Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:10:44 UTC

Tool: Infy

Names	Infy Foudre
Category	Malware
Type	Reconnaissance
Description	(Palo Alto) The malware connects to the C2 every five minutes using HTTP, posting: <computer name> <user name> dn = n1 ver = 30 lfolder= f cpuid= machineguid (from hklm\SOFTWARE\Microsoft\Cryptography\machineguid) tt= time
Information	<https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/> <https://www.intezer.com/prince-of-persia-the-sands-of-foudre/> <https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/> <https://github.com/pan-unit42/iocs/blob/master/prince_of_persia/hashes.csv>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.infy>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:infy>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Infy

Changed	Name	Country	Observed	
APT groups				
	Infy, Prince of Persia		2007-Feb 2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cfe90b10-0ec9-47d0-9774-a163fd3b7321