# Mythbusting: Anti-Virus Research considered dangerous

Posted on **August 18,2017** by **sanna**

Everyone doing research in information security or doing any work in this field takes some risks. Since most of the „cyber stuff“ is black magic to others not working in this context, there are a lot of problems and severe misunderstandings. The Crypto Wars still haven't been decided in favour of mathematics. Real people prefer end-to-end encryption over insecure communication all of the time. Proposals of severely damaging information security for all of us by using sanctioned malicious software are still being debated in parliaments. Backdoors, covert or otherwise, are no line of any defence, as many military strategists will readily tell you. Marcus Hutchins was in the news recently, because of claims that he developed a strand of malware tied to attacks on financial institutions. While you can debate all you want about the charges, this case has the potential to set a dangerous precedent for information security researchers. This is why we have translated the article titled *Anti-Virus-Spezialisten werden von US-Justiz kriminalisiert* written by Erich Möchel:

# Anti-Virus Specialists criminalized by US Justice

## Marcus Hutchins, who has put a stop to the "WannaCry" outbreak through a risky action, will be brought to court this week in Wisconsin. His "criminal offenses" are so incompetently formulated that according to the indictment every security investigator would have one foot in jail.

The arrest of British security expert Marcus Hutchins a week ago, including the charge of production and distribution of Trojan malicious software in the US, has triggered a real shock wave in the industry. The "offenses" listed in the indictment are formulated in such a way that "*all security researchers of anti-virus companies have one foot in US prison"* said Viennese security technician Michael Kafka to ORF.at.

Since then, "good" hackers ("white hats") - mainly from Great Britain - have stopped to co-operate with government agencies. Because Hutchins case demonstrates, how a "white hat" can quickly get caught in the crossfire at a time when state actors and malware criminals ("black hats") are less and less distinguishable. Hutchins (23) achieved world fame at the end of 2016, when he stopped the devastating outbreak of the "WannaCry" software single-handed in a risky action.

### Criminals, Cops, Agents, Security Researchers

The arrest of Hutchins on his return from the security conference DefCon in Las Vegas a week ago is apparently due to the raid on the infamous illegal website AlphaBay, which disappeared a few weeks ago from the TOR network. The site was frequented mainly by criminals of all kinds, the rest of the audience consisted of covert investigators, agents of various secret services, and security researchers.

*"That Whitehats are getting patterns of malicious software through such sites, and then testing them in lab environments, is simply part of their work. It is also important to share the findings with other security researchers and to discuss them in order to develop counter-measures. Especially Marcus was known to share his results very freely, and this accusation was apparently constructed from it“*, says Michael Kafka.

**A Trojan Video**

Kafka has been interested in Hutchin's work since 2013, he also met him during the 44CON security conference in the autumn of 2016 in London for a lengthy exchange of ideas. In the indictment, Hutchins is accused ,among other things, of writing the Trojan "Kronos" in 2014 and producing an instructional video. Both claims are especially ridiculous because of the fact that instructional videos for malicious software are virtually never made by criminals, but always by their antagonists.

At the time between the middle of 2014 and the summer of 2015, to which the indictment refers for several similar "offences", the then 20-year-old Hutchins has already been a new shooting star of the worldwide security scene. Hutchins' work had contributed significantly to rendering the Botnet "Caberp"harmless – a Botnet attributed to notorious Russian criminals – and have it thoroughly analysed.

**Expert shakes his Head in Disbelief**

*"No criminal would put the the results of analysis of malicious software up for public discussion"*, Kafka said and shook his head in disbelief: *"Criminals do the opposite. Public attention is ruinous for their business, which is based on undetected security gaps. And for this very reason there never has been the slightest suspicion that Marcus could work for the other side."* However, Hutchins openness could have caused his downfall, because one of the charges obviously refers to his work on so-called "rootkits", malicious software for the camouflage of an espionage Trojan.

Apparently, unknowns used a few routines of his malicious software demonstration for their purposes, Hutchins himself publicly announced in an angry tweet in 2015. Such malware demos of security researchers are only isolated modules of a malicious software suite, the code of which is modified for demonstration purposes to explain its operating principle. From a technical point of view, this software is used to modify malicious software, which by itself can not be used to do anything bad.

**The Charge in Wisconsin**

Now this turned into a count of an indictment in the US state of Wisconsin, where another defendant resides, with which Hutchins had then communicated via AlphaBay. He is said to have offered a version of the lesser-known Trojan "Kronos" for sale, which contained modified elements of Hutchins code. Therefore, absurdly, Hutchins is now accused of being the author of the "Kronos" malware - which originates from the circle of Russian criminals - and of being involved in the sale. At the time, Hutchins was involved in the takedown of another large Botnet.

It's rather likely that the enraged tweet mentioned above was directed at this unknown communication partner on AlphaBay, when Hutchins realized that his modified "hooking engine" had been built into malware by criminals. A "hooking engine" is a code for an entry point in an operating system to execute commands thereon. The possible applications for such an auxiliary software are numerous.

**How "WannaCry" was stopped**

The fact that Hutchins, in general, handled malware in a nonchalant way with a hands-on approach was shown in the case of "WannaCry". On the day of the outbreak of the "WannaCry" worm, which paralysed in particular control computers for medical devices of British hospitals in series and brought logistics centres and production plants to a halt, Hutchins had quite quickly received a copy. When he first skimmed over the code, he found an

Internet domain open in the code, which was not assigned and which, without further ado, he registered in his name.

*"This was a very risky action. In the middle of such a malware explosion to be seen as the owner of a central element of this attack, is not everyone's cup of tea,"* says Kafka.

*"The installation of the malicious software in an isolated network would have been the safe way to work out what the function of this domain was. But that would have taken several hours."* By performing the same action in the wild, Hutchins, to his own amazement, had hit the "emergency stop switch" of the "WannaCry" software. The command-control servers, which directed the outbreak, regularly queried this domain. When it was suddenly no longer free, "WannaCry" stopped its own distribution.

**„WannaCry“ & „Petya“, Courtesy NSA**

*"Such a 'killswitch' is a clear indicator of governmental malicious software, which usually also includes de-installation routines. To remove traces is paramount to state actors. For Criminals, on the other hand, this tends to be a minor matter"* Kafka continued. *The WannaCry worm* (malicious software that replicates itself in order to spread to other computers is called a "worm") *came with an encrypted exploit for a capital Windows security gap, which captured computer in the infected net in a flash."*

**NSA Malware hit the NATO Partners**

The same or another military "cyber" group used NSA's malicious software to shake the UKs healthcare system, pharmaceutical companies and logistics companies from Scandinavia ("WannaCry"), and then the energy supply of the Ukraine ("Petya"). It seems Hutchins has directly landed himself in a "cyber" skirmish between East and West. Therefore, other reasons than mere incompetence of US prosecutors, who can not even distinguish between black and white, might be involved in his arrest a week ago in Las Vegas.

Hutchins was released from prison in Las Vegas on Tuesday, but now he has to go to court in Wisconsin, where the unknown co-defendant, who made windy deals with small criminals over the allegedly so impenetrable "Darknet",is imprisoned.

**More on this Topic**

- One of the first security investigators who have stopped to cooperate with state organs was the well-known British Whitehat Kevin Beaumont
- The Prosecution against Marcus Hutchins
- Hutchin's work on the Caberp-Botnet that made him known in 2013

Posted in:High Entropy,Internet,Security Intelligence,Stories |
Tagged:Cybercrime,Justice,Law,Malware,NSA,Research,WannaCry | With 0 comments