Brave Prince - Threat Group Cards: A Threat Actor Encyclopedia

Tool: Brave Prince

Names	Brave Prince
Category	Malware
Type	Reconnaissance, Backdoor
Description	(McAfee) Brave Prince is a Korean-language implant that contains similar code and behavior to the Gold Dragon variants, specifically the system profiling and control server communication mechanism. The malware gathers detailed logs about the victim's configuration, contents of the hard drive, registry, scheduled tasks, running processes, and more. Brave Prince was first observed in the wild December 13, 2017, sending logs to the attacker via South Korea's Daum email service. Later variants posted the data to a web server via an HTTP post command, in the same way that Gold Dragon does.
Information	<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0252/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool Brave Prince

Changed	Name	Country	Observed	
APT groups				
	Hades		2017-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=013caf25-e9ef-4511-8111-db7cdb7978c1