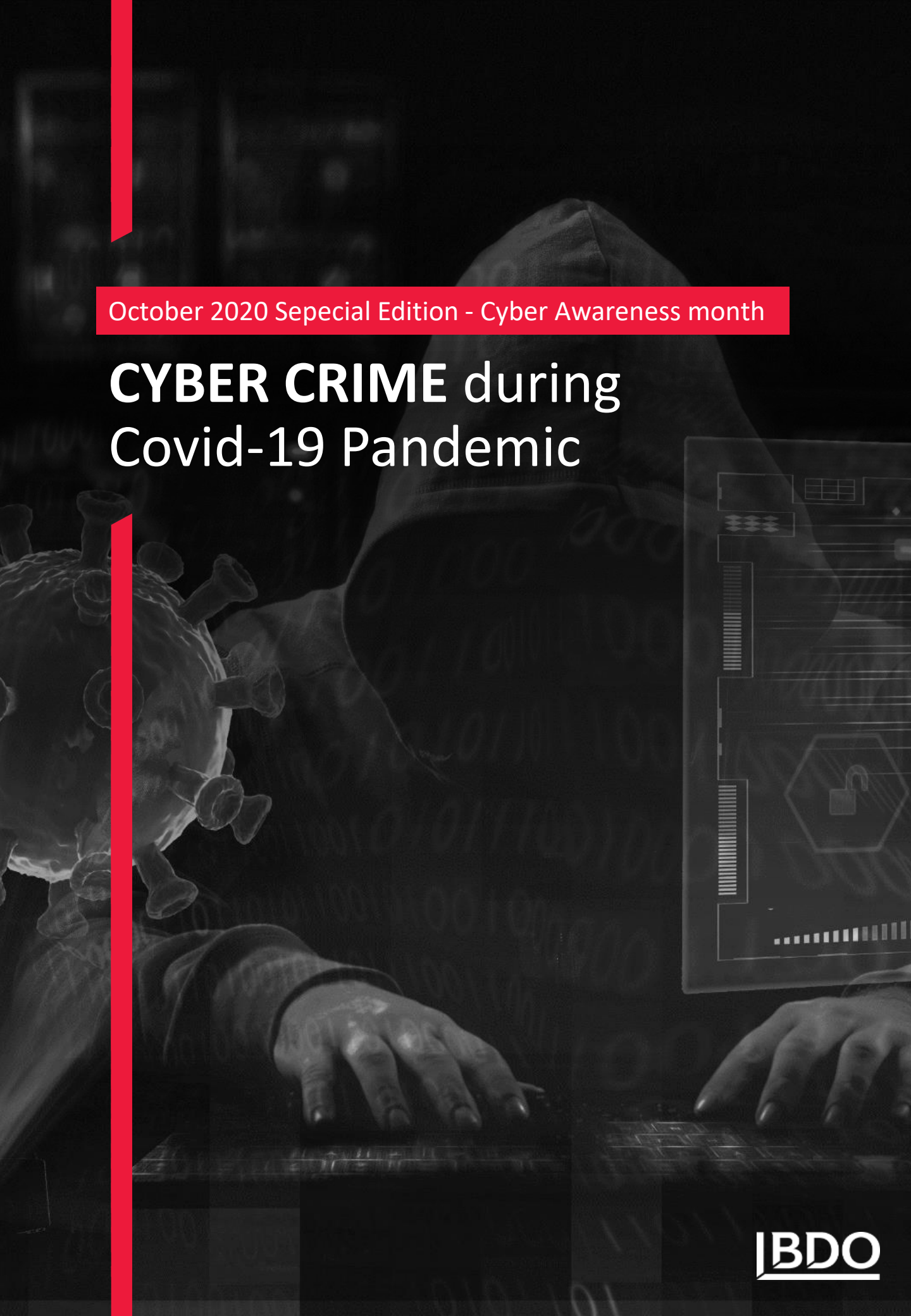


October 2020 Sepecial Edition - Cyber Awareness month

CYBER CRIME during Covid-19 Pandemic

BDO

It was recently reported that a death of a patient in a German Hospital was blamed on a cyber-attack. A ransomware attack disabling access to the hospital's information systems prompted the doctors to move the patient to a different hospital. The patient died on the way to the distant hospital.

Not too long ago, NotPetya and WannaCry ransomware attacks have crippled hospitals and healthcare organizations around the world, but no lives were lost due to those attacks. This is the first time a cyber-attack is directly related to the loss of a human life. This definitely changes the paradigm not just for health organizations, but also for other sectors such as Critical Infrastructure, Industrial Manufacturing, Automotive and others that are in the process of Digital Transformation of their businesses' safeguards and safety controls.

