2020 Ransomware Report

Covington & Associates, LLC
P O Box 752844
Las Vegas, NV 89137
(702) 381-7452

Table of Contents

Table of Contents _____ ***1***

OVERVIEW _____ ***2***

January - 2020 _____ **3**

February - 2020 _____ **4**

March - 2020 _____ **5**

April - 2020 _____ **6**

May - 2020 _____ **8**

June - 2020 _____ **10**

July - 2020 _____ **12**

August - 2020 _____ **14**

September – 2020 _____ **17**

October - 2020 _____ **21**

November - 2020 _____ **27**

December – 2020 _____ **31**

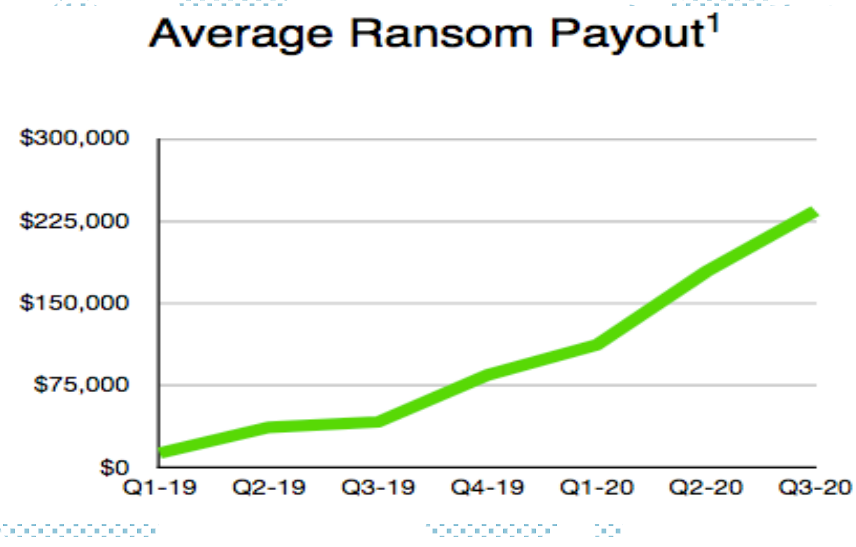
Inference – Synopsis - Recommendations _____ **35**

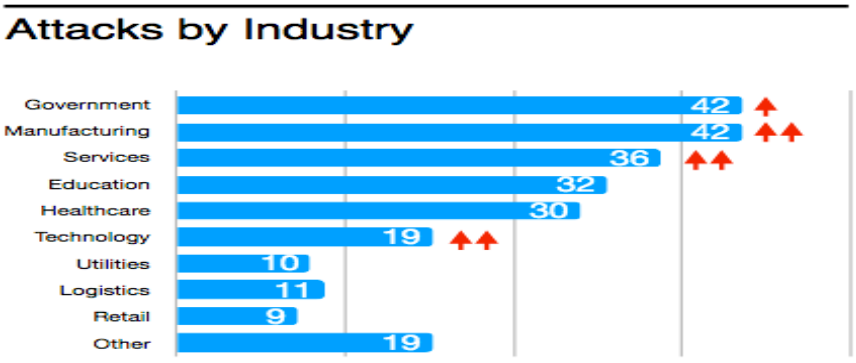
Need More Information… _____ **35**

OVERVIEW

Ransomware is a malicious software designed by organized cyber criminals, who determinedly work to infiltrate Commercial and Government enterprise systems. Their goal is to steal and encrypt your data to prevent you access from the data. Ultimately, they want to extort tens, hundreds of thousands to millions of dollars from you to grant you access to YOUR company's data.

In the past, most of the attackers simply ask for the money in exchange for a key to the encryption so that you can get access to your data again. However recently we have seen an uptick in selling your proprietary data to others as well as demanding monies from you.





**Source – Blackfog.com*

January - 2020

1.) **Travelex**, lost its websites across 30 countries and causing chaos for foreign exchange transactions worldwide during the month of January. The ransom was rumored to be the sum of $6M.

2.) **Oman's largest insurance company** was hit by a ransomware attack causing data loss but no publicized monetary loss.

3.) **Richmond Community Schools** in Michigan had to postpone opening after the Christmas break when hackers demanded $10K in Bitcoin to restore access to the server.

4.) **Pittsburgh Unified School District of Pennsylvania** were left without internet access after a ransomware attack disabled the district's network systems during the festive break.

5.) **A Medical Practice in Miramar Florida** reported that they received ransom demands from a cybercriminal threatening to release their private medical data unless a ransom was paid.

6.) **Panama - Buena Vista School District in California** experienced a ransomware attack that caused a technology and phone outage at multiple schools. While the school was working with the FBI regarding the attack, they let parents and students know that they couldn't access any grades so report cards would be delayed.

7.) **The small town of Colonie New York** cybercriminals hacked into the computer system and demanded $400K in Bitcoin cryptocurrency to unlock it.

8.) **A synagogue in New Jersey** fell victim to a cyberattack and a ransom demand of around $500K.

9.) **Volusia County (Florida) Public Library,** 600 computers were taken offline after a cyberattack.

10.) **German car parts company Gedia**. The group used two Russian- speaking underground forums on the Dark Web to threaten to publish 50GB of sensitive data, including blueprints and employees' and clients' details, unless Gedia agreed to pay a ransom.

11.) **Bouygues construction company in France** was paralyzed by a major cyberattack affecting the entire computer network and shutting down all of

the company's servers. A ransom of €10M was requested by the cybercriminals.

12.) ***Electronic Warfare Associates (EWA)**, a 40-year-old electronics company and a well-known US government contractor suffered a ransomware infection.*

13.) ***Tillamook County, Oregon** all of the computer systems went down. Despite early thoughts that the outages were a technical issue it was later confirmed they suffered a ransomware attack.*

14.) ***The City of Racine, Wisconsin** a ransomware attack caused the city's website, email, voicemail, and payments systems to be knocked offline.*

February - 2020

15.) *ITI Technical College in Baton Rouge Louisiana became the victim of a cyberattack via a phishing email sent at the end of January.*

16.) ***Scotland's Dundee and Angus College** was hit with what they described as a cyber-bomb which took down their system.*

17.) ***Australia** reported attack as logistics company **Toll Group** confirmed they had to shut down their systems because of ransomware.*

18.) ***North Miami Beach Police Department** who reported they had become a victim of ransomware.*

19.) ***Two Texas schools** in the same district who were affected. The city of Garrison managed to make a quick recovery but the Nacogdoches Independent School District faced more of a struggle to rebound from the attack.*

20.) ***England** a ransomware attack on **Redcar Council** forced staff back to pen and paper and 35,000 UK residents were without online public services.*

21.) ***INA Group, Croatia**'s biggest oil company and its largest petrol station chain. Were the victims of yet another attack. The suspected ransomware attack had a crippling effect on business operations.*

22.) ***Denmark** where facilities firm **ISS World** was crippled by a ransomware attack that left hundreds of thousands of employees without access to their systems or email.*

23.) *The South Adams Schools district in Indiana where an overnight ransomware attack affected all of the school's IT systems.*

24.) *Gadsden Independent School District in Alabama suffered a ransomware attack that managed to take down all of their internet and communications systems across all of its 24 school sites.*

25.) *La Salle County, Texas confirmed a ransomware demand was responsible for its ongoing technology issues.*

26.) *Jordan Health in New York State, a non-profit organization that operates 9 health centers in Rochester and Canandaigua NY was the next to suffer at the hands of cybercriminals when they reported a ransomware attack had shut down all of their IT systems.*

