Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:47:41 UTC

Tool: Asruex

Names	Asruex
Category	Malware
Type	Backdoor, Worm
Description	(Trend Micro) Since it first emerged in 2015, Asruex has been known for its backdoor capabilities and connection to the spyware DarkHotel. However, when we encountered Asruex in a PDF file, we found that a variant of the malware can also act as an infector particularly through the use of old vulnerabilities CVE-2012-0158 and CVE-2010-2883, which inject code in Word and PDF files respectively. The use of old, patched vulnerabilities could hint that the variant was devised knowing that it can affect targets who have been using older versions of Adobe Reader (versions 9.x up to before 9.4) and Acrobat (versions 8.x up to before 8.2.5) on Windows and Mac OS X.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.asruex>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Asruex>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Asruex

Changed	Name	Country	Observed
APT groups			

	DarkHotel		2007-2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=39c65a96-a0e8-42fa-80d5-5d36c0be61c3