Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:15:04 UTC

Tool: Datper

Names	Datper
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(JPCERT/CC) Datper communicates with a C&C server using HTTP protocol and operates based on the received commands. One of the characteristics is that it only communicates within a specific period of time. The malware receives a command as a response to the above HTTP request, and it executes functions based on the commands. Functions that Datper can execute are the following: • Obtain host names, OS versions etc. • Obtain drive information • Configure communication intervals • Sleep for a set period of time • Execute a program • Operate on files (Obtain file lists, download, upload, delete) • Execute shell commands After executing these functions, Datper sends the results to a C&C server.
Information	<https://blogs.jpcert.or.jp/en/2017/08/detecting-datper-malware-from-proxy-logs.html> <http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/> <https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.datper>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Datper>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Datper

Changed	Name	Country	Observed	
APT groups				
	Bronze Butler, Tick, RedBaldNight, Stalker Panda		2006-Apr 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=26cad6ce-54da-4ad1-8f06-24d59dd4603d