Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:35:39 UTC

APT group: Safe

Names	Safe *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2013
Description	(Trend Micro) Whether considered advanced persistent threats (APTs) or malware-based espionage attacks, successful and long-term compromises of high-value organizations and enterprises worldwide by a consistent set of campaigns cannot be ignored. Because “noisier” campaigns are becoming increasingly well-known within the security community, new and smaller campaigns are beginning to emerge. This research paper documents the operations of a campaign we refer to as “Safe,” based on the names of the malicious files used. It is an emerging and active targeted threat. While we have yet to determine the campaign’s total number of victims, it appears that nearly 12,000 unique IP addresses spread over more than 100 countries were connected to two sets of command-and-control (C&C) infrastructures related to Safe. We also discovered that the average number of actual victims remained at 71 per day, with few if any changes from day to day. This indicates that the actual number of victims is far less than the number of unique IP addresses. Due to large concentrations of IP addresses within specific network blocks, it is likely that the number of victims is even smaller and that they have dynamically assigned IP addresses, which have been compromised for some time now.
Observed	Sectors: Education, Government, Media, NGOs, Technology. Countries: Algeria, Australia, Brazil, Bulgaria, Canada, China, Egypt, Hungary, India, Malaysia, Mongolia, Pakistan, Philippines, Romania, Russia, Saudi Arabia, Serbia, South Korea, South Sudan, Syria, UAE, USA.
Tools used	DebugView, LZ77, OpenDoc, Safe, TypeConfig, UPXShell, UsbDoc, UsbExe and an MS Office 0-day exploit.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-sight-a-new-apt-campaign/>

	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-safe-a-targeted-threat.pdf>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