Our article details how cyber-threats affected businesses during Covid-19, pointing to some unanticipated events that followed this terrible, unnecessary death.

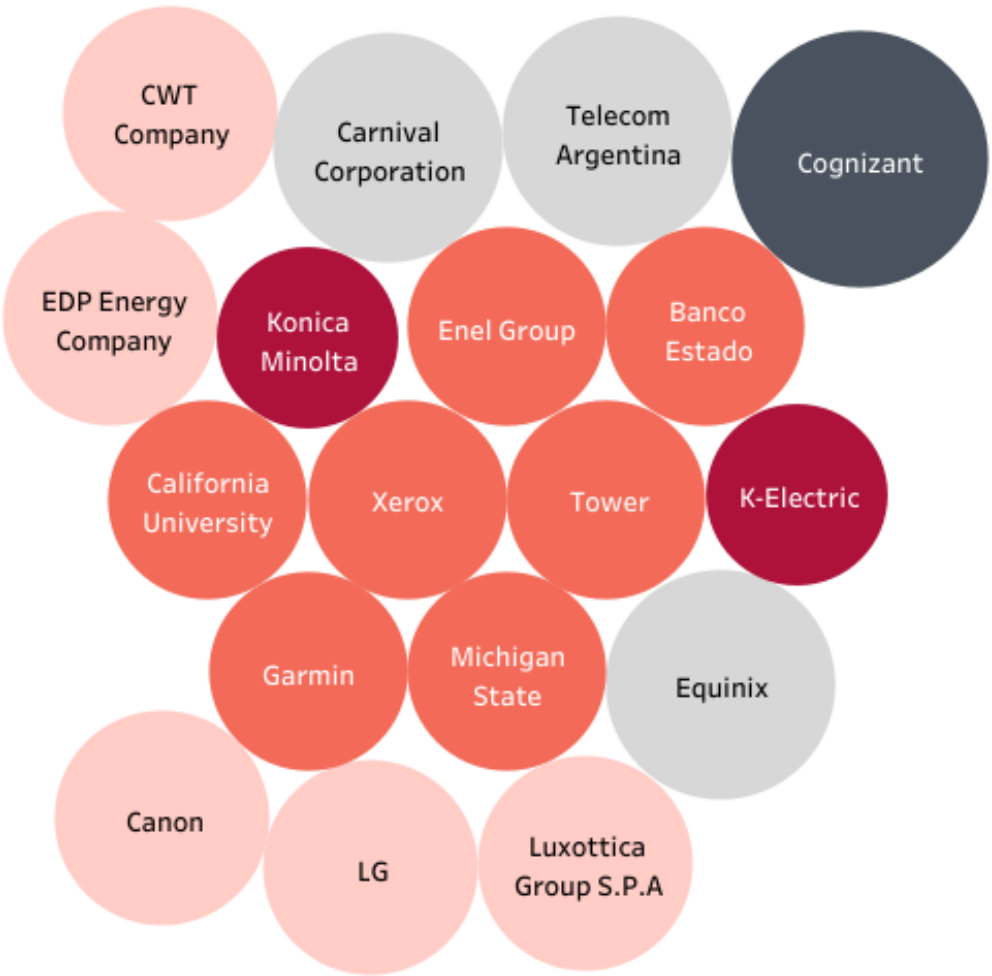
Upon realizing that his attack was against a Hospital the malicious actor withdrew its ransomware demand and provided the decryption keys. Following that too-late show of morality, other leading ransomware gangs that have been in the spotlight the last couple years and were responsible for some of the highest profile ransomware attacks, have issued declarations they will stop targeting hospitals, and if they determine that they had inadvertently attacked a hospital, they would provide the decryption keys. In contrast, the Netwalker ransomware gang declared that they would continue to demand ransom, even from hospitals.

Reading between the lines, the main take-away from these recent cyber-attacks is that these malicious-actors are here to stay. Eventually, they will be an inherent part of the business eco-system (Digital Transformation, Covid-19, Remote Workforce), will aim to grow (exploit any eco-system weaknesses) and become even more profitable. All these present a real concern for us.

HOW CYBER-THREATS AFFECTED BUSINESSES DURING COVID-19

Hackers have stepped-up their game during the Covid-19 pandemic. Cyber security threats have grown and become more sophisticated, breaking old records, impacting on a wide range of corporate victims from different sectors and industries.

