Abnormal

THREAT INTELLIGENCE REPORT

The Evolution of Ransomware: Victims, Threat Actors, and What to Expect in 2022

Executive Summary

While ransomware has been a problem for three decades, the last few years brought rapid changes to the threat ecosystem. Our research shows that ransomware delivery methods have evolved, payouts are growing in frequency and total cost, and there are more malicious actors participating in ransomware than ever before.

The average payment amount in ransomware attacks has skyrocketed from hundreds of dollars just five years ago to tens of thousands of dollars today, with some payments reaching millions of dollars. Today's ransomware landscape is primarily driven by three factors, most notably ransomware-as-a-service (RaaS), extortion beyond encryption, and the evolution of cryptocurrency payments. Combined, it creates an environment where ransomware attacks have become more popular, particularly in the last two years.

From the start of 2020 to the end of 2021, the Abnormal team identified 4,200 companies, organizations, and government institutions that have all fallen victim to a ransomware attack. While manufacturing companies were the most common victims, representing 20% of ransomware attacks, **all industries are at risk.**

Enterprise companies represent a larger payout, but **small businesses are the most common victims** due to opportunistic targeting and fewer cybersecurity resources. The median revenue of ransomware victims since 2020 is just $27 million, and only 10% of victims have revenue above $1 billion.

Although companies in the United States have received half of the attacks since 2020, **ransomware is a global problem**. It's most prevalent in countries with a high GDP, although it's not as pervasive in Asian countries and is nonexistent in Russia. Because many top ransomware groups are based in Russia, they may purposefully avoid ruffling feathers by not targeting domestic companies.

4,200

Number of ransomware victims identified

$27M

Median revenue of a ransomware victim

33%

Percentage of victims making less than $10 million a year

Abnormal™

Only five ransomware groups are responsible for more than half of the attacks since 2020. We saw noticeable spikes in attacks in August 2020 due to the emergence of Conti and REvil, and again in October 2021 due to an escalation in activity from Conti, LockBit, and Pysa. The growth of RaaS as a delivery method means **a small number of ransomware groups can drive substantial malicious activity.** One silver lining is that the centralized hierarchy of RaaS means law enforcement efforts can disrupt a large portion of attacks. But the threat is evolving: when one group is taken down, new ones sprout to take its place, often capitalizing on the experience of their predecessors.

In short, the threat of ransomware is growing, and attacks and payout amounts are increasing substantially. Attackers target companies of all sizes across all industries, and even small groups of cybercriminals can cause disproportionate damage. This threat is difficult to stop, and **it is vital that organizations invest in cybersecurity solutions against ransomware to protect themselves and their end users—before it's too late.**

110

Countries where victims were identified

5

Number of ransomware groups responsible for over half of all attacks.

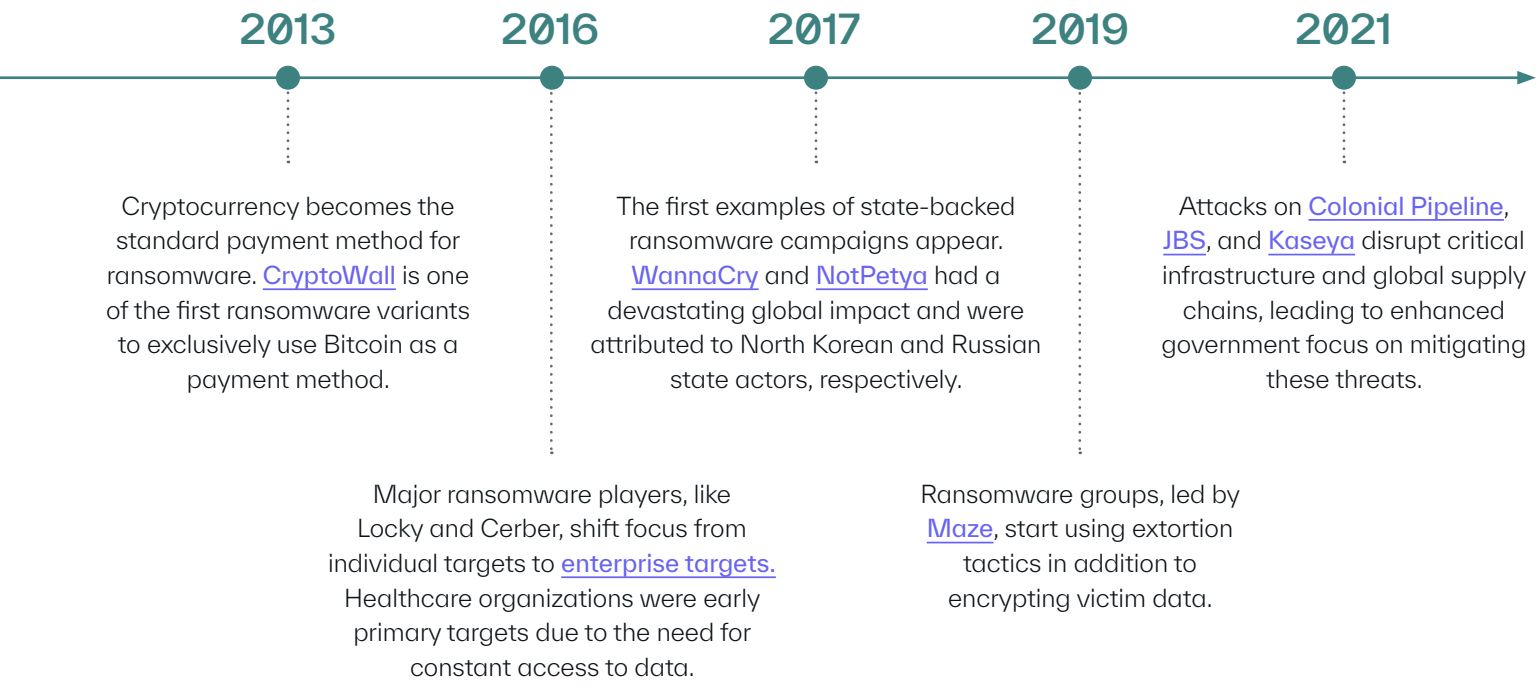
Table of Contents

A Brief History of Ransomware

Ransomware is not a new threat and in fact, has been used by cybercriminals for more than three decades. The first documented cyber attack using malware dates back to a 1989 piece of malware targeting AIDS researchers that was delivered via floppy disk.

Thankfully, early ransomware was very rudimentary, using very basic data encryption techniques. However, starting in the mid-2000s, cybercriminals started using asymmetric encryption—marking the beginning of modern ransomware.

While ransomware has been active for more than 30 years, there have been a number of important milestones over the past decade that have shaped ransomware into the threat we see today.



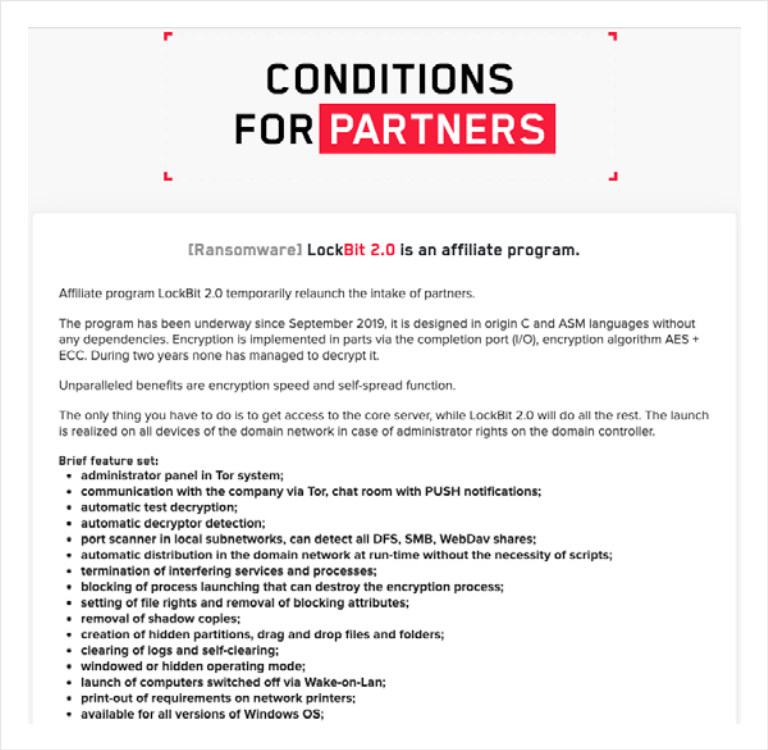
The delivery mechanism for ransomware has also seen a significant shift in recent years. While it is still delivered through email, most cybercriminals today also rely on new tactics—exploiting network access footholds established by other malware infections or exploited software vulnerabilities to deploy ransomware on a corporate network.

What's New? The Driving Factors Behind the Ransomware Landscape

The ransomware landscape has changed a great deal over the past ten years. Today, ransomware attacks are driven by three primary factors—ransomware-as-a-service, extortion, and cryptocurrency—and each of these variables influences the overall threat of ransomware in distinctly different ways.

01. Ransomware-as-a-Service (RaaS)

The "as-a-service" model has been a fixture in the cybercrime landscape for more than a decade. This business model has been successful because, like legitimate software-as-a-service companies, cybercrime groups are able to develop a "product" and license it to other cybercriminals in exchange for either a fixed price or a cut of an affiliate's proceeds. These as-a-service offerings are commonly advertised on various underground cybercrime forums.



Affiliate program advertisement on the LockBit blog.

This model is attractive to cybercriminals for two reasons:

1. It allows them to focus on monetizing their product without worrying about the additional overhead required to launch a cyber attack.
2. It puts them an arms-length away from an actual attack, letting affiliates assume a majority of the risk.

Nearly all of today's most prolific ransomware groups operate on a RaaS model. The primary reason RaaS drives the ransomware landscape is because it allows less technically sophisticated actors to enter the space—cybercriminals don't have to develop malware on their own in order to conduct ransomware attacks, which significantly increases the population of actors able to carry out an attack.

However, this model does create a very centralized hierarchy. Affiliates rely on the main ransomware developers for access to the resources needed to facilitate their attacks. If a primary ransomware group is disrupted by law enforcement or its infrastructure is taken down, it can have a noticeable impact on the entire ecosystem, at least in the short term. This is different from other cyber threats like business email compromise, which has a much more decentralized hierarchy and where the arrest of one group does not impact the rest of the ecosystem.

02. Extortion

Until a few years ago, the most common guidance to prepare for a potential ransomware attack was to ensure that an organization had regular, secure, and offline backups of all critical data. In case of a successful attack, any encrypted data could just be restored using those backups, which mitigated the data loss impact of the attack. This all changed in 2019 when ransomware groups like Maze added secondary extortion tactics to their playbook. Instead of just encrypting the files of an impacted organization, most ransomware groups today also download those files and threaten to publicly release them if the ransom isn't paid.

Attention!

| What happened?

All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You have a chance! It is easy to recover in a few steps.

| How to get my files back?

The only method to restore your files is to purchase a unique for you private key which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR Browser.
c) Open the TOR Browser.
d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/
e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

a) Open our website: https://mazedecrypt.top/
b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.
Also it has a live chat with our operators and support team.

Maze ransomware extortion note.

For organizations that refuse to pay the ransom, ransomware groups have launched blogs on the dark web where files can be downloaded by anyone visiting the site. This tactic changes the calculus of how an organization may decide to respond to a ransomware attack by adding an additional incentive to the equation. Instead of only weighing the cost of backup restoration and remediation, an organization must also factor in the cost of potentially sensitive information being leaked publicly. In some cases, this may persuade a victim company to pay a ransom they wouldn't have previously paid.

Examples of ransomware blogs on the dark web.

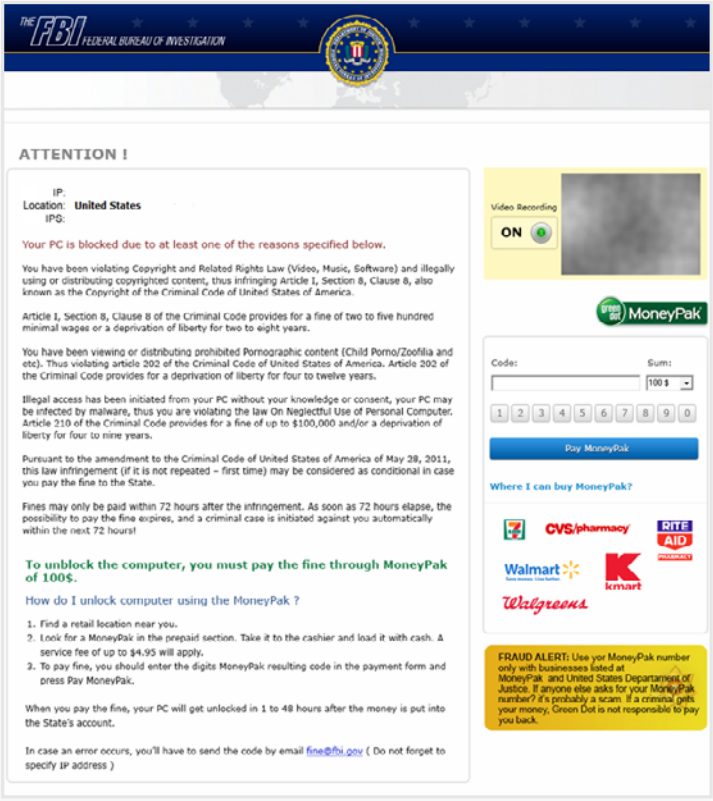
Abnormal™

03. Cryptocurrency

The third and largest driver of ransomware today is cryptocurrency. In the early days of ransomware, ransoms were requested using obscure payment methods, such as MoneyPak, Ukash, or PaysafeCard. Not only did these methods require a victim to purchase a physical payment card, but it also put an artificial ceiling on ransom amounts. Because of the practical challenges of these payment methods, the average amount paid in ransomware attacks a decade ago hovered around $100.

While bitcoin was created in 2008, it wasn't until 2013 that cybercriminals started using cryptocurrency as the exclusive method for the ransom payment. Cryptocurrency affords a number of advantages over previous payment methods used in ransomware attacks, including:

1. The relative anonymity of cryptocurrency payments (particularly on the receiving end) and the availability of tumbling services help cybercriminals protect their identities.
2. The ability to send payments via cryptocurrency is relatively frictionless and quick, unlike other payment methods like wire transfers.
3. Most importantly, the total amount that can be easily sent using cryptocurrency is substantially higher than other payment methods.



Reveton ransom message, circa 2012.

These factors, combined with the explosion of cryptocurrency prices over the past few years, have resulted in substantially higher ransom payments—and bigger profits for the cybercriminals. As a result, the average payment amount in ransomware attacks has skyrocketed from hundreds of dollars just five years ago to tens of thousands of dollars today, with some payments reaching millions of dollars.

Who's Targeted? A Look at Ransomware Victimology

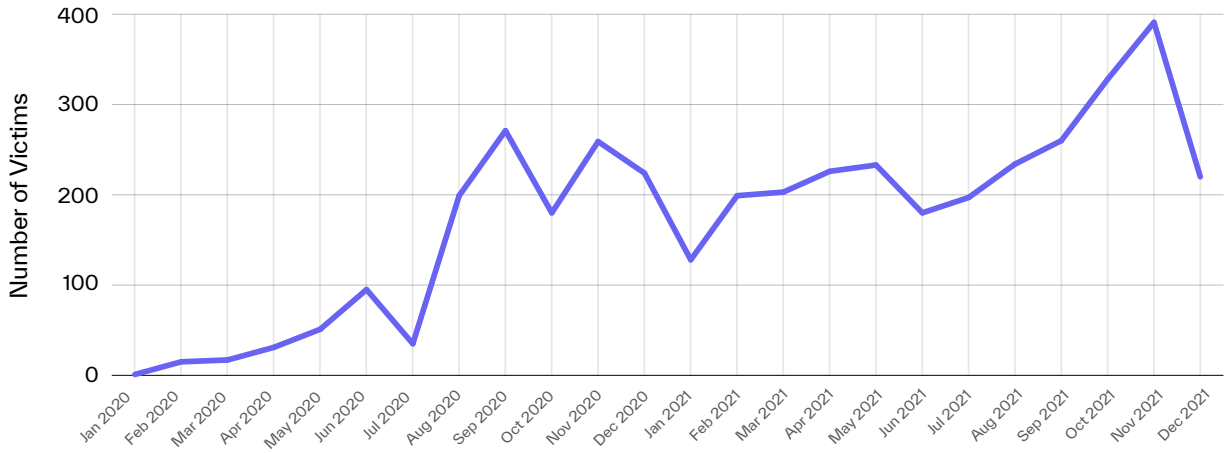
Since the beginning of 2020, we identified nearly 4,200 companies, organizations, and government institutions around the world that have been the victims of ransomware attacks. We identified these victims through a combination of ransomware extortion blog monitoring on the dark web and open source intelligence collection. While this is by no means the entire population of victims impacted by ransomware during this time period, the size is likely representative of the overall threat landscape, which allows us to make inferences about global ransomware trends.

The Recent Ransomware Explosion

Looking at the overall volume trends, there have been two main spikes in ransomware activity over the last two years. The first half of 2020 was relatively quiet; however, in August and September 2020, we observed a significant increase in ransomware victims. This surge corresponds to the arrival of two of the most prolific ransomware groups in recent years: Conti and REvil.

After this initial spike, the number of ransomware victims remained relatively consistent month-to-month until October and November 2021, when we saw our second significant surge in ransomware victims. This second increase can be attributed to a noticeable escalation in activity from a handful of top ransomware groups, including Conti, LockBit, and Pysa.

Monthly Ransomware Victim Volume



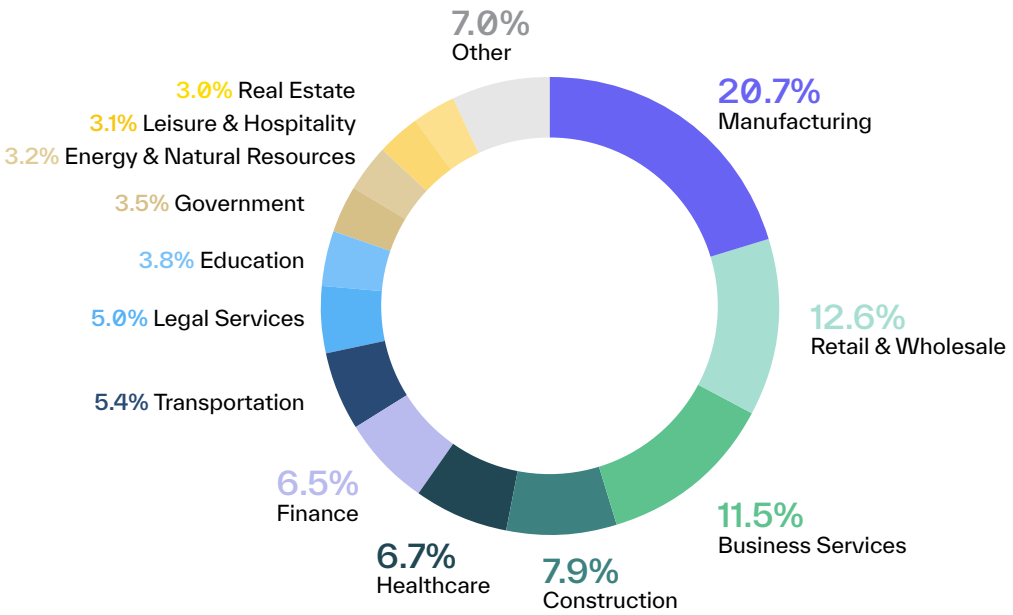
Victims by Industry

Ransomware is not a threat that targets only certain industries, but is what we would consider to be industry agnostic. This means that, like other financially-motivated cyber attacks, the focus of most ransomware attacks is more about the ability to quickly profit from the exploitation of a corporate network and less about the characteristics of the victim company itself.

A great example of this was DarkSide's response to the impact of their attack on Colonial Pipeline in May 2021. In a post to their blog, DarkSide released a statement saying, "Our goal is to make money, and not creating [sic] problems for society. From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

This indifference to industry can also be seen in our data, as there isn't one sector that clearly overshadows others in terms of attack volume. That said, one out of every five ransomware victims fell within the manufacturing industry—a sector that has also been a preferred target of business email compromise (BEC) attacks due to the frequency of large invoices and international payments. Rounding out the top five most impacted sectors were retail and wholesale, business services, construction, and healthcare.

Ransomware Victims by Primary Industry



Abnormal™

Breaking the primary industry data into sub-sectors gives us a more granular picture of ransomware targets. Ironically, the sub-sector that saw the largest number of ransomware attacks was the computer and technical business solutions sector. Almost 300 companies providing technical solutions were hit with ransomware attacks over the course of these two years, reminiscent of APT targeting of similar services. One of the most high profile of these attacks was against Kaseya, a technology company that offers software to managed service providers (MSPs), by the ransomware group REvil in July 2021.

Other notable sub-sectors commonly targeted by ransomware attacks included legal services, freight and shipping services, computer and electronics manufacturing, healthcare services, and state and local government agencies.

Top 10 Sub-Sectors Impacted by Ransomware Attacks

Sub-Sector	Number of Victims
Computer & Technical Solutions	**295**
Construction Services	**227**
Legal Services	**210**
Freight and Shipping Services	**191**
Industrial & Commercial Equipment Manufacturing	**189**
Computer & Electronics Manufacturing	**123**
Motor Vehicle & Accessory Sales	**121**
Healthcare Services	**116**
State & Local Government	**102**
Insurance	**85**

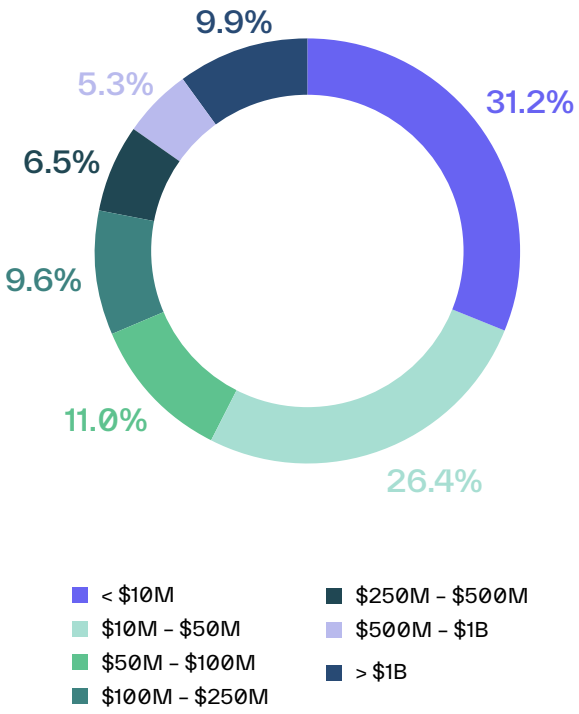
To learn more about how ransomware is impacting your industry, email us at ransomware@abnormalsecurity.com.

Victims by Revenue

One of the biggest misconceptions about ransomware attacks is that they primarily impact large organizations that can afford to pay substantial ransoms. After all, most of the attacks reported in the media are generally those that victimized big, notable companies. Based on our data, however, the belief that these large enterprises are the preferred targets of ransomware actors is a myth.

The median estimated annual revenue for companies victimized by ransomware was just $27 million. Nearly a third of all victims had an annual revenue of less than $10 million and just under 60% of victims generated an annual revenue of less than $50 million, meaning a majority of ransomware targets can be classified as small businesses. Only 10% of ransomware victims were enterprise-sized companies with an annual revenue of more than $1 billion.

Estimated Annual Revenue of Ransomware Victims



While this appears to run counter to the conventional wisdom that the largest entities with the choicest data and heftiest budgets are the most attractive ransomware targets, this distribution makes sense. As we discussed earlier, the primary motivation for almost all ransomware groups is financial gain, so they will take money wherever they can get it.

And because smaller companies are generally unable to invest large amounts of money in cybersecurity, they're more likely to have fewer defenses in place that may prevent ransomware attacks, making them opportunistic targets. If ransomware actors were more focused on selecting ideal targets that could deliver a higher payday, we'd expect the proportion of large enterprise victims to be much larger.

Victims by Location

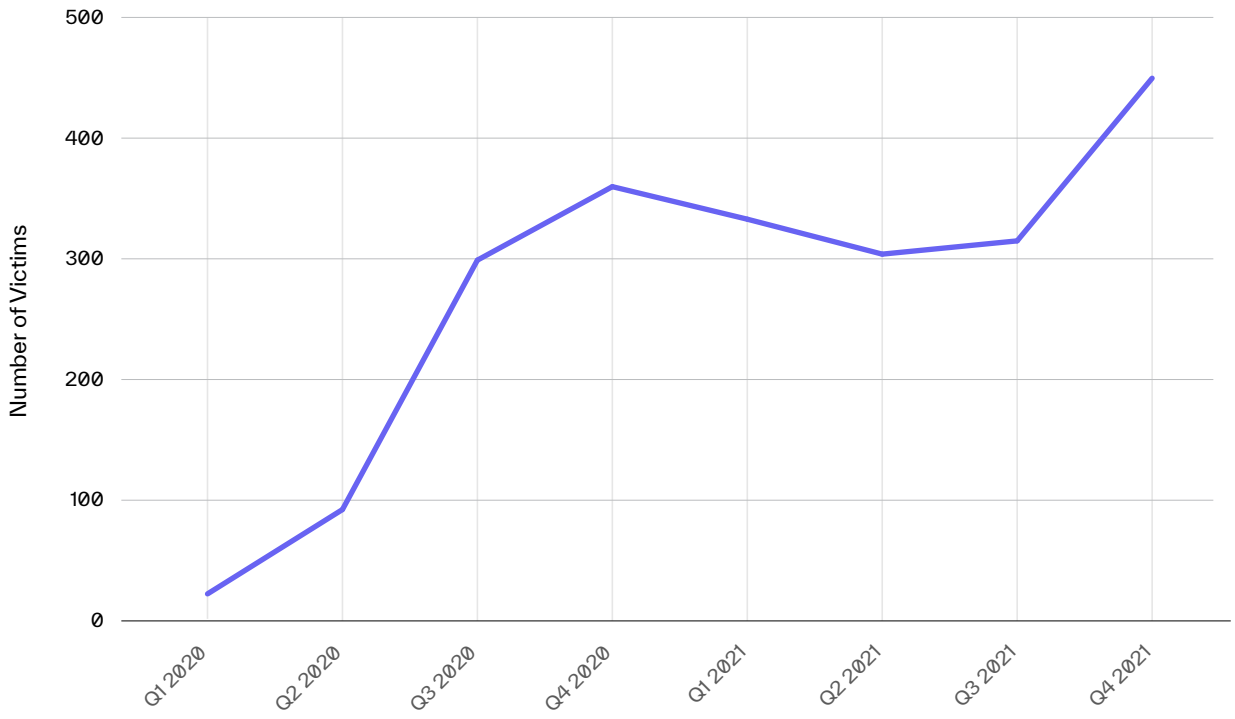
A look at the locations of ransomware victims provides a good sense of the global impact of this threat. We identified victims located in 110 countries around the world. Notably, of the top 67 counties in the world by GDP, Russia is the only country where a ransomware victim was not located. Of course, these findings aren't exactly surprising.

It's commonly known that a significant number of prolific ransomware actors are located in Russia, and it has been an open secret that groups actively avoid targeting Russian companies to steer clear of the attention of Russian authorities. However, when a vast majority of the world's most developed countries are negatively affected by ransomware, it's eye-opening that there is a massive Russian void on the map.

Locations of Ransomware Victims by Country

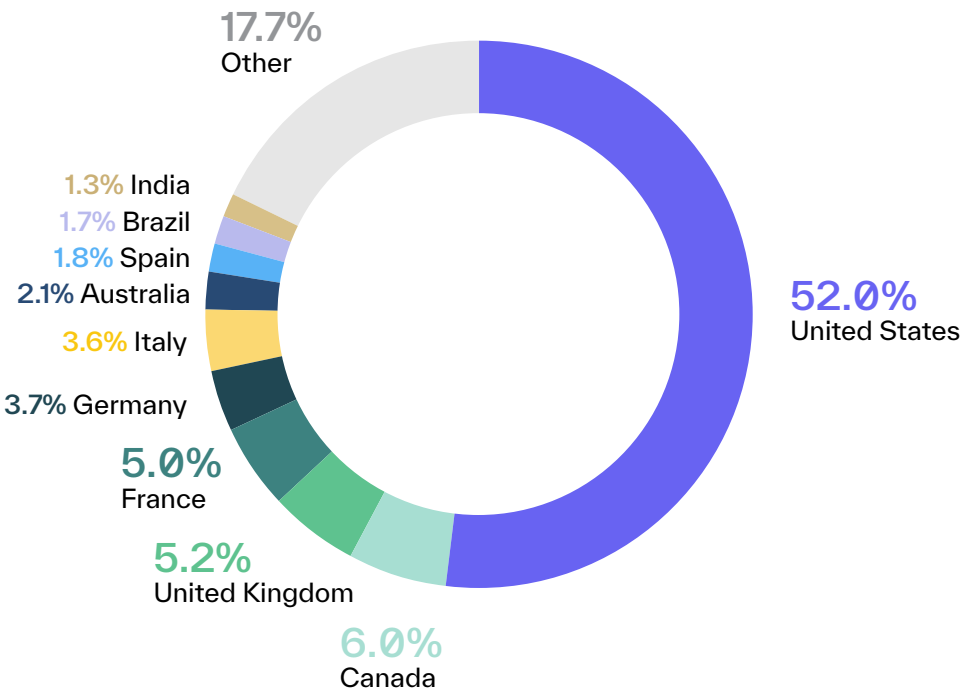
Like most cyber attacks, the United States is the home for a majority of ransomware victims, with just over half of ransomware victims located in one of the fifty states. Interestingly, the significant focus from United States authorities on ransomware in the first half of 2021 seems to have done little to deter ransomware actors from targeting American companies. The last quarter of 2021 saw the highest number of ransomware victims in the United States in the past two years—a 43% increase from the previous quarter.

Trend of Ransomware Victims in the United States



After the United States, the rest of the top 10 countries linked to ransomware victims include most of the next wealthiest countries in the world, primarily in Western Europe and North America. This list consists of Canada, the United Kingdom, France, Germany, Italy, Australia, Spain, Brazil, and India.

Ransomware Victim Locations by Country



Notably absent from this list, however, are the richest countries in East Asia—China, Japan, and South Korea. Each of these countries ranks among the top 10 nations globally by GDP, but the number of ransomware attacks impacting companies in these countries is much lower than expected.

So why is this? Perhaps the language barrier is more difficult to overcome and cybercriminals find it more difficult to communicate with victims in these countries, as compared to European or North American companies. The issue may be technical, as languages with large character sets like Japanese are challenging to encode and must use a more complicated double or multiple byte system. Or maybe cultural norms concerning cybersecurity in these countries decrease the overall success rate for ransomware attacks. While we don't know exactly why the number of successful ransomware attacks in these countries is lower than expected, it certainly stands out.

Comparison of Country GDP Rank to Ransomware Victim Rank

GDP Rank[1]	Country	Ransomware Victim Rank
1	United States	1
2	China	14
3	Japan	11
4	Germany	5
5	United Kingdom	3
6	India	10
7	France	4

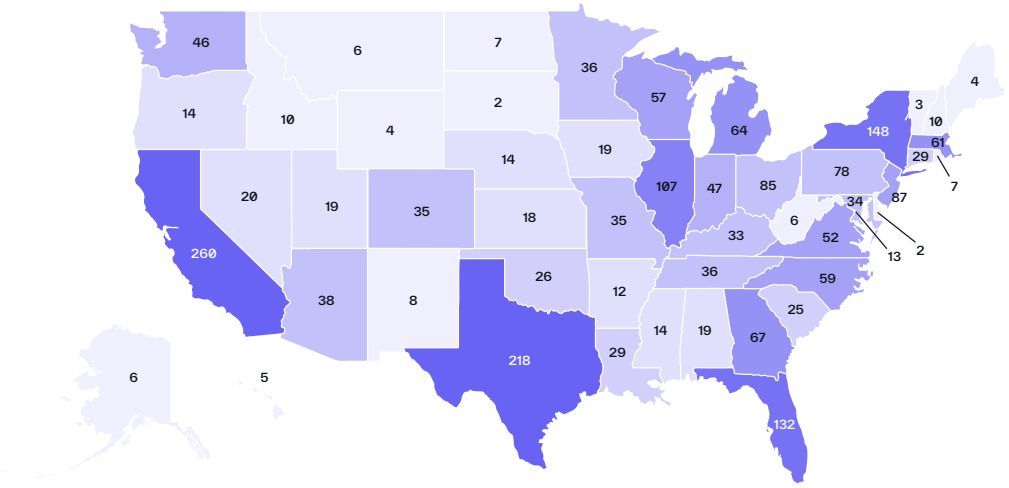
GDP Rank[1]	Country	Ransomware Victim Rank
8	Italy	6
9	Canada	2
10	South Korea	36
11	Russia	N/A
12	Australia	7
13	Brazil	9
14	Spain	8

[1] *International Monetary Fund (IMF)*

Similar to the global distribution of ransomware attack locations, the states linked to ransomware victims in the United States also map closely to GDP. California, Texas, New York, Florida, and Illinois were home to the most ransomware victims and made up 36% of all attacks targeting US companies. Those five states also make up the top five states for GDP, in the exact same order.

To put the volume of attacks impacting companies in these states in context, if California were a country, it would have been the second-most victimized country in the world, trailing only the United States. Texas would have been tied for third with the United Kingdom.

Ransomware Victim Locations by State



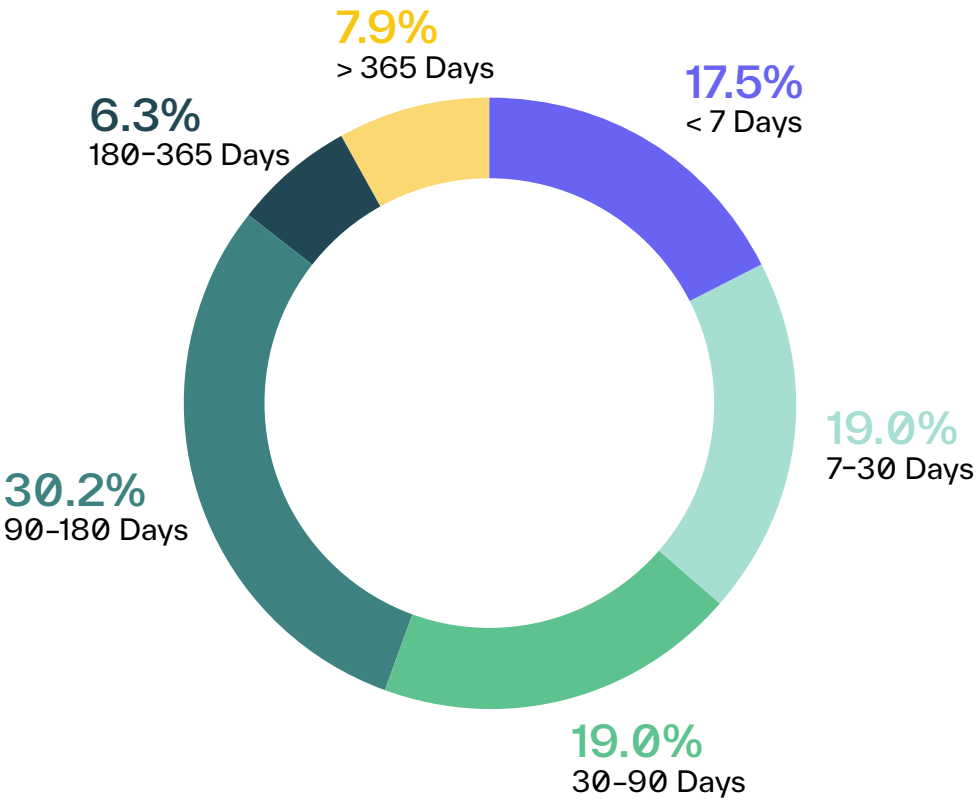
Abnormal™

Repeat Victims

Of the nearly 4,200 victims we identified over two years, 67 of them fell within an unfortunate category—repeat victims of ransomware attacks. After falling victim to a ransomware attack from one group, these companies were later targeted in another attack by a different group. Two companies in our data set were victimized by three different groups. And one company, a manufacturing business based in the United States, had the unlucky honor of being a four-time target of different ransomware groups between June 2020 and September 2021.

While a few of these repeat victims were linked to rebranded ransomware groups, such as Maze/Egregor or Astro Locker/Mount Locker, a vast majority of these victims were targeted by two completely different groups. The median time between repeat victims being announced on the blogs of different ransomware groups was 110 days. Half of these victims were re-targeted within three months and one year of their initial attack.

Days Between First and Second Attacks for Repeat Ransomware Victims



Who's Behind the Attacks? A Look at Ransomware Groups

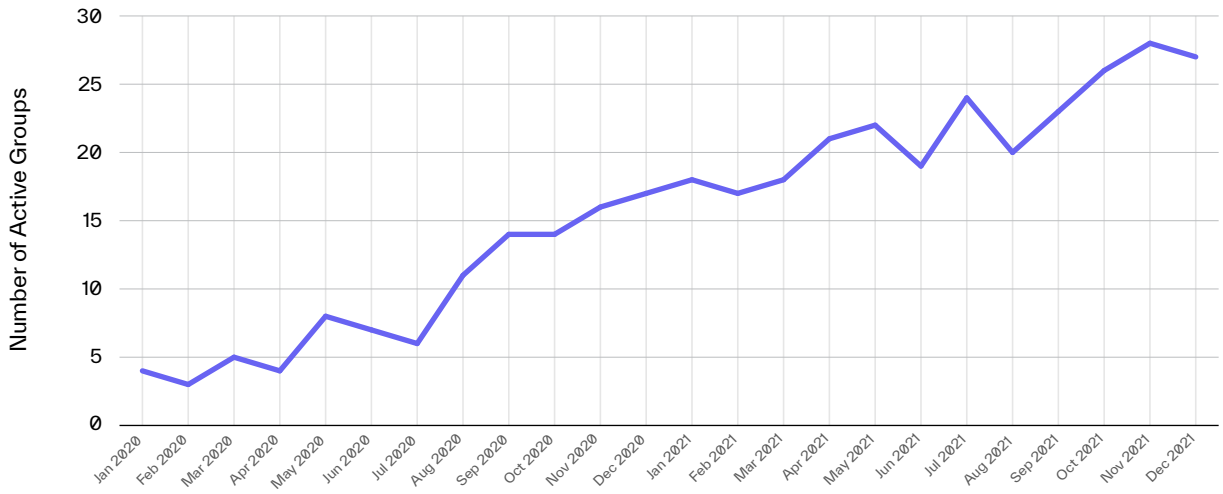
As the number of victims has increased over the last two years, the number of players in the ransomware space has also grown substantially. Similar to what we saw in 2016, when ransomware saw its initial global explosion, a growing number of minor threat groups have entered the scene—piggybacking on the success of the more established groups.

Abnormal™

A Centralized Ecosystem

We tracked 62 different ransomware groups and their activities since January 2020. While some of these were merely rebranded variations of previous ransomware strains, such as Maze rebranding to Egregor or DarkSide renaming itself BlackMatter, most of these groups are unique threats that have emerged for a few months at a time in smaller volumes. The number of active ransomware groups each month has increased dramatically, growing from just three in February 2020 to a peak of 28 in November 2021.

Monthly Active Ransomware Groups

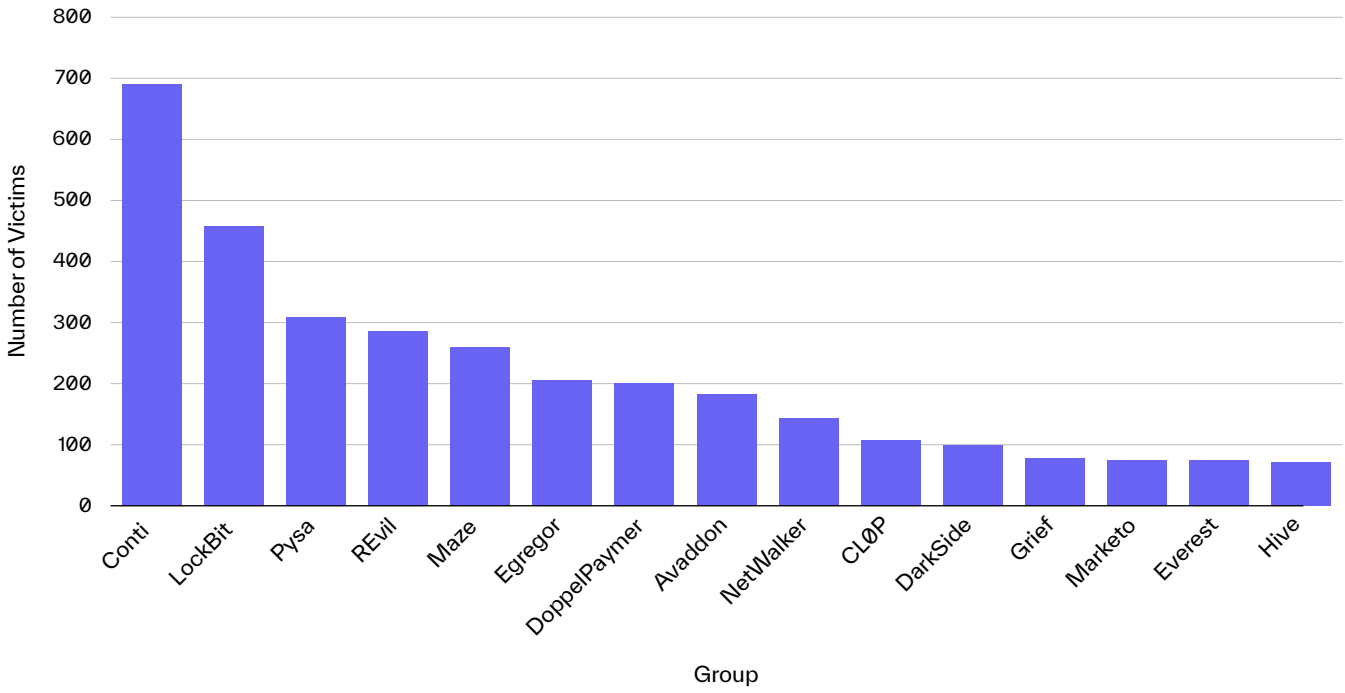


Five groups—Conti, LockBit, Pysa, REvil, and Maze/Egregor—were responsible for more than half of all ransomware attacks over the past two years. Three of those groups (Conti, LockBit, and Pysa) are still active today and they make up nearly two-thirds of the present ransomware attack volume.

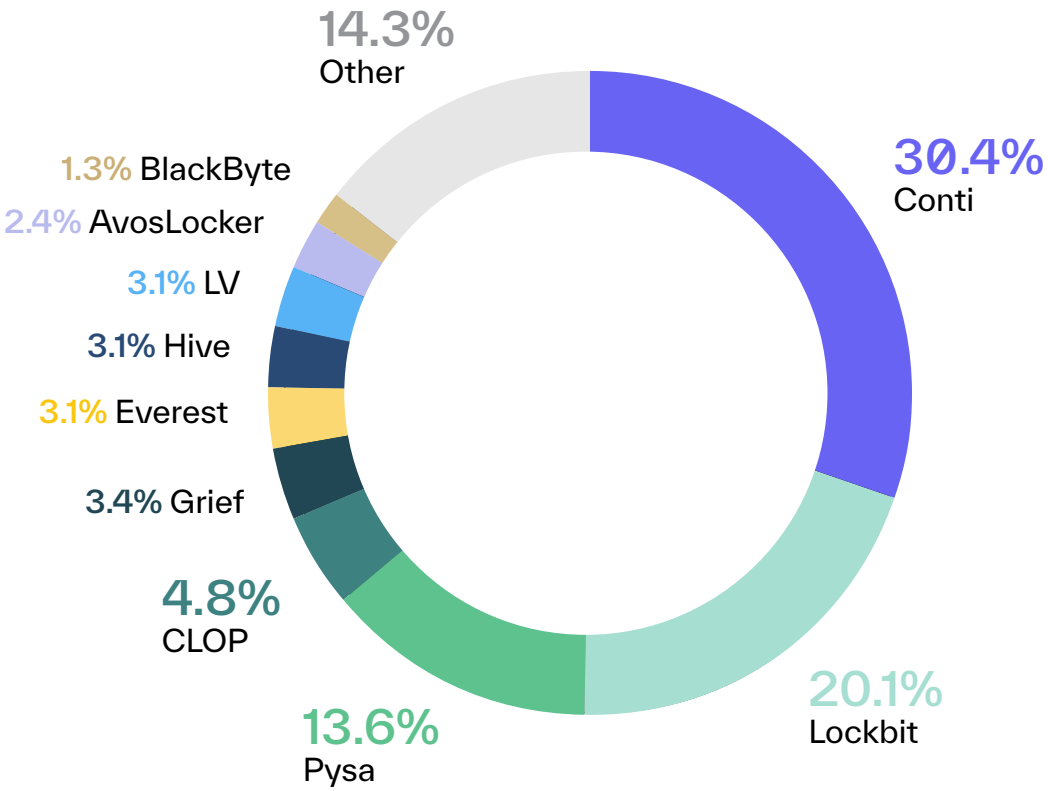
Abnormal™

This demonstrates the centralized nature of the ransomware landscape, where a very small number of RaaS threat groups drive most of the malicious activity. The silver lining to this top-heavy ecosystem is that disruptive actions against one of these primary groups, such as law enforcement takedowns, can have a significant impact on the overall landscape. This is different from a threat like business email compromise, where targeted disruptive actions are generally less impactful to overall attack volume due to the decentralized structure of the threat landscape.

Number of Victims for Top 15 Ransomware Groups



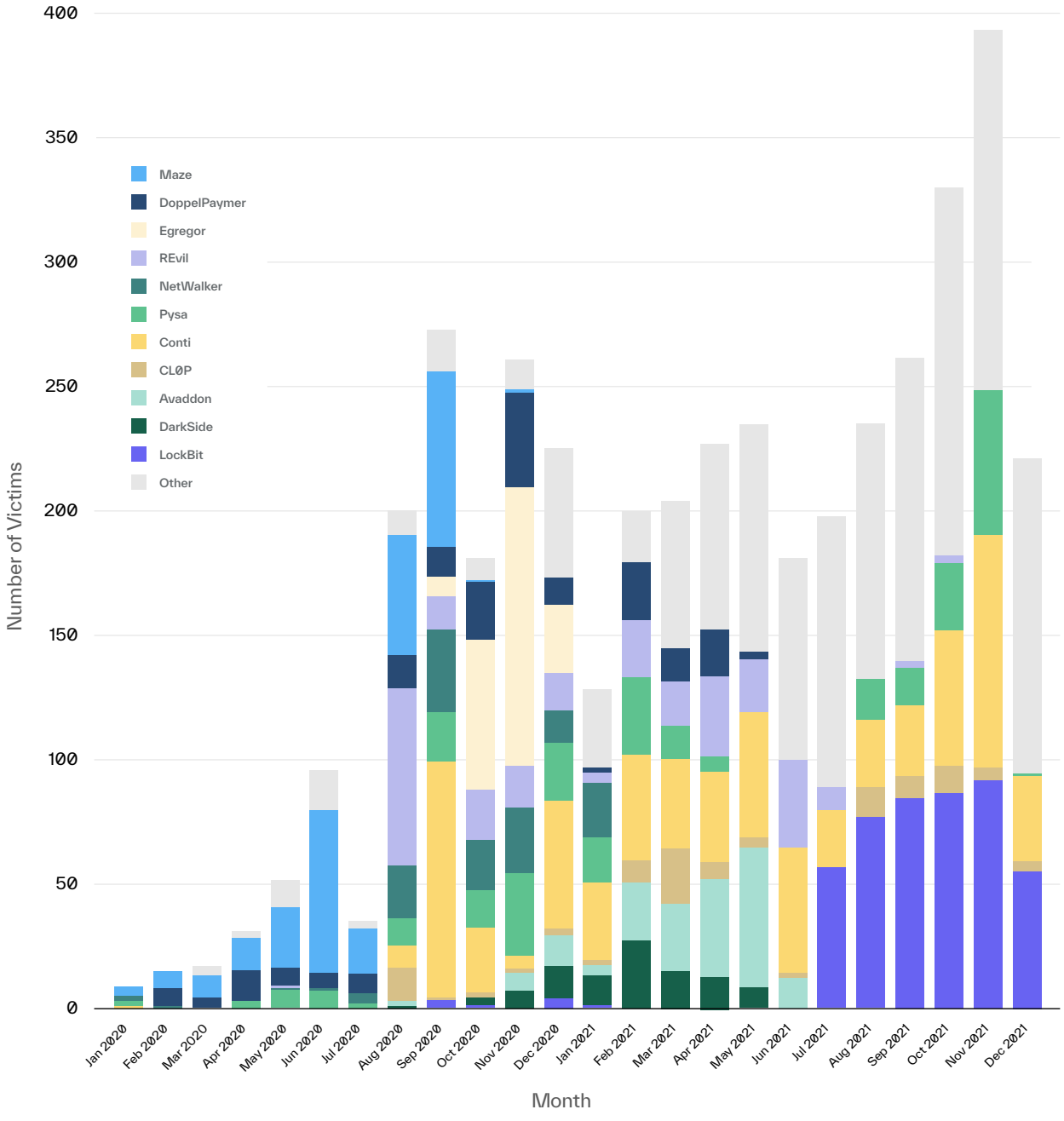
Active Ransomware Group Attack Volume



One of the biggest challenges to disrupting the ransomware landscape in the past few years has been the hydra-like nature of how it has grown. Whenever a primary group has exited the scene, one or more new big groups enter, along with even more smaller groups. For example, when Maze shut down in December 2020, Conti and REvil had both just emerged to fill the void. Similarly, when REvil went offline and Avaddon shut down in the early summer of 2021, LockBit resurfaced with a new version of their malware and became the most prolific ransomware group over the remainder of the year.

So while we've actually seen a fair amount of turnover among the top ransomware groups, the total volume of attacks has remained consistently high. This is because exiting groups are being replaced by new ones, leading to the **overall number of active groups increasing by seven times** since January 2020.

Monthly Distribution of Ransomware Attacks by Group

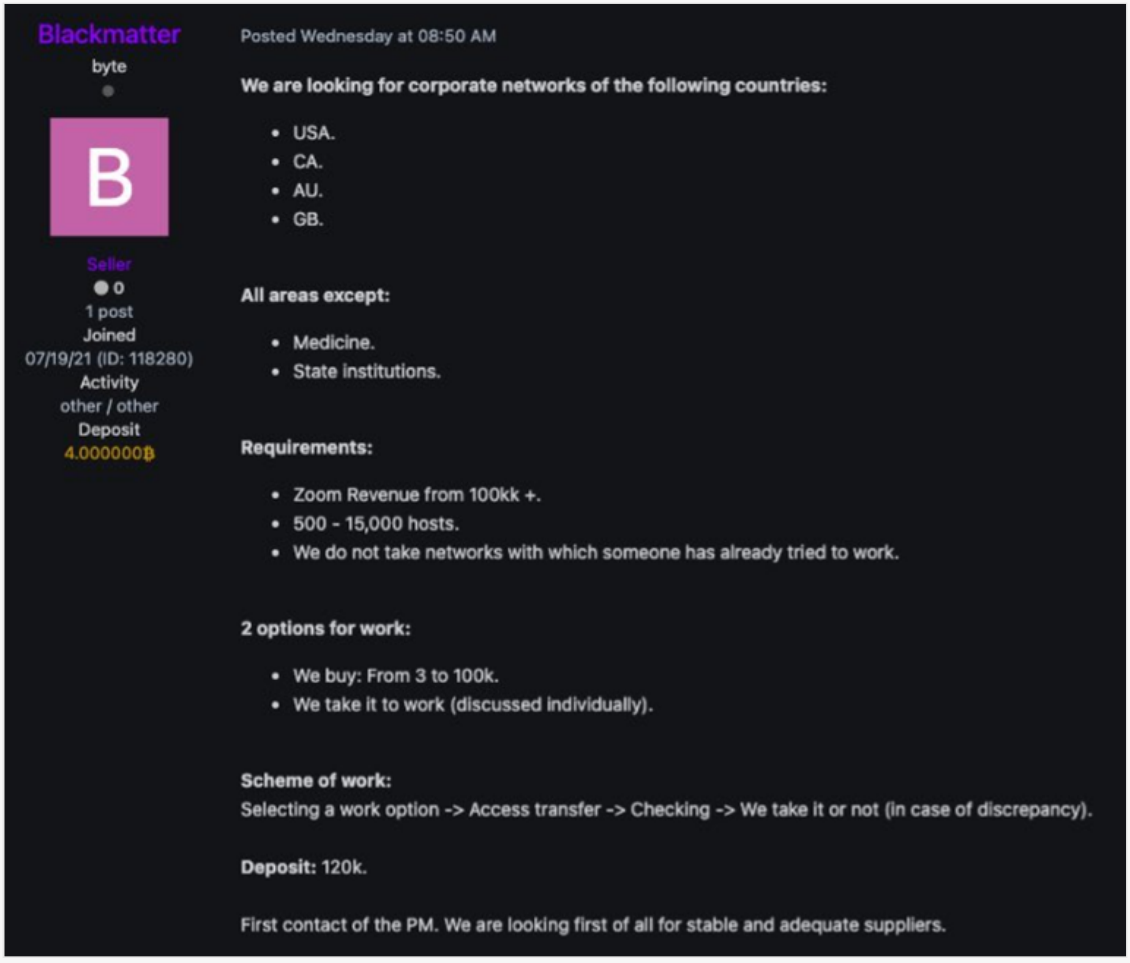


Abnormal™

Indications of Target Profiles by Group

As mentioned earlier in the report, ransomware actors are collectively opportunistic when selecting their targets, preferring to settle for easy victims rather than consciously singling out specific companies to attack. Individually, however, some groups have solicited access to companies that meet certain criteria on underground forums. For example, in July 2021, an actor associated with the BlackMatter ransomware group, the successor to DarkSide, posted on the Exploit forum that the group was looking for access to corporate networks of companies meeting specific location, revenue, and industry specifications.

We can also see evidence of this preferred targeting in our data. Some groups significantly deviate from the overall baseline characteristics of ransomware victims, indicating that while these groups may not be targeting specific companies, they seem to have a preferred target profile.



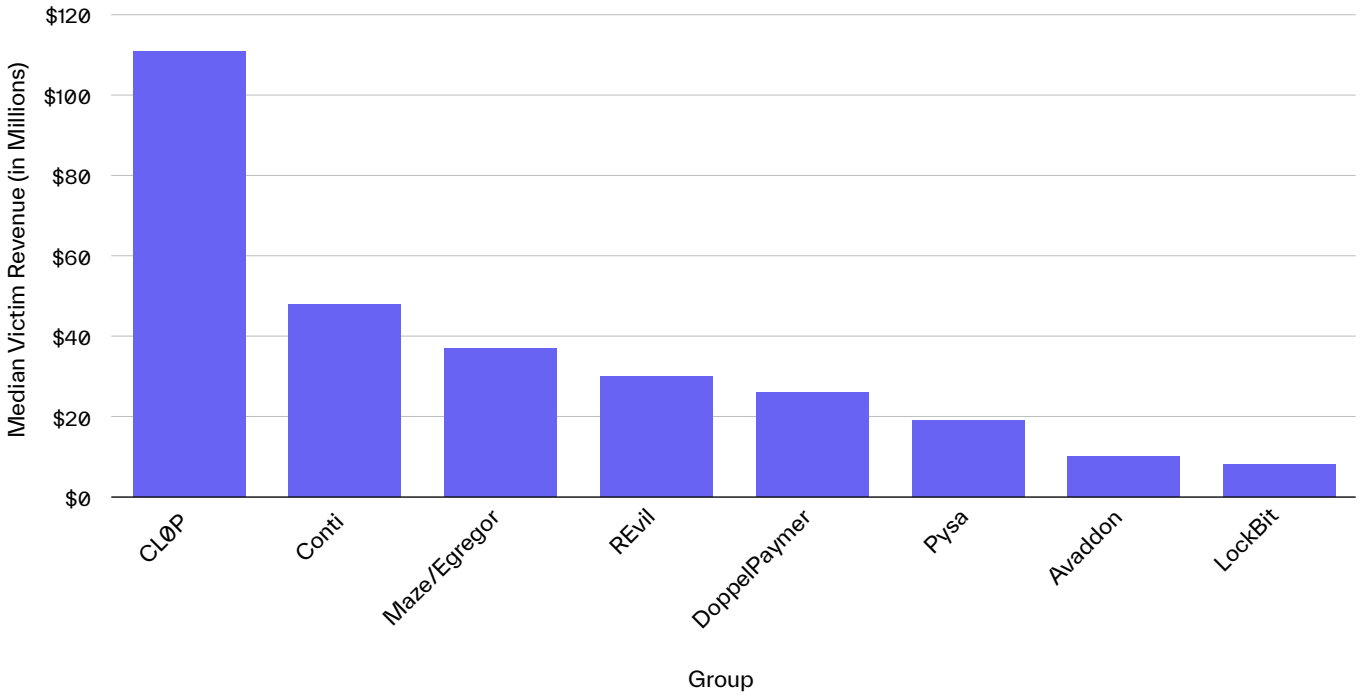
BlackMatter forum post detailing specific target profile.

