Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:31:40 UTC

Tool: updater.mod

Names	updater.mod
Category	Malware
Type	Backdoor, Exfiltration, Downloader
Description	(Kaspersky) This module is implemented as a dynamic-link library with only one exported function, called callme@16. This module is responsible for such tasks as providing communication with the C2 server, providing the malware integrity and persistence mechanism and managing other malware modules. The persistence mechanism is provided by a link file, which is placed by updater.mod into the startup folder, ensuring malware execution after a reboot. If the link file becomes corrupted, the updater.mod module restores it. In this campaign the C2 servers were mostly based on cloud storage at mydrive.ch. For every victim, the operators created a new account there and uploaded additional malware modules and a configuration file with commands to execute it. Once executed, the updater.mod module connected to the C2 and performed the following actions: • downloaded the command file to the working directory; • uploaded files collected and prepared by additional malicious modules (if any) to the C2. These files were located in a directory called ‘queue’ or ‘ntfsrecover’ in the working directory. Files in this directory could have one of two extensions: .d or .upd depending on whether they had already been uploaded to the server or not. • downloaded additional malware modules: o dfrgntfs5.sqt – a module for executing commands from the C2; o msvcrt58.sqt – a module for stealing mail credentials and emails; o zl4vq.sqt – legitimate zlib library used by dfrgntfs5; o %victim_ID%.upe – optional plug-in for dfrgntfs5. Unfortunately, we were unable to obtain this file.
Information	<https://securelist.com/darkuniverse-the-mysterious-apt-framework-27/94897/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool updater.mod

Changed	Name	Country	Observed	
APT groups				
	DarkUniverse	[Unknown]	2017	

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