BIZCOMMUNITY

Cyber security professionals are no Darth Vader

By Simeon Tassev

19 Mar 2019

Cybercrime is undoubtedly a growing problem, and the costs involved are significant. The cybersecurity industry is therefore also growing to meet the threat head-on.

Simeon Tassev, managing director at Galix

The terms ‘white hat’, ‘black hat’ and ‘grey hat’ have emerged to describe the various players in the field. Those in the cybersecurity industry are known as white hats and those on the ‘dark side’ are the black hats. Those who continue to operate as cybersecurity professionals while dabbling in the criminal underworld are known as grey hats and are perceived to be a growing threat. The reality though is that the vast majority of cybersecurity professionals are no ‘Darth Vader’, and are unlikely to be swayed to the ‘dark side’.

A recent report released by Malwarebytes, entitled “White Hat, Black Hat and the Emergence of the Grey Hat; The True Costs of Cybercrime”, highlights that “a significant proportion of security professionals are suspected of being “grey hats” – those who continue as security practitioners while also getting involved in cybercrime.”

The report also states that globally, “one in 22 security professionals are perceived to be grey hats”, and “12% of security professionals admit to considering participation in black hat activity, 22% have actually been approached about doing so, and 41% either know or have known someone who has participated in this activity.”

Is money the main motivator for dabbling in cybercrime?

These statistics seem to be alarming, but in truth the problem is not what it appears to be. Money is often cited as the main motivator for dabbling in cybercrime, but this is not necessarily the whole picture. Generally, the skills and capabilities required to successfully participate in cybercrime activities are high level and take many years to acquire. These types of senior cybersecurity experts are in short supply and are therefore highly sought after and well paid.

In addition, the pay-out from cybercrime is nowhere near as inflated as Hollywood portrays it to be. And while it may be true that many cybersecurity professionals have participated in so-called grey hat activity, the vast majority back out quickly. The fear of getting caught, as well as the realisation that criminal activities are still working, without significant pay-out, often causes a rapid return to the 'light'.

The motivation to dabble in criminal activity is therefore not driven by money alone. In many instances, those who turn to cybercrime are doing it for the challenge or the thrill. Certain personality types will always be drawn to the 'bad', much like Anakin Skywalker was drawn to the dark, and they are easily influenced to make their transformation to the dark side complete. This happens regardless of their industry and is not specific to cybersecurity and cybercrime.

Cybercrime is seldom driven by desperation, but more frequently by curiosity, boredom, unhappiness or the need to prove something. The key to curbing the threat of the grey hat is to first clearly define the laws around what constitutes cybercrime activities. There are many blurred lines, and crimes that previously did not exist was due to the fact that the technology previously did not exist. These loopholes are what grey hats take advantage of and hide behind, and they need to be eliminated so they can no longer be exploited.

Highly skilled 'jedi' like employees need to be challenged and paid well to prevent them from straying from the 'light side', and laws need to be put into place across typical jurisdictional boundaries to govern cybercrime activities on a global scale. With tangible fines and potential jail time involved, more people will think twice before straying into the grey areas.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...