Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:37:42 UTC

Tool: ELECTRICFISH

Names	ELECTRICFISH Alreay
Category	Malware
Type	Tunneling
Description	(US-CERT) This report provides analysis of two malicious 32-bit Windows executable file. The malware implements a custom protocol that allows traffic to be tunneled between a source and a destination Internet Protocol (IP) address. The malware continuously attempts to reach out to the source and the designation system, which allows either side to initiate a tunneling session. The malware can be configured with a proxy server/port and proxy username and password. This feature allows connectivity to a system sitting inside of a proxy server, which allows the actor to bypass the compromised system's required authentication to reach outside of the network.
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar19-252b> <https://securelist.com/blog/sas/77908/lazarus-under-the-hood/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.electricfish> <https://malpedia.caad.fkie.fraunhofer.de/details/win.alreay>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ElectricFish>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool ELECTRICFISH

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=0b56379e-b63d-4c34-824f-93e096ee8316