Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:48:49 UTC

Tool: DOGCALL

Names	DOGCALL
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(FireEye) DOGCALL is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex. DOGCALL was used to target South Korean Government and military organizations in March and April 2017. The malware is typically dropped using an HWP exploit in a lure document. The wiper tool, RUHAPPY, was found on some of the systems targeted by DOGCALL. While DOGCALL is primarily an espionage tool, RUHAPPY is a destructive wiper tool meant to render systems inoperable.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0213/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:dogcall>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool DOGCALL

Changed	Name	Country	Observed

APT groups

	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=26caccee-f011-40c9-b1a7-e29e763f3d39