DuQu: Briefing Note

DuQu is a newly discovered malware variant, dubbed “son of Stuxnet”, due to the strong similarities in their architecture and targets. According to the CrySyS Lab in Budapest, Hungary, the original discoverer of DuQu, large sections of the DuQu code are similar to the code of Stuxnet [CrySyS 2011]. A subsequent Symantec report reinforced the similarities in structure and behaviour between DuQu and Stuxnet suggests that DuQu was written by attackers who had access to the Stuxnet source code or even by the Stuxnet authors themselves [Symantec Security Response 2011]. Moreover, DuQu uses an identical driver to inject the main malware module into the target computer. Infected organisations were reported in Iran, Sudan, France, the Netherlands, Switzerland, Ukraine, India and Vietnam.

There are important differences however. The 2010 Kaspersky analysis [Gostev 2011] concluded that Stuxnet consists of the two parts:

- A component responsible for the propagation of the malware (a *carrier platform*),
- A separate module targeting Programmable Logic Controllers (an *attack module*).

According to Kaspersky, the carrier platform of Stuxnet could be reused, for example with a different attack module. But, unlike Stuxnet, DuQu can also be reconfigured remotely to install new malware payloads and to direct attacks at new targets.

The attack module of DuQu, found together with the detected samples was a general purpose keylogger[1] (enriched with some additional spying capabilities) able to perform a reconnaissance in any organisation. However, according to Symantec, the aim of DuQu is to infiltrate organisations operating in industrial environments. This conclusion is based on the fact that the majority of the detected threats were found in industrial infrastructures, and because of the connection to Stuxnet code. Unlike Stuxnet, DuQu is an intelligence gathering tool, apparently aiming to prepare the ground for attacks such as Stuxnet. It should be emphasised, however that there is no direct evidence for the intentions behind DuQu.

The Symantec report shows a highly targeted attack directed at a limited number of organizations and specific assets within them. This is part of a wider pattern of increasingly targeted attacks, threatening intellectual property and critical infrastructures[2]. Targeted attacks on critical infrastructures pose a high risk to society: an important difference in Industrial Control Systems (ICS) malware is the ability to

[1] The name DuQu comes from the fact that the keylogger component saves its data in files with names containing the two letters “DQ”.

[2] For example, a June 2011 Cisco security white paper concludes: “the annualized cybercrime business activity caused by mass, indiscriminate email attacks has declined by more than half. At the same time, the business activity caused by highly-personalized targeted attacks is growing rapidly, tripling in the last year.”

intervene in physical processes, for example (as in the case of Stuxnet), increasing the speed of a centrifuge in a uranium enrichment plant.

Information on the vectors used to install DuQu is still incomplete, although the CrySyS Lab found that the attackers used a specifically targeted email with a Microsoft Word document containing a zero-day kernel exploit. Another instance of the dropper was later identified by Kaspersky Lab. The exploit targets the TrueType font processing kernel component of Windows. Details cannot be published until a patch has been released by Microsoft.

Related ENISA work

The attack draws attention to the importance of securing critical networked infrastructures and industrial control systems. In 2011/Q1 2012, ENISA will publish a study on ICS protection focusing on European systems[3]. The report identifies over 100 threats, risks and challenges for ICS protection as well as providing a survey of existing pan-European and international ICS security initiatives. This study was performed through research and consultation with all stakeholders involved.

The ENISA study reveals that Europe's critical infrastructures are still not sufficiently prepared for attacks like DuQu. In particular, Europe lacks specific initiatives and policies to address ICS security. There are no commonly adopted ICS security standards, guidelines or regulations, corporate management is not sufficiently involved, and there are numerous technical vulnerabilities.

The study proposes seven major recommendations for securing ICS, which call for the development of pan-European and national ICS strategies, preparation of good practices, security plan templates, awareness raising, test beds/maturity frameworks as well as ICS CERTs and fostering research.

References

- Laboratory of Cryptography of Systems Security (CrySyS). "DuQu: A Stuxnet-like malware found in the wild, technical report", 14 October 2011, retrieved from http://en.wikipedia.org/wiki/DuQu (accessed December 5, 2011).
- Symantec Security Response. "W32.DuQu: The precursor to the next Stuxnet." 2011.
- Gostev, Alexander (Kaspersky Lab). *The Mystery of DuQu: Part One.* October 20, 2011. http://www.securelist.com/en/blog/208193182/The_Mystery_of_DuQu_Part_One (accessed November 10, 2011).

[3] "Protecting Industrial Control Systems. Recommendations for Europe and Member States" to be released, Dec, 2011.