Cyber Espionage in the Caribbean Risks and Challenges[1]

Cyber espionage is the use of computers to gain access to critical and confidential information residing on personal, business, or government computers or networks. Access to the information is unauthorised, obtained by stealth, in most cases without the user knowing and in others, finding out after the fact. The susceptibility to cyber espionage arises because these computers or networks are either connected to each other on a private network or to the internet. Generally speaking, however, the risk is associated with connection to the internet. Cyber espionage manifests as threats to the security of the target computer or network. The likelihood that a threat would occur is determined by the value of the target network. Initially, it was thought that the Caribbean was immune from attack as the perpetrators focussed primarily on governments in developed countries. Later this transitioned to an increase in economic espionage as consumer online activity increases.

Rise in Risk Exposure

The disinterest in the Caribbean was set to change with increased connectivity to the internet. By 2016, the Caribbean and Latin America was identified as the fourth largest mobile market in the world.[2] In addition, regional governments are transitioning to

---

1 M. Georgia Gibson Henlin, QC

2 Cybersecurity Are we Ready in Latin America and the Caribbean - Joint Report – IDB OAS

online platforms as a means of providing services to their citizenry. Hackers have now set their sights on the Caribbean since 2012 - 2013:

> It must not be overlooked, however, that our increasing connectivity to and dependency on internet based platforms and services has significantly raised our risk exposure – that of our citizens, commercial enterprises, and governments – to a host of security and crime related actors and activities. The available data clearly indicates that cyber-attacks and incidents particularly those carried out with criminal intent, are increasing in frequency and sophistication… It is now widely understood that cybercrime does not recognise national borders, and that a multilateral and multi-dimensional effort is required to address the range of cyber threats…[3]

The attacks initially focussed on individuals by offering them incentives, or other opportunities for wealth transfer in exchange for either visiting a website, updating personal information or claiming prizes or large inheritances from their oil rich uncle or other unknown relative in Bahrain or on the African contact.[4] Other instances, include the installation of malicious code on the target network or device. The Dominican Republic reported 963 cases of phishing in 2013, as well as 432 cases of banking data theft from 2009-2014.[5]

Since 2013, the threats expanded to governments, financial institutions, and utility and communications companies. In Jamaica[6] there was a spate of attacks against

---

3 *Ibid* at IX

4 Phishing

5 *Ibid* at Page 70. The internet penetration is 50% of the population.

6 *Ibid* at Page 86 – The internet penetration is 40% of the population.

government websites[7] as also in Guyana.[8] The attackers in one case claimed to be ISIS. In Barbados, the Government's information Service website was specifically targeted for attack in June 2015.[9]

The Tools

The tools that enable this unauthorised access are the same in most cases except where there is insider activity. These tools have names such as phishing, spearing phishing, denial of service attacks, distributed denial of service attacks malware attacks and insider activity. There are more sophisticated methods such as unauthorised port scans,[10] vulnerability scans[11] and brute force attacks.[12] Through the use of these tools, the hackers take a strategic or systematic approach to stealing data or information from their target. The tool utilised depends on whether the hacker's immediate or ultimate goal is to test the system for vulnerability or exfiltrate data. Service providers report that these are detected on a daily basis across the region. It is difficult to provide statistical information as companies fear reputational harm.

Cyber Espionage as Unauthorised Access

---

7 Ibid - 2014

8 Ibid 2013 - 2014

9 There is 77% internet penetration

10 This occurs where a hacker sends messages or packets to the target device in order to determine the programme or services being run as part of his/her reconnoitering or surveillance activities.

11 Computer software or programmes that search for weaknesses that may be exploited by the hacker.

12 These are unscientific methods of attempting to get access to networks and computers, often described as "trial & error"

A review of life cycle models relative to an attack demonstrates that aspects of cyber espionage falls squarely within conduct prohibited by cybercrimes legislation across the region.[13] The attack starts with social engineering or the automated gathering of information about the target. In these instances, the hacker either sends emails containing malware which when executed can collect information. The hacker furthers his objective by escalating privileges and thereafter extracts the files. The extracted files are either used for the hacker's benefit or sold on the dark web or otherwise to the detriment of the victim.

Transnational, Anonymous & Enforcement

Most of the literature focus on preparedness in terms of security and institutional framework including legislation. Probably with good reason because the decentralised structure and philosophy of privacy and anonymity underlying internet fosters cyber espionage. In other words, cyber espionage capitalises and thrives in this environment because neither physical presence nor contact are required. This reality makes enforcement difficult if not, at least for now, impossible. The activities transcend national borders and currently originates mainly from geographically external sources. It is difficult to trace the perpetrators of these threats. In some cases they are traced to as far afield as Nigeria. The consequence is that there are difficulties of enforcement even though most of the countries in the Caribbean have legislation similar to Jamaica's

13 For Example: Jamaica, Trinidad, The Bahamas, St. Lucia

Cybercrimes Act, 2015 that prohibit unauthorised access or modification of computers and greater penalties for critical infrastructure.

The difficulty with detection and enforcement, commends an approach that is directed at prevention and security such that more resources may definitely be needed to curb the risk posed by these attacks. Caribbean governments are now engaged in various cyber awareness campaigns modelled off the ITU think click surf campaign.[14] The realities makes prevention and security and attractive alternative.

[14] Jamaica, Curacao and Barbados