Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:00:44 UTC

Tool: Janicab

Names	Janicab
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(F-Secure) For Windows OS, this malware was delivered via a document that exploited CVE-2012-0158. In addition, we've also seen it delivered in a form of a Microsoft Shell Link (.lnk) file that drops an embedded encoded VBScript, sometime from 2013 until recently. There are several tricks the dropper uses for obfuscating its purpose: - Filename with double extension (Example: .jpg.lnk or .doc.lnk) - Using the icon of notepad.exe (instead of the default, cmd.exe) - Possibly sensitive data zeroed out, for example, machine identifier and relative path But the most interesting part is the use of an undocumented method for hiding the command line argument string from Windows explorer. Typically, the target and its arguments are visible in Windows explorer as a single string in the shortcut properties, when the user right-clicks on the shortcut icon. However, the command line argument is not visible in this scenario.
Information	<https://archive.f-secure.com/weblog/archives/00002803.html> <https://archive.f-secure.com/weblog/archives/00002576.html> <https://securelist.com/deathstalker-mercenary-triumvirate/98177/> <https://www.macmark.de/blog/osx_blog_2013-08-a.php> <https://sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0163/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.janicab>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Janicab

Changed	Name	Country	Observed	
APT groups				
	Deceptikons, DeathStalker	[Unknown]	2012-Jun 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=44b545b8-3815-40f9-8e4d-e6e49aec793d