Cyber Security Month
October 2021

BDO CYBER H1 2021 THREAT INTELLIGENCE REPORT

FIND YOUR BLIND SPOT

BDO

INTRODUCTION

2021 has been a particularly interesting year as it comes off the heels of the partially recovered COVID-19 world, and with it, partial social distancing measures. Still, the world is more connected than ever as workforce remains remote to some degree, and unfortunately, that means cybersecurity has become increasingly relevant to virtually everyone. Moreover, firms, governments, and individuals alike tend to view information security retroactively, where issues are often analysed after they occur, and this presents high risk while giving little value in preventing them from recurring.

Despite fields within information security spheres being full of an incredible amount of unorganised, highly technical data, it should be leveraged to generate quality intelligence that increases awareness of probable threats, assesses risk, and re-evaluates priorities and resources that secure an organisations interests.

That said, our report aims to inform decision makers who are not always technically proficient with C-Suite level intelligence that supports business decisions when confronted with cybersecurity risks and allows for adequate preventative and mitigation procedures to be ready when needed.

UNDERSTANDING OUR DATA

The report presents an analysis of confirmed cybersecurity incidents we determined either damaged, threatened, or negatively impacted organisational data assets, directly or indirectly via broader networks and systems.

To ensure relevancy and consistency, it deliberately distinguishes incidents from breaches:

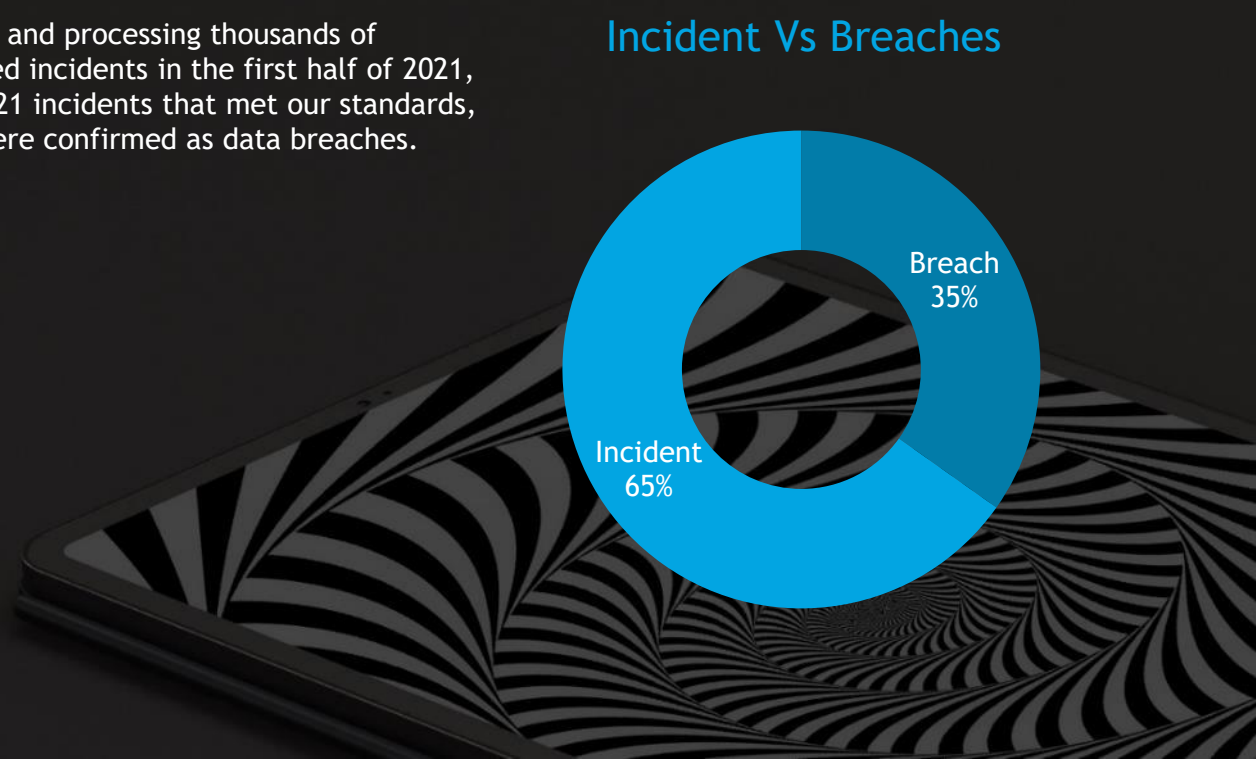
- **Incidents** are defined as either successful or attempted damage to the confidentiality + integrity and access of organisational data assets by an unauthorised party.
- **Breaches** are defined when either the victim or an unauthorised party has confirmed that an organisation's private data assets have been compromised, stolen, or released without authorisation.

We also refer to threat actors as groups, gangs, families, and strains interchangeably, given the high degree of uncertainty associated with attribution in the cyber realm, which as we will explain later, has been complexified by affiliate schemes.

Lastly, given that all data collected is publicly disclosed, actual figures are likely higher as revealing information often conflicts with the victim's interests. In this context, the report refers to large data gaps typical within information security as Not Defined (N/D).

EXECUTIVE SUMMARY

After collecting and processing thousands of publicly reported incidents in the first half of 2021, we analysed 1021 incidents that met our standards, 355 of which were confirmed as data breaches.

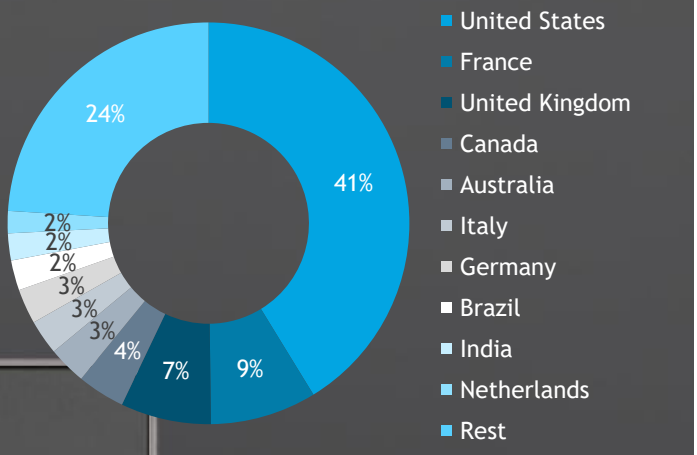


KEY FINDINGS

We identified key areas that pose considerable risks which can and should be managed to some degree. The key takeaways are:

- The Ransomware as a Service (RaaS) market grows in scale and type and continues to dominate the threat landscape in general. Despite the total amount of ransoms payments demanded in H12021 equaling $306 million, ransomware groups are more than willing to negotiate.
- Software vulnerabilities remain far too common despite feasible preventative measures being available, namely adequate Cyber Threat Intelligence.
- Weakly defended sectors such as critical infrastructure and essential services sectors continue to be attacked, given they pose as highly profitable, low-risk targets.
- The human element continues to remain the greatest vulnerability as employees, at all levels, are not sufficiently informed on existing and emerging threats.

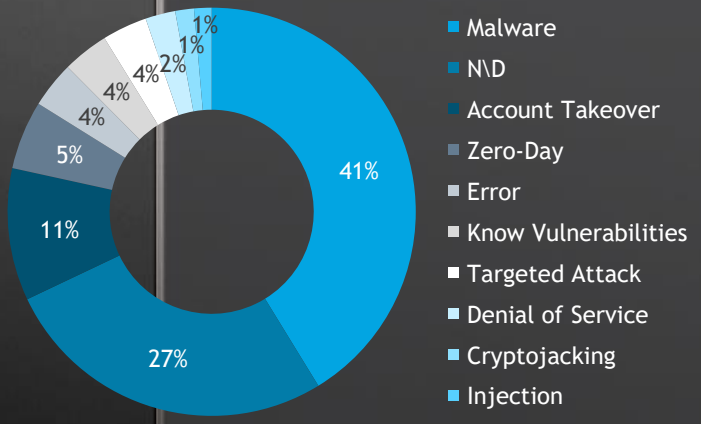
Incidents By Country



LOCATION

Unsurprisingly the United States accounted for the vast majority of attacks at 41%, while almost every G7 country made it into the top ten, (accounting for 76% of all attacks) except for Japan which stayed just outside at 11th place. While it makes sense that the world's leading economies continue to be the focus of financially-motivated actors, it must also be noted that these countries also have relatively stronger regulatory regimes, meaning the data may reflect confirmed breach disclosures rather than actual incidents.

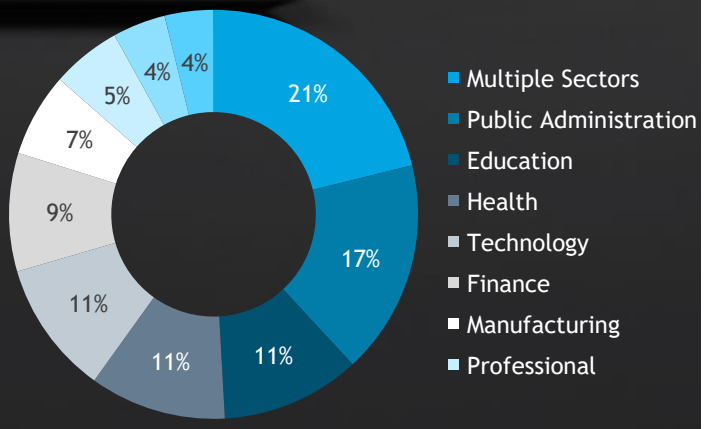
Attack Techniques



PRIMARY ATTACK TECHNIQUES

Malware continues to lead Attack Techniques used by threat actors, accounting for 47% percent of all incidents, 79% of which is Ransomware, a tactic that constituted 33% of all attacks in total. It should be noted that a high level of complexity exists in every incident, meaning significant overlap exists between all categories. For example, malware is often delivered via Trojans, another tactic under the Malware category. For the sake of simplicity, the report categorises Techniques and Tactics as Primary and Secondary attacks.

