BREACH & ATTACK SIMULATION

RECAPPING THE LARGEST CYBER TRENDS OF 2018 & PREDICTIONS FOR 2019

By Eyal Wachsman, Co-Founder & CEO of Cymulate

CYMULATE

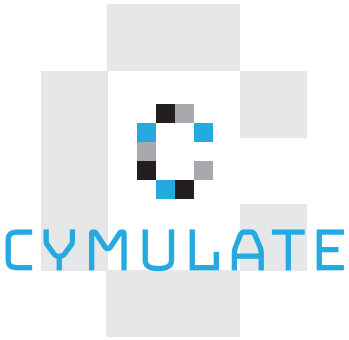

TABLE OF CONTENTS

GLOSSARY

APPI	Japanese Act on the Protection of Personal Information
APT	Advanced Persistent Attack
AV	Anti-virus
BAS	Breach & Attack Simulations
BEC	Business Email Compromise
CEO	Chief Executive Officer
GDPR	General Data Protection Regulation
HIPAA	Health Maintenance Organization
OAIC	Office of the Australian Information Commissioner
PDPA	Singapore Personal Data Protection Act 2012
POPIA	South African Protection of Personal Information Act

1 / INTRODUCTION

A new year is just around the corner, so it's time to look back at what happened in cybersecurity during 2018. As in previous years, we have seen that the number and scope of attacks has increased, resulting in 4.5 billion files compromised in the first half of 2018 alone, and the year is not over...

Cybercrooks not only increased their number of attacks, they also succeeded to perform a high number of data breaches. Hackers launched multi-vector attacks using social engineering (e.g., Phishing, Whaling) and ransomware to monetize, using e.g., GandCrab and Magniber ransomware to widen their target range to more countries as well as adding a stronger encryption. We also saw modular banking Trojans such as Emotet on the rise and ransomware attacks wreaking havoc around the world.

Despite C-level executives ranking cybersecurity as their number 1 challenge and more than 85% of companies reported experiencing a breach in the past three years, only 39% stated that their company has a fully developed and implemented cyber defense strategy in place.

This is especially problematic if we look at the largest data breaches on 2018 so far.

Cathay Pacific	The personal information of 9.4 million customers was compromised
Facebook	The accounts of around 29 million users were compromised
Singapore government's health database	The health records of ~1.5 million patients were compromised, including those of Prime Minister Lee Hsien Loong.
T-Mobile	The account information of ~2 million US-based T-Mobile customers were compromised.
MyHeritage	92 million user accounts were compromised
Sacramento Bee	Ransomware attack exposed 53,000 subscribers' information along with the personal data of 19.4 million Californian voters.
Cambridge Analytica/ Facebook	It was revealed that at least 87 million records were "harvested" during 2015 in order to create a program that would predict and influence voters.
Under Armour	The information of 150 million MyFitnessPal users was compromised.

In general, the effectiveness of cyberattacks is high since:

1. In most cases, multiple cybersecurity products not only overlap, but there is also no indication that all of these are actually effective.
2. Organizations do not "test themselves" enough (e.g., by using pen testing), and when they do, it's cosmetic since traditional tests do not produce / simulate real attacks using multiple attack vectors.

In this whitepaper, we will take a closer look at the main trends we saw in 2018.
We will also give some predictions to where we see cybersecurity heading in the coming year.

2 / TRENDS IN 2018

TREND #1 - EMAIL ATTACKS REMAIN POPULAR

As in previous years, social engineering of employees via phishing attacks keeps paying off for cybercriminals. On average, each email user receives 16 malicious spam emails per month. According to Verizon's 2018 Data Breach Investigations Report, users only reported 17% of phishing campaigns. Popular "disguises" were: sending fake invoices, fake delivery of failure notifications, fake messages from law enforcement and governments, malicious scanned documents, and fake package delivery notifications by email.

Tabnabbing, a phishing attack that asks users to enter their login details to popular websites, has been on the rise. **Drive-by** and **watering hole** attacks have resurfaced, displaying advanced evasive characteristics and using custom protocols on non-filtered ports.

Whaling, CEO Impersonation and BEC attacks were also on the rise. By targeting the C-suite in organizations, hackers got top-down access to all business operations; in some cases access to critical assets.

