Scully Spider, TA547 - Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: Scully Spider, TA547

Names	Scully Spider *(CrowdStrike)* TA547 *(Proofpoint)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2017
Description	(Proofpoint) TA547 is responsible for many other campaigns since at least November 2017. The other campaigns by the actor were often localized to countries such as Australia, Germany, the United Kingdom, and Italy. Delivered malware included ZLoader (a.k.a. Terdot), Gootkit, Ursnif, Corebot, Panda Banker, Atmos, Mazar Bot, and Red Alert Android malware. It is worth noting that samples of DanaBot found in a public malware repository contained different campaign IDs (the “a=” parameter) than the ones we observed in the wild, suggesting that there may be activity other than that which we observed. Finally, we should mention that DanaBot bears some similarities in its technical implementation and choices of technology to earlier malware, in particular Reveton and CryptXXX [1], which were also written in Delphi and communicated using raw TCP to port 443. These malware strains also featured similarities in the style of C&C traffic. DanaBot has been observed to be distributed by Smoke Loader (operated by Smoky Spider). DanaBot itself has been observed to distribute CoreBot (Boson Spider), GandCrab and Sodinokibi (Pinchy Spider, Gold Southfield) and TrickBot (Wizard Spider, Gold Blackburn).
Observed	Sectors: Financial. Countries: Austria, Australia, Brazil, Canada, Colombia, Germany, Hong Kong, Iraq,

	Italy, New Zealand, Poland, Spain, Switzerland, UK, Ukraine, USA.	
Tools used	DanaBot, LummaC2, NetSupport Manager, Rhadamanthys, Stealc.	
Operations performed	Sep 2018	Recently, we have spotted a surge in activity of DanaBot, a stealthy banking Trojan discovered earlier this year. The malware, first observed in campaigns targeting Australia and later Poland, has apparently expanded further, with campaigns popping up in Italy, Germany, Austria, and as of September 2018, Ukraine. <https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/>
	Nov 2018	DanaBot appears to have outgrown the banking Trojan category. According to our research, its operators have recently been experimenting with cunning email-address-harvesting and spam-sending features, capable of misusing webmail accounts of existing victims for further malware distribution. <https://www.welivesecurity.com/2018/12/06/danabot-evolves-beyond-banking-trojan-new-spam/>
	Jan 2019	The fast-evolving, modular Trojan DanaBot has undergone further changes, with the latest version featuring an entirely new communication protocol. The protocol, introduced to DanaBot at the end of January 2019, adds several layers of encryption to DanaBot's C&C communication. <https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/>
	Apr 2019	DanaBot Demands a Ransom Payment <https://research.checkpoint.com/2019/danabot-demands-a-ransom-payment/>
	Sep 2019	Like most of the other notable banking trojans, DanaBot continues to shift tactics and evolve in order to stay relevant. F5 malware researchers first noticed these shifting tactics in September 2019, however, it is possible they began even earlier. <https://www.f5.com/labs/articles/threat-intelligence/danabot-s-new-tactics-and-targets-arrive-in-time-for-peak-phishi>
	Mar 2024	Security Brief: TA547 Targets German Organizations with Rhadamanthys Stealer <https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer>
Information	<https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0>	

	<https://h3collective.io/review-of-a-danabot-infection/> <https://www.fortinet.com/blog/threat-research/breakdown-of-a-targeted-danabot-attack.html>

Last change to this card: 22 April 2024

Download this actor card in PDF or JSON format
