Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

April 26, 2021

Table of Contents

The Coveware Quarterly Ransomware Report describes ransomware incident response trends during Q1 of 2021. Data exfiltration extortion continues to be prevalent and we have reached an inflection point where the vast majority of ransomware attacks now include the theft of corporate data. Q1 saw a reversal of average and median ransom amounts. The averages in Q1 were pulled up by a raft of data exfiltration attacks by one specific threat actor group that opportunistically leveraged a unique vulnerability (more on this below).

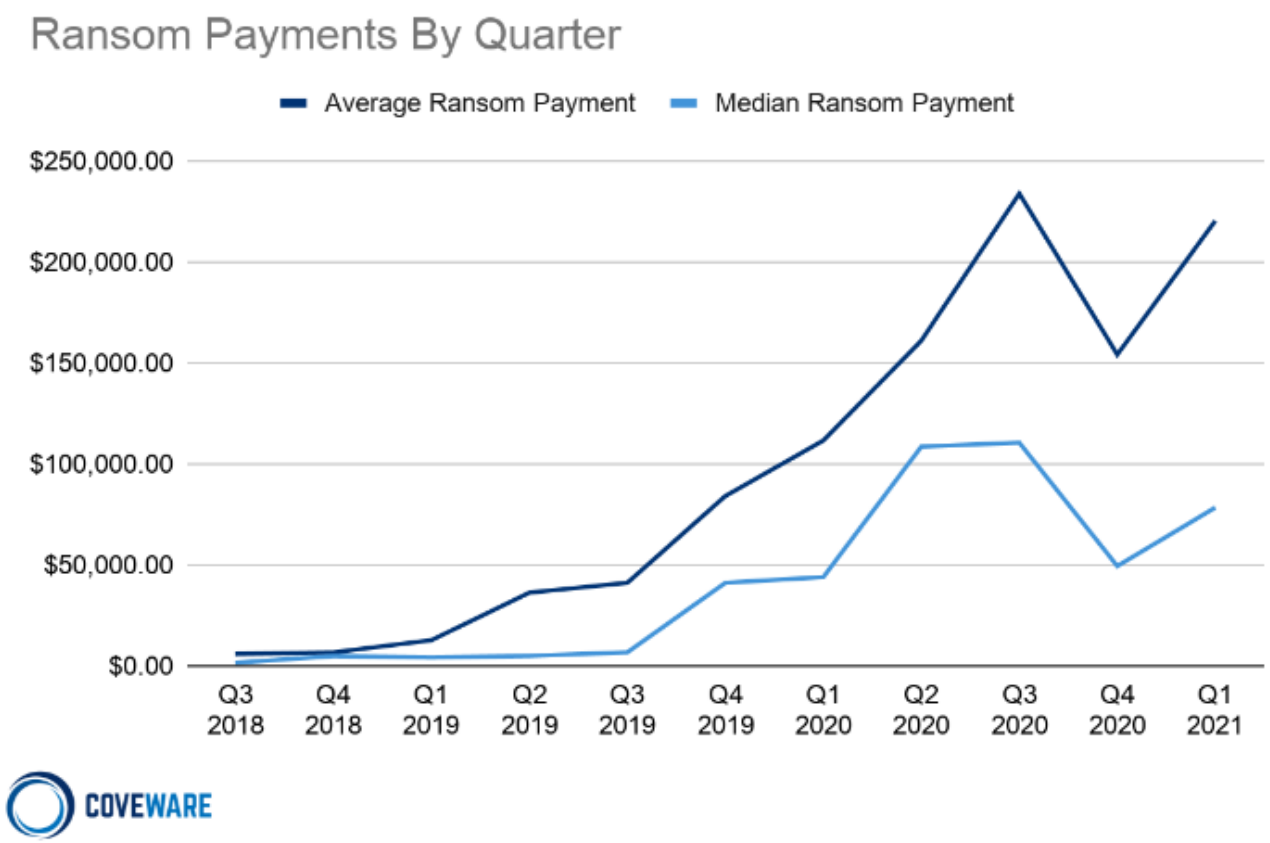
Average and Median Ransom Payments in Q1 2021