TREND #2 - CRYPTOJACKING AND CRYPTO HIJACKING

Cryptocurrency thefts have risen to almost $1 billion over the course of 2018, mainly from robbing cryptocurrencies and trading platforms.

Cybercriminals use cryptojacking botnets (networks of compromised computers) to mine cryptocurrency. Cryptominers, Coinhive and Cryptoloot were the favorite malware tools, while the cryptocurrency **Monero** was a favorite target. It seems that cybercriminals follow the price development of cryptocurrencies to strike when the prices are high. To illustrate, in August 2018, 1.7 million Russians were victimized followed by another attack in September 2018, with another 5 million victims. Other victims of cryptojacking malware include various government websites in the UK, US, and Australia.

Recent reports indicate that **WannaMine** is being used to harness crypto mining power. This malware is based on the leaked NSA exploit **EternalBlue**. Another commonly used malware is **PowerGhost** which stealthily downloads itself on a victim's device and spreads all over the corporation and workstation servers to attain their computing resources for mining of cryptocurrencies.

TREND #3 - ZERO-DAY AND FILELESS ATTACKS

According to a recent report of the Ponemon Institute, zero-day vulnerabilities and fileless attacks are now deemed as the most dangerous threats to the enterprise. Zero-day exploits are so dangerous because vendors (software and/or hardware) have not yet had the chance to detect and fix them.

Zero-day vulnerabilities are previously unknown bugs which are unpatched by vendors. These types of security flaws, depending on the severity and the affected software, can be used to conduct attacks including account hijacking, network compromise, and data theft.

Fileless attacks (also known as zero footprint, non-malware, and in-memory attacks) became popular during 2018 since they offer a way to circumvent cyber defenses. Such rogue code resides in the memory and is very difficult to detect even by sophisticated AV solutions.

TREND #4 - RANSOMWARE KEEPS PAYING OFF

Ransomware attacks started slowly in 2018, but peaked during the second half of 2018. Healthcare remained the most reported targeted industry by ransomware. Attacks took place all over the world, offering cybercrooks plenty of soft targets, high profits and virtually no way to be traced.

This trend was only encouraged by a recently discovered ransomware pack, which is available for $750 on the dark web. Similar packs bundle 23 different kinds of ransomware (including the notorious SamSam), making ransomware attacks accessible for non-technical cybercrooks.

In the US, there was a major attack on the City of Atlanta using **SamSam**. It was reported that it required an estimated $10m to mitigate the damage. Apart from the US, organizations were also targeted in Portugal, France, Australia, Ireland and Israel.

As for the ransom sum, the average stands at $10,000 in 2018. To put pressure on their victims, we saw that hackers started to conduct reconnaissance on their network and compromising back-ups before deploying the encrypting malware.

TREND #5 - VERTICALS AND INDUSTRIES REMAIN PRIME TARGETS

Cybercriminals are still attacking individuals and companies, but are focused on targeting the healthcare, government, and energy & utilities sector.

HEALTHCARE

If we look at healthcare breaches, we see that hospitals, doctor offices, healthcare clinics and other healthcare facilities were hit hard in 2018. As recent as October 2018, the personal files of about 75,000 individuals have been accessed by hackers who breached a US government system that is connected to the HealthCare.gov website.

Due to the rise in electronic healthcare technology, healthcare data is spread throughout (and exchanged between) healthcare organizations. The increased connectivity makes medical data a prime target for cyberattackers, also since it's relatively easy to hack.

Furthermore, healthcare institutions are more inclined to pay ransom to recover their systems making them attractive targets for cybercriminals. They operate 24/7 so their systems are rarely taken down for maintenance and cybersecurity updates, making them vulnerable for cyberattacks. For example, a hacker might exploit a known weakness such as an outdated installed security patch to attack and exploit.

INFRASTRUCTURE, ENERGY & UTILITIES

During 2018, we saw an increase of cyberattacks on infrastructure, energy and utilities all over the world. To illustrate the severity, a study by Bitkom shows that cyberattacks cost the German industry almost $50 billion. Hackers kept on manipulating critical industrial safety systems to cause damage.

