Researchers Uncover 'TeamSpy' Attack Campaign Against Government, Research Targets

By Dennis Fisher

Published: 2013-03-20 · Archived: 2026-04-05 13:53:01 UTC

Researchers have uncovered a long-term cyber-espionage campaign that used a combination of legitimate software packages and commodity malware tools to target a variety of heavy industry, government intelligence agencies and political activists. Known as the TeamSpy crew because of its affinity for using the legitimate TeamViewer application as part of its toolset, the attackers may have been active for as long as 10 years, researchers say.

Researchers have uncovered a long-term cyber-espionage campaign that used a combination of legitimate software packages and commodity malware tools to target a variety of heavy industry, government intelligence agencies and political activists. Known as the TeamSpy crew because of its affinity for using the legitimate TeamViewer application as part of its toolset, the attackers may have been active for as long as 10 years, researchers say.

The attack appears to be a years-long espionage campaign, but experts who have analyzed the victim profile, malware components and command-and-control infrastructure say that it's not entirely clear what kind of data the attackers are going after. What is clear, though, is that the attackers have been at this for a long time and that they have specific people in mind as targets.

Researchers at the CrySyS Lab in Hungary were alerted by the Hungarian National Security Authority to an attack against a high-profile target in the country and began looking into the campaign. They quickly discovered that some of the infrastructure being used in the attack had been in use for some time and that the target they were investigating was by no means the only one.

"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," Boldizsár Bencsáth, assistant professor at at Budapest University of Technology and Economics and member of the CrySyS Lab said in an analysis.

As they dug into the attack against the Hungarian target, the researchers found that the toolset used included some modules that were designed specifically to retrieve certain kinds of documents. Specifically, the modules would look for files with extensions such as .pgp, or where keywords such as "secret" or the Russian equivalent were found.

By observing the C2 activities of the malware, the CrySyS researchers were able to identify a number of other targets that the attackers were going after, including the embassy of a NATO country inside Russia, a manufacturer in Russia, educational institutions in France and Belgium and a government-connected electronics company in the Middle East.

“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,” CrySyS said.

The TeamSpy crew relies on watering-hole attacks, trying to attract their intended victims to various Web sites that are of interest to the targeted organizations. Researchers say that the attackers have used multiple sites as bait over the years, and have employed several C2 servers as well, including two that were analyzed at “politnews.org” and “bannetwork.org”. After analyzing the malware and toolsets used in the attacks, experts say that there are some similarities between the TeamSpy attackers and the Red October attack campaign discovered earlier this year.

There are a number of indications that the attackers are Russian-speakers, and researchers say that the highest number of targets was found in Russia and Turkey. When victims hit one of the attacker-controlled watering-hole sites, they were greeted with a variety of typical drive-by download infection methods, such as iframe redirections and exploits from the notorious Eleonore exploit pack.

“Over the past years, the attackers added exploit packs like Eleonore on their news aggregation sites. Then, the attackers injected iframes into carefully selected web sites frequently visited by their target victims. The iframes redirect these target visitors (and some extras) to their previously-prepared malicious sites. For instance, redirections from “konflikt.ru” to the attackers’ “bannetwork.org” started in October 2005. In February 2006, users were redirected from “daymohk.org” to “bannetwork.org”, followed by “www.turkmenistan.gov.tm” and “chechentimes.net” in March. The list of infected watering hole sites continued to grow from there,” Kaspersky Lab researchers, who did a separate investigation, said in an analysis.

As part of the infection routine, the attackers install a Russian-localized version of the TeamViewer software package, an application that’s used as a legitimate remote support tool. The installation of this application may help to fool security systems and curious users into thinking that the attack tools are benign. However, the CrySyS team said that the TeamSpy crew appears to have two separate and distinct missions.

“During our investigations, we detected two radically different types of activities of the TeamSpy

attackers. In the actual targeted attack detected by the Hungarian National Security Agency, they used components of the TeamViewer tool combined with other malware modules. In other cases, they used “traditional” self-made malware tools to form a botnet and perform their attacks. For the TeamViewer-based activities, we have traces in the past until September 2012. The forensics material on other malware campaigns suggests that the attackers’ activities may go back as far as 2004,” the lab’s technical analysis says.

In addition to the C2 servers at bannetwork.org and politnews.org, researchers also identified severall others: planetanews.org, newslite.org, bulbanews.org, r2bnetwork.org and kortopla.org. The latter two servers have been sinkholed by Kaspersky Lab.

By looking through the databases on some of the C2 servers the researchers found that they contained not just details of the current TeamSpy attack campaign but also data related to older attacks, suggesting a long-term operation by this same group.

“It seems that the C&C servers are used for longer duration and contain data not just relevant to current attacks, but also historical information. This reveals the incremental work method of the attackers: reuse of code, reuse of servers, and only make incremental changes on the existing material,” CrySyS said.

“The database tables contain information about different attack campaigns and their related log information and statistics. The numbers 5057, 5058, 5016, etc. might be campaign IDs or version (build) numbers. We observed similar numbers in the malware samples we collected from this and other C&C servers. The string “TV” refers to TeamViewer, so these tables probably contain statistics of attacks that used TeamViewer as the command channel between the attackers and the victim.”

Some of the data that the researchers found indicates that older attack campaigns had targeted victims inside the United States, Canada, China, Brazil and many other countries, as well. Many of the malicious modules discovered in the investigation are disguised as text files or JPEGs.

While cyber-espionage campaigns like the TeamSpy attacks have been going on for years now, it’s unusual to find one that has lasted as long as this one. CrySyS researchers said that they believe this same group has been active for as long as 10 years.

“Most likely the same attackers are behind the attacks that span for the last 10 years, as there are clear connections between samples used in different years and campaigns. Interestingly, the attacks began to gain new momentum in the second half of 2012,” they said. “The attackers use distinct tools for nearly every simple activity – this means that most likely the group is small and technically professional people carry out all types of activities, including strategic planning and executing the attacks.”

Source: https://threatpost.com/researchers-uncover-teamspy-attack-campaign-targeting-government-research-targets-032013/77646/