Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:30:45 UTC

APT group: TeamSpy Crew

Names	TeamSpy Crew *(Kaspersky)* SIG39 *(NSA)* Iron Lyric *(SecureWorks)* Team Bear *(CrowdStrike)* Anger Bear *(CrowdStrike)*
Country	Russia
Motivation	Information theft and espionage
First seen	2010
Description	(Kaspersky) 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.
Observed	Sectors: Education, Government, Industrial and Electronics and high-profile targets. Countries: Algeria, Australia, Bangladesh, Belgium, Benin, Bhutan, Brazil, Cameroon, Canada, Central-African Republic, Chad, China, Congo, Costa Rica, Cote d'Ivoire, Croatia, Djibouti, Egypt, France, Gabon, Georgia, Germany, Hungary, India, Indonesia, Iran, Italy, Japan, Kazakhstan, Kenya, Madagascar, Mali,

	Mauritania, Mongolia, Morocco, Nepal, Netherlands, Norway, Peru, Philippines, Portugal, Romania, Russia, Saudi Arabia, Senegal, Slovakia, South Africa, Spain, Sudan, Sweden, Switzerland, Tanzania, Thailand, Tunisia, Turkey, UK, Ukraine, USA, Vietnam.	
Tools used	TeamSpy, TeamViewer and JAVA RATs.	
Operations performed	Feb 2017	A new spam campaign emerged over the weekend, carrying the TeamSpy data-stealing malware, which can give cybercriminals full access to a compromised computer. <https://heimdalsecurity.com/blog/security-alert-teamspy-turn-teamviewer-into-spying-tool/>
Information	<https://www.crysys.hu/publications/files/teamspy.pdf> <https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20134928/theteamspystory_final_t2.pdf>	

Last change to this card: 01 January 2023

Download this actor card in PDF or JSON format
