ICS-CERT Alerts > ICS Focused Malware (Update A)

More ICS-CERT Alerts

ICS Alert (ICS-ALERT-14-176-02A)

ICS Focused Malware (Update A)

Original release date: June 27, 2014 | Last revised: August 22, 2018

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

Summary

This alert update is a follow-up to the original NCCIC/ICS-CERT Alert titled ICS-ALERT-14-176-02 ICS Focused Malware that was published June 25, 2014 on the ICS-CERT web site, and includes information previously published to the US-CERT secure portal.

--------- Begin Update A Part 1 of 2 --------

ICS-CERT is analyzing malware and artifacts associated with an ICS focused malware campaign that uses multiple vectors for infection. These include phishing emails, redirects to compromised web sites and most recently, trojanized update installers on at least 3 industrial control systems (ICS) 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, the software installers for these vendors were infected with malware known as the Havex Trojan. According to analysis, these techniques could have allowed attackers to access the networks of systems that have installed the trojanized software. The identities of these 3 known industrial control system vendors are available along with additional indicators of compromise to critical infrastructure owners and operators on the US-CERT secure portal.

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. F-Secure and ICS-CERT 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 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 Class Identification (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. Specifically the server is queried for tag name, type, access, and id. 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.

It is important to note that 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.

ICS-CERT is also evaluating possible linkages between this activity and previous watering hole compromises and malware campaigns. ICS-CERT will actively provide additional information including indicators of compromise as analysis progresses.

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 payload do not appear to target devices using the newer OPC UA standard.

--------- End Update A Part 1 of 2----------

More information including indicators of compromise can be found on the F-Secure web site:

http://www.f-secure.com/weblog/archives/00002718.html

In addition, ICS-CERT has posted a TLP Amber report regarding this activity to the portal library that also documents this activity. This report was developed by a trusted partner and provides additional technical details and analysis of the malware.

ICS-CERT encourages US asset owners and operators to join the control systems compartment of the US-CERT secure portal. To request access to the secure portal send your name, email address, and company affiliation to ics-cert@hq.dhs.gov.

Follow-up

ICS-CERT released the follow-up advisory ICSA-14-178-01 ICS Focused Malware to the Web site on June 30, 2014.

--------- Begin Update A Part 2 of 2 --------

Mitigation

Both the 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.

OPC specific recommendations include:

- Enforce strict access control lists and authentication protocols for network level access to OPC clients and servers.
- Consider using OPC tunneling technologies to avoid exposure of any legacy DCOM based OPC services.
- 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.

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.
- If an incident occurs, leave the computer on if possible. Do not run antivirus as it modifies the time stamp on all files that it accesses.
- ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT requests that any company that identifies activity related to this report, please notify ICS-CERT immediately for tracking and correlation.

ICS-CERT recommends that organizations review the ICS-CERT Technical Information Paper ICS-TIP-12-146-01B Targeted Cyber Intrusion Detection and Mitigation Strategies for high-level strategies that can improve overall visibility of a cyber intrusion and aid in recovery efforts should an incident occur.

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.

--------- End Update A Part 2 of 2----------

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

This product is provided subject to this Notification and this Privacy & Use policy.