Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands

coveware.com/blog/ransomware-marketplace-report-q4-2020

February 1, 2021

Table of Contents

The Coveware Quarterly Ransomware Report describes ransomware incident response trends during Q4 of 2020. Ransomware groups continue to leverage data exfiltration as a tactic. However, the trust that stolen data will be deleted is eroding; defaults are becoming more frequent when exfiltrated data is made public despite the victim paying. As a result, fewer companies are giving in to cyber extortion when they are able to recover from back ups. This inflection led to a large decline in average ransom amounts paid. Stemming the tide of cyber extortion will only happen if the industry is starved of its profitability. This trend was a distinct positive during Q4.

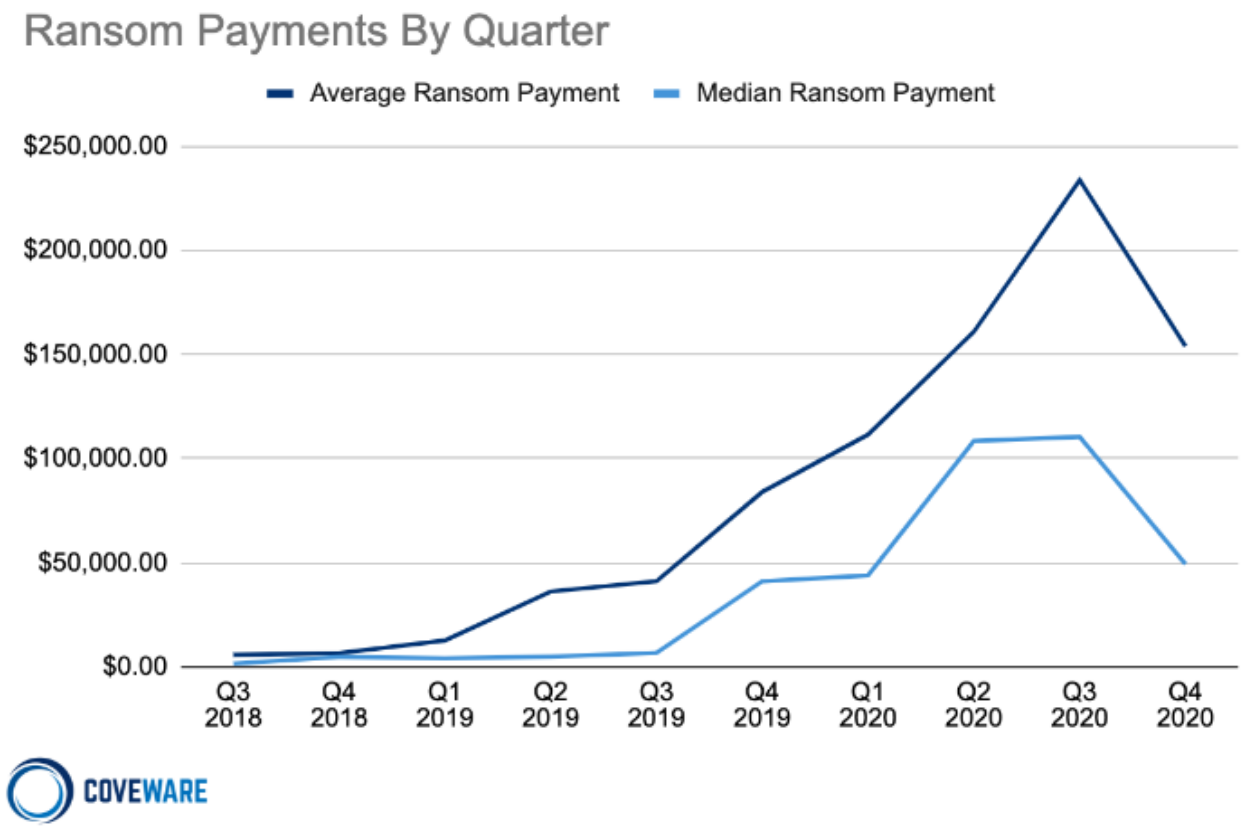
Average Ransom Demand Q4 of 2020

Average Ransom Payment

$154,108
-34% from Q3 2020

Median Ransom Payment

$49,450
-55% from Q3 2020



Average and Median Ransom Payments

The average ransom payment decreased 34% to $154,108 from $233,817 in Q3 of 2020. The median payment in Q4 also decreased to $49,450 from $110,532, a 55% reduction. The dramatic reduction was attributed to more victims of data exfiltration attacks saying "ENOUGH" and choosing not to pay. We noted in our Q3 report that the value of paying criminal extortionists to suppress the release of stolen data has poor risk/reward characteristics. With more companies falling victim, more are having the opportunity to constructively consider the trade offs, and are increasingly choosing not to pay. Attacking the raw economics of the cyber extortion economy from multiple angles is the best way to retract the volume of attacks. When fewer companies pay, regardless of the reason, it causes a long term impact, that compounded over time can make a material difference in the volume of attacks. However, even with this single incremental data point, profit margins remain very high for ransomware actors, and risk of arrest also remains low.