27.) *Australia This time ransomware affected the Australian wool industry when sales were stopped by a ransomware attack at wool industry software company Talman.*

28.) *Kansas where legal services giant Epiq Global reported they had suffered a ransomware attack on the last day of the month. The attack affected the organization's entire fleet of computers across its 80 global offices.*

March - 2020

29.) *La Salle County in Illinois a cyberattack affected around 200 computers and 40 servers in the county government.*

30.) *Visser, a parts manufacturer for Tesla based in Colorado. Security researchers say the attack was caused by the DoppelPaymer ransomware, a new kind of file-encrypting malware which first exfiltrates the company's data.*

31.) *The government in P.E.I. Canada suffered a data breach when internal government documents were posted online following a ransomware attack.*

32.) *Missouri where Three Rivers College were forced to cancel almost all of their classes following a ransomware attack.*

33.) *California based defense contractor CPI had been knocked offline by a ransomware attack. Sources say the company who makes components for military devices and equipment paid a ransom of about $500,000 after an attack in January but they were not yet operational.*

34.) ***EVRAZ, owned by Roman Abramovich*** *and one of the world's largest steel manufacturers, suffered a Ryuk ransomware infection that managed to take down its North American branches.*

35.) ***Durham city*** *was the next target when a Ryuk ransomware attack affected everything from the police to fire services. The county government services were also taken offline when 80 servers were impacted by the attack.*

36.) ***The Fort Worth Independent School District*** *in Texas suffered a string of cyberattacks after the ones that took place across several Texas school districts in 2019.*

37.) ***Champaign-Urbana Public Health District in Illinois.*** *Their website was taken down by the Net Walker ransomware attack, hampering the organization's response efforts amid the Coronavirus pandemic.*

38.) ***The United Kingdom*** *- cybercriminals hit London based* ***Hammersmith Medical Research firm*** *who were on standby to carry out trials of a possible future vaccine for the Covid-19 coronavirus.*

39.) ***London based. Finastra,*** *a fintech firm that provides technology solutions to banks were forced to shut down their key systems globally after detecting a cyberattack.*

40.) ***Connecticut based medical and military contractor Kimchuk*** *who announced they were hit by DoppelPaymer, a newer strain of ransomware that exfiltrates data out of an infected network before encrypting user files.*

41.) ***Missouri - TI Power Systems,*** *a supplier of the energy company Ameren Missouri was hit by a ransomware attack that allowed the malicious actors behind the attack to steal information from the firm.*

42.) ***South Carolina - Bluffton Fire and Rescue*** *was the next in a long line of government entities in the state to be compromised by cyberattacks in recent months.*

April - 2020

43.) ***Portuguese Energy giant Energias de Portugal (EDP)*** *was a victim of a major attack when cybercriminals held them to ransom for a massive 9.9 million Euros!*

44.) **Canada, the Law Society of Manitoba** *revealed that two un-named law firms in the province had been locked out of their computer systems after they were infected with ransomware.*

45.) **City of Olean in New York**. *a ransomware attack shut down all of the computers at the Olean Municipal Building.*

46.) **Cognizant** *- The New Jersey headquartered organization is one of the largest IT managed services company in the world with close to 300,000 employees and over $15 billion in revenue.*

47.) **Denmark Agribusiness group Danish Agro**, *were the target of a ransomware attack.*

48.) **Colorado-based Parkview Medical Center** *reported that their technology infrastructure was hit with a ransomware attack causing a number of IT network outages amid the battle with Covid-19.*

49.) *City of Torrance in the Los Angeles metropolitan area who was allegedly attacked by DoppelPaymer Ransomware. The attackers demanded a 100 bitcoin ($689,147) ransom for a decryptor, to take down files that have been publicly leaked, and to not release more stolen files.*

50.) **Canada - accounting firm MNP** *was hit by a cyberattack which forced a company- wide shutdown of its computer systems.*

51.) **Zaha Hadid Architects in London** *a hacker accessed the servers of and had stolen confidential information in an attempt to extort money from the firm.*

52.) **CivicSmart, a Milwaukee**, *USA based company known for its parking meter technology was the next victim of a ransomware attack that exposed internal files in an attempt to elicit a ransom payment.*

53.) **Pennsylvania headquartered pharmaceutical giant** *ExecuPharm revealed that ransomware attackers had recently encrypted its servers and had stolen corporate and employee data.*

54.) **Canada, Northwest Territories Power Corporation** *had their website and email services attacked shut down after they received a ransomware message from unknown hackers.*

May - 2020

55.) **The Toll Group** revealed it had found itself at the mercy of cybercriminals for the second time this year. The incident was unrelated to their previous attack in February and was thought to be a relatively new form of ransomware known as Nefilim.

56.) **Taiwan's state-owned energy company CPC Corp** was the next victim. Luckily the attack didn't affect any energy production, but it did cause some disruption for customers attempting to purchase gas.

57.) **Fresenius in Germany**, Europe's largest private hospital operator. The company who employs around 300,000 people across more than 100 countries confirmed that a cyberattack had affected every part of the company's operations around the globe.

58.) **Ruhr University Bochum** were forced to shut down large parts of their central IT infrastructure, including their backup systems after a ransomware attack occurred overnight.

59.) **Grubman Shire Meiselas & Sacks**, a NYC law firm with a host of celebrity clients including Elton John, Robert DeNiro and Madonna were a victim of REvil ransomware used to steal the personal information of celebrity clients. Hackers threatened to expose nearly 1TB of private celebrity data unless a ransom was paid in Bitcoin.

60.) **Swiss Rail construction firm Stadler** the company disclosed that hackers had threatened to publish sensitive data to harm the firm and its employees if the large ransom was unpaid.

61.) **Pitney Bowes** disclosed that they had been hit by Maze ransomware less than a year after they were hit by a similar attack. The group behind Maze specializes in double extortion, an attack that increases pressure on its victims to pay by threatening to release important data in addition to encrypting systems.

62.) **Elexon,** the organization that helps balance and settle the UK's electricity market was attacked by hackers using the REvil/Sodinokibi ransomware. Sensitive internal data was stolen in the attack with some posted on the Dark Web to pressure the organization into making the ransom payment.

63.) **The Office of Court Administration in Texas** *revealed that a ransomware attack was launched against its court system. It's thought that no sensitive data was stolen, and at the time of writing they insisted that no ransom would be paid.*

64.) **Diebold Nixdorf**, *a major provider ATMs and payment technology, disclosed that a ransomware attack had disrupted some of their operations. The company said the hackers didn't affect the ATMs or customer networks and that the intrusion only affected its corporate network.*

65.) **Magellan Health**, *a major US healthcare provider based in Phoenix, Arizona found themselves a victim of ransomware after falling for a phishing email that appeared to be from a client. The hackers proceeded to exfiltrate records containing personal information before launching ransomware to encrypt files.*

66.) **BlueScope Steel** *who suffered IT disruption that impacted production across its global operations. The ransomware incident was thought to be caused by employees opening contaminated email attachments.*

67.) **Bam Construct**, *a firm that had recently delivered Nightingale Hospitals for the NHS during the Covid-19 crisis had fallen victim to a ransomware attack. The company said that the business "stood up well" after the incident despite being forced to take services offline to mitigate the attack.*

68.) **The Texas Department of Transportation** *who revealed they has been hit by ransomware just days after the state's judiciary system suffered the same fate. It appears that Texas is becoming a popular destination for cybercriminals as 22 local governments were targeted by ransomware in a single attack in 2019.*

69.) **Anglo-Eastern**, *one of the largest ship managers based in Hong Kong was hit with a ransomware attack.. The incident was quickly contained, and it was reported that no data was lost.*

70.) **New South Wales** *A retailer In Sport's head office was hit by ransomware. The firm was unable to confirm what data had been accessed but they revealed that the attackers used REvil/Sodinokibi ransomware.*

71.) **The customer experience firm Stellar** *appeared to have taken a hit from a group of attackers using NetWalker ransomware. Images of data stolen from the company were posted on the Dark Web and according to a*

countdown timer on the site, the company had just over six days to respond to the hacker's ransom demands.

