Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:37:31 UTC

Tool: AutoIt backdoor

Names	AutoIt backdoor
Category	Malware
Type	Backdoor
Description	AutoIt backdoor is malware that has been used by the actors responsible for the MONSOON campaign. The actors frequently used it in weaponized .pps files exploiting CVE-2014-6352. This malware makes use of the legitimate scripting language for Windows GUI automation with the same name.
Information	<https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0129/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:autoit>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool AutoIt backdoor

Changed	Name	Country	Observed	
APT groups				
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	Operation HangOver, Monsoon, Viceroy Tiger		2010-Jan 2020	
	Patchwork, Dropping Elephant		2013-Jun 2025	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f02e029b-a4e4-4672-aba5-331bcd5c9bd0