KIVU in partnership with HISCOX CYBERCLEAR®

Trends in Ransomware and Doxing

H1 2020 Review

The Insurance Edit

Executive Summary

The COVID-19 pandemic prompted global disruption to professional and private lives but provided plenty of opportunities for cyber-criminals. Organizations were forced to shift their operations to digital and remote platforms overnight without preparation. Preoccupied with addressing the public health crisis and its economic consequences, organizations scrambled to address the security implications of this swift evolution in labor practice. Subsequently, cyber threat actors have proven to be highly adaptive, modifying their tactics to strategically capitalize on organizational and individual vulnerabilities.

Our research demonstrates that cyber-crime is continuing to evolve during the COVID-19 pandemic. In the first half of 2020 (1H20), we observed markedly higher ransom demands from attackers, a general trend of opportunistic attacks turning into targeted attacks (and a swing back around in some cases), and an increase in organized cyber-criminal syndicates leveraging theft of sensitive information to extort high ransoms from victims, even from those with valid and unaffected back-ups.

Phishing persisted as the ubiquitous attack vector for malware distribution and business disruption while cyber criminals increasingly exploited vulnerabilities in remote infrastructure in 1H20. Even prior to the rise in remote work, Hiscox noted in its Q1 2020 Cyber Claims Report a spike of European claims in February linked to VPN vulnerabilities. Upon close examination of our H1 data, we identified a shift in the methodology of how phishing tactics launched ransomware attacks from Q1 to Q2 in 2020. Phishing techniques evolved from opportunistic “spray and pray” attacks to more targeted approaches. Additionally, we discovered a reversion back to mass-spam campaigns to generate revenue from easy targets, courtesy of Ransomware-as-a-Service suites such as Avaddon at the end of Q2. We predict attackers will continue to practice phishing throughout 2H20, resulting in more ransomware attacks, inventive Business Email Compromise (BEC) scams and the proliferation of other malware.

Doxing is the act of stealing a ransomware victim’s data and threatening to publish and/or sell it on the dark web. We began tracking doxing when Maze launched the first dedicated website to leaking and discrediting companies with compromised security postures in November 2019. The victims featured on the Maze site sustained infiltration by unauthorized threat actors that executed ransomware attacks against them. The practice of doxing, or data exfiltration, matured as we found ten ransomware groups resorting to the practice in 1H20. The number of doxing victims increased each week throughout May and June 2020, with Maze significantly contributing to this trend. Most notably we found that the doxed industries that attracted the most media attention, such as schools, public sectors, and healthcare, do not actually represent the most targeted industries.

Hiscox view

Our cyber claims data is telling a similar story to the trends uncovered in Kivu's research, in that the cost and intensity of criminal activity in this area are markedly higher. In 2019, we experienced a 404% increase in ransomware demands across the US, compared to 2018, and a 470% increase since 2016.

Historically, between 2015 and 2017, organizations with revenues greater than $5b have been relatively unaffected by ransomware; however, there's been a rapid increase in larger companies being successfully compromised. In 2020 we have already observed more attacks against this customer segment than the whole of 2019.

In 2019, the total claims cost for an insured without a back-up strategy was 3.5x higher than an insured with a back-up strategy in place. Back-ups remain an important risk management tool, but they are not the panacea they once were. Ransomware gangs have adapted to better back-up behavior by exfiltrating and destroying data, rather than encrypting it.

Ransomware Review

Attackers are continuing their big-game hunting tactics, selecting larger entities as targets and demanding larger ransoms. Threat actors further honed their strategy to select entities with time-critical operations, such as entities in the manufacturing and healthcare industries, or enterprises that hold valuable personal identifiable information, such as professional services organizations.

Kivu's empirical data from paid ransoms demonstrates a 200% increase in the size of ransom demands and payments in 1H20 as compared to 1H19. The average ransom payment equaled $231,373.11 in the first half of this year (Chart 1). Comparatively, the average ransom payment amounted to $116,210.39 in the same period last year.

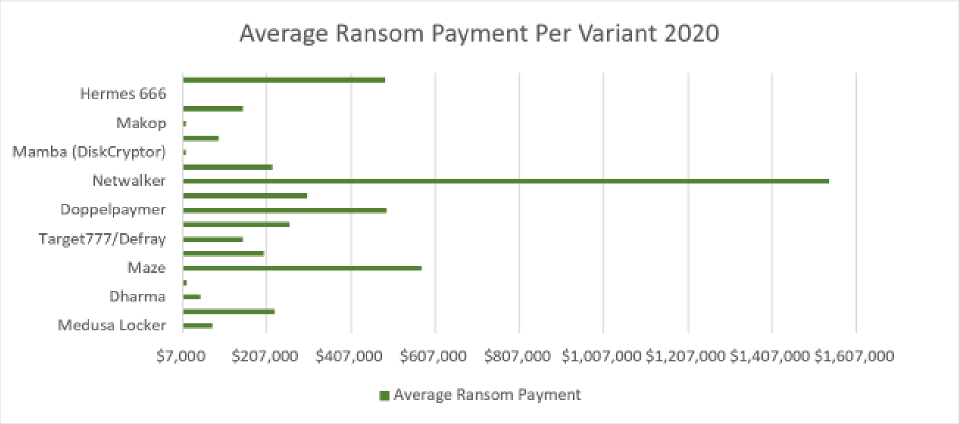


Chart 1. Average ransom payment per variant in 1H20 based on Kivu's internal data.

The highest ransom payment was $1,800,000 in 1H19. In contrast, the highest ransom payment facilitated by Kivu reached $3,000,000 in 1H20 (Chart 2). Increased ransom payments are a result of heightened ransom demands. For example, the largest demand Kivu worked on in the first half of this year came to $12,000,000 pre-negotiation.

