Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:09:14 UTC

Tool: CroxLoader

Names	CroxLoader
Category	Malware
Type	Loader
Description	(Trend Micro) During the deployment of the second campaign, we found two different variants of CroxLoader with respective patterns of use. The first variant is commonly used when attackers use publicly facing applications as the entry point of attack. It decrypts the embedded payload and injects the decrypted payload into the remote process. Meanwhile, the second variant of CroxLoader is often deployed through spearphishing emails to lure victims into opening it. The variant used for each targeted victim depends on the applicable attack scenario.
Information	<https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.croxloader>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool CroxLoader

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Earth Longzhi		2020-Apr 2023	

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