72.) ***Halifax in Canada where the Northwest Atlantic Fisheries Organization*** *(NAFO), an intergovernmental organization that manages fish stocks in international waters in the northwest Atlantic Ocean, was hit by a ransomware attack. The organization who counts a dozen countries as members, including Japan, Norway, Canada, the European Union, and Russia admitted the attack had locked them out of their data systems and knocked their website offline in a letter to stakeholders.*

73.) ***Michigan State University****. The operators of the NetWalker ransomware gang reportedly gave MSU officials seven days to pay the ransom before they planned to leak the stolen university files.*

74.) ***IT Services Giant Conduent*** *disclosed that a ransomware attack had affected its European operations and although customer data had hit the Dark Web, they had managed to restore their systems in 8 hours.*

75.) ***The city of Weiz, Austria*** *where a NetWalker ransomware attack was launched. The attack affected the public service system and leaked some of the stolen data from building applications and inspections.*

June - 2020

76.) ***The South African telecom firm Telkom SA SOC Ltd****. It was reported that the attack led to outages across several systems with remote staff unable to connect to the servers or VPN.*

77.) ***Columbia College in Chicago*** *was attacked just one week after* ***Michigan State University****. On the Netwalker blog the cybercriminals claimed to have exfiltrated very highly- sensitive data during the attack.*

78.) ***The University of California*** *on the same day. Important Covid-19 research was encrypted during the attack and it was later disclosed that the school paid out $1.14 million to recover the data.*

79.) ***The City of Florence in Alabama*** *became the next victim when a cyberattack shut down the city's email system. The city reportedly paid over $250K to recover the encrypted data.*

80.) *VT San Antonio Aerospace, the US subsidiary of ST Engineering Aerospace in Singapore. The ransomware attack resulted in the exposure of confidential company data including government contracts.*

81.) *Automotive giant Honda suffered a Snake ransomware attack which targeted its offices in the United States, Europe and Japan. The attack forced many offices to shut down in what was likely the most publicized ransomware incident of the month.*

82.) *Australian beverage giant Lion disclosed they had been the victim of a cyberattack, they later confirmed it was ransomware. The company's data was said to be available on the Dark Web but at the time of writing the company said they did not have any evidence of data being exfiltrated.*

83.) *Missile contractor Westech International was the victim of a Maze ransomware attack. Hackers were able to access sensitive employee information, but it is still unconfirmed whether any classified military information was accessed.*

84.) *Norwegian shipbuilder Vard, reported that company servers were hit with an encryption attack which led to disruption and downtime. The overall extent of the damage has not yet been disclosed.*

85.) *Fisher and Paykel, a white-goods manufacturer based in New Zealand disclosed they had been targeted by Nefilim ransomware. Although the attack was quickly identified, the hackers did disclose an initial leak of the company's corporate files on the Dark Web.*

86.) *New York company Threadstone Advisors, a mergers and acquisitions firm whose client list includes Victoria Beckham. The Maze ransomware gang insisted that they had exfiltrated and encrypted sensitive company data.*

87.) *The City of Knoxville in Tennessee. Fortunately, emergency services were not affected in the attack, but by the time it was noticed by the IT department, the ransomware had already encrypted multiple systems.*

88.) *European energy giant Enel Group. The incident was the work of the Snake ransomware group who were also responsible for the attack at Honda earlier in the month.*

89.) *Rhode Island-based Care New England (CNE) was victim of a cyberattack that hit its servers on June 16. The suspected ransomware attack forced the shutdown of its website and other internal systems.*

90.) ***Florida based ConnectWise*** *who hit the headlines when it was revealed that their partners were hit by ransomware through a software flaw in their platform.*

91.) ***Electronics giant LG*** *is reportedly being threatened by the Maze ransomware gang, however at the time of writing no official statement had been issued by the company.*

92.) ***Mitsubishi****. The Doppelpaymer gang are allegedly threatening to leak data from the organization, although at the time of writing there has been no official statement from the company.*

July - 2020

93.) ***Blackbaud.*** *The incident was reported late in July but it has been revealed that the actual ransomware attack occurred in May.*

94.) ***Texas-based government institution, Trinity Metro****, a transit agency that operates bus and commuter rail transportation services in Fort Worth. Phone lines and booking systems were down following the attack and a post on the NetWalker gang website showed more than 200 Trinity Metro folders containing information that was apparently exfiltrated from the agency before its systems were disrupted.*

95.) ***Xchanging, a subsidiary of IT Services giant DXC*** *announced in a press release that certain systems of* ***London based MSP*** *Xchanging had been affected by a ransomware attack. Xchanging offers IT services and business process outsourcing to aerospace, banking, defense and insurance firms.*

96.) ***Texas again where Cooke County*** *found themselves the next victim of REvil ransomware. The attackers threatened to start releasing data within 7 days of the attack after posting screenshots thought to be documents and data from the county's police department on the Dark Web.*

97.) ***Chilton County Alabama*** *implemented a shutdown after being targeted by an attack on the morning of July 7. The incident which caused a temporary disruption to the County's computer records systems including the tag office and probate court records was announced via social media.*

98.) ***New Jersey based IT Staffing firm Collabera*** *was the next firm to find themselves victim of a Maze ransomware attack. Hackers were able to*

exfiltrate employees' names, addresses and other personal information and infect its systems during the cyberattack.

99.) ***French telecommunications company Orange*** *was the next company to fall victim, this time to Netfilim ransomware. Luckily for Orange and its 266 million customers, the incident was only related to its business services division. Data exfiltrated from Orange customers was later added to the Nefilim Dark Web site that details corporate leaks.*

100.) ***Telecom Argentina*** *fell victim to what has been described as a massive ransomware attack with the cybercriminals demanding that $7.5 million be paid in the privacy coin Monero. Twitter posts suggested that the criminal gang demanded payment prior to July 21, if the payment wasn't made the ransom would double while the systems would remain locked.*

101.) ***State owned New Hampshire Radio****. The organization revealed that they had been hit by a ransomware attack but no personal information had been accessed. The organization also revealed that third party supplier Blackbaud had discovered and stopped an attack back in May and had contacted them in July with details.*

102.) ***Kansas*** *a ransomware attack took place at the GPS and smartwatch business* ***Garmin****. The attack took the business entirely offline for more than three days and is believed to have been carried out by a Russian cybercriminal gang which calls itself "Evil Corp".*

103.) ***Atlanta based SiteOne****, the largest national wholesale distributor of landscape supplies in the United States. The company reacted quickly to the attack and managed to recover its critical business data with little disruption.*

104.) ***Germany, Dussman Group****, a global facility management specialist providing cleaning, catering, security, technical, and commercial services worldwide. The multinational company which employs over 66,000 staff worldwide and makes billions of euros in sales annually was reportedly struck by the Nefilim variant. After the attack the criminal group began posting 16,000 files to the Dark Web as proof of the attack.*

August - 2020

105.) **Japan where Konica Minolta** *was hit by their second ransomware attack which took down company services for almost a week. The group behind the attack reportedly used RansomEXX ransomware, a relatively new malware that needs to be operated manually and does not have the ability to steal files. Meaning whoever was behind the attack needed to compromise the network and infiltrate all of the devices before running the malware.*

