APT 20, Violin Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: APT 20, Violin Panda

Names	APT 20 *(FireEye)* APT 8 *(Mandiant)* Violin Panda *(Crowdstrike)* TH3Bug *(Palo Alto)* Crawling Taurus *(Palo Alto)*
Country	China
Motivation	Information theft and espionage
First seen	2014
Description	(Palo Alto) We've uncovered some new data and likely attribution regarding a series of APT watering hole attacks this past summer. Watering hole attacks are an increasingly popular component of APT campaigns, as many people are more aware of spear phishing and are less likely to open documents or click on links in unsolicited emails. Watering hole attacks offer a much better chance of success because they involve compromising legitimate websites and installing malware intended to compromise website visitors. These are often popular websites frequented by people who work in specific industries or have political sympathies to which the actors want to gain access. In contrast to many other APT campaigns, which tend to rely heavily on spear phishing to gain victims, "th3bug" is known for compromising legitimate websites their intended visitors are likely to frequent. Over the summer they compromised several sites, including a well-known Uyghur website written in that native language. This group could be related to Axiom, Group 72.
Observed	Sectors: Aviation, Chemical, Construction, Defense, Energy, Engineering, Financial, Government, Healthcare, High-Tech, Pharmaceutical, Telecommunications, Transportation and Uyghur sympathizers.

	Countries: Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, Thailand, UK, USA and East Asia.	
Tools used	BloodHound, KeeThief, Kerberoast, Mimikatz, PlugX, Poison Ivy, ProcDump, PsExec, SharpHound, SMBExec, WinRAR, XServer, Living off the Land.	
Operations performed	2017	Operation “Wocao” <https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf>
Information	<https://unit42.paloaltonetworks.com/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=crawling-taurus>	

Last change to this card: 10 March 2024

Download this actor card in PDF or JSON format
