# Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting

coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting

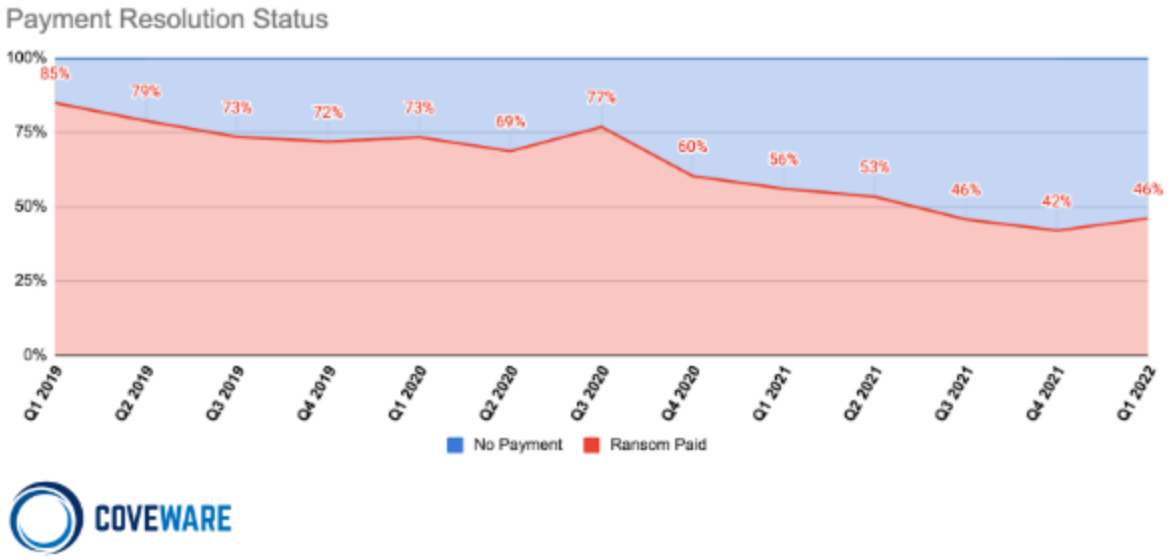
May 3, 2022

## Table of Contents



## No Silver Bullets, Just Pressure and Time

In the fight against ransomware, there is no magic bullet or single solution that will fix ANY aspect of this problem. Much as there is no single way to secure a network, there is no single method to make the unit economics of cybercrime worse for attackers. This is a double edged sword. For constituents that are in this fight for the long haul, the complexity of the problem actually allows for many levers to be tested and tried over long periods of time. For the casual short term observer, it can be difficult to tell if the problem is getting better or worse. Worse, short term observers are tempted to rationalize a single idea or thesis as THE fix. A recent report (survey based) showed that an *increasing* number of companies are resorting to ransom payments as the ultimate resolution of a ransomware incident. We have been tracking the resolution status on ransomware attacks since the early days of Coveware. While results quarter to quarter can hop and skip, the trend is very clear over the past 3 years. In Q1 of 2019, 85% of the cases we handled ended in the cyber criminal receiving a ransom payment. Three years later, that number is down to 46% in Q1 of 2022.




This is what progress looks like against ransomware. It is slow. There is no single variable that explains it, but it is fact. This fight will not be over by next quarter, but if this trend continues, the frequency and severity of this problem may look very different several years from now. In an industry where it can sometimes feel quite futile, our message to IR first responders, defenders, and LE agents is….persistence will pay off for the good guys in the long term.