106.) **Netherlands based travel management company CWT**. *A ransomware attack knocked 30,000 company computers offline and cost the company a $4.5 million ransom to get up and running again. Hackers allegedly obtained corporate data although this was denied by the company.*

107.) **Australia, aged care operator Regis** *was the victim of an international cyberattack that led to the loss of personal data. The company told investors that an "overseas third party" was responsible for the attack which resulted in data being copied from its servers and publicly released. Following the incident, the federal Australian government's cybersecurity center issued a critical warning that Maze ransomware was threatening aged care facilities across the country.*

108.) **Ohio based Muskingum Valley Health Center** *made the headlines next when they notified more than 7,000 patients that their personal information may have been exposed in a ransomware attack on its EHR system.*

109.) **Boyce Technologies**, *a manufacturer of transit communication systems that pivoted to build ventilators during the COVID-19 pandemic was the next victim of the DoppelPaymer ransomware gang. The gang posted examples of the stolen data on the Dark Web and threatened to release it unless the ransom was paid.*

110.) **North Carolina based Cornerstone Building Brands**, *a top manufacturer of windows in North America was the next reported victim. The company confirmed the attack and launched an investigation. At time of writing the publicly traded company had reportedly recovered many of its critical systems and did not expect the attack to have a material impact on its business.*

111.) **Japan, Canon Camera** *whose services division experienced an outage caused by a Maze ransomware attack. Internal applications, email servers, Microsoft Teams, and the US website were impacted.*

112.) **Carnival, the world's largest cruise line operator** *disclosed they had become a victim of ransomware. With over 150,000 employees and 13 million guests every year, Carnival Corporation is the largest cruise operator in the world. In an 8-K form filed with the Securities and Exchange Commission (SEC), the company disclosed that one of its brands had suffered a ransomware attack and that data was likely to have been stolen.*

113.) **Brown-Forman, the Louisville, Kentucky** *based manufacturer of Jack Daniels. The company was reportedly able to intervene before attackers could encrypt its systems and is working with law enforcement and third-party experts to mitigate the incident. While there is no confirmation on when the attack took place, a Forbes report indicates the intruders were in Brown-Forman's environment for more than a month.*

114.) **The University of Utah** *reported that following an earlier ransomware attack they paid a $457K ransom. As data stolen during the attack contained student and employee information, the university decided to work with its cyber insurance provider to pay the ransom to prevent it from being leaked.*

115.) **Chicago, medical debt collection firm R1 RCM** *suffered a ransomware attack. The company with more than 19,000 employees and revenues of $1.18 billion in 2019 have contracts with at least 750 healthcare organizations nationwide. The company acknowledged they had been targeted in an attack but declined to discuss it further.*

116.) **South Korea based semiconductor manufacturer SK Hynix**. *Although the company has yet to comment on the incident the gang behind the attack released screenshots of some of the stolen company documents.*

117.) **TFI International, a Canadian transport and logistics company** *was next to disclose that four of their courier divisions were hit by ransomware just two days after they raised $219 million in a share offering. A company notice stated that they would continue to meet most customer shipping needs that they were not aware of any misuse of client information.*

118.) **Haywood County Schools in North Carolina** *were forced to close following an attack. In a statement released by the school, it was disclosed that school staff discovered the incident and that the third-party attacker has requested a ransom to stop the attack.*

119.) **Southeastern Pennsylvania Transportation Authority (SEPTA)** *were unable to provide real-time transportation information after an attack caused their systems to fail. SEPTA declined to provide further information about the attack but experts speculate that disruption to its systems has been significant.*

120.) **Brookfield Residential Properties**, *the home construction division of one of* **Canada's** *largest publicly-traded companies, was next to fall victim to an attack. Although the organization did not confirm that the attack was ransomware, a threat group known as DarkSide claimed the attack and threatened to release stolen data unless a ransom was paid.*

121.) **Gosnell School District in Arkansas**. *Little has been reported about the attack but it was disclosed that ransomware software infiltrated the school's system and at the time of writing personal data had not been compromised.*

122.) **The Royal Military College in Kingston, Ontario**. *A cyberattack was reported in July but at the time it was unclear if it was ransomware. Ransomware was later confirmed when hackers posted documents that revealed sensitive personal information online.*

123.) **California based MA LABS**, *one of the leading computer component distributors in the United States was the next company to make the list. The REvil ransomware gang claim to have exfiltrated 949 gigabytes of confidential information from the central servers of the company. REvil said the attack affected more than 1,000 servers, and also claimed that the distributor didn't tell the public about the attack.*

124.) **Fresno, California** *where back to school was disrupted when a ransomware attack took down the entire network at the* **Selma Unified School District** *forcing Fresno-area schools to cancel online classes.*

September – 2020

Ransomware gangs seemingly worked overtime this month as the most attacks of the year, occurred netting a whopping 31 incidents. The most notable attack was on a German hospital which caused a woman to lose her life. The first cyberattack homicide investigation is currently underway and the EU Cybersecurity Agency is calling for countries to consider making company bosses liable for deaths in the future.

125.) ***Australia, Tandem Corp*** *became a victim of NetWalker ransomware. Screenshots of data allegedly stolen during the attack were published on the Dark Web. The screenshots included files which appeared to contain financial data, personnel information and passport details.*

126.) ***Miami where staff at Key West City Hall*** *were forced to go back to pen and paper when a ransomware attack took their systems offline.*

127.) ***Boston headquartered cybersecurity and threat detection company Cygilant*** *suffered a NetWalker ransomware attack. In a statement their CFO confirmed that the attack had impacted a portion of the company's technology environment. At the time of writing it was unclear whether or not a ransom had been paid.*

128.) ***Argentina's official immigration agency, Dirección Nacional de Migraciones****. The attack temporarily halted border crossing into and out of the country, and the attackers initially demanded $2 million but this was doubled to $4 million after a 7 day period.*

129.) ***South America a REvil attack on BancoEstado in Chile****. The bank, which is one of Chile's three largest, was forced to close all of its branches following the attack.*

130.) ***Hartford Public Schools in Connecticut*** *when hackers knocked their critical systems offline over Labor Day weekend.*

131.) ***Newcastle University in the UK*** *was the next reported attack on education. The disruption to the school's systems is ongoing and the DoppelPaymer group has been posting documents it claims to have stolen from its servers to its dedicated "Doppel Leaks" site.*

132.) ***California based data center giant Equinix*** *was the next firm to reveal they had been hit with a ransomware attack. The organization confirmed that its*

data centers and managed services remained intact as it was only internal systems affected.

133.) ***Saraburi Hospital in Thailand*** *the hospital confirmed they had been hit with ransomware but that no demand for money had been made.*

134.) ***Ukraine software developer and IT services provider SoftServe*** *suffered a ransomware attack that may have led to the theft of customers source code.*

135.) ***The Fourth District Court of Louisiana*** *suffered a Conti attack , a relatively new ransomware strain. The administrative infrastructure of the courts was affected which led to the website being breached and internal documents being posted online.*

136.) ***Fairfax County Public Schools****, Virginia's largest school system were forced to begin the new school year with remote learning after a ransomware attack affected its systems. The hack reportedly didn't impact distance learning or personal devices.*

137.) ***Manitoulin Transport****, one of Canada's largest trucking companies was the next to disclose that they had become the latest victim of attacks targeting firms in Canada's supply chain. The Conti gang posted stolen data but following discussions with the hackers the firm decided not to pay as the information stolen in the attack wasn't important.*

138.) ***Veiligheidsregio Noord- en Oost- Gelderland (VNOG) in the Netherlands****. The attack damaged internal systems and it is still unclear who was behind it.*

139.) ***The Development Bank of Seychelles (DBS)*** *was next to find themselves a ransomware victim. DBS is a joint venture by the Seychelles government and several shareholders and at the time of writing they were reportedly unclear about how the attack occurred and the damage was still being assessed.*

140.) ***K-Electric, the sole power distributor in Karachi, Pakistan*** *experienced a ransomware attack by the Netwalker gang. The attack led to the disruption of the power utility's billing and online services and the attackers requested a ransom of $3.8 million.*

141.) ***Great Falls Public Schools in Montana****. The school district shut down most of its systems to investigate and recover from the attack. At the time of writing they were working with the department of Justice, the National*

Guard, FBI and other private consultants to remedy the problem and were yet to disclose where the attack came from or what the attackers were requesting as a ransom.

