Joint Security Awareness Report

JSAR-11-312-01–W32.DUQU-MALWARE

November 08, 2011

OVERVIEW

This report is a follow-up and summary of the series of six alerts and updates titled "ICS-ALERT-11-291-01– W32.Duqu: An Information-Gathering Malware" that were originally published beginning October 18, 2011, with the last update "E" published November 01, 2011, on the ICS-CERT web page. One update, ICS-ALERT-11-291-01CP, was released as For Official Use Only (FOUO) to a limited distribution on October 24, 2011.

ICS-CERT and US-CERT independent analysis, along with the findings from the original Hungarian researchers (Laboratory of Cryptography and System Security [CrySyS]),[a] and several security vendors (Symantec, McAfee, Kaspersky, SecureWorks) have found no evidence that Duqu targeted owners and operators, vendors, or manufacturers of industrial control systems (ICSs). As of November 1, 2011, few infections have been reported or discovered.

Analysis of the known Duqu variants identifies this malware as a remote access Trojan (RAT). As with other malware of this type, Duqu infects a vulnerable system and inserts itself into memory, giving it the look of a trusted running process. Once the system is infected, attackers can infect other computers in secure zones and control them through a peer-to-peer command and control (C&C) protocol.

According to Symantec, its researchers have confirmed six possible infected organizations geographically located in eight countries including France, Netherlands, Switzerland, Ukraine, India, Iran (2), Sudan, and Vietnam. Symantec notes the organizations are only traceable back to their ISPs. 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.

Based on the information reported by antivirus vendors, multiple variants of Duqu exist, each with its own signature. In addition, Duqu configuration files contain a self-deletion time-window that is typically set between 30 and 36 days. Symantec reports that Duqu has downloaded updated configuration files that could contain new self-deletion times. Thus, C&C servers could control the lifespan of Duqu by providing modified configuration files. The removal mechanism is thought to be an attempt by Duqu to prevent its discovery.

On November 1, 2011, CrySyS reported that it had located a dropper used to infect systems. Symantec has updated its Security Response Report[b] and described the dropper as a Microsoft Word document (file

a. Laboratory of Cryptography and System Security (CrySyS), Budapest University of Technology and Economics, http://www.crysys.hu/, website last accessed November 07, 2011.

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

extension: .doc) that exploits a previously unknown (0-day) kernel 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. The presence of the dropper indicates that multiple undiscovered droppers may yet exist.

CVE-2011-3402[c] has been assigned to the previously unknown kernel vulnerability known to be exploited by the Duqu dropper. Microsoft is currently working to produce a patch for this vulnerability and has issued a Security Advisory (2639658).[d] An interim mitigation has also been introduced by Microsoft until a full patch can be developed and issued.[e]

Although several pattern detection files from the major antivirus manufacturers exist, ICS-CERT/US-CERT recommend that asset owners continue to use and improve their defense-in-depth strategy. Some of these strategies that may help detect any instances of Duqu running on systems include:

- Understand your normal internal and external network traffic. Look for any unusual or unknown data traffic to or from unknown or unexpected IP addresses including internal systems. This may indicate an internal system is being used as a pivot point by attackers to move throughout your network.
- Keep antivirus software up to date.
- Consider whitelisting if appropriate to your operating environment.
- Monitor system directories and services for any new or unknown entries.

ICS-CERT/US-CERT will continue to analyze the malware, monitor the threat landscape, and report additional information as appropriate.

TIMELINE

- According to the Symantec report,[f] Duqu attacks may have been conducted as early as December 2010, based on the dates the binary files were compiled.
- CrySyS delivered its sample of W32.Duqu to Symantec on October 14, 2011.
- After receiving information from CrySyS, Symantec reviewed its archive of submissions and found it had seen a Duqu variant on September 1, 2011.
- On October 18, 2011, Symantec released the first of several versions of its Security Response report entitled "W32.Duqu, The Precursor to the Next Stuxnet."[g] These reports give a technical overview of Duqu functionality and classify it as a RAT.

---

c. CVE-2011-3402, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402, website last accessed November 07, 2011.

d.Microsoft Security Advisory (2639658), http://technet.microsoft.com/en-us/security/advisory/2639658, website last accessed November 07, 2011.

e. Microsoft Security Advisory: Vulnerability in TrueType font parsing could allow elevation of privileges, http://support.microsoft.com/kb/2639658, website last accessed November 07, 2011.

f. 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 07, 2011.

g.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 07, 2011.

- On October 18, 2011, McAfee Labs[h] published a blog entry on the Duqu malware with additional information that stated Duqu was targeting certificate authorities.
- On October 25, 2011, Kaspersky Labs released an article[i] entitled "The Mystery of Duqu: Part Two" in which it reported that four additional Duqu infections were detected on its security network: one in Sudan and three in Iran. Kaspersky reported that each of these detections had a unique signature.
- On October 26, 2011, Dell SecureWorks released an article[j] entitled "Duqu Trojan Questions and Answers."
- On November 01, 2011, CrySyS released a statement that it had identified a dropper file with a Microsoft 0-day kernel exploit, and Symantec released Version 1.3 of its Duqu report. Significant in this report are the identification of a second infostealer (page 16) and the version history with content changes (page 20).