The motives behind each attack included:

- **Hacktivism:** The attack on energy provider RWE in Essen, Germany.
- **Ransom**
- **State sponsored cyber-attacks:** China is the main suspect in hack of the TSMC, the world's largest contract chipmaker)
- **Revenge:** Hacktivists shutdown the websites of energy provider RWE in Essen, Germany to retaliate against cutting down the Hambach forest
- **Political motives:** Russia has been hacking the US electric grid for some time now on what looks like an intelligence gathering mission
- **Plain greed:** The Port of Barcelona, Spain and the Long Beach port terminal of the China Ocean Shipping Company (COSCO).

FINANCIAL SECTOR

Throughout 2018, financial services firms remained the favorite targets for cyber criminals since they are a treasure trove of tradeable data. Stolen data such as credit card credentials, customer information, and corporate data were abused or sold on the dark web. Even when no funds were stolen and no customer credentials were released, cyberattacks still posed a major problem for financial institutions, especially when other parties were compromised because of the attack.

During 2018, we saw that apart from traditional online bank heists, digital token exchange Bancor (hackers stole $22.5 million in total in cybercurrency) and other cryptocurrency companies were robbed.

Robbing of ATMs became more sophisticated with the popularity of ATM jackpotting with hacker groups. In September 2018, hackers used malware to compromise Cosmos Bank's ATM server to steal the credit card information of customers, alongside SWIFT codes required for transactions. They got away with $11.5 million in multiple countries, and another $2 million via debit card transactions across India.

ACADEMIA

Also in 2018, academic institutions remained the favorite targets of cybercriminals as they have for the past three decades. The scope was truly global. To illustrate: In March 2018, it came to light that Iranian hackers had accessed data valued at $3 billion by stealing 31 terabytes of academic data and intellectual property from more than 8,000 professors at more than 300 institutions worldwide. In August 2018, universities in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States, were hacked to gain access to the universities' online library systems to access online academic resources.

OTHER AT-RISK SECTORS

Other at-risk sectors include smart cities and social media platforms.

Smart cities have become a lucrative target for cyber attackers due to the increasing number of connected IoT systems embedded throughout the smart city's infrastructure. Hackers know that the networks of municipalities often lack sufficient security defenses, which makes them vulnerable for cyber attacks.

Social media platforms are abused in two ways:

a. Cybercriminals hack accounts to obtain personal data to turn into profit.

   An example: The cyberattack on Facebook where **nearly 30 million accounts** were compromised

b. Cybercriminals abuse social media platforms to influence elections.

   An example: Swedish institutions and political groups were under attack from the new "bots" on Twitter that were primarily supporting the nationalist, anti-immigration Sweden Democrats and attacking the ruling Social Democrats.

TREND #6 - LAW, CRIME AND PUNISHMENT

During 2018, we saw two interesting trends regarding compliance regulations: (a) companies were hit with sizable fines and settlements for data breaches pursuant to existing regulations (e.g., HIPAA), and (b) new regulations came into force in more and more countries.

During 2018, enterprises started to pay for data breaches that took place in previous years:

Uber	$148M	Settlement with 50 States for 2016 data breach
Yahoo	$85M	Settlement for 3 billion accounts breached since 2013
Tesco Bank	$21M	Fined by the UK Financial Conduct Authority for failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyberattack in 2016
Anthem	$16M	HIPAA settlement for breach in 2015
The University of Texas MD Anderson Cancer Center	$4.3M	Court ruling to pay penalties for HIPAA violations in 2011 - 2013
Fresenius Medical Care	$3.5M	Settlement for failing to comply with HIPAA's risk analysis and risk management rules resulting in multiple data breaches in 2012-2013

There could be even bigger fines in the horizon now that the European Union's General Data Protection Regulation (GDPR) has come into force. Data regulators in the EU are able to fine upwards of €20 million. A number of high profile companies have already suffered large-scale breaches since the new regulations came into force. Quite likely, we will see the cost of failure skyrocket in the coming years.

Law enforcement agencies have been cracking down on cybercrime during 2018.

- Polish law enforcement arrested Tomasz "Armageddon" T., a well-known cybercriminal believed to be the author of the Polski, Vortex, and Flotera ransomware strains.
- The United States imposed sanctions on the Iranian Mabna Institute and 10 individuals for cyberattacks on hundreds of universities, stealing 31 terabytes of "valuable intellectual property and data".
- Romanian and Italian authorities arrested a total of 20 people suspected of being involved in a banking phishing scam that had defrauded hundreds of bank customers of the equivalent of US$1.24 million.
- An American computer hacker who launched attacks on Rutgers University was ordered to pay $8.6m in restitution, and was sentenced to six months of home arrest.

