Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:45:16 UTC

Tool: POORAIM

Names	POORAIM Backdoor.APT.POORAIM
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(FireEye) POORAIM malware is designed with basic backdoor functionality and leverages AOL Instant Messenger for command and control communications. POORAIM includes the following capabilities: System information enumeration, File browsing, manipulation and exfiltration, Process enumeration, Screen capture, File execution, Exfiltration of browser favorites, and battery status. Exfiltrated data is sent via files over AIM. POORAIM has been involved in campaigns against South Korean media organizations and sites relating to North Korean refugees and defectors since early 2014. Compromised sites have acted as watering holes to deliver newer variants of POORAIM.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0216/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool POORAIM

Changed	Name	Country	Observed
APT groups			

	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3e017ae6-9f5a-4c0b-8720-e567567c51e3