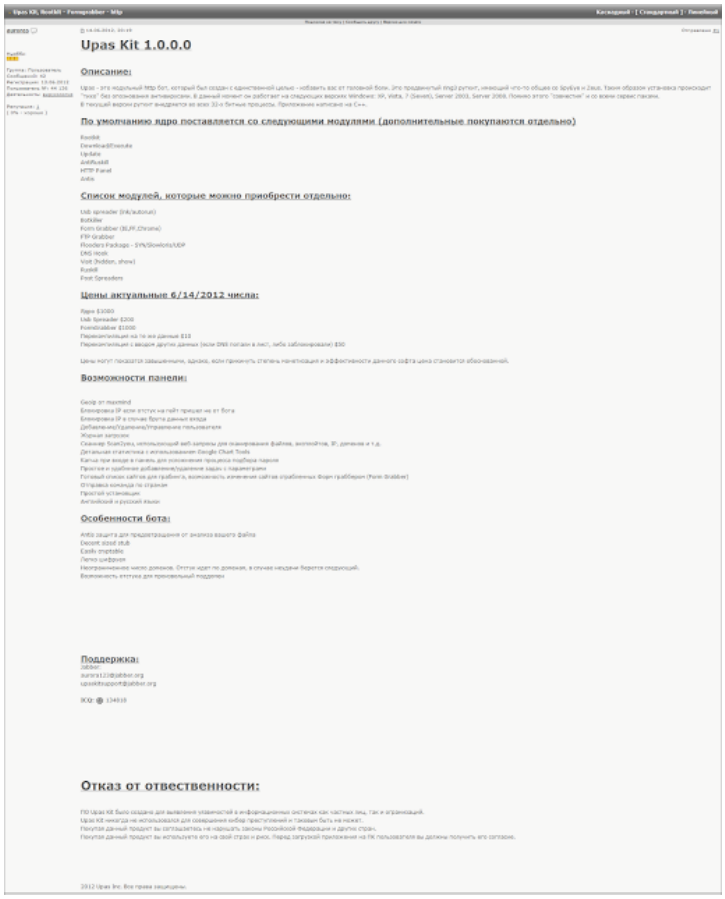
DOJ'S MINOR DESPERATION WITH MALWARETECH

Best as I can tell (this is way not my forté – this was done with the help of S – so please recreate my work), this screen shot shows "auroras" selling UPAS Kit 1.0.0.0 on June 14, 2012.



June 14, 2012 was before Marcus Hutchins turned 18.

Some of the Russian translates as:

> Upas is a modular http bot, which was created for the sole purpose – to save you from a headache. This is an advanced ring3 rootkit that has something in common with SpyEye and Zeus. Thus, the installation is "quiet" without recognition by antiviruses.Currently it works on the following versions of

> Windows: XP, Vista, 7 (Seven), Server 2003, Server 2008. In addition, it is "compatible" with all service packs.
>
> [snip]
>
> The Upas Kit was created to identify vulnerabilities in information systems of individuals and organizations.
>
> Upas Kit has never been used to commit cyber crimes and it can not be so.
>
> Buying this product, you agree not to violate the laws of the Russian Federation and other countries.
>
> Buying this product, you use it at your own risk. Before downloading the application to the user's PC, you must obtain its consent.

The support address is aurora123@jabber.org. This matches the UPAS Kit described in Marcus Hutchins' superseding indictment.

> "UPAS Kit" was the name given to a particular type of malware that was advertised as a "modular HTTP bot." UPAS Kit was marketed to "install silently and not alert antivirus engines." UPAS Kit allowed for the unauthorized exfiltration of information from protected computers. UPAS Kit allowed for the unauthorized exfiltration of information from protected computers. UPAS Kit used a form grabber and web injects to intercept and collect personal information from a protected computer.

All of which is to say that when the superseding indictment describes the following as overt acts in the conspiracy to violate CFAA and to wiretap, it describes code placed on sale before Hutchins turned 18.

> On or about July 3, 2012, [VinnyK],

> using the alias “Aurora123,” sold and distributed UPAS Kit to an individual located in the Eastern District of Wisconsin in exchange for $1,500 digital currency.

Now, as I said yesterday, it’s not clear what UPAS Kit is doing in the superseding indictment. Alone, the coding behind the listing above necessarily happened while Hutchins was a minor and the sale itself happened over five years ago. So the government can only present it as part of a conspiracy sustained by more recent overt acts, like the sale of Kronos in 2015, arguing they’re part of the same conspiracy, which extends the tolling (but doesn’t change Hutchins’ birthday).

Given the claim that he lied to the FBI in his Las Vegas interrogation, however, I think they’re suggesting that when he admitted to coding a form grabber, but not the one in Kronos, he was lying about knowing that this earlier code got used in Kronos.

> Chartier: So you haven’t had any other involvement in any other pieces of malware that are out or have been out?
>
> Hutchins: Only the form-grabber and the bot.
>
> Chartier: Okay. So you did say the form-grabber for Kronos, then?
>
> Hutchins: Not the form-grabber for Kronos. It was an earlier one released in about I’m gonna say 2014?

In other words, to get this admission into trial, the government is going to claim he was lying about knowing there was continuity between UPAS and Kronos in a way to deny any more recent involvement, even though they’re on the record (though Dan Cowhig’s statements to the court) that he had admitted that.

Which further suggests the evidence they have

that he actually coded Kronos itself isn’t that strong, and need to rely on code that Hutchins coded when he was a minor to be able to blame this malware on him.