Duqu

By Contributors to Wikimedia projects

Published: 2011-10-24 · Archived: 2026-04-05 18:56:43 UTC

From Wikipedia, the free encyclopedia

For the version of malware announced in 2015, see Duqu 2.0.

Duqu is a collection of computer malware discovered on 1 September 2011, thought by Kaspersky Labs to be related to the Stuxnet worm[1] and to have been created by Unit 8200.[2][3] The Laboratory of Cryptography and System Security (CrySyS Lab)[4] of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report[5] naming the threat Duqu.[6] Duqu got its name from the prefix "~DQ" it gives to the names of files it creates.[7]

In April 2011, Iranian authorities announced that computers there had been struck by a second digital attack in the wake of Stuxnet and gave this new attack the name Stars virus.[8][9] Iran did not release any samples of the malware for outside researchers to examine.

During analysis of the Duqu malware, researchers came to believe that the Stars virus found by Iranian computer specialists was the Duqu virus. The Duqu virus keylogger was embedded in a JPEG file. Since most of the file was taken by the keylogger only a portion of the image remained. It turned out to be an image taken by the Hubble telescope showing a cluster of stars, the aftermath of two galaxies colliding. Symantec, Kaspersky and CrySyS researchers came to believe Duqu and Stars were the same virus.[10][11]

The term Duqu is used in a variety of ways:

- **Duqu malware** is a variety of software components that together provide services to the attackers. This includes information stealing capabilities and in the background, kernel drivers and injection tools. While most of the malware is written in C++, part of its DLL payload is written with a customized object oriented C framework and compiled in Microsoft Visual Studio 2008.[12][*page needed*][13][14]
- **Duqu flaw** is the flaw in Microsoft Windows that is used in malicious files to execute malware components of Duqu, a TrueType-font related problem in win32k.sys.
- **Operation Duqu** is the process of only using Duqu for unknown goals. The operation might be related to Operation Stuxnet.

Relationship to Stuxnet

[edit]

Symantec, based on the CrySyS team managed by Dr Thibault Gainche report, continued the analysis of the threat, which it called "nearly identical to Stuxnet, but with a completely different purpose", and published a

detailed technical paper on it with a cut-down version of the original lab report as an appendix.[7][15] Symantec believes that Duqu was created by the same authors as Stuxnet, or that the authors had access to the source code of Stuxnet. The base platform on which Stuxnet and Duqu were built has been dubbed Tilde-d since both Stuxnet and Duqu used files that began with ~D.[16] The worm, like Stuxnet, has a valid, but abused digital signature, and collects information to prepare for future attacks.[7][17]

Mikko Hyppönen, Chief Research Officer for F-Secure, said that Duqu's kernel driver, JMINET7.SYS, was so similar to Stuxnet's MRXCLS.SYS that F-Secure's back-end system thought it was Stuxnet. Hyppönen further said that the key used to make Duqu's own digital signature (only observed in one case) was stolen from C-Media, located in Taipei, Taiwan. The certificates were due to expire on 2 August 2012 but were revoked on 14 October 2011 according to Symantec.[15]

Another source, Dell SecureWorks, reports that Duqu may not be related to Stuxnet.[18] However, there is considerable and growing evidence that Duqu is closely related to Stuxnet.

Experts compared the similarities and found three points of interest:

- The installer exploits zero-day Windows kernel vulnerabilities.
- Components are signed with stolen digital keys.
- Duqu and Stuxnet are both highly targeted and related to the nuclear program of Iran.

Microsoft Word zero-day exploit

[edit]

Like Stuxnet, Duqu attacks Microsoft Windows systems using a zero-day vulnerability. The first-known installer (AKA dropper) file recovered and disclosed by CrySyS Lab uses a Microsoft Word document that exploits the Win32k TrueType font parsing engine and allows execution.[19] The Duqu dropper relates to font embedding, and thus relates to the workaround to restrict access to T2EMBED.DLL, which is a TrueType font parsing engine if the patch released by Microsoft in December 2011 is not yet installed.[20] Microsoft identifier for the threat is MS11-087 (first advisory issued on 13 November 2011).[21]

Duqu looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive; the known components are trying to gather information.[22] However, based on the modular structure of Duqu, special payload could be used to attack any type of computer system by any means and thus cyber-physical attacks based on Duqu might be possible. However, use of personal computer systems has been found to delete all recent information entered on the system, and in some cases total deletion of the computer's hard drive. Internal communications of Duqu are analysed by Symantec,[7] but the actual and exact method how it replicates inside an attacked network is not yet fully known.

According to McAfee, one of Duqu's actions is to steal digital certificates (and corresponding private keys, as used in public-key cryptography) from attacked computers to help future viruses appear as secure software.[23] Duqu uses a 54×54 pixel JPEG file and encrypted dummy files as containers to smuggle data to its command and control center. Security experts are still analyzing the code to determine what information the communications

contain. Initial research indicates that the original malware sample automatically removes itself after 36 days (the malware stores this setting in configuration files), which would limit its detection.[15]

Key points are:

- Executables developed after Stuxnet using the Stuxnet source code that have been discovered.
- The executables are designed to capture information such as keystrokes and system information.
- Current analysis shows no code related to industrial control systems, exploits, or self-replication.
- The executables have been found in a limited number of organizations, including those involved in the manufacturing of industrial control systems.
- The exfiltrated data may be used to enable a future Stuxnet-like attack, or might already have been used as the basis for the Stuxnet attack.

