Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:40:59 UTC

Tool: TwoFace

Names	TwoFace Minion HighShell HyperShell SEASHARPEE
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	According to Unit42, TwoFace is a two-staged (loader+payload) webshell, written in C# and meant to run on webservers with ASP.NET. The author of the initial loader webshell included legitimate and expected content that will be displayed if a visitor accesses the shell in a browser, likely to remain undetected. The code in the loader webshell includes obfuscated variable names and the embedded payload is encoded and encrypted. To interact with the loader webshell, the threat actor uses HTTP POST requests to the compromised server. The secondary webshell, which we call the payload, is embedded within the loader in encrypted form and contains additional functionality that we will discuss in further detail. When the threat actor wants to interact with the remote server, they provide data that the loader will use to modify a decryption key embedded within the loader that will be in turn used to decrypt the embedded TwoFace payload. Commands supported by the payload are execution of programs, up-, download and deletion of files and capability to manipulate MAC timestamps.
Information	<https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/> <https://unit42.paloaltonetworks.com/unit42-oilrig-performs-tests-twoface-webshell/> <https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0185/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/asp.twoface>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool TwoFace

Changed	Name	Country	Observed	
APT groups				
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	
	UNC215		2019	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f02989df-45bc-4162-ba5b-8617795ee749