PRESS RELEASE

- EMBARGOED UNTIL MONDAY 14TH JANUARY 2013 AT 13.00 UK TIME -

Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide

Attackers created unique, highly-flexible malware to steal data and geopolitical intelligence from target victims' computer systems, mobile phones and enterprise network equipment

Abingdon, UK, 14 January 2013 - Today Kaspersky Lab published a new research report which identified an elusive cyber-espionage campaign targeting diplomatic, governmental and scientific research organisations in several countries for at least five years. The primary focus of this campaign targets countries in Eastern Europe, former USSR Republics and countries in Central Asia, although victims can be found everywhere, including Western Europe and North America. The main objective of the attackers was to gather sensitive documents from the compromised organisations, which included geopolitical intelligence, credentials to access classified computer systems, and data from personal mobile devices and network equipment.

In October 2012 Kaspersky Lab's team of experts initiated an investigation following a series of attacks against computer networks targeting international diplomatic service agencies. A large scale cyber-espionage network was revealed and analysed during the investigation. According to Kaspersky Lab's analysis report, Operation Red October, called "Rocra" for short, is still active as of January 2013, and has been a sustained campaign dating back as far as 2007.

Main Research Findings

Red October's Advanced Cyber-espionage Network: The attackers have been active since at least 2007 and have been focusing on diplomatic and governmental agencies of

various countries across the world, in addition to research institutions, energy and nuclear groups, and trade and aerospace targets. The Red October attackers designed their own malware, identified as “Rocra,” that has its own unique modular architecture comprised of malicious extensions, info-stealing modules and backdoor Trojans.

The attackers often used information exfiltrated from infected networks as a way to gain entry into additional systems. For example, stolen credentials were compiled in a list and used when the attackers needed to guess passwords or phrases to gain access to additional systems.

To control the network of infected machines, the attackers created more than 60 domain names and several server hosting locations in different countries, with the majority being in Germany and Russia. Kaspersky Lab’s analysis of Rocra’s Command & Control (C2) infrastructure shows that the chain of servers was actually working as proxies in order to hide the location of the ‘mothership’ control server.

Information stolen from infected systems includes documents with extensions: txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa. In particular, the “acid*” extensions appears to refer to the classified software “Acid Cryptofiler”, which is used by several entities, from the European Union to NATO.

Infecting Victims

To infect systems, the attackers sent a targeted spear-phishing email to a victim that included a customised Trojan dropper. In order to install the malware and infect the system the malicious email included exploits that were rigged for security vulnerabilities inside Microsoft Office and Microsoft Excel. The exploits from the documents used in the spear-phishing emails were created by other attackers and employed during different cyber attacks including Tibetan activists as well as military and energy sector targets in Asia. The only thing that was changed in the document used by Rocra was the embedded executable, which the attackers replaced with their own code. Notably, one of the commands in the Trojan dropper changed the default system codepage of the command prompt session to 1251, which is required to render Cyrillic fonts.

Targeted Victims & Organisations

Kaspersky Lab's experts used two methods to analyse the target victims. First, they used detection statistics from the Kaspersky Security Network (KSN), which is the cloud-based security service used by Kaspersky Lab products to report telemetry and deliver advanced threat protection in the forms of blacklists and heuristic rules. KSN had been detecting the exploit code used in the malware as early as 2011, which enabled Kaspersky Lab's experts to search for similar detections related to Rocra. The second method used by Kaspersky Lab's research team was creating a sinkhole server so they could monitor infected machines connecting to Rocra's C2 servers. The data received during the analysis from both methods provided two independent ways of correlating and confirming their findings.

- KSN statistics: Several hundred unique infected systems were detected by the data from KSN, with the focus being on multiple embassies, government networks and organisations, scientific research institutes and consulates. According to KSN's data, the majority of infections that were identified were located primarily in Eastern Europe, but other infections were also identified in North America and countries in Western Europe, as Switzerland and Luxembourg.
- Sinkhole statistics: Kaspersky Lab's sinkhole analysis took place from November 2nd, 2012 – January 10th, 2013. During this time more than 55,000 connections from 250 infected IP addresses were registered in 39 countries. The majority of infected IP connections were coming from Switzerland, followed by Kazakhstan and Greece.