Threat Groups by Target Revenue

As mentioned above, the median annual revenue for a ransomware victim is $27 million; however, our data shows that a few ransomware groups aim for bigger targets than others. The group that is most prevalently involved in big game hunting is CL0P, whose victims had a median annual revenue of $111 million—more than four times higher than the average. Although not as drastic, the median revenue for victims of Conti ransomware attacks was almost two times higher than average at $48 million.

On the other end of the spectrum, a few groups seem to prefer smaller prey. Avaddon's victims had a median annual revenue of $10 million, while the revenue for LockBit victims was even lower at only $8 million.

Median Victim Revenue of Major Ransomware Groups

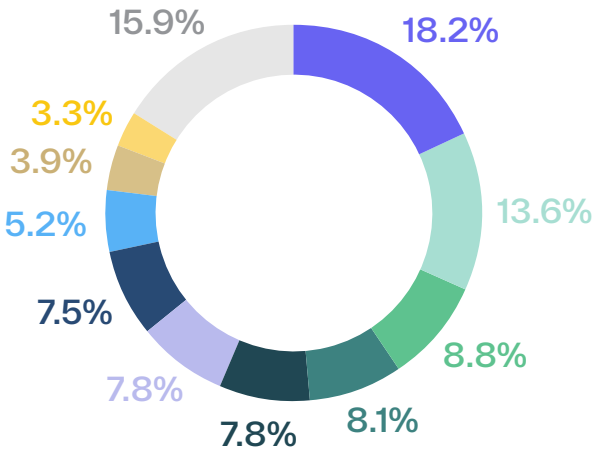


Threat Groups by Target Industry

While most ransomware groups stick to the strategy of being industry-agnostic, a few groups have shown a propensity for targeting some particular industries more than others. Across all ransomware attacks in 2020 and 2021, education and healthcare organizations comprised only a combined 11% of targets, but Pysa, one of the most prolific ransomware groups over the past two years, attacked these industries at a much higher rate. A third of Pysa's ransomware attacks targeted victims in one of these two key sectors.

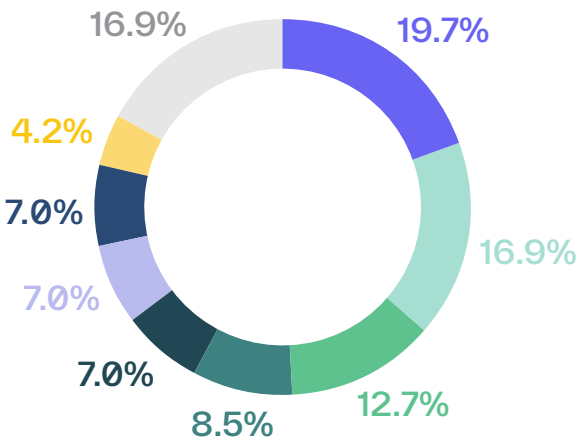
Similarly, while firms in the legal services industry only comprise 5% of all ransomware victims, the sector is the favorite target of the Everest ransomware group, with one in five of their attacks focusing on law firms.

Industry Distribution of Pysa Ransomware Victims



- Education
- Healthcare
- Retail & Wholesale
- Manufacturing
- Construction
- Business Services
- Government
- Transportation
- Energy & Natural Resources
- Finance
- Other

Industry Distribution of Everest Ransomware Victims



- Legal Services
- Construction
- Manufacturing
- Government
- Real Estate
- Finance
- Retail & Wholesale
- Transportation
- Other

Abnormal™

Threat Groups by Target Location

While most ransomware victims over the last two years have been located in North America or Western Europe, some groups have made these two regions their almost exclusive hunting grounds. Nearly all of Conti's almost 700 targets (94%) were located in one of these two regions. Similarly, Grief ransomware and its predecessor DoppelPaymer both almost exclusively targeted North American and Western European companies, with 92% of their victims in those areas.

Other groups have focused their efforts on other parts of the world. Ragnarok, which was active between December 2020 and August 2021, was the only group we observed where a majority (61%) of their targets were based in Europe. In fact, none of Ragnarok's corporate victims in 2021 were located in North America—a definite outlier in the ransomware world.

Prometheus, which was active between March 2021 and July 2021 before rebranding as Spook, was the only group where a plurality (37%) of their targets were located in South America. And while companies in the Asia-Pacific region are generally lower down on a ransomware group's list of targets, two groups—LV and LockBit—targeted organizations in the region at a significantly higher rate. In fact, 20% of LV's victims and 15% of LockBit's victims were located in the APAC region, compared to just 8% across all ransomware groups.

What's Next? The Future of Ransomware

So where do we go from here? Due to a number of disruptive ransomware attacks on high-profile targets in 2021, governments around the world have taken notice and started developing new strategies to attempt to hamper the effectiveness of these threats. For example, in September 2021, the US government placed sanctions on Suex, a Russia-based virtual currency exchange commonly used by ransomware actors to receive illicit payments. In November 2021, new cryptocurrency reporting requirements were included in the Infrastructure Investment and Jobs Act. Additionally, in October 2021, a global summit consisting of representatives from 30 different countries was held to discuss ways to combat ransomware on an international level.

So what happens if cryptocurrency is no longer a viable option for ransomware payments due to enhanced regulations? How would that impact the overall ransomware threat landscape? Because cybercriminals are financially-motivated, it's almost certain that ransomware actors would adapt their tactics and pivot to a different money-making scheme. Based on the current cyber threat landscape, it would make perfect sense that some of these actors could move to business email compromise, which already causes the most financial losses each year.

We've seen more sophisticated actors based in Eastern Europe and Russia move into the business email compromise space, and it's not a secret that the financial impact of BEC attacks has grown exponentially in recent years. Additionally, the primary methods ransomware actors use to gain access to corporate networks could easily be adapted to focus on email access rather than network access, which has the potential to lead to devastating vendor email compromise (VEC) attacks.

In the near future, we could end up with a new threat that combines the scale and sophistication of ransomware with the effectiveness and financial impact of business email compromise, which would be an incredibly difficult challenge to defend against. Regardless of what happens, it's clear that ransomware is here for the foreseeable future, and organizations worldwide should take measures to protect themselves not only from ransomware, but from all cyber attacks that can come from email.

Conclusion

As our research has shown, ransomware continues to be a significant threat vector across all industries, all company sizes, and all countries. Ransomware actors have proven that they are focused on one thing: making money in whatever way possible.

Malware delivered via email continues to be the initial foothold for ransomware and once this first payload has been delivered, threat actors can deploy additional malware to gain access to the company network. From there, they can encrypt information and hold it for ransom using a final ransomware payload. With the largest payout ever costing CNA Financial $40 million in March 2021, it is clear that ransomware is a threat against which every organization should protect itself. Now is the time to secure your environment and protect your end users from these malicious emails—before the next ransomware attack impacts you.

Interested in Stopping Ransomware?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@AbnormalSec

To learn more about how ransomware is impacting your industry, email us at ransomware@abnormalsecurity.com.

Abnormal™

Abnormal

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com