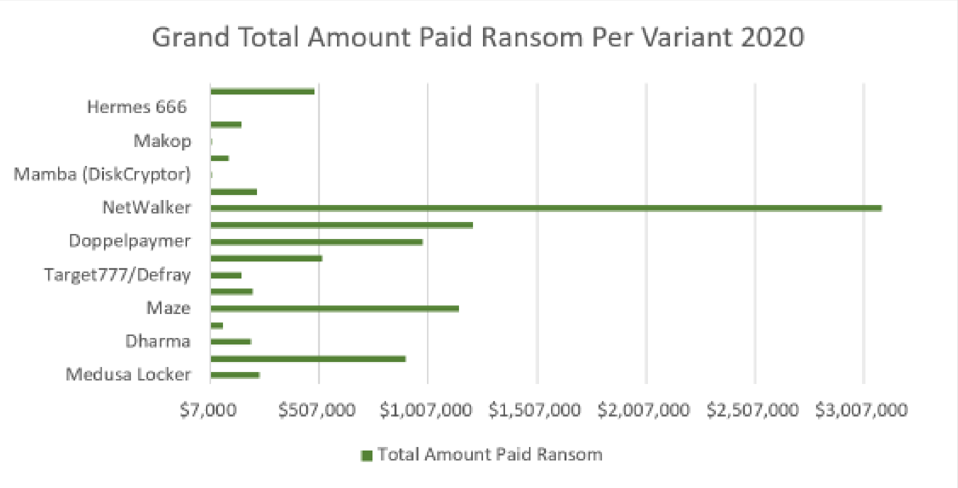


Chart 2. Total ransom paid per variant in 1H20 based on Kivu's internal data.

The continued rise in ransom demands is due to the attackers' success in network reconnaissance and persistence, which allowed them to place a more accurate value on victim data and thus justify higher ransom demands. In addition, attackers realized that leaking and/or selling stolen data on dark web markets increases legal complications for victims. This tactic, which has been dubbed 'doxing', led threat actors to abuse regulatory measures to leverage higher ransom demands. We expect attackers will continue to deploy all these techniques to further increase the profitability of their attacks in the second half of 2020.

The most sought-after ransomware targets remain the Manufacturing, Construction, Healthcare, Information Technology (IT) and Education sectors. IT services are an attractive target due to the crucial nature of their services for a range of other organizations. Attackers will target IT providers and use them as a gateway to clients' systems, allowing them to seed ransomware through the IT provider's network infrastructure. Once the malware is distributed this way, criminals are able to chronologically extort multiple companies to ransom at once. An unenviable position for the victim, but a very lucrative one for the cyber-criminals. Additionally, the two highest ransom payments referenced above from 2019 were made on behalf of clients in the manufacturing industry. Threats actors target manufacturing organizations because of the often time-sensitive nature of production. Manufacturing entities also commonly fail to invest in IT services which leaves them vulnerable to attacks.

Attackers are also targeting businesses integral to the facilitation of critical services during the COVID-19 pandemic. The largest payment Kivu facilitated in 1H20 amounted to

$3,000,000 for a client in the education sector - the original demand was over $9,000,000. We anticipate attackers will continue to target educational entities, especially as they continue to navigate remote learning, in the second half of 2020. We break down targeted industries in a later section, starting on page 8.

While often the headline-grabbing figure, ransom demands are not the only cost incurred by victims. An estimated half of the cost of a ransomware infection comes from business income loss. The average financial cost of ransomware – including the loss of income during downtime, continued payments of staff salaries, and technical repairs or replacements - increased by 81% from $142,000 in 2019 to $257,000 in 2020.[1]

Ransomware operators use increasingly destructive tactics, seeking to destroy evidence and, often as a result, causing serious damage to victim environments. By encrypting backups attackers force victims into paying for a decryption key, but this tactic also causes greater need for restoration services.

The top five ransomware variants Kivu encountered in 1H20, ranked by highest to lowest ransoms paid to the threat actor groups, are NetWalker, Ryuk, Maze, DoppelPaymer and Sodinokibi/REvil. We discuss ransomware variants in more detail on page 13.

We anticipate ransom demands and payments will continue to rise throughout 2020 and into 2021. We found that the Manufacturing, Construction, Healthcare, IT, and Education sectors will remain the most targeted industries. Ransomware variants executed by organized criminal syndicates, like Netwalker and Ryuk, will continue to incur the highest ransom payments.

Hiscox view

According to our Hiscox Cyber Readiness Report 2020[2], an annual report that surveys companies of various sizes and industries across eight countries, the numbers that have paid a ransom following a malware infection are chilling. In the 2020 report survey, more than 6% of the 5,569 respondents paid a ransom, and their combined losses came to $381 million. The U.S. and France had the largest percentage of businesses that experienced a cyber-attack pay a ransom - 18% compared with an average of 16%.

Ransomware is also the most expensive type of attack - the mean losses for all firms subjected to a ransomware attack in the Hiscox Readiness Report 2020 were nearly twice

[1] *Cyber Claims Study 2019 Report,* Net Diligence, 2019, **https://netdiligence.com/wp-content/uploads/2020/05/2019_NetD_Claims_Study_Report_1.2.pdf**.

[2] *Hiscox Cyber Readiness Report 2020.* Hiscox. 2020. **https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf**.

as much as those that only had to grapple with other malware – $927,000 compared with $492,000. It pays to stop a malware infection from becoming ransomware. Companies with good detection capabilities can do this, leading to shorter outages, lower overall costs and less impact to business; however, if ransomware does occur, back-ups are still important. Cyber criminals are evolving their tactics to increase doxing, yet ransomware is still occurring without data exfiltration and back-ups are the best defense. As an example, for all Q1 2020 Hiscox ransomware claims in Germany, we brought our insureds back online without paying a ransom. It is true that COVID-19 has made recovery from back-ups more challenging. In Q2 2020, one of our insureds had back-ups that were dated two months prior because a local lockdown meant they were unable to take off-line back-ups.

Phishing Review

Phishing continues to proliferate, disrupting businesses globally. While the spread of targeted ransomware via phishing was initially favored by attackers, a more scattergun approach to deploying ransomware emails resurged towards the end of H1.

