MALWARETECH'S FBI-INDUCED TOUR TO MILWAUKEE, WI

On Friday, WannaCry hero Marcus Hutchins (AKA MalwareTech) was granted bail by a Las Vegas judge; he will pay his bail on Monday, then have to travel, without a passport to show TSA, to Milwaukee for a court appearance Tuesday (I'm contemplating hopping the ferry for the hearing).

I'd like to focus on the venue, how it is that a British malware researcher came to be charged in Flyover USA for the crime of making malware.

Thomas Brewster-Fox wrote an important piece on Friday trying to figure out what a lot of people have been asking: what is Kronos, which a lot of researchers never really heard of. He notes that the malware was a bust in the criminal malware market.

> The reduced price hints at another truth about Kronos: it was largely a failure amongst serious cybercriminals. There was early anticipation in 2014 it could go big, as prolific and profitable as one of its forbears, the banking malware known as Zeus. In an email to your reporter from RSA's Daniel Cohen in 2014, he wrote: "Waiting to see whether Kronos turns into something. At this point it's just a post on a forum, no sample or binary yet. It could be an interesting development if it does, as it would point to more movement away from the Zeus code."
>
> In the last 24 months, according to IBM global executive security advisor Limor Kessem, the Trojan emerged with a hefty $7,000 price tag in mid-2014, but actual attacks didn't launch until the third and fourth quarter of 2015, when the company saw some Kronos malware

> campaigns hitting UK banks. “But after that timeframe, have not seen much more activity from the malware,” Kessem told *Forbes*.
>
> “The very last time we saw Kronos activity was a small campaign in November 2016, when Kronos infected a very small number of machines mostly in Brazil, the UK, Japan, and Canada. At that particular time, we did not see fraudulent activity from Kronos, but rather, believe it was used a loader for other malware.

Importantly, IBM global executive security advisor Limor Kessem names the few places where the malware *has* been deployed: Some UK banks in the last two quarters of 2015 and then, in altered form and function, in a “very small number of machines” in Brazil, UK, Japan, and Canada.

So: UK, Brazil, UK, Japan, and Canada.

Not the US, as far as Kessem notes.

And in fact, the most commonly cited victim, the UK, is where Hutchins is from! Yet among the things the British National Cyber Security Centre — the folks who worked closely with Hutchins as he saved a bunch of NHS hospitals from being shut down due to the WannaCry malware — has been really circumspect about since Hutchins’ arrest is what the case is doing over here in the States.

> We are aware of the situation. This is a law enforcement matter and it would be inappropriate to comment further.

So why are we seeing this case in the US — in Milwaukee, of all places?!?! — rather than in the UK where some of its few victims are?

The indictment against Hutchins includes just two actions he is alleged to have taken personally.

> Defendant MARCUS HUTCHINS created the Kronos malware. (¶4a)
>
> [snip]
>
> In or around February 2015, defendants MARCUS HUTCHINS and [redacted] updated the Kronos malware. (¶4d)

All the other overt actions described in the indictment were done by Hutchins' as yet unknown (even to him, per reports!) and still at-large co-defendant. That includes this action:

> On or about June 11, 2015, defendant [redacted] sold *a version* of the Kronos malware in exchange for approximately $2,000 in digital currency. [emphasis mine]

Most the other charges — counts three through six — cite that June 11 sale. So it's that sale, in which Hutchins was not alleged to be involved and the alleged perpetrator of which hasn't yet been arrested, that seems to be the core of the crime.

This Beeb article, by far the most detailed accounting of Hutchins' arraignment, provides these details.

> Prosecutors told a Las Vegas court on Friday that Mr Hutchins had been caught in a sting operation when undercover officers bought the code.
>
> They claimed the software was sold for $2,000 in digital currency in June 2015.
>
> Dan Cowhig, prosecuting, also told the court that Mr Hutchins had made a confession during a police interview.
>
> "He admitted he was the author of the code of Kronos malware and indicated he sold it," said Mr Cowhig.
>
> The lawyer claimed there was evidence of chat logs between Mr Hutchins and an

> unnamed co-defendant — who has yet to be arrested — where the security researcher complained of not receiving a fair share of the money.

From this, it might be safe to assume that some law enforcement officer, possibly working undercover in the Eastern District of WI, bought a bunch of shit off AlphaBay in 2015, including a copy of (a version of) the Kronos malware. The purchase (and the version of code) wasn't sufficiently interesting last year to arrest Hutchins when (I believe) he came for the Las Vegas cons.

Nor was it interesting enough to the UK, where some of Kronos' few victims are, to prosecute the sale (which, because conspiracy laws are not as broad as they are here in the US, might not have reached Hutchins in any case, and certainly wouldn't have exposed him to decades of incarceration).

But this year, in the days after the Alpha Bay seizure (and several months after Hutchins helped to shut down WannaCry), prosecutors presented that $2000 sale to a grand jury in ED WI, after which an arrest warrant was sent out to Las Vegas, just in time to arrest Hutchins on his way out of the country, after most the unruly hackers had departed from Las Vegas.

Arresting Hutchins only as he left — and playing whack-a-mole moving him from one detention center to another — gave authorities the opportunity to interview Hutchins without an attorney, where — prosecutor Dan Cowhig claims, Hutchins "made a confession," — not that he "created the Kronos malware," which is what the indictment alleges, but instead that he "was the author of the code of Kronos malware." That "confession" sounds like the kind of thing an overly helpful person might explain if asked to explain this tweet in circumstances where he didn't have a lawyer.

MalwareTech 
@MalwareTechBlog

Just found the hooking engine I made for my blog in a malware sample. This is why we can't have nice things, fuckers.

4:34pm · 7 Feb 2015 · Twitter Web Client

So here's what may be going on.

In the aftermath of the AlphaBay seizure, authorities in the US decided to wade through what they could charge from past purchases off the marketplace, and either remembered or stumbled on this remarkably minor sale. Perhaps because of Hutchins' fame, or perhaps because someone is unhappy about Hutchins' fame, it was prioritized in a way it otherwise would not have been. And, as always, the US used convenient travel as a way to nab foreign alleged hackers to pull into America's far more onerous than its allies criminal justice system.

It's not even clear, however, that that explains the Milwaukee venue. Recall that DOJ first charged Pyotr Levashov (and therefore first deployed its now legally sanctioned Rule 41 warrant) for the Kelihos botnet in Alaska, even though he'll be tried in CT if he's ever extradited to the US. The FBI reorganized the way they investigate cyber crimes in 2014 (no longer tying the investigation to the geography of the crime) and with Rule 41 and international crimes, they'll be able to do so far more in the future. But at least with Levashov, there were victims referenced in the complaint, whereas here, the only act that may have taken place in ED WI is that purchase, if it even did.

All that said, the venue is a far less interesting question than whether the FBI really has evidence tying Hutchins to intending his code to be used for malware, or if they've just made a horrible mistake.