Research Methods and Professional Practice January 2022

« Collaborative Learning Discussion 1

Kin Wong

Initial Post

5 days ago

1 reply

Last now

About the case of malware disruption, the service provider, Rogue Service, achieves its slogan "cheap, guaranteed uptime, no matter what" and allows whatever the clients are hosting on the website. Rogue Service even enables some customers who host their website with spam and malware to use their Service to get businesses.

Nowadays, every user won't only use one machine to access their data or the internet—for example, only a laptop. Users will use many devices, such as tablets, smartphones, and different IoT. They also connect the internet in different ways, from traditional LAN/WAN connection to public WiFi, Bluetooth, 4G and 5G, etc. Also, users will access the same file on a shared application, which is installed across different devices (IEEE, 2016)

The service provider allows the customers to spread their malware and spam to affect the whole community. For example, a compromised device with malware is synchronised with the cloud account. Other devices of the user will be affected after synchronisation; if the compromised machine is shared within users, other users will be affected once logged in and using the shared software. Furthermore, network sharing, email attachments, wireless sharing (Bluetooth, airdrop) will then spread out the malware to everyone with the internet or the virtual online communities (IEEE, 2016). This may cause a serious data loss and disruption of society's daily life, as people are relying on IT devices heavily nowadays.

According to the Computer Misuse Act 1990 (CPS, 2017), the retailed companies may be prosecuted by making and spreading the malware; but as the service provider provides a platform for these companies to spread this malware, and the service provider fully understand what they are doing, but no actions are taken. Therefore, the service provider may be included as part of the "criminal group", under this circumstance.

References:

1 1. A. Alexeev, D. S. Henshel, M. Cains and Q. Sun, "On the malware propagation in heteroge-
neous networks," 2016 IEEE 12th International Conference on Wireless and Mobile Computing,
Networking and Communications (WiMob), 2016, pp. 1-5, doi: 10.1109/WiMOB.2016.7763252

2. Crown Prosecution Service (2019). *Cybercrime - Prosecution Guidance | The Crown
Prosecution Service*. [online] Cps.gov.uk. Available at: https://www.cps.gov.uk/legal-
guidance/cybercrime-prosecution-guidance.

Reply

1 reply

1　　Post by **Jan Küfner**

now

peer response

> Since the company has chosen a place where legal prosecution is comparably
> low, I would argue that the company and their managers will not face legal ac-
> tions in the near future. Since they also have clearly shown that they do not have
> any ethics in place, since they do not have regard for public privacy, security and
> wellbeing, another entity was forced to step in to stop their operation. This entity
> a coalition of security companies and government organization used a worm to
> disrupt their operation by deleting data. Whilst the deletion of data of one entity is
> unethical, it can to my opinion nonetheless be argued, that by protecting the se-
> curity and wellbeing of many others the overall operation is nonetheless ethical.
> Especially since the coalition tried to limit collateral damage their worm will
> cause. BCS (2021), ACM (N.D.)
>
> References
>
> BCS (2021) Code of Conduct for BCS Members. Available from:
> https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 25 January
> 2022].
>
> ACM (N.D.) Case: Malware Disruption. Available from:
> https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption
> [Accessed 25 January 2022].

Reply　　**Edit**　**Delete**

Maximum rating: -

Add your reply

Your subject

Type your post

Dateien auswählen | Keine ausgewählt

Submit   Use advanced editor and additional options

OLDER DISCUSSION   NEWER DISCUSSION

Initial Post   Initial Post