Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:08:34 UTC

Tool: Kegotip

Names	Kegotip
Category	Malware
Type	Info stealer
Description	(IBM) One of Kegotip's main functions is scraping email addresses from hard drives of endpoints it infects, even crossing to additional partitions on the endpoint. This generates quite a handsome bounty for its operators, likely in the form of the Necurs botnet itself, which then uses these addresses in its spam runs. Kegotip has been appearing alongside Dridex and Locky infections since April 2016, either via the RockLoader or Upatre.
Information	<https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kegotip>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:kegotip>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Kegotip

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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