Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:57:10 UTC

Tool: Enfal

Names	Enfal Lurid
Category	Malware
Type	Downloader
Description	(Trend Micro) The Lurid Downloader, often referred to as Enfal, is a well-known malware family. It is, however, not created with a publicly available toolkit that can be purchased by any aspiring cybercriminal. This malware family has, in the past, been used to target both the U.S. government and nongovernmental organizations (NGOs). However, there appear to be no direct links between this particular network and previous ones.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-exposes-lurid-apt/> <https://www.bsk-consulting.de/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/> <https://researchcenter.paloaltonetworks.com/2015/05/cmstar-downloader-lurid-and-enfals-new-cousin/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0010/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.enfal>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:enfal>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Enfal

Changed	Name	Country	Observed

APT groups

	PittyTiger, Pitty Panda		2011-2014	
	Vicious Panda		2015-Mar 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3f7ba2f1-b299-4601-8965-6ccf900ebdde