Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:19:45 UTC

Tool: IHEATE

Names	IHEATE
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) These attacks targeting users in the United States used a variant of IXESHE which has been seen in Taiwan since 2009 named IHEATE. These showed some differences from known IXESHE variants: they had a different command-and-control (C&C) communication model and encryption methods. One IHEATE sample we found contains the string “EMC112” as part of the C&C traffic. Such strings are frequently used to identify different campaigns. In this particular case, the 112 part of the string matched the malware sample’s compilation date of January 12.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/ixeshe-derivative-iheate-targets-users-america/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:iheate>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool IHEATE

Changed	Name	Country	Observed	
APT groups				
	APT 12, Numbered Panda		2009-Nov 2016	

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