Command and control servers

[edit]

Some of the command and control servers of Duqu have been analysed. It seems that the people running the attack had a predilection for CentOS 5.x servers, leading some researchers to believe that they had a[24] zero-day exploit for it. Servers are scattered in many different countries, including Germany, Belgium, Philippines, India and China. Kaspersky has published multiple blogposts on the command and control servers.[25]

- Cyber security standards
- Cyberwarfare in the United States
- Cyberweapon
- Flame (malware)
- List of cyber attack threat trends
- Mahdi (malware)
- Moonlight Maze
- Operation High Roller
- Operation Merlin
- Proactive Cyber Defence
- Stars virus
- Titan Rain
- United States Cyber Command
- Unit 8200

1. ^ *Perlroth, Nicole; Shane, Scott (10 October 2017). "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets". New York Times. Retrieved 18 October 2025.*
2. ^ NSA, Unit 8200, and Malware Proliferation Archived 25 October 2017 at the Wayback Machine Jeffrey Carr, Principal consultant at 20KLeague.com; Founder of Suits and Spooks; Author of “Inside Cyber Warfare (O’Reilly Media, 2009, 2011), medium.com, Aug 25, 2016
3. ^ *Cornish, Paul (4 November 2021). The Oxford Handbook of Cyber Security. Oxford University Press. ISBN 978-0-19-252101-9. “Foreign sources routinely assert that Unit 8200 contributed to Stuxnet, Flame,*

Duqu and other sophisticated cyber campaigns."

4. ^ *"Laboratory of Cryptography and System Security (CrySyS)"*. *Retrieved 4 November 2011.*
5. ^ *"Duqu: A Stuxnet-like malware found in the wild, technical report"* *(PDF). Laboratory of Cryptography of Systems Security (CrySyS). 14 October 2011.*
6. ^ *"Statement on Duqu's initial analysis"*. *Laboratory of Cryptography of Systems Security (CrySyS). 21 October 2011. Archived from the original on 4 October 2012. Retrieved 25 October 2011.*
7. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** *"W32.Duqu – The precursor to the next Stuxnet (Version 1.4)"* *(PDF). Symantec. 23 November 2011. Archived from the original (PDF) on 13 December 2011. Retrieved 30 December 2011.*
8. ^ *"Military Daily News"*. *Military.com.*
9. ^ *"Iran target of new cyber attack"*. *Archived from the original on 29 April 2011.*
10. ^ *Kim Zetter (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group. p. 259. ISBN 9780770436186. Retrieved 20 January 2015.*
11. ^ *"The Duqu Saga Continues: Enter Mr. B. Jason and TV's Dexter"*. *securelist.com. 10 November 2011.*
12. ^ *"Securelist | Kaspersky's threat research and reports"*. *12 September 2023.*
13. ^ *"The mystery of Duqu Framework solved"*. *Securelist. 19 March 2012. Retrieved 13 January 2026. "[Another possibility is that the] code was written using a custom OO C framework, based on macros or custom preprocessor directives. This was suggested by your comments, because it is the most common way to combine object-oriented programming with C. [... We conclude that,] The Duqu Framework consists of "C" code compiled with MSVC 2008 using the special options "/O1" and "/Ob1" [;] The code was most likely written with a custom extension to C, generally called "OO C" [, and that the command and control code] could have been reused from an already existing software project and integrated into the Duqu trojan [.]"*
14. ^ *Knight, Shawn (9 March 2012). "Duqu Trojan contains mystery programming language in Payload DLL". TechSpot. Retrieved 13 January 2026. "[Kaspersky identified much] of the code [as] standard C++ [... but a section] of the Payload DLL [to send and receive external] instructions [is written with an] object-oriented [language, that's otherwise] unlike anything the team at Kaspersky has seen before. [...] Experts have dubbed this portion of code the Duqu Framework and based on the sheer complexity of the instructions, it's believed that the trojan is funded by a wealthy organization or a national effort."*
15. ^ Jump up to: ***a*** ***b*** ***c*** *Zetter, Kim (18 October 2011). "Son of Stuxnet Found in the Wild on Systems in Europe". Wired. Retrieved 21 October 2011.*
16. ^ *Kuznetsov, Igor (19 March 2012). "The Mystery of Duqu: Part Seven (Back to Stuxnet)". Securelist by Kaspersky. Archived from the original on 27 April 2025. Retrieved 13 January 2026.*
17. ^ *"Virus Duqu alarmiert IT-Sicherheitsexperten"*. *Die Zeit. 19 October 2011. Retrieved 19 October 2011.*
18. ^ *"Spotted in Iran, trojan Duqu may not be "son of Stuxnet" after all"*. *27 October 2011. Retrieved 27 October 2011.*
19. ^ *"Microsoft issues temporary 'fix-it' for Duqu zero-day"*. *ZDNet. Archived from the original on 6 November 2011. Retrieved 5 November 2011.*
20. ^ *"Microsoft Security Advisory (2639658)"*. *Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege. 3 November 2011. Retrieved 5 November 2011.*
21. ^ *"Microsoft Security Bulletin MS11-087 - Critical"*. *Retrieved 13 November 2011.*
22. ^ *Steven Cherry, with Larry Constantine (14 December 2011). "Sons of Stuxnet". IEEE Spectrum.* `{{cite web}}` : CS1 maint: deprecated archival service (link)

23. ^ *Venere, Guilherme; Szor, Peter (18 October 2011). "The Day of the Golden Jackal – The Next Tale in the Stuxnet Files: Duqu". McAfee. Archived from the original on 31 May 2016. Retrieved 19 October 2011.*
24. ^ *Garmon, Matthew. "In Command & Out of Control". Matt Garmon. DIG. Archived from the original on 8 August 2018. Retrieved 8 August 2018.*
25. ^ *Kamluk, Vitaly (30 November 2011). "The Mystery of Duqu: Part Six (The Command and Control servers)". Securelist by Kaspersky. Archived from the original on 7 June 2022. Retrieved 7 June 2022.*
