VAPOROUS VOIDS: QUESTIONS REMAIN ABOUT DUQU 2.0 MALWARE

The use of stolen Foxconn digital certificates in Duqu 2.0 gnaws at me, but I can't put my finger on what exactly disturbs me. As detailed as reporting has been, there's not enough information about this malware's creation. Nor is there enough detail about its targeting of Kaspersky Lab and the P5+1 talks with Iran.

Kaspersky Lab carefully managed release of Duqu 2.0 news – from information security firm's initial post and an op-ed, through the first wave of media reports. There's surely information withheld from the public, about which no other entities know besides Kaspersky Lab and the hackers.

Is it withheld information that nags, leaving vaporous voids in the story's context? Possibly.

But there are other puzzle pieces floating around without a home, parts that fit into a multi-dimensional image. They may fit into this story if enough information emerges.

Putting aside how much Duqu 2.0 hurts trust in certificates, how did hackers steal any from Foxconn? Did the hackers break into Foxconn's network? Did they intercept communications to/from Foxconn? Did they hack another certificate authority?

If they broke into Foxconn, did they use the

same approach the NSA used to hack Syria – with success this time? You may recall the NSA try to hack Syria's communications in 2012, by inserting an exploit into a router. But in doing so, the NSA bricked the router. Because the device was DOA, the NSA could not undo its work and left evidence of hacking behind. The router's crash took out Syria's internet. Rapid recovery of service preoccupied the Syrians so much that they didn't investigate the cause of the crash.

The NSA was ready to deny the operation, though, should the Syrians discover the hack:

> …Back at TAO's operations center, the tension was broken with a joke that contained more than a little truth: "If we get caught, we can always point the finger at Israel."

Did the NSA's attempted hack of Syria in 2012 provide direction along with added incentive for Duqu 2.0? The failed Syria hack demonstrated evidence must disappear with loss of power should an attempt crash a device – but the malware must have adequate persistence in targeted network. NSA's readiness to blame Israel for the failed Syria hack may also have encouraged a *fuck-you* approach to hacking the P5+1 Iran talks.

WIRED's Kim Zetter noted Taiwan as a common factor among other recent malware attacks relying on certificates. If the hackers broke into Foxconn, did they also break into other equipment manufacturers located in Taiwan at the same time, or using the same approach?

Which might make one wonder if hackers used a cut to an undersea cable serving Taiwan to that end. Such submarine communication line cuts have increased in number over the last handful of years. Cable APCN-2 experienced two major disruptions between March 2014 and February 2015, characterized as cuts or fiber breaks, though the cable is supposed to have self-

healing capabilities.

The installation of a new undersea cable (APG) serving East Asia also offered an opportunity for access, perhaps during installation. This cable's service began in 3Q2014, ahead of the Foxconn certificate theft, believed to have happened in early 2015.

And what of Foxconn's information security? Hackers known as SwaggSec broke into the company in late 2011/early 2012, stealing a large quantity of corporate information to post online. Didn't this breach encourage better security? Or were employees compromised after their information had been released online?

Electronic device manufacturers and certificate authority companies had already been on notice about lax security since 2012. A nation-state-sponsored hack was blamed for the theft of 200 certificates that year after discovery of Duqu 1.0. Considering the increase in malware attacks using stolen certificates since 2011, it seems odd certificates weren't more secure.

All these unanswered questions about Duqu 2.0 combined with other dangling disconnects leave me still curious, but uneasy.