Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority

Web Clip

Rapport COVEWARE 2021

If you had told us at the beginning of 2021 that then President elect Biden would be having a nose to nose face off with Putin over ransomware, we would have speculated that some serious escalation must have occurred. In reality, the lackadaisical indifference of one threat actor (DarkSide) set off a compounding series of events that have led us to where we are today. Given the volume of attacks that Ransomware-as-a-service (RaaS) groups conduct, and the de minimis diligence that these groups perform, we are quite certain that the DarkSide affiliate that attacked Colonial Pipeline, had no idea that a) Colonial controlled 45% of the gasoline supply on the US east coast, b) that shutting down that pipeline would cause a consumer run on gasoline, c) that NOTHING gets voters and their duly elected representatives out of their chairs like rising gasoline prices, and finally d) that if you mess with US gasoline prices, you are going to get the attention of the President. Other high profile attacks that would have otherwise garnered 12 hours of media attention were (FINALLY) codified proof that the US indeed has a major problem with ransomware.

In reality, the volume and severity of ransomware attacks have been extreme but relatively stable for at least 18 months. The focus and attention could not come at a

better time, and the true scope of what US organizations and enterprises are up against may still not be fully appreciated. Ransomware groups now have operating budgets that may rival small nations themselves. For context, in late June, FBI Director Christopher Wray requested an additional $40 million for the FBI's cybersecurity budget. Coveware estimates that REvil alone may have collected close to $100 million in ransom payments in just the first 6 months of 2021. And that is one group. A note to anyone in Congress reading this, please add at least one zero to Director Wray's requested cyber budget. What will these groups do with these war chests? So far, we are seeing signs that some groups are moving up market and purchasing more expensive tools to compromise networks, even investing large dollars on single zero day vulnerabilities. CloP was one of the first groups to be observed purchasing a single appliance vulnerability in Q1, and it may turn out that REvil did something similar in their attack on Kaseya. This development is especially scary for well prepared enterprises. Previously, well prepared and secured enterprises could feel sufficiently de-risked if they were too expensive to compromise. While making oneself an expensive target is still the most effective way to avoid a catastrophic ransomware attack, the offensive operating budgets that these groups now carry enables them to spend more time and effort (read cost) attacking targets that they really have an eye for. This is a bad thing. In order to turn the tides of this fight, the economics of ransomware and cyber extortion need to be degraded. That is the only way to contract the volume and severity of these financially motivated crimes. While there is no single silver bullet, there is renewed focus and so far we think the efforts will be successful in containing the extortion economy. The economic lens can contextualize the efforts that we are

seeing unveiled. Any effort that increases the risk for ransomware threat actors, and lowers the profitability is helpful. These efforts will compound and have the potential to turn the tides. We would point out four major changes that have the potential to materially lower the volume of ransomware attacks in the future. Three of them are new as of Q2 2021:

1 - The Colonial hearings were a wake up call for enterprise CEO's: We sense that a lot of CEO's watched those hearings and immediately dialed their CISO with the directive of "spend whatever you need to spend to ensure I never end up in that situation." While money never solves all problems, responsibly increasing IT security spending in the right ways can materially lower the risk of a crippling ransomware attack, AND make attacks more expensive for threat actors to carry out. This is especially true of organizations that were previously very vulnerable. If the aggregate profitability of ransomware attacks decreases, the overall extortion economy will contract. Additionally, making attacks more costly to carry out raises the barrier to entry for new cyber criminals. Less attackers means less attacks.

2 - Ransomware has the attention of Heads of State: The level of state involvement is unprecedented in the history of cybercrime. Jason Healy has an excellent mapping on the Spectrum of State Responsibility for cyber crime, that has come into acute focus as pressure gets applied to foreign governments that may be condoning the activity from within their borders. Already, it has been widely speculated that the disappearance of the most prolific ransomware group REvil / Sodinokibi, may have been at least partly due to pressure from their native government. This pressure increases the risk for ransomware actors to possibly get in trouble on their home turf.

3 - Law Enforcement focus has sharpened: Following the recommendations of the IST Ransomware Task Force, the government and its many branches of law enforcement are reorganizing for a protracted focus on quelling ransomware. We should expect more arrests, infrastructure takedowns and general disruption of ransomware threat actor activities. This increases the risk of being a ransomware actor, and increases the costs for ransomware actors. Both intended effects will help in shrinking the cyber extortion economy.

