



BREACH & ATTACK SIMULATION

RECAPPING 2017'S BIGGEST CYBER TRENDS & PREDICTIONS FOR 2018

By Eyal Wachsman, Co-Founder & CEO of Cymulate

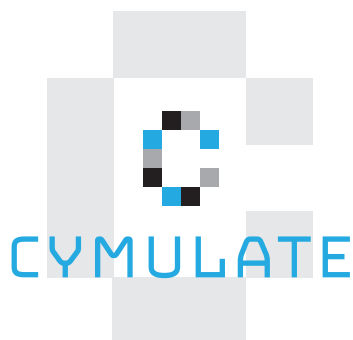


TABLE OF CONTENTS

Glossary	3
1 / Introduction	4
2 / Trends in 2017	6
Trend #1 - Email Attacks.....	6
Trend #2 - Drive-By & Watering Hole Remain Popular	6
Trend #3 - Attackers Use Stolen NSA Hacking Tools	7
Trend #4 - Ransomware Made A Global Impact.....	7
Trend #5 - Verticals and Industries Became Prime Targets	8
• Healthcare	8
• Infrastructure, Energy & Utilities.....	8
• Other At-Risk Sectors	9
Trend #6 - New Compliance Regulations	9
Trend #7 - New Cybersecurity Solutions Have Become Popular	10
3 / Predictions For 2018.....	11
4 / Forewarned Is Forearmed.....	12
Mitigate Social Engineering	12
Taking Standard Precautions	12
Deploying Proactive Cybersecurity Solutions	12
5 / About Cymulate.....	13

GLOSSARY

APT	Advanced Persistent Attack
BAS	Breach & Attack Simulations
BEC	Business Email Compromise
CISO	Chief Information Security Officer
GDPR	EU General Data Protection Regulation
CVE	Common Vulnerabilities and Exposures
HMO	Health Maintenance Organization
NYCRR	New York Codes, Rules and Regulations
PCI	Payment Card Industry Data Security Standard
SOX	Sarbanes-Oxley Act of 2002

This document includes proprietary and confidential information of cymulate and/or its affiliates and subsidiaries and may not be used, circulated or quoted except in accordance with explicit written authorization from cymulate.

1 / INTRODUCTION

A new year is around the corner, so it's time to look back what happened in cybersecurity during 2017. Cybercrooks did not only increase their number of attacks, they were also able to reach a global scale of data breaches. [WannaCry](#), [NotPetya](#) and [Bad Rabbit](#) wreaked havoc around the world. Hackers launched multi-vector attacks using social engineering (e.g., whaling) and ransomware to monetize. As a result, we have seen attacks and breaches at a scale and with a focus never seen before, with over **2 billion data records compromised**.

THE EQUIFAX

breach resulted in the theft of personal information of **145.5 million U.S. individuals**, and the exposure of **15.2 million UK** and **8,000 Canadian records**.

THE NHS BREACH

exposed the records of **26 million patients**.

THE EMAIL OF UK MPS

dozens of MPs in the UK were hacked, including those of Prime Minister Theresa May and senior ministers.

HACKERS

dumped a **9GB** of leaked emails from then candidat and now French president, Emmanuel Macron.

PHARMACEUTICAL GIANT MERCK

reported that NotPetya will cost the company **~\$ 600 million** in total.

THE NOTPETYA

attack cost shipping giant Maersk **\$200-300 million** and **FedEx ~\$300 million**.

Last but not least, the offshore law firm Appleby was hacked as a batch of **3.4 million confidential electronic documents** relating to offshore investment were stolen. Dubbed the [Paradise Papers](#), they relate to 120,000 individual and corporate clients. The Boston Consulting Group estimated the value at around **\$10 trillion**.

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 security solutions actually function.
2. Organizations very rarely “test themselves” (e.g., by using pen testing), and when they do, it’s cosmetic since most tests do not produce / simulate real attacks using multiple attack vectors

In the next sections, we will have a closer look at the 7 main trends of 2017.

We will also give some predictions to where we see cybersecurity going in the coming year. Last but not least, we offer some helpful tips to stay cybersafe.



