Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:22:52 UTC

Tool: GROK

Names	GROK
Category	Malware
Type	Keylogger
Description	It is the case of a very sophisticated keylogger used by the Equation Group called “Grok”, which was also mentioned in one of the documents leaked by Edward Snowden. Grok is considered a keylogging component of the UNITEDRAKE malware, which experts linked to Regin malware. “The codename GROK appears in several documents published by Der Spiegel, where ‘a keylogger’ is mentioned. Our analysis indicates EQUATIONGROUP’s GROK plugin is indeed a keylogger on steroids that can perform many other functions,” reads the report. “Grok” is referred to for the first time in a post published by The Intercept titled, “How the NSA Plans to Infect ‘Millions’ of Computers with Malware.” The article introduces an NSA-developed keylogger called Grok.
Information	<https://resources.infosecinstitute.com/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.grok>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool GROK

Changed	Name	Country	Observed
APT groups			

	Equation Group		2001-Aug 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5135e7d5-5c40-4e5a-b580-f8610ad7852b