Subgroup: Goldmouse, APT-C-27 - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Goldmouse, APT-C-27

Names	Goldmouse *(Qihoo 360)* Golden Rat *(Qihoo 360)* APT-C-27 *(Qihoo 360)* ATK 80 *(Thales)*
Country	Syria
Sponsor	Syrian Electronic Army
Motivation	Information theft and espionage
First seen	2014
Description	A subgroup of Syrian Electronic Army (SEA), Deadeye Jackal. (Qihoo 360) On March 17, 2019, 360 Threat Intelligence Center captured a target attack sample against the Middle East by exploiting WinRAR vulnerability (CVE-2018-20250), and it seems that the attack is carried out by the Goldmouse APT group (APT-C-27). There is a decoy Word document inside the archive regarding terrorist attacks to lure the victim into decompressing. When the archive gets decompressed on the vulnerable computer, the embedded njRAT backdoor (Telegram Desktop.exe) will be extracted to the startup folder and then triggered into execution if the victim restarts the computer or performs re-login. After that, the attacker is capable to control the compromised device.
Observed	Countries: Syria and Middle East.
Tools used	GoldenRAT, njRAT and a WinRAR exploit.
Information	<https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/> <https://blog.360totalsecurity.com/en/the-sample-analysis-of-apt-c-27s-recent-attack/> <http://blogs.360.cn/post/SEA_role_influence_cyberattacks.html>

Last change to this card: 20 April 2020

Download this actor card in PDF or JSON format
