Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:56:31 UTC

Tool: Amadey

Names	Amadey
Category	Malware
Type	Reconnaissance, Dropper
Description	(Cylance) Amadey is a simple Trojan bot first discovered in October of 2018. It is primarily used for collecting information on a victim's environment, though it can also deliver other malware. A major infection vector for Amadey are exploit kits such as RigEK and Fallout EK. During our monitoring, we also observed this Trojan being delivered via AZORult Infostealer on February 23rd to March 1st, and April 18th to June 5th. The sample hash values were not changed frequently. Recently, TA505 used Amadey for their campaign in April 2019.
Information	<https://threatvector.cylance.com/en_us/home/threat-spotlight-amadey-bot.html> <https://krabsonsecurity.com/2019/02/13/analyzing-amadey-a-simple-native-malware/> <https://securelist.com/fake-captcha-delivers-lumma-amadey/114312/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1025/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:amadey>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool Amadey

Changed	Name	Country	Observed
APT groups			

	FIN11	[Unknown]	2016-Mar 2025	
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=26428c47-8df5-4c3c-864f-5c526f5bbdfc