# Duqu 2.0: Reemergence of an aggressive cyberespionage threat

symantec.com/connect/blogs/duqu-20-reemergence-aggressive-cyberespionage-threat

June 9, 2015

Symantec Official Blog

Attackers use new version of Duqu worm in ambitious attacks against telecoms, electronics and even information security sectors.

By: Symantec Security ResponseSymantec Employee

- Created 10 Jun 2015
- : 日本語, 한국어

- 0
- 0

Duqu 2.0, the cyberespionage tool that was used to compromise security firm Kaspersky Lab, has also been used in a number of other attack campaigns against a range of targets, including several telecoms firms. Analysis by Symantec concurs with Kaspersky's assessment today that Duqu 2.0 (detected by Symantec as W32.Duqu.B) is an evolution of the older Duqu worm, which was used in a number of intelligence-gathering attacks against a range of industrial targets before it was exposed in 2011. Although their functionalities were different, the original Duqu worm had many similarities with the Stuxnet worm used to sabotage the Iranian nuclear development program.

**New attacks**

Symantec has found evidence that Duqu has been used in a number of different attack campaigns against a small number of selected targets. Among the organizations targeted were a European telecoms operator, a North African telecoms operator, and a South East Asian electronic equipment manufacturer. Infections were also found on computers located in the US, UK, Sweden, India, and Hong Kong.

In addition to the attack against itself, Kaspersky believes Duqu was used to target countries involved in international negotiations surrounding Iran's nuclear program. Given the diversity of targets, Symantec believes that the Duqu attackers have been involved in multiple cyberespionage campaigns. Some organizations may not be the ultimate targets of the group's operations, but rather stepping stones towards the final target. The group's interest in telecoms operators could be related to attempts to monitor communications by individuals using their networks.

Symantec has found no evidence to suggest that it has been affected by attacks using this malware.

**Duqu 2.0 in operation**

This new version of Duqu is stealthy and resides solely in the computer's memory, with no files written to disk. It comes in two variants. The first is a basic back door that appears to be used to gain a persistent foothold inside the targeted entity by infecting multiple computers.

The second variant is more complex. It has the same structure as the first, but contains several modules that provide a range of functionality to the malware, such as gathering information on the infected computer, stealing data, network discovery, network infection, and communication with command-and-control (C&C) servers. This variant appears to be deployed to computers deemed to be targets of interest by the attackers.

**Common code and code flow**

Duqu and Duqu 2.0 share large amounts of code, in addition to similarities in how that code is organized. The shared code includes a number of helper functions. For example, as shown in Figure 1, there is a "gen_random" function (as labelled by an engineer) that is shared between Duqu and Duqu 2.0.

Not only is that gen_random code shared, but the code that calls that function is also organized almost identically. Such similarities in how code is called is repeated in several other locations throughout Duqu 2.0, including in how C&C IP addresses are formatted, how network messages are generated, and how files are encrypted and decrypted.

