

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:03:48 UTC

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



Tool: Cridex

Names	Cridex Bugat Feodo
Category	Malware
Type	Banking trojan , Credential stealer , Worm
Description	(Kaspersky) Dridex made its first appearance as an independent malicious program (under the name “Cridex”) around September 2011. An analysis of a Cridex sample (MD5: 78cc821b5acfc017c855bc7060479f84) demonstrated that, even in its early days, the malware could receive dynamic configuration files, use web injections to steal money, and was able to infect USB media. This ability influenced the name under which the “zero” version of Cridex was detected — Worm.Win32.Cridex.
Information	< https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/ > < http://www.sempersecurus.org/2012/08/cridex-analysis-using-volatility.html >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.feodo >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:cridex >

Last change to this tool card: 24 May 2020

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

All groups using tool Cridex

Changed	Name	Country	Observed	
APT groups				
	Indrik Spider		2007-Oct 2024	

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=a4d512bf-990c-4bb4-93bc-6cca12d429f9>