Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:41:44 UTC

Tool: BIOLOAD

Names	BIOLOAD
Category	Malware
Type	Loader
Description	(Fortinet) The loader file name is WinBio.dll (note the uppercase characters) and is placed by the attacker alongside the executable in the same folder ('WinBioPlugIns'), thus leveraging the default DLL search order. Because the file path is under %WINDIR%, it means that in order to plant it the attacker needed to have elevated privileges on the victim's machine such as administrator or a SYSTEM account. Like Boostwrite, this loader was also developed in C++. It exports only a single function which is the one FaceFodUninstaller.exe imports.
Information	<https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bioload>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BIOLOAD>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool BIOLOAD

Changed	Name	Country	Observed	
APT groups				
	FIN7		2013-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fa66fc13-61f7-44c0-869d-8c5f8509b1bb