Endpoint Protection

community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument

Jan 22, 2015 08:57 AM

Migration User

Contributor: Yi Li

A group of attackers, which we call Scarab, has been performing highly targeted attacks against particular Russian-speaking individuals both inside and outside of Russia since at least January 2012. In each campaign, the attackers typically target a small amount of individuals—rather than enterprises or governments—using economic, military, topical, or generic lures. On average, less than ten unique computers are infected per month and there is no indication that the attackers are trying to spread through the victim's local network, suggesting that Scarab's campaigns are extremely targeted in nature.

Many of Scarab's campaigns focus on distributing the group's custom malware (Trojan.Scieron and Trojan.Scieron.B) through emails with malicious attachments. These files contain exploits that take advantage of older vulnerabilities that are already patched by vendors. If the attackers successfully compromise the victims' computers, then they use a

basic back door threat called Trojan.Scieron to drop Trojan.Scieron.B onto the computer. Trojan.Scieron.B has a rootkit-like component that hides some of its network activity and features more enhanced back door functionality.

Who are the Scarab attackers?

Based on our research, the Scarab attackers are a technically capable group, judging on how they have custom-developed several malicious tools for these campaigns. However, they are not highly skilled or well resourced, as they rely on older exploits and executables stored in compressed archives to distribute their threats.

There are some indications (based on language resources) that the attackers are familiar with Chinese-language characters, and they seem to mostly target Russian speakers located in Russia and other regions around the world.

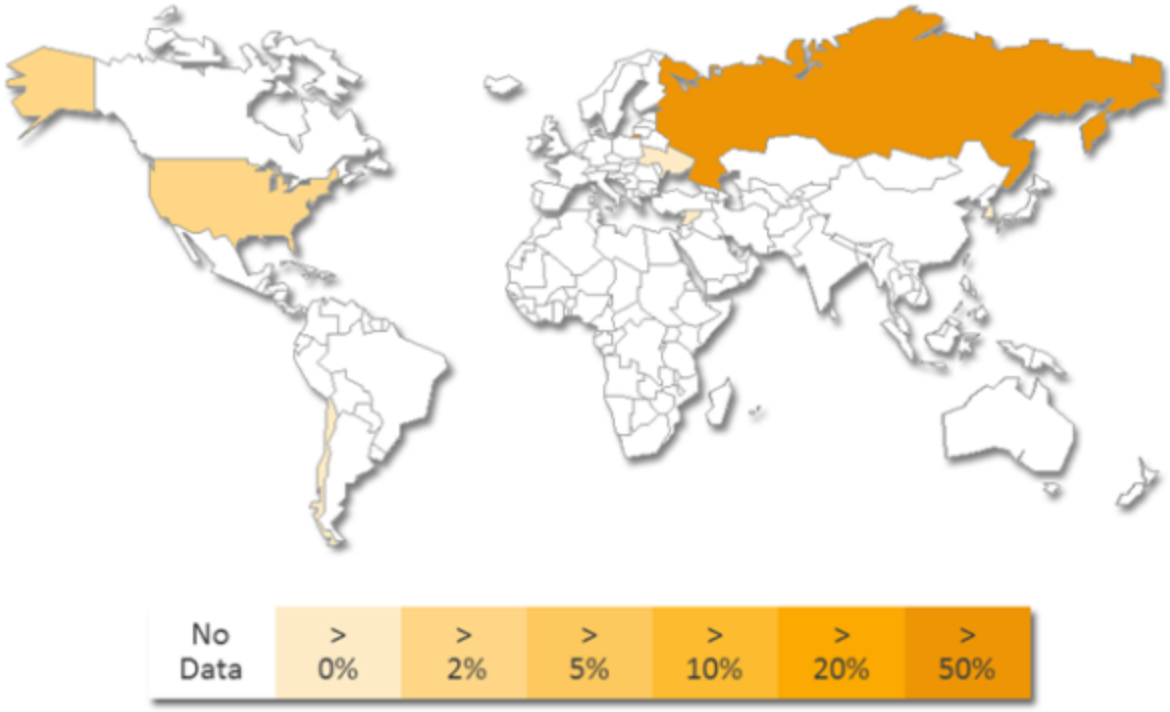

Figure 1. Scarab victims based on Symantec telemetry

The group conducts command-and-control (C&C) operations almost exclusively through the use of dynamic domain name system (DNS) domains. The C&C servers are usually hosted in South Korea; however, there have been instances where servers were located in other countries.

For the majority of 2012, there was not much information about Scarab's victims. However from October 2012, a number of emails used by Scarab were blocked by Symantec .Cloud. All of the emails were sent from @yandex.ru email addresses.

Early attacks
On October 29, 2012, an email with the Russian-language subject “Экспериментальное определение эффективно” was sent to two individuals working for a large retail organization. Translated to English, the email’s subject is “Experimental definition is effective.”

