Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:09:46 UTC

Tool: Sinowal

Names	Sinowal Anserin Mebroot Quarian Theola Torpig
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer, Downloader, Exfiltration
Description	(Fortinet) The installer drops a dynamic-link library (DLL) onto the local hard disk. The DLL acts as a loader module and will load other components, if any exist, and download a manager module which plays a central role in conducting banking fraud. The manager module downloads several plug-in modules from the C&C server, aimed at different target applications. These modules are used to steal sensitive information including bank account details, email addresses and FTP accounts. All plug-in modules contact the manager module through a named pipe, while the manager module communicates directly with the C&C server, uploading stolen information, reporting the local status of the trojan and downloading configuration and plug-in modules, as well as script commands for the plug-in modules to run.
Information	<https://www.virusbulletin.com/virusbulletin/2014/06/sinowal-banking-trojan> <https://www.welivesecurity.com/2013/03/13/how-theola-malware-uses-a-chrome-plugin-for-banking-fraud/> <https://en.wikipedia.org/wiki/Torpig>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sinowal>

Last change to this tool card: 22 May 2020

Download this tool card in JSON format

All groups using tool Sinowal

Changed	Name	Country	Observed

APT groups				
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

2 groups listed (1 APT, 0 other, 1 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=40636fe0-6160-4e7e-a7d0-e0dbc599d7aa