Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:56:47 UTC

Tool: SocksBot

Names	SocksBot BIRDDOG Nadrac
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration, Downloader, Loader
Description	(Accenture) The SOCKSBOT implant has the following capabilities: • Enumerate processes (process list) • Take screenshots • Download, upload, write, and execute files • Create and inject into new processes • Communicate to C2 via sockets. This implant will communicate with the designated C2 server by first creating a buffer and will, on first execution, communicate to the C2 server that it has successfully infected a target by using a .php URI that is pseudo-randomly generated. SOCKSBOT uses the ObtainUserAgentString API to determine the default user-agent of the machine.
Information	<https://www.accenture.com/_acnmedia/pdf-83/accenture-goldfin-security-alert.pdf> <https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html> <https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0273/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.socksbot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:socksbot>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool SocksBot

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	Patchwork, Dropping Elephant		2013-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=43ced180-196d-4510-95cf-a4f7d9f05d2a