142.) ***Newhall School District in California*** *were next to find themselves victimized by ransomware. The attack locked up the systems and led to the cancellation of remote classes as students where told not to log on to the learning systems or use any district device.*

143.) ***Artech Information Systems****, one of the largest IT staffing companies in the US reported their second ransomware attack in nine months. The REvil gang were responsible for the attack which was picked up by the company following reports of suspicious activity on an employee device.*

144.) ***Duesseldorf University Hospital in Germany*** *suffered an attack which meant they were unable to accept emergency patients. Sadly, this resulted in a loss of life after a patient was re-routed to another facility 20 miles away. A German news outlet reported that the cyberattack was not intended for the hospital and that the ransom note was addressed to a nearby university. The attackers stopped the attack after authorities told them it had actually shut down a hospital.*

145.) ***Massachusetts based IPG Photonics****, a leading developer of fiber lasers for cutting, welding, medical use, and laser weaponry was next to suffer a ransomware attack. It was reported that RansomExx was behind the attack that shut down the IT systems worldwide, affecting email, phones, and network connectivity in the offices.*

146.) ***Ontario's College of Nurses****, the organization that oversees 188,000 members, was next to be hit by an attack. At the time of reporting it was disclosed that personal information may have been impacted but a ransom demand had not yet been received.*

147.) ***University Hospital in New Jersey****. It was reported that the institution suffered a massive 48,000 document data breach after the ransomware operation leaked their stolen data. The SunCrypt ransomware gang claimed to be responsible for the attack.*

148.) ***College in Bolton, UK*** *was the next reported incident in the education sector. Post attack the college engaged a specialist team to launch an investigation*

and mitigate the impact. At time of writing the forensic investigation was ongoing but it was confirmed that some data had been exfiltrated.

149.) ***Italy based Luxottica**, the parent company of Ray Ban made the headlines next. The organization reported widespread service outages but claimed that no customer data had been stolen in the incident.*

150.) ***Anglicare Sydney**, a not-for-profit that provides social services such as aged care was next to report they had been hit by a ransomware attack that saw attackers exfiltrate 17GB of data. Once the cyberattack was detected they immediately embarked on remediation and investigation before strengthening their cybersecurity.*

151.) ***Texas based Tyler Technologies**, the largest provider of software to the United States public sector disclosed that they had become a victim of an attack that affected their internal systems. Tyler reported that there had been no impact on the software they host for their clients and at time of writing, the company, the FBI and the Department of Homeland Security all declined to answer questions on the extent of the hack, the risk of related breaches and the suspected identity of the perpetrators.*

152.) ***French carrier CMA CGM** became the latest big name in container shipping to reveal it had become a victim of ransomware, following other leading liners including Maersk, MSC and Cosco in recent years. The Ragnar Locker ransomware gang instructed them to make contact within two days via live chat to pay for the ransom key.*

153.) ***Universal Health Services**, one of the largest healthcare providers in the United States was next to be hit by a ransomware attack. Its speculated that the Ryuk gang was behind the attack and details of how widespread the issue is are still unknown. UHS has 400 hospitals and healthcare facilities in the US and the UK and serves millions of patients each year.*

154.) ***Clark County School District in Las Vegas**. The attack which activated at the end of August triggered a data breach involving Social Security numbers, student information and other private information according to the Wall Street Journal. An investigation is ongoing and the district has pledged to keep parents, employees and the public informed as new information about the incident becomes available.*

155.) *International insurance brokerage firm Arthur J. Gallagher & Co. The company confirmed that the attack had occurred on September 26th and that the incident impacted a "limited portion" of its internal a material impact on its operations or finances.*

October - 2020

156.) *Philadelphia based eResearch Technology (ERT) where a ransomware attack disrupted clinical trials being run to develop tests, treatments, and a vaccine for COVID-19.*

157.) *UK's second largest privately owned insurance broker, Jersey headquartered Ardonagh Group. According to reports from The Register, the firm was forced to suspend 200 internal accounts with admin privileges as the incident progressed through its IT estate. The firm didn't deny that the attack was ransomware but they did not confirm any specifics.*

158.) *Texas based customs broker and freight forwarder Daniel B. Hastings. The company, who specialize in U.S.-Mexico cross-border shipments didn't comment on the attack, but the exfiltrated company files were posted online from the Conti ransomware gang.*

159.) *Hall County Government in Georgia. Officials didn't release details of how the attack happened or what was being done to resolve it, government offices including the courthouse, community centers, and the sheriff's precincts were experiencing issues with phone and email services. It's thought that no employee or resident data had been compromised.*

160.) *Springfield Public Schools district. With over 25,000 students, 4500 employees and 60 schools, the is the third largest school district in Massachusetts. Once the attack was identified the district shut down all systems and closed the schools to prevent spread of the attack.*

161.) *Software AG, one of the largest software companies in the world suffered an attack from the Clop ransomware gang who demanded more than $20 million. After negotiations failed the Clop gang published screenshots of the company's data on the Dark Web, the screenshots showed employee passport and ID scans, employee emails, financial documents, and directories from the company's internal network.*

162.) *US trucking company Daseke became a victim of the Conti ransomware gang next. Thousands of internal documents exposing the personal information of their drivers and other sensitive data was posted to the Dark Web. Texas-based Daseke declined to offer further information as the investigation into the attack continues.*

163.) *City of Mount Pleasant in Michigan was next to fall victim. According to a press release, a remote ransomware attack was detected on the city's computer and phone systems. Michigan State Police were conducting an investigation and it's not thought that any personal data had been breached.*

164.) *Australian based facilities services provider Spotless Group was the next company to hit the headlines when a number of their servers were compromised in a ransomware attack. They join other large Australian companies including Toll Group, Lion, BlueScope and Regis Healthcare as 2020 victims of ransomware.*

165.) *Yazoo County School District in Mississippi. Following the attack, the school took its IT systems offline and engaged a cybersecurity firm to help recover data encrypted by threat actors. The school board voted to pay $300,000 to recover the data that was encrypted by malware.*

166.) *The Lake George Land Conservancy in New York was the target of a ransomware attack on its internal computer server. The organization revealed that no sensitive donor data was compromised and all data had been backed so they did not intend to pay a ransom.*

167.) *Global legal firm Seyfarth Shaw disclosed that they had become a victim of a sophisticated and aggressive ransomware attack. At time of writing, it's unknown who was behind the attack and the extent of the incident.*

168.) *German based game developer Crytek suffered an attack at the hands of the Egregor ransomware gang. In addition to encrypting the devices, the gang claims they have stolen unencrypted files from Crytek and have leaked a 380MB archive on their data leak site.*

169.) *A ransomware attack caused outages at Sports data provider Stats Perform during the college football slate, causing issues at daily fantasy sports sites including FanDuel, DraftKings and others.*

