Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: TA554

Names	TA554 *(Proofpoint)* TH-163 *(Yoroi)*
Country	[Unknown]
Motivation	Financial crime
First seen	2017
Description	(Proofpoint) Since May 2018, Proofpoint researchers have observed email campaigns using a new downloader called sLoad. sLoad is a PowerShell downloader that most frequently delivers Ramnit banker and includes noteworthy reconnaissance features. The malware gathers information about the infected system including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad can also take screenshots and check the DNS cache for specific domains (e.g., targeted banks), as well as load external binaries. While initial versions of sLoad appeared in May 2018, we began tracking the campaigns from this actor (internally named TA554) since at least the beginning of 2017.
Observed	Sectors: Financial. Countries: Canada, Italy, UK.
Tools used	DarkVNC, Godzilla, Gootkit, Gozi ISFB, PsiXBot, Ramnit, sLoad, Snatch, Living off the Land.
Information	<https://www.proofpoint.com/us/threat-insight/post/sload-and-ramnit-pairing-sustained-campaigns-against-uk-and-italy> <https://isc.sans.edu/forums/diary/Malicious+Powershell+Targeting+UK+Bank+Customers/23675/> <https://blog.dynamoo.com/2017/02/highly-personalised-malspam-making.html>

Last change to this card: 29 April 2020

Download this actor card in PDF or JSON format
