INSEAD
The Business School for the World®

KNOWLEDGE

The Professionalisation of Cyber Criminals

Opportunistic hackers are taking advantage of the maturing dark web markets and Cybercrime-as-a-Service business model to professionalise their activities.

Once confined to the darkest corners of the internet and executed by experts with deep technical knowledge (often driven by ideology or an appetite for challenge), cybercrime has matured to become a business sector driven by consumer demand, and competitive development of quality goods and services. Just as the ongoing digitisation of business activities has lead legitimate companies to fuse digital and operational strategies, criminals are also adapting their approach. Like any industry, cybercrime periodically goes through change in paradigms, the latest one has been the development of the "Cybercrime-as-a-Service" (CaaS) framework.

Greater maturity means that market transparency and depth have improved. Corporate employees can now sell their corporate login credentials for several thousand dollars. Individuals can purchase hacking software, with demo sites, online support and training, for a few hundred dollars. A modest subscription will ensure that you receive the monthly updates. Cryptocurrencies such as Bitcoins are increasingly common but continue to evade traceability. Market resiliency has also improved. When Silkroad, the eBay of illegal activities, was taken down by law enforcement agencies, Agora, **AlphaBay** and other dark markets stepped in to offer comparable services. It is doubtful at this point that any arrest will lead to significant long term market disruption.

A professional hacking industry

CaaS is both a Business-to-Business (B-to-B) and Business-to-Consumer (B-to-C) industry. On the B-to-B side, maturity has led to a greater integration across "business" functions and greater technical specialisation. Experts on money laundering, drug trafficking and **hacking** collaborate much more effectively, while cyber-jacks-of-all-trades have been replaced by specialists in system penetration, network exploration or data extraction. The advanced persistent threat (APT), a long term tactic combining different means (such as social engineering, intelligence or Trojan horse) is no longer the prerogative of cyberwarfare. Last year the **Carbanak** series of attacks had exactly the same features, long term intrusion and lateral movements within the information system, before harvesting significant proceeds, leading to a collective loss of $1 billion from banks.

The underground part of the internet (known as the "dark web") can deliver industrial grade products, while dual-use products are freely available on the "surface" web. **RAT software,** for example, which allows remote system administrators to control

machines under their responsibility, has created opportunities for hackers to illegally take over machines without proper credentials.

Legitimate developments in the Information Technology (IT) industry are also replicated in the dark web. Cloud computing has become a ubiquitous way of delivering high quality IT services built on three types of products: Software-as-a-Service which provides applications that can be easily deployed; **Platform-as-a-Service** which offers development tools for IT specialists; and Infrastructure-as-a-Service which enables the efficient use of hardware. These capabilities have been adapted for hacking purposes. For example, would-be hackers can obtain ready-to-use software that allows them to deny access to site or system (a so-called DDOS attack) for a few hundred dollars. Developers have the capacity to easily customise malwares (hostile or intrusive software), such as SpyEye, to fit their specific needs. And, unscrupulous access providers offer the capacity to spam on a massive scale (the so-called "**bulletproof hosting**"). At the time of its service termination, McColo customers were allegedly responsible for two-thirds of the global **spam volume**. More generally, many botnet managers rent their zombie computers armies for any criminal purposes.

Anyone can do it

On the B-to-C side, products that are advertised on the dark web are increasingly easy to use and generally do what they say they do. Although the underground market is still subject to numerous scams, it has reached a surprisingly good level of self-regulation. Trust rating systems have emerged and actors sometimes behave with an unexpected level of "ethics". When Agora closed down, alleging security reasons, it apparently gave users advance notice so that they could withdraw their bitcoins stored in the market escrow.

All these developments have changed the business environment for legitimate organisations. External threats are more common. Just a few years ago, hacking costs were sufficiently high so that only high value targets were likely to be victims of cyber-attacks. With the reduction in cost instead of asking "why me?" firms ought to nw be asking "why not me". Internal threats are also more prevalent. A disgruntled employee could put intellectual property worth $15 million on the web, not for profit but for retribution. Until recently that would have required a high level of technical sophistication. This is no longer needed.

Large firms in sensitive sectors have been able to keep up with recent developments in cyber-crime. This is much less the case for smaller firms and start-ups. Part of the solution is probably technological in nature. Better cooperation with law enforcement agencies can also help. However, no matter how carefully planned these answers are, they will inevitably fail, often at the worse moment. Managerial solutions such as **out-boarding programmes** can complement a more technical approach by focusing on the human element. Ultimately, realising the existence of these threats and **planning for contingencies** may be the most effective way of dealing with them.

Gilles Hilary is The Mubdala Chaired Professor of Corporate Governance and Strategy at INSEAD. Christophe Durand is INTERPOL's central point of contact for cyber strategy.

*Follow INSEAD Knowledge on **Twitter** and **Facebook***

Find article at
https://knowledge.insead.edu/blog/insead-blog/the-professionalisation-of-cyber-criminals-4626