Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:52:53 UTC

Tool: Regin

Names	Regin Prax WarriorPride
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Tunneling
Description	Regin is a sophisticated malware and hacking toolkit attributed to United States' National Security Agency (NSA) for government spying operations. It was first publicly revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. Regin malware targeted victims in a range of industries, telecom, government, and financial institutions. It was engineered to be modular and over time dozens of modules have been found and attributed to this family. Symantec observed around 100 infections in 10 different countries across a variety of organisations including private companies, government entities, and research institutes.
Information	<https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/> <https://en.wikipedia.org/wiki/Regin_(malware)>
MITRE ATT&CK	<https://attack.mitre.org/software/S0019/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.regin>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Regin

Changed	Name	Country	Observed
APT groups			

	Equation Group		2001-Aug 2016	
	GCHQ		1919-2010	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ccaa85ad-0371-471b-9369-9d6d0c0f1bc6