Attacks By Sector



PRIMARY SECTORS

Multiple industries lead the target distribution at 21%, followed by Public Administration at 17%, and Education, Health, and Tech Sectors at 11%. This is likely due to Public Administration, Healthcare, and Education lacking sufficient cybersecurity resources and IT infrastructure. Increased digitalisation and connectivity via 5G saw all sectors experiencing cybersecurity challenges stemming from APIs services, IoT devices, and cloud infrastructure via inadequately secured wireless networks between different providers.

PUBLIC ADMINISTRATION

Malware takes the first spot for attacks on Public Administration at 47%, followed by Targeted Attacks at 12% and Denial of Service attacks taking third place with 5%. This makes sense given local and federal entities make easy pickings for both ransomware groups, hacktivists, and state-sponsored threat actors.

HEALTH

The data shows that threat actors are willing to exploit virtually any type of organisation for financial gain, and this has largely been expressed by the steady targeting of healthcare institutions. While misconfiguration errors were traditionally the main source of client and patient personal data breaches, 54% of known incidents recorded were the result of Malware as cybercriminals find the perfect extortion victims in hospitals and clinics, while Account Takeover took second place at 13%. In H12021, the US Department of Health and Human Services alone opened 349 investigations into breaches compared to 121 in H12020, a 180% increase. [1]

EDUCATION

Education had a particularly challenging year with post-pandemic online classes continuing in 2021 to some degree. Financially motivated cybercrime actors attempting to access data and systems saw Malware also take the lead in this sector with 49%, followed by 10% Account Takeover and Zero-day vulnerabilities at 7% in the Education vertical.

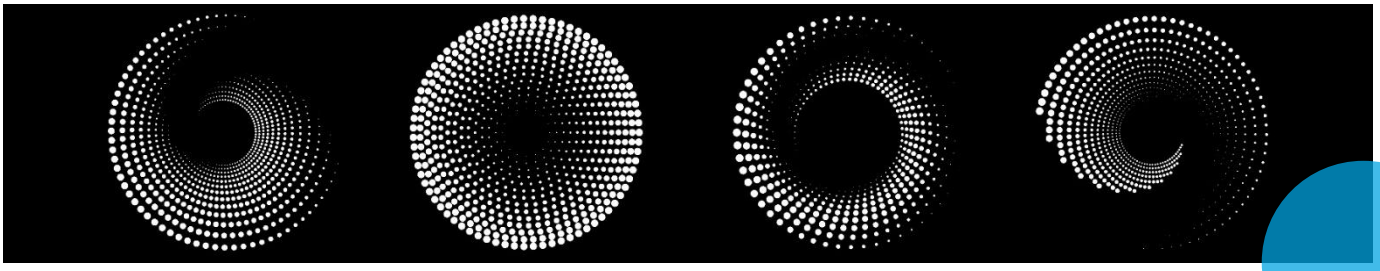
FINANCE AND INSURANCE

The Financial and Insurance Services sector also experienced a wide array of issues stemming from the forced adoption of technologies that present significant changes to the entire industry. This led to the natural increase in cooperation between traditional financial institutions like banks and the FinTech industry, and tech providers in general, presenting supply chain challenges stemming from new partners with whom they share customer databases.

While Malware lead with 31% and Account Takeover at second with 17% are consistent with other verticals, the difference with this sector was evident with cryptocurrency-related techniques, which accounted for 7%, taking over more common Error and Software Vulnerabilities at third place. This is probably because digital banking has seen an acceleration of online transfers during the COVID-19 pandemic, a trend that is projected to continue in the coming years.

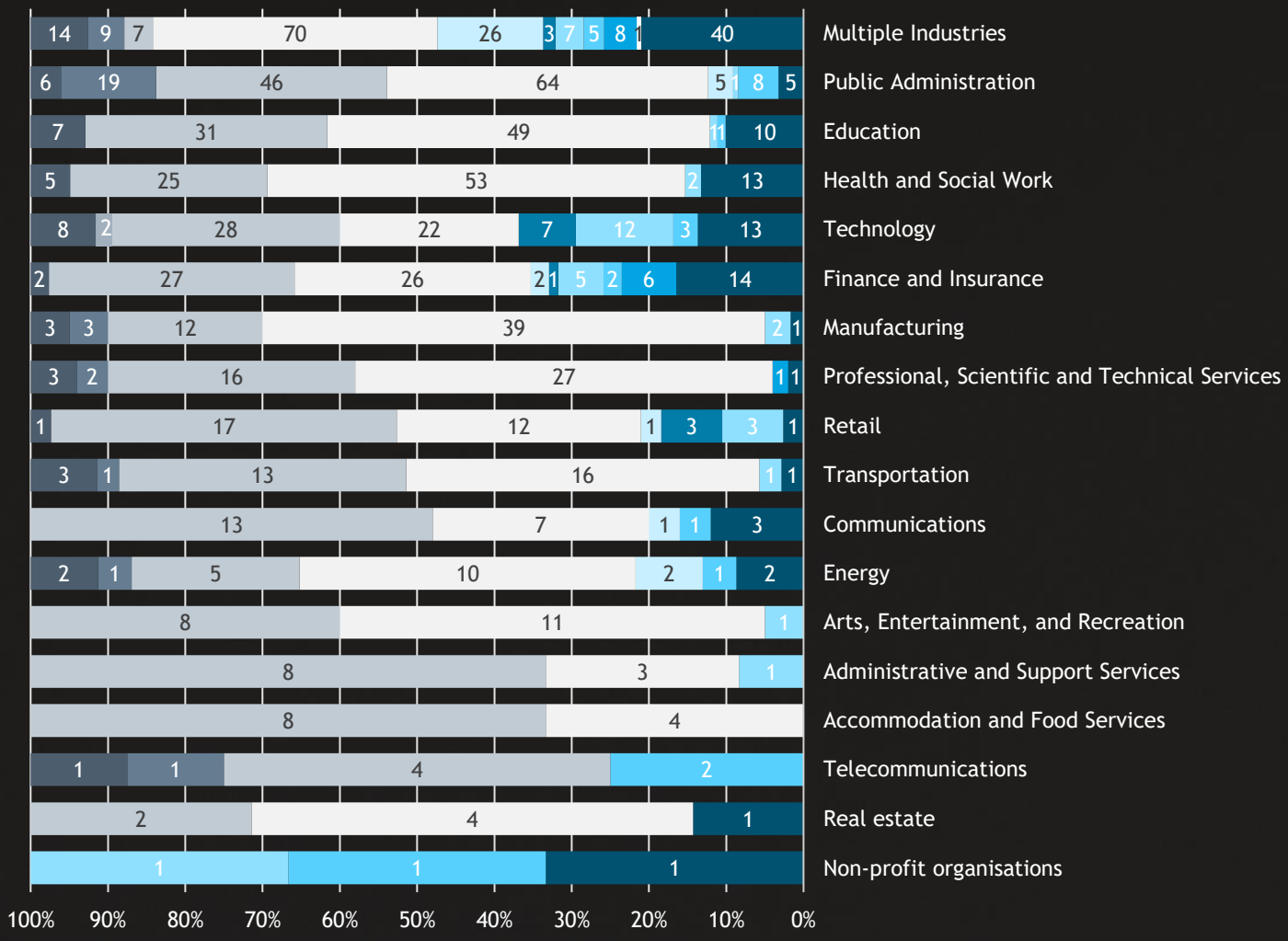
MANUFACTURING

As advancements in information technology have inevitably led to further digitalisation in manufacturing, IT has successfully facilitated improvements in operational technology (OT) and Industrial Control Systems (ICS), leading to the growth in the Industrial Internet of Things (IOT). That said, threat actors sought to exploit the strain on the manufacturing supply chain. Again, Malware leads at a staggering 65% of attacks, with Targeted Attacks and Zero-day vulnerabilities both taking second at 5%, while Error and Account takeover took 3% and 2% of the attack distribution.



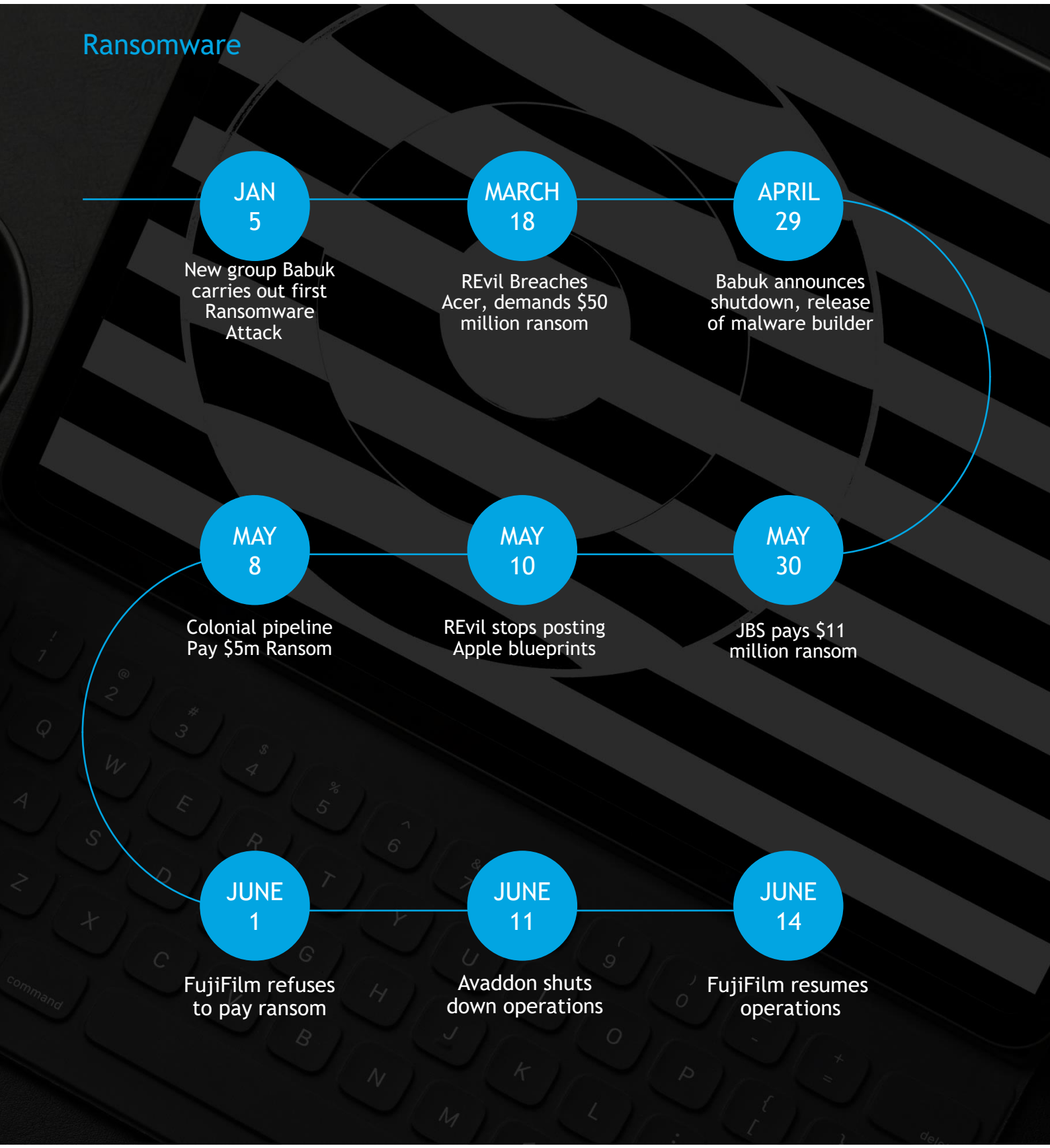
1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

