Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues

coveware.com/blog/q3-2020-ransomware-marketplace-report

November 4, 2020

Table of Contents

Average Ransom Payment

Types of Ransomware

Data Exfiltration

Attack Vectors

Companies Targeted

Costs of Attacks

The Coveware Quarterly Ransomware Report describes ransomware incident response trends during Q3 of 2020. Ransomware groups continue to leverage data exfiltration as a tactic, though trust that stolen data will be deleted is eroding as defaults become more frequent when exfiltrated data is made public despite the victim paying. In Q3, Coveware saw the Maze group sunset their operations as the active affiliates migrated to Egregor (a fork of Maze). We also saw the return of the original Ryuk group, which has been dormant since the end of Q1.

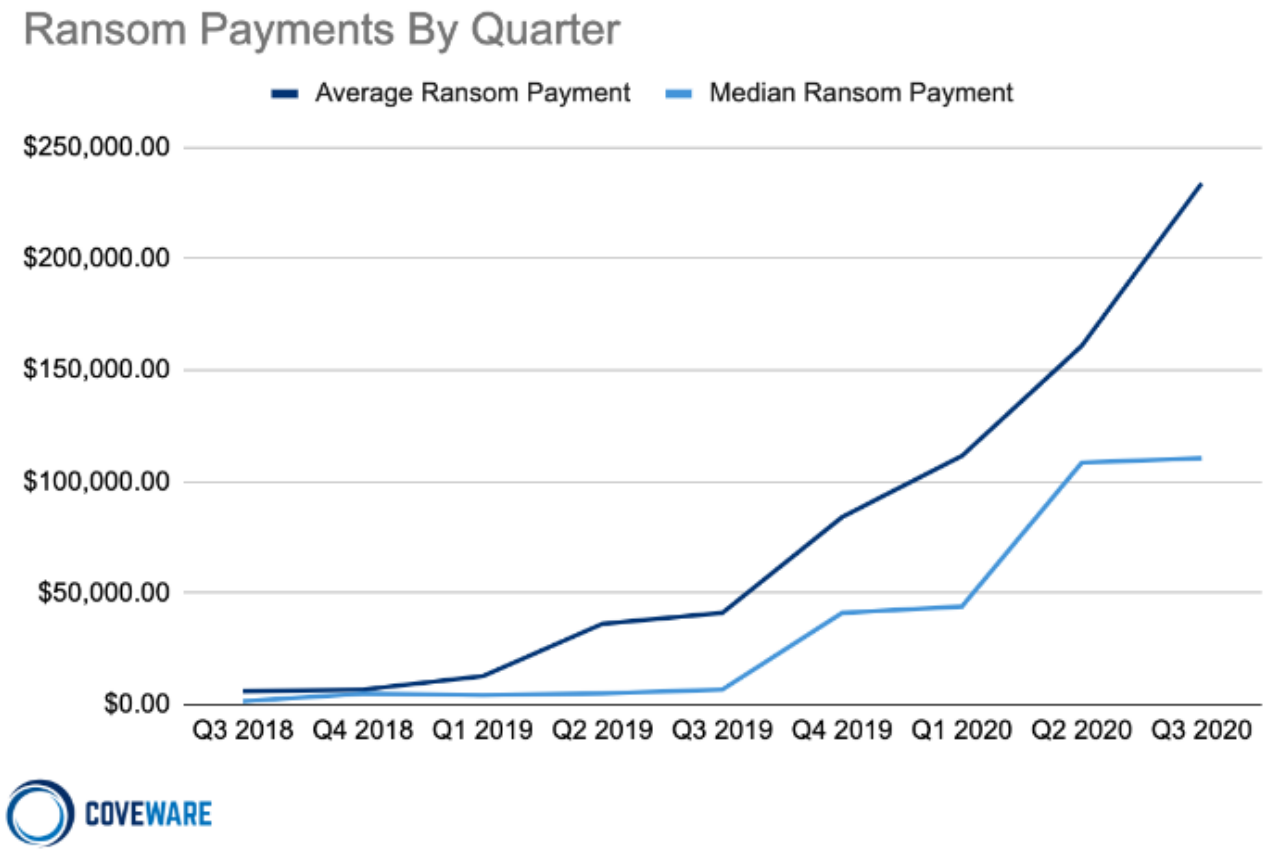
Average Ransomware Increases as Attackers Target Bigger Companies

Average Ransom Payment

$233,817
+31% from Q2 2020

Median Ransom Payment

$110,532
+2% from Q2 2020



Average and Median Ransom Payments

The average ransom payment increased to $233,817 in Q3 of 2020, up 31% from Q2. The median payment in Q3 rose slightly from $108,597 to $110,532, reflecting how large, big game payments continue to drag the averages up. The disequilibrium within the cyber extortion industry was evident when attackers discovered that the same tactics, techniques, and procedures (TTPs) that work on a 500 person company can work on a 50,000 person company and the potential payoff is substantially higher. The dramatic increase in ransom amounts may imply a higher degree of sophistication as attackers go upmarket, but Coveware does not believe that the attacks are more sophisticated.

The biggest change over the past 6 quarters is threat actors now realize that their tactics scale to much larger enterprises without much of an increase in their own operating costs. The profit margins are extremely high and the risk is low. This problem will continue to get worse until pressure is applied to the unit economics of this illicit industry. It is also possible that the influx of remote and work-from-home setups using RDP and other remote technologies allowed threat actors to leverage attack vectors that previously didn't exist.