2 / TRENDS IN 2017

TREND #1 - EMAIL ATTACKS

Social engineering of employees via phishing attacks was widespread this year, and proved to be quite effective. According to the [Verizon Data Breach Investigation Report \(DBIR\)](#), 66% of malware linked to data breaches or other attacks such as ransomware, was installed via malicious email attachments. Phishing attacks and malicious email attachments were also used in corporate espionage attacks.

Furthermore, Business Email Compromise (BEC) scams were also widespread, especially wire transfer requests or business requests dealing with personal information. To illustrate, at least 200 cases of BEC attacks targeted W-2 information, impacting more than 120,000 taxpayers.

It seems that although organizations invest more in email security solutions and awareness, these kinds of attacks are still very successful. There is a need to continuously verify the effectiveness of these security solutions against live attacks and employees need to be educated and instructed more often regarding the dangers of these attacks.

During an analysis of email security assessments performed during 2017 by our internal lab, it was found that a staggering **61.5% of malicious e-mails** and files managed to penetrate targeted organizations. Four categories of malware were used to assess which percentage in each category would breach the organization.

It was found that 52% of files with ransomware, 40% of files containing worms, 57% of files containing some kind of exploit, and 39% containing malware would have penetrated the organization.

TREND #2 - DRIVE-BY & WATERING HOLE REMAIN POPULAR

As [Cerber](#) and [Bad Rabbit](#) show, the use of “drive by” and “watering hole” attacks are still popular since they provide an easy way to spread malware. These kinds of attacks target specific groups of users to infect their computer and gain access to the network of the organization they work for. A watering hole attack is similar in nature to **spear phishing** or **whaling**, which also remained popular in 2017.

Although organizations’ security architecture seems to be robust and mature, all of the installed security solutions are unable to detect when an infected website is accessed, and malicious content is picked up and introduced to the internal network.

TREND #3 - ATTACKERS USE STOLEN NSA HACKING TOOLS

A hacker group that calls itself the “[Shadow Brokers](#)” stole top-secret NSA hacking tools that included the Windows XP vulnerability Eternal Blue. This enabled the WannaCry and NotPetya ransomware attacks of 2017 to be so successful, resulting in **~\$300 million in lost revenues** for shipping giant Maersk.

In May 2017, a new network worm dubbed EternalRocks was detected. The malware uses 7 NSA hacking tools and does not contain a kill-switch. By disguising itself as WannaCry, it is able to fool security researchers and circumvent security solutions. Instead of dropping ransomware, EternalRocks gains unauthorized control on the affected computer to launch future cyberattacks.

TREND #4 - RANSOMWARE MADE A GLOBAL IMPACT

In 2017, ransomware attacks eclipsed the majority of other global cybercrime threats.






















































































- The **WannaCry** ransomware attack, which was delivered via email in May 2017, infected as many as 300,000 targets in 150 countries including some high-profile ones such as Britain’s National Health Service, Spanish telco Telefonica, and logistics company Fed-Ex.
- In June 2017, **Petya and NotPetya** hit companies in Europe, the Middle East and the US via email, wreaking havoc for employees and customers alike. The attack caused computers to stop working, followed by displaying a ransom note demanding \$300. The widespread attack affected global and national organizations including the Ukrainian National Bank, British advertising firm WPP, pharmaceutical company Merck, FedEx’s TNT Express division, and logistics company Maersk
- In October 2017, a new strain of ransomware dubbed **Bad Rabbit** has been spreading in Europe through malicious / compromised websites, tricking victims into installing it by pretending to be a software update. The ransom this time is \$280 to be paid in bitcoin. The first targets were in Russia, but has since spread to Germany, Ukraine, Turkey, Bulgaria, Japan, and elsewhere.

TREND #5 - VERTICALS AND INDUSTRIES BECAME PRIME TARGETS

Cybercriminals are still attacking individuals and companies, but they also started to focus on other target groups such as entities in risk sectors. More specifically: the healthcare, governmental and energy & utilities sector.

HEALTHCARE

If we look at healthcare breaches, we see that hospitals, doctor's offices, healthcare clinics and other healthcare facilities have been hit particularly hard in 2017. HMOs and hospital networks were favored targets, and hackers know exactly how to use access to get their hands on valuable data.

