Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:08:11 UTC

Tool: More_eggs

Names	More_eggs SpicyOmelette Terra Loader SKID
Category	Malware
Type	Backdoor, Downloader
Description	More_eggs is a JavaScript backdoor used by the Cobalt group. It attempts to connect to its C&C server and retrieve tasks to carry out, some of which are: - d&exec = download and execute PE file - gtfo = delete files/startup entries and terminate - more_eggs = download additional/new scripts - more_onion = run new script and terminate current script - more_power = run command shell commands
Information	<https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/> <https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/> <https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/> <https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish> <https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/> <https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html> <https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers> <https://asert.arbornetworks.com/double-the-infection-double-the-fun/> <https://quointelligence.eu/2018/11/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using/> <https://www.esentire.com/blog/hackers-spearphish-corporate-hiring-managers-with-poisoned-resumes-infecting-them-with-the-more-eggs-malware> <https://www.esentire.com/blog/more-eggs-activity-persists-via-fake-job-applicant-

	lures> <https://denwp.com/more-eggs-venom-spider-phishing-campaign/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0284/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.more_eggs>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:More_eggs>

Last change to this tool card: 27 June 2025

Download this tool card in JSON format

All groups using tool More_eggs

Changed	Name	Country	Observed	
APT groups				
	Cobalt Group		2016-Oct 2019	
	Evilnum	[Unknown]	2018-2022	
	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021	
	Venom Spider, Golden Chickens		2017-Jan 2025	

4 groups listed (4 APT, 0 other, 0 unknown)

↑