Elirks (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:32:27 UTC

Elirks is a basic backdoor Trojan, first discovered in 2010, that is primarily used to steal information from compromised systems. Mostly attacks using Elirks occurring in East Asia. One of the unique features of the malware is that it retrieves its C2 address by accessing a pre-determined microblog service or SNS. Attackers create accounts on those services and post encoded IP addresses or the domain names of real C2 servers in advance of distributing the backdoor. Multiple Elirks variants using Japanese blog services for the last couple of years.

▶ [TLP:WHITE] win_elirks_auto (20251219 | Detects win.elirks.)
