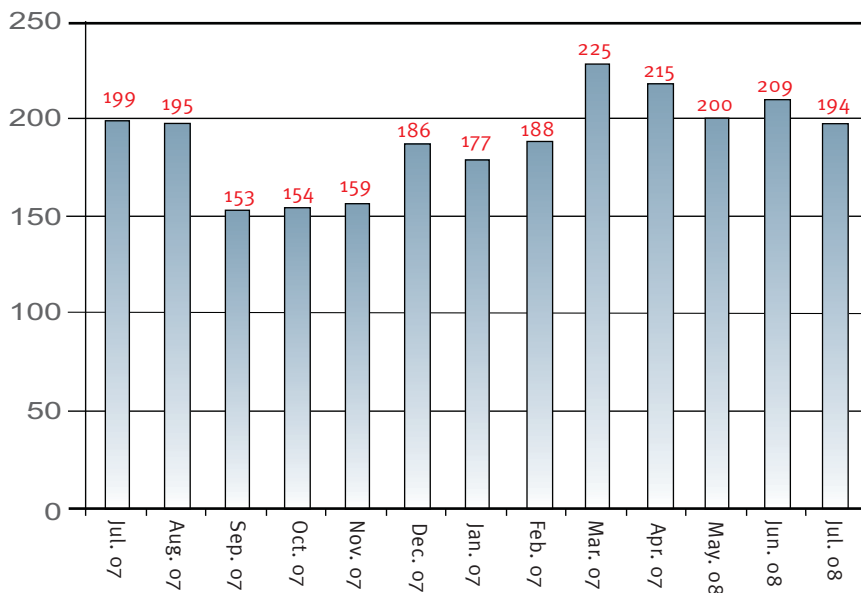
During July 2008, the distribution of attacked global brands remained relatively similar to that of previous months. Consistent with prior months, U.S. brands were the most attacked - receiving 60% of the total phishing attacks during the month. Brazil dropped to tenth place after entering the list for the first time last month, when it was ranked third. Canada, Italy, Spain, Australia and Germany maintained similar positions to prior months.



2. Number of Brands Attacked Per Month

Trend Analysis

The total number of brands attacked decreased in July - down to the lowest rate since February 2008. However, new brands continue to be targeted and the RSA Anti-Fraud Command Center detected first-time attacks against 29 entities during July 2008. This is an increase of approximately 20-30% when compared against first-time attacks during the prior two months.

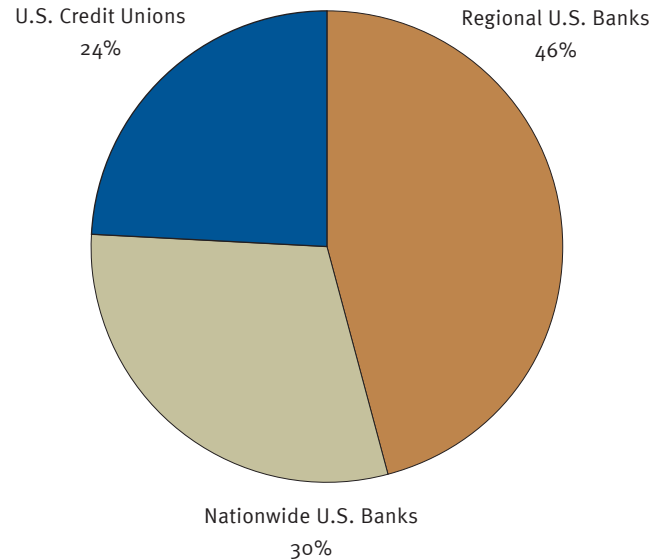




3. Segmentation of U.S. Banking Brands Attacked by Phishing

Trend Analysis

In July 2008, the RSA Anti-Fraud Command Center noted a continuing decrease in the proportion of Federal credit unions coming under attack, tumbling almost 50% since May. Regional banks were attacked more than Federal credit unions and nationwide banks combined, and the rate of attacks against nationwide banks remained proportional to June 2008.



4. Top Hosting Countries

Trend Analysis

In July, Luxembourg moved up to second place within the distribution of hosting countries, moving the U.K. down to sixth place. On the list for only the third month, the prominence of Luxembourg is primarily the result of Rock Phish domains hosted within that country - even though Rock Phish activity has generally decreased. France, Germany, Canada, South Korea and Russia continue to host similar percentages of online attacks on a monthly basis. July saw China return to the list after its absence in June.

