Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:34:44 UTC

Tool: MechaFlounder

Names	MechaFlounder
Category	Malware
Type	Backdoor
Description	(Palo Alto) MechaFlounder begins by entering a loop that will continuously attempt to communicate with its C2 server. The Trojan will use HTTP to send an outbound beacon to its C2 server that contains the user's account name and hostname in the URL. The code builds the URL by concatenating the username and hostname with two dashes "–" between the two strings. The code then creates the URL string by using the username and hostname string twice with the back-slash "\" character between the two and by appending the string "-sample.html".
Information	<https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0459/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:MechaFlounder>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool MechaFlounder

Changed	Name	Country	Observed	
APT groups				
	Chafer, APT 39		2014-Sep 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=662241e8-4952-4cfc-8d1f-e96dc38593e5