170.) *New York based Yorktown and Croton-Harmon schools both reported cybersecurity attacks. Croton-Harmon confirmed the incident was a ransomware attack, however Yorktown did not confirm the attack was indeed ransomware.*

171.) *Toledo Public Schools (TPS) was next report an incident. The district confirmed that a cyberattack had occurred in September but they were unaware that data had been compromised. It has since been confirmed that Maze ransomware was responsible for the attack and more than nine gigabytes of data were dumped which included social security numbers, addresses and more for employees as well as current and former students.*

172.) *India based snacks manufacturer Haldiram's experienced a ransomware attack on its servers. Hackers left a message on all affected services confirming it was a ransomware attack and that all data, files, applications and systems had been encrypted and a ransom would have to be paid to release the data.*

173.) *Major US bookseller Barnes and Noble was the next company to hit the headlines when they experienced a number of outages. This led to some customers being unable to access their Nook libraries while others were locked out of the platform completely.*

174.) *Australia based container logistics platform Containerchain. According to the firm they quickly identified the ransomware cyberattack and immediately implemented an emergency response procedure resulting in limited data loss and downtime.*

175.) *The City of Shafter in California announced that its IT system has been compromised by ransomware. In an Instagram post they revealed that the city's IT system appeared to be frozen and locked. According to the city, it is not believed that any personal information has been obtained and in a follow up post they revealed that they had hired a privacy legal counsel and a forensic investigation firm to determine if any personal information had been compromised.*

176.) **Dickinson County Healthcare System** *were the victim of an attack that disrupted access to computer systems across its hospital and clinics. The hospital is working with third-party forensic experts to determine the full impact of the attack to restore its systems. At time of writing, they claimed there was no indication that any data was accessed or taken as a result of this incident.*

177.) **Montreal public transport agency The Société de transport de Montréal (STM).** *Hackers demanded a ransom of US $2.8m to restore normal network operations but according to the agency no data was exfiltrated and they were not intending to pay the ransom. Bleeping Computer reported that the RansomExx gang had been responsible for the attack that knocked the agency's reservation system and caused an outage that affected around 1,000 of STM's 1,600 servers.*

178.) **The Caribbean's largest conglomerate, Ansa McAl** *became the victim of REvil ransomware. It's understood that work at Tatil, the country's biggest insurer was stalled for two weeks as the IT department works to find and expel the ransomware from the company's servers. It is unclear exactly what data and systems were compromised, but Newsday was told whatever was attacked is "very important (mission-critical) data that is crucial to Ansa's operations." Clients' personal data was not compromised, Newsday was told.*

179.) **Boston commuter operator Keolis Commuter Services**. *The company's threat detection systems alerted the operator who managed to deactivate its network within a few hours. Passenger data isn't stored by the company but it is possible that employee data may have been stolen in the attack.*

180.) **French-headquartered IT outsourcer Sopra Steria** *was next to be struck by a cyberattack. At time of reporting the business declined to say what had happened but French media reports indicated that Sopra Steria's Active Directory infrastructure had been compromised by hackers linked to the Ryuk malware gang.*

181.) **Mental health records** *of hundreds of patients from* **Finland based psychotherapy center Vastaamo**. *Hackers demanded 450,000 Euros in exchange for ceasing publication of the data which included that of minors. It has been speculated that the ransom was paid after the data leakage ceased.*

182.) *Indian news agency Press Trust of India (PTI) was hit by a massive ransomware attack which shut its servers down for hours. The attack disrupted operations and the delivery of news to subscribers but no ransom was paid.*

183.) *India restaurant chain Mithaas was hit with ransomware. The case comes within two weeks of the attack at snack company Haldiram's.*

184.) *Michigan based golf and ski resort operator Boyne Resorts was hit by a WastedLocker attack that forced the company to shut down parts of its network. As a result of the attack customers were unable to make online reservations when the booking system was knocked offline.*

185.) *Steelcase Furniture, another Michigan based company was next to be hit. Steelcase is the largest office furniture manufacturer globally, with 13,000 employees and $3.7 billion in revenues. The Ryuk gang is thought to be behind the attack which forced the shutdown of their network.*

186.) *Sky Lakes Medical Center in Klamath Falls Oregon was victimized by the Ryuk ransomware gang. The attack took computer systems offline and forced clinicians to switch to pen and paper to record patient information. No evidence has been found to indicate patient information was compromised, although the Ryuk gang is known to exfiltrate patient data prior to file encryption.*

187.) *Multinational energy company Enel Group were hit by ransomware for the second time this year. The Netwalker gang demanded a $14 million ransom for the decryption key and to not release several terabytes of stolen data.*

188.) *Lawrence Health System in New York were forced to divert ambulances at three area hospitals after a ransomware attack. The three hospitals hit included Canton-Potsdam Hospital, Gouverneur Hospital and Massena Hospital.*

189.) *Australia media monitoring company Insentia became the next victim. Most government departments and large corporations in the country are clients of the firm. The firm told the Australian Stock Exchange that it was urgently investigating a cybersecurity incident that was disrupting services involving its media portal – a service customers use to see media reporting on them, or issues of interest to them, and find journalists.*

190.) *Chenango County in New York found themselves a victim of ransomware when around half of their 400 computers were found locked. The attack primarily targeted the county's email system. It's thought the attackers were Hong Kong based according to an investigation by the New York state Department of Homeland Security. The hackers demanded $450 for the release of each machine, making the total bill around $90,000. At time of writing the county claimed they did not intend to pay the ransom.*

191.) *The networks of the Hanover Chamber of Crafts experienced ransomware attacks at all four of its locations as well as the wholly owned subsidiary Projekt- und Servicegesellschaft. The Sodinokibi ransomware gang was responsible for the attack.*

192.) *Indian company Dr Reddy's Laboratories admitted to a ransomware attack following a cyberattack earlier this month. The company refused to divulge details of the ransom and said they are working with a third party to recover and restore their data. They don't believe the attack is connected with the Russian Covid-19 vaccine Sputnik V. that Dr Reddy's plans to distribute in India.*

193.) *The University of Vermont Health Network - the Ryuk gang strikes again. An anonymous source who spoke to the press stated that as many as 20 medical facilities have been hit by the recent wave of ransomware. The figure includes multiple facilities within the same hospital chain.*

194.) *The city of Salem, New Hampshire announced that they had become the victim of a sophisticated cybersecurity attack involving ransomware. The attack cut off access to internal systems and may have exposed data. Investigators probing the incident learned that data may have been exfiltrated from certain servers.*

195.) *Las Vegas, international casino equipment supplier Gaming Partners International became a victim of the REvil gang. According to a recent interview with a Russian tech blog, REvil hacked and encrypted all servers and working computers at the company. The hackers also exfiltrated more than 500 gigabytes of data during the breach including casino contracts, banking information and technical documents related to GPI products. REvil gave the company 72 November was the third busiest month of the year with 28 hours to respond.*

November - 2020

196.) **US toymaker Mattel** *revealed they had been a victim of a ransomware attack earlier in the year. Mattel claimed that the attack was initially successful and it resulted in the encryption of some of its systems. The toymaker said that a subsequent forensic investigation concluded that the ransomware gang did not steal any data relating to its business, customers, suppliers or employees.*

197.) **Sonoma Valley Hospital** *confirmed that its system - wide computer shutdown in October was due to a ransomware attack. Hackers demanded a ransom to release data but at time of writing the hospital had not paid the ransom. The attack was likely part of the Russia backed campaign that recently targeted as may has 400 healthcare organizations across the US.*

198.) **Japanese game developer Capcom** *fell victim to an attack at the hands of the Ragnar Locker gang who claimed to have stolen 1TB of sensitive data from their corporate networks in the US, Japan, and Canada. The ransom note included screenshots of stolen files, including employee termination agreements, passports, sales reports and bank statements.*