SECTOR BREAKDOWN



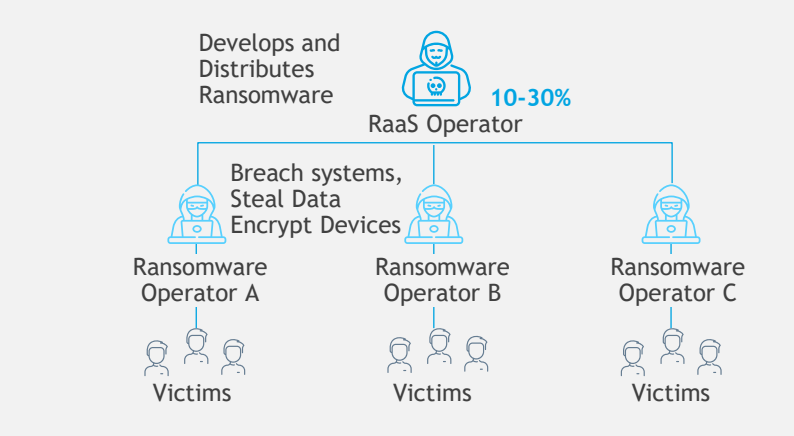
NOTABLE INCIDENTS

Ransomware



EXTORTIONOMICS

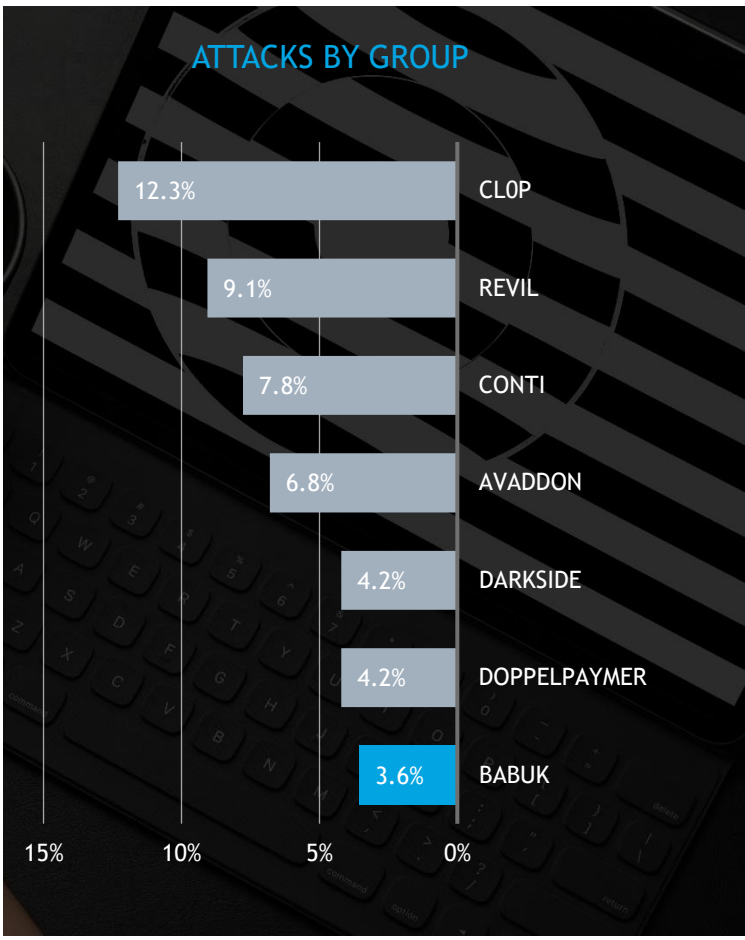
Ransomware continues to be the biggest threat to organisations, accounting for 33% of total incidents, roughly 28% of which were confirmed breaches. Its dominance can probably be attributed to the Ransomware as a Service (RaaS) business model, where operators develop and distribute ransomware to affiliates, who then conduct the reconnaissance and execution of attacks. The former collects anywhere from 10%-30% of the profit, while the latter keeps the rest. This has led to a self-sufficient RaaS market which has seen a particular growth various in schemes, and is perhaps the result of a few key factors.



The first is undoubtedly the growing use of the Double, Triple, and Quadruple Extortion methods. Where traditional ransomware attacks consist of encrypting data and forcing the victim to pay to unlock it, in Double Extortion, ransomware operators also encrypt and threaten to release sensitive data to coerce victims into paying. Triple/Quadruple Extortion occurs when groups go further by threatening victims with distributed denial-of-service (DDoS) attacks on their systems, and/or engage their customers and partners to participate in paying ransoms directly.

The growth of RaaS schemes can also be closely linked to advancements in cryptocurrency, which reassures aspiring cybercriminals with anonymity. Lastly, the uptick in 2021 possibly came after many prominent cybercrime forums banned ransomware-related topics after the practice gained considerable attention from authorities, forcing ransomware operators to promote their services through alternative methods.

NEW KIDS ON THE BLOCKCHAIN



The first ransomware operation in 2021 was recorded by several security researchers who identified the new Babuk ransomware after it hit at least five enterprises by mid-January. After only a few months of activity, the Babuk group posted its intention to quit the extortion business on its leak site, claiming to have achieved their goal. Unlike other groups who releasing their decryption keys after shutting down, Babuk stated it would instead release the source code for its file-encrypting malware. By late June, the Babuk Locker builder was leaked online and was used to attack multiple targets throughout multiple industries worldwide, placing the group in seventh for overall attacks during H12021.

Babuk's entrance and exit within the space of four months, and its subsequent return just two months after retiring, represents a common pattern among ransomware families, which interestingly resembles economic behaviours of normal firms that enter highly profitable markets.