70% of Ransomware Attacks Involved the Threat to Leak Exfiltrated Data (+43% From Q3 2020)

The percentage of ransomware attacks that involved the threat to release stolen data increased from 50% in Q3, to 70% in Q4. Despite this, fewer companies are giving in and paying the extortion demand. In Q3, 74.8% of companies that were threatened with a data leak opted to pay. In Q4, that percentage declined to 59.6%.

The 4th quarter of 2020 marked a turning point with the data exfiltration tactic. Coveware continues to witness signs that stolen data is not deleted or purged after payment. Moreover, we are seeing groups take measures to fabricate data exfiltration in cases where it did not occur. These tricks and tactics put a premium on ensuring that threats are thoroughly validated. While victims of data exfiltration extortion may conclude to pay regardless of the risks, Coveware's position remains unchanged, and we advise all victims of data exfiltration extortion to expect the following if they opt to pay:

> The data may not be credibly destroyed by the threat actor. Victims should assume it might be traded, sold, misplaced, 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 be deliberately or mistakenly published anyway before a victim can even respond to an extortion attempt.
- Complete records of what was taken may not be delivered by the threat actor, even if they explicitly promise to provide such artifacts after payment.

Hasty Threat Actors Are Wiping Data

A concerning trend Coveware will be monitoring in Q1 2021 is the increase in the incidence of irreversible data destruction as opposed to just targeted destruction of backups or encryption of critical systems. In Q4, Coveware received multiple reports from victims that entire clusters of servers and data shares had been permanently wiped out, with no recourse for retrieving the data even with the purchase of the decryption key. Ransomware actors are typically attentive when it comes to deleting data, as they know victims are only incentivized to pay for a tool if the data is still there, and merely encrypted. The uptick in haphazard data destruction has led some victims to suffer significant data loss and extended business interruption as they struggle to rebuild systems from scratch. It remains unclear whether these events have been outliers or a symptom of less experienced bad actors handling the attack execution.

16 Variants Now Make up the Top 10 Most Common Ransomware List

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
1	Sodinokibi	17.5%	-
2	Egregor	12.3%	New in Top 10

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
3	Ryuk	8.7%	New in Top 10
4	Netwalker	6.0%	-1
5	Maze	5.2%	-3
6	Conti v2	4.8%	New in Top 10
7	DopplePaymer	4.0%	-2
8	Conti	2.4%	-2
8	Suncrypt	2.4%	New in Top 10
8	Zeppelin	2.4%	New in Top 10
9	Avaddon	2.0%	+1
9	Phobos	2.0%	-5
9	Nephilim	2.0%	+1
9	MedusaLocker	2.0%	New in Top 10
9	Lockbit	2.0%	-1
10	GlobeImposter 2.0	1.6%	New in Top 10

Top 10: Market Share of the Ransomware attacks

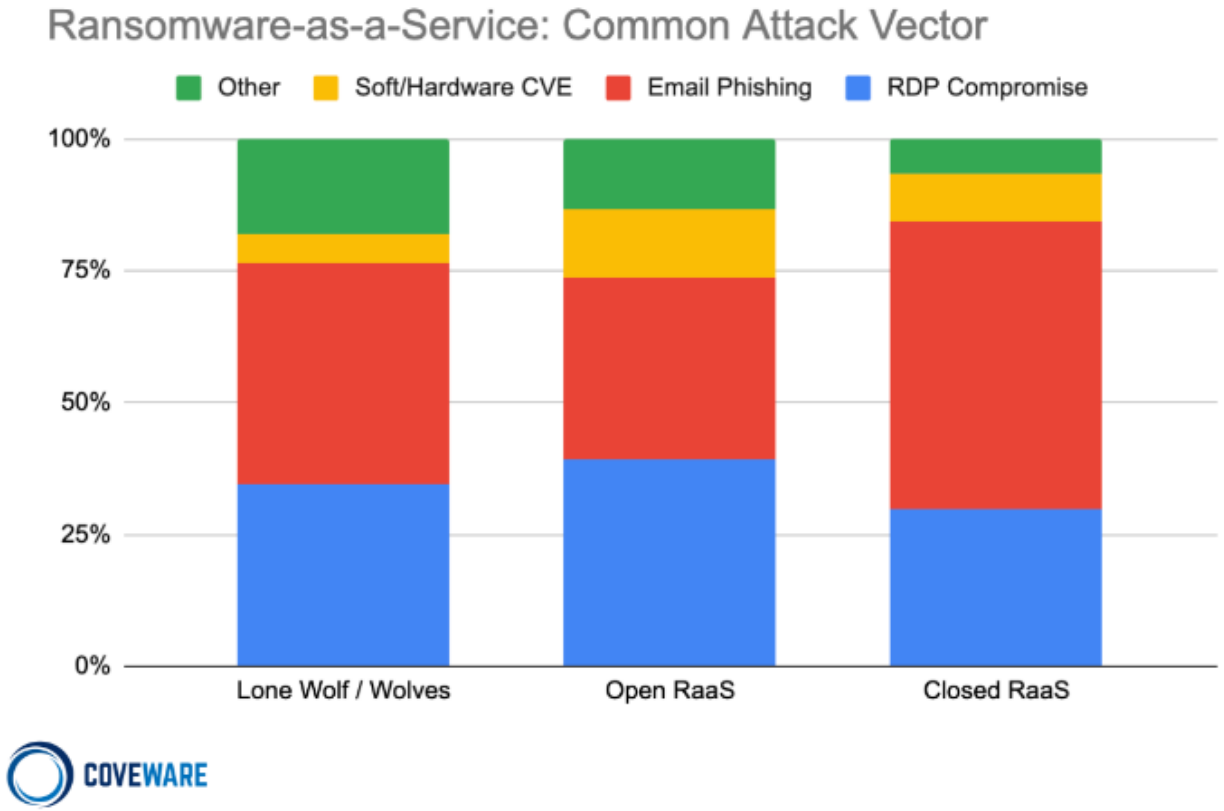
Concentrations for the top ransomware-as-a-service variants continued to dilute in Q4 as new variants took market share, and old variants re-emerged. In Q4, we saw the Maze operation fully wind down with their remaining active affiliates swapping into Egregor. Ryuk also re-emerged in Q4, but then abruptly disappeared at the end of the quarter leaving multiple victims without the option to recover their data. As Ransomware-as-a-Service ("RaaS") has evolved, we have also seen a continuation of how different types of RaaS operations target specific segments of enterprise victims. We have outlined these differences further in this report.