199.) **Italian beverage giant Campari Group** *was the next big-name brand to suffer an attack. An investigation into the attack is ongoing and some researchers suspect the Ragnar Locker gang is responsible.*

200.) **Brazilian Superior Court of Justice (STJ).** *The ransomware operators behind the attack claimed that the entire STJ database has been encrypted and any attempt to restore the files would be in vain. It is the hackers demanded an unknown amount of ransom to decrypt the encrypted court data.*

201.) **The GEO Group**, *the company best known for operating illegal immigration detention centers and private prisons in the US were next to disclose that they had been victim of an attack earlier in the year. The attack exposed sensitive inmate and resident information. The group said that the incident impacted only a small part of its network of 123 private prisons, processing centers, immigration detention centrer and mental health facilities, spanning the US, South Africa, Australia and the UK.*

202.) ***E-commerce software vendor X-Cart*** *disclosed that they had suffered a ransomware attack that brought down customer stores hosted on the tech company's platform. The attackers gained access to a small number of servers which they encrypted which effectively shut down X-Cart stores running on top of the impacted systems. Although they claim only a small percentage of the infrastructure was affected, some of the store owners are said to be considering a class-action lawsuit as a result.*

203.) ***Taiwanese electronics giant Compal****, was next to make the ransomware headlines. The company who builds laptops for some of the world's largest computer brands suffered an attack at the hands of the DoppelPaymer gang. The attack is said to have impacted around 30% of Compal's computer fleet.*

204.) ***UK based housing association Flagship Group*** *were forced to take their IT systems offline after the Sodinokibi ransomware strain entered the company via a phishing attack. The association, a landlord for over 30,000 homes in the east of England admitted that there had been some data encryption and some personal customer and staff data has been compromised. It remains unclear how many individuals have been affected.*

205.) ***Iowa based medical billing company Timberline Billing Service LLC*** *is boosting its cybersecurity after an unknown attack encrypted files and exfiltrated data earlier in the year. The security incident was reported to the Department of Health and Human Services' Office for Civil Rights as a data breach affecting up to 116,131 individuals.*

206.) ***Biomedical and clinical research company Miltenyi Biotec*** *suffered a Mount Locker attack that affected the firm's global IT infrastructure. The company's 2,500 employees from 28 countries are working to develop cell research and therapy products for clinicians and researchers working on covid-19 vaccines. The company said that it has successfully restored all operational processes impacted but they were still facing issues with email and telephone services in some countries.*

207.) ***Chilean-based multinational retail giant Cencosud*** *was hit by an Egregor Ransomware attack that impacted services across its stores. Cencosud is one of the largest retail companies in Latin America with revenues of $15 billion and over 140,000 employees.*

208.) **Managed.com**, *one of the biggest providers of managed web hosting solutions was forced to shut down all of its servers following a ransomware attack. The attack impacted the company's public-facing web hosting systems resulting in some customer sites having their data encrypted.*

209.) *A ransomware attack on cold storage giant* **Americold** *impacted their operations including, email, phone systems and inventory and order management. The company who manages 183 warehouses worldwide and has around 13,000 employees offers supply-chain services and inventory management for retailers, food service providers, and producers.*

210.) **The City of Saint John in Canada** *was next to confirm that a recent cyberattack against them was indeed ransomware. Officials have declined to say how much money was demanded by the attackers or what systems had been affected.*

211.) **Lehigh Valley Library in Pennsylvania** *was forced to close after falling victim to an attack. Affected servers were taken offline and the library remained closed while the attack was investigated and systems were restored.*

212.) **Nexia Australia and New Zealand**, *a network of solutions-focused accountancy and consultancy firms were next to disclose that they had been hit by REvil ransomware. The attackers claimed to have stolen 76GB of data during the incident, however, Nexia denied this and said that the incident was swiftly dealt with by their IT providers and there was no evidence of any movement of data or files.*

213.) **New Zealand based flower wholesaler New Zealand Bloom**. *The company stated that they had no intention of paying a ransom as the consequences of the attack were not serious and the data leaked online was not of a sensitive nature.*

214.) **Jackson County in Oregon**. *The attack downed the county's website following the recent ransomware attack on their web-hosting service provider, Managed.com*

215.) **South Korean fashion and retail company E-Land** *was forced to shut down 23 of its 50 branches following a ransomware attack. E-Land is most known for its fashion and apparel line and is one of the most famous companies in South Korea. The company is working with police and cyber experts to investigate the attack.*

216.) ***Manchester United Football Club*** *made serious headlines when it was revealed that they had suffered a cyberattack. Later confirmed to be ransomware, the club disclosed that although the attack was sophisticated, they had extensive protocols and procedures in place for such an event and they were prepared. They maintain their cyber- defenses identified the attack and shut down affected systems to contain the damage and protect data.*

217.) ***Law In Order, an Australian supplier of document and digital services*** *to law firms. The company were victims of the Netwalker ransomware gang. It had been initially reported that they had seen no evidence of data exfiltration, however, this was later updated to say a very small proportion of data had been exfiltrated after online accounts linked to Netwalker posted proof of the attack and threatened to publish data online if a ransom was not paid.*

218.) ***Ritzau, the largest independent news agency in Denmark*** *responsible for delivering news to virtually all major media in in the country, had their editorial systems shut down following a ransomware attack. In a statement they confirmed that they did not intend to pay the ransom. While the ransomware group who successfully encrypted their systems is not yet known, the attack which managed to encrypt around 25% of the servers has been described as "very professional". Ritzau's IT department is working on restoring all affected computers and bringing them back online.*

219.) ***US Fertility****, a network of fertility clinics was hit by a ransomware attack that compromised patient information. A security incident had been identified in September after some devices on the network became inaccessible. The company then found multiple systems had been affected by ransomware. Further investigation revealed that an unauthorized party accessed data including patient names, addresses, birthdates and Social Security numbers during August and September.*

220.) ***Advantech****, the industrial automation and IoT chip maker confirmed that a ransomware attack that hit its network and that company data had been exfiltrated. The attack was carried out by the Conti ransomware gang who demanded a $14 million ransom to decrypt the affected systems and to stop leaking stolen company data. Advantech employs 8,000 people in 92 cities globally.*

221.) **Delaware County in Pennsylvania** were the next reported victim of the DoppelPaymer gang. Systems were taken offline while the organization worked with computer forensic specialists to determine the nature and scope of the event. Emergency services were not affected but the county did opt to pay the $500,000 ransom.

222.) **Baltimore Public Schools** was forced to cancel online learning for its 115,000 students after a ransomware affected its systems. Very little information has been released about the attack but county police are working with the FBI.

223.) **Endemol Shine**, the global production company behind television shows such as "Big Brother," "MasterChef" and "The Voice". The company has disclosed that they have reason to believe personal employee data and commercially sensitive information may have been compromised. The attack was claimed by the DopplePaymer who have shared several documentson the Dark Web.

December – 2020

224.) **Online education vendor K12**. Threat actors accessed back office systems during the attack and a press release stated that student and staff information was on the systems. A spokesperson confirmed that a ransom had been paid.

225.) **Translink, Vancouver's transportation network** disclosed they had been a victim of ransomware at the hands of the Egregor gang. Payment systems were affected but customers were assured that credit card and payment information had not been accessed.

226.) **US retailer Kmart**. The attack resulted in a number of servers on its network becoming encrypted. A ransom note showed that an HR website used by the store had also been brought offline by the hackers. Kmart's e-commerce site was unaffected.