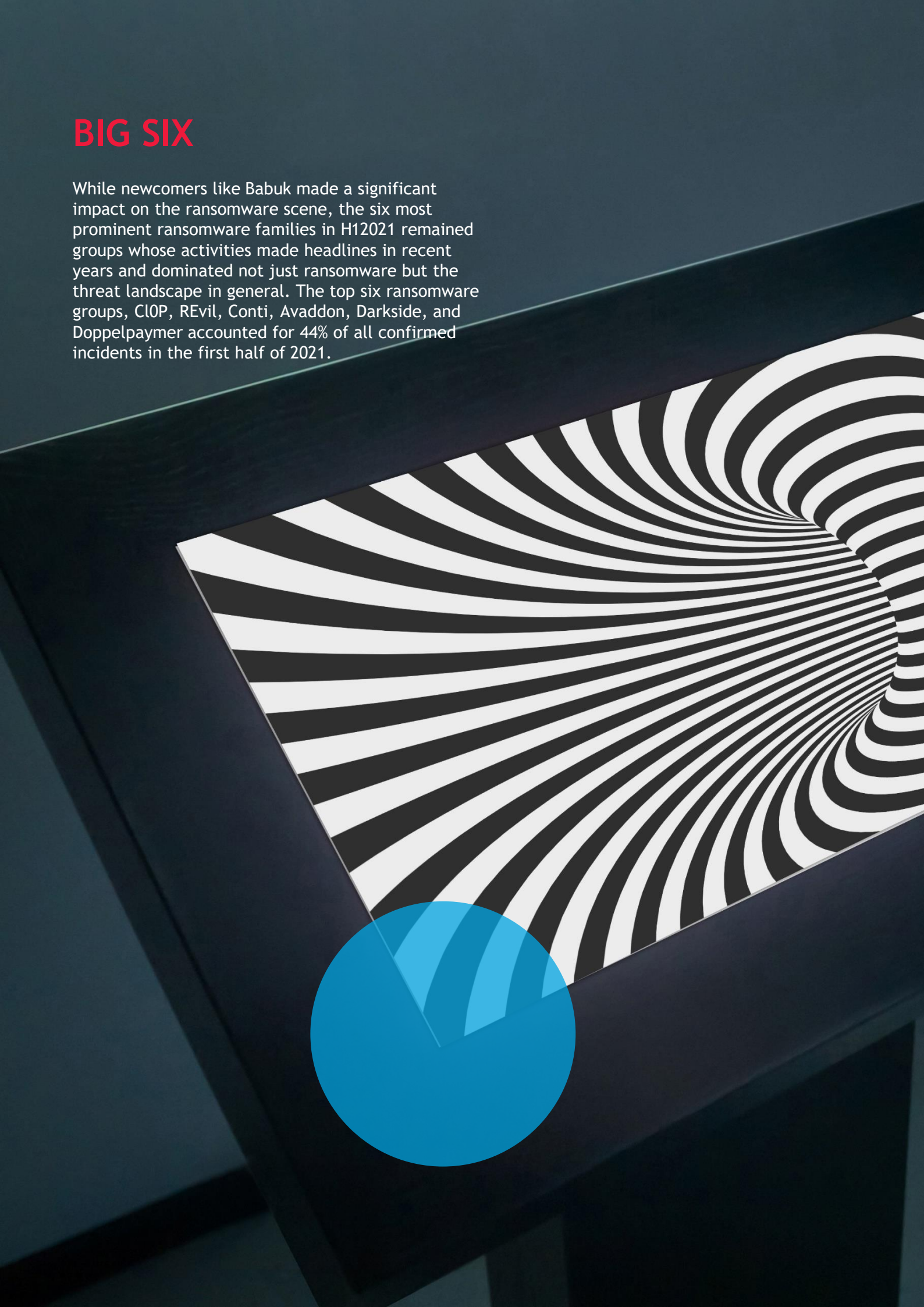
MARKET ENTRANCE, EXIT STRATEGIES

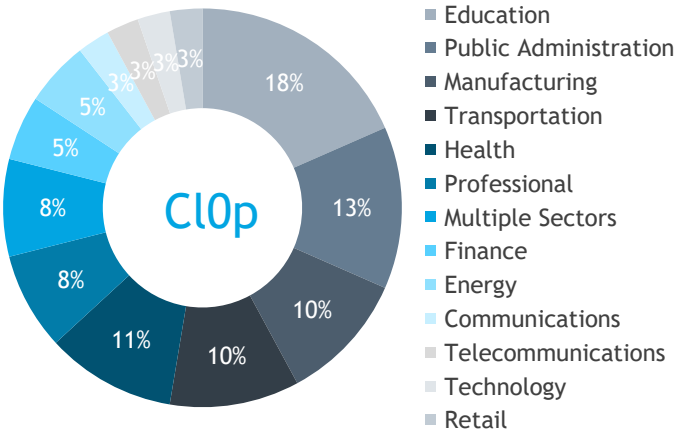
While several high-profile ransomware groups are likely laying low or being arrested, new groups have already begun filling the void. This is probably because many older groups decided to reboot or rebrand their operations by enlisting new affiliates. Increased syndication between experienced and amateur cybercriminals is the result of the growing demand for RaaS variants sold on the dark web, which is supplied by groups that shut down after gaining the attention of authorities.[2] In this context ransomware attacks have increased considerably in both frequency and size, as variants can be easily acquired for an affiliate fee as low as $100. That said, ransomware remains too much of a profitable business to give up. When Babuk returned it spread risk by leaking its builder, while broadening its sector by operating a new leak platform offering new affiliate schemes for actors who created their own Babuk strains to join, including the option of starting their own RaaS operations.[3] Moreover, they only released an older version of their malware and created a new one to get back into extortion operations by focusing on corporate networks, reportedly stating that recent attacks on smaller targets using their older builder were not conducted by them.[4]

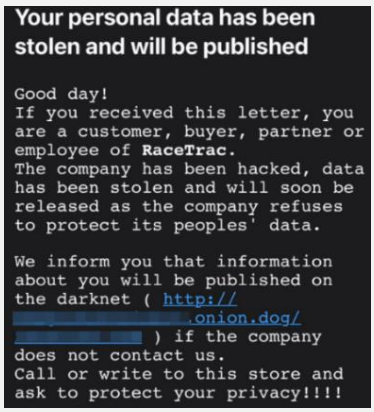
2 https://www.virsec.com/blog/were-it-not-illegal-ransomware-as-a-service-raas-would-be-a-practically-perfect-business-model
Figure 1 - https://www.digitalshadows.com/uploads/2021/05/ransomware-operator.jpg
3 https://securityaffairs.co/wordpress/119467/cyber-crime/babuk-locker-ransomware-builder.html?utm_source=rss&utm_medium=rss&utm_campaign=babuk-locker-ransomware-builder
https://www.technadu.com/builder-babuk-locker-ransomware-leaked-online/286444/
4 https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/

BIG SIX

While newcomers like Babuk made a significant impact on the ransomware scene, the six most prominent ransomware families in H12021 remained groups whose activities made headlines in recent years and dominated not just ransomware but the threat landscape in general. The top six ransomware groups, ClOP, REvil, Conti, Avaddon, Darkside, and Doppelpaymer accounted for 44% of all confirmed incidents in the first half of 2021.





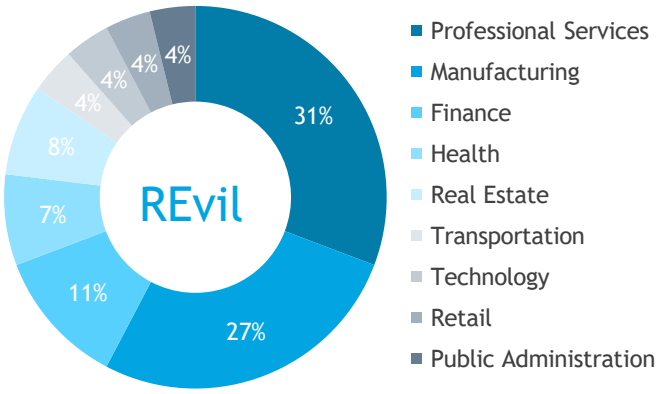


Source: KrebsOnSecurity

Most of Clop's victims in H12021 were the result of the supply chain attack on the Accellion File Transfer Application (FTA) servers which were used by multiple organisations worldwide. It remains unclear whether Cl0p hacked the Accellion servers or was given access to the data by other groups who did. Regardless, Clop managed to obtain the data of multiple high-profile targets such as oil giant Royal Shell, cloud and compliance firm Qualys, U.S. banks Morgan Stanly and Flagstar, international law firm Jones Day, Canadian multinational aircraft manufacturer Bombardier and hundreds of other organisations.

Our data shows Cl0p targeted the Education sector more than any other, which accounted for 18% of its victims, followed by Public Administration and Transportation at 10% each, with Health, Professional Services, Multiple Industries and Manufacturing all accounting for 8% of the attack distribution. Cl0p's activities were particularly notable given their triple extortion tactic of contacting the victim's customers and partners via contact information obtained from the stolen data, to encourage them to pressure the victim company to pay the ransom or else their personal data would be leaked.

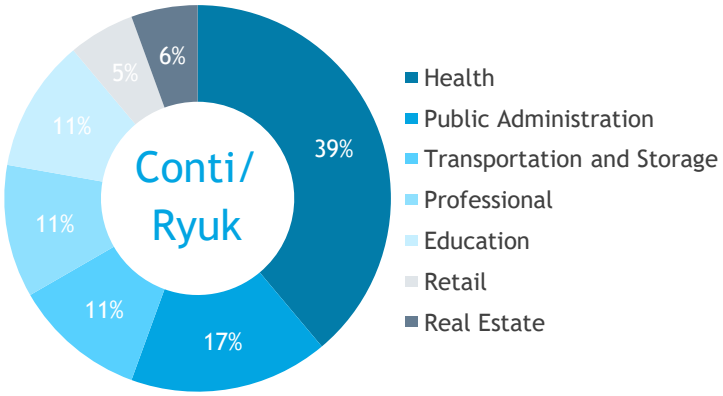
Also known as Sodin/Sodinokibi, the big game hunting ransomware group is perhaps the most notorious of all given the number of high-profile, lucrative enterprises on its victim list. In late 2020, REvil claimed it made over $100 million within one year using the RaaS model, and that its goal is to make at least 2 billion USD.[5] A third of REvil's targets were in the Professional, Scientific and Technical Services, as well as Manufacturing sectors, while Financial, Real Estate and Education accounted for roughly a tenth each.

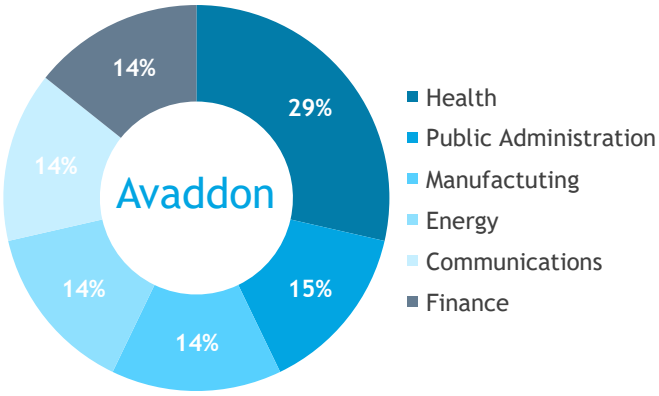


Notable REvil operations recorded this year include attacks on computer and electronics manufacturing giant Acer on March 18 which saw a $50 million ransom, the highest ever recorded. On April 20, the group made headlines by breaching Apple notebook hardware manufacturer Quanta Computer, also reportedly demanding $50 million. After Quanta refused to negotiate, REvil reportedly demanded that Apple pay the ransom or else they would leak technical details of current and future hardware, publishing notebook blueprints every day the ransom was not paid. By May 10, all data relating to the Quanta incident was suddenly removed from the group's darknet site.

Despite Apple not commenting on the breach, given REvil's history of following through on their threats, many experts have speculated that the stolen data was taken down after some form of payment was discreetly agreed between both parties. The group's capability of extracting significant ransoms was confirmed on May 30, when it attacked the IT systems of the world's largest meat processor, JBS SA, shutting down its U.S. and Australia operations. REvil reportedly demanded a $22.5 million ransom, and on June 9, JBS confirmed it paid $11 million.[6]

5 https://www.bleepingcomputer.com/news/security/fbi-revil-cybergang-behind-the-jbs-ransomware-attack/
6 https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/





The Conti/Ryuk ransomware family has a history of focusing on healthcare and public administration.7 This trend remained consistent in 2021, with Human health making up for 39% of its targets. In late May, the FBI identified at least 16 attempted Conti ransomware attacks targeting U.S. healthcare and first responder networks, which included law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities since the beginning of the year. Public Administration accounted for second-most at 17% of total incidents, more than half of which targeted organisations that employ over 1000 people.