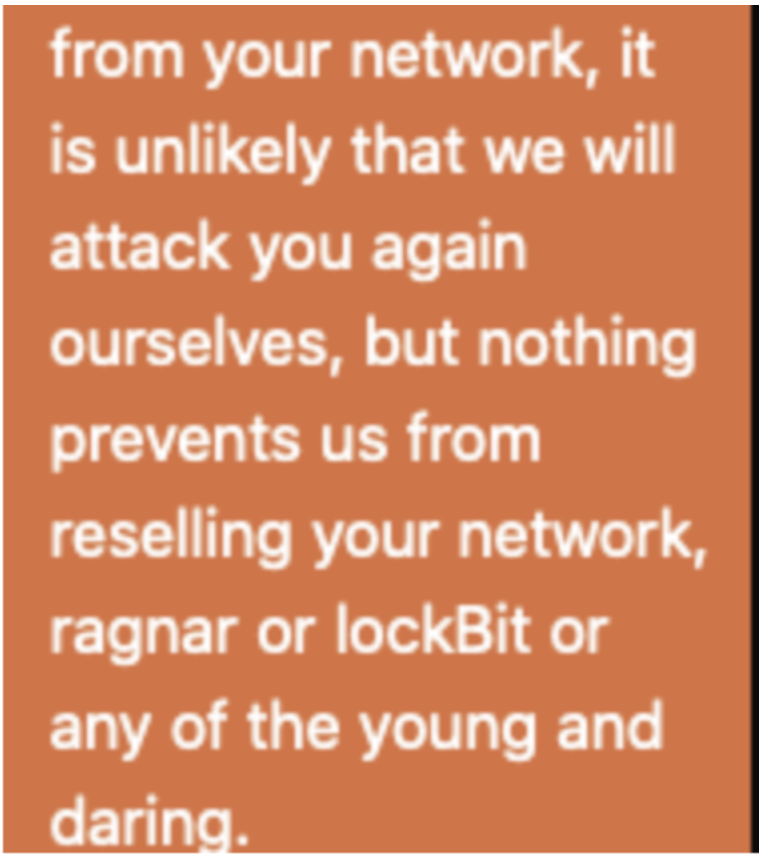
DopplePaymer, Conti, Wasted, Nephilim and Avvadon make it to the Top 10, Egregor inherits Maze

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
1	Sodinokibi	16.2%	-
2	Maze	13.6%	-
3	Netwalker	9.9%	+1
4	Phobos	5.0%	-2
5	DopplePaymer	4.3%	New in Top 10
6	Snatch	4.0%	+2
6	Conti	4.0%	New in Top 10
8	Lockbit	3.6%	+1
9	Dharma	2.3%	-4
10	Nephilim	2.0%	New in Top 10
10	Avaddon	2.0%	New in Top 10

Top 10: Market Share of the Ransomware attacks

The third quarter marked both the peak and the end of Maze ransomware. Based on our tracking of Maze activity, their last enterprise attacks occurred in late September, and they have since announced they are sunsetting. Since then, less senior affiliates, the 'young and daring', have likely forked the Maze ransomware code into the Sekhmet and Egregor ransomware variants. Judging by their prolific rise and similar tactics, Egregor seems to be the heir apparent.



Screenshot of a message from Maze about sharing victim data with other groups

Half of the Ransomware Cases use Data Exfiltration as a Tactic - Exfiltrated Data Cases Doubled in Q3 2020

Almost 50% of ransomware cases included the threat to release exfiltrated data along with encrypted data. The threat to release exfiltrated data was used as a monetization conversion kicker. Previously, when a victim of ransomware had adequate backups, they would just restore and go on with life; there was zero reason to even engage with the threat actor. Now, when a threat actor steals data, a company with perfectly restorable backups is often compelled to at least engage with the threat actor to determine what data was taken.

Paying a Ransom may not stop Ransomware Groups from Leaking the Exfiltrated Data

Coveware feels that we have reached a tipping point with the data exfiltration tactic. Despite some companies opting to pay threat actors to not release exfiltrated data, Coveware has seen a fraying of promises of the cybercriminals (if that is a thing) to delete the data. The below list includes ransomware groups whom we have observed publicly DOX victims after payment, or have demanded a second extortion payment from a company that had previously paid to have the data deleted / no leaked:

Sodinokibi: Victims that paid were re-extorted weeks later with threats to post the same data set.

- **Maze / Sekhmet / Egregor** (related groups): Data posted on a leak site accidentally or willfully before the client understood there was data taken.
- **Netwalker**: Data posted of companies that had paid for it not to be leaked
- **Mespinoza**: Data posted of companies that had paid for it not to be leaked
- **Conti**: Fake files are shown as proof of deletion

Although victims may decide there are valid reasons to pay to prevent the public sharing of stolen data, Coveware's policy is to advise victims of data exfiltration extortion to expect the following if they opt to pay:

The data will not be credibly deleted. Victims should assume it will be traded to other threat actors, sold, or held for a second/future extortion attempt

- Stolen data custody was held by multiple parties and not secured. Even if the threat actor deletes a volume of data following a payment, other parties that had access to it may have made copies so that they can extort the victim in the future
- The data may get posted anyway by mistake or on purpose before a victim can even respond to an extortion attempt

Unlike negotiating for a decryption key, negotiating for the suppression of stolen data has no finite end. Once a victim receives a decryption key, it can't be taken away and does not degrade with time. With stolen data, a threat actor can return for a second payment at any point in the future. The track records are too short and evidence that defaults are selectively occurring is already collecting. Accordingly, we strongly advise all victims of data exfiltration to take the hard, but responsible steps. Those include getting the advice of competent privacy attorneys, performing an investigation into what data was taken, and performing the necessary notifications that result from that investigation and counsel. Paying a threat actor does not discharge any of the above, and given the outcomes that we have recently seen, paying a threat actor not to leak stolen data provides almost no benefit to the victim. There may be other reasons to consider, such as brand damage or longer term liability, and all considerations should be made before a strategy is set.

