Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:40:34 UTC

Tool: Jaff

Names	Jaff Rakhni
Category	Malware
Type	Ransomware
Description	(Fortinet) Like many ransomware variants, Jaff ransomware commonly arrives as a pdf attachment. Once you open the attachment, it displays a one-line document along with a pop-up message asking whether you want to open an embedded. After downloading the binary file, Jaff ransomware starts decrypting part of the malware code. It uses a simple code redirection routine as an anti-analysis trick to stretch the time it requires to analyze the actual malicious code. In between code execution, it uses garbage code that is not relevant to the malware execution.
Information	<https://www.fortinet.com/blog/threat-research/looking-into-jaff-ransomware.html> <http://malware-traffic-analysis.net/2017/05/16/index.html> <https://www.proofpoint.com/us/threat-insight/post/jaff-new-ransomware-from-actors-behind-distribution-of-dridex-locky-bart> <http://blog.talosintelligence.com/2017/05/jaff-ransomware.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.jaff>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:jaff>
Playbook	<https://www.nomoreransom.org/uploads/RakhniDecryptor_how-to_guide.pdf>

Last change to this tool card: 25 April 2021

Download this tool card in JSON format

All groups using tool Jaff

Changed	Name	Country	Observed

APT groups

	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7e7db440-de10-4fa9-89f2-60aba7351ac4