# Kaspersky Lab publishes results of internal investigation related to incident with Equation APT source code

New findings point to possible access by multiple third-parties to a computer containing classified data

In early October, a story was published in The Wall Street Journal alleging Kaspersky Lab software was used to download classified data from an NSA employee's home computer. Given that Kaspersky Lab has been at the forefront of fighting cyberespionage and cybercrime for over 20 years, these allegations were treated very seriously by the company. To gather facts and address any concerns, Kaspersky Lab conducted an internal investigation.

The preliminary results of the investigation were published on October 25. These outlined the general findings of the company's search for evidence of the alleged event reported by the media. The new report published today confirms the initial findings and provides additional insight on the analysis of Kaspersky Lab products' telemetry related to the incident. This telemetry describes suspicious activity registered on the computer in question during the timeframe of the incident, which took place in 2014.

Background summary:

- On September 11, 2014, a Kaspersky Lab product installed on the computer of a U.S.-based user reported an infection of what appeared to be variants of malware used by the Equation APT group – a sophisticated cyber threat actor whose activity had already been under active investigation since March 2014.
- Sometime after this, the user seems to have downloaded and installed pirated software on their machine, specifically a Microsoft Office ISO file and an illegal Microsoft Office 2013 activation tool (aka "keygen").
- To install the pirate copy of Office 2013, the user appears to have disabled the Kaspersky Lab product on their computer, because executing the illegal activator tool would not have been possible with the antivirus enabled.
- The illegal activation tool contained within the Office ISO was infected with malware. The user was infected with this malware for an unspecified period while the Kaspersky Lab product was inactive. The malware consisted of a full-blown backdoor which could have allowed other third-parties to access the user's machine.
- When re-enabled, the Kaspersky Lab product detected the malware with the verdict Backdoor.Win32.Mokes.hvl and blocked this malware from calling out to a known command and control server. The first detection of the malicious setup program was on October 4, 2014.
- In addition, the antivirus product also detected new and previously known variants of Equation APT malware.
- One of the files detected by the product as new variants of Equation APT malware was a 7zip archive which was sent back, in accordance to the end-user and KSN license agreements, to the Kaspersky Virus Lab for further analysis.
- Upon analysis, it was discovered that the archive contained a multitude of files, including known and unknown tools of Equation group, source code, as well as classified documents. The analyst

reported the incident to the CEO. Following a request from the CEO, the archive itself, source code, and any apparently classified data were deleted within days from the company’s systems. However, files that are legitimate malware binaries currently remain in Kaspersky Lab storage. The archive was not shared with any third-parties.

- The reason Kaspersky Lab deleted those files and will delete similar ones in the future is two-fold: first, it needs only malware binaries to improve protection and, secondly, it has concerns regarding the handling of potentially classified material.
- Because of this incident, a new policy was created for all malware analysts: they are now required to delete any potentially classified material that has been accidentally collected during anti-malware research.
- The investigation did not reveal any other similar incidents in 2015, 2016 or 2017.
- To date, no other third-party intrusion aside from Duqu 2.0 has been detected in Kaspersky Lab’s networks.

To further support the objectivity of the internal investigation we ran it using multiple analysts including those of non-Russian origin and working outside of Russia to avoid even potential accusations of influence.

Additional findings

One of the major early discoveries of the investigation was that the PC in question was infected with the Mokes backdoor – a malware allowing malicious users remote access to a computer. As part of the investigation, Kaspersky Lab researchers took a deeper look at this backdoor and other non-Equation threat-related telemetry sent from the computer.

- Curious Mokes backdoor background

It is publicly known that the Mokes backdoor (also known as “Smoke Bot” or “Smoke Loader”) appeared on Russian underground forums as it was made available for purchase in 2014. Kaspersky Lab research shows that, during the period of September to November 2014, the command and control servers of this malware were registered to presumably a Chinese entity going by the name “Zhou Lou”. Moreover, deeper analysis of Kaspersky Lab telemetry showed that the Mokes backdoor may not have been the only malware infecting the PC in question at the time of the incident as other illegal activation tools and keygens were detected on the same machine.

- More non-Equation malware

Over a period of two months, the product reported alarms on 121 items of non-Equation malware: backdoors, exploits, Trojans and AdWare. All of these alerts, combined with the limited amount of available telemetry, means that while we can confirm our product spotted the threats, it is impossible to determine if they were executing during the period the product was disabled. Kaspersky Lab continues to research the other malicious samples and further results will be published as soon as the analysis is finished.

Conclusions:

The overall conclusions of the investigation are the following:

- The Kaspersky Lab software performed as expected and notified our analysts of alerts on signatures written to detect Equation APT group malware that was already under investigation for six months. All of this in accordance with the description of the declared product functionality, scenarios, and legal documents which the user agreed to prior to the installation of the software.

- What is believed to be potentially classified information was pulled back because it was contained within an archive that fired on an Equation-specific APT malware signature.

- Beside malware, the archive also contained what appeared to be source code for Equation APT malware and four Word documents bearing classification markings. Kaspersky Lab doesn’t possess information on the content of the documents as they were deleted within days.

• Kaspersky Lab cannot assess whether the data was “handled appropriately” (according to U.S. Government norms) since our analysts have not been trained on handling U.S. classified information, nor are they under any legal obligation to do so. The information was not shared with any third party.

• Contrary to multiple media publications, no evidence has been found that Kaspersky Lab researchers have ever tried to issue “silent” signatures aimed at searching for documents with words like “top secret” and “classified” and other similar words.

• The Mokes backdoor infection and potential infections of other non-Equation malware point to the possibility that user data could have been leaked to an unknown number of third-parties as a result of remote access to the computer.

As a completely transparent company, Kaspersky Lab is ready to provide additional details of the investigation in a responsible manner to relevant parties from government organizations and clients concerned about recent media reports.