227.) **Brazilian aerospace giant Embraer** reported that they had been a victim of ransomware. The company chose to restore its affected systems and refused to negotiate with the attackers which promoted the RansomExx gang to leak some company data.

228.) **Randstad, the world's largest staffing agency** *was the next reported victim of the Egregor gang. Unencrypted files were stolen during the attack and a subset of the data was later published.*

229.) **Swiss helicopter manufacturer Kopter** *fell victim to the LockBit gang who encrypted the company's files and published a subset of them after they refused to engage. The hackers claimed that they broke into the company's network by taking advantage of weak password used by a VPN appliance.*

230.) **Greater Baltimore Medical Center (GBMC HealthCare)** *was hit by a ransomware attack that impacted its computer systems and operations. The hospital initially stated they had robust systems in place to deal with the attack. However, a GBMC nurse who spoke to the press anonymously said that the attack had set the facility back decades.*

231.) **Electronics giant Foxconn** *suffered a ransomware attack at a Mexican facility during the Thanksgiving break. Following the attack, the DoppelPaymer ransomware gang published files belonging to Foxconn NA on their ransomware data leak site. The attackers demanded a ransom of $34 million.*

232.) **Minnesota based Managed IT Services provider NetGain Technologies** *were forced to take its data centers offline following a ransomware attack. While the company declined to speak to the press about the attack, its clients were informed and were told they were running tools and scans to detect, isolate, and clean-up any affected environments whilst working alongside security specialists.*

233.) **Haberdashers' Monmouth Schools**, *an independent schools' group in Wales was hit by the Sodinokibi ransomware gang. The hackers deleted files belonging to staff and pupils and encrypted records.*

234.) **The town of Independence Missouri** *revealed that they had been a victim of a ransomware attack that resulted in technical difficulties and disruption to multiple services but it had been halted before the full city network had been infected. The City Council had previously approved over $4 million worth of IT and cybersecurity upgrades designed to prevent these types of attacks; however, it was unclear how many upgrades were in place at the time.*

235.) *Georgia based payment processing company TSYS. The attackers claimed to have published over 10 gigabytes of TSYS data but the company said the attack only impacted its administrative wing and not any payment data. TSYS did not confirm if any ransom had been paid.*

236.) *Intel-owned AI processor developer Habana Labs suffered an attack at the hands of the Pay2Key ransomware operation. The hackers leaked company data and, in a threat, posted to their leaked data site they stated that Habana Labs had 72hrs to stop the data leaking process.*

237.) *Australian automotive services provider Inchcape became the next victim of RansomEXX. The gang leaked data on the Dark Web following the attack.*

238.) *Weslaco ISD in Texas reported that the school district's computer network was attacked by ransomware and that the FBI were investigating the incident. A statement from the organization said they did not know if personal information relating to staff and students had been compromised.*

239.) *Norwegian cruise company Hurtigruten disclosed that its systems had been hit by a significant ransomware attack in which the cruise lines global IT infrastructure had been affected. At time of writing, it's not known who was behind the attack.*

240.) *Germany based flavor and fragrance developer Symrise were forced to halt production following an attack claimed by the Clop ransomware gang. The attackers allegedly stole 500 GB of unencrypted files and encrypted close to 1000 devices. Images of the stolen files were posted on the attackers' data leak site.*

241.) *Trucking and logistics firm Forward Air revealed they had been targeted by a ransomware attack and warned that it may defer or lose revenue as a result. This attack is the first we have recorded for the Hades ransomware group.*

242.) *The City of Ellensburg in Washington were next to announce they had been the victim of a ransomware attack. Not much is known about the attack but the city is now working with both local and federal law enforcement to investigate.*

243.) *Canadian Sangoma Technologies were struck by a ransomware attack involving the Conti gang. Private and confidential data stolen during the attack was later posted online and the company said that it has launched*

a comprehensive investigation to fully ascertain the extent of the data breach and it's working closely with outside cybersecurity experts.

244.) ***Whirlpool*** *suffered a ransomware attack by the Netfilim gang who stole data before encrypting their devices. The hackers later published stolen data which included documents relating to employee benefits, medical information requests, and background checks.*

245.) ***The City of Cornelia in Georgia****. In a press release to local media officials confirmed the attack and disabled the network while they work with law enforcement to investigate.*

246.) ***General Medical Laboratory (AML) in Antwerp****, a laboratory working closely on the management of the Covid-19 pandemic suffered an attack by the Clop ransomware gang. Hackers installed ransomware on the lab's website which brought it to a standstill. They demanded a ransom before they would release the site from captivity.*

247.) ***Arizona-based healthcare organization GenRx Pharmacy*** *issued a warning to patients over a potential data breach following a ransomware attack earlier in the year. Malicious hackers successfully removed some files that included patient information including first and last name, address, phone number, date of birth, gender, allergies, medication list, health plan information, and prescription information. An entry on the US Department of Health and Human Services' HIPAA breach portal indicated that more than 137,000 GenRx patients were being informed about the incident.*

248.) ***New Zealand based financial services firm Staircase Financial Management*** *NetWalker blog had a countdown clock indicating how much time was left before the data was made public. That clock has since run out and the data was made public across multiple third-party file sharing sites.*

249.) ***Richter Advisory Group Inc.,*** *the court-appointed receiver of* ***Canadian company Nygard's assets*** *confirmed that Nygard was a victim of a ransomware attack. IT staff identified the ransomware responsible as Netwalker. The initial ransom demand was approximately 99 bitcoins — equivalent to more than $3.6 million but this rose to 198 bitcoins — equivalent to more than $7.2 million when the company failed to respond.*

250.) ***Fergus Falls Minnesota*** *The systems at Lake Region Healthcare were affected by a ransomware attack.*

Inference – Synopsis - Recommendations

Malware has come into a new age with attacks on computer systems increasing rapidly. ***What is Ransomware?*** *It is a form of malicious software that targets your computer limiting access until you pay a ransom. In the last few months, hackers have actively resumed ransomware attacks.*

Simply put, hackers are hindering people from accessing their networks and asking for huge payments to regain access. The hackers have managed to cripple government networks. Small businesses were crippled and hospitals were forced to turn away patients. These events were blamed on ransomware in which entire computer networks shut down. The hackers then demanded colossal amounts of money to have them running again.

How often do these attacks take place? ***Every Single Day and Increasing…***

*At least three-quarters of ransomware attacks end up in data being encrypted. In the last year alone, 51% of businesses were affected by ransomware. Most of these attacks resulted in data being encrypted. At least 26% of the victims paid a ransom to get their data back. **

*26% of victims whose data was encrypted got their data back by paying the ransom. A few of those who paid the ransom did not get their data back. However, 95% of businesses that paid the ransom got back their information. **

Also, most of the organizations got back data that was encrypted. Many got their information back through alternative options such as backup rather than paying the ransom.

*A further 1% paid the ransom but didn't get their data back. Overall, 95% of organizations that paid the ransom had their data restored. When you pay the ransom, you multiply the cost of enduring a ransomware virus attack.**

And Now you have legal requirements that you must adhere to. In short, being attacked is a nightmare!

We at Covington & Associates, offer ***Free consulting*** *on solutions that assist you in preparing your anti-Malware/Ransomware strategy. We additionally have solutions that work with your existing technology that will* ***a.) Harden your environment to protect against Ransomware, and b.) Rapidly recover (3-5 minutes) your IT environment in the event of an attack****.*

Need More Information…

Visit our Website: - https://www.CovingtonCA.com

Call us at: (702) 381-7452 or;

Email Us at: info@CovingtonCA.com

Your Business Partner for:

- *Data Loss Protection*
- *Outage Reduction*

**Source Comodo*