Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:34:25 UTC

Tool: Emdivi

Names	Emdivi Newsripper
Category	Malware
Type	Backdoor
Description	(Kaspersky) The emdivi family stores important data about itself, including C2, API name, strings for anti-analysis, value of mutexes, as well as the md5 checksum of backdoor commands and the internal proxy information. They are stored in encrypted form, and are decrypted when necessary. Therefore, to analyze an emdivi sample in detail, we need to locate which hex codes are encrypted, and how to decrypt them. In the process of decryption, a unique decryption key is required for each sample.
Information	<https://securelist.com/new-activity-of-the-blue-termite-apt/71876/> <https://blogs.jpcert.or.jp/en/2015/11/emdivi-and-the-rise-of-targeted-attacks-in-japan.html> <http://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/> <http://blog.trendmicro.com/trendlabs-security-intelligence/attackers-target-organizations-in-japan-transform-local-sites-into-cc-servers-for-emdivi-backdoor/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.emdivi>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:emdivi>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Emdivi

Changed	Name	Country	Observed

APT groups

	Blue Termite, Cloudy Omega		2013	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bdd9c8ab-168e-4a3f-a35a-3dd670a9bd02