Operation Red Signature - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:20:42 UTC

APT group: Operation Red Signature

Names	Operation Red Signature *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2018
Description	(Trend Micro) Together with our colleagues at IssueMakersLab, we uncovered Operation Red Signature, an information theft-driven supply chain attack targeting organizations in South Korea. We discovered the attacks around the end of July, while the media reported the attack in South Korea on August 6. The threat actors compromised the update server of a remote support solutions provider to deliver a remote access tool called 9002 RAT to their targets of interest through the update process. They carried this out by first stealing the company's certificate then using it to sign the malware. They also configured the update server to only deliver malicious files if the client is located in the range of IP addresses of their target organizations. 9002 RAT also installed additional malicious tools: an exploit tool for Internet Information Services (IIS) 6 WebDav (exploiting CVE-2017-7269) and an SQL database password dumper. These tools hint at how the attackers are also after data stored in their target's web server and database.
Observed	Countries: South Korea.
Tools used	9002 RAT.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/>

Last change to this card: 29 April 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=b097cbfd-9d8d-4899-9e51-c3d673cdd74d