Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:46:35 UTC

Tool: ArtraDownloader

Names	ArtraDownloader Artra Downloader
Category	Malware
Type	Downloader
Description	(Palo Alto) Overall, the ArtraDownloader malware family is not sophisticated, leveraging simple registry keys for persistence and HTTP requests to download and execute a remote file. Important strings within these samples are obfuscated by adding or subtracting from each byte within a string. This same obfuscation routine is used when sending data via HTTP. This downloader has frequently been observed downloading the Remote Access Trojan (RAT) BitterRAT which is associated with BITTER threat operations.
Information	<https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.artra>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ArtraDownloader>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool ArtraDownloader

Changed	Name	Country	Observed	
APT groups				
	Bitter	[South Asia]	2013-Nov 2024	

	Patchwork, Dropping Elephant		2013-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b8d91e49-6460-40aa-9a70-28398600fb95