How different Ransomware Groups Leak Stolen Data

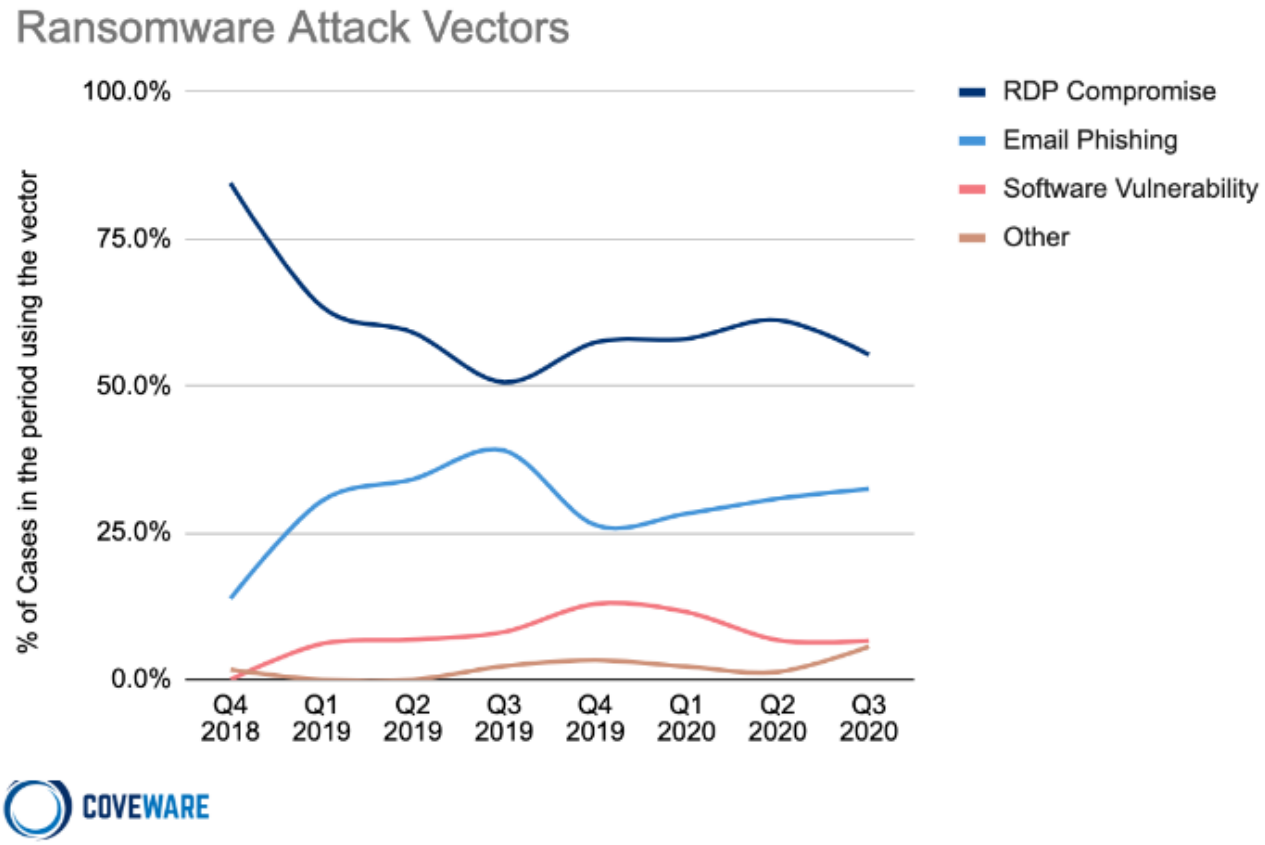
One interesting comparison between variants of ransomware that rely upon data exfiltration as an extortion tactic is a velocity with which these variants doxxed their victims. Maze was the first ransomware to use a public leak site to release the data of victims that didn't pay a ransom. As the below table reveals, it took Maze approximately 6 months to post the data of

its first 50 victims. Similar timelines were observed for Sodinokibi and DoppelPaymer. For comparison, it took Egregor ***3 weeks*** to post the same number of victims. The only other variant that seems to match Egregor's pace is Conti. Given the lead time necessary to gain a foothold within a vulnerable company, complete data exfiltration, and allow the extortion process to play out before a leak would occur, the rapid velocity at which Egregor reached this milestone is puzzling. Even though Egregor seems stocked with prior Maze affiliates that were clearly well organized when the variant was released, the volume of doxxed victims seems artificially high.

Ransomware Variant	Time to 'Doxx' 50 victims
Maze	6 Months
DoppelPaymer	6 Months
Sodinokibi	6 Months
Netwalker	3 Months
Conti	6 Weeks
Egregor	3 Weeks

Approximate Timelines By Variant From Start of Doxxing Behavior To Posting 50th Victim

