Digital forensics is crucial to the security chain

By Simon Campbell-Young

6 Nov 2018

The past decade has seen developments in technology that were previously unimagined. Businesses around the globe are increasingly reliant on the internet and other technologies that keep them connected to their customers, supply chains and crucial business applications.

Simon Campbell-Young is CEO of MyCybercare and Managing Director of Credence Security

However, while these technologies have brought significant benefits in terms of productivity and efficiency, they have also become tools for cybercriminals to steal money and information.

Cybercrooks use technology to breach networks to exfiltrate valuable data or damage systems. They also use sophisticated tools to hide their malfeasance and to evade detection.

This has resulted in the IT department having to employ new solutions to detect malicious activity and mitigate the damage.

Where does digital forensics come in?

The ability to root out and track illegal activities has become an integral part of the security chain, and this is where digital forensics come in. These tools help to investigate fraudulent activity and conduct a thorough analysis to expose the criminals and hopefully retrieve any stolen information.

Many think of forensics as a bunch of people in white coats taking swabs at crime scenes. In reality, it is quite different. It

involves the application of forensic tools to recover, scrutinise and analyse of masses of data and logs to uncover what has happened and to track and build a case against the perpetrators of online fraud.

Not an easy task

Digital forensics is not without its challenges. The collection, classification, evaluation and analysis of digital evidence is a highly complex process, requiring digital tools and technologies.

Remember, today it's seldom about a standalone PC. We have complex networks, multiple services, connected devices, and of course the cloud, which has significantly added to the complexity of the exercise.

Moreover, all these sources and infrastructure can be spread over multiple locations and jurisdictions, and with that, a variety of rules and regulations governing them.

There will also be the question of duplicate and modified data, and mountains of other information that simply isn't relevant to the investigation, but still needs to be looked at. Sometimes it's a case of finding the proverbial needle in the haystack.

What next?

The first step is identifying, collecting and producing all the data that is stored electronically, which, due to its sheer volume, is an onerous task, he says. Following this, digital forensics, which means analysing and recovering data from the plethora of devices such as servers, smartphones, wearables, printers, PCs, laptops - any device that stores electronic information.

Then there is securely storing all this information to avoid tampering and to follow the letter of the law in the jurisdiction in question. Any tampering or mishandling of this data could ruin the entire investigation.

Once all the information has been captured, stored and preserved, the true process of analysis can take place. This is done by forensic professionals who use highly specialised skills and tools to extract the relevant information from the data. Doing this manually would be impossible, so sophisticated algorithms and tools are employed to drill down into the data and retrieve the desired information. Then a case can be properly built.

There's no doubt that cybercriminals are using increasingly complex and sophisticated tools to carry out their evil deeds and avoid getting caught. However, even these tools leave a digital trail that a digital forensics professional can follow to identify them, and possibly even recover stolen assets, Campbell-Young concludes.

ABOUT SIMON CAMPBELL-YOUNG

Having started his career as a startup partner for FSA Distribution in 1990, Simon Campbell-Young went on to start his own company called Memtek Distribution in 1995. This was sold to a public company called Siltek Holdings between 1998 to 2000. Shortly thereafter, he took his experience in the technology sector, garnered over more than 23 years, to form specialist distribution company Phoenix Distribution in 2000.

- Adding threat intelligence to the security mix - 26 Nov 2018
- Digital forensics is crucial to the security chain - 6 Nov 2018
- App permissions can be used to exploit your data - 26 Oct 2018
- 57 million riders, drivers affected by Uber breach - 13 Dec 2017
- Prevention through awareness - 12 May 2014

View my profile and articles...