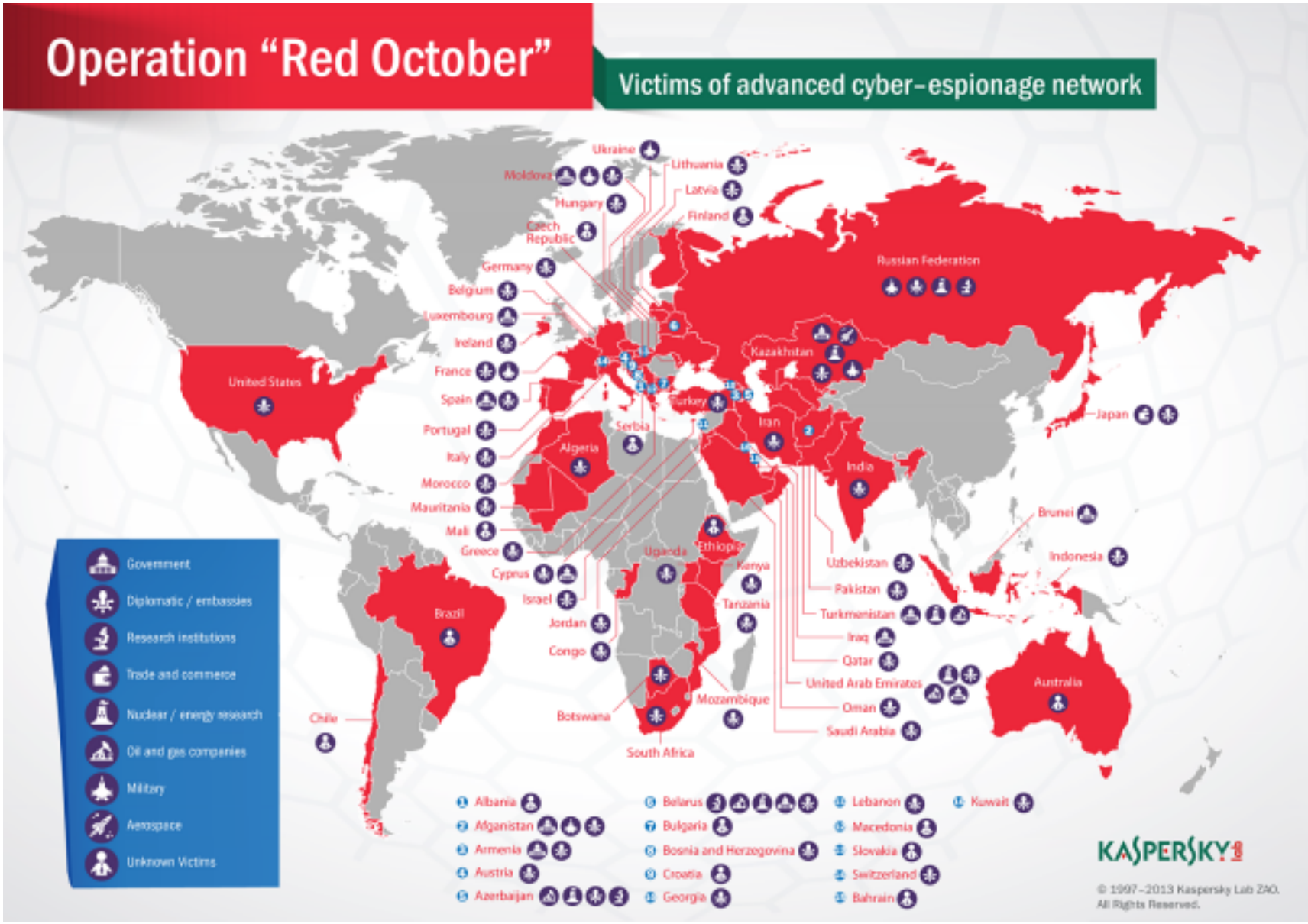
Operation "Red October"

Victims of advanced cyber-espionage network



Enlarge
Kaspersky Lab

Massive espionage malware targeting governments undetected for 5 years

"Red October" command-and-control setup more sophisticated than that of Flame.

by **Dan Goodin** - Jan 14 2013, 12:15pm EST

> Researchers have uncovered an ongoing, large-scale computer espionage network that's targeting hundreds of diplomatic, governmental, and scientific organizations in at least 39 countries, including the Russian Federation, Iran, and the United States.

Operation Red October, as researchers from antivirus provider Kaspersky Lab have dubbed the highly coordinated campaign, has been active since 2007, raising the possibility it has already siphoned up hundreds of terabytes of sensitive information. It uses more than 1,000 distinct modules that have never been seen before to customize attack profiles for each victim. Among other things, components target individual PCs, networking equipment from Cisco Systems, and smartphones from Apple, Microsoft, and Nokia. The attack also features a network of command-and-control servers with a complexity that rivals that used by the Flame espionage malware that targeted Iran.

