Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:49:13 UTC

Tool: Bankshot

Names	Bankshot COPPERHEDGE Trojan Manuscript FoggyBrass
Category	Malware
Type	Backdoor, Tunneling
Description	(US-CERT) This report provides analysis of seven (7) malicious executable files. Five (5) of these files are proxy applications that all use a similar cipher algorithm to mask traffic between the malware and the remote operator. Additionally, two of the five proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors. The remaining two (2) executables are remote access tools (RATs), providing remote users with the ability to run various commands on an infected system. One of these RATs uses a cipher and the OpenSSL library to add a layer of encryption to communications between the infected system and its command and control (C2) server; this RAT may have been used to install the proxy servers onto compromised systems.
Information	<https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF> <https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/> <https://www.us-cert.gov/ncas/analysis-reports/ar20-133a>
MITRE ATT&CK	<https://attack.mitre.org/software/S0239/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bankshot>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool Bankshot

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=92386fd7-132d-4a22-a582-1d4460daa5e5