ICS Focused Malware | CISA

Published: 2021-07-20 · Archived: 2026-04-05 14:51:23 UTC

Updated July 20, 2021: The U.S. Government attributes this activity to Russian nation-state cyber actors and assess that Russian nation-state cyber actors deployed Havex malware against industrial control systems. For more information on Russian malicious cyber activity, refer to us-cert.cisa.gov/Russia.

OVERVIEW

This advisory is a follow-up to the updated alert titled ICS-ALERT-14-176-02A that was published June 27, 2014, on the NCCIC/ICS-CERT web site. This advisory provides additional details regarding ICS Focused Malware Havex.

NCCIC/ICS-CERT is analyzing malware and artifacts associated with an industrial control system (ICS) focused malware campaign that uses multiple vectors for infection. These include phishing emails, redirections to compromised web sites and most recently, trojanized update installers on at least three ICSs vendor web sites, in what are referred to as watering-hole style attacks. Based on information ICS-CERT has obtained from Symantec and F-Secure (web site last accessed June 27, 2014). The software installers for these vendors were infected with malware known as the Havex Trojan (Backdoor.Oldrea), web site last accessed June 27, 2014. According to analysis, these techniques could have allowed attackers to access the networks of systems that have installed the trojanized software. Symantec describes the victims as Spain, US, France, Italy, and Germany in that order.

Symantec has posted a Security Response whitepaper that details this activity and provides indicators of compromise. Symantec also ties this campaign with previous watering hole activity, namely Trojan.Karagany and the Lightsout exploit kit.

The Trojan.Karagany was previously identified by Cisco as part of another watering hole attack targeting energy and oil sectors. This malware was analyzed and detailed by ICS-CERT in Analysis Report-14-30001 Cisco Watering-Hole Malware, located within the secure portal library.

OPC PAYLOAD

Havex is a Remote Access Trojan (RAT) that communicates with a Command and Control (C&C) server. The C&C server can deploy payloads that provide additional functionality. ICS-CERT has identified and analyzed one payload that enumerates all connected network resources, such as computers or shared resources, and uses the classic DCOM-based (Distributed Component Object Model) version of the Open Platform Communications (OPC) standard to gather information about connected control system devices and resources within the network. The known components of the identified Havex payload do not appear to target devices using the newer OPC Unified Architecture (UA) standard.

In particular, the payload gathers server information that includes CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth. In addition to more generic OPC server

information, the Havex payload also has the capability of enumerating OPC tags. ICS-CERT is currently analyzing this payload; at this time ICS-CERT has not found any additional functionality to control or make changes to the connected hardware.

ICS-CERT testing has determined that the Havex payload has caused multiple common OPC platforms to intermittently crash. This could cause a denial of service effect on applications reliant on OPC communications.

OPC provides an open standard specification that is widely used in process control, manufacturing automation, and other applications. The technology facilitates open connectivity and vendor equipment interoperability. The original version of the OPC specification, referred to as OPC classic, was implemented using Microsoft's COM/DCOM (Distributed Component Object Model) technology. In 2006, the OPC Foundation released a new standard, referred to as OPC Unified Architecture (UA), which does not use COM/DCOM. The known components of the identified HAVEX malware payload do not appear to target devices using the newer OPC UA standard.

ICS-CERT tested the payload against multiple OPC servers. An example of the information gathered can be seen below.

Program was started at 09:20:11

****

09:20:11.0828: Start finging of LAN hosts...

09:20:18.0109: Was found 3 hosts in LAN:

01) [\\vmware-host\Shared Folders]

02) [\\FEAE35F]

03) [\\SBWIN7]

****

09:20:18.0203: Start finging of OPC Servers...

09:20:39.0390: Thread 01 return error code: 0x800706ba

09:20:39.0390: Thread 02 return error code: 0x80070005

09:20:39.0390: Thread 03 return error code: 0x800706ba

09:20:39.0390: Thread 05 return error code: 0x80070005

09:20:39.0390: Thread 06 return error code: 0x80070005

09:20:39.0390: Was found 2 OPC Servers.

1) [Redacted Vendor Name]

CLSID: {Redacted Class ID}

UserType: Redacted Vendor Name

VerIndProgID: Redacted Vendor Name

OPC version support: +++

2) [Redacted Vendor Name]

CLSID: {Redacted Class ID}

UserType: Redacted Vendor Name

VerIndProgID: Redacted Vendor Name

OPC version support: ++-

****

09:20:39.0500: Start finging of OPC Tags...

09:20:39.0500: Thread 01 running...

