

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:10:54 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Corkow

Tool: Corkow

Names	Corkow
Category	Malware
Type	Banking trojan
Description	<p>(ESET) The malware, which has been in the wild since at least 2011, has demonstrated continuous activity in the past year, infecting thousands of users. Version numbering of the various Trojan modules is another indicator that the malware authors are continually developing the trojan.</p> <p>The most common infection vector – drive-by downloads – has been used to spread the malware.</p> <p>This Russian tool for committing bank fraud shares many characteristics with other malware families with a similar purpose, such as Zeus (also known as Zbot), JHUHUGIT, HesperBot, or Qadars, for example, but also contains some unique functionality.</p> <p>Several features, like enumeration of smart cards, targeting of dedicated banking applications mostly used by corporate customers and looking for user activity regarding online banking sites and applications, electronic trading platform sites and applications and so forth, all suggest that the attackers are focusing their sights on financial professionals and enterprises, whose bank accounts usually hold a higher balance than those of most individuals.</p>
Information	<https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/>

Last change to this tool card: 22 April 2020

Download this tool card in [JSON](#) format

All groups using tool Corkow

Changed	Name	Country	Observed
---------	------	---------	----------

APT groups

	Corkow, Metel		2011	
--	-------------------------------	---	------	--

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

Source: <https://apt.eta.da.or.th/cgi-bin/listgroups.cgi?u=2fb7e563-76f5-4ba4-a9e8-51f509dc804c>