Cyst Downloader - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:33:32 UTC

Tool: Cyst Downloader

Names	Cyst Downloader
Category	Malware
Type	Downloader
Description	(Proofpoint) In at least in one case we observed an MWI document install a previously unknown malware (SHA256: af17a3b5bf4c78283b2ee338ac6d457b9f3e7b7187c7e9d8651452b78574b3d3). We are calling it the Cyst Downloader. The functionality of this loader is limited. It can create a mutex such as “syst<10 digits>” and communicate with the the C&C server to receive a DLL plugin. The URI path pattern of the C&C beacon contains a folder (random alphanumeric name) followed by a file (random alphanumeric name) with a .jpg, .php, .gif, or .png extension. The downloaded DLL is encrypted with a hardcoded '\x28\xBF\x0A\xBE\x5B\x6E\x70\x03' RC4 key and base64 encoded. The server sends the DLL in HTML comments in a fake 404 response.
Information	<https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Cyst Downloader

Changed	Name	Country	Observed	
APT groups				
	Cobalt Group		2016-Oct 2019	

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