Threat Group Cards: A Threat Actor Encyclopedia

APT group: UNC215

Names	UNC215 *(FireEye)*
Country	China
Motivation	Information theft and espionage
First seen	2019
Description	(FireEye) In early 2019, Mandiant began identifying and responding to intrusions in the Middle East by Chinese espionage group UNC215. These intrusions exploited the Microsoft SharePoint vulnerability CVE-2019-0604 to install web shells and FOCUSFJORD payloads at targets in the Middle East and Central Asia. There are targeting and high level technique overlaps with between UNC215 and Emissary Panda, APT 27, LuckyMouse, Bronze Union, but we do not have sufficient evidence to say that the same actor is responsible for both sets of activity. APT27 has not been seen since 2015, and UNC215 is targeting many of the regions that APT27 previously focused on; however, we have not seen direct connection or shared tools, so we are only able to assess this link with low confidence.
Observed	Sectors: Education, Government, IT, Telecommunications. Countries: Israel, USA and Middle East, Europe and Asia.
Tools used	AdFind, certutil, China Chopper, HyperBro, Mimikatz, nbtscan, ProcDump, PsExec, SysUpdate, TwoFace, WHEATSCAN, WinRAR.
Information	<https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html>

Last change to this card: 29 December 2022

Download this actor card in PDF or JSON format