LuckyMouse Group is back and using a legitimate certificate to sign Malware

Monday, 10th September 2018; The Kaspersky Lab Global Research and Analysis Team (GReAT) has discovered several infections from a previously unknown Trojan, which is most likely related to the infamous Chinese-speaking threat actor – LuckyMouse. The most peculiar trait of this malware is its hand-picked driver, signed with a legitimate digital certificate, which has been issued by a company developing information security-related software.

The LuckyMouse group is known for highly targeted cyberattacks on large entities around the world. The group's activity is posing a danger to whole region, including South-Eastern and Central Asia, as their attacks seem to have a political agenda. Judging by victim profiles and the group's previous attack vectors, Kaspersky Lab researchers think that the Trojan they've detected might have been used for nation-state backed cyber-espionage.

The Trojan discovered by Kaspersky Lab experts infected a target computer via a driver built by the threat actors. This allowed the attackers to execute all common tasks such as command execution, downloading and uploading files, and to intercept network traffic.

The driver turned out to be the most interesting part of this campaign. To make it trustworthy, the group apparently stole a digital certificate, which belongs to an information security-related software developer and used this to sign malware samples. This was done in an attempt to avoid being detected by security solutions, as a legitimate signature makes the malware look like legal software. Another noteworthy feature of the driver is that despite Luckymouse's ability to create its own malicious software, the software used in the attack appeared to be a combination of publicly available code samples from the public repositories and custom malware. Such simple adoption of a ready-to-use third-party code, instead of writing original code, saves developers time and makes attribution more difficult.

"When a new LuckyMouse campaign appears, it's almost always around the same time as the leadup to a high-profile political event, and the timing of an attack usually precedes world leader summits. The actor isn't too worried about attribution – because they are now implementing third-party code samples into their programs, it's not time-consuming for them to add another layer to their droppers, or to develop a modification for the malware and still remain untraced," notes Denis Legezo, security researcher at Kaspersky Lab.

Kaspersky Lab has previously reported on the LuckyMouse actor attacking a national data center to organise a country-level waterholing campaign.

How to protect yourself:

- Do not automatically trust the code running on your systems. Digital certificates do not guarantee the absence of backdoors.
- Use a robust security solution, equipped with malicious-behaviour detection technologies that enable even previously unknown threats to be caught.

Subscribe your organisation's security team to a high quality threat intelligence reporting service in order to get early access to information on the most recent developments in the tactics, techniques and procedures of sophisticated threat actors.