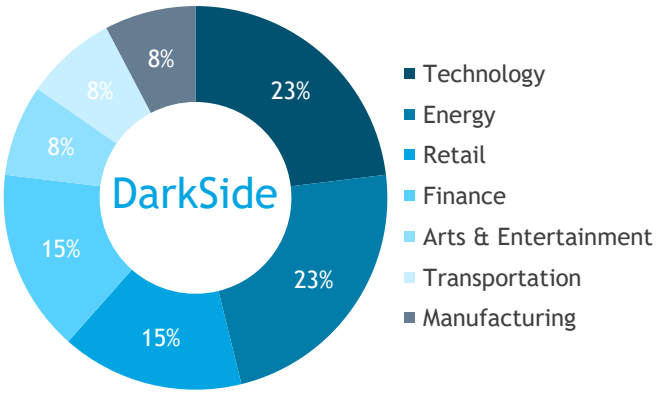
While most of its victims haven't been publicised, confirmed attacks include UK clothing retailer Fat Face, who received a $2 million ransom demand after it was targeted on January 17. More notably, on March 2, the Broward County School District received a $40 million ransom demand, which was dropped to $10 million after the school district offered no more than $500 thousand, causing the data to be leaked after negotiations broke down. French paper cup manufacturer CEE Schisler's data was also confirmed to have been leaked by Conti after they also refused to pay an exorbitant demand.

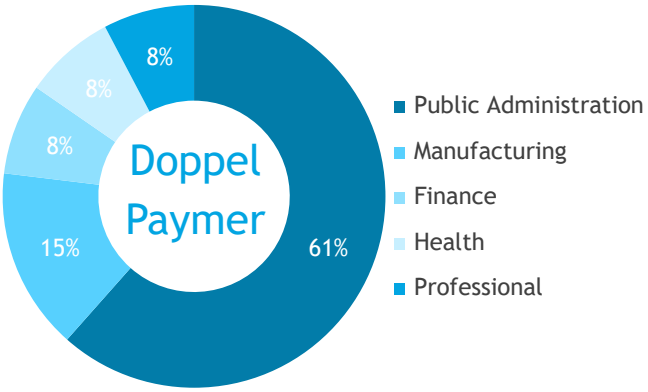
Avaddon is another group known for its proclivity to attack healthcare organisations, our data shows that a third of all its targets were in fact in the Healthcare sector. This is an especially troubling fact given the group and its affiliates are also known to threaten victims who don't pay with DDoS attacks, another example of triple extortion, which in the healthcare sector can in a literal sense be fatal. Public Administration, Manufacturing, Energy, Communications, and Finance made up roughly an equal share of the remaining target list.

Interestingly, on June 11, after deciding to shut down its operations, Avaddon shared its victims' decryption keys to cyber news outlets BleepingComputer, which despite deciding not to name previously unknown corporate targets, did provide valuable insights after security researchers analysed the unique identifiers attached to the released keys.

Unsurprisingly, Avaddon's total victims throughout the years mainly resided in the United States, followed by Canada. The top three industries targeted in recent years include Retail at 12.5%, Manufacturing at 12.2%, and Finance at 7.5%. More interestingly, over 50% of Avaddon's victims earned income below $10 million, while the group used a "5x5" rule to formulate its ransom demands. Avaddon calculated 5% of the annual revenue, estimated as one-fifth of the total revenue, to start the negotiations before dropping the ransom price during negotiations. For example, if a victim company earned a total revenue of $10 million, annual revenue would be calculated as $2 million, and the starting ransom price will be $100 thousand. Avaddon would then drop the price during negotiations, and the end ransom would likely be around $70 thousand. Using this information, security researchers reportedly estimated Avaddon's total earnings were just under $90 million.

7 https://us-cert.cisa.gov/ncas/alerts/aa20-302a





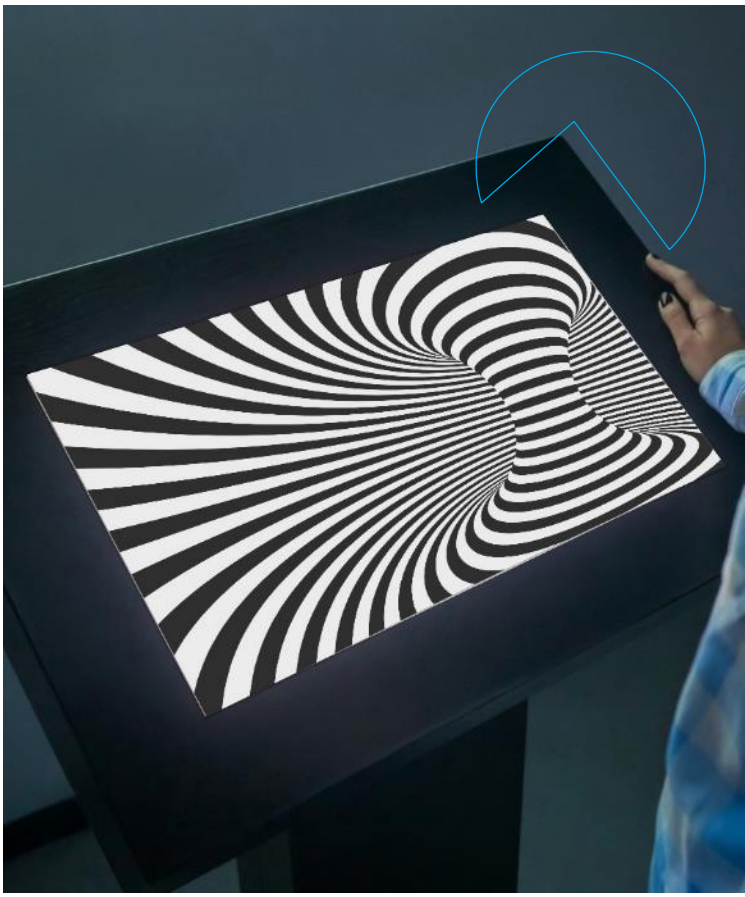
While DarkSide is a relatively new ransomware group that emerged in 2020, several security experts believe it is either an offshoot or former affiliate of REvil, given similarities in their malware and its big game hunting practices. Technology and Energy sectors took the biggest hit, both accounting for roughly a quarter of Darkside's targets, while Retail and the Financial services sectors accounted for 15% each, with Arts, Transport, and Manufacturing accounting for 8% of DarkSide's victims.

Like REvil, the group has proven its ability to extract vast ransom payments. On April 24 the group shut down the U.S. operations of Brenntag AG, the second-largest chemical distributor in North America, who confirmed they paid a $4.4 million ransom. However, DarkSide became notoriously famous on May 7, after it attacked the Colonial Pipeline Company, which operates a major fuel transport system throughout the east coast of the United States, halting all pipeline operations. DarkSide demanded somewhere between $4.4-5 million, which Colonial Pipeline operators paid.[8] Despite U.S. authorities later recovering almost half of the 75 bitcoins used to pay the ransom, Colonial reportedly lost millions in revenue from shutting down the 45% of the fuel it supplies across 5,500 miles (8851 km) throughout the east coast, for five days.

While some reports assert that the ransomware operators were not aware of the Colonial attacks and that it was carried out by an affiliate, this is a largely moot point given RaaS proliferates significant disruption capabilities to multiple actors. Moreover, the extremely high-profile attack garnered significant attention from not just law enforcement but the US federal government, leading to disruptions to the group's recent activities, which is expected to facilitate another ransomware rebranding pattern. Moreover, it brought the ransomware issue to the geopolitical sphere, culminating in a joint G7 statement to the Russian government over its lack of enforcement efforts against Russian speaking ransomware groups in June, and a summit between US President Joe Biden and his Russian counterpart Vladimir Putin days later.

In December 2020, the FBI issued a Private Industry Notification (PIN) regarding increasing DoppelPaymer Ransomware attacks on Critical Infrastructure and industries worldwide, with the group's victims including a disproportional amount of government institutions and organisations.[9]

Many of the private or public sector entities DoppelPaymer claimed to have breached have never been reported in the press. That said, our data seems to correlate with the FBI's warning. Public Administration accounted for two-thirds of their targets, most notably a breach of the Illinois Attorney General's Office on April 10, 2021. Manufacturing accounted for the second most at 15%, leaving Financial and Insurance Services, Healthcare, and the Professional Services sectors at 8% of total attacks each.



8 https://cybernews.com/security/us-colonial-pipeline-hack-an-earthquake-in-the-critical-infrastructure-industry/

9 https://www.ic3.gov/Media/News/2020/201215-1.pdf

LOW HANGING FRUIT

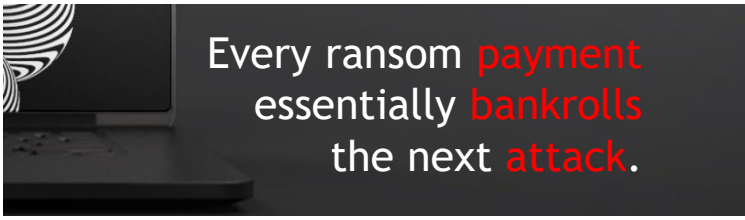
It comes as no surprise that Public Administration, Health, Education, and other utilities that make up critical infrastructure have topped ransomware victim lists. Despite these sectors' data assets, systems, and networks being so vital that any disruption poses debilitating effects on security, economic, and essential services for millions of citizens, most have poor cybersecurity hygiene. This almost guarantees some form of payment. Alternatively, given cybercriminals understand large companies' shutdown costs are in the millions or tens of millions, and when confronted with a price to get operations back online, paying a ransom is business as usual.

SHOULD YOU PAY?

While ransomware attacks are nothing new, the use of "triple" and "quadruple extortion" has brought forth strategic issues to firms, namely, should ransoms be paid? Testifying in front of Congress on June 8, Colonial Pipeline CEO Joseph Blount Blount's defense reflects such concerns, saying that it was Colonial understanding that the decision to pay the ransom was solely theirs to make, meaning the company sought to uphold its interest. However, every ransom payment essentially bankrolls the next attack.

JBS, which is the second-largest meat producer in the US, issued a statement on June 3 claiming it was able to limit supply loss to less than a days' worth of production, and that global production losses would be "fully recovered by the end of next week". Despite its projected optimism, disruption to a fifth of the U.S. beef processing poses potentially significant ripple effects in the market besides short-term supply shortages, such as rising prices for beef and other proteins. Disruptions to major food distributors hold larger strategic consequences beyond short-term monetary loss. JBS also supplies over 150 countries, meaning potential risks associated with longer disruptions to the global food supply chain, along with precedence for ransoms being paid, lends to a higher probability for threat actors to progressively be attracted to similar low-risk, highly profitable targets.

