Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:03:14 UTC

Tool: USBferry

Names	USBferry
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) USBferry has variants that perform different commands depending on specific targets; it can also combine capabilities, improve its stealth in infected environments, and steal critical information through USB storage. Specific functions will be embedded in the trojan downloader to adopt the target environment. Our in-depth analysis found that when Tropic Trooper first penetrates the victim's environment, they will use basic sourcing scripts to collect the host network's topology, connection capability, and volume information. The second function uses USB storage to copy highly classified documents from the physically isolated environment. Moreover, this function copies certain files into the USB %RECYCLER% folder, monitors files' modified time, and updates the newest one to the USB device. The last function will infiltrate the target's internal machine with a customized Windows command and reverse backdoor malware.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments/> <https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0452/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.usbferry>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool USBferry

Changed	Name	Country	Observed	
APT groups				
	Tropic Trooper, Pirate Panda, APT 23, KeyBoy		2011-Jun 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0089ab73-bdcf-4834-ba12-4eb76d2dbd25