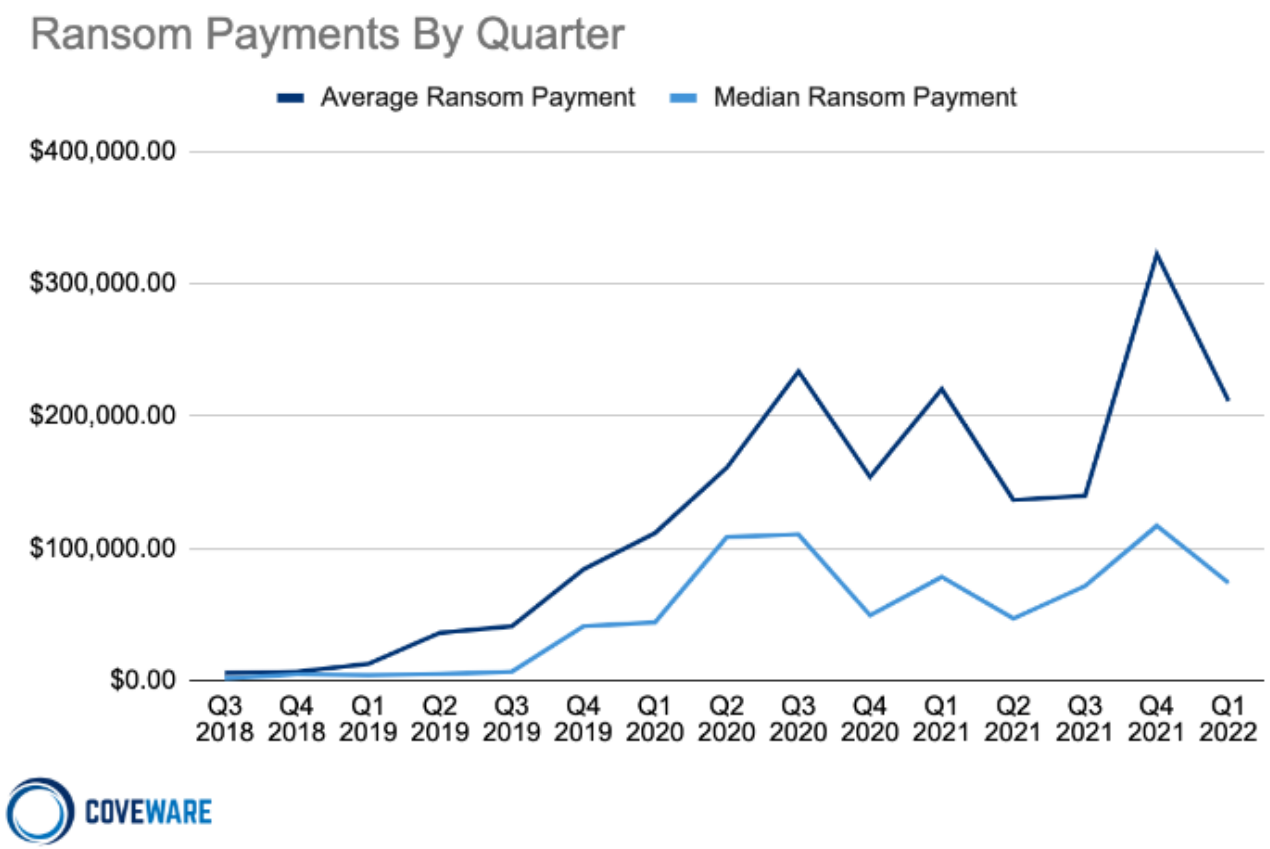
## Average and Median Ransom Payments in Q1 2022

