Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:13:50 UTC

Tool: OddJob

Names	OddJob
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer
Description	(IBM) OddJob's most obvious characteristic is that it is designed to intercept user communications through the browser to steal or inject information and terminate user sessions inside Internet Explorer and Firefox. We have extracted OddJob's configuration data and concluded that it is capable of performing different actions on targeted websites, depending on its configuration. The code is capable of logging GET and POST requests, grabbing full pages, terminating connections and injecting data into Web pages. All logged requests and grabbed pages are sent to the C&C server in real time, allowing fraudsters to perform session hijacks — also in real time but hidden from the legitimate user of the online bank account. By tapping the session ID token, which banks use to identify a user's online banking session, the fraudsters can electronically impersonate the legitimate user and complete a range of banking operations.
Information	<https://securityintelligence.com/oddjob-new-financial-trojan-keeps-online-banking-sessions-open-after-users-logout/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.oddjob>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool OddJob

Changed	Name	Country	Observed
APT groups			

	Equation Group		2001-Aug 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e86e1ae5-b560-4be2-bdf5-a5ee26ebcaa9