Average Ransom Payment

$220,298
+43% from Q4 2020

Median Ransom Payment

$78,398
+59% from Q4 2020



Average and Median Ransom Payments

The average ransom payment increased 43% to $220,298 from $154,108 in Q4 of 2020. The median payment in Q1 also increased to $78,398 from $49,450, a 58% increase. Averages and median were pulled higher by a small number of threat actor groups, most specifically CloP, that were extremely active during Q1 and impacted large victims with very high ransom demands. As the data exfiltration tactic has proliferated, the risk / reward characteristics of paying to suppress a leak has not changed. We first noted this trend in our Q3 report; victims of data exfiltration extortion have very little to gain by paying a cyber criminal, and despite the increase in demands, and higher prevalence of data theft, we are encouraged that a growing number of victims are not paying. Over hundreds of cases, we have yet to encounter an example where paying a cyber criminal to suppress stolen data *helped* the victim mitigate liability or avoid business / brand damage. On the contrary, paying creates a false sense of security, unintended consequences and future liabilities. Coveware's position remains unchanged and we advise victims of data exfiltration extortion to assume the following:

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

77% of Ransomware Attacks Involved the Threat to Leak Exfiltrated Data (+10% From Q4 2020)

The percentage of ransomware attacks that included a threat to release stolen data increased from 70% in Q4, to 77% in Q1. The majority of ransomware attacks that involve data exfiltration have two main goals 1) exfiltrate corporate data from the most convenient file server 2) escalate privileges and deploy ransomware on as many endpoints as possible. Most RaaS affiliates purchase network access and use stolen data solely as additional leverage against the victim. This means that despite the threats, threat actors rarely take the time to steal data that any other criminals or interested parties would want to purchase. The stolen data is just proof that the attack occurred and sometimes creates legal obligations for the victim.

The CloP ransomware group took a very different strategy in their Q1 exploitation of Accellion's FTA product. Beginning in late December and continuing through much of Q1, CloP exploited two zero day vulnerabilities that allowed for remote code execution within unpatched Accellion FTA instances. This was a highly sophisticated and targeted exploitation of a single software appliance, only used by a handful of enterprises. The CloP group may have purchased the exploit used in the initial stages of the attack, so as to have exclusive use. This behavior stands in stark contrast to how most unauthorized network access is brokered through the cyber extortion supply chain to any willing purchaser post exploitation. Moreover, the Accellion exploit did not allow for the deployment of ransomware across the victims environment, so data theft from the appliance was the sole target of CloPs campaign from the outset.

Unlike most exploits used by ransomware threat actors, unpatched Accellion FTA instances are rare (likely less than 100 total), especially when compared to vulnerable RDP instances which number hundreds of thousands globally. CloP's confidence that such a small number of targets would yield a positive financial return must have been high and, unfortunately, they were correct. Dozens of CloP victims were extorted for tens of millions of dollars even though the majority of the victims opted not to pay and were subsequently doxxed on the CloP leak site. As of early April, the CloP/Accellion campaign seems to have run its course, and the CloP group has returned to using traditional network access vectors and encryption ransomware in its attacks.

Most Common Ransomware Variants in Q1 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2020
1	Sodinokibi	14.2%	-
2	Conti V2	10.2%	+4
3	Lockbit	7.5%	+6
4	Clop	7.1%	New in Top Variants
5	Egregor	5.3%	-3
6	Avaddon	4.4%	+3
7	Ryuk	4.0%	-4
8	Darkside	3.5%	New in Top Variants
9	Suncrypt	3.1%	-1
9	Netwalker	3.1%	-5
10	Phobos	2.7%	-1

