EvilGrab RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:08:41 UTC

Tool: EvilGrab RAT

Names	EvilGrab RAT EvilGrab Vidgrab Wmonder BKDR_HGDER BKDR_EVILOGE BKDR_NVICM
Category	Malware
Type	Backdoor, Info stealer
Description	(Trend Micro) Recently, we spotted a new malware family that was being used in targeted attacks – the EvilGrab malware family. It is called EvilGrab due to its behavior of grabbing audio, video, and screenshots from affected machines. We detect EvilGrab under the following malware families: • BKDR_HGDER • BKDR_EVILOGE • BKDR_NVICM Looking into the feedback provided by the Smart Protection Network, EvilGrab is most prevalent in the Asia-Pacific region, with governments being the dominant sector targeted. These are consistent with known trends in targeted attacks.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0152/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.evilgrab>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:evilgrab>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool EvilGrab RAT

Changed	Name	Country	Observed	
APT groups				
	Nightshade Panda, APT 9, Group 27		2013-Sep 2016	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=39a329d8-f8a8-4bee-af71-a1a2035b9786