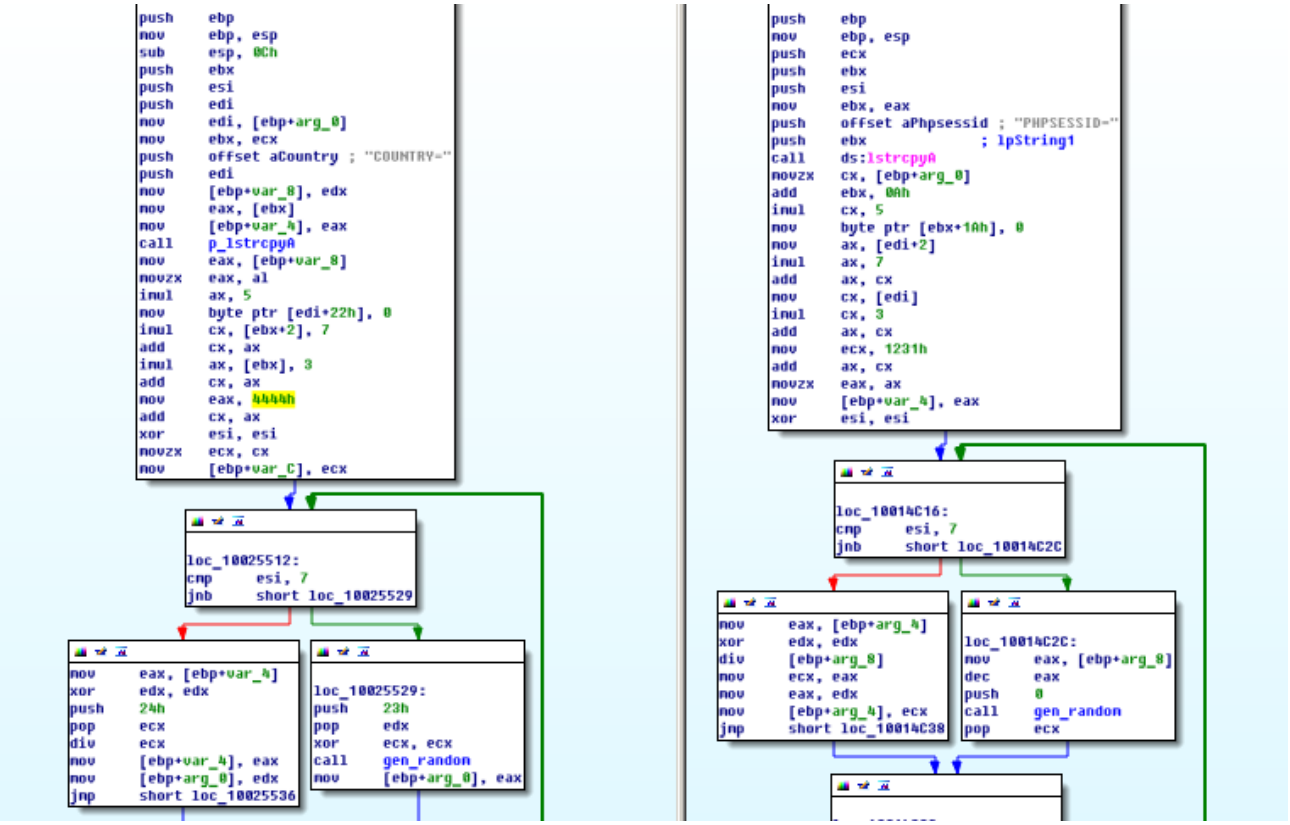


*Figure 1. Duqu vs Duqu 2.0 code flow*

When a program needs to store data, the program author will design structures to store that data in a logical and easily accessible manner. Duqu and Duqu 2.0 share a number of these data structures.

**Network communications**

Another shared feature between the two variants, as shown in Figure 1, is the use of a cookie header with a hardcoded string and a random string when sending messages to a C&C server. For example:

- Duqu: Cookie: PHPSESSID=<random_str_0x1A_size>
- Duqu 2.0: Cookie: COUNTRY=<random_str_0x1A_size>

A second shared feature in the network communications code is to connect to a number of Microsoft URLs to retrieve a proxy address, as shown in Figure 2.

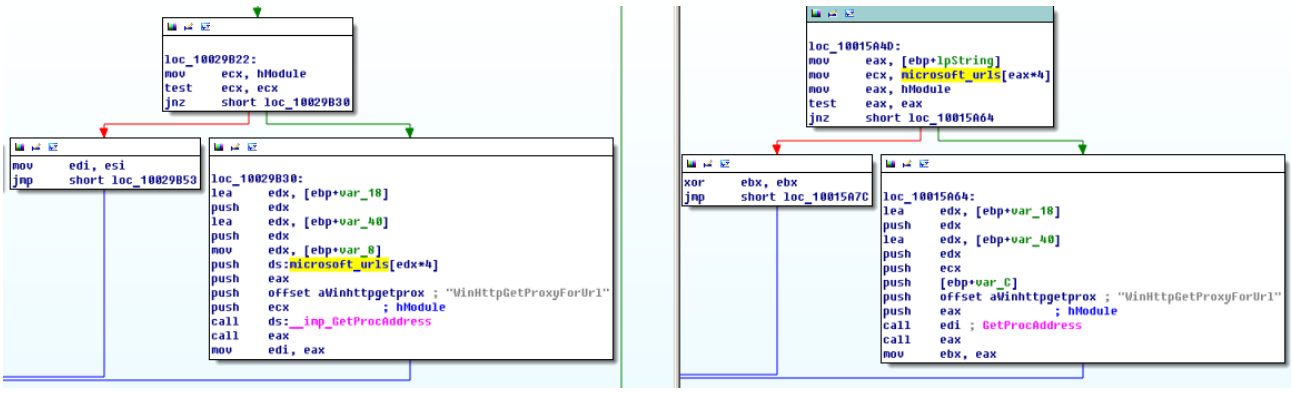

*Figure 2. Duqu vs Duqu 2.0 network code*

The list of Microsoft URLs connected to, by both variants, is identical.

Finally, for network communications, when Duqu uses HTTP, it will use image names in the "Content-Disposition" header. For Duqu, the value "DSC00001.jpg" was used, whereas for Duqu 2.0, the value "%05d.gif" is used.

**Conclusion**

Based on our analysis, Symantec believes that Duqu 2.0 is an evolution of the original threat, created by the same group of attackers. Duqu 2.0 is a fully featured information-stealing tool that is designed to maintain a long term, low profile presence on the target's network. Its creators have likely used it as one of their main tools in multiple intelligence gathering campaigns.

Given that activity surrounding the original version of Duqu dropped off following its discovery, it is likely that the group may now retreat before re-emerging with new malware.

**Protection**

Symantec and Norton products detect this threat as:

W32.Duqu.B