Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:23:54 UTC

Tool: Komplex

Names	Komplex
Category	Malware
Type	Reconnaissance, Banking trojan, Backdoor, Info stealer, Dropper, Downloader
Description	(Palo Alto) The Sofacy group created the Komplex Trojan to use in attack campaigns targeting the OS X operating system – a move that showcases their continued evolution toward multi-platform attacks. The tool is capable of downloading additional files to the system, executing and deleting files, as well as directly interacting with the system shell. While detailed targeting information is not currently available, we believe Komplex has been used in attacks on individuals related to the aerospace industry, as well as attacks leveraging an exploit in MacKeeper to deliver the Trojan. The Komplex Trojan revealed a design similar to Sofacy's JHUHUGIT variant Trojan, which we believe may have been done in order to handle compromised Windows and OS X systems using the same C2 server application with relative ease.
Information	<https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/> <https://blog.malwarebytes.com/threat-analysis/2016/09/komplex-mac-backdoor-answers-old-questions/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0162/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.komplex>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:komplex>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Komplex

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=28ee7912-b778-42e0-a062-f0c08ff18850