Characteristics of Ransomware-as-a-Service Operations

As barriers to entry have dropped, different business models have proliferated to support the flood of inbound participants in the cyber extortion industry. Ransomware-as-a-Service is designed to scale the distribution of attacks below a centralized developer that controls the underlying code of the ransomware payload and access to the decryption keys. After observing several thousand ransomware cases, we can classify variants into three distinct buckets based on the characteristics of the group that distributes the variant.

Lone Wolves

By definition, these groups are not actually affiliate-based models, like most RaaS operations, but they can be small groups. Examples of lone wolf groups include THT, which uses commercial full disk encryption software and a boot locker program (which services as their ransom note) to attack victims. This is also known as Mamba Ransomware, though we note there is no actual malicious software used in these attacks. The encryption is accomplished using legitimate, off-the-shelf encryption software. Mamba-style groups like THT are comprised of one to three individuals that have different specialties. Lone wolf groups do not solicit new members to join them and are typically dormant for periods of time. The individuals in these groups are likely to have regular jobs and distribute their attacks for supplemental income. The active/dormant periods demonstrate that they are not always campaigning.

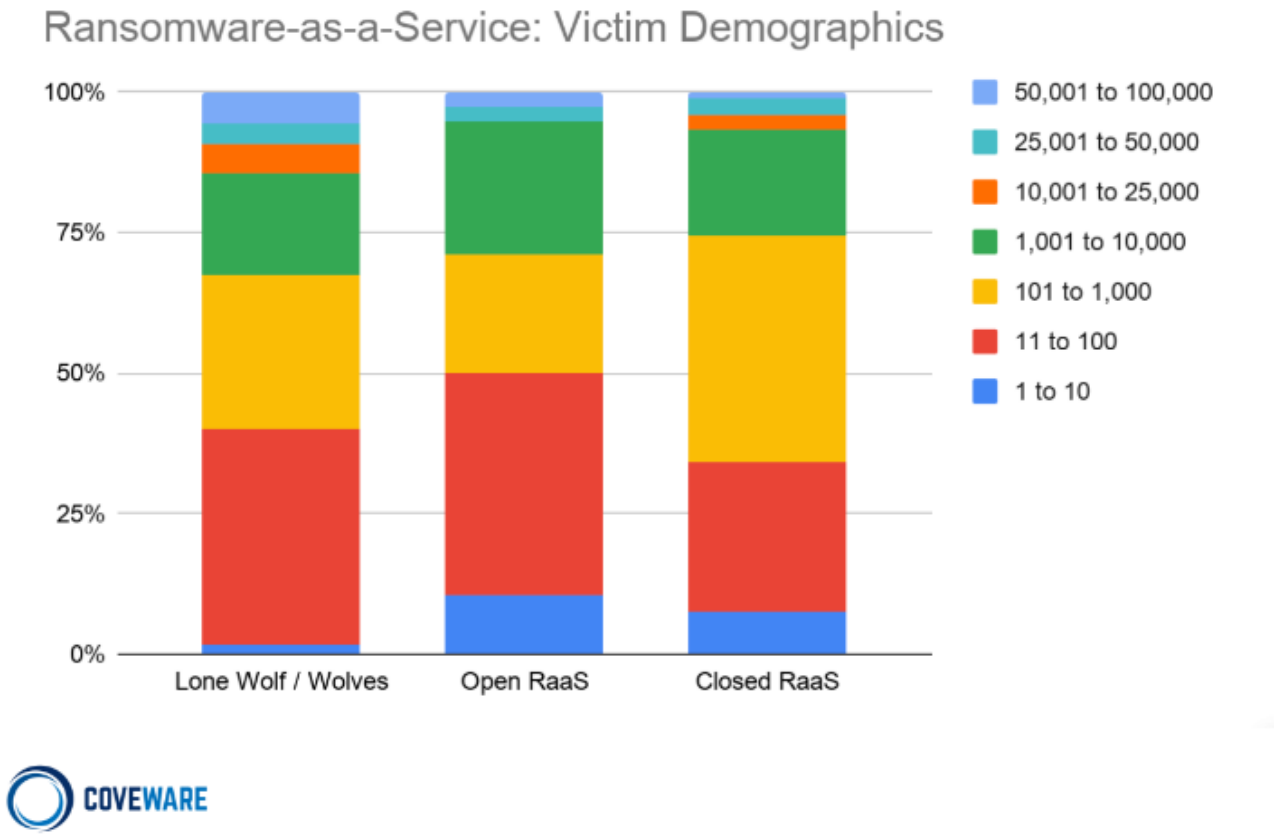


Common Attack Vectors: Soft/Hardware CVE, email phishing, RDP compromise, and others.

Open RaaS

Open RaaS operations openly solicit any and all would-be cyber criminals that want to use the variant. The ubiquitous Dharma ransomware variant is a good example of an open RaaS variant. Dharma, and its cousin Phobos, are regularly advertised in dark market forums, and charge no fee for those who wish to become an affiliate. Open RaaS distributors skew towards the lower end of the sophistication spectrum and their attack

profiles reflect this. They are much more likely to target small companies with 71% of attacks occurring against victims that have less than 1,000 employees. They are also much more likely to use cheap and easy methods to gain initial ingress with almost 40% of attacks leveraging RDP intrusion to gain initial access to a network.

