Subgroup: Greenbug, Volatile Kitten - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Greenbug, Volatile Kitten

Names	Greenbug *(Symantec)* Volatile Kitten *(CrowdStrike)*	
Country	Iran	
Sponsor	State-sponsored, Ministry of Intelligence and Security (MOIS)	
Motivation	Information theft and espionage	
First seen	2016	
Description	A subgroup of OilRig, APT 34, Helix Kitten, Chrysene. (Symantec) Symantec discovered the Greenbug cyberespionage group during its investigation into previous attacks involving W32.Disttrack.B (aka Shamoon). Shamoon (W32.Disttrack) first made headlines in 2012 when it was used in attacks against energy companies in Saudi Arabia. It recently resurfaced in November 2016 (W32.Disttrack.B), again attacking targets in Saudi Arabia. While these attacks were covered extensively in the media, how the attackers stole these credentials and introduced W32.Disttrack on targeted organizations' networks remains a mystery. Could Greenbug be responsible for getting Shamoon those stolen credentials? Although there is no definitive link between Greenbug and Shamoon, the group compromised at least one administrator computer within a Shamoon-targeted organization's network prior to W32.Disttrack.B being deployed on November 17, 2016.	
Observed		
Tools used		
Operations performed	Nov 2016	Greenbug cyberespionage group targeting Middle East, possible links to Shamoon

		<https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon>
	May 2017	Researchers have identified a possible new collaborator in the continued Shamoon attacks against Saudi organizations. Called Greenbug, this group is believed to be instrumental in helping Shamoon steal user credentials of targets ahead of Shamoon's destructive attacks. <https://threatpost.com/shamoon-collaborator-greenbug-adopts-new-communication-tool/125383/>
	Jul 2017	OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group In July 2017, we observed an attack on a Middle Eastern technology organization that was also targeted by the OilRig campaign in August 2016. Initial inspection of this attack suggested this was again the OilRig campaign using their existing toolset, but further examination revealed not only new variants of the delivery document we named Clayslide, but also a different payload embedded inside it. <https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/>
	Oct 2017	Iranian Threat Agent Greenbug has been registering domains similar to those of Israeli High-Tech and Cyber Security Companies. On 15 October 2017 a sample of ISMdoor was submitted to VirusTotal from Iraq. <https://www.clearskysec.com/greenbug/>

Last change to this card: 18 June 2024

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=1839228a-7fb6-4d8b-a7cd-486e728ba9b1