

Ryan Sherstobitoff takes us into the AV lab at Panda Security USA

Targeted Scams: A new trend

By Ryan Sherstobitoff

In the last couple of months the trend seems to have shifted towards cybercriminals employing a great number of resources to commit financial fraud through targeted scams. The latest attempt surfaced around the recent launch of the Apple iPhone. Cybercriminals established a phony Apple Shop which sold iPhones to the public. However, this was not your common run-of-the-mill phishing attack. This one used a Trojan to guide the user into purchasing an iPhone through the fake shop where the hackers could capture personal details.

The Trojan works by registering a browser helper object (BHO) within Internet Explorer (RWERA21S1.dll) and monitoring all Internet activity. When the user infected with the Trojan visits www.iphone.com, the Trojan injects code that automatically redirects the user to a fake identical page. Not only is the Trojan registered as a BHO within Internet Explorer – *watching every move the user makes* – but it also joins the infected computer to a botnet as a slave. Thus the infected computer can receive remote commands such as downloading additional malicious executables. The Trojan also includes adware popups to entice users to visit the spoofed iPhone shops.

The user receives no hint that his details have been captured and sent to cybercriminals while he waits for his iPhone – which, of course, is never shipped.

Most cybercriminals understand the “business” needs of the hackers who are their customers. For example, sophisticated command and control centers which display stats are usually included in the purchase price of the custom, made-to-order Trojans they sell. Hackers can compromise a legally registered website or domain to host the control panel for their botnet.

To infect users on a massive scale to join a botnet, a common method used by cybercriminals is tainting the HTML code (Iframe reference) within legally registered domains in order to establish a staging point for infections. For example, malware generated with the MPACK hacker toolkit¹ infected users through domains that otherwise would not be suspected as malware transmission points. High volume traffic sites are

particularly of interest to cybercriminals, obviously due to the higher potential of infections. It is suspected that MPACK has been used to transmit many forms of malware, including the Limbo 1.5 banking Trojan, that exploit and compromise users’ Internet browsers so further infections can occur.

As always, these “toolkits” are sold through the Internet as made-to-order with specific customizations. MPACK was seen for as low as \$150 on some sites. Cybercriminals are making a lot of money by selling tools that make it fairly easy for anyone to commit financial fraud utilizing Trojan building kits such as MPACK and PINCH.²

In order for malware to avoid detection by AV software, several obfuscation techniques are being used within the malware binaries themselves:

- Writing custom routines to pack the Malware, thus confusing AV engines that do not incorporate generic unpacking algorithms.³
- Not actually installing the payload portion of the malicious code on users’ PC itself, but instead it resides on a remote server that is accessed by a skeleton Trojan on the infected computer.⁴

Normally these scams are associated with botnets for stealing banking credentials. However, the most recent trend is shifting toward scams that precisely target a huge opportunity to exploit, such as the consumer demand for iPhones.

About the Author

Ryan Sherstobitoff is the Product Technology Officer at Panda Security USA (www.pandasecurity.com). Ryan lectures across the USA on cybercrime trends as well as corporate risk assessments. He can be reached at ryans@pandasecurity.com.

1 <http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/07/20/More-about-Mpack-II.aspx>.

2 http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/07/18/PINCH_2C00_-THE-TROJAN-CREATOR.aspx.

3 <http://research.pandasoftware.com/blogs/research/archive/2007/02/12/Packing-a-punch.aspx>.

4 http://research.pandasoftware.com/blogs/research/archive/2007/05/22/Malware_2D00_friendly-countries.aspx.