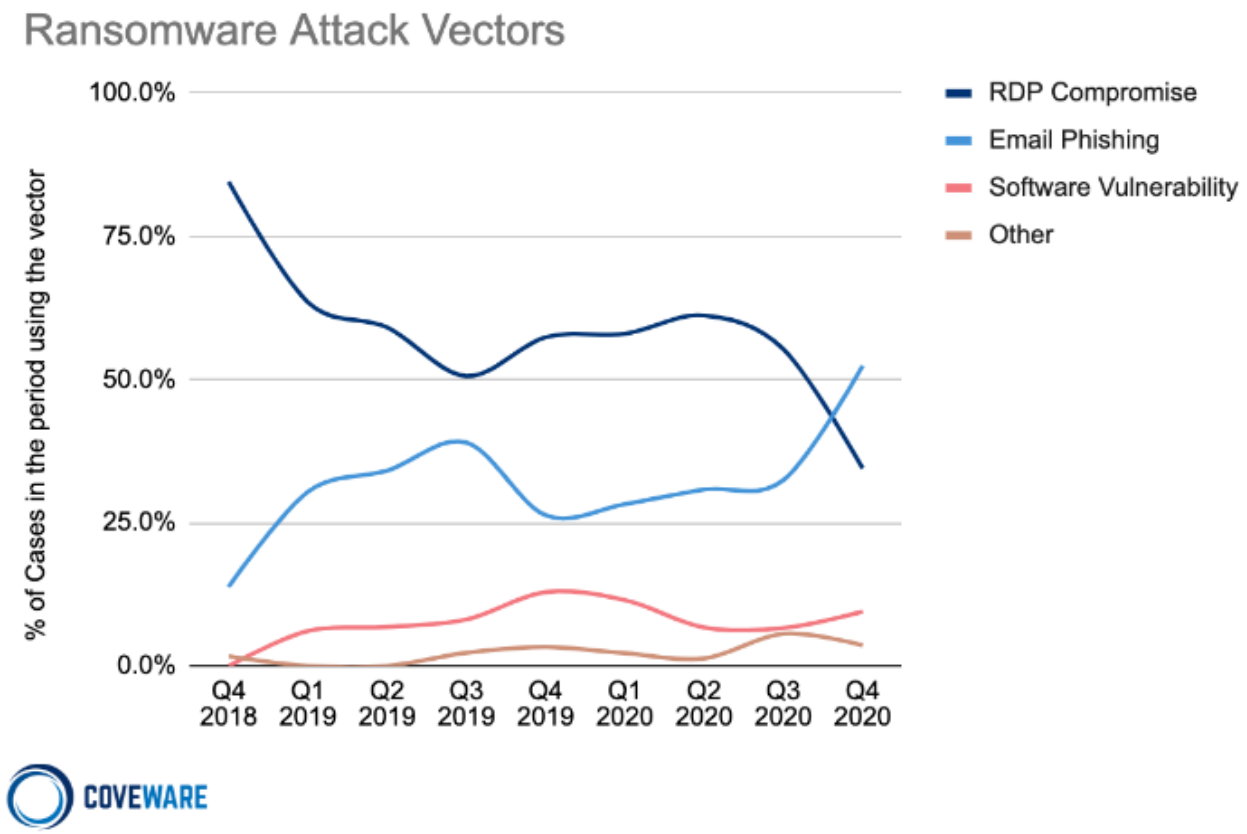


Attacks by Victim Employee count

Closed RaaS

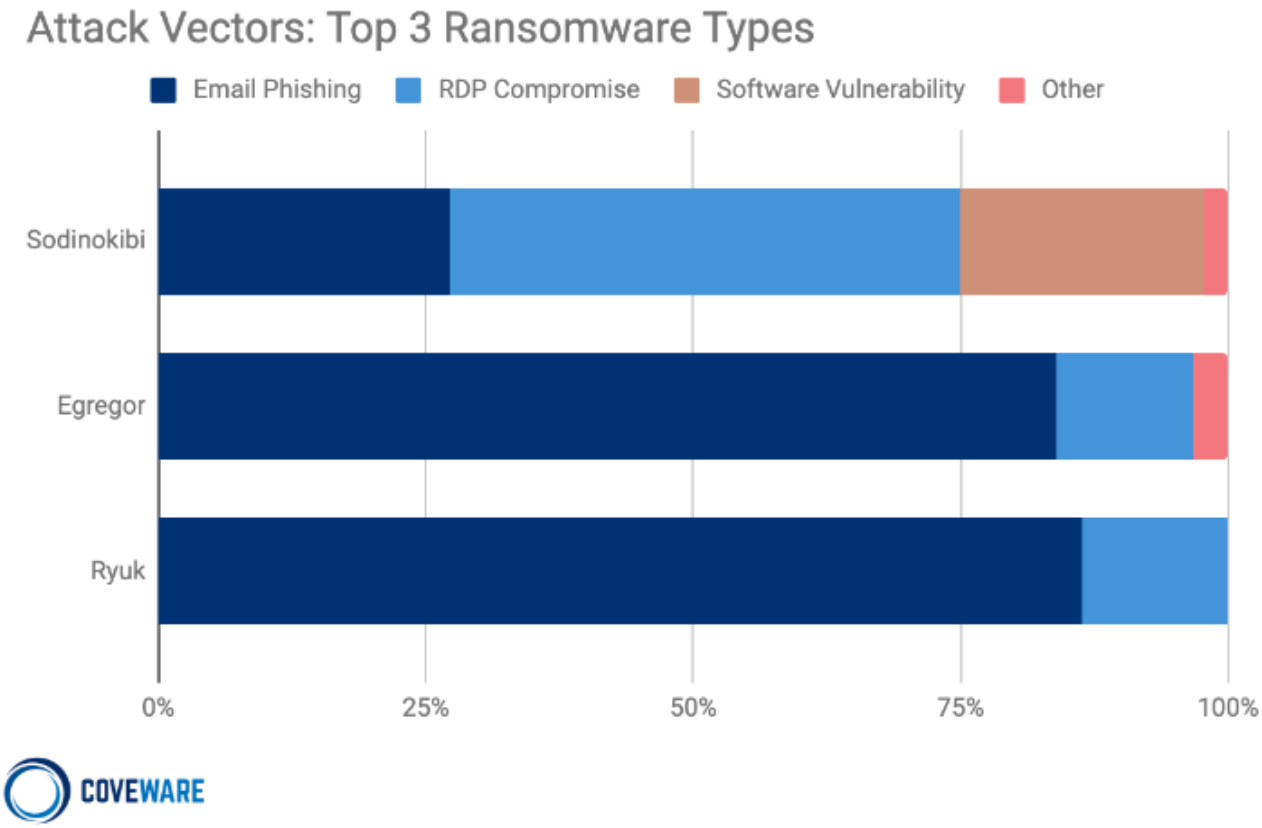
Closed RaaS operations utilize larger groups of individuals as affiliates or distributors, but they are highly selective about *who* they allow to distribute the branded ransomware. Examples of this include Sodinokibi, Egregor and Conti Ransomware. These groups can have dozens of affiliates that are carrying out attacks, but they are all vetted by the core developers before they are allowed to participate. Affiliates that do not demonstrate exceptional performance may also be kicked out of the group. Closed RaaS groups skew towards the higher sophistication scale and accordingly tend to attack larger enterprises using more sophisticated attack vectors. Closed RaaS groups are also much more likely to bundle data exfiltration with encryption during their attack.

