

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:07:36 UTC

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

Tool: THREEBYTE

Names	THREEBYTE
Category	Malware
Type	Reconnaissance , Backdoor
Description	(Check Point) Threebyte is a Backdoor that targets the Windows platform. This malware contacts a remote server to receive commands to execute on the infected system. It sends out information about the targeted system. Furthermore, it has been reportedly delivered to a victim's machine via exploitation of a Microsoft Word Document vulnerability (CVE-2012-0158). In order to survive system reboots, it adds a value to the Run key in the Registry.
Information	< https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=malwarefamily&threatId=2098 > < https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.threebyte >

Last change to this tool card: 14 May 2020

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

All groups using tool THREEBYTE

Changed	Name	Country	Observed
APT groups			
	APT 12, Numbered Panda		2009-Nov 2016

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=02dfdac5-9b39-43b2-aea4-8b91f3999064>