Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:29:20 UTC

Tool: OLDBAIT

Names	OLDBAIT Sasfis
Category	Malware
Type	Credential stealer
Description	(FireEye) OLDBAIT is a credential harvester that installs itself in %ALLUSERPROFILE%\\Application Data\Microsoft\MediaPlayer\updatewindws.exe. There is a missing space in the MediaPlayer directory and the filename is missing the 'o' character. Both the internal strings and logic are obfuscated and are unpacked at startup. Credentials for the following applications are collected: • Internet Explorer • Mozilla Firefox • Eudora • The Bat! (an email client made by a Moldovan company) • Becky! (an email client made by a Japanese company) Both email and HTTP can be used to send out the collected credentials. Note: In some places it is mistakenly named Sasfis, which however seems to be a completely different and unrelated malware family.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> <https://www.secjuice.com/fancy-bear-review/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0138/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.oldbait>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool OLDBAIT

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=487c6c1a-4baa-4586-85fb-032677f460be