Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:48:28 UTC

Tool: Cannon

Names	Cannon
Category	Malware
Type	Backdoor
Description	(Palo Alto) We were able to collect a second delivery document that shared the Joohn author from the crash list(Lion Air Boeing 737).docx document, as well as the 188.241.58[.]170 C2 IP to host its remote template. Structurally this sample was very similar to the initially analyzed document, but the payload turned out to be a completely new tool which we have named Cannon. The tool is written in C# whose malicious code exists in a namespace called cannon, which is the basis of the Trojan's name. The Trojan functions primarily as a downloader that relies on emails to communicate between the Trojan and the C2 server. To communicate with the C2 server, the Trojan will send emails to specific email addresses via SMTPS over TCP port 587. The specific functions of Cannon can be seen in Table 1. This tool also has a heavy reliance on EventHandlers with timers to run its methods in a specific order and potentially increase its evasion capability.
Information	<https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0351/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cannon>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Cannon

Changed	Name	Country	Observed

APT groups

	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1aec48e0-cc52-4706-944d-e04a84c41452