On May 28, Sturdy Memorial Hospital, a 126-bed facility in the city Massachusetts-based hospital confirmed that they paid an undisclosed ransom to an unidentified group in exchange for promises that they would destroy the stolen data. This reportedly contained patient insurance claim numbers, medical history, treatment information, social security numbers, bank routing, and credit card numbers, of 57,400 individuals. Such incidents occurred consistently throughout the first half of 2021, highlighting inherent weaknesses in the Healthcare sector.



Another factor likely to arise is the insurance industry, especially with entities lacking cyber resources. Global cyber reinsurance rates have reportedly risen by up to 40% due to the increase in ransomware attacks.10 The more companies pay, the higher premiums cyber-insurers are expected to start charging customers that don't implement cybersecurity best practices, likely even forcing them to hand over control of ransom negotiation and recovery entirely during underwriting to reduce impact.[11]

The bottom line is, in the short run it's more cost-effective to pay. Beyond the short-term, such attacks pose significant strategic challenges to companies, as they allow cybercriminals to successfully dictate the economics of extortion. The cost of rebuilding systems can be significantly higher than the ransom amounts, which, as revealed in Avaddon's released keys, are designed to incentivize firms to pay. However, governments and insurers are projected to penalise the paying of ransoms that fund the next cybercriminal incident, likely by enacting laws that force public disclosure of ransom payments and raise higher insurance premiums.

10 https://www.reuters.com/technology/cyber-reinsurance-rates-rocket-july-renewals-willis-re-2021-07-01/

11 https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-pricing-spikes-32--report-259795.aspx

NEGOTIATING "NO"

Unlike on-site systems which can be breached, maintaining secured, offline backups is essential to having a recovery process in place that is far more cost-effective than paying a ransom in the long run. The key is to test, and constantly re-test how long a potential data restoration process takes if such an attack arises. Time and cost-efficient recovery must be simulated, formulated, and executed. This develops more resilient and better-configured backup systems which identify key issues likely to arise during real incidents, such as core-system-applications which are essential for data recovery, and therefore also need to be backed up, or knowing how long it would take for the data transfers to occur ahead of time instead of discovering it could take weeks or months in real-time once the attack happens.

The backup strategy was best exemplified when Japanese multinational conglomerate FujiFilm broke the mold following a series of high-profile ransomware attacks, by refusing to pay and instead relying on backups to resume business operations. On June 2 the company shut down portions of IT systems to prevent a possible ransomware attack after an unauthorised actor accessed servers of its Tokyo headquarters. On June 4 it shut down its entire network, blocking access to its email, billing, and internal reporting systems, and by June 14 started operating servers and computers confirmed to be safe. It took the company 10 t0 14 days to resume normal operations and communication within its customers' and partners' and stated that it found no evidence of information being leaked to the outside world.

However, while its recovery plan could have been far worse, the company still lost 10 to 14 days to downtime despite not paying. Furthermore, while it did not name a specific ransomware operator; experts reportedly stated Fujifilm's systems were infected with the Qbot remote access trojan (RAT) botnet as early as May 15.[12] Qbot trojan operators have historically been used by threat actors to gain remote access to networks that were previously infected. This means that despite organisation's recovery strategies, the potential risk of future ransomware attacks using the same vulnerabilities remains.

> **It was not a Colonial123-type password.**
> Colonial Pipeline CEO Joseph Blount

This was this case when Colonial CEO Blount confirmed that DarkSide's affiliates accessed the companies network using a legacy Virtual Private Network (VPN) system that did not use multifactor authentication, meaning it was accessed via one password without a second step like a one-time-password (OTP) text message. Two-factor authentication, which requires multifactor authentications to access all internal applications, is a common safeguard employed by virtually all major companies. Blount claimed that Colonial Pipeline invested more than 200 million USD into securing its systems in the past 5 years, however, this incident underscores the reality where poor cybersecurity hygiene failed to prevent the simplest breach.[13]

NEGOTIATING LOWER PRICE

Limited publicised details regarding paid ransoms, including insights from Avaddon's released keys, show us that cybercriminals, in general, are more than willing to negotiating. If the risk of a breach is presented, ransomware groups should not be perceived as being any different than competing parties who enter negotiations. Instead of conceding that threat actors hold all the power, organisations should determine what leverage they do hold and form a negotiation strategy. In fact, a whole new ransomware negation industry has sprung up following the sharp increase in ransomware attacks in the last years, with many firms providing dedicated services to the issue.

Victims must also understand that paying a ransom does not prevent further attacks, if poor practices and vulnerabilities that allowed an attack to happen in the first place still exist, ransomware groups will attack the company that paid over and over and over again as long as the low-risk high-profit opportunity remains.

12 https://www.bleepingcomputer.com/news/security/fujifilm-resumes-normal-operations-after-ransomware-attack/
13 https://cybernews.com/news/one-password-allowed-hackers-to-disrupt-colonial-pipeline-ceo-tells-senators/

SOFTWARE VULNERABILITIES

Software vulnerabilities accounted for 13% of all attacks in H12021, with 8% being Zero-day vulnerabilities. At least 5% resulted from known Common Vulnerabilities and Exposures (CVE), the majority of which have patches.

Between December 2020 and January 2021, multiple users of Accellion's legacy enterprise-grade software File Transfer Appliance (FTA) product were hit with two zero-day exploits, and while patches were released as early as December 2, vulnerabilities in the third-party software had already been exploited.[14] On February 22 Accellion confirmed that that financial cybercrime group FIN11 and the Clop ransomware were behind attacks, which by then reportedly hit around 100 companies across the world. It remains unknown if Cl0p managed to infiltrate unpatched FTA servers or gained data from hackers, but it seems that the group did not encrypt the victims' files and instead attempted to extort them by threatening the data would be dumped on its leak site if they didn't pay. [15]

REDUCING ATTACK SURFACES

Supply chain attacks occur when threat actors attack a single vulnerable third-party vendor to breach multiple organisations that use unpatched versions of the software appliance. These highly sophisticated attacks have become highly prolific since the state-sponsored supply chain attack on SolarWinds saw multiple organisations in the US being hit in 2020.

While Accellion received widespread criticism for faults in its 20-year-old FTA product, this just shows how multiple organisations still rely on legacy IT systems with larger attack surfaces prone to inevitable zero-day exploits. In its latest patch update, Accellion emphasised its plan to retire its FTA product in April after working on transitioning clients onto its new platform Kiteworks for almost three years. However, by May, only 75% of its customers migrated, meaning 25% were still susceptible to attacks. By June, roughly 300 organisations were affected the supply chain attack, at least 37 were confirmed to have suffered significant data breaches in the first half of 2021. The final patch was issued on March 1, despite the vulnerability persisting for almost three months.

PATCHING

Such attacks highlight the failure to mitigate potential damage by employing two of the most crucial cybersecurity practices, threat intelligence and vulnerability management, or Threat based Vulnerability Management to actively identify potential and relevant threats before they become active cyber-attacks.

The Reserve Bank of New Zealand (RBNZ), which was attacked on December 25, 2020, raised such concerns, claiming Accellion email alert service failed to alert them of the breach until only January 6.[16]

A failure to receive Threat Intelligence feeds, highlights the lack of effective Threat and vulnerability management practices needed to not only stay up to date on alerts and advisories, but to identify actionable intelligence such indicators of compromise (IOC), and broader developments essential in protecting potentially exposed services.

14 https://techcrunch.com/2021/07/08/the-accellion-data-breach-continues-to-get-messier/
15 https://www.zdnet.com/article/fireeye-links-0-day-attacks-on-fta-servers-extortion-campaign-to-fin11-group/
16 https://www.rbnz.govt.nz/news/2021/05/reserve-bank-taking-action-to-respond-to-data-breach-reports

HUMAN VULNERABILITIES

The most consistent variable in almost every cybersecurity incident is human vulnerability. Unintentional human actions, or mistakes, such as clicking on malicious links, misconfiguring systems, applications, databases and even security controls, too often lead to far-reaching consequences to victim organisations.

EMAIL

The most common initial attack vector (method or pathway used to access or penetrate a target's system) recorded this year was Email, and this is likely due to email fatigue, where users inevitably click on malicious links embedded within emails. 94% of all malware, including ransomware, is delivered via email, 80% of which is done by phishing. This is because cybercriminals, particularly ransomware groups, continuously perfect email phishing strategies by using social engineering tactics that play on user emotions, social interests, workload etc.

Moreover, cybercriminals continued to prove their capability of performing extensive reconnaissance on high profile targets to identify key pieces of information, like the target's interests or associates, to increase the probability of a malicious link being clicked in targeted spear-phishing campaigns. For example, on April 4 security researchers discovered a new campaign distributing the more_eggs backdoor via unsolicited job offers targeting LinkedIn profiles whose job descriptions were identified as senior executives. The more_eggs downloader, which can distribute multiple malwares shows how complex social engineering like personalised lures can be used to distribute multi-vector attack techniques.

In April Microsoft revealed that threat actors used legitimate corporate contact forms to send phishing emails threatening enterprise targets with lawsuits, attempting to infect them with information-stealing malware using legitimate Google URLs. Similarly, on May 12 the FBI revealed that threat actors impersonated Truist, the sixth-largest holding company in the US, in a spear-phishing campaign attempting to infect recipients with a remote access trojan (RAT) malware.