4 - Cyber Insurance Underwriting standards are hardening: As claims for ransomware and other attacks have rolled in, the loss rates on many cyber insurance policies have far exceeded the original actuarial estimates. In response, premiums are rising, underwriting capacity is shrinking, and MOST importantly, underwriting diligence standards are hardening significantly. Most enterprises HAVE to hold a cyber insurance policy to be in compliance with normal customer and counterparty agreements. Non-renewal is not an option. Much of the new standards of underwriting revolve around basic security requirements such as multi-factor authentication, network segmentation, EDR use, and BCDR. The renewal cycle is forcing relatively less secure enterprises that need their cyber policy, to enact security and continuity reforms. This cycle will take 9-12 months, but should harden a large proportion of the mid-large enterprise market. When companies become harder to attack, the cost of carrying out attacks increases which lowers the profitability of the cyber extortion industry. It also raises the barrier to entry for cyber criminals as more technical sophistication, or more expensive ingress methods are required in order to compromise a hardened network.

In addition to the above which are already in motion and having an impact, there is also the potential for new

regulation. Already, several states have drafted proposed legislation that ranges from a complete prohibition on ransom payments, to mandatory reporting. Mandatory federal reporting of any ransom payment, along with submitting a standardized subset of incident data would have a positive impact on the government's grasp of the problem, and create a decreased propensity for victims to pay.

Average and Median Ransom Payment Amounts Declined in Q2 2021

Average Ransom Payment

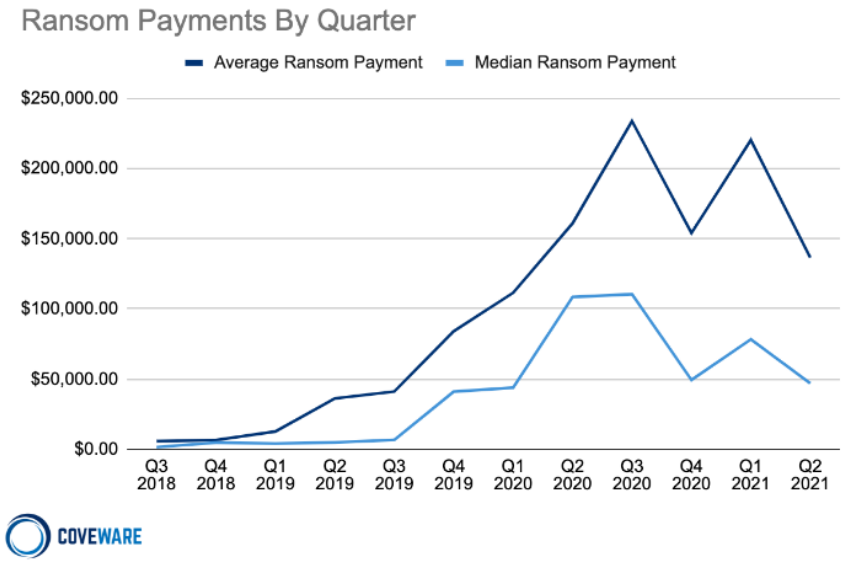
$136,576

-38% from Q1 2021

Median Ransom Payment

$47,008

-40% from Q1 2021



Average and Median Ransom Payments

The average ransom payment declined to $136,576 while the median fell to $47,008, levels not seen since the beginning of 2021. The decrease was primarily driven by a growing number of disparate Ransomware-as-a-Service brands that have proliferated recently, and which have diluted the concentration of attacks controlled by just a few. The lower prevalence of several groups that have historically made some of the highest demands (such as Ryuk and Clop) allowed the average and median ransom payment to drift lower during the quarter. Additionally, the efficacy of data exfiltration as an overall tactic appears to also be diminishing. During Q2, over 80% of ransomware attacks also included the threat to leak stolen data.

81% of Ransomware Attacks Involved the Threat to Leak Exfiltrated Data (+5% From Q1 2021)

Despite the prevalence of the tactic, fewer organizations that are JUST facing a data exfiltration threat (i.e. they are not concerned or impacted by encrypted files or data loss) are opting to pay a ransom. In 2020, almost 65% of victims that were just faced with a data leak threat opted to pay, despite the reality that paying to suppress a leak provides almost zero value. In Q2, only 50% of data leak victims opted to pay. We hope to see this trend continue until the percentage reaches zero. We feel very strongly that mandatory federal reporting of a ransom payment will have a positive material impact on this as well. Mandatory reporting may not seem like a major forcing function, but piercing the veil of disclosure will tilt the mindset of decision makers further away from making this specific kind of payment.

