THE KRONOS NEEDLE IN THE ALPHABAY HAYSTACK

To set up a future post (see my earlier posts here and here), I want to show how remarkable it is that the Feds decided to prosecute Marcus Hutchins, a guy who allegedly contributed code to a piece of malware sold in June 2015 for $2,000 on AlphaBay, out of all the illicit sales they might have chosen to prosecute in the month after taking the site down.

First, let's look at the Alexandre Cazes indictment, sworn by a Fresno Grand Jury on June 1, 2017, 41 days before the Hutchins indictment. It lists the following illicitly sold goods.

- Redacted month 2015, redacted vendor sells a false driver license to an undercover officer in CA
- Redacted month 2015, redacted vendor sells an ATM skimmer to an undercover officer in CA
- Redacted month 2015, redacted vendor sells an ATM skimmer to an undercover officer in CA
- December 29, 2015, vendor CC4L sells marijuana to MG, an undercover officer, which is mailed from Merced to Buffalo
- Redacted short month date 2016, redacted vendor sells marijuana to an undercover officer, which is mailed

from Los Angeles to a redacted city

- Redacted month 2016, redacted vendor sells a false driver license to an undercover officer in CA
- Redacted month 2016, redacted vendor sells a false driver license to an undercover officer in CA
- Redacted month 2016, redacted vendor sells a false driver license to an undercover officer in CA
- May 16, 2016, vendor A51 sells heroin to an undercover officer, which is mailed from Brooklyn to Fresno
- May 24, 2016, vendor A51 sells heroin to an undercover officer, which is mailed from Brooklyn to Fresno
- October 20, 2016, vendor BSB sells heroin and fentanyl to an undercover officer, which is mailed from San Francisco to Fresno
- Redacted (short month) date 2017, redacted vendor sells meth to an undercover officer, which is mailed between two CA cities

The sale of a piece of malware for $2,000 on June 11, 2015 would be earlier than most of those listed in the indictment that brought

AlphaBay's operator down. And while there are several ATM skimmers listed (a violation of 18 USC 1029) there is no malware listed (in two of Hutchins' charges listed as violations of 18 USC 1030, the CFAA statute).

Now look at the overall numbers FBI boasted for AlphaBay when it announced its takedown on July 20, nine days after the indictment targeting Hutchins.

> AlphaBay reported that it serviced more than 200,000 users and 40,000 vendors. Around the time of takedown, the site had more than 250,000 listings for illegal drugs and toxic chemicals, and more than 100,000 listings for stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services. By comparison, the Silk Road dark market—the largest such enterprise of its kind before it was shut down in 2013—had approximately 14,000 listings.
>
> The operation to seize AlphaBay's servers was led by the FBI and involved the cooperative efforts of law enforcement agencies in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, along with the European law enforcement agency Europol.
>
> "Conservatively, several hundred investigations across the globe were being conducted at the same time as a result of AlphaBay's illegal activities," Phirippidis said. "It really took an all-hands effort among law enforcement worldwide to deconflict and protect those ongoing investigations."

Of the 40,000 vendors charged within a month of takedown, of the 250K drug listings and the 100K

fraudulent services listings, the guy who sold Kronos once for $2,000 (whom Tom Fox-Brewster thinks might be a guy named VinnyK) — and by virtue of American conspiracy laws, Hutchins — were among the first 20 or so known to be charged for using AlphaBay.

Admittedly, we're seeing EDCA's sales in Cazes' indictment because they had the lead on the overall takedown. Perhaps EDWI has 1,000 more malware buys it will get around to charging, as soon as its perpetrators decide to come to the US, as Hutchins did.

But put in this light, it looks even more remarkable how quickly they got around to arresting to the alleged co-conspirator of a guy who sold a piece of malware.