Top 10: Market Share of the Ransomware attacks

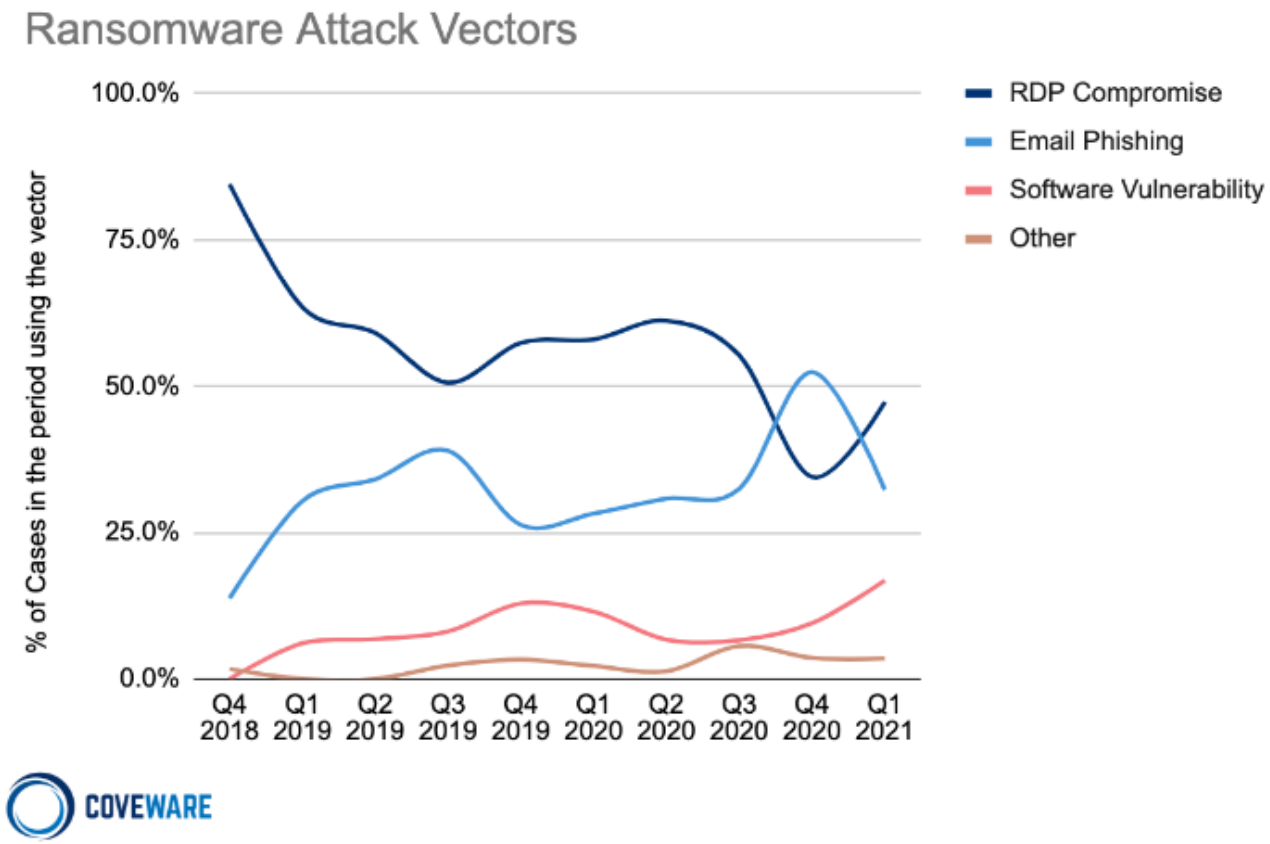
Ransomware-as-a-Service operations ratcheted up the competition for affiliates and credibility in Q1. As these groups have grown in size, so has associated operational complexity and risk. Some failures of operating a criminal enterprise at scale were observed during Q1 include:

- Egregor: Sunsetting operations only 4 months after taking the torch from the Maze group.
- Netwalker: Ceased activities following a complete law enforcement take down of infrastructure and arrest of affiliate participants.
- Conti: Growing pains as their outsourced chat operations complicated victim recoveries and negotiations. Additionally, Conti has also been re-attacking prior victims and launching new attacks shortly after an initial attack was sustained. A practice at odds with a RaaS organization interested in maintaining a reputation that compels victims to pay a ransom.
- Lockbit: Technical flaws in the ransomware that resulted in data loss of encryption victims. The group has also been associated with numerous re-extortion demands.
- Sodinokibi: Technical flaws that resulted in victims unable to match encryption keys, resulting in total data loss.

- BlackKingdom: Attempted a mass exploit of exchange webshells, but flaws in their encryption led to permanent data loss.

A new trend in Q1, several RaaS operations turned their focus to developing encryption modules for Unix and Linux. We have now observed this development from Defray777, Mespinoza, Babuk, Nephilim and Darkside. Sodinokibi is also making rumblings about releasing a Unix version. Victims running Unix and Linux should expect complications and data loss. Early versions of any ransomware generally include bugs that the threat actors either don't know about or don't care to fix before targeting victims.