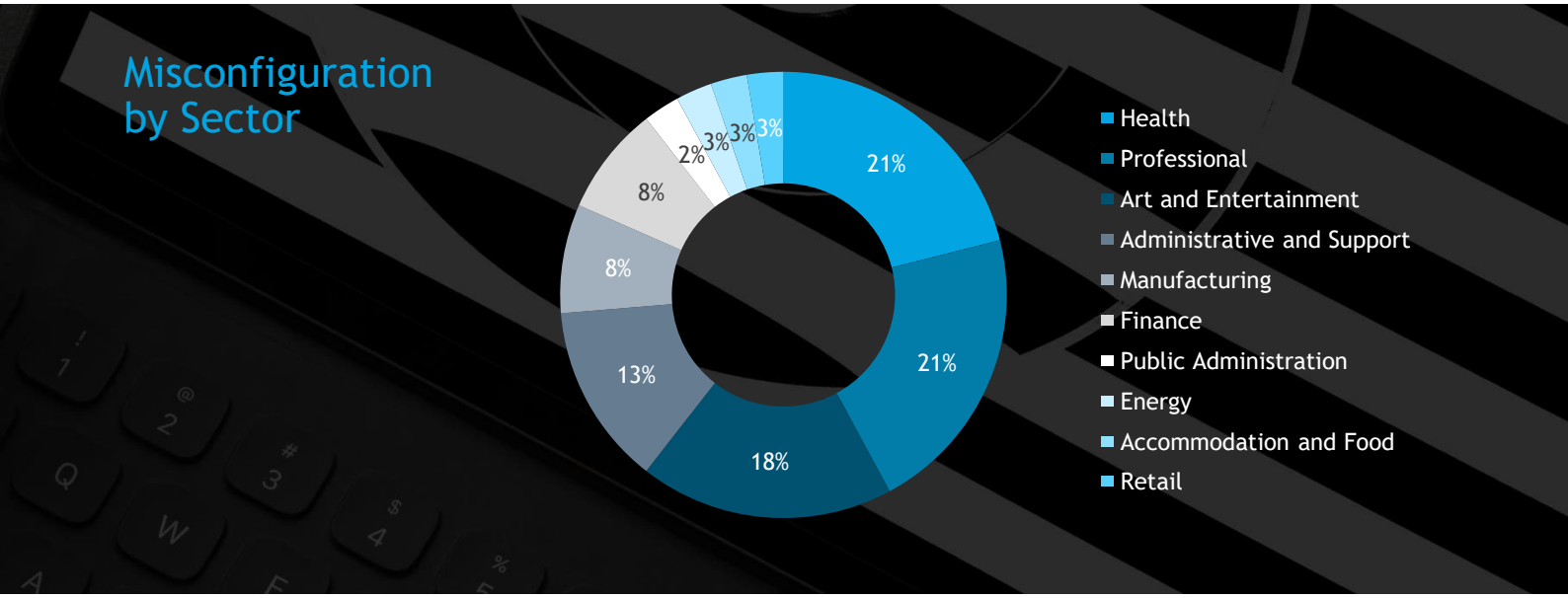
Other notable incidents came on June 22, when the Financial Industry Regulatory Authority (FINRA), which supervises more than 624,000 brokers, securities firms, and exchange markets across the US, warned of an ongoing phishing campaign for the second time in the same month. Like its first warning on June 7, FINRA warned that the phishing campaign impersonated the regulatory body, and threatened recipients with penalties unless they provide the information requested by the attackers. [17]

Preventing email vulnerabilities lies in continuous user education, whether it be an office secretary or C-Suite executives, on what new attacks look like. The problem however lies in the extremely dynamic cybersecurity landscape, where new threats emerge while old ones persist via increasingly sophisticated new approaches to social engineering strategies.

17 https://www.bleepingcomputer.com/news/security/us-brokerage-firms-warned-of-ongoing-phishing-with-penalty-threats/

MISCONFIGURATION

Unintentional actions taken by internal actors have always been a problem, however, systems, applications and database Misconfigurations, either discovered by security researchers or too late after data has been dumped on a darknet leak site, is a particularly growing problem, accounting for 5% of all incidents in H12021.



Many cloud-native breaches are the result of threat actors exploiting errors in a cloud deployment without even using malware. Once gaining access to misconfigured, or weakly configured online repositories on public clouds, unauthorised actors can not only easily locate valuable data assets, but exfiltrate the data using the same misconfiguration. Healthcare and professional services shared top spot with both at 21%, followed by Arts, Entertainment and Recreation at 18%, while Financial and Manufacturing accounting for 8% of incidents.

Notable breaches include risk and compliance company LogicGate confirming on February 23 that an unauthorised party accessed its customer's backups after obtaining credentials to its Amazon Web Services (AWS) hosted cloud storage server. Indian mobile payments company MobiKwik, which also hosted its data on AWS, reported on March 30 that sometime during February 2021 the data of nearly 100 million users were leaked on the dark web. Similarly, Mercedes Benz USA disclosed that 1.6 million customer records were leaked on June 11, and on June 12, the Volkswagen Group of America confirmed that 3.3 million of its customer's data was being sold on a hacking forum after being stolen from an exposed Microsoft Azure server.

CYBER THREAT OPERATIONS

IDENTIFY

Cyber Threat Intelligence for Executive Management

This report presents multiple data breaches that demonstrate how the lack of intelligence-backed risk management solutions can result in long-lasting damage to businesses, partners, and customers. This is why leaders who make business decisions from cyber risk management processes need strategic level cyber threat intelligence.

To be more precise C-suite personnel need CTI for executive management in the form of less technical reports and briefings disseminated in various formats and timeframes, which provide a broader overview of an organisation's threat landscape. Executive level CTI delivers both strategic and actionable insight into a wide range of areas, such as risks associated with taking specific actions, threat actor tactics, techniques, and procedures (TTPs), what sectors and industries are targeted, and other general security developments. In practical terms, having a broad overview of trends can generate options for addressing immediate impacts, support security investment decisions for the next quarter, and develop a long-term security roadmap.

Threat Modeling in S-SDLC

When it comes to implementing security in application development, it often comes as an afterthought as developers give it less priority due to a lack of cybersecurity acumen or because security concerns, in general, can impede production deadlines. This eventually leads to critical vulnerabilities that increase risk and remediation costs that become much larger when implemented after the design stages of the software development life cycle (SDLC). That said, threat modeling can be an easy and cost-effective way to implement security in the design phase of the SDLC.

Threat modeling is the security process by which you can identify, categorise, and analyse threats for the purpose of reducing risk by coming up with solutions to potential damage. That said, threat modeling should be implemented to address foreseen vulnerabilities during early stages of the SDLC, as well as later stages when changes to architecture are made.

Moreover, while traditional DevOps combines software development with IT operations teams into a single unit that share skills and a common goal, threat modeling can take synergistic thinking one step further by incorporating security from the start by developing a DevSecOps culture. In this context, security architect, operations, and infrastructure developers can communicate input within a whole team to foster a culture of collaboration, allowing team members to understand each other's roles, objectives and weaknesses, and improve business operations in general. Thus, effective threat modeling can enable organisations to identify potential attacks, vulnerabilities, and mitigations within the context of protecting software, applications, or systems before they arise, while facilitating a better overall software development culture.

PROTECT

Threat (Risk) Based Vulnerabilities Management

Virtually all organisations employ some form of Vulnerability Management to identify weaknesses in their system infrastructure before they are exploited by malicious actors. However, in reality, organisations face an incredible number of potential threats, which often leads to inaccurate prioritising and time wasted on remediation processing of non-critical vulnerabilities instead of mitigating critical threats in time, thus increasing the risk of breach. Moreover, inefficient mitigative processes often lead to inconsistencies and tensions between security operations teams, whose purpose is to remove all security flaws and IT operations, whose primary focus is to perpetuate system availability.

This is where Threat (Risk) Based Vulnerability Management can correctly prioritise against the most critical vulnerabilities and use more manageable remediation processes by using threat intelligence to identify factors like asset values, impact severity, and malicious actor intent.

This approach facilitates a more realistic risk rating framework that allows for effective prioritisation, where highly critical vulnerabilities are patched immediately, while less- urgent non-critical ones can be managed subsequently or even monitored for risk development if business optimisation allows it.

Zero Trust

Breaches almost always involve some form of intrusion into a "perimeter" such as a system or network, which is then followed by subsequent lateral movement once within through escalation of privileges. This perimeter, unfortunately, has become larger as data and apps are increasingly moving to the cloud, while the number of endpoints have also increased due to the significant growth in remote work under COVID-19. That said, the Zero Trust Architecture (ZTA) approach presents a viable solution to proactively manage secured connections by relying on the assumption that an organisation is compromised and that connections between every user, device, application and dataset need to be continually validated to meet certain conditions for use. While the idea of over securing connections between business units seems like a recipe for stagnant workflow, it can be used to limit cyber risk without impeding growth.

By wrapping a defense around each connection in a dynamic way that adjusts access control rights and privileges depending on risk status, business units can keep running smoothly while remaining secure. Using threat intelligence that leverages location, app use, and other variables that enrich data for every user, device, and connection, admins can use risk profiles to adjust privilege, which maintain safety by matching changing risk levels based on context. Going beyond binary deny/allow access frameworks allows users that pose major or minor risks to access relevant assets such as tools needed to complete business tasks. In this context, system administrators can grant users latitude as they pose more or less of a risk, while taking direct actions to limit or expand access.

The Zero Trust philosophy has become increasingly relevant to all sectors in recent years, and in critical infrastructure sectors during 2021 following the recent high-profile ransomware attacks. According to the Microsoft 2021 Zero Trust Adoption Report, 96 percent of security decision-makers stated that Zero Trust has become critical to their organisation’s success, 76% of which are already in the process of implementation (an increase from 20% in 2020), while 73% expect their Zero Trust budgets to increase in the next two years. In the same regard, President Joe Biden's Executive Order on Improving the Nation’s Cybersecurity, issued on May 12, 2021, explicitly defines ZTA implementations as a key national security priority following the attacks on its critical infrastructure.

18 https://www.microsoft.com/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/

19 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

DETECT

Continuous Attack Surface Monitoring

Initial mapping of any organisation's attack surface can no longer be considered relevant as businesses' expansion and investment into digitalization and cloud migration expose more internet surfaces, and with it, new vectors for attack. While attack surface monitoring (ASM) has been around for some time, organisations must now conduct Continuous Attack Surface Monitoring (CASM) to identify not just vulnerabilities in known assets, but emerging unknown ones such as new endpoints in decentralised environments like remote workforce devices.

CASM increases new assets attribution and discovers vulnerabilities in systems and services through external attack surface enumeration and lateral movement by conducting continuous penetration testing and vulnerability scanning, and applications assessment. Moreover, at present various CASM platforms pose enough maturity to provide existing cyber threat intelligence, vulnerability assessment management, and incident response solutions with enough support.

