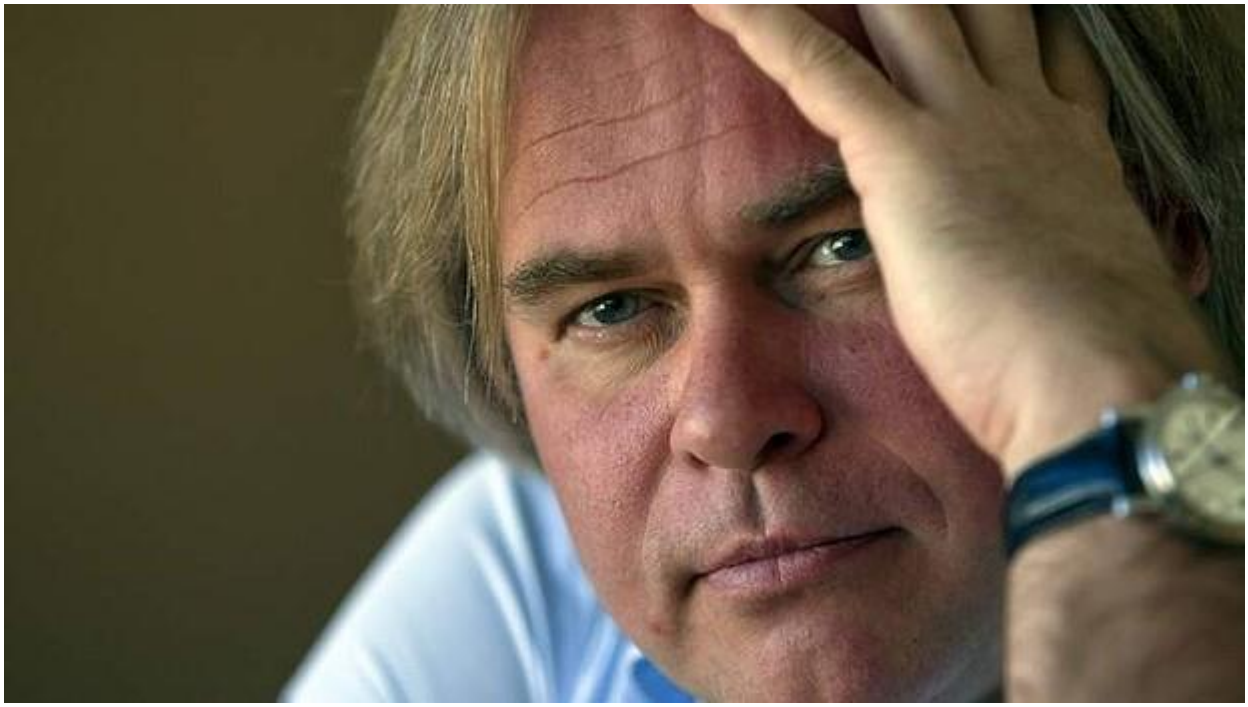
The hunt for Red October: five-year cyber espionage campaign uncovered



Eugene Kaspersky, CEO of Kaspersky Labs, has told Fairfax Media millions of dollars are invested every year by cyber criminals to developed sophisticated viruses. *Photo: Lee Besford*

A Russian cybersecurity company issued a report on Monday saying that it had identified a sophisticated cyber espionage campaign that has been in operation since 2007.

The spy campaign targeted a range of government and diplomatic organisations, mostly in Eastern Europe and Central Asia, but also in Western Europe and North America.

Kaspersky Lab, the firm behind the discovery, said digital clues suggested the perpetrators were Russian-speaking, but that the campaign did not appear to be the work of a nation state. However, as with a number of other alarming recent reports on computer spying, Kasperky's report offered few details that would allow for independent verification and did not specifically call out the names of the organisations affected.

In an interview, Kurt Baumgartner, a senior security researcher at Kaspersky Lab, said that among the "several hundreds" of victim organisations were "embassies, consulates and trade centers." The vast majority of infected machines were based in Russia — where Kaspersky identified 38 infected machines — followed by Kazakhstan, where 16 infected machines were identified. Six infected machines were found in the United States.

Baumgartner described the campaign as a "sophisticated and very patient multi-year effort" to extract geopolitical and confidential intelligence from computers, network devices like routers and switches, and smartphones. The malware was designed to extract files, emails and passwords from PCs, record keystrokes and take screenshots, and steal a user's web browsing history on Chrome, Firefox, Internet Explorer and Opera browsers. It could also pilfer contacts, call histories, calendars, text messages and browsing histories from smartphones, including iPhones, Windows, Nokia, Sony, and HTC phones. And it collected information about installed software, including Oracle's database

software, remote administration software and instant messaging software, like that made by Mail.Ru, a Russian email and instant messaging service.

But Kaspersky said what set the campaign apart was the fact that the attackers engineered their malware to steal files that have been encrypted with a classified software, called Acid Cryptofiler, that is used by several countries in the European Union and NATO to encrypt classified information.

Researchers discovered several Russian words embedded in the malware's code, suggesting the attackers are of Russian-speaking origin. For instance, the word "Zakladka" appears in the malware, which, in Russian and Polish, can mean "bookmark." It is also a Russian slang term meaning "undeclared functionality" in computer software or hardware. Intriguingly, Kaspersky's researchers said that, in Russian, it also refers to a "microphone embedded in a brick of the embassy building." (The United States and Russia have a history of bugging each other's embassies.)

But as sophisticated as the malware was, Kaspersky said the methods attackers used to infect systems were not. Machines were infected using a basic "spearphishing" attack, in which they sent malicious emails to people within targeted organisations that contained malicious Microsoft Excel or Microsoft Word documents. Once opened, attackers were given full access to victims' machines through well-known security exploits that were previously used in campaigns by Chinese hackers to spy on Tibetan activists and military and energy sector targets in Asia.

Baumgartner said the attackers either used well-known exploits out of "laziness or as a clever way to hide their tracks."

The firm said attackers created more than 60 domain names and used several server locations, mainly in Germany and Russia, to manage the network of infected machines. But it said those servers were "proxies" designed to hide the true "mother ship" command and control server.

Asked why Kaspersky decided not to identify the targets of the attack by name, Baumgartner said that Kaspersky's investigation was still in place.

Cybersecurity has become a significant and growing concern globally, with hackers gaining access to private corporate and military secrets, and intellectual property.

Last year, Kaspersky Lab discovered several state-sponsored computer viruses including Flame, a sophisticated virus that spied on computers in Iran, and Gauss, a separate virus that targeted Lebanese banks. The firm said it believed both viruses were sponsored by the same nation states that created Stuxnet, the virus *The New York Times* has reported was a joint effort by the United States and Israel.
But Kaspersky has been less forthcoming on viruses originating in its own backyard, in Russia and neighboring states, where Russian-speaking criminal syndicates control a third of the estimated $US12 billion global cybercrime market, according to the Russian security firm Group-IB.

This latest discovery could signal a turning point. The firm nicknamed the campaign by Russian speakers "Operation Red October" — Rocra for short — because it was first tipped off to the campaign in October, after one of its partners passed Kaspersky a sample of the malware used. Since then, the firm has discovered over 1000 "modules" or components of the malware, with the earliest crafted in 2007 and the most recent component having been built as recently as last week.

"The attackers managed to stay in the game for over five years and evade detection of most antivirus products while continuing to exfiltrate what must be hundreds of terabytes by now," Kaspersky said in its report.

The New York Times