Blockchain Analysis Shows Connections Between Four of 2020’s Biggest Ransomware Strains

blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer

Chainalysis Team

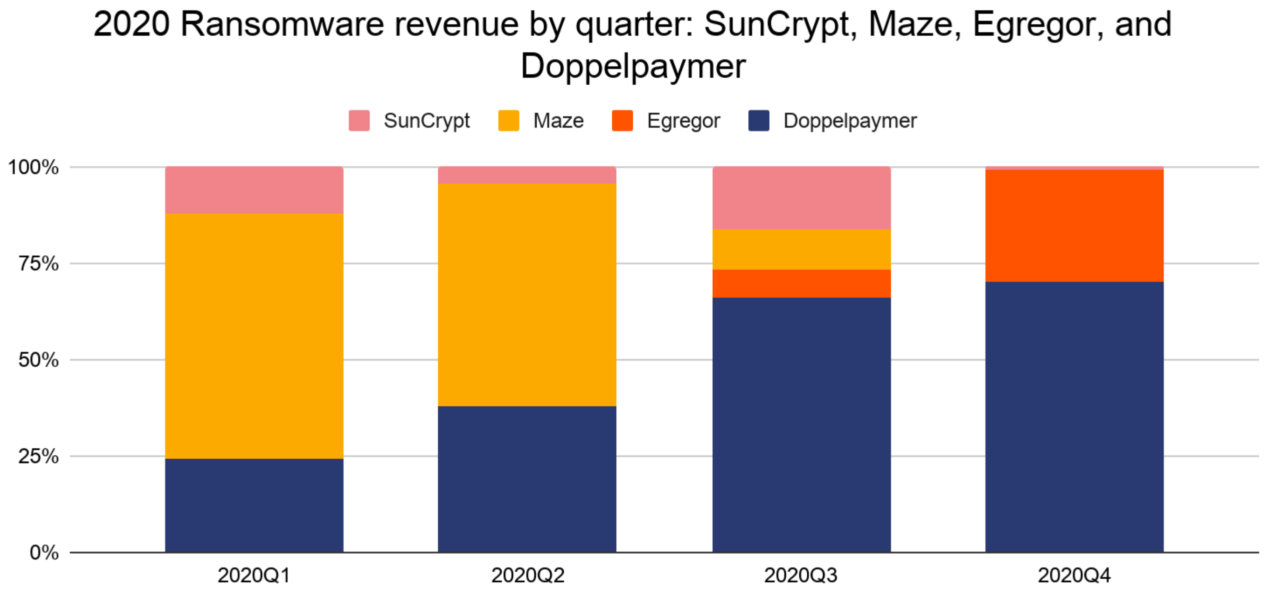
February 4, 2021

This blog is an excerpt from the Chainalysis 2021 Crypto Crime Report. Click here to download the whole thing!

As we’ve covered on our blog, there may be fewer cybercriminals responsible for ransomware attacks than one would initially think given the number of individual attacks, distinct strains, and amount stolen from victims. Cybersecurity researchers point out that many RaaS affiliates carrying out attacks switch between different strains, and many believe that seemingly distinct strains are actually controlled by the same people. Using blockchain analysis, we’ll investigate potential connections between four of 2020’s most prominent ransomware strains: Maze, Egregor, SunCrypt, and Doppelpaymer.

The four ransomware strains were quite active last year, attacking prominent companies such as Barnes & Noble, LG, Pemex, and University Hospital New Jersey, amongst others. All four use the RaaS model, meaning that affiliates carry out the ransomware attacks themselves and pay a percentage of each victim payment back to the strain’s creators and administrators. All four also use the "double extortion" strategy of not just withholding victims' data, but also publishing pieces of it online as an extra incentive for victims to pay the ransom.

Below, we see the four strains' revenue since late 2019 broken out quarterly.