The phishing landscape—as it pertains to ransomware—has shifted in recent years. For some time, Ransomware-as-a-Service was established by attackers to enable ransomware phishing operations for anyone with basic cyber prowess. However, the use of Ransomware-as-a-Service waned towards the mid-year as attackers found less success in the indiscriminate and widespread distribution of ransomware.[3] Instead, they shifted their tactics to targeted phishing emails as a vector for a more selective ransomware attack. Aiming at vulnerable organizations and those that require high-availability systems meant the highest returns for infections – for a while. COVID-19 disrupted this new strategy as employees increasingly worked from home, rendering infrastructure infections less successful. The transition to targeted ransomware via phishing was especially true after Gandcrab, an infamous Ransomware-as-a-Service provider accounting for many of the widespread and indiscriminate ransomware phishing emails, exited the market after netting an alleged two billion USD.[4] Ransomware continues to represent a distinct threat, with reports of as much as a 25% spike in attacks in Q1 2020 as compared to Q4 2019.[5]

[3] Alan Rainer, "Ransomware: A Mid-Year Summary," *Cofense,* July 22, 2019, **https://cofense.com/ransomware-mid-year-summary/**.

[4] Catalin Cimpanu, "GandCrab ransomware operation says it's shutting down," *ZDNet,* June 1, 2019, **https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/**.

[5] *Beazley 2020 Breach Briefing,* Beazley, 2020, **https://www.beazley.com/Documents/2020/beazley-breach-briefing-2020.pdf**.

Overall, phishing continues to increase, displaying a continued cycle of evolution that incorporates geopolitical events and new intrusion tactics. There are mixed reports on to what extent phishing operators have incorporated COVID-19 messaging into their attacks. An informal Kivu survey noted that 24% of insurance industry respondents either received, or knew someone that received, a COVID-19 themed phish. Conversely, a Microsoft report posits that less than two percent of email attacks contained a COVID-19 phishing email.[6] We assess that Microsoft analyzed public rather that professional industries in this report. Therefore, it is plausible that different methodology is employed in targeting certain groups of people over others.

Many attackers favored simple, easy to use phishing malware in 1H20. This includes the broadly applied opportunistic varieties in lieu of targeted ransomware infections. The Avaddon Ransomware-as-a-Service provider distributed over a million emails with ransomware as the initial payload in a single week in early June. Proofpoint and Cofense reporting offers evidence of this trend, indicating that the second half of 2020 will likely see a resurgence in widespread phishing laden with ransomware.[7]

Focusing on Business Email Compromise (BEC), numerous reports conflict in the posture of attackers. Some organizations suggest that a decrease in BEC has been noted, while others maintain that BEC scams are on the rise.[8] Experts agree, however, that phishing has increased overall and is responsible for a significant share of intrusions.[9] In fact, according

[6] "Exploiting a crisis: How Cybercriminals behaved during the outbreak," *Microsoft,* June 16, 2020, **https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/**.

[7] Sherrod Degrippo, "Ransomware as an Initial Payload Reemerges: Avaddon, Philidelphia, Mr. Robot, and More," *Proofpoint,* June 25, 2020, **https://www.proofpoint.com/us/blog/security-briefs/ransomware-initial-payload-reemerges-avaddon-philadelphia-mr-robot-and-more**; *Cofense Q2 2020 Phishing Review,* Cofense, 2020, **https://cofense.com/wp-content/uploads/2020/07/Q2-2020_Phishing-Review.pdf**.

[8] "The enduring threat of ransomware," Beazley, June 9, 2020, **https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html**?; "Abnormal Security Data Reveals 200 Percent Monthly Increase in Invoice and Payment Fraud Business Email Compromise Attacks," *Business Wire,* June 29, 2020, **https://www.businesswire.com/news/home/20200629005113/en/Abnormal-Security-Data-Reveals-200-Percent-Monthly**.

[9] Jason Cohen, "Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine," *PCMag,* March 30, 2020, **https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine**.

to the Hiscox Cyber Readiness Report 2020, 21% of companies who experienced a breach in 2019 also suffered from BEC.[10]

Looking at internal data, Kivu facilitated an average of $379,000 in ransom payment for attacks resulting from a BEC scam in 1H20. This metric demonstrates the actual cost of failing to properly defend against phishing. Kivu's in-house phishing defense teams primarily came across BEC and impersonation scams, while also noting trends in malware such as AgentTesla and stage one loaders like the Equation Editor vulnerability macro. Organizations should expect an increased need to bolster phishing defenses, incorporating a multi-layered defense of automated email gateway security, email reporting, proactive indicator blocking, and holistic security awareness.

Doxing Review

Doxing is the act of stealing a ransomware victim's data and threatening to publish and/or sell it on the dark web. It is used by attackers to increase the pressure on a victim to pay the ransom, regardless of the existence and viability of data backups. Our research has shown that despite similarities in deployment, doxing styles and target profiling varies between threat actors.

At Kivu, we are frequently asked if certain industry sectors are more attractive targets for attackers, or if specific clients are targeted by certain ransomware groups. We tracked and analyzed nearly 400 victims who were publicly blackmailed on doxing sites from around the world over the first half of 2020. As part of this research, we profiled ten ransomware group variants that engaged in this practice: AKO, Cl0p, DoppelPaymer, Maze, NetWalker, Sodinokibi/REvil, RagnarLocker, Nephilim, Mespinoza (PYSA) and Sekhmet.

Our aim was to understand whether: 1) certain regions of the world faced a higher probability of attacks, and 2) certain sectors and industries encounter a higher probability of attacks. In our methodology for categorization of victim company, we use Bloomberg's proprietary Industry Classification Systems (BCIS).[11] For example, Bloomberg categorizes industries such as Oil, Gas, and Coal and Renewable Energy under *Energy*, while the

[10] *Hiscox Cyber Readiness Report 2020,* Hiscox, 2020, **https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf**.

[11] Richard Di Clemente et. al, "Supplementary Information: Diversification versus specialization in complex ecosystems," *Instituto dei Sistemi Complessi,* 2020, **https://journals.plos.org/plosone/article/file%3Ftype%3Dsupplementary%26id%3Dinfo:doi/10.1371/journal.pone.0112525.s002#:~:text=Sectors%20(or%20subsectors)%20are%20hierarchically,classification%20system%20for%20stock%20companies**.

Utilities industry is filed under the same sector name, Utilities. We found that ransomware groups vary not only in doxing methods, but also in which industries and sectors they victimize.