Most Common Ransomware Attack Vectors in Q1 2021

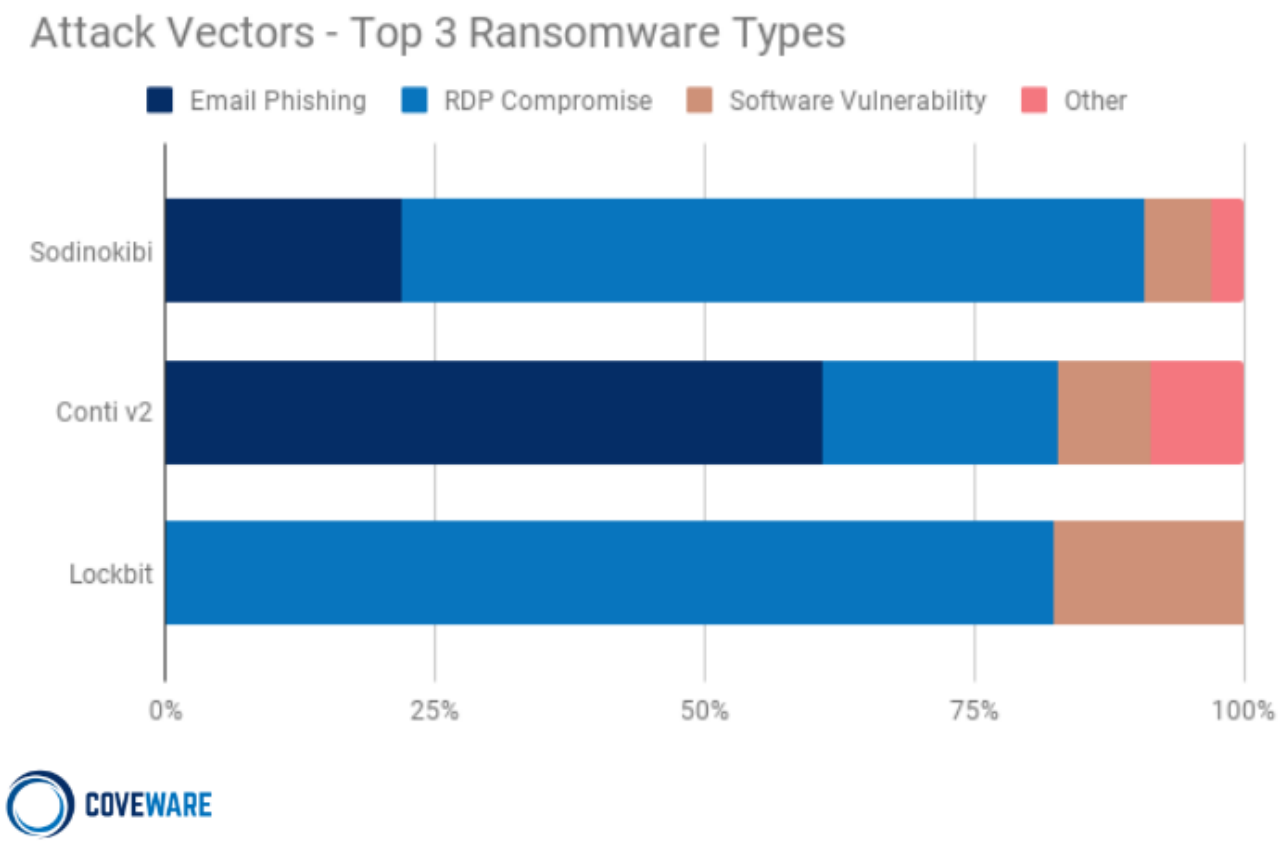


Ransomware attack vectors: RDP compromise, email phishing, software vulnerability, and others.

In Q1 compromised remote desktop protocol connections regained the top position as the most common attack vector. RDP remains a frustratingly common vulnerability despite well known secure remote connection best practices. Phishing emails that install credential stealing malware, or a remote access trojan also remain a common attack vector. Like RDP, defense techniques that include least privilege and two factor authentication can easily limit the ability of an attacker to escalate privileges beyond the initially compromised machine.

Defending against the escalatory impact of a successful phishing attack requires no new hardware or software, just the will to implement and follow simple tools and configurations properly.