Ransomware Attacks by Methods, Victims size, and Complexity

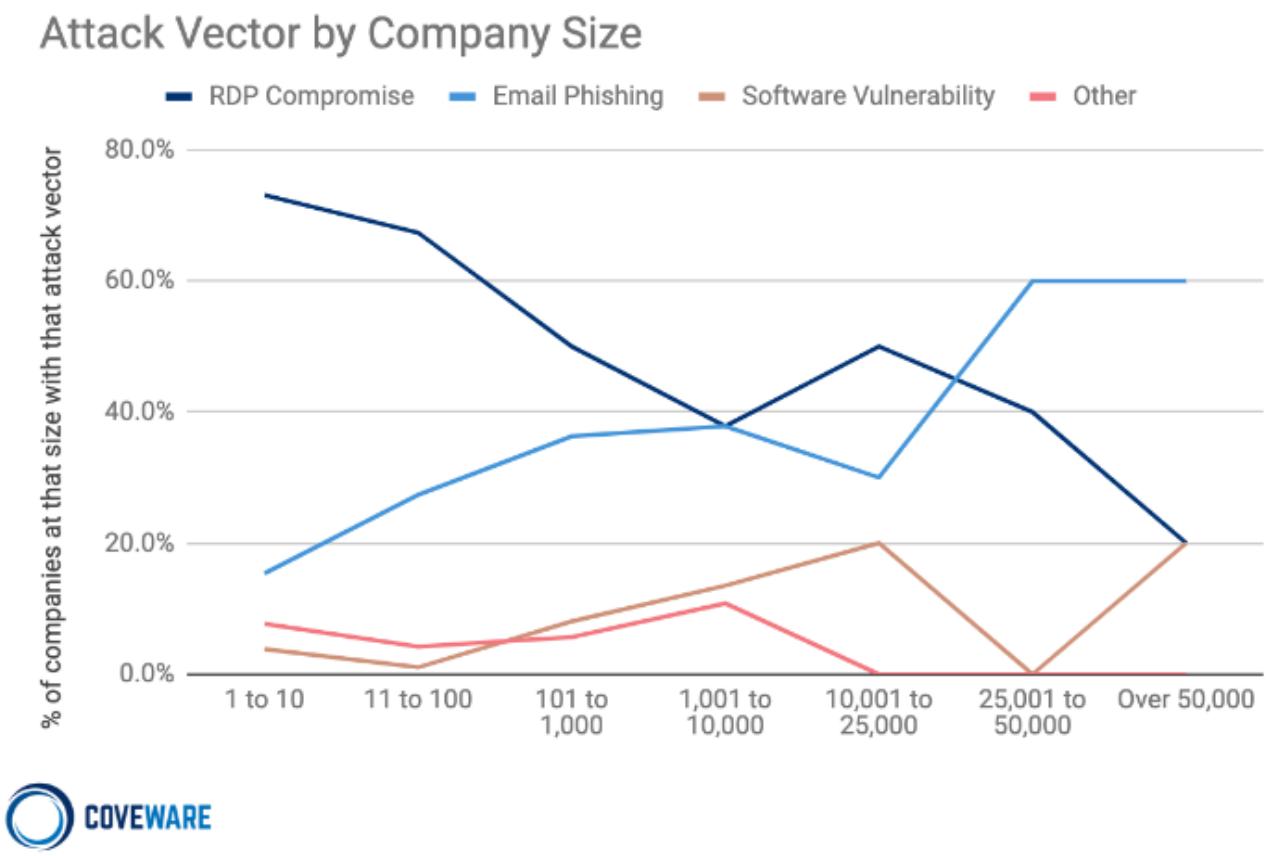


Ransomware attack vectors: RDP compromise, email phishing, software vulnerability, and others.

Ransomware Attack Vectors - RDP continues to top all attacks

The repetitive exploitation of improperly secured Remote Desktop Protocol (RDP) is the gift that keeps on giving for the cyber extortion economy. The supply of already compromised RDP credentials is so large, that the price is actually decreasing. This is a very worrisome sign as it signals that supply is outstripping demand. A larger supply of RDP credentials is the feedstock that draws DOWN the barriers to entry for progressively less technically sophisticated cybercriminals to begin distributing ransomware. Until companies properly heed the risk of an improperly secured RDP connection, this attack vector will continue to be the most cost-effective target for ransomware threat actors to exploit.

