Duqu Trojan Questions and Answers

- **URL:** http://www.secureworks.com/research/threats/duqu/
- **Date:** October 26, 2011
- **Author:** SecureWorks Counter Threat Unit Research Team

The Dell SecureWorks Counter Threat Unit^{SM} (CTU) research team has been analyzing an emerging malware threat identified as the Duqu trojan. This Trojan horse has received a great deal of attention because it is similar to the infamous Stuxnet worm of 2010. This report includes answers to questions about this threat. CTU researchers have put countermeasures in place to detect Duqu C2 traffic, and they continue to monitor for new Duqu samples and update protections as needed.

What is Duqu?

The Duqu trojan is composed of several malicious files that work together for a malicious purpose. The first component is a Windows kernel driver that searches for and loads encrypted dynamic link library (DLL) files. The decrypted DLL files implement the main payload of Duqu, which is a remote access trojan (RAT). The RAT allows an adversary to gather information from a compromised computer and to download and run additional programs.

In addition to the RAT, another piece of malware was recovered with Duqu in one instance. This malware is an information stealer designed to log user keystrokes and other information about the infected system. This piece of malware is believed to be related due to programming similarities with the main Duqu executables.

What is the relationship to Stuxnet?

There has been much speculation that Duqu is a new version of Stuxnet or that it was written by the same authors. There are several factors that could influence these speculations:

- Duqu and Stuxnet both use a kernel driver to decrypt and load encrypted DLL (Dynamic Load Library) files. The kernel drivers serve as an "injection" engine to load these DLLs into a specific process. This technique is not unique to either Duqu or Stuxnet and has been observed in other unrelated threats.
- Encrypted DLL files are stored using the .PNF extension. This is normally the ex-

tension Microsoft Windows uses for precompiled setup information files. The commonality exists due to the kernel driver implementation being similar.

- The kernel drivers for both Stuxnet and Duqu use many similar techniques for encryption and stealth, such as a rootkit for hiding files. Again, these techniques are not unique to either Duqu or Stuxnet and have been observed in other unrelated threats.
- Both Stuxnet and Duqu have variants where the kernel driver file is digitally signed using a software signing certificate. One variant of the Duqu kernel driver was signed by a certificate from C-Media Electronics Incorporation. An unsigned Duqu kernel driver claimed to be a driver from the JMicron Technology Company, which was the same company whose software signing certificate was used to sign one of the Stuxnet kernel driver files. The commonality of a software signing certificate is insufficient evidence to conclude the samples are related because compromised signing certificates can be obtained from a number of sources. One would have to prove the sources are common to draw a definitive conclusion.

Attribute	**Duqu**	**Stuxnet**
Infection Methods	Unknown	USB (Universal Serial Bus) PDF (Portable Document Format)
Dropper Characteristics	Installs signed kernel drivers to decrypt and load DLL files	Installs signed kernel drivers to decrypt and load DLL files
Zero-days used	None yet identified	Four
Command and Control	HTTP, HTTPS, Custom	HTTP
Self propagation	None yet identified	P2P (Peer to Peer) using RPCs (Remote Procedure Call) Network Shares WinCC Databases (Siemens)
Data exfiltration	Add-on, keystroke logger for user and system info stealing	Built-in, used for versioning and updates of the malware
Date triggers to infect or exit	Uninstalls self after 36 days	Hard coded, must be in the following range: 19790509 => 20120624
Interaction with control systems	None	Highly sophisticated interaction with Siemens SCADA control systems

Table 1. Comparison of Duqu and Stuxnet.

Both Duqu and Stuxnet are highly complex programs with multiple components. All of the similarities from a software point of view are in the "injection" component implemented by the kernel driver. The ultimate payloads of Duqu and Stuxnet are significantly different and unrelated. One could speculate the injection components share a common source, but supporting evidence is circumstantial at best and insufficient to confirm a direct relationship. The facts observed through software analysis are inconclusive at publication time in terms of proving a direct relationship between Duqu and Stuxnet at any other level.

Does Duqu target industrial control systems?

Unlike Stuxnet, Duqu does not contain specific code that pertains to supervisory control and data acquisition (SCADA) components such as programmable logic controllers (PLCs). Duqu's primary purpose is to provide an attacker with remote access to a compromised computer, including the ability to run arbitrary programs. It can theoretically be used to target any organization.

Is there any evidence in the code indicating specific targets?

