A TALE OF TWO MALWARE RESEARCHERS: DOJ PRESENTED EVIDENCE YU PINGAN KNEW HIS MALWARE WAS USED AS SUCH

The government revealed the arrest in California of a Chinese national, Yu Pingan, who is reportedly associated with the malware involved in the OPM hack.

The complaint that got him arrested, however, has nothing to do with the OPM hack. Rather, it involves four US companies (none of which are in the DC area), at least some of which are probably defense contractors.

> Company A was headquartered in San Diego, California, Company B was headquartered in Massachusetts, Company C was headquartered in Los Angeles, California, and Company D was headquartered in Arizona.

Yu is introduced as a "malware broker." But deep in the affidavit, the FBI describes Yu as running a site selling malware as a penetration testing tool.

> UCC #1 repeatedly obtained malware from YU. For example, on or about March 3, 2013, YU emailed UCC #1 samples of two types of malware: "adjesus" and "hkdoor." The FBI had difficulty deciphering adjesus, but open source records show that it was previously sold as a penetration testing tool (which is what legitimate security researchers call their hacking. tools) on

> the website penelab.com.5 Part of the coding for the second piece of malware, hkdoor, indicated that "Penelab" had created it for a customer named "Fangshou."6 Seized communications and open source records show that YU ran the penelab.com website (e.g., he used his email address and real name to register it) and that UCC #1 used the nickname "Fangshou."

For that reason — and because Yu was arrested as he arrived in the US for a conference — a few people have questioned whether a fair comparison can be made between Yu and Marcus Hutchins, AKA MalwareTech.

It's an apples to oranges comparison, as DOJ rather pointedly hasn't shared the affidavit behind Hutchins' arrest warrant, so we don't have as much detail on Hutchins. That said, Hutchins' indictment doesn't even allege any American victims, whereas Yu's complaint makes it clear he (or his malware) was involved in hacking four different American companies (and yet, thus far, Yu has been accused with fewer crimes than Hutchins has).

In any case, at least what we've been given shows a clear difference. Over a year before providing Unindicted Co-Conspirator 1 two more pieces of malware, the complaint shows, UCC #1 told Yu he had compromised Microsoft Korea's domain.

> YU and UCC #1 's communications include evidence tying them to the Sakula malware. On or about November 10, 2011, UCC #1 told YU that he had compromised the legitimate Korean Microsoft domain used to download software updates for Microsoft products. UCC #1 provided the site http://update.microsoft.kr/hacked.asp so YU could confirm his claim. UCC #1 explained that he could not use the URL to distribute fraudulent updates, but the compromised site could be used

> for hacking attacks known as phishing.

So unlike in Hutchins' case, DOJ has provided evidence (and there's more in the affidavit) that Yu knew he was providing malware to hack companies.

Indeed, unless the government has a lot more evidence against Hutchins (more on that in a second), it's hard to see why they've been charged with the same two crimes, Conspiracy to violate CFAA and CFAA.