

Havex RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:27:39 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Havex RAT

Tool: Havex RAT

Names	Havex RAT Havex Oldrea Backdoor.Oldrea Fertger PEACEPIPE
Category	Malware
Type	ICS malware , Reconnaissance , Backdoor
Description	<p>Havex is a remote access trojan (RAT) that was discovered in 2013 as part of a widespread espionage campaign targeting industrial control systems (ICS) used across numerous industries and attributed to a hacking group referred to as 'Dragonfly' and 'Energetic Bear'. Havex is estimated to have impacted thousands of infrastructure sites, a majority of which were located in Europe and the United States. Within the energy sector, Havex specifically targeted energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers. Havex also impacted organizations in the aviation, defense, pharmaceutical, and petrochemical industries.</p> <p>Once installed, Havex scanned the infected system to locate any Supervisory Control and Data Acquisition (SCADA) or ICS devices on the network and sent the data back to command and control servers. To do so, the malware leveraged the Open Platform Communications (OPC) standard, which is a universal communication protocol used by ICS components across many industries that facilitates open connectivity and vendor equipment interoperability. Havex used the Distributed Component Object Model (DCOM) to connect to OPC servers inside of an ICS network and collect information such as CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth.</p> <p>Havex was an intelligence-collection tool used for espionage and not for the disruption or destruction of industrial systems. However, the data collected by Havex would have aided efforts to design and develop attacks against specific targets or industries.</p>

Information	< https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html > < https://www.f-secure.com/weblog/archives/00002718.html > < https://en.wikipedia.org/wiki/Havex >
MITRE ATT&CK	< https://attack.mitre.org/software/S0093/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.havex_rat >

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool Havex RAT

Changed	Name	Country	Observed	
APT groups				
	Energetic Bear, Dragonfly		2010-Mar 2022	
	Sphinx	[Unknown]	2014	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=459f329c-969d-4046-9d42-504e0d48ca4d>