In the last few years, we have seen the mobile space explode with malware. According to a recent report by Trend Micro, the number of malware and high-risk apps available on the Android platform has crossed the one million mark, growing more than a thousand fold in under 3 years.

To the financial industry, the threat manifests itself in the form of rogue apps (apps that mimic the legitimate banking apps) and in the form of SMS-sniffers. The latter becoming standard functionality when it comes to banking Trojans, designed to overcome a single obstacle: out-of-band authentication using mobile devices. By installing a malicious app on the device, the botmaster can intercept SMS messages and/or telephone calls thus defeating the OOB authentication. It is one such app that we recently analyzed.

The app, which has been around for a while and uses the moniker mToken, disguises itself as a fake token app (AV classification), and displays “standard” functionality as far as SMS message interception goes. During the installation process, it would ask the user for the necessary SMS-, and communication-related permissions; and to appear legitimate it made use of the customers’ logos, not to mention displaying a “random” token code when launched (a detailed analysis of the app is available below).

But the most interesting finding was the analysis of the Web-based control panel. This offered a behind-the-scenes glimpse into a mobile botnet operation and demonstrated the ease of commanding it, but more importantly—its flexibility and resilience.

The panel we analyzed was used in attacks targeting several financial institutions around the globe along with a well-known social media platform. At the time of RSA’s analysis, it was commanding over 2,000 mobile devices and had intercepted over 25,000 SMS messages (see Figure 1 on the following page).
MOBILE APP DEVELOPMENT ON-THE-FLY

The panel’s standard functionality provided the fraudster with the ability to review bot-related information, send HTTP-based commands (to the bot), and review the intercepted SMS messages. But the flexibility and resiliency of the operation was apparent when we hit the application builder screen (see Figure 2).

Built into the control panel was functionality to create custom-looking malicious mobile apps on-the-fly. Asking the botmaster to provide basic app-related information (such as name) and default communication points, it would offer a selection of existing designs or the ability to create new designs using image files and a simple HTML file.

In order to build the app, the panel makes use of APKTool, a freeware, command-line tool used to decompile and recompile Android application packages. The tool wraps the HTML and images in a standard Android APK and makes it available to the fraudster for immediate use.

ANALYSIS OF A ROGUE APP

The delivery method of the app uses basic social engineering techniques to get the user to download and install the malicious app. Once logged into the bank’s website (on the PC), the malware presents additional, custom screens (using HTML-injection) asking the victim to select the mobile device’s operating system (only Android is supported) and the device’s phone number to which the fraudster then sends an SMS message with a link to download the app.
During the installation process, the app requests permissions to communicate via the internet and to gain access to the SMS messages (send and receive).

The app then waits for the botmaster to enable the SMS-sniffing function (via the control panel) at which point it begins to intercept all inbound and outbound SMS messages, forwarding them to the drop server.

Analysis of the bot’s communication revealed that it would regularly beacon its command and control server receiving updated communication parameters as well as commands to carry out on the device. Commands included enabling (or disabling) SMS-interception and sending SMS messages from the infected device to a third party. This can be used to send SMiShing messages to other devices that will originate from the victim device and possibly allow the botmaster to grow his botnet.

SUMMARY

The ability to create custom-looking apps, as well as to command the botnet over HTTP and SMS, makes this operation very resilient. Having two separate communication channels (to the bots) means that any take down effort must affect both points simultaneously. Not to mention the PC-based Trojan operation that can be used to re-infect the mobile devices if needed.

It is no secret that relying solely on SMS-based out-of-band authentication is not practical. Taking today’s mobile threat landscape into account will require organizations to consider stronger authentication measures to protect the identities and transactions of their customers.
Phishing Attacks per Month
RSA identified 42,364 phishing attacks marking a 31% decrease from October’s record setting number. Typically, November sees a slight increase from October, but last month’s spike could indicate cybercriminals are focused on cashing out.

US Bank Types Attacked
U.S. nationwide banks saw an increase in phishing volume in November and remained the most targeted with 71% of phishing attacks targeted at that sector.

Top Countries by Attack Volume
The U.S. remained the most targeted country in November with an overwhelming 76% of total phishing volume, followed by the UK, India and South Africa.
**Top Countries by Attacked Brands**

In November, 26% of phishing attacks were targeted at brands in the U.S., followed by the UK, India, France and Brazil.

---

**Top Hosting Countries**

The U.S. continues to host the most phishing attacks, hosting 47% of global phishing attacks in October, followed by Germany, the UK and the Netherlands.

---

**CONTACT US**

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.emc.com/rsa

©2013 EMC Corporation. EMC, RSA, the RSA logo, and FraudAction are trademarks or registered trademarks of EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned are the property of their respective holders. DEC RPT 1213