Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:54:49 UTC

Tool: Elirks

Names	Elirks
Category	Malware
Type	Backdoor, Info stealer
Description	(Palo Alto) Elirks, less widely known than PlugX, is a basic backdoor Trojan, first discovered in 2010, that is primarily used to steal information from compromised systems. We mostly observe 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. We have seen multiple Elirks variants using Japanese blog services for the last couple of years.
Information	<https://unit42.paloaltonetworks.com/unit42-tracking-elirks-variants-in-japan-similarities-to-previous-attacks/> <https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.elirks>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:elirks>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Elirks

Changed	Name	Country	Observed	
APT groups				
	Blackgear		2018-Jul 2018	

	Bronze Butler, Tick, RedBaldNight, Stalker Panda		2006-Apr 2021	
	Scarlet Mimic		2015-Aug 2022	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=51e51b03-0133-427f-8465-bceeefc52ee9