Havex

By Contributors to Wikimedia projects

Published: 2018-04-14 · Archived: 2026-04-06 02:58:24 UTC

From Wikipedia, the free encyclopedia

Havex	
Malware details	
Technical name	• BKDR_HAVEX.[letter] (Trend Micro) • Backdoor:Win32/Havex.[letter] Microsoft • Backdoor:W32/Havex (F-Secure)
Alias	Oldrea
Type	RAT
Author	Energetic Bear
Technical details	
Platforms	Windows, Linux, iOS, Android
Ports used	44818, 105 and 502
Written in	PHP

Havex malware, also known as Backdoor.Oldrea, is a Remote Access Trojan (RAT) employed by the Russian attributed APT group "Energetic Bear" or "Dragonfly".[1][2] Havex was discovered in 2013 and is one of five known ICS tailored malware developed in the past decade. These malwares include Stuxnet, BlackEnergy, Industroyer/CRASHOVERRIDE, and TRITON/TRISIS.[3] Energetic Bear began utilizing Havex in a widespread espionage campaign targeting energy, aviation, pharmaceutical, defense, and petrochemical sectors.[1] The campaign targeted victims primarily in the United States and Europe.[2]

The Havex malware was discovered by cybersecurity researchers at F-Secure and Symantec and reported by ICS-CERT utilizing information from both of these firms in 2013.[4][5] The ICS-CERT Alert reported analyzing a new malware campaign targeting ICS equipment via several attack vectors and using OPC to conduct reconnaissance on industrial equipment on the target network.[2]

The Havex malware has two primary components: A RAT and a C&C server written in PHP.[4] Havex also includes an OPC (Open Platform Communications) scanning module used to search for industrial devices on a

network.[2] The OPC scanning module was designed to scan for TCP devices operating on ports 44818, 105 and 502.[6] Researchers at SANS noted these ports are common to ICS/SCADA companies such as Siemens and Rockwell Automation.[6] By abusing the OPC protocol, Havex mapped industrial networks once inside victim systems.[7] Researchers note the OPC scanning module only operated on the older DCOM-based (Distributed Component Object Model) OPC standard and not the more recent OPC Unified Architecture (UA).[2] Havex joins the category of ICS tailored malware because it is written to conduct information gathering on these specific systems. Havex also exploited supply chain and watering-hole attacks on ICS vendor websites in addition to spear phishing campaigns to gain access to victim systems.[5][6] The watering-hole and supply chain attacks were twofold in methodology. In the first method, victims were redirected from legitimate vendor websites to corrupted pages containing the Havex malware.[1] In the second method, the attackers compromised vulnerable vendor websites and corrupted legitimate software to inject the Havex RAT. Users would then unknowingly download the malware when downloading otherwise legitimate software from vendor websites.[6] This method allowed the malware to bypass traditional security measure because software was downloaded by users with authorization to install programs onto the network. Known compromised vendors were MESA Imaging, eWON/Talk2M, and MB Connect Line.[8] While the attack vectors were aimed at business networks, the lack of robust airgaps in many ICS environments could allow malware like Havex to jump easily from business networks to industrial networks and infect ICS/SCADA equipment. Havex, like other backdoor malwares, also allows for the injection of other malicious code onto victim devices. Specifically, Havex was often used to inject the Karagany payload onto compromised devices. Karagany could steal credentials, take screenshots, and transfer files to and from Dragonfly C&C servers.[6]

Affected Regions & Victims

[edit]

The Dragonfly group utilized Havex malware in an espionage campaign against energy, aviation. pharmaceutical, defense, and petrochemical victims in primarily the United States and Europe.[1] Cybersecurity researchers at Dragos estimated the campaign targeted over 2,000 sites in these regions and sectors.[9] Researchers at Symantec observed Havex malware began seeking energy infrastructure targets after initially targeting US and Canadian defense and aviation sectors.[10] Through the discovery process, researchers examined 146 C&C servers associated with the Havex campaign and 88 variants of the malware.[11]

Website Redirect Injection

[edit]

Havex infected systems via watering hole attacks redirecting users to malicious websites.[1] Corrupted websites in this campaign used the LightsOut and Hello exploit kits to infect systems with the Havex and Karagany trojans.[10] The LightsOut exploit kit abused Java and browser vulnerabilities to deliver the Havex and Karagany payloads.[10] The Hello exploit kit is an updated version of the LightsOut exploit kit and came into use in 2013.[10] The updated Hello exploit kit uses footprinting to determine target OS versions, fonts, browser add-ons, and

other user information.[10] Once this information is gathered, the exploit kit redirects the victim to a malicious URL based on the most efficient exploits to gain access to the target.[10]

1. ^ Jump up to: **a** **b** **c** **d** **e** *"Havex"*. *NJCCIC. Retrieved 2018-04-18.*
2. ^ Jump up to: **a** **b** **c** **d** **e** *"ICS Focused Malware | ICS-CERT"*. *ics-cert.us-cert.gov. Retrieved 2018-04-18.*
3. ^ *"Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure | FireEye"*. *Retrieved 2018-05-14.*
4. ^ Jump up to: **a** **b** *"ICS Focused Malware (Update A) | ICS-CERT"*. *ics-cert.us-cert.gov. Retrieved 2018-04-18.*
5. ^ Jump up to: **a** **b** *"Cyber espionage campaign based on Havex RAT hit ICS/SCADA systems"*. *Security Affairs. 2013-06-25. Retrieved 2018-04-18.*
6. ^ Jump up to: **a** **b** **c** **d** **e** *Nelson, Nell (18 January 2016). "The Impact of Dragonfly Malware on Industrial Control Systems". SANS Institute.*
7. ^ *"CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations" (PDF).*
8. ^ *"Full Disclosure of Havex Trojans - NETRESEC Blog"*. *Netresec. 27 October 2014. Retrieved 2018-04-15.*
9. ^ *"CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations" (PDF).*
10. ^ Jump up to: **a** **b** **c** **d** **e** **f** *"Dragonfly: Cyberespionage Attacks Against Energy Suppliers" (PDF). 7 July 2014. Archived from the original (PDF) on August 1, 2014.*
11. ^ *"Attackers Using Havex RAT Against Industrial Control Systems | SecurityWeek.Com"*. *www.securityweek.com. Retrieved 2018-04-18.*
