APT 6 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:43:55 UTC

APT group: APT 6

Names	APT 6 *(FireEye)* 1.php Group *(Zscaler)*
Country	China
Motivation	Information theft and espionage
First seen	2011
Description	(Kaspersky) The FBI issued a rare bulletin admitting that a group named Advanced Persistent Threat 6 (APT6) hacked into US government computer systems as far back as 2011 and for years stole sensitive data. The FBI alert was issued in February and went largely unnoticed. Nearly a month later, security experts are now shining a bright light on the alert and the mysterious group behind the attack. “This is a rare alert and a little late, but one that is welcomed by all security vendors as it offers a chance to mitigate their customers and also collaborate further in what appears to be an ongoing FBI investigation,” said Deepen Desai, director of security research at the security firm Zscaler in an email to Threatpost. Details regarding the actual attack and what government systems were infected are scant. Government officials said they knew the initial attack occurred in 2011, but are unaware of who specifically is behind the attacks. “Given the nature of malware payload involved and the duration of this compromise being unnoticed – the scope of lateral movement inside the compromised network is very high possibly exposing all the critical systems,” Deepen said.
Observed	Sectors: Government. Countries: USA.
Tools used	Poison Ivy.
Information	<https://threatpost.com/fbi-quietly-admits-to-multi-year-apt-attack-sensitive-data-stolen/117267/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