Ransomware Attack Vectors vary by the Size of the Victim

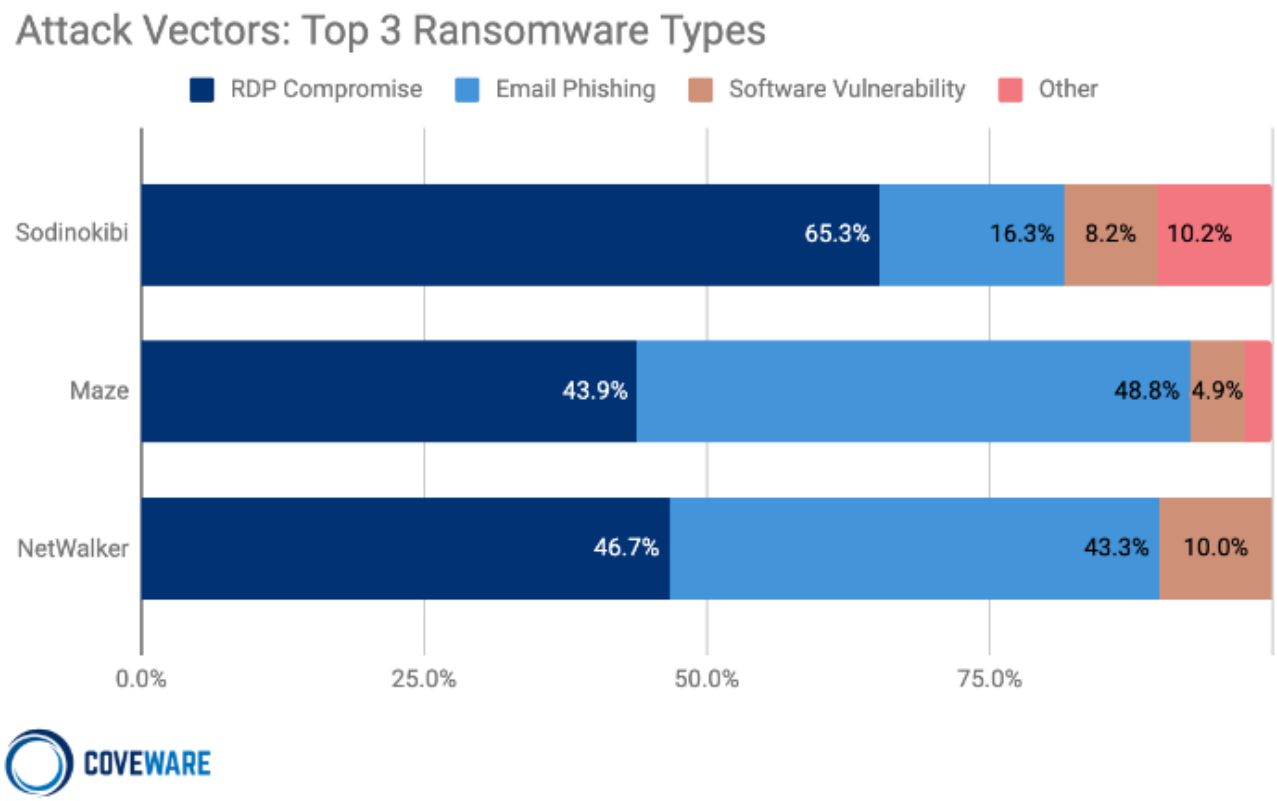


Ransomware Attack Vectors vary by the Size of the Victim Q3 2020

The path to carry out a ransomware attack against a given company is driven by the unit economics of the attack. Small companies are not capable of paying millions of dollars in ransom. Accordingly, attacking small companies has to be fast and cheap in order for it to be profitable for the criminal. Luckily for the threat actors, improperly secured RDP ports, and their associated compromised credentials can be purchased for less than $50 and are plentiful. As the size of an organization grows, the method of ingress shifts to the next cheapest and most plentiful attack vector. This tends to be either email phishing or unpatched vulnerabilities. Regardless, the end goal is always the same for the threat actor.

The foothold created by the phishing email or CVE exploit is used to escalate privileges until the attacker can command a domain controller with senior administrative privileges. Once that occurs, the company is fully compromised and data exfiltration + ransomware are likely to transpire within hours or days. We can see from the charts that use of RDP trails off with larger companies as they are typically wise enough to secure it. Defending against ransomware that begins with email phishing or a CVE requires more nuanced and in-depth defense.

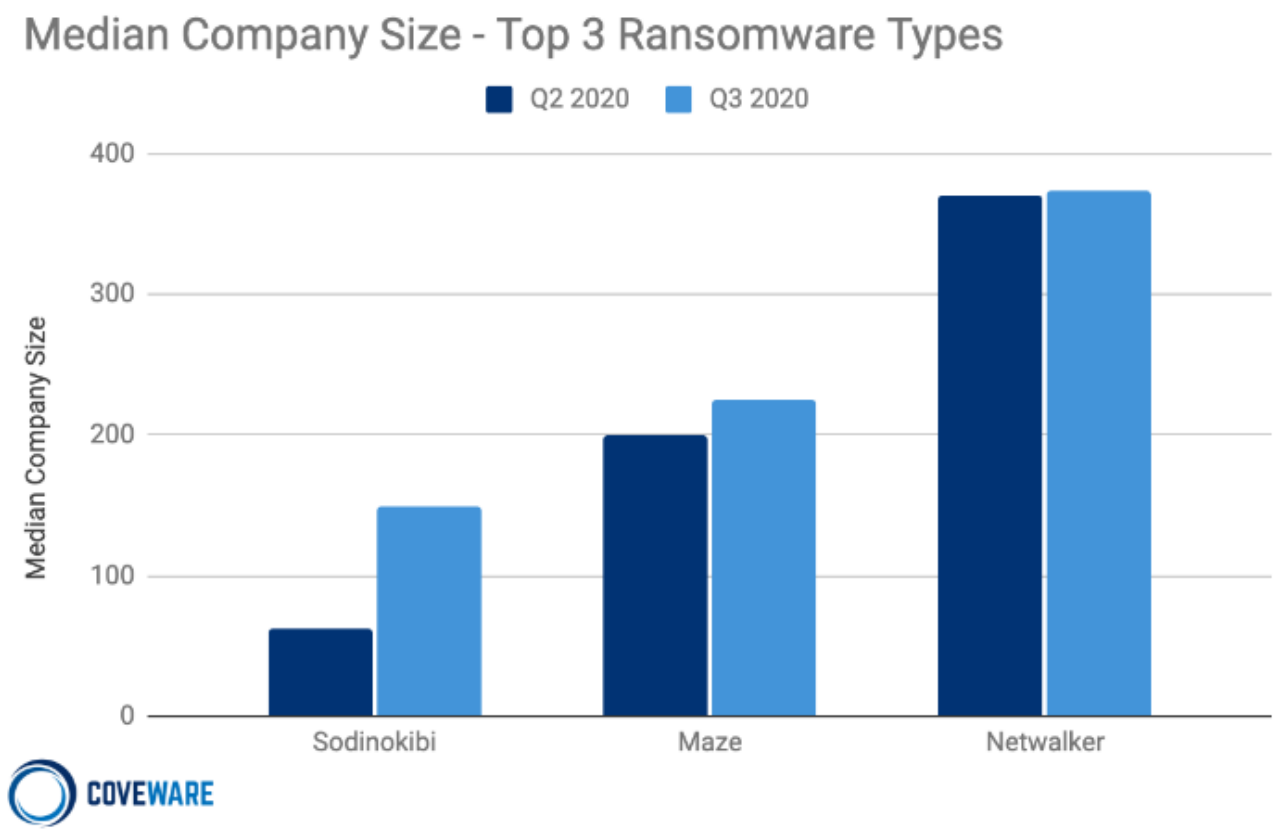
The Most Prevalent Types of Ransomware use Reliable and Economical Attack Vectors]



Top 3 Ransomware Types: Sodinokibi, Maze, and NetWalker.

