Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:58:53 UTC

Tool: Geppei

Names	Geppei
Category	Malware
Type	Dropper
Description	(Symantec) The first malicious activity Symantec researchers saw on victim machines was the presence of a previously undocumented dropper (Trojan.Geppei). It uses PyInstaller, which converts Python script to an executable file. Geppei reads commands from a legitimate IIS log. IIS logs are meant to record data from IIS, such as web pages and apps. The attackers can send commands to a compromised web server by disguising them as web access requests. IIS logs them as normal but Trojan.Geppei can read them as commands. The commands read by Geppei contain malicious encoded .ashx files. These files are saved to an arbitrary folder determined by the command parameter and they run as backdoors.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cranefly-new-tools-technique-geppei-danfuan>

Last change to this tool card: 18 November 2022

Download this tool card in JSON format

All groups using tool Geppei

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=46e2b498-934d-47a5-9dab-9d4cdda34c97