Attacked Entity	Number of individuals affected
Commonwealth Health Corp. (data theft)	697,800                 
Airway Oxygen (breach)	500,000                 
Urology Austin	279,663                 
Harrisburg Gastroenterology	93,323                 
VisionQuest Eyecare	85,995                 

Source: U.S. Department of Health and Human Services

The reason why healthcare organizations have become a prime target is twofold.

Firstly, they are more inclined to pay ransom to recover their systems and operations than e.g., commercial enterprises as illustrated by the Locky attack of last year. During that breach, the Hollywood Presbyterian Medical Center in Los Angeles, California became infected with Locky ransomware that encrypted systems throughout the facility, locking staff out of computers and electronic records. Eventually, the hospital paid a ransom of \$17,000 in bitcoins to get the decryption key to restore its data.

Secondly, healthcare organizations operate 24/7 which means that their systems are rarely taken down for maintenance and cybersecurity updates. This makes them vulnerable for cyberattacks since e.g., installed security patches are often outdated. Hackers use those known weaknesses to attack and exploit.

INFRASTRUCTURE, ENERGY & UTILITIES

Industrial control systems (ICS) and critical infrastructure have become common targets for cybercriminals. In October 2017, Odessa airport and the metro system in Kiev were at the receiving end of cyberattacks. Using Bad Rabbit malware, the breach resulted in flight delays at Odessa airport since workers had to process passenger data manually. Kiev's metro system reported that its payment system had been hacked, but that the trains were running as usual.

In Ireland, hackers targeted energy networks to infiltrate control systems. The attackers (linked to the Russia's GRU intelligence agency) sent personalized emails containing malicious software to senior engineers at the Electricity Supply Board.

Following the use of an Industrial Controls Systems (ICS) attack platform last year during a cyberattack on the critical utilities infrastructure in Ukraine, utilities have been on high alert. In October 2017, the US government issued a [warning](#) about ongoing cyberattacks targeting critical national infrastructure, saying some networks and at least one power generator have been compromised.

OTHER AT-RISK SECTORS

Additional sectors have also become prone to being hacked or becoming the victim of ransomware attacks. **Federal institutions** and other **government agencies** have become lucrative targets since they provide time-sensitive, integral services ranging from law enforcement to disaster relief and first aid response. In case of emergency, these federal and state agencies must be able to act quickly. Due to the pressure they are under, attackers feel that they are inclined to pay the demanded ransom.

Law enforcement agencies are also being targeted, with various police departments becoming the victim of hacking and ransomware attacks. But also **law and accountancy firms** are at risk since they possess sensitive data that can be monetized. Recently, [Deloitte](#), one of the world's "big four" accountancy firms, was targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients.

TREND #6 - NEW COMPLIANCE REGULATIONS

New compliance regulation came into effect:

- Cybersecurity has become a staple in regulatory compliance. Cybersecurity requirements are already part of ISO 27001, PCI for protecting payments and HIPAA for patient protection. In 2017, another important regulation was launched. In March 2017, the New York State Department of Financial Services (NYDFS) issued its [23 NYCRR part 500](#). This new regulation consists of a new set of standards and requirements for banks, insurance companies, and other financial services organizations.

TWO MORE REGULATIONS IN THE MAKING MADE HEADLINES IN 2017:

- On May 25, 2018, the EU [General Data Protection Regulation \(GDPR\)](#) will come into force, aimed to stem the increasing number of reported data breaches, especially those relating to online systems and services. As a result, organizations must be prepared to avoid fines. Cybersecurity experts are hired and proactive cybersecurity solutions are sought after.
- In 2017, a new bill, the [Cybersecurity Systems and Risks Reporting Act](#), was proposed that will amend SOX to include regulation regarding cybersecurity systems and cybersecurity systems offices.

TREND #7 - NEW CYBERSECURITY SOLUTIONS HAVE BECOME POPULAR

As organizations found out the hard way, traditional perimeter defenses such as antivirus are not enough to block ransomware and other cyberthreats. As tested by our internal lab in **45 cases**, the latest generation in malware managed to bypass existing solutions and penetrate the organizations, as shown below.