The distribution of attack vectors by variant demonstrates how economics rule the attack pattern choices of ransomware distributors. There is no reason to use an expensive zero-day exploit or similar software vulnerability when RDP credentials are so cheap and reliable. Software vulnerabilities, while used, require comprehensive scanning and reconnaissance. Our sense is that when a CVE is the vector of attack, the ransomware actor themselves was unlikely to be the actual purveyor of the access. Specialists that can harvest network access and have skill sets related to the specific CVE were likely the first attackers in the door. Access was then sold down the supply chain to the ransomware distributors. The same goes for email phishing. The campaigns that install trickbot, bazaarloader, or other RATs (remote access trojans), are typically campaigned by separate threat actor specialists. Once network access is achieved, the access is subsequently sold.

The attack vectors used by Ransomware groups leads them to certain sized victims



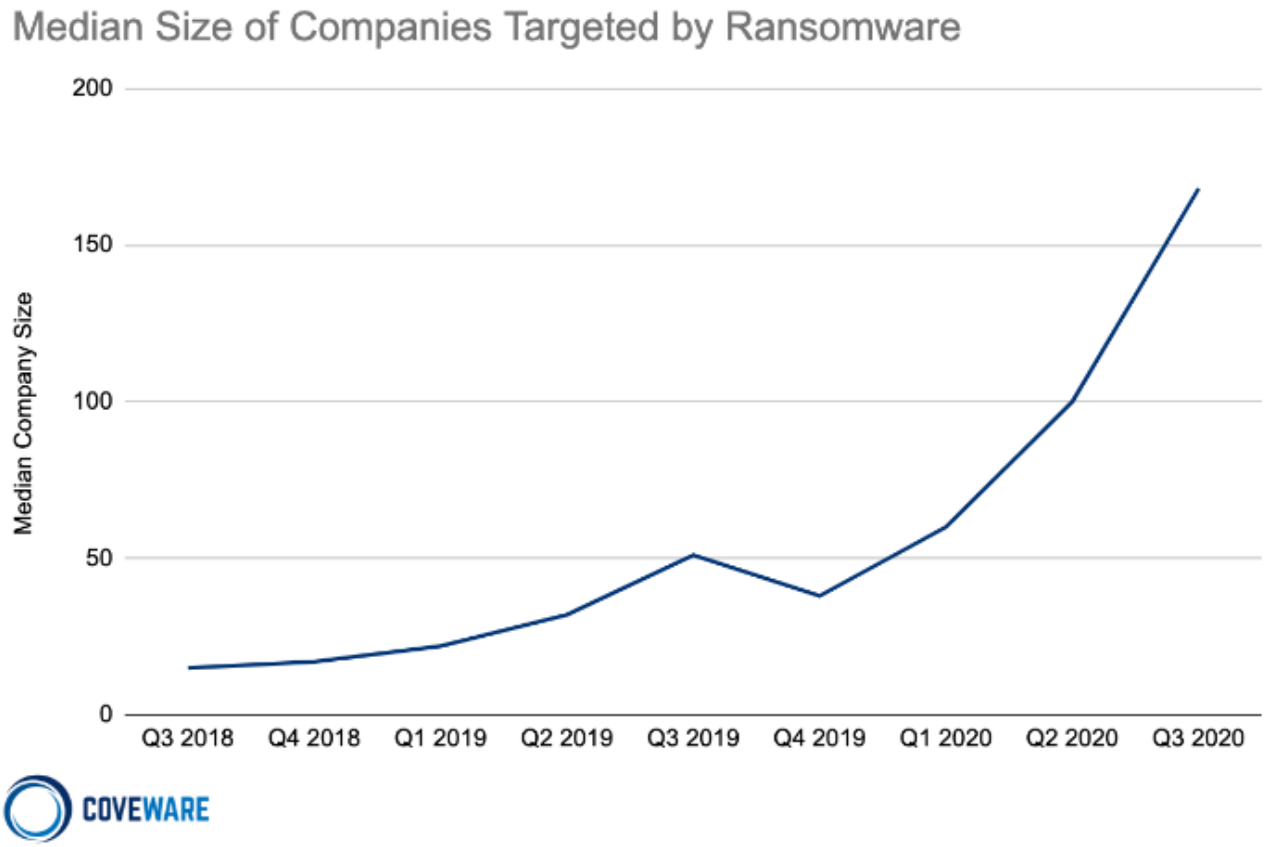
Median company size of the top 3 ransomware types.

The size, as measured by the median number of employees, of a specific variant's targets is indicative of both the vulnerabilities that the threat actors prefer, but also of the size and character of the ransomware operation. Both Maze and Sodinokibi are ransomware-as-a-service (RaaS) models, meaning that there are individual affiliates that campaign and distribute the same variant. These affiliates then rely on the ransomware developer for shared services such as the encryption executable and a cut of the extortion payments. While not as large as more open RaaS platforms like Dharma or Phobos, both Sodinokibi and Maze each have dozens of affiliates that distribute the ransomware. Netwalker is a bit more tightly distributed, with a smaller number of affiliates, who generally target larger organizations.

Ransomware is still a Disproportionate Problem for Small and Medium Sized Businesses

