Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:14:38 UTC

Tool: KRBanker

Names	KRBanker Blackmoon
Category	Malware
Type	Banking trojan
Description	(Proofpoint) First analyzed in early 2014, the Blackmoon banking Trojan targets a user's online banking credentials using a type of pharming that involves modifying or replacing the local Hosts file with one that redirects online banking domain lookups to an IP address controlled by the attacker. Blackmoon has been observed targeting primarily customers of South Korean online banking sites and services, and is usually distributed via drive-by download.
Information	<https://www.proofpoint.com/us/threat-insight/post/Updated-Blackmoon-Banking-Trojan> <https://unit42.paloaltonetworks.com/unit42-krbanker-targets-south-korea-through-adware-and-exploit-kits-2/> <https://www.peppermalware.com/2019/03/analysis-of-blackmoon-banking-trojans.html> <http://training.nshc.net/ENG/Document/virus/20140305_Internet_Bank_Pharming_-_BlackMoon_Ver_1.0_External_ENG.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.krbanker>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:krbanker>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool KRBanker

Changed	Name	Country	Observed

Unknown groups

	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fc359147-48b8-4b01-b018-bc3a0b7f4727