"This is a pretty glaring example of a multiyear cyber espionage campaign," Kaspersky Lab expert Kurt Baumgartner told Ars. "We haven't seen these sorts of modules being distributed, so the customized approach to attacking individual victims is something we haven't seen before at this level."

The main purpose of the campaign is to gather classified information and geopolitical intelligence. Among the data collected are files from cryptographic systems such as the Acid Cryptofiler, with the collected information used in later attacks. Stolen credentials, for instance, were compiled and used later when the attackers needed to guess secret phrases in other locations.

Little is known about the people or organizations responsible for the project, and conflicting data makes it hard to attribute the nationality of the attackers. While the malware developers spoke

Russian, many of the exploits used to hijack victim computers were initially developed by Chinese hackers. Also clouding the identity of the attackers is the long roster of victims. The Russian Federation was the most targeted country, followed by Kazakhstan, Azerbaijan, Belgium, India, Afghanistan, Armenia, Iran, and Turkmenistan. In all computers belonging to 39 countries from a variety of continents are infected.

The command-and-control infrastructure that receives the stolen data uses more than 60 domain names as proxy servers to obscure the final destination. These domains are believed to funnel data to a second tier of proxy servers, which in turn are believed to send the information to a "mother ship" that Kaspersky researchers still know little about. The ability of the infrastructure to shield the identity of the attackers and to resist takedown efforts rivals the command-and-control system used by Flame, the espionage malware reportedly developed by the US and Israel to spy on Iran. The Red October malware itself has remained undetected on more than 300 PCs and networks for more than five years.

"It's been a very-well-maintained and set-up infrastructure that's supported with multiple levels of proxies in order to hide away the mothership," Baumgartner said. "They've been very effective at cycling through these domains and staying under the radar for the past five years."

“Foolproof” backdoor

One novel feature contained in Red October is a module that creates an extension for Adobe Reader and Microsoft Word on compromised machines. Once installed, the module provides attackers with a "foolproof" way to regain control of a compromised machine, should the main malware payload ever be removed.

"The document may be sent to the victim via e-mail," the researchers explained. "It will not have an exploit code and will safely pass all security checks. However, like with exploit case, the document will be instantly processed by the module and the module will start a malicious application attached to the

document."

Red October is also notable for the broad array of devices it targets. Beside PCs and computer workstations, it's capable of stealing data from iPhones and Nokia and Windows Mobile smartphones, along with Cisco enterprise network equipment. It can also retrieve data from removable disk drives, including files that have already been deleted, thanks to a custom file recovery procedure.

Each infection is indexed by a unique ID that's assigned to the compromised machine. The identifier helps to ensure that each attack is carefully tailored to the specific attributes of the victim. For example, the initial documents designed to lure in a potential victim are customized to make them more appealing. Every single module is specifically compiled for the victim with a unique victim ID inside. What's more, when connecting to the control channel, backdoors identify themselves with a specific string that appears to be the victim's unique ID. "Presumably, this allows the attackers to distinguish between the multitudes of connections and perform specific operations for each victim individually," Kaspersky said.

Despite the sophistication and organization of Red October, the researchers said they have found no evidence that the campaign is related to Flame, Gauss, Duqu, or other espionage malware discovered in the wild over the past few years.

"Currently, there is no evidence linking this with a nation-state sponsored attack," Kaspersky researchers wrote in a blog post published Monday morning. "The information stolen by the attackers is obviously of the highest level and includes geopolitical data which can be used by nation states. Such information could be traded in the underground and sold to the highest bidder, which can be of course, anywhere." (A corresponding research report is here.)

Kaspersky said it came across the operation in October after a request from an unidentified partner. Researchers were able to peer inside the operation after "sinkholing"—that is gaining control of—six

of the 60 domains used as first-tier proxies and observing the traffic sent between infected machines and the control servers. From early November 2012 until Thursday, researchers observed more than 55,000 connections to the sinkhole coming from 250 different IP addresses. In at least some of the cases, Kaspersky was able to obtain the domains because they remained unregistered even after they had been hardcoded into the malware. That would appear to have been a major oversight by the attackers.

The discovery of Red October opens yet another chapter in the just-begun era of highly advanced espionage malware that already included Duqu, Flame, and Gauss. With its high degree of customization and its ability to evade detection for five years, the operation has rivaled previous espionage campaigns including the Aurora attacks that hit Google and dozens of other large companies three years ago.

"All of these are very well-coordinated, very professionally run projects," Baumgartner said. "There's not enough evidence to link it to a nation-state, but certainly this level of interest and multi-year, ongoing campaign puts it up there with something like Flame and Duqu in the amount of effort it takes to seek out those targets and infiltrate the networks."