Average Ransom Payment

$211,529
-34% from Q4 2021

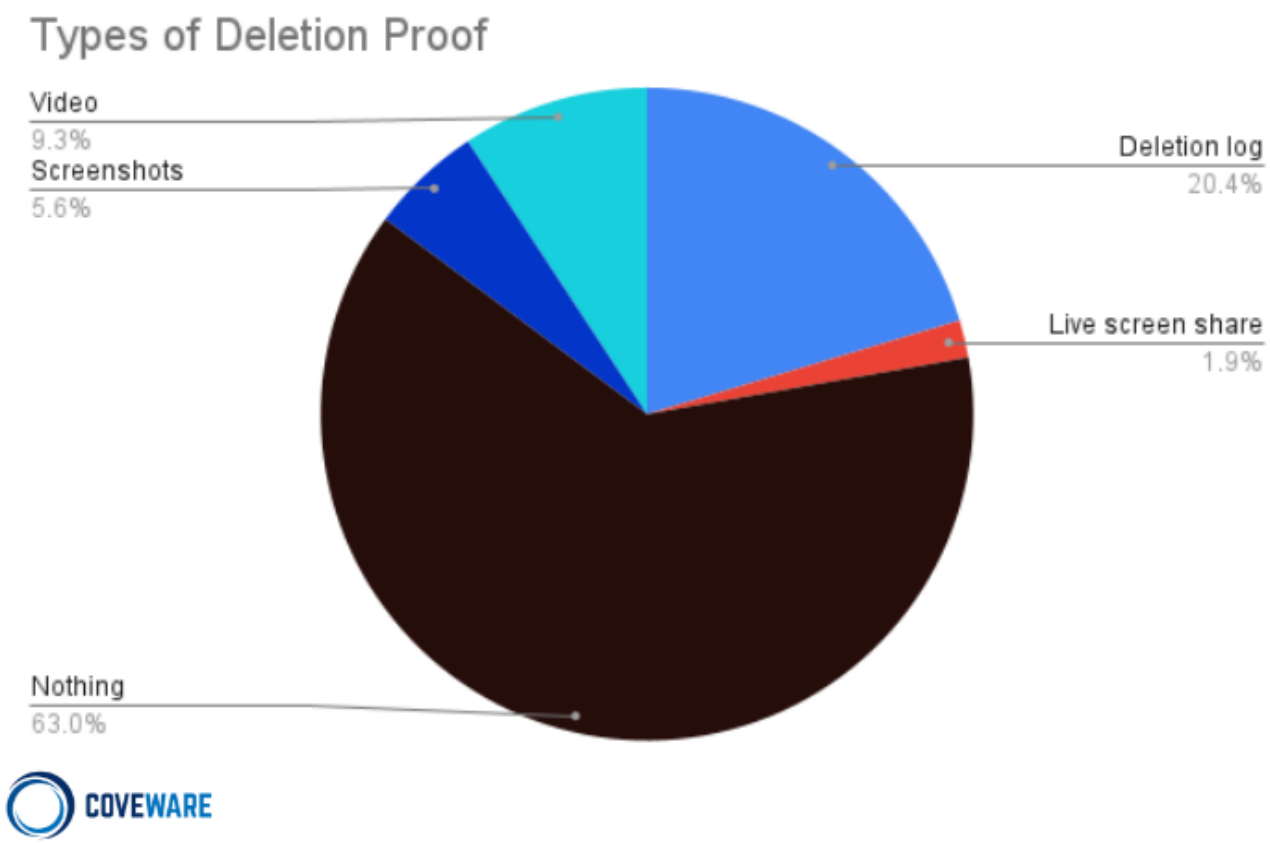
Median Ransom Payment

$73,906
-37% from Q4 2021




In Q1 2022, the average ransom payment amount dropped to **$211,529**, down34% from Q4 2021. The median ransom payment amount also fell in similar fashion to **$73,906,** down37% from Q4 2021. There was no single contributory factor that explains this reduction. A confluence of fewer companies paying, smaller companies being attacked (less big game hunting), and more diffusion among threat actors likely explains the reduction. As large RaaS brand affiliation becomes less of an asset to ransomware affiliates (due to the focus of law enforcement), ransomware affiliates are becoming very fluid in their movement and sampling of different RaaS kits, or even developing their own kits based on leaked ransomware source code (such as Hello Kitty's source code or even Conti's leaked source code).

## Big Game turns to Big *Shame* Hunting




The ‘double extortion tactic of encrypting AND exfiltrating data lost a bit of momentum during the quarter, with **77%** of cases using data exfiltration as a tactic, compared to 84% in Q4 of 2021.  Despite the decrease in the proportion of attacks that leverage data exfiltration, this tactic will likely continue as threat actors look for more efficient, less disruptive ways to extort large companies. One of the lessons learned from the pipeline attacks is that massively disrupting very large companies can bring law enforcement attention and even geopolitical attention from an attacker's home country. Data theft without encryption results in no operational disruption, but preserves the ability of the threat actor to extort the victim. We expect this shift from Big Game Hunting to Big *Shame* Hunting to continue. This being the case, actually paying a ransom to prevent the release of stolen data remains a poor decision. To highlight this, we have noted above what the outcome of these payments typically is. In the majority of cases, the victims that pay to have a leak suppressed receive NO evidence that their stolen data will be deleted or that they will not be extorted again in the future. In one notable case, we observed a threat actor explicitly state that they would not be deleting the stolen data if paid, and would keep it for future leverage against the victim.