Figure 1 - Noteable Ransomware Attacks
(June to September 2020)

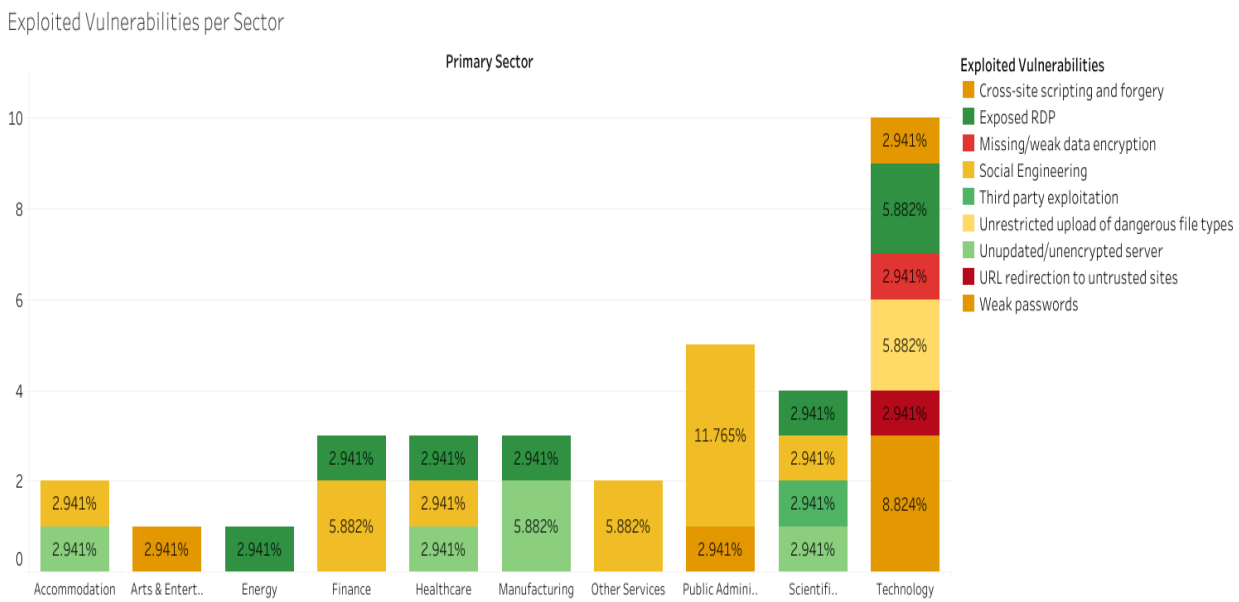


COGNIZANT EXPECTS TO LOSE BETWEEN $50M AND $70M IN Q2 2020 FOLLOWING RANSOMWARE ATTACK

Cyber criminals have taken advantage of the business-critical atmosphere around the world and redoubled their efforts to exploit the various weaknesses created during this unusual period.

Companies had to quickly adapt to some unique tactical changes as a result of the pandemic such as moving most or some of their workforce to work remotely, quickly creating digital front facing initiatives and putting heavy workloads on IT departments, expecting them do deliver faster than ever. The ability of IT to be agile in response to ad-hoc business requirements and the sudden massive move to remotely connected workforce, has become a determinant of organizations' success in adapting to the new business eco-system. In many cases Cybersecurity was left behind, either directly by relinquishing critical security controls or indirectly by failing to provide the appropriate attention to other security issues.

Figure 2 - Exploited Vulnerabilities (June to September 2020)