09:20:39.0531: Thread 02 running...

09:20:51.0437: Thread 01 was terminated by ThreadManager(2)

09:20:51.0546: Thread 02 was terminated by ThreadManager(2)

09:20:53.0140: Thread 01 return error code: 0xfffffffe

09:20:53.0171: Thread 02 return error code: 0xfffffffe

1) Redacted Vendor Name

Saved in 'OPCServer01.txt'

These data are stored in a file that is created in the user's TEMP directory under a random name with an extension of ".tmp.dat." When all information has been written to this file, an encrypted version of this file is created in the same directory with a random name and a ".tmp.yls" extension. The plain text file is then deleted.

In addition to more generic OPC server information, the Havex payload also has the capability of enumerating OPC tags. Specifically, the server is queried for tag name, type, access and id. OPC tag information that is collected is written to a separate file "OPCServerXX.txt" where XX is a number beginning from one and incrementing every time OPC tag information has been retrieved from an OPC server.

OPC Server[\\Redacted Vendor Name]

Server state: 1

Group count value: 0

Server band width: ffffffff

[root]

Redacted Vendor Info

None of the versions of the Havex malware payload that have been analyzed thus far contain any functionality to control or make changes to connected control system devices.

MITIGATIONS

Symantec and F-Secure reports include technical indicators of compromise that can be used for detection and network defense. ICS-CERT strongly recommends that organizations check their network logs for activity associated with this campaign. Any organization experiencing activity related to this report should preserve available evidence for forensic analysis and future law enforcement purposes. For more questions about incident handling or preserving data, please reference ICS-CERT Incident Handling guidelines.

ICS-CERT has provided a Havex_Karagany.xlsx file on the US-CERT portal containing SHA1 hashes of malware for both Havex and Karagany.

OPC specific recommendations include:

- Enforce strict access control lists and authentication protocols for network level access to OPC clients and servers.
- Recommend DCOM/RPC communications are limited via the DCOMCNFG utility, because of well-known vulnerabilities inherent to RPC and DCOM.
- When using OPC.NET-based communications, ensure that the HTTP server enforces proper authentication and encryption of the OPC communications for both clients and servers.
- Leverage the OPC Security specification when possible.
- Avoid wide-scale use of local mirrored user accounts to facilitate DCOM authentication.
- Follow recommended guidelines for securing OPC communications via accounts that possess least-user privileges.
- When tunneling cannot be used, limit the range of DCOM/RPC communications via the DCOMCNFG utility, and pay special attention to the use of OPC “callbacks” across security perimeters.

Vendor specific mitigation:

- Digitally signing code provides a mechanism for detecting software tampering and helps assure recipients that the software does come from the vendor.
- Vendors who have not digitally signed their code should compare cryptographic hashes from their secure software repositories with the cryptographic hashes of files stored on public servers. These cryptographic hashes should also be made available to customers who are downloading the code, so that they can verify the integrity of their download. Vendors may also consider scanning installation files stored on public

servers using current antivirus software. ICS-CERT tested 16 common antivirus software applications against the Havex malware and found that most antivirus were able to detect the malware.

Additional mitigations to consider include:

- Always keep your patch levels up to date, especially on computers that host public services accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Maintain up-to-date antivirus signatures and engines, and apply them based on industrial control system vendor recommendations.
- Build host systems, especially critical systems such as servers, with only essential applications and components required to perform the intended function. Where possible remove or disable any unused applications or functions to limit the attack surface of the host.
- Implement network segmentation through V-LANs to limit the spread of malware.
- Exercise caution when using removable media (USB thumb drives, external drives, CDs).
- Consider the deployment of Software Restriction Policy set to only allow the execution of approved software (application whitelisting)
- Whitelist legitimate executable directories to prevent the execution of potentially malicious binaries.
- Consider the use of two-factor authentication methods for accessing privileged root level accounts or systems.
- When remote access is required, consider deploying two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access. Be prepared to operate without remote access during an incident if required.
- Implement a secure socket layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Place control system networks behind firewalls and isolate or air gap them from the business network.
- Provide robust logging such as network, host, proxy, DNS and IDS logs.
- Leverage the static nature of control systems to look for anomalies.
- Use configuration management to detect changes on field devices. Produce an MD5 checksum of clean code to verify any changes.
- Prepare for an incident with a dedicated incident response team and an incident response plan. Test both your plan and your team.
- ICS-CERT and US-CERT remind organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (www.ics-cert.org).

ICS-CERT also provides a recommended practices section for control systems on the US-CERT web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.