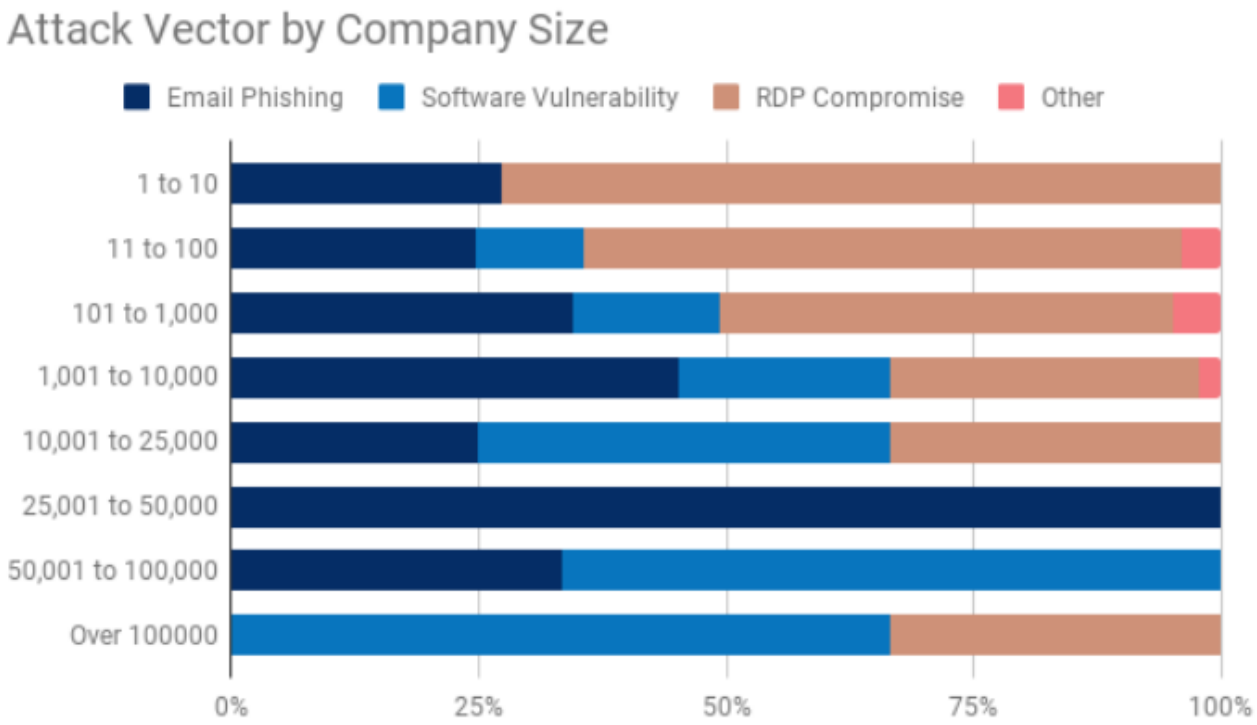
Attack Vectors used by the Top Three Ransomware Variants



Top 3 Ransomware Types: Sodinokibi, Conti V2, and Lockbit.

The most common software vulnerabilities exploited during Q1 involved VPN appliances, such at Fortinet and Pulse Secure. Several RaaS services leveraged these VPN vulnerabilities during Q1. Again, it is likely that the actual RaaS operators and affiliates were NOT the party that achieved network access via these vulnerabilities, but rather specialist actors that harvest network credentials and are specifically trained to mass scan for vulnerable IP addresses. These specialists then resell network access to ransomware affiliates who use the access to stage the extortion phase of the attack. This deliberate division of labor sheds light on how open RaaS operations that focus on smaller victims, like Lockbit, were able to take advantage of vulnerabilities outside of their skillset. Specialization and supply chain coordination also highlights the continued evolution of the cyber extortion economy.

