TeamSpy – Obshie manevri. Ispolzovat' tolko s razreshenija S-a – CrySyS Blog

Published: 2013-03-20 · Archived: 2026-04-05 14:27:57 UTC

The CrySyS Lab, Budapest has been notified by the Hungarian National Security Authority (www.nbf.hu) about the detection of an ongoing high profile targeted attack affecting our home country, Hungary. During our investigation of the incident, we discovered a number of C&C servers, and a large number of malware samples that have been used in multiple attacks campaigns in the last couple of years. Indeed, the collected evidences suggest that part of the attack toolkit we discovered was used back in 2010. It seems that the main objective of the attackers was information gathering from the infected computers. Many of the victims appear to be ordinary users, but some of the victims are high profile industrial, research, or diplomatic targets, including the case that triggered our investigation. As part of the attackers' activities is based on misusing the TeamViewer remote access tool, we named the entire malicious toolkit TeamSpy.

We detail the findings in our technical report.

As mentioned above, a distinct feature of the attack is the abuse of the legitimate TeamViewer remote access tool. The attackers install an original, legitimate TeamViewer instance on the victim computer, but they modify its behavior with DLL hijacking, and they obtain remote access to the victim computers in real-time. Therefore, the attackers are not only able to remotely observe the infected computers, but they can also misuse TeamViewer to install other tools to obtain important information, files, and other data from the victim.
The collected evidences suggest that attacks have been carried out in multiple campaigns. In addition to the TeamViewer based campaigns, we also saw signs indicating a number of older attacks based on proprietary malware with C&C server based control. We estimate the number of distinct campaigns to be in the order of tens.

The activities of the attackers might be related to other known attack campaigns, like the TeamBot/Sheldor campaign (banking cyber-crime), as we describe later in this document. Despite of this relation to cyber-crime activities, we believe TeamSpy has been used in high-profile targeted attacks too. This is underpinned by the following observations:

• In case of the Hungarian incident, the signs clearly show that the target is high-profile.
• Some malware samples were created just for the retrieval of specific office documents (see the analysis of module 2016_11.txt below) whose name (e.g. "gaza tunnel") indicate that the target is probably high-profile.
• The telemetry revealed additional high-profile victims outside Hungary. Indeed, multiple victims were found in Iran, including victims at http://www.sashiraz.co.ir, which is an electronics company with government background. The possible date of infection for this victim is from 2010.
• Some tools used by the attackers run traceroute to an unknown host on a subnet, where some other hosts belong to the Ministry of Foreign Affairs of Uzbeghistan.
• Some tools used in the attacks look for files matching the following templates *saidumlo secret*.* *секрет*.* *парол*.* *.xls *.pdf *.pgp *pass*.* *.rtf *.doc. This list shows the interest of the attackers in "secret" and "password"

documents. In addition, the attackers' interest in .pgp and .p12 files indicates that they were looking not only for passwords, but also for cryptographic keys, which goes beyond attacks against ordinary users.

During our investigation, we uncovered a large set of malware samples that were probably utilized back in the past; hence, our analysis can also shed light on older malware campaigns and might help victims to reveal incidents that are several years old. Therefore, the information disclosed in this report could be used to perform a longitudinal study of targeted malware attacks.
While identity of most of the victims could not be revealed, we have information on some high-profile victims, e.g.:

- 11/2012: Hungarian high profile governmental victim.
- 03/2013: Embassy of NATO/EU state in Russia
- 04/2010: Electronics company in Middle-East, Govt. background
- 03/2013: Multiple research/educational organizations in France and Belgium
- 03/2013: Industrial manufacturer in Russia

Please read the detailed technical report.