## Most Common Ransomware Variants in Q1 2022

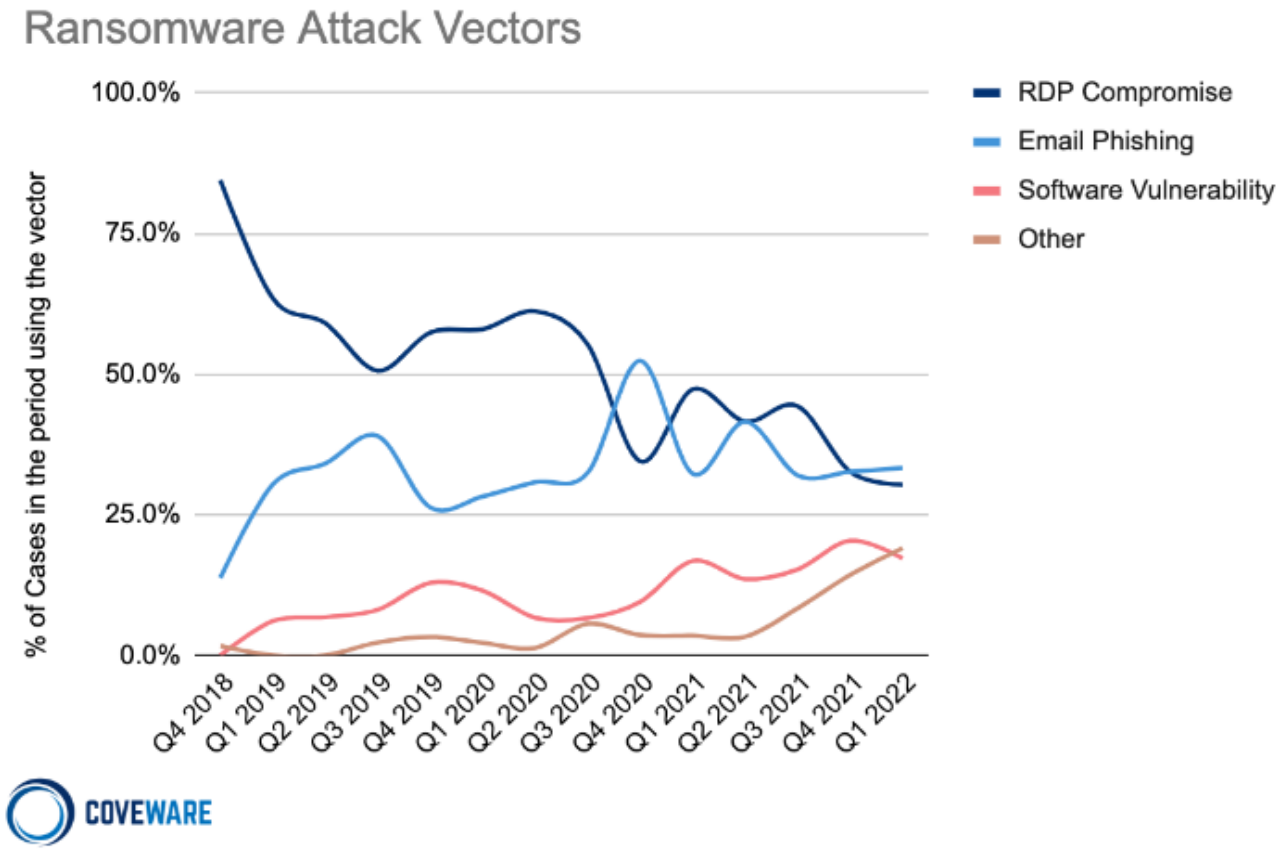
| Rank | Ransomware Type | Market Share % | Change in Ranking from Q4 2021 |
|---|---|---|---|
| 1 | Conti V2 | 16.1% | - |

| Rank | Ransomware Type | Market Share % | Change in Ranking from Q4 2021 |
|---|---|---|---|
| 2 | LockBit 2.0 | 14.9% | - |
| 3 | BlackCat | 7.1% | New in Top Variants |
| 4 | Hive | 5.4% | -1 |
| 5 | AvosLocker | 4.8% | +1 |
| 6 | Karakurt | 4.1% | - |
| 7 | Phobos | 3.0% | New in Top Variants |
| 7 | Suncrypt | 3.0% | -1 |
| 8 | Deadbolt | 2.4% | New in Top Variants |

*Market Share of the Ransomware attacks*

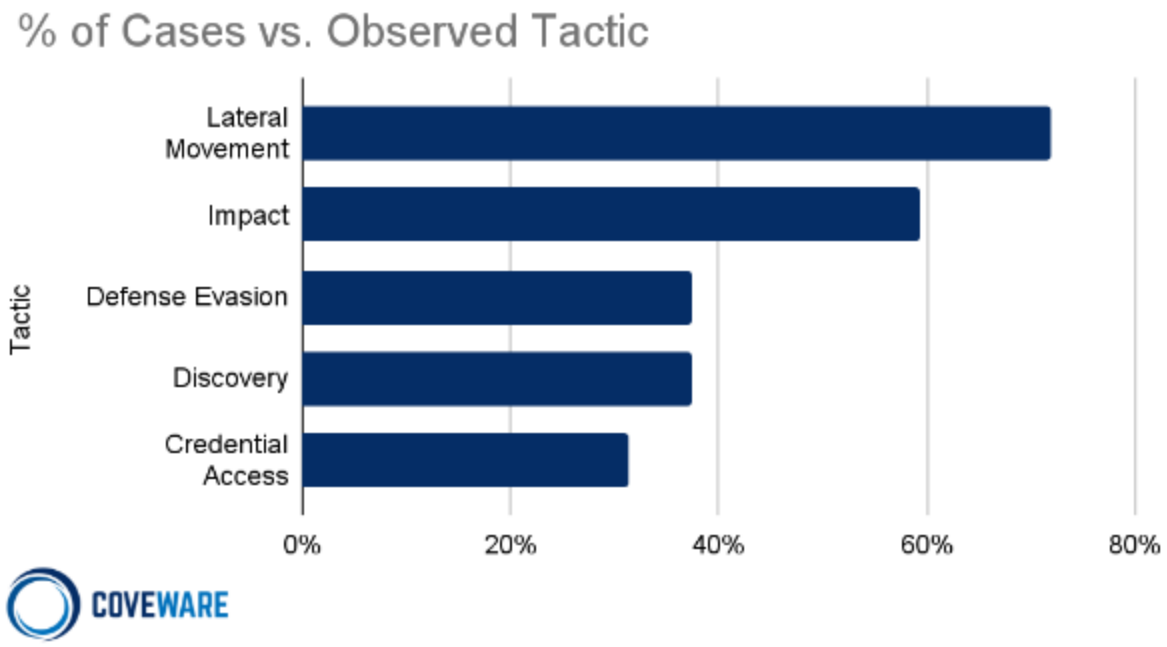
While Conti and Lockbit held their #1 and #2 positions from Q4 2021, we expect Conti to drop in the wake of their group fracturing and their internal communications being leaked in early Q1. We also saw the emergence of BlackCat ALPHV RaaS, which is using a brand new encryption binary written in Rust, and is thought by some to be composed of affiliates from a multitude of different other RaaS groups. The top five variants absorbed 48.3% of attacks in Q1 2022, as compared to 52.6% in Q4 2021. This demonstrates the beginnings of the diffusion trend which we forecast will continue in 2022 as ransomware affiliates move more fluidly between groups.

## Initial Attack Vectors used by Ransomware Threat Actors




Notable shifts in attack vectors during the quarter involved the rise of the ‘other’ category which includes social engineering and direct compromising of insiders, along with a few other methods. The social engineering attacks differ from phishing in that they are highly targeted and typically involve some priming or grooming of a target employee, before they are coaxed into allowing an attacker to gain a foothold into the network. We differentiate this from phishing which involves more automated and voluminous emailing of emails with malicious attachments or links.

## Top MITRE ATT&CK TTPs observed in Q1 2022




In addition to the Top MITRE ATT&CK TTPs that we have visualized above, we have seen an emergence of attacks by small lone wolf threat actor(s) involving highly tailored methods of ingress against well secured enterprises. This trend picked up in late 2021 and carried into Q1 2022, with the Lapsus$ group being the most discussed, albeit not the most prolific. These were financially motivated attacks, with data exfiltration extortion being the main motive of the threat actor. There was no data encryption attempted in these attacks, and no malware used for any part of the attack. The incidents involve relatively well secured organizations (we say relatively, as compared to the average security of a ransomware victim). Victims of these attacks generally had multi factor authentication properly enabled for all employees and critical resources. Given the recent focus on Lapsus$, and other actors that behave similarly, we are highlighting some observations and suggested mitigations. Below is a description of the TTP's by MITRE ATT&CK category along with mitigation steps.

**Reconnaissance** [TA0043]

Gather Victim Identity Information [T1589, T1591]: These threat actors gather extensive information about specific employees and the company's IT support desk functions. This information may include an employee's role, managers, team members, working hours and frequently used applications. The depth of understanding demonstrated may appear to denote insider collaboration, but to date, no insider collaboration with the threat actors has been proven. A key part of the reconnaissance is to map out how an employee may interact with an internal IT support desk agent. The goal is then to replicate this interaction using social engineering, as a means to bypass multi factor authentication.

Phishing for Information [T1598]: This threat actor will perform reconnaissance on employees that are candidates for further targeting to determine their technical sophistication and likelihood of being successfully socially engineered.

**Initial Access** [TA0001]

Phishing [T1566]: The threat actor will target specific employees that have access to common applications that contain sensitive data such as CRM applications, cloud based file servers, HR applications, or customer support ticketing applications. The targeted employees may be first contacted by either spoofed email or a spoofed phone call. They are subsequently socially engineered into installing remote access software onto their work machines. Please note the phishing emails are NOT the single click kind. They are email threads that appear to be legitimate work subject matter, and the target is tricked into replying and engaging.

