# The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns

securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/

By GReAT

Earlier this year, during a security sweep, Kaspersky Lab detected a cyber-intrusion affecting several of our internal systems.

Following this finding, we launched a large scale investigation, which led to the discovery of a new malware platform from one of the most skilled, mysterious and powerful groups in the APT world – Duqu. The Duqu threat actor went dark in 2012 and was believed to have stopped working on this project – until now. Our technical analysis indicates the new round of attacks include an updated version of the infamous 2011 Duqu malware, sometimes referred to as the stepbrother of Stuxnet. We named this new malware and its associated platform "Duqu 2.0".

Some of the new 2014-2015 Duqu infections are linked to the P5+1 events and venues related to the negotiations with Iran about a nuclear deal. The threat actor behind Duqu appears to have launched attacks at the venues for some of these high level talks. In addition to the P5+1 events, the Duqu 2.0 group has launched a similar attack in relation to the 70th anniversary event of the liberation of Auschwitz-Birkenau.

In the case of Kaspersky Lab, the attack took advantage of a zero-day in the Windows Kernel, and possibly up to two other, currently patched vulnerabilities, which were zero-day at that time. The analysis of the attack revealed that the main goal of the attackers was to spy on Kaspersky Lab technologies, ongoing research and internal processes. No interference with processes or systems was detected. More details can be found in our technical paper.

From a threat actor point of view, the decision to target a world-class security company must be quite difficult. On one hand, it almost surely means the attack will be exposed – it's very unlikely that the attack will go unnoticed. So the targeting of security companies

indicates that either they are very confident they won't get caught, or perhaps they don't care much if they are discovered and exposed. By targeting Kaspersky Lab, the Duqu attackers probably took a huge bet hoping they'd remain undiscovered; and lost.

At Kaspersky Lab, we strongly believe in transparency, which is why we are going public with this information. Kaspersky Lab is confident that its clients and partners are safe and that there is no impact on the company's products, technologies and services.

## Duqu 2.0 – Indicators of Compromise (IOCs)

### MD5s

**Action loaders:**

089a14f69a31ea5e9a5b375dc0c46e45
16ed790940a701c813e0943b5a27c6c1
26c48a03a5f3218b4a10f2d3d9420b97
a6dcae1c11c0d4dd146937368050f655
acbf2d1f8a419528814b2efa9284ea8b
c04724afdb6063b640499b52623f09b5
e8eaec1f021a564b82b824af1dbe6c4d
10e16e36fe459f6f2899a8cea1303f06
48fb0166c5e2248b665f480deac9f5e1
520cd9ee4395ee85ccbe073a00649602
7699d7e0c7d6b2822992ad485caacb3e
84c2e7ff26e6dd500ec007d6d5d2255e
856752482c29bd93a5c2b62ff50df2f0
85f5feeed15b75cacb63f9935331cf4e
8783ac3cc0168ebaef9c448fbe7e937f
966953034b7d7501906d8b4cd3f90f6b
a14a6fb62d7efc114b99138a80b6dc7d
a6b2ac3ee683be6fbbbab0fa12d88f73
cc68fcc0a4fab798763632f9515b3f92

**Cores:**

3f52ea949f2bd98f1e6ee4ea1320e80d
c7c647a14cb1b8bc141b089775130834

### C&C IPs

182.253.220.29
186.226.56.103

To check your network for Duqu's 2.0 presence, you can also use the open IOC file available here.