Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:04:22 UTC

Tool: MirageFox

Names	MirageFox
Category	Malware
Type	Backdoor, Info stealer
Description	MirageFox is a remote access tool used against Windows systems. It appears to be an upgraded version of a tool known as Mirage, which is a RAT believed to originate in 2012. (SecureWorks) Mirage phones home to its C2 servers using a standard HTTP request. From the activity CTU researchers have observed when executing Mirage in a malware sandbox, this communication commonly occurs over ports 80, 443 and 8080, and it can implement SSL for added security.
Information	<https://www.secureworks.com/research/the-mirage-campaign> <https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0280/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.miragefox>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:MirageFox>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool MirageFox

Changed	Name	Country	Observed
APT groups			

	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=850be0f0-e2cf-4c68-a739-6691ec513e99