ALMOST 20% OF THE SIGNIFICANT ATTACKS DURING THE 3rd QUARTER OF 2020 EXPLOITED EXPOSED RDP PORTS

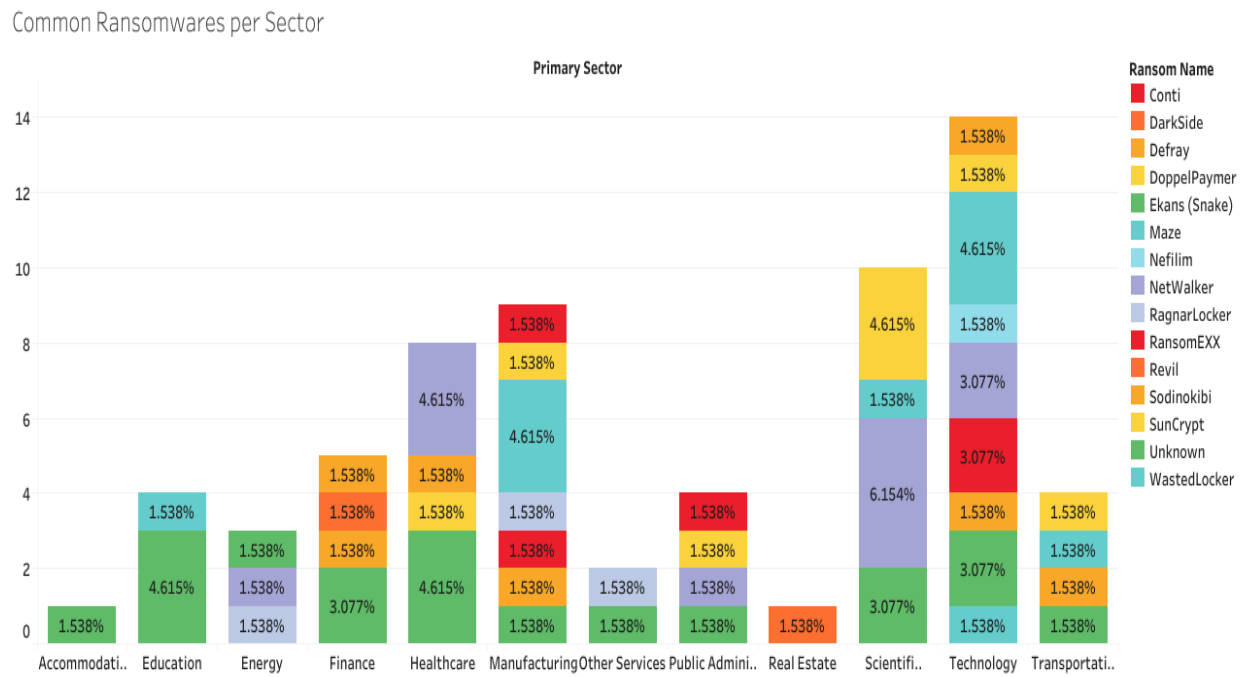
During the early stages of the "panic", vulnerable remote connectivity communication ports were left publicly exposed, allowing employees to easily connect from home. These exposed ports were easy to discover and were exploited by cyber-criminals to gain hold of corporate networks, propagating malware and executing other cyber-attacks.

Cyber-criminals have also realized that employees were craving for information about the pandemic and how it would affect their lives. They elevated social engineering attacks to whole new level of sophistication, focusing mainly on email campaigns convincing employees to click on malicious links, downloading infected files and providing their corporate credentials. The criminals used this to take control of email accounts and expanded their attacks to targeting C-level employees and to data breaches.

Ransomware gangs have not relented either. They have raised their sights to attack bigger, high profile companies while improving their techniques and malware capabilities to inflict more damage.

Ransomware demands increased to millions of dollars, leaving many companies with no alternative other than paying for decryption keys. The last couple of months Ransom Distributed Denial of Services (RDOS) attacks have also become more frequent, focusing on banking and financial institutions worldwide, forcing them to block international access to their websites and other digital assets.

Figure 3 - Common Ransomware (June to September 2020)



14% OF THE SIGNIFICANT RANSOMWARE ATTACKS DURING THE 3rd QUARTER OF 2020 TARGETED THE TECH INDUSTRY

Another somewhat disturbing trend emerged during the pandemic. More and more companies hit by various ransomware attacks are paying the ransom, counting on making claims against their cyber-insurance. Cybersecurity professionals have expressed real concern about this becoming a global trend, not only motivating the criminals to continue to carry out these attacks, but also causing companies to minimize or neglect actual prevention and detection security controls under the false pretense that being insured will "save the day". This has raised questions of whether there should be some kind of regulatory intervention in the cyber-insurance industry as it is currently practiced and the global implications on motivating criminals and discouraging safeguards.

Ransomware attacks are causing extensive damage to business operations, sometimes causing a complete shutdown of critical business functions and as previously noted, have recently resulted in the death of a patient in an attack on a hospital.

KEY RECOMMENDATIONS - RANSOMWARE PREVENTION KIT

A Ransomware Prevention Kit would help companies learn from the experience of other cyber-attack victims and assist in implementing appropriate defensive measures, before the attack has an opportunity to "knock on our door". Here are some key recommendations:

Offline Backups	Active Directory Sanitation	Endpoint Detection & Response (EDR)	Vulnerability Management	Situational Awareness
Offline backup of data and servers with periodic restoring tests	Active Directory misconfiguration, misuse and vulnerability Assessment	Endpoint Protection for computers and servers	Frequent vulnerability testing and mitigation of critical and high risk vulnerabilities	Act once Cyber Threats hit others and before you are in danger

Network Segregation	Email, Web, USB Sanitation	Strict Remote Access Policy	Cyber Security Awareness	Self-Assessments
Segregating Internet facing networks from production networks	File & Link sanitation received by Email, Web or USB	Disallow exposing RDP and other exploitable ports	Focused on Power users and IT personnel	Periodic or Continuous Penetration testing

CONTACTS:

TOMMY BABEL
Senior Manager
Head of Cyber Reselience Services
BDO Cybersecurity Center, Israel
TommyB@bdo.co.il