Subgroup: Pat Bear, APT-C-37 - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Pat Bear, APT-C-37

Names	Pat Bear *(Qihoo 360)* APT-C-37 *(Qihoo 360)* Racquet Bear *(CrowdStrike)*
Country	Syria
Sponsor	Syrian Electronic Army
Motivation	Information theft and espionage
First seen	2015
Description	A subgroup of Syrian Electronic Army (SEA), Deadeye Jackal. (Qihoo 360) Since October 2015, the Pat Bear Organization (APT-C-37) has launched a well-organized, targeted and persistent attack against the “Islamic State”. Watering hole was used to delivery sample in this attack. The malicious samples were mainly disguised as chat software and some common software in specific fields. This Trojan has many functions such as stealing messages, contacts, WhatsApp and Telegram data, and uploading files using FTP. After reversing and correlation, we found that there is a strong correlation between the Pat Bear Organization and the Golden Rat issue, so this attack activity belongs to another branch of the Syrian Electronic Army.
Observed	Sectors: Defense. Countries: Egypt, Israel and “Islamic State”.
Tools used	DroidJack, H-Worm, njRAT, SpyNote RAT, SSLove RAT.
Information	<http://blogs.360.cn/post/SEA_role_influence_cyberattacks.html> <https://cybersecurity.att.com/blogs/labs-research/alien-labs-2019-analysis-of-threat-groups-molerats-and-apt-c-37#When:14:00:00Z>

Last change to this card: 01 January 2023

Download this actor card in PDF or JSON format