These emails contained Microsoft Word attachments that triggered an exploit taking advantage of the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158). Once triggered, the exploit dropped a copy of Trojan.Scieron onto the victim’s computer. The attackers continued to intermittently send emails with .doc malware droppers until August 2013.

On January 22, 2013, the Scarab attackers sent an email with the English-language subject “Joint Call For Papers - Conferences / Journal Special Issues, January 2013” to two individuals. The attackers sent the message to email accounts associated with an Australian-funded academic research project that had concluded in 2010. It is possible that the researchers were continuing to use the email accounts for unrelated topics and this was why the attackers chose to target them. Seven days later, another email was sent to the same two individuals, this time with a Russian-language subject of “Информация по обслуживанию высвобожденны,” which translates to “Service-related information are released” (sic).

G20 summit focus
From this point on, at least until January of 2014, the attackers moved to finance-related lures and targets. In April, the attackers sent an email with the subject “G20 receives clean bill of health at Boao” to a European government target.

In August, they sent another email to six people working for an international economic organization. This email had the Russian language subject of “G20 на 2013 г” which translates to “G20 for 2013.”

In August, a final G20-related email was sent to two individuals working in the Economic Ministry of a European government. That email had the English-language subject “About G20 details.”

Russian news lures
There were no further emails discovered and no active infections detected until January 2014, when Scarab’s activity resumed and continued up to now. From that month on, the attackers have been using “.scr” files to drop Trojan.Scieron. The titles of these .scr files are usually in Russian, and are a hint as to the nature of the targets. It’s very likely that the .scr files are being delivered by email; however, this has not been confirmed. It is also likely and again, unconfirmed that the .scr files are embedded in .rar files.

One example of the group's malicious .scr file names is "Россия к 2016 году проведет испытания газовых турбин для военных кораблей." This translates to "Russian Federation to 2016 will test gas turbines for warships." The title comes from an article, published in June 2014, on a Russian media website.

Figure 2. The attackers used the titles of news articles from a Russian media site for their malicious files' names

Another more recent file name was "план работы на июнь 2014 года.doc.scr" which translates to the quite generic "work plan for June 2014 year.doc.src."

Looking at the total number of infections per country in Figure 1 based on Symantec telemetry, it's clear that Russia, or at least Russian speakers, are the primary targets of the Scarab attackers, although non-Russian speakers have been targeted as well.

Scarab's malware

In all of these campaigns, the attackers have attempted to compromise victims' computers with a variant of Trojan.Scieron. This is a basic back door threat that is used to download additional malware onto the target's computer.

The main payload of Trojan.Scieron is within a DLL file. This file is dropped either from a Trojanized Microsoft Word document or from other PE files.

Once the Trojan compromises the victim's computer, it is able to perform the following actions:

- Gather system information, such as the computer name, host name, operating system version, and drive type
- Download additional files
- Execute files
- Retrieve specific files from the victim's computer
- List directories
- Delete files
- Move files to other folders

In most of the investigated incidents, Trojan.Scieron has been used to download an enhanced version of itself, which Symantec detects as Trojan.Scieron.B. This threat includes a basic 'rootkit-like' tool which hides some of its network activity.

Trojan.Scieron.B's file names seen to date are usually seclog32.dll (back door) and hidsvc.dat (rootkit). The back door's functionality includes the following features:

- Create, list, and terminate processes
- Read, set, and delete registry entries
- Read, write, list, and delete files and directories
- Gather cached URLs
- Launch remote shell
- Gather recent active files
- Retrieve details from its configuration file

Trojan.Scieron.B's 'rootkit' functionality allows it to hide a Transmission Control Protocol (TCP) port in communications.

Symantec and Norton protection

The Scarab attackers have been consistently targeting a select number of victims with custom malware over the last few years. While the group uses older exploits, their campaigns seem to have had some success, judging on how they have continued to operate similar campaigns over the years. The attackers' focus on Russian speakers shows that they have specific targets in mind and they continue to adjust the subject of their email campaigns to successfully compromise their victims.

Symantec .Cloud blocks emails that come from the Scarab attackers. Symantec and Norton products also offer the following detections against Scarab's custom malware:

- Trojan.Scieron
- Trojan.Scieron.B

In general, you should adhere to the following best practices to prevent Scarab's attacks from compromising your computer:

- Exercise caution when receiving unsolicited, unexpected, or suspicious emails.
- Avoid clicking on links in unsolicited, unexpected, or suspicious emails.
- Avoid opening attachments in unsolicited, unexpected, or suspicious emails.
- Update the software, operating system, and browser plugins on your computer to prevent attackers from exploiting known vulnerabilities.
- Use comprehensive security software, such as Norton Security, to protect yourself from malware.

Indicators of compromise (IoC)

For a full list of IoCs, please check out our indicators of compromise document.