Attack Vectors used by Ransomware Actors on Different Sized Victims

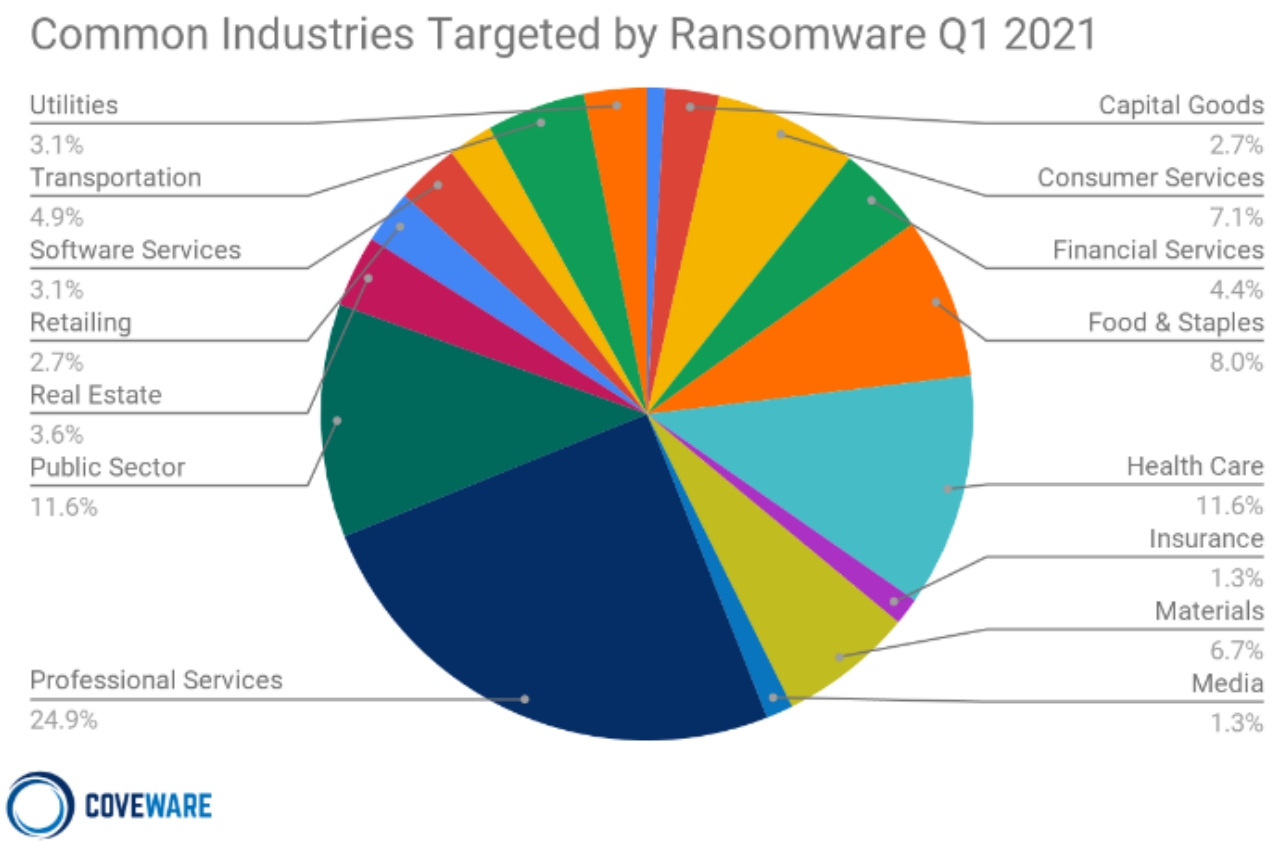


Attack Vector by Company Size Q1 2021

During Q1, the cyber extortion economic supply chain demonstrated how a vulnerability in widely used VPN appliances can be identified, exploited and monetized by ransomware affiliates. It is rare to see software vulnerabilities directly leveraged by affiliates of RaaS groups, but when specialists broadly market the results of their elicit skills then the costs of carrying out an attack decline and lower the barriers to entry for new cyber criminals.

The continued evolution and specialization of the ransomware supply chain is a worrisome trend. Lower overall operating costs drop the barrier to entry AND boost the profitability of attacks. Until the unit economics of ransomware attacks becomes less profitable, we should expect the volume of attacks to continue to increase. Even more worrisome is the maturity and progression of the supply chain within the cyber extortion economy. The infrastructure that is being created to run this economy will be difficult to unwind. The more mature the supply chain is allowed to become, the harder it will be to dismantle.

Most Industries Impacted by Ransomware in Q1 2021



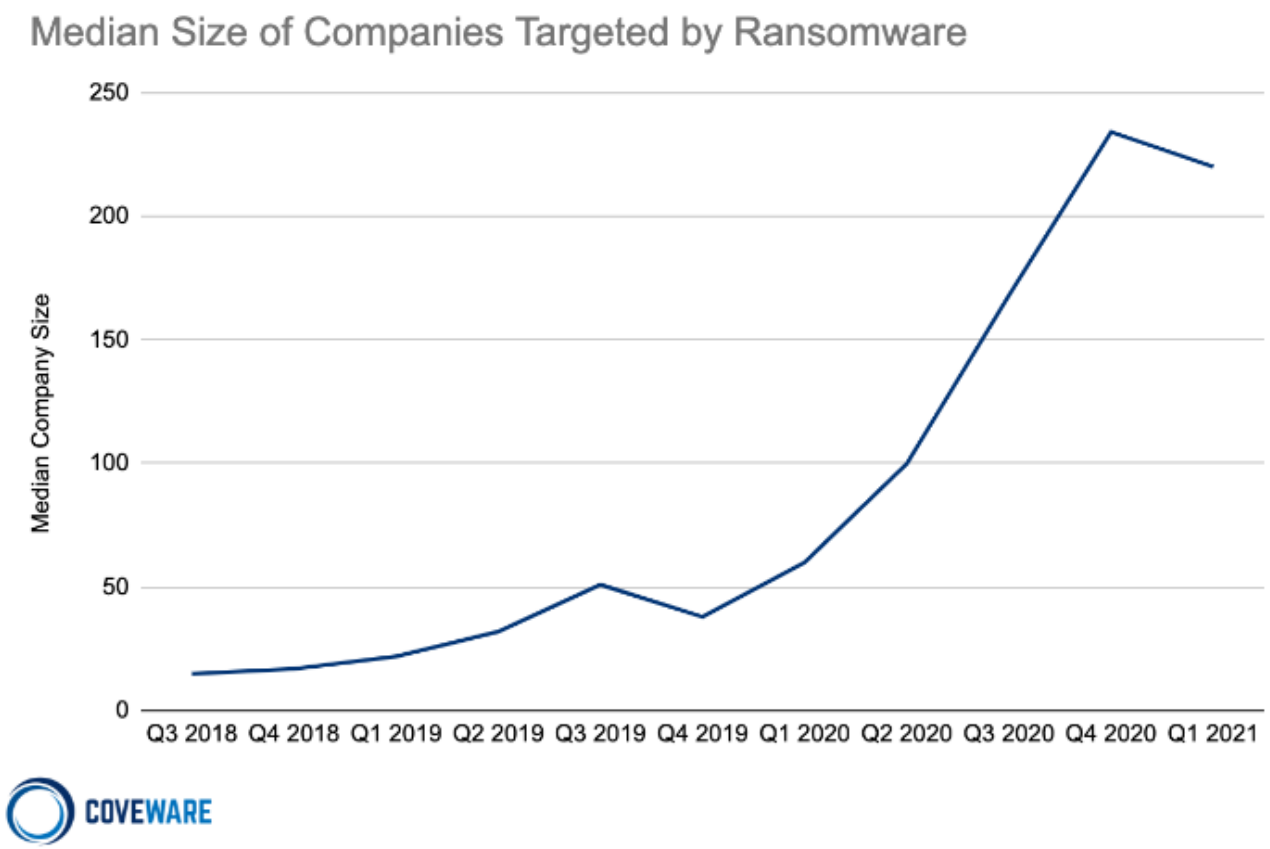
Common Industries Targeted by Ransomware in Q1 2021

The most notable change in industries impacted by ransomware attacks in Q1 was the Professional Services industry, specifically law firms. Small and medium sized law firms continue to succumb to encryption ransomware and data exfiltration extortion attacks. Unfortunately, the economics of many small professional service firms do not encourage or enable adequate cyber security.

For example, many law firms are structured as limited partnerships for tax purposes. This means the firm pays out all its profit to the partners every year. The desire to maximize profits and income to the partners can marginalize the priority of investing in cybersecurity. Another example is the third party vendor relationships of a small law firm. These firms generally do not work with major enterprises that would perform rigorous cyber risk assessments, the most basic of which would immediately surface common vulnerabilities and weaknesses that may result in a future ransomware attack. Rather, small firms tend to have equally sized clients that do not demand vendor assessments of cyber risk.

