Hacking Team - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:10:13 UTC

DescriptionThe many 0-days that had been collected by Hacking Team and which became publicly available during the breach of their organization in 2015, have been used by several APT groups since.

(ESET) Since being founded in 2003, the Italian spyware vendor Hacking Team gained notoriety for selling surveillance tools to governments and their agencies across the world.

The capabilities of its flagship product, the Remote Control System (RCS), include extracting files from a targeted device, intercepting emails and instant messaging, as well as remotely activating a device's webcam and microphone. The company has been criticized for selling these capabilities to authoritarian governments – an allegation it has consistently denied.

When the tables turned in July 2015, with Hacking Team itself suffering a damaging hack, the reported use of RCS by oppressive regimes was confirmed. With 400GB of internal data – including the once-secret list of customers, internal communications, and spyware source code – leaked online, Hacking Team was forced to request its customers to suspend all use of RCS, and was left facing an uncertain future.

Following the hack, the security community has been keeping a close eye on the company's efforts to get back on its feet. The first reports suggesting Hacking Team's resumed operations came six months later – a new sample of Hacking Team's Mac spyware was apparently in the wild. A year after the breach, an investment by a company named Tablem Limited brought changes to Hacking Team's shareholder structure, with Tablem Limited taking 20% of Hacking Team's shareholding. Tablem Limited is officially based in Cyprus; however, recent news suggests it has ties to Saudi Arabia.
