Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:24:31 UTC

Tool: Evilnum

Names	Evilnum EVILNUM Marvel
Category	Malware
Type	Loader, Backdoor
Description	(ESET) This component communicates with a C&C server and acts as a backdoor without the need for any additional program. However, in most attacks that we have seen, the attackers deployed additional components as they saw fit and used the JS malware only as a first stage. The first known mention of this JavaScript malware was in May 2018 in this pwncode article.
Information	<https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/> <http://www.pwncode.io/2018/05/javascript-based-bot-using-github-c.html> <https://blog.prevailion.com/2020/05/phantom-in-command-shell5.html> <https://securelist.com/deathstalker-mercenary-triumvirate/98177/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0568/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.evilnum> <https://malpedia.caad.fkie.fraunhofer.de/details/win.evilnum>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:evilnum>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Evilnum

Changed	Name	Country	Observed

APT groups

	Deceptikons, DeathStalker	[Unknown]	2012-Jun 2020	
	Evilnum	[Unknown]	2018-2022	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=57ac4c19-94d8-4e6e-9240-f10c0e2e3940