Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:43:09 UTC

Tool: METALJACK

Names	METALJACK denesRAT
Category	Malware
Type	Loader, Reconnaissance, Backdoor
Description	(FireEye) The malware also loads shellcode in an additional resource, which contains the METALJACK payload. The shellcode performs a system survey to collect the victim's computer name and username and then appends those values to a URL string using libjs.inquirerjs[.]com. It then attempts to call out to the URL. If the callout is successful, the malware loads the METALJACK payload into memory.
Information	<https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html> <https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf> <https://ti.qianxin.com/blog/articles/coronavirus-analysis-of-global-outbreak-related-cyber-attacks/> <https://s.tencent.com/research/report/944.html> <https://www.secrss.com/articles/17900> <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf> <https://m.threatbook.cn/detail/2527> <https://www.youtube.com/watch?v=ftjDH65kw6E> <https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-1/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.metaljack>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool METALJACK

Changed	Name	Country	Observed

APT groups

	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9454a6a5-f24f-456a-970b-89182881719f