# CYBER-SPAWN DUQU 2.0: WAS MALWARE INFECTION ‘PATIENT ZERO’ MAPPED?

Kaspersky Lab reported this morning a next-generation version of Duqu malware infected the information security company’s network.

Duqu is a known reconnaissance malware. Its complexity suggests it was written by a nation-state. The malware appears closely affiliated with the cyber weapon malware Stuxnet.

WSJ reported this particular version may have been used to spy on the P5+1 talks with Iran on nuclear development. Dubbed ‘Duqu 2.0,’ the malware may have gathered audio, video, documents and communications from computers used by talk participants.

Ars Technica reported in depth on Kaspersky’s discovery of the malware and its attributes. What’s really remarkable in this iteration is its residence in memory. It only exists as a copy on a drive at the *first* point of infection in a network, and can be wiped remotely to destroy evidence of its occupation.

The infosec firm killed the malware in their networked devices by mimicking a power outage. They detached from their network suspect devices believed to contain an infecting copy.

Kaspersky’s Patient Zero was a non-technical employee in Asia. Duqu 2.0 wiped traces of its own insertion from the PC’s drive.

Neither WSJ or Ars Technica noted Kaspersky's network must have been subject to a program like TREASUREMAP.

> …Because the rest of the data remained intact on the PC and its security patches were fully up to date, researchers suspect the employee received a **highly targeted spear phishing e-mail** that led to a website containing a zero-day exploit. … (bold mine – source: Ars Technica)

How was a single non-technical point of contact in Asia identified as a target for an infected email?

Targeting did more than identify a non-technical person. Collection and analysis of users' activities earmarked a singular useful tool.

Duqu's team had to find the one person in a infosec company like Kaspersky who'd be careless or stupid enough to open a phishing email…

OR they had to know how to prepare an email so that it would appear safe on sight…

OR they inserted HUMINT in the one place screened as suitable for a plant and infection.

Duqu's cousin Flame was a reconnaissance software, too. Perhaps it was dispatched earlier to gather info, wiped, then Duqu 2.0 followed.

But the possible pre-infection target mapping may remain unknown, if early reconnaissance malware also wiped up in the same manner as Duqu 2.0.

Marcy's post this morning shares an important concern related to Duqu 2.0's implementation. Some entity mapped OPM, identifying all current and near-term former federal employees. Now this entity can identify which targets are best for Duqu 3.0.

Mapping could have been prevented several ways, had DHS, OPM, and Congress taken their roles and

the nature of cyber warfare security seriously during the Bush administration. (Somewhere Richard Clarke chuckling darkly over a hot cup of coffee this morning…)

The U.S. government collaborated on cyber weapon creation, without adequate consideration to long-term repercussions.

Other government agencies and the public know more now about this new threat because Kaspersky was open with its own exposure and with its findings. Risk reduction techniques can be improved because Kaspersky was willing to share this information.

Public exposure of cyber attacks also has a deterrent effect, as seen with Flame; the malware "suicided" after media reports.

Duqu's current reconnaissance operations are scary enough. Imagine next not an inert Duqu, but a focused Stuxnet 3.0 launched on the private sector – likely beginning with suppliers linked to federal employees.

Imagine businesses and individuals unable to defend themselves because they could not request by FOIA government-held information about cyber attacks.

Should the public accept exposure to a next-gen Duqu 3.1 or 4.0 because Sen. Richard Burr insisted on greater opacity in undead CISA?