# W32.Duqu: The Precursor to the Next Stuxnet

Eric Chien (Symantec), Liam OMurchu (Symantec), Nicolas Falliere

## I. Introduction

On October 14, 2011, we were alerted to a sample by the Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics. The threat appeared very similar to the Stuxnet worm from June of 2010 [1]. CrySyS named the threat Duqu [dyü-kyü] because it creates files with the file name prefix "~DQ" [2]. We confirmed Duqu is a threat nearly identical to Stuxnet, but with a completely different purpose of espionage rather than sabotage.

## II. Motivation

Duqu is the precursor to a future Stuxnet-like attack. The threat was written by the same authors, or those that have access to the Stuxnet source code, and used after the last-discovered version of Stuxnet. Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on various industries, including industrial control system facilities.

## III. Telemetry

The first recording of an attack occurred in early April, 2011. However, based on file-compilation times, attacks using these variants may have been conducted as early as March 2010. Additional variants were created as recently as October 17, 2011 and new payload modules downloaded October 18, 2011. Thus, at the time of discovery, the attackers were still active.

Duqu infections have been confirmed in eight countries (France, Netherlands, Switzerland, Ukraine, India, Iran, Sudan, Vietnam) and unconfirmed reports exist in an additional 4 countries (Austria, Hungary, Indonesia, United Kingdom). Between 6 and 10 organizations were believed affected.

## IV. Execution Flow

Duqu does not contain any code related to industrial control systems and is primarily a remote access Trojan. The threat does not self-replicate. In two cases, the attackers used a specifically targeted email with a Microsoft Word document. The Word document contained a 0-day kernel exploit that was able to install Duqu. The 0-day took advantage of TrueType Font (TTF) parsing via Microsoft Word however, parsing of TTF objects occurs in the kernel where graphics device interface code is located. We were unable to confirm how Duqu was introduced in all organizations.

During the installation process, seven different files are executed in memory, at least three processes are injected into, and ntdll.dll is hooked multiple times. However, during the entire process Duqu is in its decrypted form only in memory and at the end, only three files exist on disk – the load point driver, the main DLL, and the configuration file. Of these, only the load point driver is a recognizable executable as the others are encrypted data blobs.

One of the variant's driver files was signed with a valid digital code signing certificate that expires on August 2, 2012. The digital code signing certificate was issued to C-Media, headquartered in Taipei, Taiwan and was revoked on October 14, 2011. We believe the private keys used to generate the certificate were stolen from the company. Having a legitimate certificate allows Duqu to bypass default restrictions on unknown drivers and common security policies.

Duqu will also inject itself into a trusted process to attempt to bypass security products. This code is the same as in Stuxnet, but has been updated to handle two additional security products: Kaspersky (version 10 and 11) and Rising Antivirus. Duqu checks for security products from Kaspersky, McAfee, AntiVir, Bitdefender, Etrust, Symantec, ESET, Trend, Rising.

The attackers used Duqu to install another infostealer that can record keystrokes and collect other system information. The attackers were searching for information assets that could be used in a future attack. In one case, the attackers did not appear to successfully exfiltrate any sensitive data and in other cases successful exfiltration occurred.

## V. Command and Control

Duqu primarily uses HTTP and HTTPS to communicate directly with a command and control (C&C) server, but can also reach the C&C via other

infected peers using a peer-to-peer command and control channel. Using a peer-to-peer C&C model allows the threat to access computers that may not be connected directly to the external Internet and also avoid the detection of potentially suspicious external traffic from multiple computers. Duqu also has proxy-aware routines, but these are only used if enabled by the attacker.

Each attack used one or more different C&C servers. Multiple C&C servers have been discovered in multiple countries including India, Belgium, Vietnam, Germany, Singapore, Switzerland, the UK, Netherlands, and South Korea. Some of these servers appear to be legitimate servers that were hacked by the Duqu attackers. The C&C servers were configured to simply forward all port 80 and 443 traffic to other servers. These servers forwarded traffic to further servers, making identification and recovery of the actual C&C server difficult. The traffic-forwarding C&C servers were scrubbed on October 20, 2011, so limited information was recovered. Even if the servers were not scrubbed, little actionable information would likely have been found due to their sole purpose of simply forwarding traffic.

Through the command and control server, the attackers were able to download additional executables, including an infostealer that can perform actions such as enumerating the network, recording keystrokes, and gathering system information. The information is logged to a lightly encrypted and compressed local file, and then must be exfiltrated out. In addition to this infostealer, three more DLLs were pushed out by the C&C server on October 18.

The threat uses a custom command and control protocol, primarily downloading or uploading what appear to be .jpg files. However, in addition to transferring dummy .jpg files, additional encrypted data is appended to the .jpg file for exfiltration, and likewise received. The use of the .jpg flies is simply to obfuscate network transmissions.

## VI. Additional Behaviors

The threat does not self-replicate, but based on forensic analysis of compromised computers, the threat was copied to network shares to infect additional computers on the network.

The threat is configured to run for 30 days by default. After 30 days, the threat will automatically remove itself from the system. However, Duqu has downloaded additional components that can extend the number of days to live. Thus, if the attackers are discovered and they lose the ability to control compromised computers (for example, if the C&C servers are shutdown), the infections will eventually automatically remove themselves, preventing possible discovery.

## VII. Related Attacks

Reports of a similar threat in April, 2011, known as "Stars" by Iranian officials, may in fact be Duqu. While suspected, no complete set of similar precursor files have been recovered that date prior to the Stuxnet attacks. Similar driver files dating back to January 2008 that predate Stuxnet have been discovered, but without the associated main binaries their purpose is unknown [3].

## VIII. Conclusion

The attackers behind Stuxnet and Duqu have been developing code for at least three years and likely more. The code serves as a framework to deliver specific functionality for particular attack scenarios -- in the case of Stuxnet, the desire to sabotage uranium enrichment activities in Iran and in the case of Duqu to collect information from specific organizations to mount a future attack. Given the high-profile discovery of Stuxnet did not deter the attackers from the subsequent continuation of the attacks with Duqu, we expect future threats from the same attackers based on the same code platform with likely similar targets.

## Acknowledgements

We wish to thank CrySyS of Budapest University of Technology and Economics, who notified us of the sample, provided their research and samples, and have continued to work with us. In addition, we wish to thank our colleagues in Symantec Security Response who contributed to this work. This work has been abridged from *W32.Duqu: The Precursor to The Next Stuxnet* [4].

## References

[1] *N. Falliere, L. OMurchu, E. Chien*, "W32.Stuxnet Dossier", February 2011

[2] Personal communication with *Dr. Boldizsar Bencsath*

[3] *A Gostev, I Soumenkov*, "Stuxnet/Duqu: The Evolution of Drivers", December, 2011

[4] N. Falliere, L. OMurchu, E. Chien, "W32.Duqu: The Precursor to The Next Stuxnet", http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf