Gangnam Industrial Style - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:15:51 UTC

APT group: Gangnam Industrial Style

Names	Gangnam Industrial Style *(CyberX)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2019
Description	(CyberX) Section 52, CyberX's threat intelligence team, has uncovered an ongoing industrial cyberespionage campaign targeting hundreds of manufacturing and other industrial firms primarily located in South Korea. The campaign steals passwords and documents which could be used in a number of ways, including stealing trade secrets and intellectual property, performing cyber reconnaissance for future attacks, and compromising industrial control networks for ransomware attacks. For example, the attackers could be stealing proprietary information about industrial equipment designs so they can sell it to competitors and nation-states seeking to advance their competitive posture. Also, credentials can provide attackers with remote RDP access to IoT/ICS networks, while plant schematics help adversaries understand plant layouts in order to facilitate attacks. Design information can also be used by cyberattackers to identify vulnerabilities in industrial control systems.
Observed	Sectors: Engineering, Manufacturing. Countries: China, Ecuador, Germany, Indonesia, Japan, South Korea, Thailand, Turkey, UK.
Tools used	LaZagne, MOVEit Freely, NcFTPPut, Secure FTP Client, Separ, Living off the Land.
Information	<https://cyberx-labs.com/blog/gangnam-industrial-style-apt-campaign-targets-korean-industrial-companies/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
