THE UK'S NEW REVOLVING DOOR HACKER PROSECUTION

Given that I talk a lot about Lauri Love and Marcus Hutchins' treatment vis a vis the UK's willingness to ship them to the US to be tried for hacking charges that could be tried at home, I wanted to flag what happened to Daniel Kaye, who got extradited back to his native UK to face charges of launching attacks with the Mirai botnet.

His extradition to the UK is actually a return trip, after having been shipped to Germany to face charges there in February.

> Kaye, meanwhile, was arrested on February 22 at London-area Luton Airport by the NCA at the request of Germany's BKA (see *British Cops Bust Suspected German ISP Mirai Botnet Hacker*). In March, he was extradited to Germany.
>
> Appearing last month at a court in Cologne, Kaye pleaded guilty to infecting 1.25 million Deutsche Telekom routers with Mirai malware. He also pleaded guilty to launching attacks designed to infect devices with Mirai malware for the purpose of selling stresser/booter services – aka distributed denial-of-service attacks.
>
> [snip]
>
> Last month, Kaye was given a suspended sentence – of one year and eight months – by the German court after he pleaded guilty to related charges, characterizing what he'd done as being "the worst mistake of my life," Agence France Presse reported.

Now Kaye is being extradited back home to face

charges he attack Lloyds, too.

> Kaye is due to appear Thursday in Westminster Magistrates' Court in London to face nine charges against him under the U.K. Computer Misuse Act, as well as two charges of blackmail and one relating to possession of criminal property, an NCA spokesman tells Information Security Media Group.
>
> Kaye has also been charged with having allegedly "endangered human welfare with an alleged cyberattack against Lonestar MTN," which is the biggest internet provider in the West African coastal republic of Liberia, which has a population of nearly 5 million, NCA says (see *Liberia Latest Target for Mirai Botnet*).
>
> The NCA says it filed charges against Kaye following a complex investigation that involved assistance from Germany's BKA, the Federal Criminal Police Office of Germany.

So … arrest in the UK, sent to Germany to receive a suspended sentence there, now shipped back home to face even more charges.

Here's why that's interesting, though:

> [S]ecurity experts say Kaye has also been tied to attacks launched by a hacker who has used the handles "Peter Parker," "Spiderman," "BestBuy," "Popopret" and "Spidr," and that he also appears to be the author of the remote-access Trojan and keylogger called GovRAT.
>
> *Security firm InfoArmor says GovRAT has been sold on darknet forums since 2014.*

You don't have to be a dummy to ask why Germany

was willing to let this guy go back to the UK, to face another set of charges that don't, however, reach to his alleged extensive involvement in creating the tools other hackers use.

In his July post reporting on Kaye's suspended sentence, Brian Krebs noted that no one has gone after the authors of the Mirai botnets yet.

> In January 2017, this blog published the results of a four-month investigation into who was likely responsible for not only for writing Mirai, but for leaking the source code for the malware — spawning dozens of competing Mirai botnets like the one that Kaye built. To my knowledge, no charges have yet been filed against any of the individuals named in that story.

Shortly after that, though, Krebs wrote a post successfully IDing Kaye, noting a lot of the things alluded to in the Kaye article, as well as Spider's ties to the Israelis who attacked his own site.

> Interestingly, both of these email addresses — parkajackets@gmail.com and spdr01@gmail.com — were connected to similarly-named user accounts at vDOS, for years the largest DDoS-for-hire service (that is, until KrebsOnSecurity last fall outed its proprietors as two 18-year-old Israeli men).

He also included the curious detail that Spider — Kaye — had been accused of sharing his access to the vDOS database when he traveled overseas.

> The technical support logs from vDOS indicate that the reason the vDOS database shows two different accounts named "bestbuy" is the vDOS administrators banned the original "bestbuy" account after it was seen logged into the account from both the UK

> and Hong Kong. Bestbuy's pleas to the vDOS administrators that he was not sharing the account and that the odd activity could be explained by his recent trip to Hong Kong did not move them to refund his money or reactivate his original account.

All of which is to say that Kaye appears to have been deep in a number of other key networks, on top of attacking banks in two countries with Mirai. Which probably explains why Kaye has been on such an interesting revolving door trip through two of Europe's legal systems, all for charges that don't get at a fraction of the stuff he is alleged to have been involved with.