KEY POINTS

- According to Symantec and Kaspersky reports, the executables share some code with Stuxnet and were compiled after the last Stuxnet sample was recovered.
- Duqu is not self replicating.
- Duqu variants use a custom protocol to communicate with its C&C server.
- Variants of Duqu have used different C&C servers.
- No ICS-specific attack code has been detected in Duqu.
- The "infostealer" tools reported by Symantec have not been found at all infected sites.
- Only one primary infection vector for Duqu deployment has been identified.
- Based on reported detections, the number of targeted organizations appears to be limited.
- Some Duqu variants employed a valid digital certificate (revoked as of October 14, 2011). For further information please see Symantec's report.[g]
- Duqu has a built-in removal mechanism. The time to live is configurable, and Symantec has discovered additional downloaded components that may extend this time window.
- Each variant of Duqu found has had different signature characteristics. This may make it more difficult for antivirus software to detect new infections.
- At least two types of infostealer tools have been observed at this time.
- Information is lightly encrypted and compressed locally on the infected system. This file is then appended to a .jpg file for exfiltration. The use of the .jpg files is an attempt to disguise the data transmission as normal HTTP traffic.

---

h. 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 07, 2011.

i. 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 07, 2011.

j. Duqu Trojan Questions and Answers, http://www.secureworks.com/research/threats/duqu, website last accessed November 07, 2011.

MALWARE CHARACTERIZATION

MALWARE OVERVIEW

1. Antivirus manufacturers have already created and updated several versions (at least three known variants at the time of this publication) of pattern files to detect and remove Duqu. However, changing signatures and use of multiple C&C servers makes detecting infections very difficult at this time.
2. Symantec reports in Version 1.3[k] of its report that the Duqu C&C server can download and execute additional binaries. These binaries were injected directly into memory and not saved on the disk.

MALWARE DETAILS

POSSIBLE INDICATORS

The first Duqu samples appeared to use HTTP and HTTPS to communicate with a C&C server at 206.183.111.97.[l] This server has been disabled by the ISP. Symantec has identified a new C&C server with the IP address reported as 77.241.93.160. This C&C server has also been disabled by the host 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 in the Table 1.

ICS-CERT/US-CERT strongly recommend that organizations check network and proxy logs for any suspicious data communications. If any suspicious data communication is identified, please contact ICS-CERT/US-CERT for further guidance. Table 1 contains known indicators associated with this threat.[m] This table will be updated as additional confirmed indicator files are discovered and confirmed.

Table 1. Indicator files.

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

k. 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 07, 2011.

l. 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.

m. Courtesy of Symantec (www.symantec.com), Contagio (caution – active malware is available on this site – http://contagiodump.blogspot.com/2011/10/duqu-rat-trojan-precursor-to-the-next.html) and SecureWorks (http://www.secureworks.com/research/threats/duqu).

File Name	MD5 Hash
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

MALWARE CAPABILITIES

One variant of this attack used a previously unknown (0-day) kernel exploit embedded in a Word document. Other infection methods may be possible, however, neither ICS-CERT nor US-CERT have identified any at this time. Once installed, Duqu has the capability to install additional executables. Duqu is believed to have dropped infostealer tools on targeted systems from a C&C server to enumerate the network, record keystrokes, and collect other system information. At least two types of infostealer tools have been observed to date. The information is then lightly encrypted and compressed locally on the infected system. This file is subsequently appended to a .jpg file for exfiltration. The use of the .jpg files is an attempt to disguise the data transmission as normal network traffic.

Duqu does not self replicate. Symantec has reported that Duqu's RAT capabilities may have been used to selectively replicate though network shares. The latest Symantec report (Version 1.3) states that Duqu may also instruct newly infected computers to communicate using the original infected system, creating a peer-to-peer C&C model. This method of systematic infection may allow Duqu to access computers that are not directly Internet facing and may help to avoid detection caused by suspicious outbound data traffic from multiple computers.

MITIGATION

The full extent of the threat posed by W32.Duqu is currently being evaluated. At this time, no specific mitigations are available. Microsoft announced an interim mitigation for the previously unknown (0-day) vulnerability known to be exploited by the Duqu dropper. Information concerning this interim mitigation can be found in the Microsoft TechNet Security Advisory.[n]

In addition, organizations should consider taking defensive measures against this threat. Specifically, ICS-CERT/US-CERT encourages organizations to:

- Keep antivirus software up to date.
- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

n. Microsoft Security Advisory: Vulnerability in TrueType font parsing could allow elevation of privileges, http://support.microsoft.com/kb/2639658, website last accessed November 07, 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.
- Monitor systems for new and unknown services running on client machines.
- Monitor systems for new files added to system directories such as system32, and system32\drivers.
- Consider whitelisting if appropriate for your operating environment.
- Monitor for internal and external 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
  - Unexplained traffic between internal systems - this may indicate that an internal system is being used as a pivot point by attackers to move throughout your network.

As of November 04, 2011, one dropper has been identified as a Word document that exploits a Windows kernel 0-day. The targeted nature of the threat indicates social engineering as a likely attack method. ICS-CERT and US-CERT recommend that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages.
2. Refer to *Recognizing and Avoiding Email Scams*[o] for more information on avoiding e-mail scams.
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[p] for more information on social engineering attacks.

The Control Systems Security Program (CSSP) also provides a section for control system security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[q] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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

---

o. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed November 07, 2011.

p. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed November 07, 2011.

q. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 07, 2011.

ICS-CERT or US-CERT CONTACT INFORMATION

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

For any questions related to this report, please contact US-CERT at:

E-mail: soc@us-cert.gov
US-CERT Voice: 1-888-282-0870
ICS-CERT Watch Floor: 877-776-7585
Incident Reporting Form: https://forms.us-cert.gov/report/

DOCUMENT FAQ

What is a JSAR Advisory? A JSAR Advisory is a Joint Security Advisory intended to provide awareness or solicit feedback from critical infrastructure owners, integrators, peers and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. All comments or questions related to this document should be directed to either ICS-CERT or US-CERT at:
ICS-CERT - ics-cert@dhs.gov

US-CERT - soc@us-cert.gov