Source: A sample of 45 organizations evaluated by Cymulate Ltd.

Vulnerability scans and penetration tests provide insight into the security posture of an organization at a specific moment. Although useful, they do not present the full picture; especially when it comes to new attacks and sophisticated ones using multi-vector methods.

1. The vulnerability scanner can only detect known CVEs that can be mitigated by updating and patching the system. However, this will not solve the problem of misconfiguration or misuse of the infrastructure and the security solutions.
2. Manual pen testing is not possible to do on demand and not continuous, as so does not allow to immediately test new threats as they appear more often today.

More and more organizations (and their CISOs) started to look beyond the vulnerability scans and penetration tests that they normally use to verify the safety and integrity of their systems and data. They started to test their resilience against the growing cybercrime wave with new security solutions that simulate targeted attacks using multi-vector simulated attacks. These kind of simulations, also known as Breach & Attack Simulations (BAS), allow organizations to continuously test their cybersecurity posture against cyberattacks, global cybercrime campaigns and directed [APTs](#).

3 / PREDICTIONS FOR 2018

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 keep on having a hard time to protect their valuable data from hackers.

Let's have a closer look at the trends that we foresee in 2018.



2018

1. More leaks such as the Panama Papers and the Paradise Papers can be expected in the coming year, with accounting and law firms becoming prime targets for cybercrooks. Since the client information they hold is highly sensitive, it is of high value for cybercrooks. The most vulnerable will be small and medium-sized firms with up to 250 employees.
2. "Shadow Brokers" and other hacking groups will go on exploiting tools stolen from the NSA and other agencies to their benefit.
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. Social engineering of employees via phishing and whaling attacks will remain widespread.
5. The ransomware Cerber family (including Magnitude) will remain the market leader, due to its ability to evade detection by cybersecurity tools and its use of highly skilled cybercriminal developers.
6. Based on their global success with WannaCry, NotPetya and Bad Rabbit, attackers will launch more attacks of this kind in 2018. The scope and damage is expected to increase even more.
7. Countries such as Iran will become more and more active in cyberattacks against their enemies and North Korea.
8. The threat of cyberattacks on electric distribution grids and the infrastructure of utilities will increase, also since cyberattacks on critical infrastructure can cripple a town or nation remotely without a trace.

4 / FOREWARNED IS FOREARMED

Although cybercrime will keep on flourishing in 2018, not all is lost. As the saying goes: “forewarned is forearmed” - organizations can take measures to shield themselves from cyberattacks.

MITIGATE SOCIAL ENGINEERING

Social engineered malware exploit human weaknesses. By educating the users on an ongoing basis, they become better informed about the risks of the latest threats. Employers can take additional measures by limiting employees' web browsing options or enhancing secure browsing capabilities using various solutions and services. Verification of the technical security barriers of the organization would prevent the access of operational malicious files such as malware and ransomware etc. It is also important to remember that these measures need to be reviewed periodically.

TAKING STANDARD PRECAUTIONS

There are several standard precautions that organizations can take to try and prevent e.g., phishing, spear phishing, whaling and BEC attacks.

These include measures include:

- Having a data backup and recovery plan in place to preserve sensitive or proprietary data;
- Scrutinizing links contained in emails;
- Block emails with attachments that might contains code executions;
- Enabling automated patches for OS and Web browsers, etc.

DEPLOYING PROACTIVE CYBERSECURITY SOLUTIONS

The arsenal of security solutions that an organization uses to prevent cyberattacks, needs to keep pace with the latest level of cybercrime sophistication. Proactive solutions are necessary, also in view of the latest regulatory compliance provisions. However, it is important to monitor and analyze the deployment of these security solutions in order to verify that they do not overlap and make the organization vulnerable. As we have seen in Trend 7, having a sophisticated breach and attack simulation platform in place allows organizations to test their cybersecurity posture before attacks can take place.

5 / ABOUT CYMULATE

Established in 2016, Cymulate is a SaaS-based breach and attack simulation (BAS) company that helps organizations to protect their business-critical assets against cyberattacks. Cymulate allows organization to launch simulations of cyber-attacks against themselves, immediately exposing vulnerabilities and providing mitigation procedures to close each gap. 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](#).