CYBERSECURITY IN THE NEW PARADIGM

INTRODUCTION

Cyberattacks have increasingly become critical threats against which we must safeguard. Individuals, businesses, and societies must appreciate the dangers of cyber threats and work together to secure our assets.

Hackers believed to be affiliated with Russia recently targeted the US Treasury and Commerce department, Microsoft, Cisco, Intel, and FireEye (a cybersecurity service provider). Despite being at the forefront of cybersecurity and having access to sophisticated systems, these organisations were not impervious to attacks.

Hackers have proven to be extremely creative in their attacks. SolarWinds'[1] network and application monitoring platform, Orion, was recently attacked by a group of hackers who distributed trojanised[2] updates to SolarWinds' customers. Through those updates, the hackers created backdoors named 'SunBurst' in SolarWinds's client systems, which were a covert method of bypassing normal authentication in systems so that an attacker can download data or even upload more malware etc.

SolarWinds' customers include more than 400 companies of the US Fortune 500, the top ten US telecom companies, the top five US accounting firms, all branches of the US Military[3], the Pentagon, the State Department, as well as hundreds of universities and colleges worldwide. The list of cyber victims of this attack was staggering, and it has been suspected that this hacking attack was not merely for financial gain but also for political power.

Singapore, as an important financial hub in Asia, would be an attractive target for cyberattacks. As recently as 2018, hackers breached SingHealth's database and stole the personal data of 1.5 million patients, including PM Lee's.

The following paints a fictional scenario of a possible attack on Singapore inspired by the SolarWinds hacking incident:

D-DAY 30

A hacker group is preparing a massive attack on multiple organisations in Singapore, both public and private. They are highly trained, well-funded by a foreign government, and have gathered information on the targeted systems for the last months. Some government bodies' systems have already been compromised. As a result, the hacker group had successfully extracted classified information from the military and diplomatic service. This work was not just done remotely, as the hacking group had enlisted the help of spies based domestically in Singapore to help. They had also made plans to compromise the PCs of the public by infiltrating anti-virus programs to create a fleet of zombie PCs.

D-DAY 7

Simultaneously, the hacking group has successfully got the unsuspecting man on the street to install the rootkit embedded in free versions of software programs, i.e., Windows, Microsoft Office. Coupled with compromised anti-virus programs, the fleet of zombie PCs has been growing daily. All of these zombie PCs will be the source of Distributed Denial-Of-Service (DDOS) attack, whereby a flood of internet traffic to a targeted system is sent, in order to bring the system down on D-day.

D-DAY

The planned DDOS attack starts, and many banks, insurance companies and government agencies are affected. The cybersecurity response teams at these organisations immediately start defence protocols and try to remediate the attacks. However, the DDOS attack was a smoke operation.

The main target was Singapore's infrastructure – her power plants, water treatment facility, airport and port. There was huge panic in Singapore as traffic lights ceased to work, and there was disarray on the streets. All scheduled flights were cancelled, and flights which were waiting for landing were left to circle in the air. All operations were also stopped at the port. Meanwhile, the hacker group also exposed sensitive diplomatic information to Singapore's neighbours, which will cause serious political conflict.

D-DAY +7

After one week, most of the public infrastructure was restored, and people have gone back to their normal routine. However, Singapore made significant financial losses because of the 1-day cybersecurity attack on its public and key private organisations. More importantly, Singapore's global reputation and status as a financial, air and sea hub in Asia have been badly damaged.

[1] SolarWinds provides computer networking monitoring services to corporations and government agencies around the world and has become a dominant player since it was founded in 1999.
[2] A trojan horse is a type of malicious code or software that looks legitimate but can take control of your computer.
[3] Including the National Nuclear Security Administration (NNSA), which manages the nuclear programme for the US government.

HOW DO WE SAFEGUARD AGAINST CYBERATTACKS?

A good practice of cyber hygiene is essential, including keeping the operating system (OS) updated and patched and enabling firewall and endpoint protection. Also, one should use authentic software to update security patches regularly and enforce strong passwords and change this regularly. It is important for companies to educate employees on cybersecurity and conduct regular training on a corporate level, especially to prevent attacks via phishing emails. Organisations should also consider investing in third-party penetration testing audits to uncover potential vulnerabilities and secure the organisation's systems. Humans are not only the weakest link in this security paradigm but also the main attack vector in the whole scheme of things.

That said, it is equally important to prepare and build up the people, processes, and technologies required for an intelligence-based cybersecurity program so that organisations can consume, interpret, and apply intelligence on cyber threats to protect their information, systems, capabilities, and their activities against threats.

CONCLUSION

We may not be able to prevent all future hacking attempts. However, our efforts will make it harder for hackers to penetrate our systems, and we can also deter some of their attempts. When we recognise and appreciate that cybersecurity is everyone's responsibility, we will take the necessary steps to improve our chances at withstanding the ever-evolving cyberattack landscape.

Written by

Yurae Kim, Associate, BDO Cybersecurity

CONTACTS

CECIL SU
Director, Cybersecurity
+65 6829 9629
cecilsu@bdo.com.sg

GERALD TANG
Business Development Lead, Cybersecurity
+65 6828 9167
geraldtang@bdo.com.sg