Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:09:02 UTC

Tool: Octopus

Names	Octopus
Category	Malware
Type	Backdoor
Description	(Kaspersky) The name was originally coined by ESET in 2017 after the 0ct0pus3.php script used by the actor on their old C2 servers. In the case of Octopus, DustSquad used Delphi as their programming language of choice, which is unusual for such an actor. In April 2018 we discovered a new Octopus sample pretending to be Telegram Messenger with a Russian interface. We couldn´t find any legitimate software that this malware appears to be impersonating; in fact, we don´t believe it exists. The Trojan uses third-party Delphi libraries like The Indy Project for JSON-based C2 communications and TurboPower Abbrevia (sourceforge.net/projects/tpabbrevia) for compression. Malware persistence is basic and achieved via the system registry. The server side uses commercial hosting in different countries with .php scripts deployed.
Information	<https://securelist.com/octopus-infested-seas-of-central-asia/88200/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0340/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.octopus>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Octopus

Changed	Name	Country	Observed
APT groups			

	DustSquad, Golden Falcon		2014-2020	
	LazyScripter	[Unknown]	2018	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3d3bf55f-402e-4122-a52b-196aed8e6507