Email Phishing Is the Top Attack Vector



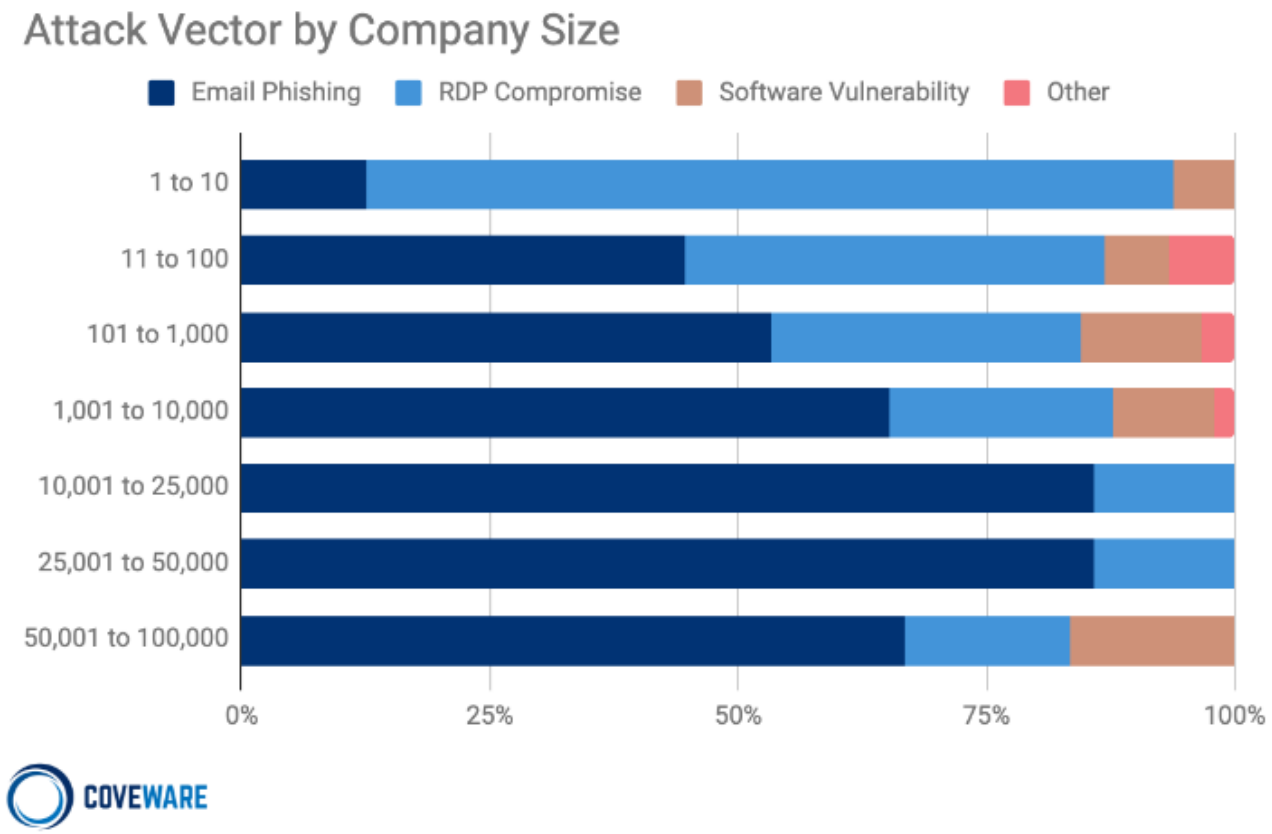
Ransomware attack vectors: RDP compromise, email phishing, software vulnerability, and others.

In Q4, email phishing overtook RDP compromises as the dominant attack vector. This is the first quarter since Coveware has been tracking data that RDP compromise has not been the primary attack vector. Precursor malware, like Trickbot / Emotet, favor widespread phishing campaigns as their primary delivery mechanism. Unlike ransomware malware, these threats possess worming capabilities that allow them to stealthily proliferate through a high volume of enterprise networks. There they lay down secure footholds that are sold further down the supply chain to ransomware actors. We expect a reshuffling of attack vectors to occur in the wake of the Emotet take down. RDP compromises remain a very common attack vector, with network credentials to brute-forced networks commonly for sale for as little as $50 USD.



Top 3 Ransomware Types: Sodinokibi, Egregor, and Ryuk.

The variants with the most market share also relied heavily on the fruits of email phishing campaigns. The affiliates that carry out these attacks generally don't have a preference on the attack vector. The only variable that matters is cost and quality of the network credentials that they are able to procure. Even with the cost of RDP credential declining, threat actors still prefer to use network access originally sourced through email phishing campaigns.