A groundbreaking new compliance regulation came into effect on May 25, 2018, when the EU General Data Protection Regulation (GDPR) came into force. This regulation is aimed to stem the increasing number of reported data breaches, especially those relating to online systems and services. One of the biggest changes is the transparency requirement, which forces businesses to reveal within 72 hours if they have suffered a breach. The penalties for breaches are onerous, and the costs for data storage keeps on rising at 20% to 30% in the next few years.

Other countries have also launched data protection regulation in the last few years:

- The Protection of Personal Information Act (POPIA) is South Africa's equivalent of the EU GDPR.
- The Singapore Personal Data Protection Act 2012 (PDPA) establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data.
- The Data Protection Act 2018 is the UK's third generation of data protection law, who's main provisions went into force on May 25, 2018. The new Act aims to modernize data protection laws to ensure they are effective in the years to come.
- The Japanese Act on the Protection of Personal Information (APPI) contains similar provisions as the European GDPR.
- The Australian Notifiable Data Breach Scheme came into force on February 22, 2018. It requires an organization to report to the OAIC and any individuals affected if they reasonably believe an eligible data breach has occurred.

3 / PREDICTIONS FOR 2019

No review of the year would be complete without predicting what is likely to happen in the coming year on the cybersecurity front. Overall, cybercrime will continue to flourish and organizations will continue to have a hard time protecting their valuable data from hackers.

Let's have a closer look at the trends that we foresee in 2019.

1. More attacks such as the latest one on Australian shipbuilder and defense contractor Austal that gave hackers access to usernames, passwords, personal details and proprietary information can be expected. Maritime firms, in particular, will be at risk.

2. We can expect to see more zero-day attacks abusing software flaws that are unknown and have no patch or fix. They will remain popular in the cybercrime world since these attacks are extremely difficult to detect, especially with traditional cyber defenses. Zero-day attackers will keep on using malware that can remain undetected in infected systems for months (even years) giving them plenty of time to cause irreparable harm.

3. The use of "drive by" and "watering hole" attacks will increase during the coming year to deliver ransomware and other malware via unsecured Internet browsing.

4. The human element remains a vulnerable spot in cybersecurity defenses. Sophisticated and targeted social engineering schemes to entice employees to download or open malicious content will keep on taking its toll. Simple spam will be replaced by targeted phishing and whaling attacks.

5. Ransomware-as-a-Service will become more widespread, making ransomware packages easily available for non-technical cybercriminals. A recent example is the Kraken Cryptor designed for members of affiliate programs to incentivize participants to spread the ransomware by offering them a cut from the Bitcoin ransom payments.

6. Rogue countries and political factions will keep on targeting critical infrastructure as well as hacking websites to steal valuable assets (e.g., patents) and get counterintelligence. They will also keep on abusing social media platforms and accounts to influence elections and political outcome for their own gain.

7. Enterprises of all sizes will invest more in cybersecurity to prevent phishing, spear phishing, whaling, BEC and APT attacks. They will not only allocate more manpower and resources to their cybersecurity, but also invest in the latest cybersecurity solutions to add to their current cybersecurity arsenal, such as a BAS platform that allows organizations to test their cybersecurity posture before attacks can take place. This solution can also monitor and analyze the deployment of current security solutions to verify that they do not overlap and make the organization vulnerable.

4 / ABOUT CYMULATE

Cymulate helps companies stay one step ahead of cyber attackers with a unique breach and attack simulation platform that empowers organizations with complex security solutions to safeguard their business-critical assets. By mimicking the myriad strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively. An on-demand SaaS-based platform lets users run simulations 24/7 from anywhere, shortening the usual testing cycle, and speeding up time to remediation. Cymulate was established in 2016 by former IDF intelligence officers and leading cyber researchers with extensive experience in offensive cyber solutions. The company serves a broad range of industries, including finance, health care, and telecommunication.

For more information, visit www.cymulate.com or contact us to schedule a demo.