Remote Access [T1219] Once remote access is installed on the employees machine, the attackers will seek to login to business applications that require multi factor authentication. This usually requires a second wave of social engineering in order to overcome the second factor of authentication.

**Defense Evasion**[TA0005]

Valid Account [T1078]:  In order to successfully login to business applications (with the intent to download sensitive data for exfiltration), the attackers must bypass multi-factor authentication. In the cases we have observed, the threat actor has achieved this in two ways. The employee whose machine was compromised may be socially engineered via a live spoofed phone call into entering multi factor authentication codes directly during a live session, and thus unwittingly provided access to applications while the attacker was remoted into the employee's machine. The attackers may also make repeated login attempts in order to create a wave of 'push notifications' to the target's mobile device, in the hope that the target just accepts one, without checking the validity of the login attempt. Since the attacker is using the employee's machine and the employee's credentials, there are no flags or security alerts triggered.  The attacker may also spoof an employee's phone number and call the target company's IT support desk to request a password reset or temporary removal of multi-factor authentication from certain applications. The justification may be that the employee has lost their phone and thus could not use their multi factor authentication application, or receive push notifications. The attackers will have done their reconnaissance and know the names of multiple employees of the help desk in order to head off any suspicion. The end goal is to convince the support team to temporarily deprecate the security controls of authentication of the employee whose machine is under the control of the attacker.

When successful, multifactor authentication is overcome, and access to critical business applications / data is achieved by the attacker.

**Exfiltration** [TA0010]

Exfiltration over Web Service [T1567]: In both cases, CRM applications, support ticketing applications, HR applications, and file server applications were searched and parsed, often with reporting functions utilized to create mass outputs from the applications. The velocity and specificity of the report generation demonstrate high level subject matter expertise with multiple common enterprise SaaS applications. The downloads are first saved locally, and then uploaded to common cloud storage services under the control of the threat actor.

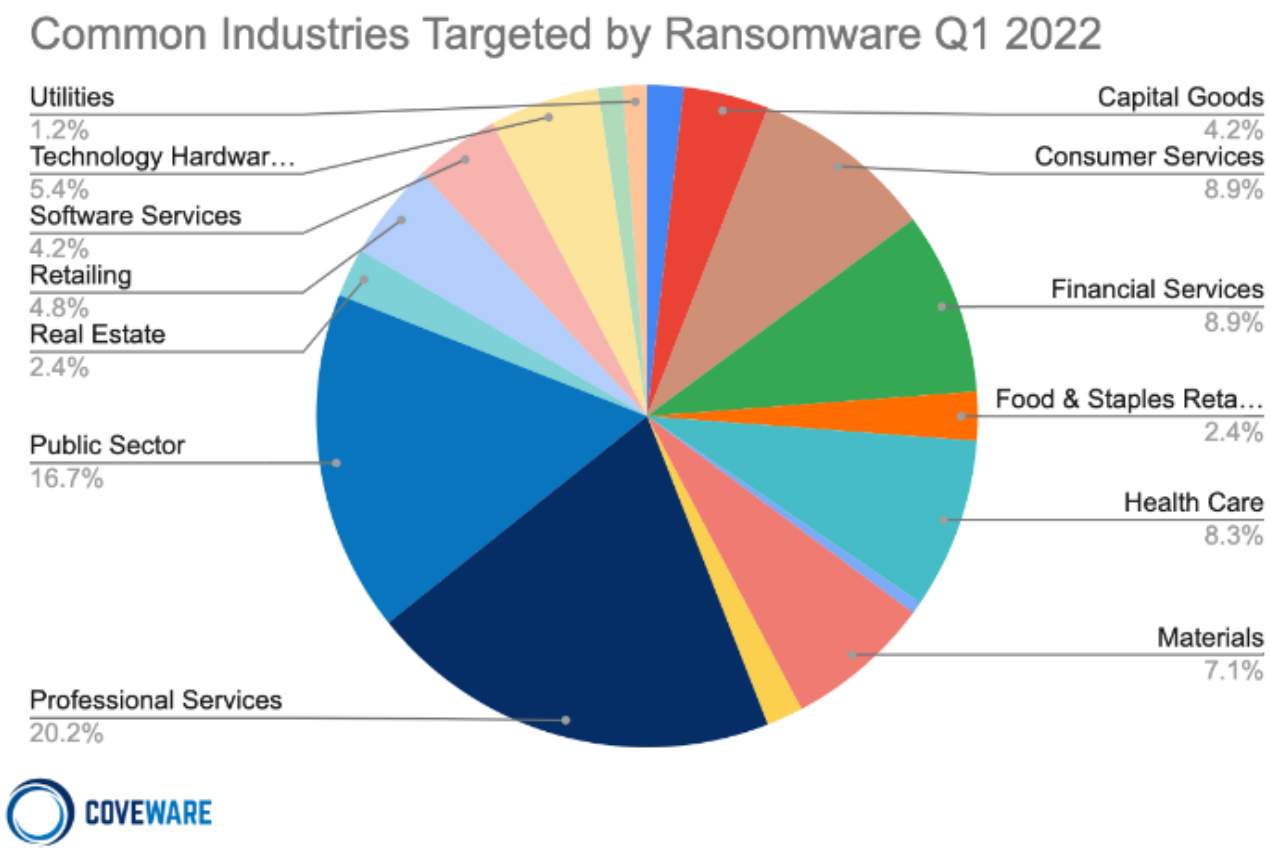
### Suggested Mitigations

These threat actor groups are using relatively bespoke techniques that involve neither malware nor noisy tactics. These tactics are designed to successfully overcome well implemented zero-trust networks with multi-factor authentication properly enabled on critical applications. Below are the two main mitigation strategies we cite that could have thwarted these attacks.

User Training [M1017]: While security awareness training is important for all employees, it is especially important for the IT helpdesk. Any inbound phone call that requests a password reset / deprecation / bypass should go through extra validation for legitimacy. In the cases we have handled, if the IT support team had dropped the initial inbound call (which was spoofed so the number appeared legitimate), and called the employee back on the phone number listed on an internal directory, the social engineering attempt would have been foiled. For additional security, any employee soliciting a password reset or changes to multifactor authentication should require the user to submit a selfie photo of them holding both their government issued ID and a piece of paper stating the request to temporarily suspend multifactor authentication. This ‘selfie’ method is commonly used within the crypto-currency exchange industry to validate the identity of users requesting lost access to hot wallet accounts. Given the prevalence of theft within the crypto-currency exchange industry, some of their best practices are worth studying.

Execution Prevention [M1038]: This threat actor relies on remotely accessing an employee’s work computer in order to bypass authentication protocols and login to SaaS applications. Preventing the installation of legitimate (but not approved) remote access tools such as TeamViewer, LogmeIn, or Go2assist would prevent this attacker from gaining initial access to a user’s machine.

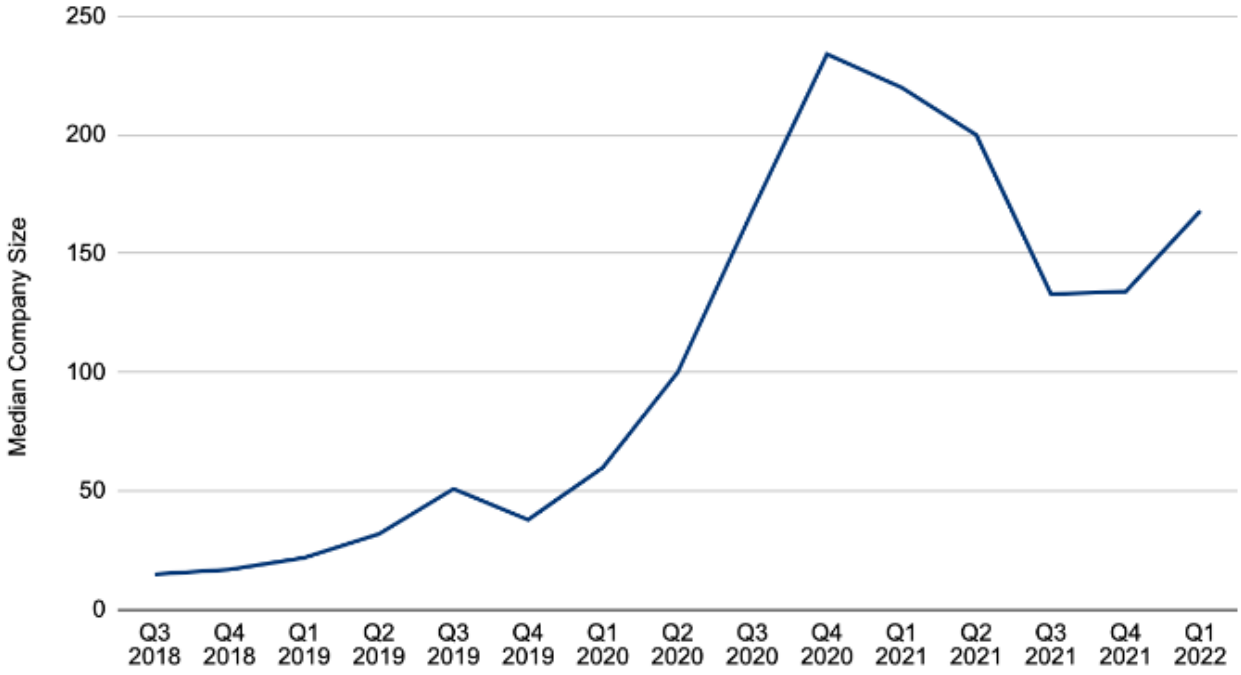
## Common Industries Impacted by Ransomware in Q1 2022




