ICS-CERT ALERT

ICS-ALERT-11-291-01E—W32.DUQU: AN INFORMATION-GATHERING MALWARE

UPDATE E

November 1, 2011

ALERT

SUMMARY

--------- Begin Update E Part 1 of 4 --------

This updated Alert is a follow-up to the Alert titled "ICS-ALERT-11-291-01D—W32.Duqu: An information-gathering malware" published October 26, 2011 on the ICS-CERT web. A Version C (containing FOUO-related content) was released on the US-CERT Secure Portal.

On November 1, 2011 Symantec[a] and the Laboratory of Cryptography and Systems Security (CrySyS)[b] released updated reports identifying possible affected organizations, the dropper used to infect systems, and a new command and control (C&C) IP address. The below sections highlight the new information identified.

ICS-CERT is in the process of compiling and re-organizing all of the data in this alert for release in an upcoming advisory.

--------- End Update E Part 1 of 4 --------

ICS-CERT, in close coordination with Symantec and the original researchers, has determined after additional analysis that neither industrial control systems (ICSs) nor vendors/manufacturers were targeted by Duqu. In addition, as of October 21, 2011, there have been few infections, and there is no evidence based on current code analysis that Duqu presents a specific threat to ICSs.

--------- Begin Update E Part 2 of 4 --------

According to Symantec, they have confirmed six possible infected organizations in eight countries including France, Netherlands, Switzerland, Ukraine, India, Iran (2), Sudan, and Vietnam. Symantec notes the organizations are only traceable back to an ISP. Other security vendors have reported infections in Austria, Hungary, Indonesia, United Kingdom, and Iran. At this point, a comprehensive list of infected organizations is not available.

--------- End Update E Part 2 of 4 ----------

a http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit, website last accessed November 01, 2011. Symantec also has a link to version 1.3 of their whitepaper on this site.

b http://www.crysys.hu/, Laboratory of Cryptography and System Security (CrySyS), Department of Telecommunications, Budapest University of Technology and Economics, website last accessed November 01, 2011.

However, organizations should still remain vigilant against this and other sophisticated malware. ICS-CERT also recommends that the ICS community update intrusion prevention systems (IPSs) and antivirus systems to detect Duqu and other new threats.

ICS-CERT will continue to analyze the malware, monitor the threat landscape, and report additional information as appropriate. ICS-CERT will also continue coordination with Symantec, McAfee, the international community, and ICS stakeholders.

On October 18, 2011, Symantec released a Security Response Report[c] describing W32.Duqu, an information-gathering threat targeting specific organizations, including 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.

--------- Begin Update E Part 3 of 4 --------

On November 1, 2011 the researchers, CrySyS, reported they had located the installer being used to infect systems. Symantec has updated their Security Response Report[d] and described the installer as a Microsoft Word document (file extension: .doc) that exploits a previously unknown (0-day) kernel vulnerability. According to the report, Microsoft is working to issue a patch and advisory for this vulnerability.

Symantec's report also indicates that the malicious Word document was specially crafted to target the intended receiving organization. This appears to support the assertion that Duqu was highly targeted.

Once infected, attackers can infect other computers in secure zones and control them through a peer-to-peer C&C protocol.

--------- End Update E Part 3 of 4 ----------

Key points from the report include:

c.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 November 01, 2011.

[d]http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit, website last accessed November 01, 2011

- 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 (C&C) servers are hosted in India (Specific IPs unknown at this time).

McAfee Labs[e] 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.

On October 25, 2011, Kaspersky Labs released an article[f] entitled "The Mystery of Duqu: Part Two" in which four additional Duqu infections were detected on their security network: one system in Sudan and three in Iran.

In addition, Kaspersky Labs has reported that the name and size of the driver file in the infections they analyzed differs from the previously reported file making it difficult for antivirus software to detect it. As of October 26, 2011, neither Kaspersky Labs nor ICS-CERT has copies of the new files making a full set of new indicators impossible to determine at this time. In addition, it is possible that the malware authors will continue to craft new variants to avoid detection.

POSSIBLE INDICATORS

Duqu uses HTTP and HTTPS to communicate with a C&C server at 206.183.111.97[g]. 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.

--------- Begin Update E Part 4 of 4--------

Symantec has identified a new C&C server that is hosted in Belgium. The IP address reported is 77.241.93.160. This C&C server has been disabled by the hosting provider.

Symantec has provided sample names and hashes for the files identified as part of this threat. Additional indicators from Contagio and Kaspersky are also listed below:

e 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 November 01, 2011.

f. The Mystery of Duqu: Part Two, Kaspersky Labs, http://www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two, website last accessed November 01, 2011.

g. Updated C&C information has been published in Update C located on the US-CERT Secure Portal. Please contact ICS-CERT for questions regarding this FOUO/TLP AMBER update.

File Name	MD5 Hash
cmi4432.pnf	0a566b1616c8afeef214372b1a0580c7
netp192.pnf	94c4ef91dfcd0c53a96fdc387f9f9c35
cmi4464.PNF	e8d6b4dadb96ddb58775e6c85b10b6cc
netp191.PNF	b4ac366e24204d821376653279cbad86
cmi4432.sys	4541e850a228eb69fd0f0e924624b245
jminet7.sys	0eecd17c6c215b358b7b872b74bfd800
keylogger.exe	9749d38ae9b9ddd81b50aad679ee87ec
Recon DLL pushed by C&C server	4c804ef67168e90da2c3da58b60c3d16
Lifetime updater pushed by C&C server	856a13fcae0407d83499fc9c3dd791ba
Reduced functionality infostealer pushed by C&C server	92aa68425401ffedcfba4235584ad487
nfred965.sys	c9a31ea148232b201fe7cb7db5c75f5e
nred961.sys	f60968908f03372d586e71d87fe795cd
adpu321.sys	3d83b077d32c422d6c7016b5083b9fc2
iaStor451.sys	bdb562994724a35a1ec5b9e85b8e054f

--------- End Update E Part 4 of 4 ----------

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:

- Update antivirus definitions for detection of the Duqu Trojan.
- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- 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.

With new variants of Duqu reported on October 25, 2011, by Kaspersky Labs,[h] current antivirus software may not be able to identify all variants of this malware. Organizations should consider adding the following items to their network security plans:

h. The Mystery of Duqu: Part Two, Kaspersky Labs, http://www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two, website last accessed November 01, 2011

- Monitor for new and unknown services running on client machines.
- Monitor systems on their network for new files added to system directories such as system32, and system32\drivers.
- Monitor for network traffic anomalies; such as:
  - Beaconing to unknown IP addresses
  - Spikes in traffic
  - Outgoing binary files such as jpg
  - HTTP and HTTPS traffic from machines that do not have browsers installed.

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* [i] for more information on avoiding e-mail scams
2. Refer to *Avoiding Social Engineering and Phishing Attacks*[j] 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.

i. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed November 01, 2011.

j. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed November 01, 2011.