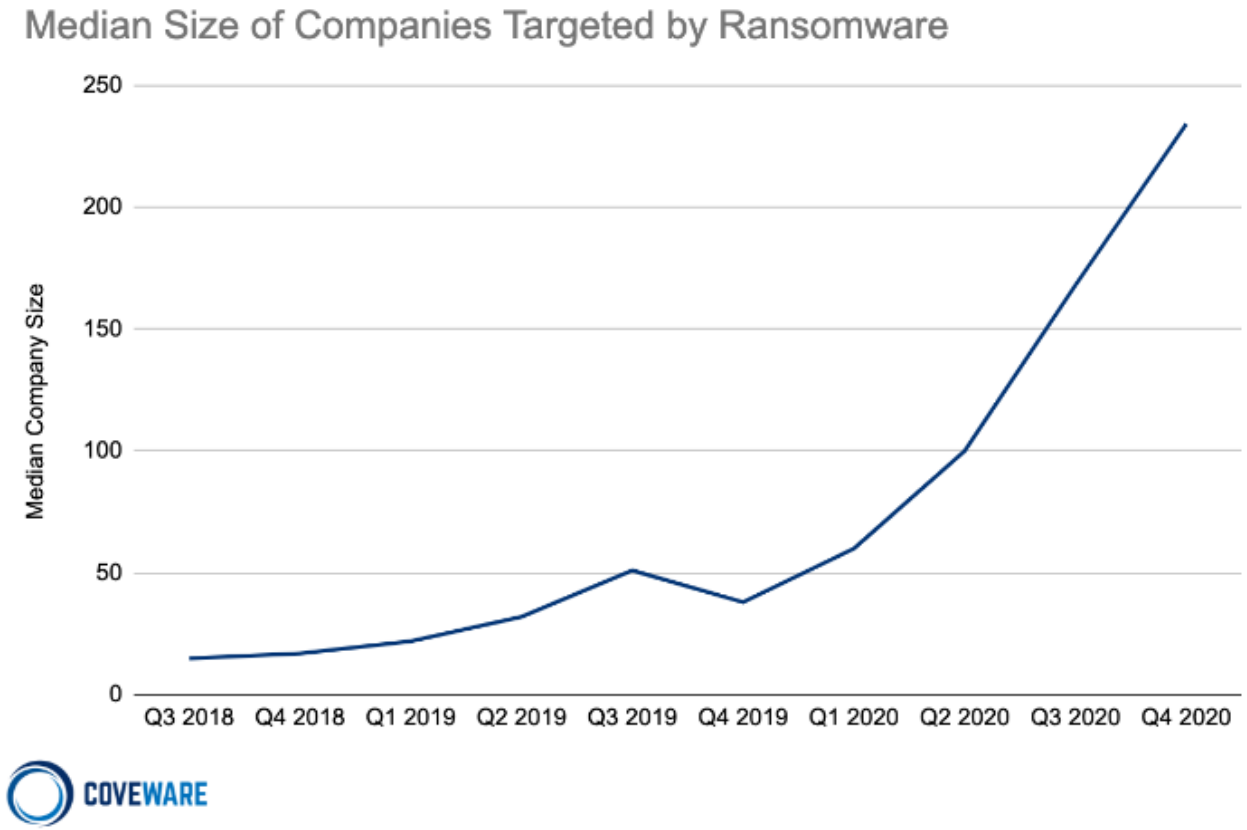


Attack Vector by Company Size Q4,2020

Ransomware Is Predominantly a Small Business Problem

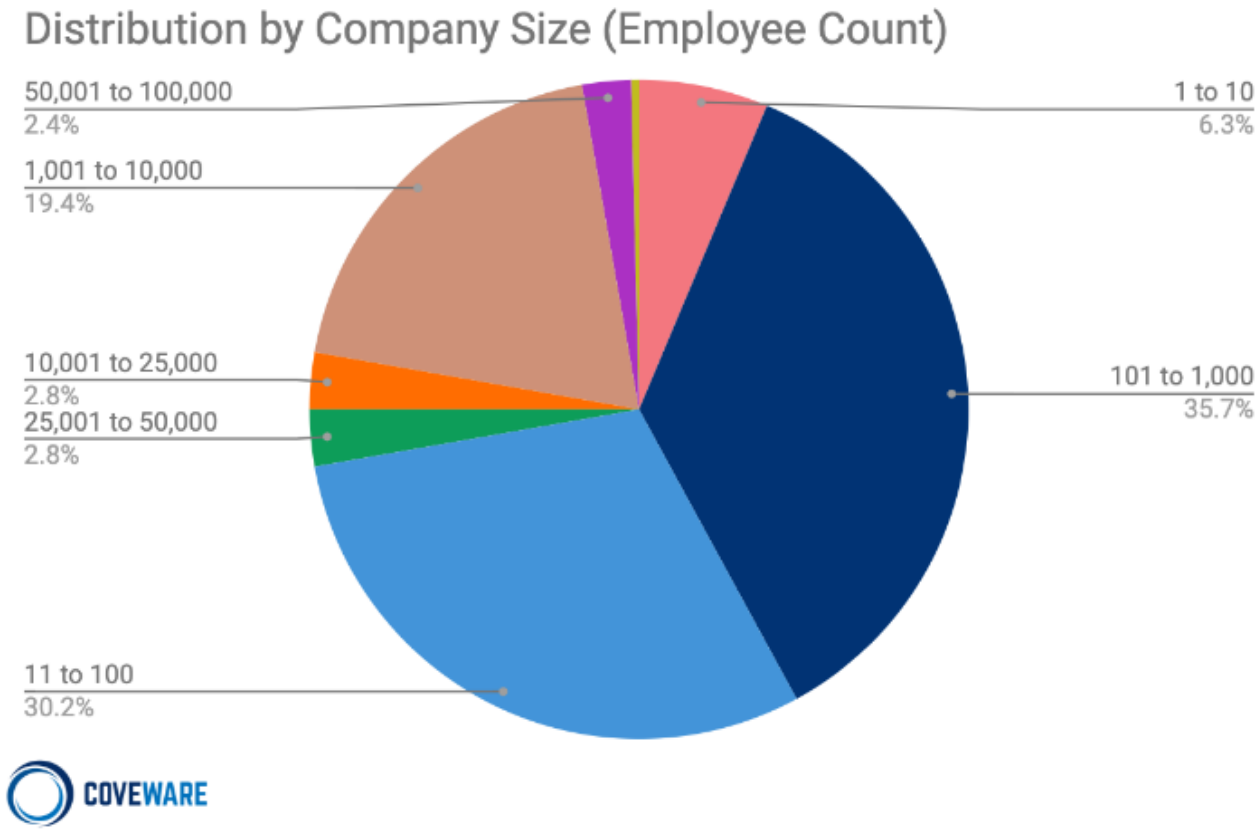
Median # of Employees

234
+39% from Q3 2020



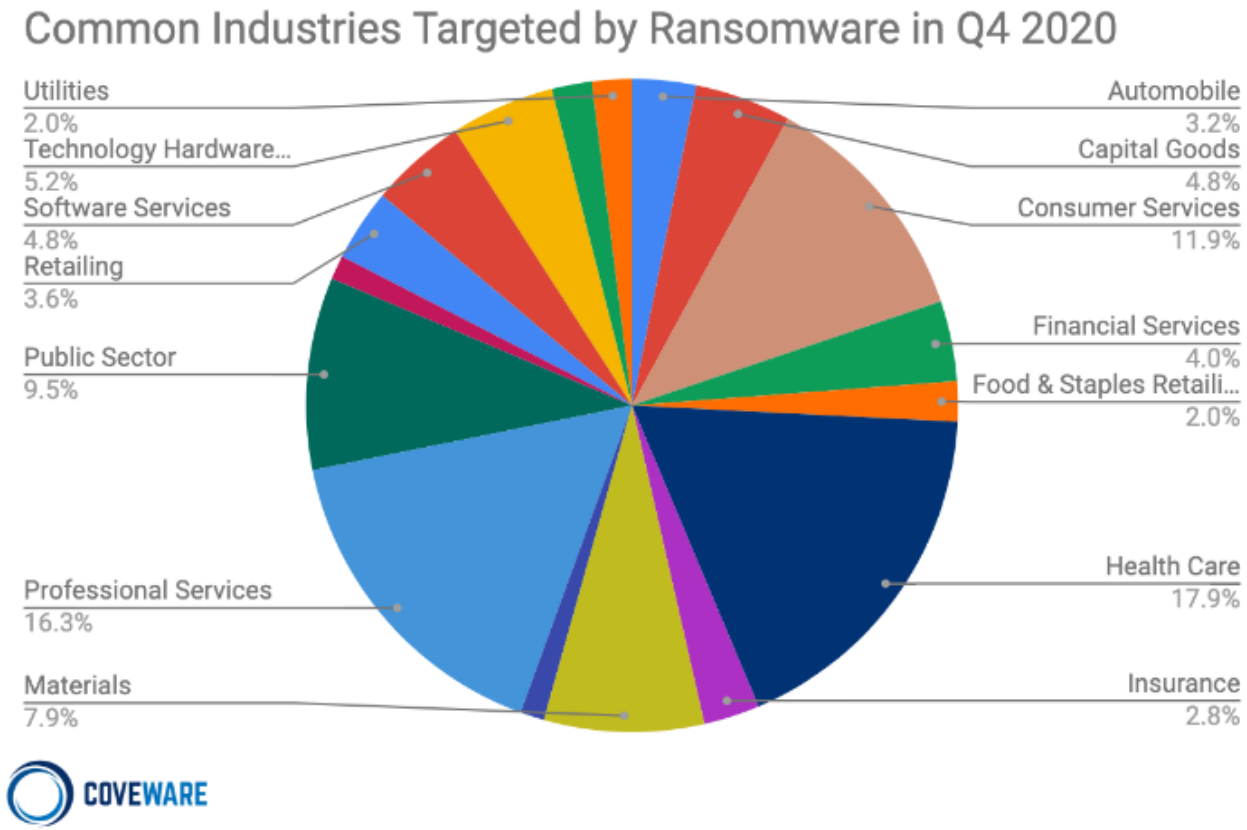
Median Size of Companies Targeted by Ransomware

The median company that fell victim to ransomware in Q4 2020 had 234 employees. This was a +39% from Q3 of 2020. Mid-market companies are increasingly coming under attack as their demographic makes them a favorable target.



Distribution by Company Size Q4, 2020

The allocation of ransomware attacks remained somewhat evenly distributed between size buckets. A notable outlier was the 1,001-10,000 bucket which increased from 12.3% of cases to 19.4% of cases. Mid-market companies are being found more frequently in the cross hairs of ransomware actors. These companies typically are just as easy to penetrate, and have a greater capacity to pay versus very small businesses.



Common Industries Targeted by Ransomware in Q4, 2020

Professional services firms, especially small law firms and financial services firms, consistently fall victim to ransomware attacks. In general, small companies are less likely to have dedicated IT security staff. Small service firms are more likely to have network structures that are flat, and simple access control policies that are not well maintained. These firms also do not consider themselves prime targets for ransomware, and are not taking the steps needed to keep themselves safe. These vulnerabilities make them a low-hanging fruit and a cheap target.

Business Interruption Costs Are the Largest Source of Losses

Average Days of Downtime

21
+11% from Q3 2020

Downtime is still the most costly aspect of a ransomware attack. In Q4 of 2020, the average firm experienced roughly 21 days of downtime, 2 more days than in Q3. 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

Coveware is not responsible for any actions taken, errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of this content, or for the performance of any computer, hardware or software used or modified in conjunction with this content. The content is provided on an "as is" basis.

VIEWERS OF THIS REPORT AND ITS CONTENT DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

In no event shall Coveware be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the content even if advised of the possibility of such damages.