The largest change in industry concentration versus the fourth quarter of 2021 was a jump in attacks against the public sector. Public sector organizations continue to be soft targets for ransomware as they are chronically below the cybersecurity poverty line, and are often without the resources to adequately protect themselves. Legislative momentum at the state level has picked up a bit with North Carolina joining New York and Pennsylvania with state level prohibitions on using tax payor dollars to pay ransoms. It will be very interesting to monitor if this legal prohibition proves to be an effective deterrent or not.

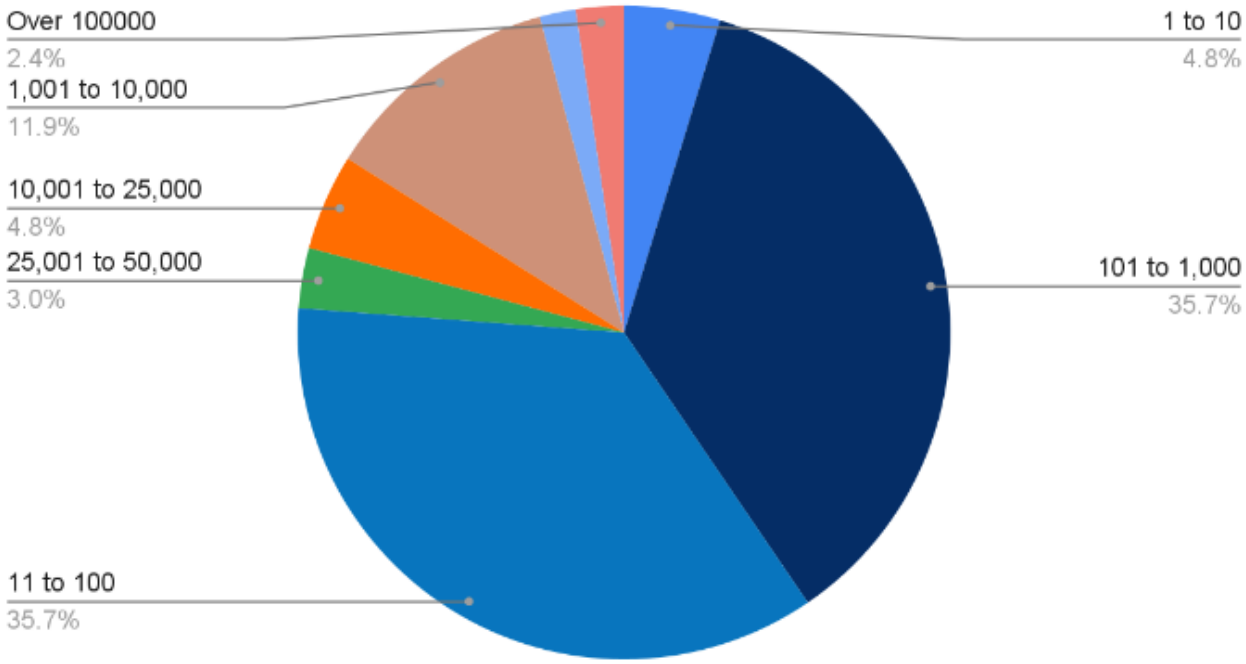
## Ransomware Victim Size in Q1 2022

## Median Size of Companies Targeted by Ransomware




COVEWARE

## Ransomware Impacted Companies by Size (Employee Count)




COVEWARE

Ransomware continues to predominantly be a small/medium sized business problem. As ransomware affiliates continue to move fluidly in a effort to stay off the radar of law enforcement, we expect the mid market to continue to bear the brunt of attacks as threat actors try to find a balance between NOT attacking companies so large as to end up in the papers, but also NOT attacking companies so small that they are not able to earn sufficient ransom proceeds. Given the average days of downtime reached 26 (+30% from Q4 2021), we hope that this strategy benefits these municipalities.