Duqu facilitates an adversary's ability to gather intelligence from an infected computer and the network. CTU malware analysts have not identified any specific market segments, technologies, organizations or countries that are targeted by the Duqu malware.

What are indicators of a Duqu infection?

The Duqu trojan attempts to use the network to communicate with a remote command and control (C2) server to receive instructions and to exfiltrate data. Analysis of Duqu revealed that it uses the 206.183.111.97 IP address as its C2 server. This IP address is located in India and has been shut down by the hosting provider. Also, Duqu may attempt to resolve the kasperskychk.dyndns.org domain name. The resulting IP address is not used for communications, so this lookup may serve as a simple Internet connectivity check. Administrators should monitor their network for systems attempting to resolve this domain or connect to the C2 IP address for possible infection.

Duqu uses multiple protocols to communicate with its C2 server, including standard HTTP on TCP port 80 and a custom protocol on TCP port 443. Some of Duqu's communications that use TCP port 443 do not use the HTTPS protocol. Organizations may be able to monitor egress traffic through proxy servers or web gateways and investigate

network traffic that does not conform to the SSL (Secure Sockets Layer) specification. Non-SSL traffic on port 443 is commonly observed with other threats, and this behavior is not exclusive to Duqu.

The CTU research team is aware of the following files that may be installed by the Duqu trojan. The byproducts in Table 2 have been collected from multiple Duqu variants and would not be present on a single infected computer.

Name	File Size	MD5
jminet7.sys	24,960 bytes	0eecd17c6c215b358b7b872b74bfd800
netp191.pnf	232,448 bytes	b4ac366e24204d821376653279cbad86
netp192.pnf	6,750 bytes	94c4ef91dfcd0c53a96fdc387f9f9c35
cmi4432.sys	29,568 bytes	4541e850a228eb69fd0f0e924624b245
cmi4432.pnf	192,512 bytes	0a566b1616c8afeef214372b1a0580c7
cmi4464.pnf	6,750 bytes	e8d6b4dadb96ddb58775e6c85b10b6cc
<unknown> (sometimes referred to as keylogger.exe)	85,504 bytes	9749d38ae9b9ddd81b50aad679ee87ec
nfred965.sys	24,960 bytes	c9a31ea148232b201fe7cb7db5c75f5e
nred961.sys	unknown	f60968908f03372d586e71d87fe795cd
adpu321.sys	24,960 bytes	3d83b077d32c422d6c7016b5083b9fc2
iaStor451.sys	24,960 bytes	bdb562994724a35a1ec5b9e85b8e054f

Table 2. Byproducts of Duqu.

The name "Duqu" was assigned to this malware because the keylogger program creates temporary files that begin with the prefix "~DQ". A computer infected with Duqu may have files beginning with "~DQ" in Windows temporary directories.

How do Duqu infections occur?

The mechanism by which Duqu infections occur is unknown. Current analysis of Duqu has not revealed any ability to infect additional systems like the Stuxnet worm could. In addition, all of the Duqu files CTU researchers have analyzed would likely have been installed by an initial installer or "dropper" malware. None of the original installers have been recovered. The recovery of one of these installers may help provide clues to how Duqu infections occurred.

Is Duqu an advanced persistent threat (APT)?

Dell SecureWorks does not identify individual tools as APT. APT is a threat actor or actors targeting an organization for assets of interest. An APT involves planning by the adversary, teams with specialized roles, multiple tools, patience and persistence. While Duqu does provide capabilities used by other tools observed in APT-related intrusions, an assessment of the particular threat requires knowledge of the adversary, targeted organization and assets and the scope of attacks.

Is antivirus and antimalware protection sufficient for detecting Duqu?

Since its discovery, security vendors have worked to improve their ability to detect Duqu. However, the author may simply release newer variants that are no longer detected by antivirus and antimalware products.

What can I do to protect my organization from Duqu?

- Administrators should use host-based protection measures, including antivirus and antimalware, as part of a holistic security process that includes network-based monitoring and controls, network segmentation and policies, user access, and controls to help mitigate the threat of malware like Duqu.
- A computer infected with Duqu may have files beginning with "~DQ" in Windows temporary directories.
- Organizations may want to monitor egress traffic through proxy servers or web gateways and investigate network traffic that does not conform to the SSL (Secure Sockets Layer) specification. Non-SSL traffic on port 443 is commonly observed with other threats, and this behavior is not exclusive to Duqu.
- Administrators should monitor their network for systems attempting to resolve Duqu-related domains or connect to Duqu C2 IP addresses for possible infection.