Infy, Prince of Persia - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:18:58 UTC

APT group: Infy, Prince of Persia

Names	Infy *(Palo Alto)* Prince of Persia *(Palo Alto)* Operation Mermaid *(Qihoo 360)* APT-C-07 *(Qihoo 360)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2007
Description	Since early 2013, we have observed activity from a unique threat actor group, which we began to investigate based on increased activities against human right activists in the beginning of 2015. In line5with other research on the campaign, released prior to publication of this document, we have adopted the name “Infy”, which is based on labels used in the infrastructure and its two families of malware agents. Thanks to information we have been able to collect during the course of our research, such as characteristics of the group’s malware and development cycle, our research strongly supports the claim that the Infy group is of Iranian origin and potentially connected to the Iranian state. Amongst a backdrop of other incidents, Infy became one of the most frequently observed agents for attempted malware attacks against Iranian civil society beginning in late 2014, growing in use up to the February 2016 parliamentary election in Iran. After the conclusion of the parliamentary election, the rate of attempted intrusions and new compromises through the Infy agent slowed, but did not end. The trends witnessed in reports from recipients are reinforced through telemetry provided by design failures in more recent versions of the Infy malware.
Observed	Sectors: Government and private sectors. Countries: Azerbaijan, Bahrain, Canada, China, Denmark, France, Germany, India,

	Iran, Iraq, Israel, Italy, Romania, Netherlands, Russia, Saudi Arabia, Sweden, Syria, Turkey, UK, USA.	
Tools used	Infy, Tonnerre.	
Operations performed	May 2015	In May 2015, Palo Alto Networks WildFire detected two e-mails carrying malicious documents from a genuine and compromised Israeli Gmail account, sent to an Israeli industrial organization. One e-mail carried a Microsoft PowerPoint file named “thanks.pps”, the other a Microsoft Word document named “request.docx”. <https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/>
	Feb 2017	In February 2017, we observed an evolution of the “Infy” malware that we’re calling “Foudre” (“lightning”, in French). The actors appear to have learned from our previous takedown and sinkholing of their Command and Control (C2) infrastructure – Foudre incorporates new anti-takeover techniques in an attempt to avoid their C2 domains being sinkholed as we did in 2016. <https://unit42.paloaltonetworks.com/unit42-prince-persia-ride-lightning-infy-returns-foudre/>
Counter operations	Jun 2016	Prince of Persia – Game Over <https://unit42.paloaltonetworks.com/unit42-prince-of-persia-game-over/>
Information	<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>	

Last change to this card: 19 April 2021

Download this actor card in PDF or JSON format
