Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:14:15 UTC

Tool: Naikon

Names	Naikon XsFunction Sacto
Category	Malware
Type	Backdoor, Info stealer
Description	(Kaspersky) The Naikon tool of choice generates a special, small, encrypted file which is 8,000 bytes in size, containing code to be injected into the browser along with configuration data. With the help of a start-up module, this whole file is injected into the browser memory and decrypts the configuration block containing the following: • C&C server • Ports and path to the server • User-agent string • Filenames and paths to its components • Hash sums of the user API functions The same code then downloads its main body from the C&C server using the SSL protocol, loads it independently from the operating system functions and, without saving it to the hard drive, hands over control to the XS02 function. All functionality is handled in memory.
Information	<https://securelist.com/the-naikon-apt/69953/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.naikon>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Naikon

Changed	Name	Country	Observed

APT groups

	Naikon, Lotus Panda		2010-Apr 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=52cf9ec4-416a-49b4-9d0c-ade91208018e