Most Common Ransomware Variants in Q2 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q1 2021
1	Sodinokibi	16.5%	-
2	Conti V2	14.4%	-
3	Avaddon	5.4%	+3

4	Mespinoza	4.9%	New in Top Variants
5	Hello Kitty	4.5%	New in Top Variants
6	Ryuk	3.7%	+1
7	Clop	3.3%	-3
8	THT v2	2.9%	New in Top Variants
9	LV	2.5%	New in Top Variants
9	Zeppelin	2.5%	New in Top Variants

Top 10: Market Share of the Ransomware attacks

The Sodinokibi variant of ransomware was the most common in Q2, but as of the date of this report's release, the group appears to have evaporated following a string of high profile attacks during the second quarter. It is not our role to speculate on the why and how, but we will remind readers of two facts. First, Sodinokibi is widely believed to be the predecessor project of GandKrab, which 'retired' in 2019. Sodinokibi was first spotted in the wild 2 weeks BEFORE GandKrab announced their retirement. We do not expect this group to remain on the bench for long. Secondly, like most other variants, Sodinokibi was a Ransomware-as-a-Service operation, with a close knit group of affiliates. Those affiliates have likely already found new RaaS operations to leverage in their attacks. We expect that RaaS operations offering Linux encryptors will attract new affiliates. We have also seen early evidence of cross variant use of Hello Kitty's linux binary in several other attacks that involved a different type of ransomware binary used on the Window's environment. The fluidity with which affiliates are able to move between variants, picking and choosing which parts they favor, attribution will become increasingly complex for incident responders.

If you had told us at the beginning of 2021 that then President elect Biden would be having a nose to nose face off with Putin over ransomware, we would have speculated that some serious escalation must have occurred. In reality, the lackadaisical indifference of one threat actor (DarkSide) set off a compounding series of events that have led us to where we are today. Given the volume of attacks that Ransomware-as-a-service (RaaS) groups conduct, and the de minimis diligence that these groups perform, we are quite certain that the DarkSide affiliate that attacked Colonial Pipeline, had no idea that a) Colonial controlled 45% of the gasoline supply on the US east coast, b) that shutting down that pipeline would cause a consumer run on gasoline, c) that NOTHING gets voters and their duly elected representatives out of their chairs like rising gasoline prices, and finally d) that if you mess with US gasoline prices, you are going to get the attention of the President. Other high profile attacks that would have otherwise garnered 12 hours of media attention were (FINALLY) codified proof that the US indeed has a major problem with ransomware.

In reality, the volume and severity of ransomware attacks have been extreme but relatively stable for at least 18 months. The focus and attention could not come at a better time, and the true scope of what US organizations and enterprises are up against may still not be fully appreciated. Ransomware groups now have operating budgets that may rival small nations themselves. For context, in late June, FBI Director Christopher Wray requested an additional $40 million for the FBI's cybersecurity budget. Coveware estimates that REvil alone may have collected close to $100 million in ransom

payments in just the first 6 months of 2021. And that is one group. A note to anyone in Congress reading this, please add at least one zero to Director Wray's requested cyber budget. What will these groups do with these war chests? So far, we are seeing signs that some groups are moving up market and purchasing more expensive tools to compromise networks, even investing large dollars on single zero day vulnerabilities. CloP was one of the first groups to be observed purchasing a single appliance vulnerability in Q1, and it may turn out that REvil did something similar in their attack on Kaseya. This development is especially scary for well prepared enterprises. Previously, well prepared and secured enterprises could feel sufficiently de-risked if they were too expensive to compromise. While making oneself an expensive target is still the most effective way to avoid a catastrophic ransomware attack, the offensive operating budgets that these groups now carry enables them to spend more time and effort (read cost) attacking targets that they really have an eye for. This is a bad thing. In order to turn the tides of this fight, the economics of ransomware and cyber extortion need to be degraded. That is the only way to contract the volume and severity of these financially motivated crimes. While there is no single silver bullet, there is renewed focus and so far we think the efforts will be successful in containing the extortion economy. The economic lens can contextualize the efforts that we are seeing unveiled. Any effort that increases the risk for ransomware threat actors, and lowers the profitability is helpful. These efforts will compound and have the potential to turn the tides. We would point out four major changes that have the potential to materially lower the volume of ransomware attacks in the future. Three of them are new as of Q2 2021:

1 - The Colonial hearings were a wake up call for enterprise CEO's: We sense that a lot of CEO's watched those hearings and immediately dialed their CISO with the directive of "spend whatever you need to spend to ensure I never end up in that situation." While money never solves all problems, responsibly increasing IT security spending in the right ways can materially lower the risk of a crippling ransomware attack, AND make attacks more expensive for threat actors to carry out. This is especially true of organizations that were previously very vulnerable. If the aggregate profitability of ransomware attacks decreases, the overall extortion economy will contract. Additionally, making attacks more costly to carry out raises the barrier to entry for new cyber criminals. Less attackers means less attacks.

2 - Ransomware has the attention of Heads of State: The level of state involvement is unprecedented in the history of cybercrime. Jason Healy has an excellent mapping on the Spectrum of State Responsibility for cyber crime, that has come into acute focus as pressure gets applied to foreign governments that may be condoning the activity from within their borders. Already, it has been widely speculated that the disappearance of the most prolific ransomware group REvil / Sodinokibi, may have been at least partly due to pressure from their native government. This pressure increases the risk for ransomware actors to possibly get in trouble on their home turf.