NetTraveler, APT 21, Hammer Panda

APT group: NetTraveler, APT 21, Hammer Panda

Names	NetTraveler *(Kaspersky)* APT 21 *(Mandiant)* Hammer Panda *(CrowdStrike)* TEMP.Zhenbao *(FireEye)*
Country	China
Motivation	Information theft and espionage
First seen	2004
Description	(Kaspersky) Over the last few years, we have been monitoring a cyber-espionage campaign that has successfully compromised more than 350 high profile victims in 40 countries. The main tool used by the threat actors during these attacks is NetTraveler, a malicious program used for covert computer surveillance. The name NetTraveler comes from an internal string which is present in early versions of the malware: NetTraveler Is Running! This malware is used by APT actors for basic surveillance of their victims. Earliest known samples have a timestamp of 2005, although references exist indicating activity as early as 2004. The largest number of samples we observed were created between 2010 and 2013. The later group RedAlpha has infrastructure overlap with NetTraveler.
Observed	Sectors: Defense, Embassies, Government, Oil and gas and Scientific research centers and institutes and Tibetan/Uyghur activists. Countries: Afghanistan, Australia, Austria, Bangladesh, Belarus, Belgium, Cambodia, Canada, Chile, China, Germany, Greece, Hong Kong, India, Indonesia, Iran, Japan, Jordan, Kazakhstan, Kyrgyzstan, Lithuania, Malaysia, Mongolia, Morocco, Nepal, Pakistan, Qatar, Russia, Slovenia, South Korea, Spain, Suriname, Syria, Tajikistan, Thailand, Turkey, Turkmenistan, UK, Ukraine, USA, Uzbekistan.
Tools used	NetTraveler, PlugX.

Operations performed	Aug 2014	NetTraveler Gets a Makeover for 10th Anniversary Most recently, the main focus of interest for cyber-espionage activities revolved around diplomatic (32%), government (19%), private (11%), military (9%), industrial and infrastructure (7%), airspace (6%), research (4%), activism (3%), financial (3%), IT (3%), health (2%) and press (1%). <https://www.kaspersky.com/about/press-releases/2014_nettraveler-gets-a-makeover-for-10th-anniversary>
	Dec 2015	Spear-Phishing Email Targets Diplomat of Uzbekistan Unit 42 recently identified a targeted attack against an individual working for the Foreign Ministry of Uzbekistan in China. A spear-phishing email was sent to a diplomat of the Embassy of Uzbekistan who is likely based in Beijing, China. <https://unit42.paloaltonetworks.com/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/>
Information	<https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-uncovers--operation-nettraveler--a-global-cyberespionage-campaign-targeting-government-affiliated-organizations-and-research-institutes> <https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests>	

Last change to this card: 19 April 2020

Download this actor card in PDF or JSON format
