Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:08:47 UTC

Tool: Speculoos

Names	Speculoos
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Palo Alto) We identified a total of five samples from our dataset, all of which were approximately the same file size, but contain minute differences amongst the sample set. The subtle differences indicate that they likely originated from the same developer and were either recompiled or patched. As described by FireEye, Speculoos was delivered by exploiting CVE-2019-19781, a vulnerability affecting the Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliances that allowed an adversary to remotely execute arbitrary commands. Based on the spread of industries and regions, in addition to the timing of the vulnerability disclosure, we believe this campaign may have been more opportunistic in nature compared to the highly targeted attack campaigns that are often associated with these types of adversaries. However, considering the exploitation of the vulnerability in conjunction with delivery of a backdoor specifically designed to execute on the associated FreeBSD operating system indicates the adversary was absolutely targeting the affected devices.
Information	<https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/> <https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html> <https://www.secureworks.com/research/threat-profiles/bronze-atlas>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.speculoos>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Speculoos

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0e4ffad1-f5b0-4e3d-af45-c3b017566c1e