Cheap, yet dangerous: How threat actors conduct Complicated Attacks at the Lowest Cost

Kaspersky Lab researchers are observing a new and rather important trend in how sophisticated threat actors operate. It is becoming more and more common for threat actors to not use sophisticated and expensive attack techniques, such as zero-day vulnerabilities, but instead utilize extremely targeted social engineering campaigns in combination with known effective malicious techniques. As a result, they are able to leverage malicious campaigns that are extremely difficult to detect with regular corporate grade security solutions.

This shift in how threat actors operate demonstrates that, in general, modern organizations' IT infrastructure contains enough weaknesses to potentially allow attackers with relatively inexpensive attack toolsets to achieve their criminal goals. Microcin, a malicious campaign recently researched by Kaspersky Lab specialists, is an example of such an inexpensive, yet dangerous attack.

It all started when Kaspersky Anti Targeted Attack Platform (KATA) discovered a suspicious RTF-file. The file included an exploit (malware that exploits security weaknesses in widely used software to install additional malicious components) to a known and already patched vulnerability in Microsoft Office. It is not uncommon for regular cybercriminals to use exploits of known vulnerabilities to infect victims with general, massively distributed malware, but as deeper research showed, this particular RTF-file didn't belong to another large infection wave, but to a much more sophisticated and highly targeted campaign.

The suspicious spear-phishing document was distributed through sites for a very specific group of people: forums for discussing issues related to obtaining subsidized housing – an exemption available mostly for employees of government and military organizations in Russia and some neighboring countries.

When the exploit is triggered, malware with a modular structure is installed on the target computer. The module installation is carried out through malicious injection into iexplorer.exe and the auto run of this module is completed through dll-hijacking. Both are known and widely used malicious techniques.

Finally, when the main module is installed, some additional modules are downloaded from the command and control server. At least one of them uses steganography – the practice of concealing information within seemingly non-harmful files, like images, yet another known malicious technique for stealthy data transferring.

Once the whole malicious platform has been deployed, the malware searches for files with extensions like .doc, .ppt, .xls, .docx, .pptx, .xlsx, .pdf, .txt and .rtf., which are then packed in a password-protected archive and transferred to the attack operators. In addition to the usage of known infection and lateral movement techniques, while conducting the operation attackers actively use known backdoors which have been seen in previous attacks and also use legitimate tools created for penetration testing and not generally detected as being malicious by security solutions.

"If taken and analyzed in parts, this attack is nothing serious. Almost any component has been well documented by the security industry, and is relatively easy to spot. However, they are combined in a way that makes the attack tricky to detect. More importantly, this malicious campaign is not one of a kind. It seems that some cyberespionage threat actors shift their focus from developing hard-to-detect malicious tools, to planning and delivering sophisticated operations, which may not involve

complex malware, but still be dangerous”, said Alexey Shulmin, Lead malware analyst at Kaspersky Lab.

In order to protect their IT infrastructure from attacks like Microcin, Kaspersky Lab experts advise organizations to use security tools that allow the detection of malicious operations, rather than malicious software.

Such complex solutions, like Kaspersky Anti-Targeted Attack Platform, include not only endpoint protection technologies, but also technologies that enable the tracking and correlation of events in different parts of the organization’s network, thus identifying the malicious patterns present in sophisticated, targeted attacks.

Kaspersky Lab products successfully detect and block Microcin and similar campaigns.

The details of Microcin campaign can be found at the Securelist blog, which also includes further technical information on the attack.