ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-291-01A—W32.DUQU: AN INFORMATION-GATHERING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS MANUFACTURERS

UPDATE A

October 19, 2011

ALERT

SUMMARY

On October 18, 2011, Symantec released a Security Response Report[a] describing W32.Duqu, an information-gathering threat targeting specific organizations, including industrial control systems (ICSs) manufacturers. According to Symantec, W32.Duqu does not contain any code related to ICSs and is primarily a remote access Trojan (RAT).

Symantec reports that the original sample of W32.Duqu was gathered from a research organization based in Europe and that additional variants have been recovered from a second organization in Europe. According to Symantec, the attackers are looking for information, such as design documents, that could potentially be used in a future attack on an industrial control facility.

This threat is highly targeted toward a limited number of organizations, apparently to exfiltrate data concerning their specific assets; the propagation method is not yet known. Symantec indicates that W32.Duqu is not self-replicating.

Symantec reports that other attacks could be ongoing using undetected variants of W32.Duqu. Symantec states that they are continuing to analyze additional variants of W32.Duqu.

Key points from the report include:

- The executables share some code with the Stuxnet worm, and they were compiled after the last Stuxnet sample was recovered.
- There is no ICS specific attack code in the Duqu or infostealer.
- The primary infection vector for Duqu deployment has not yet been discovered/recovered (Duqu does not self-replicate or spread on its own).
- The targeted organizations appear to be limited.
- The malware employed a valid digital certificate (revoked as of October 14, 2011)
- The malware is designed to self-delete after 36 days.
- The Command and Control servers are hosted in India (Specific IPs unknown at this time).

[a] W32.Duqu, The Precursor to the Next Stuxnet, Symantec, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf, website last accessed October 18, 2011.

McAfee Labs[b] has also published a blog entry on the Duqu malware.

ICS-CERT has reached out to Symantec and McAfee to obtain additional information to assess the threat and identify mitigations that manufacturers and asset owners can employ to reduce their risk to this new threat. ICS-CERT will publish more information as it becomes available.

POSSIBLE INDICATORS

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

Duqu uses HTTP and HTTPS to communicate with a command and control (C&C) server at 206.183.111.97. This server is located in India and has been disabled by the ISP. ICS-CERT strongly recommends that organizations check network and proxy logs for any communication with this IP address. If any communication is identified, please contact ICS-CERT for further guidance.

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

Symantec has provided sample names and hashes for the files identified as part of this threat.

File Name	MD5 Hash
cmi4432.pnf	0a566b1616c8afeef214372b1a0580c7
netp192.pnf	94c4ef91dfcd0c53a96fdc387f9f9c35
cmi4464.PNF	e8d6b4dadb96ddb58775e6c85b10b6cc
netp191.PNF	b4ac366e24204d821376653279cbad86
cmi4432.sys	4541e850a228eb69fd0f0e924624b245
jminet7.sys	0eecd17c6c215b358b7b872b74bfd800
Infostealer	9749d38ae9b9ddd81b50aad679ee87ec

MITIGATION

The full extent of the threat posed by W32.Duqu is currently being evaluated. At this time, no specific mitigations are available; however, organizations should consider taking defensive measures against this threat. Specifically, ICS-CERT encourages organizations to:

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

- Update antivirus definitions for detection of the Duqu Trojan.

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

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

[b] The Day of the Golden Jackal, McAfee, http://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-tales-of-the-stuxnet-files, website last accessed October 18, 2011.

- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

Although the method of propagation has yet to be determined, the targeted nature of the thread would make social engineering a likely method of attack. ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open unsolicited attachments in e-mail messages

1. Refer to *Recognizing and Avoiding Email Scams* [c] for more information on avoiding e-mail scams
2. Refer to *Avoiding Social Engineering and Phishing Attacks*[d] for more information on social engineering attacks.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ics-cert@dhs.gov

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

[c] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed October 18, 2011.

[d] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed October 18, 2011.