Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:18:15 UTC

APT group: PassCV

Names	PassCV *(Blue Coat Systems)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2016
Description	(Cylance) Snorre Fagerland of Blue Coat Systems first coined the term PassCV in a blog post. His post provides a good introduction to the group and covers some of the older infrastructure, stolen code-signing certificate reuse, and other connections associated with the PassCV malware. There are several clues alluding to the possibility that multiple groups may be utilizing the same stolen signing certificates, but at this time SPEAR believes the current attacks are more likely being perpetrated by a single group employing multiple publicly available Remote Administration Tools (RATs). The PassCV group has been operating with continued success and has already started to expand their malware repertoire into different off-the-shelf RATs and custom code. SPEAR identified eighteen previously undisclosed stolen Authenticode certificates. These certificates were originally issued to companies and individuals scattered across China, Taiwan, Korea, Europe, the United States and Russia. The PassCV group typically utilized publicly available RATs in addition to some custom code, which ultimately provided backdoor functionality to affected systems via phony resumes and curriculum vitae (CVs). PassCV continues to maintain a heavy reliance on obfuscated and signed versions of older RATs like ZxShell and Ghost RAT, which have remained a favorite of the wider Chinese criminal community since their initial public release.
Observed	Sectors: Online video game companies. Countries: China, Russia, South Korea, Taiwan, USA and Europe.
Tools used	Cobalt Strike, Excalibur, Gh0st RAT, Kitkiot, NetWire RC, Winnti, ZXShell.
Information	<https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