Most victimized sectors

When reviewing the sectors most impacted by doxing, we found the Consumer Discretionary sector to be the most prevalent of all. Consumer Discretionary entities comprise nearly 27% of all doxing cases. This was followed in descending order by the Industrials, Financial, Technology, Healthcare and Consumer Staples sectors. It should be noted that educational institutions and professional services both fall under the Consumer Discretionary category in the Bloomberg nomenclature.

Contrary to what some headlines may suggest, *we found the Public Sector, Energy, and Utilities to be the least represented in this sample*. This contrasts with the disproportionate attention given to ransomware attacks on the public sector by the media, such as the cities of Baltimore, Knoxville and Torrance. Moreover, Healthcare represented just 5% of recorded attacks, in comparison to Consumer Discretionary at 27%. Due to the added risk to life, especially during the COVID-19 pandemic, ransomware attacks on the Healthcare sector are often covered much more extensively by the media. This reality demonstrates that newsworthiness does not in it of itself provide an accurate assessment of the risk landscape.

The Technology sector represents another commonly misunderstood attack victim. 9% of publicly shamed ransomware victims on doxing sites are classified as technology companies. This single digit belies the potentially devastating impact of these attacks due to the trickle-down effect on supply chains and third-party services. Technology companies include Managed Service Providers (MSPs) such as outsourced cloud services, security intrusion detection and prevention services, as well as IT support providers, and are commonly weaponized, allowing attackers to maneuver into further victim environments.[12] The RagnarLocker variant frequently targets MSPs for precisely this reason.

Most victimized industries

We recorded doxing victim's associated industries within their designated sector to gain a more in-depth understanding of the frequency in victimized sectors. At the top of the list came Commercial Services at 10%, followed by Oil, Gas and Coal; Transportation and

[12] Catalin Cimpanu, "US Secret Service reports an increase in hacked managed service providers (MSPs)," *ZDNet,* July 6, 2020, **https://www.zdnet.com/article/us-secret-service-reports-an-increase-in-hacked-managed-service-providers-msps/**.

Logistics; and Discretionary Retail. The remaining 60% consist of a long list of industries, including Telecom, Automotive, Apparel and Textile Products, and Consumer Products.

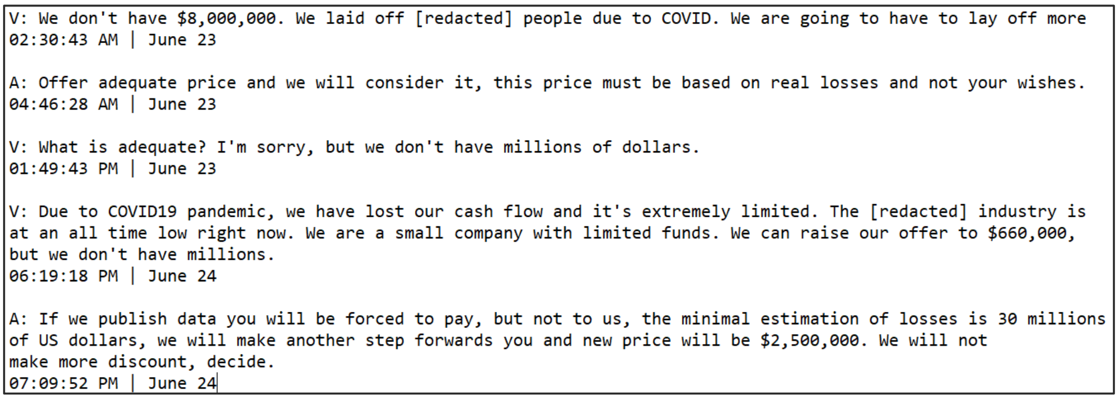
Nearly half of the victims under Commercial Services were classified as law firms and targeted by eight of the ten variants we tracked for this report. Law firms are targeted due to the proprietary and sensitive information they hold on their clients, as well as their commonly under resourced IT and cyber security infrastructure. The risk of reputational harm caused by leaked data is significant for these firms, which leads attackers to assume that they are more likely to pay a ransom. This has been borne out by a well-publicized case in 1H20 which became public when data on celebrity clients was leaked and individually auctioned off by the Sodinokibi (also known as REvil) group on their dedicated auction site. Ultimately, the victim did not pay the ransom nor has any third party threat actor made biddings on the auctioned data to date.[13]

Is the victim's revenue a factor in ransom demand?

Historically, organizations with revenues above $5B have been relatively unaffected by ransomware. Hiscox data shows that this has increased rapidly since 2017, and in 2020 to date the insurer has already observed more attacks against this customer segment than the whole of 2019.

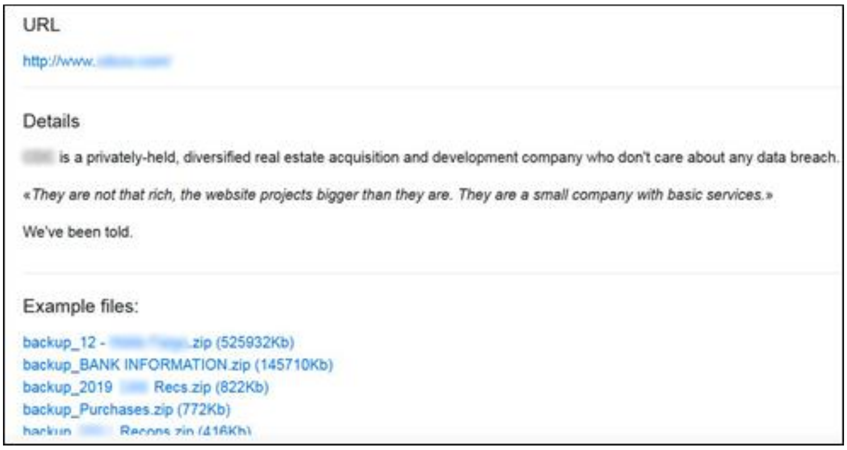
While it is tempting to assume that attackers target organizations with large revenues, Kivu's own research indicates that most attacks begin as opportunistic attacks. Attackers initially begin their assault by leveraging convenient vulnerabilities and or poor configurations before pivoting into more targeted incidents. However, once the victim's data has been evaluated by the intruders and found to be of high value, the ransom demands are often adjusted accordingly. To do this, ransomware operators use confidential internal data found during their reconnaissance work as well as victims' publicly listed revenue and organizational size to make these calculations. The fact that open source or publicly available datasets are not always accurate often causes complications during the negotiation stage (Fig.1 and Fig.2).