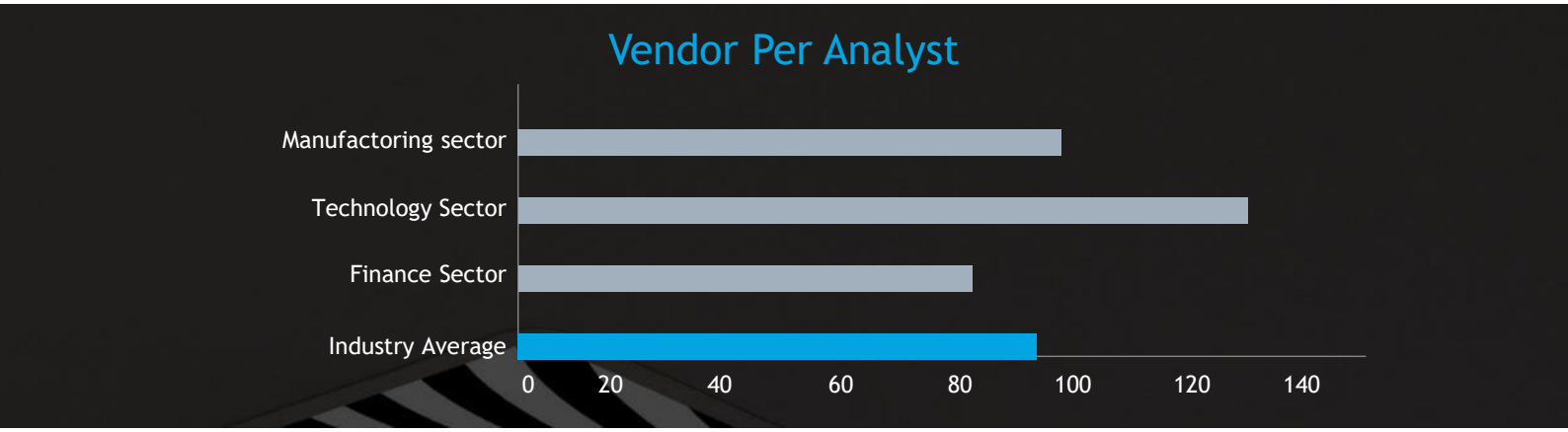
Third-Party Risk Management (TPRM)

IT outsourcing has increased substantially in recent years in general, and virtually all organisations rely on third parties for some service. However, this means when vendors or suppliers are hit with cyber-attacks, there can be significant impediments to running operations smoothly, while long-lasting impacts can become devastating. If a cloud provider, MSP, or other vendor like shipping services get shut down, then so do your website, applications, delivery times, etc., and this can negatively affect bottom line and reputation. In fact, according to a survey we conducted, 82% of the organisations do not regularly manage cyber supply chain risks, and only 7% to 15% assess their third parties. A viable risk management strategy that focuses on identifying and reducing risks associated with vendors, suppliers, service providers, or any other partner whose systems overlap with the organisation can be done through Third-party Risk Management (TPRM).

DETECT

Understanding how you use multiple third parties can identify which safeguards each one has in place, what industry standards and regulations they are subjected to, and allows you to employ universally applicable best practices to mitigate risks associated with them. In this context, TPRM allows organisations to prioritise vendors according to risk scores, giving the ability to focus time and resources on high-risk vendors by performing more stringent due diligence, in-depth or on-site assessments and validation, while limiting shared data such as client information to the most critical functions. Alternatively, cooperation with medium and low-risk vendors can continue more freely so operations can run without impact.

Our survey showed that within three months after the TPRM process was established, at least 98 closed findings assigned at least 38% as high priority. Moreover, more than 70% of the organisations assessed their third parties via a standardised questionnaire, rather than customising it to meet their needs, while the industry management scope average there was just one analyst per 100 third parties. This is where the TPRM lifecycle can leverage automation to increase consistency and efficiency, from identifying and onboarding new suppliers, to forming risk assessments, scores, owners, and mitigations, managing procurement and contracts, and conducting reporting and monitoring.



RESPOND

SOAR

Organisations often lack sufficient human resources to effectively contend with an overwhelming amount of security event data to employ effective incident response IR. This is where automation can facilitate efficient data aggregation, enrichment, correlation, and investigation by suing the next-gen approach in incident response, namely Security Orchestration, Automation, and Response (SOAR). SOAR solutions are designed to integrate all existing security tools and applications an open, centrally organised way while automating workflow to reduce response time between breach to discovery.

The Orchestration aspect in the SOAR approach uses a series of playbooks that define threats and explain how to manage them. These automated workflows integrate multiple security technologies together to respond to threats. The Automation aspect leverages machines to complete tasks usually done by humans and automates decision-making to make IR processes more effective and consistent at scale, giving humans more time to handle more complex analytical tasks and goals.

However, SAORs are only as effective as the data used to construct them, and this is where high-quality CTI which aggregates analysed data makes it smart. Integrating these capabilities improves productivity and awareness of SOC analysts, incident responders, and other security personnel by bringing together various security professionals, processes, and technologies with different strengths and weaknesses, while reducing wasted time and fatigue via automation. In this respect, SOAR gives a fully integrated overview of data on external threats to have a clearer understanding of the unfolding situation, and provides necessary responses needed to remediate respective threats.

RECOVER

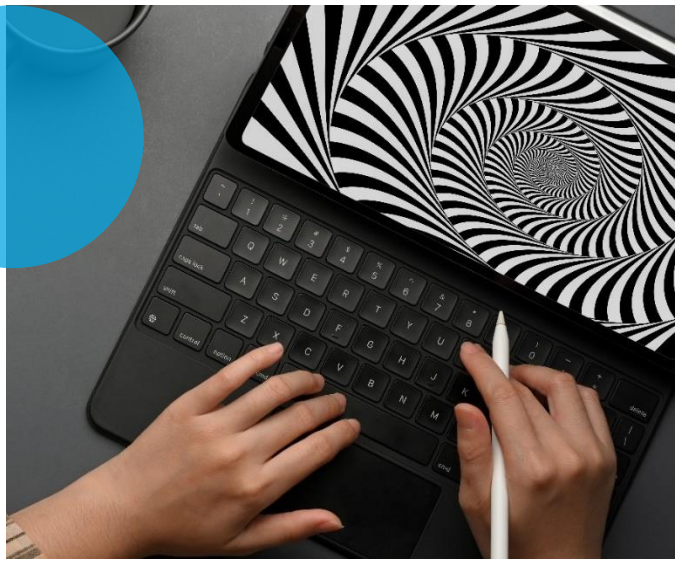
Threat based Backup & Recovery plan

Having a Backup and Disaster Recovery Plan (BDRP) that outlines detailed processes, assets, personnel, and actions needed to be taken in the event of a disaster is essential in recover assets compromised in cyberattacks like DDoS or Ransomware attacks.

A BDRP must become a key policy for most businesses, especially less technically proficient ones, as they play a vital role in ensuring business continuity both in the short-term following an but, and the long term if designed and implemented correctly. While every organisation is unique, there are universally critical elements that can benefit from a few BDRP best practices

Protected Offline Backups

Data should always be backed up in resilient and better-configured isolated, offline local systems of different types, such as scheduled full backups and incremental ones that are backed up on a more frequent schedule. Additionally, everything, including backup catalogs, processes, and critical internal applications such as those that facilitate file transfer, should also be backed up and protected to offset more sophisticated ransomware attacks which encrypt multiple asset types. A BDRP should also consider where disaster recovery sites, IT infrastructure, and other mission critical recovery operations are located, especially given these areas are designed to support organisational priorities while being remote.



Identify RTO and RPO

When designing and deploying disaster recovery processes, organisations must define projected Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO pre-establishes a deadline for full and partial system and operating recovery measured in time units like hours, days, or weeks. Alternatively, RPO regards business loss tolerance, and is measured by the number of assets which are acceptable to be lost before to determine what defines impactful damage. Both are essential metrics to gauge BDRP progress and should be refined regularly via security audits. Moreover, these metrics provide reference points to other sections of the BDRP at every stage.

Establish Roles

Organisations should also establish a disaster recovery and negotiating team consisting of various personnel and should identify each team and team member roles, inside and outside the disaster recovery process. This should include not just technical professionals but also non-technical executives such as legal advisers familiar with laws and regulations, insurance experts, other outside council, and professional negotiators, and should also determine who negotiates. Clearly define roles that are assigned to each person or team is critical to streamline BDRP efforts and communications once the recovery process is underway, and more importantly prepares management through training beforehand.

Moreover, having broad expertise in a disaster recovery council should also determine whether ransoms should even be paid, and victim organisations can benefit greatly from having professional negotiators and executives like Chief Information Security Officer (CISO) and Chief Operating Officer (COO) ready to engaging with the respective threat actors immediately. This can buy time to make sense of the situation and give disaster recovery a head start, or lower the ransom demand significantly to reduce impact.
Additionally, keeping in mind that only 28% of ransomware incidents were confirmed as breaches, having experts ready can help gain actual proof that data has actually been compromised or stolen.

RECOVER

Create Communication Plans

A carefully crafted and thorough communications plan that is established before the need for one suddenly arises is vital to limit long-term damage to an organisation's reputation. Ransomware operators and cybercriminals are fully aware that organisations are subject to the perceptions of internal and external stakeholders, and defined procedures on how to contact vendors, partners, and customers, should be determined.

This should include default responses to paying and not paying ransom demands, consideration to legal factors to breach disclosures, and should make general effort to control how the situation is being perceived in general. Communications channels should be determined, whether they are formal, official, news, or social media, to control the narrative and avoid negative media coverage and unwanted publicity.

A Perform Regular Testing

Constant auditing and testing of the BDRP need to be performed to make it not only practical but relevant over time. Regular testing ensures that disaster recovery processes keep working as businesses and organisations grow in size and type.

In this context, reconfigured backups, RTO, RPO, Communication, and roles need to be constantly tested and refined in data restoration simulations to identify critical issues likely to arise during actual incidents. This increases the likelihood of business continuity and supports investments which update efficient recovery.

OPHIR ZILBIGER

Global Cyber Leader
Partner, Head of Cybersecurity Center
BDO Israel
OphirZ@bdo.co.il

NOAM HENDRUKER

Partner
Head of Cyber Consulting Group
BDO Cybersecurity Center, Israel
NoamH@bdo.co.il

GILAD YARON

Director
Head of Privacy & GRC Division
BDO Cybersecurity Center, Israel
GiladY@bdo.co.il

TOMMY BABEL

Director
Head Threat Operations & Offensive Security
BDO Cybersecurity Center, Israel
TommyB@bdo.co.il

www.bdo.global