Rocra malware: unique architecture and functionality

The attackers created a multi-functional attack platform that includes several extensions and malicious files designed to quickly adjust to different systems' configurations and harvest intelligence from infected machines. The platform is unique to Rocra and has not been identified by Kaspersky Lab in previous cyber-espionage campaigns. Notable characteristics include:

- "Resurrection" module: A unique module that enables the attackers to "resurrect" infected machines. The module is embedded as a plug-in inside Adobe Reader and Microsoft Office installations and provides the attackers a foolproof way to regain access to a target system if the main malware body is discovered and removed, or if the system is patched. Once the C2s are operational again the attackers send a specialized document file (PDF or Office document) to victims' machines via e-mail which will activate the malware again.

- Advanced cryptographic spy-modules: The main purpose of the spying modules is to steal information. This includes files from different cryptographic systems, such as Acid Cryptofiler, which is known to be used in organisations of NATO, the European Union, European Parliament and European Commission since the summer of 2011 to protect sensitive information.
- Mobile Devices: In addition to targeting traditional workstations, the malware is capable of stealing data from mobile devices, such as smartphones (iPhone, Nokia and Windows Mobile). The malware is also capable of stealing configuration information from enterprise network equipment such as routers and switches, as well as deleted files from removable disk drives.

Attacker identification: Based on the registration data of C2 servers and the numerous artifacts left in executables of the malware, there is strong technical evidence to indicate the attackers have Russian-speaking origins. In addition, the executables used by the attackers were unknown until recently, and were not identified by Kaspersky Lab's experts while analyzing previous cyber-espionage attacks.

Kaspersky Lab, in collaboration with international organisations, law enforcement agencies and Computer Emergency Response Teams (CERTs) is continuing its investigation of Rocra by providing technical expertise and resources for remediation and mitigation procedures.

Kaspersky Lab would like to express their thanks to: US-CERT, the Romanian CERT and the Belarusian CERT for their assistance with the investigation.

The Rocra malware is successfully detected, blocked and remediated by Kaspersky Lab's products, classified as Backdoor.Win32.Sputnik.

Read the full research report of Rocra by Kaspersky Lab's experts please visit Securelist.

-END-

Kaspersky Lab Newsroom

Kaspersky Lab has launched a new online newsroom, Kaspersky Lab Newsroom Europe (http://newsroom.kaspersky.eu/en), for journalists throughout Europe. The newsroom is

specifically designed to serve many of the media's most common requests, making it easier for journalists to find product and corporate information, facts and figures, editorial copy, images, videos and audio files, as well as details about the appropriate PR contacts.

About Kaspersky Lab

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its 15-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for consumers, SMBs and Enterprises. The company currently operates in almost 200 countries across the globe, providing protection for over 300 million users worldwide. Learn more at www.kaspersky.co.uk. For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit: http://www.securelist.com/.

**The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2010. The rating was published in the IDC report Worldwide IT Security Products 2011-2015 Forecast and 2010 Vendor Shares – December 2011. The report ranked software vendors according to earnings from sales of endpoint security solutions in 2010.*

Follow us on Twitter
www.twitter.com/kasperskyuk

Like us on Facebook
http://www.facebook.com/Kaspersky

Editorial contact:
Berkeley PR
Ella Thompson
kasperskylab@berkeleypr.co.uk
Telephone: 0118 909 0909
1650 Arlington Business Park
RG7 4SA, Reading

Kaspersky Lab UK
Ruth Knowles
Ruth.Knowles@kasperskylab.co.uk
Telephone: 0871 789 1633
Milton Business Park
OX14 4RY, Oxford