[13] Pierluigi Paganini, "Sodinokibi gang hacked law firm of the celebrities and threatens to release the docs," May 9, 2020, **https://securityaffairs.co/wordpress/102960/cyber-crime/sodinokibi-gang-hacked-stars-law-firm.html**.



```
V: We don't have $8,000,000. We laid off [redacted] people due to COVID. We are going to have to lay off more
02:30:43 AM | June 23

A: Offer adequate price and we will consider it, this price must be based on real losses and not your wishes.
04:46:28 AM | June 23

V: What is adequate? I'm sorry, but we don't have millions of dollars.
01:49:43 PM | June 23

V: Due to COVID19 pandemic, we have lost our cash flow and it's extremely limited. The [redacted] industry is
at an all time low right now. We are a small company with limited funds. We can raise our offer to $660,000,
but we don't have millions.
06:19:18 PM | June 24

A: If we publish data you will be forced to pay, but not to us, the minimal estimation of losses is 30 millions
of US dollars, we will make another step forwards you and new price will be $2,500,000. We will not
make more discount, decide.
07:09:52 PM | June 24
```

Fig.1 A screen shot of a chat between a threat actor and ransomware victim. “V” indicates victim. “A” indicates attacker’s input.



URL

http://www.[redacted]

Details

[redacted] is a privately-held, diversified real estate acquisition and development company who don't care about any data breach.

«They are not that rich, the website projects bigger than they are. They are a small company with basic services.»

We've been told.

Example files:

backup_12 - [redacted].zip (525932Kb)
backup_BANK INFORMATION.zip (145710Kb)
backup_2019 [redacted] Recs.zip (822Kb)
backup_Purchases.zip (772Kb)
backup_[redacted] Recons.zip (416Kb)

Fig.2 Screen shot of a publicly listed victim on a dedicated leaking site.

Variant Focus | Maze ransomware

When analyzing victim profiles of Maze, we found that they targeted organizations with the greatest variety in revenue: the lowest revenue amounted to just over $100K and their most lucrative victim allegedly had revenues of $80B. Looking at all 1H20 attacks, Maze victims averaged over $1.5B in revenue, the highest among all ten tracked variants. This data does not suggest Maze holds a preference for more profitable organizations, rather, it suggests the group is willing to attack any and every organization they deem capable of paying a ransom.

In sum, revenue in it of itself is not initially a driver of for ransomware attacks or an enticement to attackers, rather it is the victim’s particular vulnerabilities providing the initial accessibility for threat actors to capitalize on. Once they are in the system and begin to value the organization, revenue becomes one of the factors that influence the subsequent initial ransom demand.

Case Study | Maze attack on large revenue corporation

A $5bn+ revenue healthcare provider suffered a Maze ransomware attack, with the threat actor gaining access to the company's network via a phishing email to employees. After spending several weeks in the network undetected, the threat actor exfiltrates 10GB of data, including corporate confidential information and healthcare data on 1,500 patients.

Afterward, the threat actor deployed the ransomware, which was the company's first indication of a cyber incident. The ransom was $15m in bitcoin, in exchange for a decryption key. The threat actor also threatened to begin posting small increments of patients' healthcare data online until the company pays the ransom.

The company hired a ransomware extortion specialist to negotiate with the threat actor. In the ensuing negotiations the company's critical health function during the pandemic is used to try to mitigate the extortion demand. However, the threat actor brazenly suggests that this is in fact a basis for the demand, not a reason for lessening it. The ransom is nevertheless negotiated down to less than half of the original demand.

Under applicable healthcare regulations, and following proof of data exfiltration from the threat actor and an IT forensics investigation, the company notifies the affected individuals. The company's costs total over $12m, including the ransom payment, IT forensics fees, legal fees, and breach notification with an offer of ID protection to breach victims. Just after notification, a law firm spots a commercial opportunity and files a class action on behalf of breach victims. Several more class actions follow over the next few weeks. Defence costs and a likely settlement will greatly heighten the company's exposure, the final amount of which may not be determined for years.

What can we infer from regional doxing trends?

From the nearly 400 doxed victims across the world which we analyzed for this report, 56% of victims were headquartered in the United States. The next most frequently targeted victims (6% each) hail from Brazil and the United Kingdom. Canada followed at 5%, Australia at nearly 4% and France at nearly 3%. The remaining 21% of publicly listed victims hail from a wide range of countries across South and East Asia, North Africa, Eastern Europe and the Middle East.

Based on this data, U.S.-based organizations seem to be targeted at a higher rate than those based elsewhere – and their blackmailing on doxing sites indicates they may also be more likely to refuse ransom payment due to better implemented back up policies. If we assume that the higher representation on doxing sites corresponds to a higher incidence of ransomware attacks, we can speculate on a few reasons why the United States is disproportionately victimized. First, access to IT technology and infrastructure is more widely spread across the country, allowing more businesses of all sizes and sectors to run digital operations. While greater digital adoption generally enables more business, it also means more poorly secured networks to attack. Additionally, higher GDP translates into higher infrastructural investments by small and large businesses, leading to more devices, larger networks and, ultimately, more attack vectors. And while ransomware operators claim they do not discriminate who and where they target, a greater business presence on the global stage means greater public visibility and availability of corporate data - and thus could lead to a higher chance of being targeted. Attackers may also expect U.S. businesses to hold more financial assets and being able to afford a ransomware attack. Lastly, considering the goal of blackmailing via doxing sites is to elicit payment from victims, the higher representation of U.S. businesses could also indicate that U.S. victims are more likely to refuse initial ransom demands compared to their international peers. Whether this is due to greater availability of cyber insurance coverage, better security operations (e.g. availability of backups) or a cultural stance (i.e. 'we don't deal with terrorists') is a question that requires further research to answer definitively..

