Nightshade Panda, APT 9, Group 27

APT group: Nightshade Panda, APT 9, Group 27

Names	Nightshade Panda *(CrowdStrike)* APT 9 *(Mandiant)* Group 27 *(ASERT)* FlowerLady *(Context)* FlowerShow *(Context)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2013	
Description	(Softpedia) Arbor's ASERT team is now reporting that, after looking deeper at that particular campaign, and by exposing a new trail in the group's activities, they managed to identify a new RAT that was undetectable at that time by most antivirus vendors. Named Trochilus, this new RAT was part of Group 27's malware portfolio that included six other malware strains, all served together or in different combinations, based on the data that needed to be stolen from each victim. This collection of malware, dubbed the Seven Pointed Dagger by ASERT experts, included two different PlugX versions, two different Trochilus RAT versions, one version of the 3012 variant of the 9002 RAT, one EvilGrab RAT version, and one unknown piece of malware, which the team has not entirely decloaked just yet.	
Observed	Sectors: Energy, Government, Media, Utilities. Countries: Myanmar, Thailand, USA and Europe.	
Tools used	3102 RAT, 9002 RAT, EvilGrab RAT, MoonWind RAT, PlugX, Poison Ivy, Trochilus RAT.	
Operations performed	May 2015	Operation "Seven Pointed Dagger" During that campaign, the threat actor identified as Group 27 used watering hole attacks on official Myanmar government websites to

		infect unsuspecting users with the PlugX malware (an RAT) when accessing information on the upcoming Myanmar elections. <https://news.softpedia.com/news/trochilus-rat-evades-antivirus-detection-used-for-cyber-espionage-in-south-east-asia-498776.shtml> <https://unit42.paloaltonetworks.com/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/> <http://pages.arbornetworks.com/rs/082-KNA-087/images/ASERT%20Threat%20Intelligence%20Brief%202015-05%20PlugX%20Threat%20Activity%20in%20Myanmar.pdf>
	May 2015	Chinese Actors Use '3102' Malware in Attacks on US Government and EU Media <https://unit42.paloaltonetworks.com/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/>
	Sep 2016	From September 2016 through late November 2016, a threat actor group used both the Trochilus RAT and a newly idenfied RAT we've named MoonWind to target organizations in Thailand, including a utility organization. We chose the name 'MoonWind' based on debugging strings we saw within the samples, as well as the compiler used to generate the samples. The attackers compromised two legitimate Thai websites to host the malware, which is a tactic this group has used in the past. <https://unit42.paloaltonetworks.com/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