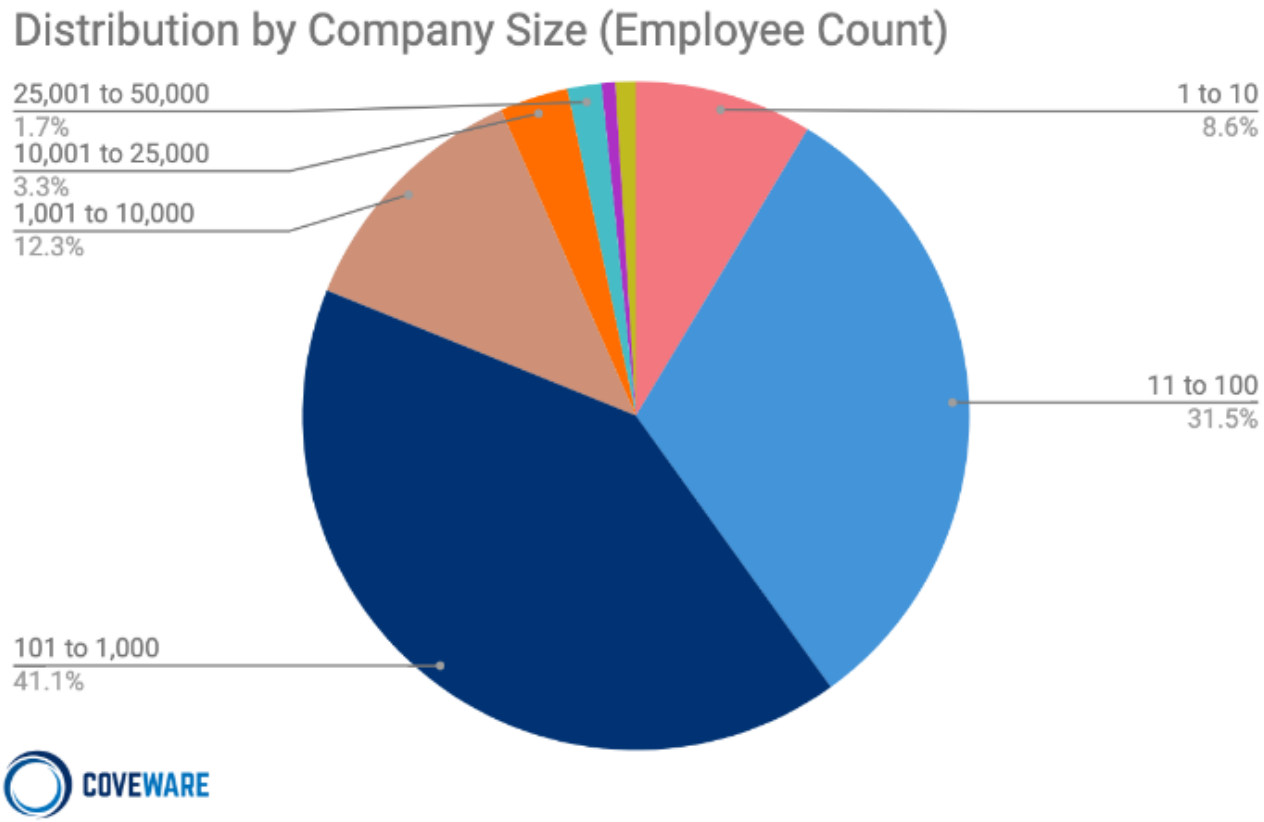
Median # of Employees

168
+68% from Q2 2020

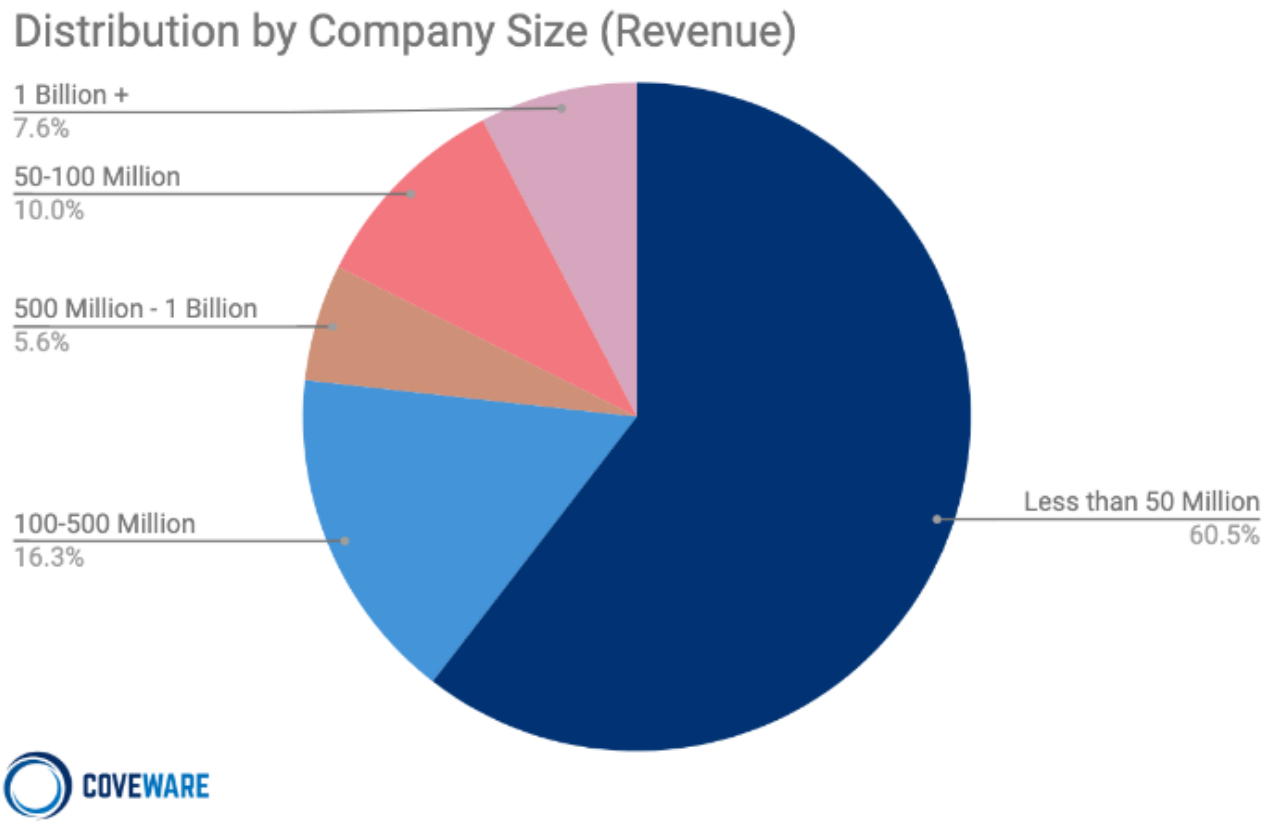


Median Size of Companies Targeted by Ransomware

Despite the headlines, ransomware remains a disproportionate problem for small businesses. Large companies make the headlines but are typically able to recover and restore even if they end up having to pay. Small companies on the other hand are much less likely to have adequate backups or the financial resources to make a full recovery following a ransomware attack.