One of the most notable differences since our initial report on the doxing trends, *What Doxing Victims Reveal About Targeted Attacks***:** was the rise in number of Brazilian victims to equal those from the United Kingdom.[14] However, while notable, the rise in Brazilian victims is not quite as surprising as it may seem initially. Brazil is the biggest technology hub in Latin America and has a large population of over 200 million people. Digital technology adoption is widespread and internet penetration lies at 70%, which is above the global average of 57%.[15] This again provides cyber-criminals with a large pool of potential attack vectors, especially if one assumes that cyber security awareness is still lower across the country. Much of the growth in ransomware attacks can be attributed to Mespinoza, Maze and Nefilim variants. Nefilim especially targets large-scale Engineering and Construction, and Oil, Gas and Coal industries – industries which are widespread in Brazil, and perhaps also a reason why the country features so dominantly.

Hiscox view

When it comes to doxing, we see attackers going for low volume, high impact confidential corporate information like intellectual property and trade secrets. They are not extracting large volumes of PII/PCI/PHI to sell on the Darkweb, but instead are hunting data that would force a business to pay a ransom to avoid having the information published externally.

[14] *What Doxxing Victims Reveal About "Targeted Attacks,"* Kivu Consulting, May 2020, **https://kivuconsulting.com/wp-content/uploads/2020/05/Kivu-Threat-Intel_What-Doxxing-Victims-Reveal-About-Targeted-Attacks_May2020.pdf**.

[15] "Brazil: Digital in 2019 Report," *PagBrazil,* 2019, **https://www.pagbrasil.com/insights/digital-in-2019-brazil**.

Though our data supports Kivu's view that different ransomware gangs apply various doxing methods, we are also seeing an increase in ransomware for different industries and sectors. According to the Hiscox Cyber Readiness Report 2020, we saw hackers focus more on industries such as Energy and Manufacturing. We believe there are three reasons for this. Firstly, reliance on automation (i.e. managed by computers). Secondly, low maturity in cyber resilience (e.g. poor back-ups, limited disaster recovery planning or testing). And finally, low tolerance to what is often a high-impact outage. This offers rich pickings for ransomware attacks. Doxing brings additional challenges since it introduces third party obligations to victims. Liability to customers and regulatory investigations increase costs and extend the time of claim settlement. Instead of a ransomware event taking six to twelve months to recover, an additional doxing incident could require three to four years to fully resolve.

Ransomware Variants and Their Targets in 1H20

Each ransomware variant – and the group which operates it - has its unique traits and characteristics. This means there is no one size fits all approach to countering and mitigating ransomware attacks. Adding to the complexity, cyber criminals often move between groups or offer their services as freelancers, bringing their unique M.O. to whoever they happen to partner with at a given time. This dynamic, in addition to business variables, victims' technology practices, the COVID-19 pandemic and, at times, geopolitical considerations, all shape and form variants' notable differences in doxing habits below.

AKO: Ransomware group AKO's victims are equally spread across the Consumer Discretionary and Industrials sectors, with both making up 33% of their attacks. Consumer Discretionary victims included school districts, law firms, and advertising and marketing agencies, while construction and machinery firms fell within the Industrials sector. These were followed by Consumer Staples, Healthcare and Technology, each making up 11% of victims. 67% of AKO victims are headquartered in the United States.

Cl0p: Ransomware group Cl0p primarily targeted the Consumer Discretionary sector (36%), followed by Industrials and Technology at 18% each. Nearly half of Cl0p's victims are headquartered in Germany, followed by 18% in the United States, and additional victims based in the UK, Austria, Spain and India.

DoppelPaymer: The majority of doxed victims of ransomware group DoppelPaymer all within the Consumer Discretionary sector, amount to a total of 36%. This was followed by Industrials (18%) and Financials (15%). DoppelPaymer's victims include automotive retailers, home improvement, and professional services, and primarily hail from the United States 55%), followed by France (12.5%) and Canada (10%).

Maze: Ransomware group Maze is arguably the most prolific and opportunistic group, known for targeting any and every sector where circumstances are exploitable. The most targeted sectors by Maze include Consumer Discretionary (23%), Industrials (25%), Financials (12%), Technology (11%), and Healthcare (7%). While an overwhelming proportion of Maze victims are from the United States (68%), these are followed by Canadian organizations (6%) and British organizations, which make up 3% of their victims. The remainder of their targets stem from an additional 25 countries across the globe. With victims from over 30 countries, Maze's operations are scaled at enterprise level and seem to follow a policy to indiscriminately target no one region or sector, unlike other groups such as AKO.

An additional defining characteristic of Maze is its tactic, likely inspired by Nephilim, to incrementally leak stolen data. By doing so the group turns a zero sum game – either the ransom is paid and no data is leaked, or it isn't paid and all data is published – into a more fluid situation which offers victims a chance to negotiate payment based on the amount of data not yet leaked. This creates urgency and pressure for the victims to respond in a timely manner, but also allows for negotiations and a certain amount of damage control.

Mespinoza (PYSA): Ransomware group Mespinoza (also known as Protect Your Systems Amigo: PYSA), is one of the most diverse in the sectors and regions it targets. They do, however, heavily target the Consumer Discretionary (29%), Healthcare (19%), and Public (14%) sectors, followed by Consumer Staples, Industrials, Materials, and Technology sectors, all at around 9.5%. PYSA's targeted regions were split at 13% between Australia, UK, and USA, followed by Colombia, Mexico, Brazil, and France at 9%.

Nephilim: Ransomware group Nephilim, as mentioned prior, was one of the first groups to incrementally leak stolen data, likely inspiring other ransomware groups to follow. Nephilim victims stem from four sectors: 33% in Energy; 33% in Industrials; 22% in Consumer Discretionary; and 11% from Financial. In addition, Nephilim's attacks generally target companies with high revenue in the upper 100s of millions stretching into the billions. During the first half of 2020, 33% of their victims originated from Brazil, while the remaining pool was made up of India, Sri Lanka, Australia, Switzerland, New Zealand and the United States.

NetWalker: Ransomware group NetWalker continues the trend of heavily targeting organizations in the Consumer Discretionary sector, with 31% of their victims operating in this field. This is followed by the Industrials (19%), and Technology and Healthcare (both 12%) sectors. NetWalker's healthcare victims are an anomaly in comparison to most other variants. When the sector began to struggle with the surge in COVID patients, NetWalker was one of the variants claiming they would not target healthcare institutions.[16] In reality, during the months of May and June NetWalker continued attacking healthcare organization

[16] Lawrence Abrams, "Ragnar Locker Ransomware Targets MSP Enterprise Support Tools," *Bleeping Computer,* February 10, 2020, **https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/**.

in the United States and Australia. An overwhelming number of NetWalker's victims are based in the USA at 65%, followed by Australia and France at 7% each.

