Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:47:51 UTC

Tool: FlowerPippi

Names	FlowerPippi
Category	Malware
Type	Reconnaissance, Backdoor, Downloader
Description	(Trend Micro) Some of FlowerPippi's variants were packed by a custom packer —the same one that TA505 uses. The unpacked payload is written in C++ and works as backdoor or downloader malware. FlowerPippi doesn't have an AutoRun function by itself; it is standalone and straightforwardly retrieves the payload. FlowerPippi collects some of the user's information, which it sends to the C&C server. When collecting information, FlowerPippi generates the victim ID from the system's MAC address using the FNV-1a hash algorithm.
Information	<https://documents.trendmicro.com/assets/Tech-Brief-Latest-Spam-Campaigns-from-TA505-Now-Using-New-Malware-Tools-Gelup-and-FlowerPippi.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool FlowerPippi

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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