RCS Galileo - Threat Group Cards: A Threat Actor Encyclopedia

Tool: RCS Galileo

Names	RCS Galileo
Category	Malware
Type	Backdoor, Info stealer
Description	(F-Secure) In all known malicious attachments, the final payload was a variant of the “Scout” tool from the HackingTeam Remote Control System (RCS) Galileo hacking platform. HackingTeam is an Italian software company that created RCS, which they describe as “the hacking suite for governmental interception”. In July 2015, news emerged that HackingTeam had been breached. One of the consequences of this incident was the then latest version of RCS Galileo being leaked to the public. As a result of the leak, both the source code and the ready-made installers for the RCS platform were made available for anyone to use. Based on our analysis of Callisto Group’s usage of RCS Galileo, we believe the Callisto Group did not utilize the leaked RCS Galileo source code, but rather used the leaked ready-made installers to set up their own installation of the RCS Galileo platform. The process for using the leaked installers to set up an RCS Galileo installation has been described online in publicly available blogposts, making the process trivial to achieve.
Information	<https://www.f-secure.com/documents/996508/1030745/callisto-group>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool RCS Galileo

Changed	Name	Country	Observed	
APT groups				
	Callisto Group	[Unknown]	2013	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5a23a112-d52e-4a02-83b1-ffb2fd8ddc3e