RagnarLocker: 33% of RagnarLocker's victims hail from the Consumer Discretionary sector. Their other victims are found in the Industrials and Communications sectors (both at 22%), followed by Technology and Utilities (also both at 11%). One of RagnarLocker preferences is leveraging compromised Managed Service Providers (MSPs), to infiltrate and expand their attack surface, as was the case with one of their highest profile attacks on Energias de Portugal (EDP). RagnarLocker victims are primarily based in the United States (67%), while the remainder stem from Germany, Singapore and Portugal.[17]

Sodinokibi/**REvil**: Ransomware group Sodinokibi, also known as REvil, has a strong preference for Consumer Discretionary services such as professional services and wholesalers, with 43% of their victims hailing from this sector. Their other targeted sectors include Industrials (16%), Financials (13%) and Technology (7%). One of their higher profile attacks targeted law firm Grubman Shire Meiselas & Sacks, P.C., which made the news when the group started auctioning off the firm's confidential data on well-known celebrities. 65% of REvil's victims are based in the United States, followed by 8% of victims from the United Kingdom and 6% from Australia.

Sekhmet: The ransomware group Sekhmet mostly targeted the Consumer Staples sector, with 33% of victims operating in this field. This was followed by Consumer Discretionary, Financials, Industrials and Technology sectors, each making up approximately 17% of their victims. Once again, most of Sekhmet victims are based in the United States (43%), 29% hail from the United Kingdom and 14% from Spain and Brazil each. Sekhmet victims include insurance providers, law firms and IT services.

Closing thoughts on variants' doxing

Ransomware groups are motivated by financial gain. Where extortion was unsuccessful, doxing becomes an exhibition of bravado. Attackers have created their own self-serving platform to showcase the success of their exploits, despite missing a pay day. In a parallel, the public leaking sites leverage the seriousness of their threat to extort a payment even if the victims have unaffected backups. Thus, where backups are viable, a ransomware attack not only halts their business operations incurring lost opportunity, but victims who do not pay can still punished by having their name and/or data publicly leaked.

[17] Lawrence Abrams, "Ragnar Locker Ransomware Targets MSP Enterprise Support Tools," *Bleeping Computer,* February 10, 2020, **https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/**

Throughout 1H20, public leaking sites was a vehicle of the success of ransomware groups, but exposed the scale and magnitude of their operations across the globe and industries associated.

Conclusion and Outlook

While the number of ransomware incidents remained consistent throughout Q1 and Q2, throughout 1H20 the number of doxed victims grew exponentially, and we found attackers using more sophisticated tactics to justify their ransom demands.

By leveraging a variety of methods for infiltration - often opportunistic vulnerabilities such as weak security configurations on remote infrastructure, Remote Desktop Protocol (RDP), or CVEs – attackers have honed their skills to remain within networks for longer periods of time, allowing them to conduct more thorough research on their victims. Attackers are also finding that the threat of regulatory penalties, reputational harm, and other legal complications is a powerful motivator for victims to pay ransoms, leading to a growing trend of data exfiltrating and doxing.

Amid the pandemic, ransomware groups attacked critical services such as educational institutions, healthcare providers and IT services, exploiting society's increased reliance on these sectors. Yet, while the public and healthcare sectors inevitably grabbed the spotlight in media coverage of ransomware attacks, the consumer discretionary, industrials, and financial sectors suffered the largest number of attacks.

Looking ahead, building cyber resilience is essential for all companies. The pandemic and its dramatic effect on working patterns the world over has arguably fast-tracked a digitalization trend that was already in progress. Businesses and individuals have had to learn the hard and fast way to move their operations online, and to secure them against cyber threats.

As these attacks evolve, and as businesses increasingly rely on digital operations for their survival, we believe we will see more social engineering and ransomware attacks in the months to come, and certainly into 2021.

The real test for cyber resilience will be the start of the academic year across the world and the overall growth of remote infrastructure as administrative and quotidian tasks and processes are moved online. Anecdotally, we are already seeing increasing ransomware attacks on educational institutions and a rush of these entities to cyber-proof their online infrastructure, albeit in some cases rather belatedly. The U.S. election will be one to watch not for any political reason per se, but for the possible effect on sanctions pertaining to ransomware groups. Already the OFAC has sanctioned Evil Corp, the group behind the WastedLocker ransomware variant. If attempts to affect the outcome of the election are identified as being carried out by nation state-affiliated ransom groups, those operators will become sanctioned as well. This will affect the options available to ransomware victims, as paying a ransom to these actors will violate U.S. law. Kivu will be watching this space closely and report on findings in early 2021.

Hiscox view

Ransomware continues to be a game of cat and mouse, and from an insurance perspective we're seeing ransomware continue to evolve. In 2019, customers and insurers worked out that good back-up management helped decrease ransomware claim severity. This improvement in risk management, however, has forced ransomware gangs to evolve their tactics and exfiltrate data in order to demand higher ransoms from fewer targets. For companies over $5b, the change has been more extreme. Not only has the tactic of doxing developed, but more generally ransomware claim frequency and severity has risen sharply as well.

The principle of insurance is for the premiums of the many to pay for the losses of the few, and when the balance shifts, generally three things start to change – price, terms and conditions, and a demand for improved risk management from customers. Up until recently insurers have been focused on setting the right price and improving their risk selection by better understanding the risk management controls of their customers. Now, we have started to see the tightening of terms and conditions in the form of co-insurance or sub-limits on ransom payments. As ransomware gangs evolve, so to must insurers. In September 2020 we saw the first death related to a ransomware incident in Germany. Loss of life and threat to life increase pressure on law enforcement and government to intervene.

