Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:12:30 UTC

APT group: DarkUniverse

Names	DarkUniverse *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2017
Description	(Kaspersky) DarkUniverse is an interesting example of a full cyber-espionage framework used for at least eight years. The malware contains all the necessary modules for collecting all kinds of information about the user and the infected system and appears to be fully developed from scratch. Due to unique code overlaps, we assume with medium confidence that DarkUniverse's creators were connected with the ItaDuke set of activities. The attackers were resourceful and kept updating their malware during the full lifecycle of their operations, so the observed samples from 2017 are totally different from the initial samples from 2009. The suspension of its operations may be related to the publishing of the 'Lost in Translation' leak, or the attackers may simply have decided to switch to more modern approaches and start using more widely available artefacts for their operations.
Observed	Sectors: Defense and civilian. Countries: Afghanistan, Belarus, Ethiopia, Iran, Russia, Sudan, Syria, Tanzania, UAE and others.
Tools used	dfrgntfs5.sqt, glue30.dll, msvcrt58.sqt, updater.mod, zl4vq.sqt.
Information	<https://securelist.com/darkuniverse-the-mysterious-apt-framework-27/94897/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format