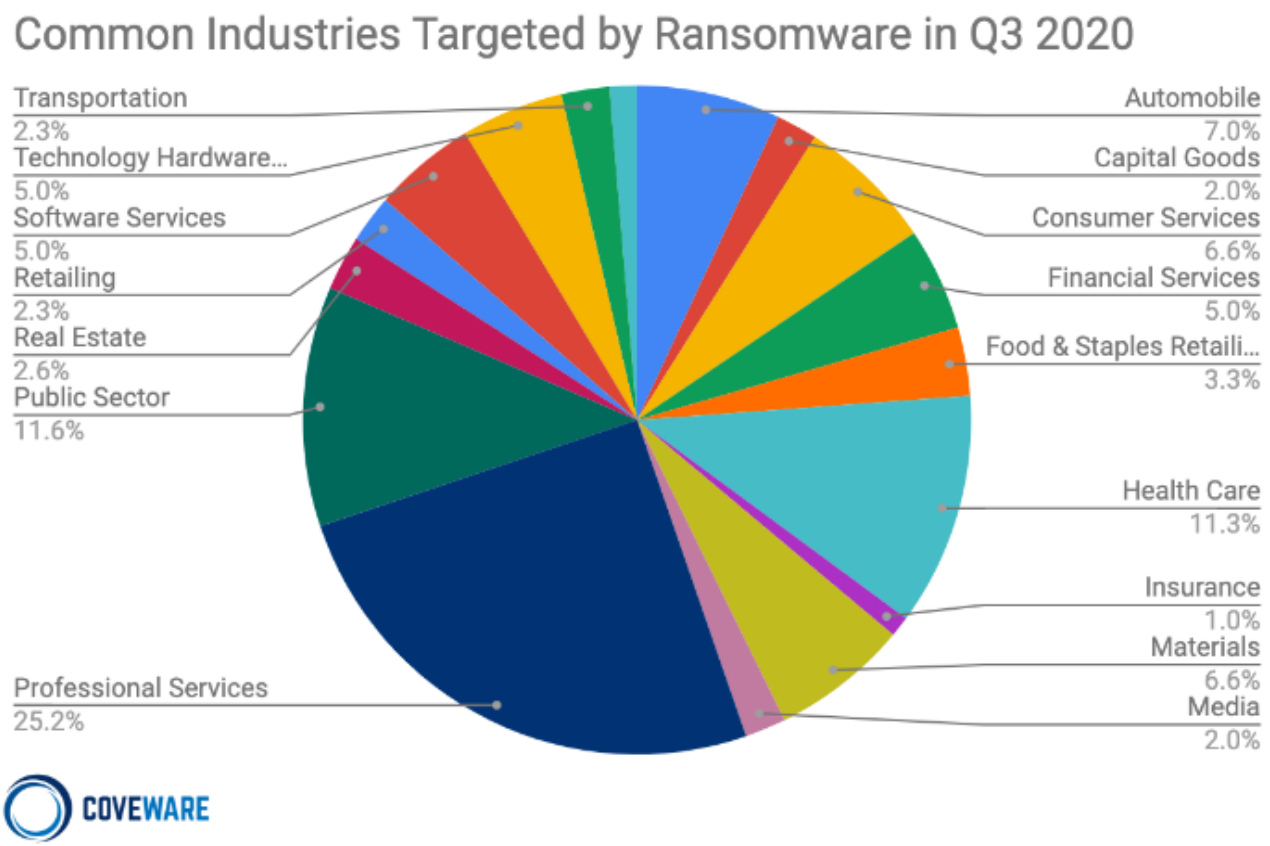


Most victims of a ransomware attack (70%+) have less than 1,000 employees.



Distribution by Company Size in Q3 2020

Most victims of ransomware have less than $50 million dollars in annual revenue. This small-mid market profile demonstrates just how damaging these attacks are to the backbone of the US economy.



Common Industries Targeted by Ransomware in Q3 2020

Certain industries, such as healthcare, may seem to be more heavily targeted than others, because of the sensitive data they hold and their relative intolerance of downtime. However, what we have observed over time is that the presence of cheap-to-exploit vulnerabilities, that happen to be common within a given industry, are what causes an industry concentration to appear. Professional service firms, especially small ones such as law firms and accounting firms are especially vulnerable. According to the Small Business Administration, there are about 4.2 million professional service firms in the US. This industry slice makes up about 14% of all businesses. Yet, from a ransomware attack perspective, professional service firms make up 25% of attacks, or almost double. Why? These firms are more likely to take the threat of ransomware less seriously. They commonly leave vulnerabilities like RDP open to the internet and are victimized much more regularly than companies in other industries. It is critical that small professional services firms recognize that there is no such thing as being 'too small' to be targeted. The cyber-extortion industry does not work like that. If you present a cheap vulnerability to the internet, you WILL get attacked. It is just a question of when, not if.

Downtime from a Ransomware Attack is still the most Dangerous Complication

Average Days of Downtime

19
+19% from Q2 2020

Downtime is still the most dangerous aspect of a ransomware attack, and one of the reasons data exfiltration should not present as much of a challenge to victims as business interruption. In Q3 of 2020, the average firm experienced roughly 19 days of downtime. Downtime can range on a spectrum from having a business be at a total standstill, to being just mildly affected by non-available machines.

Disclaimer