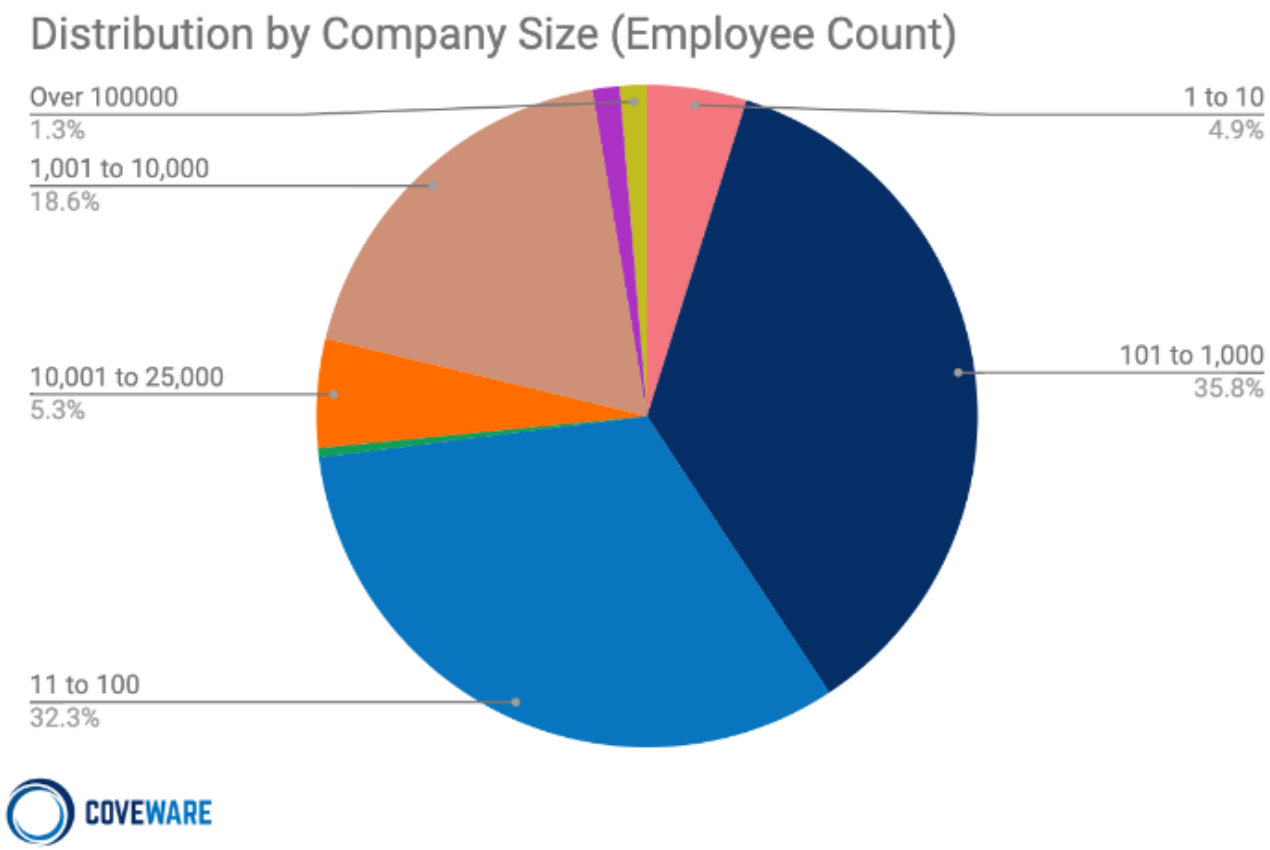
As a result of these two examples there is minimal internal or external market pressure to prioritize cyber security. The volume of professional service firms that are victimized is a result of these micro dynamics.

Median Size of Ransomware Attack Victims in Q1 2021



Median Size of Companies Targeted by Ransomware

Ransomware attacks still disproportionately affect small businesses. These small companies rarely end up in the headlines and often don't have the financial or technical expertise to properly handle the incident OR perform the proper remediation required to prevent a repeat attack. Small businesses that exist below the cyber security poverty line represent the greatest challenge to stemming the expansion of the cyber extortion economy.



Distribution by company size (employee count)

Incident Duration and Business Interruption of a Ransomware Attack

Average Days of Downtime

23
+10% from Q4 2020

Incident duration expanded slightly in Q1 to an average of 23 days. Contributing factors to this increase were the average length of time it takes to adjudicate data exfiltration incidents, and technical challenges from corrupted data (see above discussion on flaws in certain ransomware causing data loss). Q1 also included multiple instances of deliberate disruption by the threat actor during the recovery period following the initial attack. Disruptions included attempts to steal additional data or re-launch the ransomware. Prior to Q1 such behavior was a rare occurrence, but the tactic appears to be gaining traction amongst certain threat groups. This behavior not only exacerbates business interruption, but delays negotiation progress. This behavior also undermines the victim's confidence that the threat actor will assist in a successful resolution. The threat actor's expectation that re-attacking increases the pressure to pay is misguided. Re-attacks make victims less inclined to facilitate any sort of payment.

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.