Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:07:06 UTC

Tool: IXESHE

Names	IXESHE
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) The IXESHE malware binary allowed the attackers to easily take over and maintain complete control of victims' systems to do the following: • List all services, processes, and drives • Terminate processes and services • Download and upload files • Start processes and services • Get victims' user names • Get a machine's name and domain name • Download and execute arbitrary files • Cause a system to pause or sleep for a specified number of minutes • Spawn a remote shell • List all current files and directories
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0015/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:IXESHE>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool IXESHE

Changed	Name	Country	Observed

APT groups

	APT 12, Numbered Panda		2009-Nov 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b3f77eac-3137-4786-9b60-748f23797aa3