Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:54:11 UTC

Tool: Plink

Names	Plink PuTTY Link
Category	Tools
Type	Tunneling
Description	(FireEye) A common utility used to tunnel RDP sessions is PuTTY Link, commonly known as Plink. Plink can be used to establish secure shell (SSH) network connections to other systems using arbitrary source and destination ports. Since many IT environments either do not perform protocol inspection or do not block SSH communications outbound from their network, attackers such as FIN8 have used Plink to create encrypted tunnels that allow RDP ports on infected systems to communicate back to the attacker command and control (C2) server.
Information	<https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:plink>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Plink

Changed	Name	Country	Observed	
APT groups				
	Chafer, APT 39		2014-Sep 2020	
	Gallium		2018-Jun 2022	

	HomeLand Justice		2022-Jan 2024	
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	
	Parisite, Fox Kitten, Pioneer Kitten		2017-Nov 2020	

6 groups listed (6 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=598b6f11-cd88-4ce8-8179-ad644c424419