Corporate News

- Malware
- Business
- Products
- Spam
- Comparative Tests
- Events
- Other

RSS Feeds

Why Kaspersky?

How We Work

Management Team

Security Experts

Events

Webcasts

Press Center

Career Opportunities

Contact Information

Infamous Cyber-Espionage Group Sofacy Resurfaces with New Malicious Tools

04 Dec 2015
Virus News

Kaspersky Lab's Global Research and Analysis Team has spotted new attacks by the Sofacy group which make use of several upgraded techniques designed for aggressive persistency and greater invisibility of malicious activity in the attacked system.

Sofacy (also known as "Fancy Bear", "Sednit", "STRONTIUM" and "APT28") is a russian-speaking advanced threat group that has been active since at least 2008, targeting mostly military and government entities worldwide. Since appearing on the public radar in 2014, the group hasn't stopped its activities. Moreover, Kaspersky Lab experts have discovered new, even more advanced tools in Sofacy's arsenal.

New toolset:

- **Interchangeable:** The attackers use multiple backdoors to infect a target with several different malicious tools, one of which serves as a reinfection tool should another one be blocked or killed by a security solution.
- **Modular**: The attackers use malware modularization, putting some features of the backdoors into separate modules to better hide malicious activity in the attacked system. This is an increasingly popular trend which Kaspersky Lab sees regularly in targeted attacks.
- **Air-gapped:** In many recent (2015) attacks, the Sofacy group made use of a new version of its USB stealing implant, which allows it to copy data from air-gapped computers.

Resilience tactics and data exfiltration tool: how it works

In 2015, in what seemed to be a new wave of attacks, a target organization from the defense industry was hit with a new version of AZZY – a backdoor that is typically used by the Sofacy group to gain a foothold in the attacked machine and to be able to download additional malicious tools. Kaspersky Lab products successfully blocked this malware, and that should have been the end of the story. But what happened next was quite unusual: just one hour after blocking the Trojan, another – newer – version of this backdoor had been compiled by the attackers and downloaded to the target PC. This version evaded regular AV technologies, but was nevertheless detected dynamically by the host intrusion prevention subsystem (HIPS).

This recurring, blindingly-fast Sofacy attack attracted the attention of Kaspersky Lab's experts and they started to investigate further. Very soon they discovered that this new version of a backdoor was downloaded not through a zero-day exploit (which was known to be the usual practice of Sofacy group) but with another implant that was detected after further investigation (and named "msdeltemp.dll" by its authors).

The Trojan, "msdeltemp.dll" is a downloader tool which allows attackers to send commands down to the infected machine and to receive data from it. It can also be used to upload a more sophisticated Trojan into the system. If the secondary backdoor is blocked by an antivirus product, the attackers can still use the msdeltemp.dll Trojan to grab a new version from the C&C and reinstall it on the attacked machine.

This is an example of using multiple backdoors for extreme resilience. The tactic itself is not new and Sofacy has been observed implementing it in the past. However, they previously used droppers to install the two backdoors SPLM and AZZY. If one of them was detected, the other one would provide the attacker with continued access. In the new wave of attacks their tactics changed: they now download a recompiled version of AZZY to replace the blocked one with no need to go through the whole initial infection process.

Separating C&C communications functions from the main backdoor is also a way of decreasing visibility of the main backdoor. As it doesn't directly transmit data outside the attacked computer, it looks less suspicious from a security point of view.

In addition to the change in resilience tactics, Kaspersky Lab's experts have detected several new versions of the Sofacy USB stealer modules, which allow data to be stolen from air-gapped networks. The USBSTEALER module is designed to watch removable drives and collect files from these, depending on a set of rules defined by the attackers. The stolen data is copied into a hidden directory, from where it can be exfiltrated by the attackers using one of the AZZY implants.

The first versions of the new generation USB stealer module date back to February 2015, and appear to be geared exclusively towards high profile targets.

"Usually, when someone publishes research on a given cyber-espionage group, the group reacts: either it halts its activity or dramatically changes tactics and strategy. With Sofacy, this is not always the case. We have seen it launching attacks for several years now and its activity has been reported by the security community multiple times. In 2015 its activity increased significantly, deploying no less than five 0-days, making Sofacy one of the most prolific, agile and dynamic threat actors in the arena. We have reasons to believe that these attacks will continue," - said Costin Raiu, Director of Global Research and Analysis Team at Kaspersky Lab.

Protection strategies

Kaspersky Lab products detect some of the new malware samples used by Sofacy threat actor with the following detection names: Trojan.Win32.Sofacy.al, Trojan.Win32.Sofacy.be, Trojan.Win32.Sofacy.bf, Trojan.Win32.Sofacy.bg, Trojan.Win32.Sofacy.bi, Trojan.Win32.Sofacy.bj, Trojan.Win64.Sofacy.q, Trojan.Win64.Sofacy.s, HEUR:Trojan.Win32.Generic

To protect an organization against sophisticated targeted attacks, including those by Sofacy, Kaspersky Lab recommends using a multi-layered approach that combines:

- Traditional anti-malware technologies,

- Patch management,
- Host intrusion detection,
- Whitelisting and default-deny strategies.

Read more about how Kaspersky Lab products could help protect against Sofacy attacks in our Business blog.

Read our blog post about the Sofacy group at Securelist.com.

More information about the Sofacy group is available to customers of Kaspersky Intelligent Services. Contact: intelreports@kaspersky.com

Learn more about other Russian-speaking espionage campaigns discovered by Kaspersky Lab here.

Read more about what the APT landscape will look like in 2016

Watch how targeted attacks are discovered and investigated: http://www.youtube.com/watch?v=FzPYGRO9LsA