Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:06:09 UTC

Tool: Creamsicle

Names	Creamsicle
Category	Malware
Type	Downloader
Description	(FireEye) CREAMSICLE attempts to download an encoded executable from a specified location. The downloaded file is decoded, written to disk as %APPDATA%\Norton360\Engine\5.1.0.29\ccSvcHst.exe, and padded with 51,200,000 null bytes. CREAMSICLE does not appear to execute the downloaded file, presumably relying on Windows to do so (using the shortcut file in the user's Startup folder) the next time the user logs in.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.creamsicle>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:CREAMSICLE>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Creamsicle

Changed	Name	Country	Observed	
APT groups				
	APT 30, Override Panda		2005	

	Naikon, Lotus Panda		2010-Apr 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ec3678b0-7ffb-4b53-ae26-cfbd54dfc3df