Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:54:54 UTC

APT group: Blackgear

Names	Blackgear *(Trend Micro)* Topgear *(?)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2018	
Description	(Trend Micro) Blackgear is an espionage campaign which has targeted users in Taiwan for many years. Multiple papers and talks have been released covering this campaign, which used the ELIRKS backdoor when it was first discovered in 2012. It is known for using blogs and microblogging services to hide the location of its actual command-and-control (C&C) servers. This allows an attacker to change the C&C server used quickly by changing the information in these posts. Like most campaigns, Blackgear has evolved over time. Our research indicates that it has started targeting Japanese users. Two things led us to this conclusion: first, the fake documents that are used as part of its infection routines are now in Japanese. Secondly, it is now using blogging sites and microblogging services based in Japan for its C&C activity.	
Observed	Countries: Japan, South Korea, Taiwan.	
Tools used	Comnie, Elirks, Protux.	
Operations performed	Jul 2018	Resurfaces, Abuses Social Media for C&C Communication <https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication/>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-espionage-campaign-evolves-adds-japan-target-list/>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format