The COVID-19 pandemic has brought its own set of challenges when it comes to ransomware. Lockdown rendered some back-up data useless as it fell behind in time, and remote or decreased workforces have made it harder to ensure proper patching and timely software updates. More unpatched vulnerabilities means more opportunity for ransomware gangs. Cyber security resilience and doing the basics well is still imperative. In the Hiscox Cyber Readiness Report 2020, the top three spending priorities over the next 12 months were regular evaluation of security, additional security or audit requirements, and increased spending on employee training. Ransomware will continue to evolve, but it is about building cyber resilience against it.

Bibliography

"Abnormal Security Data Reveals 200 Percent Monthly Increase in Invoice and Payment Fraud Business Email Compromise Attacks." *Business Wire.* June 29, 2020. **https://www.businesswire.com/news/home/20200629005113/en/Abnormal-Security-Data-Reveals-200-Percent-Monthly**.

Abrams, Lawrence. "Ragnar Locker Ransomware Targets MSP Enterprise Support Tools." *Bleeping Computer.* February 10, 2020. **https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/**.

Abrams, Lawrence. "Ransomware Gangs to Stop Attacking Healthcare Orgs During Pandemic." *Bleeping Computer.* March 18, 2020. **https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/**.

Beazley 2020 Breach Briefing. Beazley. 2020. **https://www.beazley.com/Documents/2020/beazley-breach-briefing-2020.pdf**.

"Brazil: Digital in 2019 Report." *PagBrazil.* 2019. **https://www.pagbrasil.com/insights/digital-in-2019-brazil**.

Cofense Q2 2020 Phishing Review. Cofense. 2020. **https://cofense.com/wp-content/uploads/2020/07/Q2-2020_Phishing-Review.pdf**.

Cohen, Jason. "Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine." *PCMag.* March 30, 2020. **https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine**.

Cimpanu, Catalin. "GandCrab ransomware operation says it's shutting down." *ZDNet.* June 1, 2019. **https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/**.

Cimpanu, Catalin. "US Secret Service reports an increase in hacked managed service providers (MSPs)." *ZDNet.* July 6, 2020. **https://www.zdnet.com/article/us-secret-service-reports-an-increase-in-hacked-managed-service-providers-msps/**.

Cyber Claims Study 2019 Report. Net Diligence. 2019. **https://netdiligence.com/wp-content/uploads/2020/05/2019_NetD_Claims_Study_Report_1.2.pdf**.

Degrippo, Sherrod. "Ransomware as an Initial Payload Reemerges: Avaddon, Philidelphia, Mr. Robot, and More." *Proofpoint.* June 25, 2020. **https://www.proofpoint.com/us/blog/security-briefs/ransomware-initial-payload-reemerges-avaddon-philadelphia-mr-robot-and-more**.

Di Clemente, Richard et. al. "Supplementary Information: Diversification versus specialization in complex ecosystems." *Instituto dei Sistemi Complessi.* 2020. **https://journals.plos.org/plosone/article/file%3Ftype%3Dsupplementary%26id%3Dinf**

o:doi/10.1371/journal.pone.0112525.s002#:~:text=Sectors%20(or%20subsectors)%20are%20hierarchically,classification%20system%20for%20stock%20companies.

“Exploiting a crisis: How Cybercriminals behaved during the outbreak.” *Microsoft.* June 16, 2020. **https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/**.

Hiscox Cyber Readiness Report 2020. Hiscox. 2020. **https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf**.

Paganini, Pierluigi. “Sodinokibi gang hacked law firm of the celebrities and threatens to release the docs.” May 9, 2020. **https://securityaffairs.co/wordpress/102960/cyber-crime/sodinokibi-gang-hacked-stars-law-firm.html**.

Rainer, Alan. “Ransomware: A Mid-Year Summary.” *Cofense.* July 22, 2019. **https://cofense.com/ransomware-mid-year-summary/**.

“The enduring threat of ransomware.” Beazley. June 9, 2020. **https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html**?.

What Doxxing Victims Reveal About “Targeted Attacks.” Kivu Consulting. May 2020. **https://kivuconsulting.com/wp-content/uploads/2020/05/Kivu-Threat-Intel_What-Doxxing-Victims-Reveal-About-Targeted-Attacks_May2020.pdf**.

About this Report

This report is a joint initiative between Kivu Consulting and Hiscox, and uses data and insight from various sources, including proprietary Kivu research, public websites and Hiscox's annual Cyber Readiness Report. In addition, the authors have drawn on internal datasets available exclusively to Hiscox and Kivu staff, respectively.

All efforts have been made to ensure that information contained herein is correct and accurate as of the date of publication, 1 October 2020.

About the Authors

Tess Frieswick

Tess is a Client Success Manager at Kivu Consulting, with experience in security and crisis response as well as research. She helps clients improve their security posture.

Email | tfrieswick@kivuconsulting.com

Max Kochev

Max is a Threat Intelligence Analyst at Kivu Consulting in Washington D.C., focusing on data exfiltration and doxing trends among ransomware operators and the darknet landscape.

Email | mkochev@kivuconsulting.com

Alan Rainer

Alan Rainer is a Threat Intelligence specialist with multi-faceted experience in cyber security analysis and products as well as team leadership.

Email | arainer@kivuconsulting.com

About Hiscox

At Hiscox, we offer tailored insurance solutions to help you across all areas of your life, from business to home. With over 100 years of industry experience and the expertise of our brokers, we've fine-tuned our insurance products to provide the essential cover when things don't go exactly to plan.

For brokers looking to create more bespoke coverage, our underwriters work closely with insurance brokers across the globe to ensure the best possible level of cover for your clients.

hiscoxlondonmarket.com
hiscox.com

Contact Hiscox

For more information on Hiscox Cyber products, please contact us.

Meghan Hannes
Cyber Product Head
Hiscox USA
meghan.hannes@hiscox.com

Matthew Webb
Cyber Product Head
Hiscox London Market
matthew.webb@hiscox.com

About Kivu

Kivu is a leading global cyber security firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. By combining analyst expertise, patented proprietary technology and exclusive threat intelligence, we deliver cutting edge cyber security solutions to organizations in need across the globe.

Headquartered in the U.S. with offices worldwide, Kivu is a trusted cyber incident partner to insurance carriers and law firms.

kivuconsulting.com

Contact Us

Our purpose is to restore freedom of operation and to minimize business interruption, getting organizations back online quickly and securely.

info@kivuconsulting.com