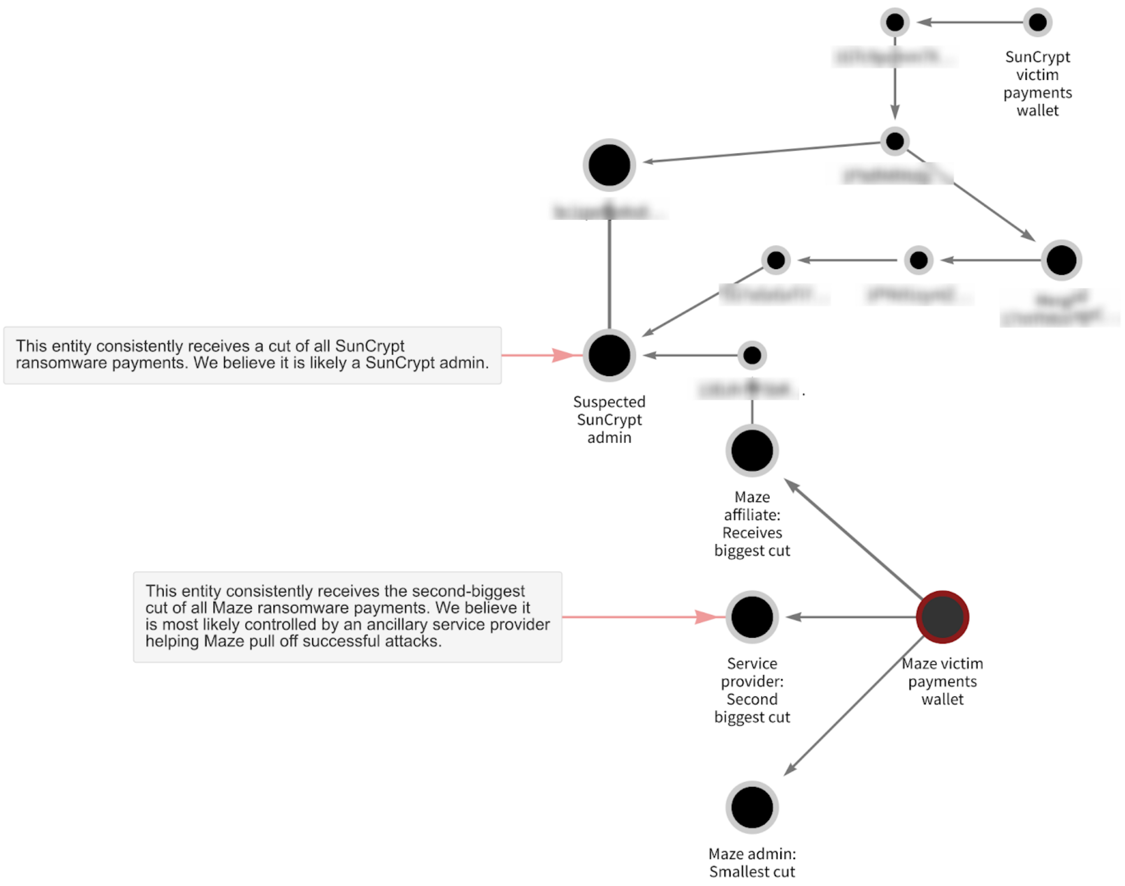


Note that Egregor only became active just before Q4 2020 (mid-September to be specific), soon after the Maze strain became inactive. Some cybersecurity researchers see this as evidence that Maze and Egregor are linked in some way. In early November, Maze's operators said the strain was shutting down in a press release posted to its website, following a slowdown in activity. Soon after, most of its affiliates migrated to Egregor, leading some to believe that the Maze operators have simply rebranded as Egregor and instructed the affiliates to join. This is relatively common in ransomware, though it's also possible that the affiliates have decided for themselves that Egregor is their best option. It's even possible that the Maze affiliates became unhappy with the Maze operators, leading to the split. However, as noted by Bleeping Computer, Maze and Egregor share much of the same code, the same ransom note, and have very similar victim payment sites. Cybersecurity firm Recorded Future notes this too, as well as similarities between Egregor and a banking trojan called QakBot.

It's not just Egregor either. In another story, Bleeping Computer claims that Suncrypt representatives contacted them claiming to be part of the "Maze ransomware cartel" prior to Maze's shutdown announcement, though Maze has denied this. However, the claim of a connection is also supported by a privately circulated report from threat intelligence firm Intel471 claiming that representatives from SunCrypt described their strain as a "rewritten and rebranded version of a 'well-known' ransomware strain." Intel471's report also claims that SunCrypt only works with a small number of affiliates at a time, whom the SunCrypt operators interview and vet extensively. Therefore, we believe any overlap in affiliates between SunCrypt and other ransomware strains would be more likely to suggest a deeper connection between the two strains, rather than just coincidence.

Blockchain analysis suggests affiliate overlap and other possible connections between Maze, Egregor, SunCrypt, and Doppelpaymer

As we outline above, there’s circumstantial evidence suggesting links between some of these four strains, as well as reports of affiliate migration. But what links do we see on the blockchain? Let’s start with Maze and SunCrypt.


SunCrypt victim payments wallet
Suspected SunCrypt admin
Maze affiliate: Receives biggest cut
Service provider: Second biggest cut
Maze victim payments wallet
Maze admin: Smallest cut

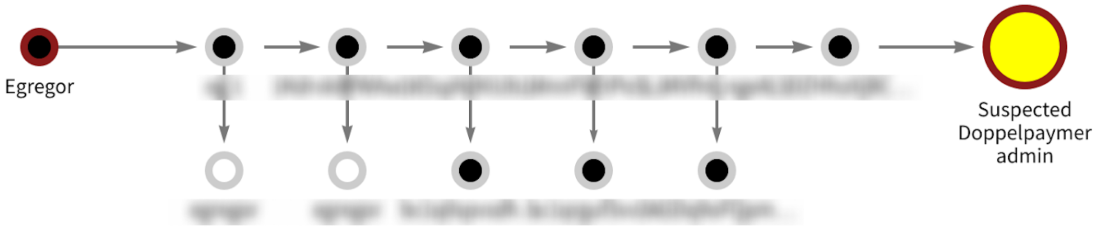
This entity consistently receives a cut of all SunCrypt ransomware payments. We believe it is likely a SunCrypt admin.

This entity consistently receives the second-biggest cut of all Maze ransomware payments. We believe it is most likely controlled by an ancillary service provider helping Maze pull off successful attacks.

The Chainalysis Reactor graph above provides strong evidence suggesting that a Maze ransomware affiliate is also an affiliate for SunCrypt. Starting at the bottom of the graph, we see how Maze distributes funds taken in ransomware attacks. First, the majority of each successful ransom payment goes to the affiliate, as they’re taking on the risk of actually carrying out the ransomware attack. The next biggest cut goes to a third party. While we can’t know for sure what that third party’s role is, we believe it’s likely an ancillary service provider who helps Maze pull off attacks. Ransomware attackers often rely on third parties for tools like bulletproof hosting, penetration testing services, or access to vulnerabilities in victims' networks. These ancillary service providers can be found peddling their wares on cybercriminal darknet forums, but aren't necessarily involved in all ransomware attacks. Finally, the smallest cut of each ransom payment goes to another wallet that we believe belongs to the strain's administrators.

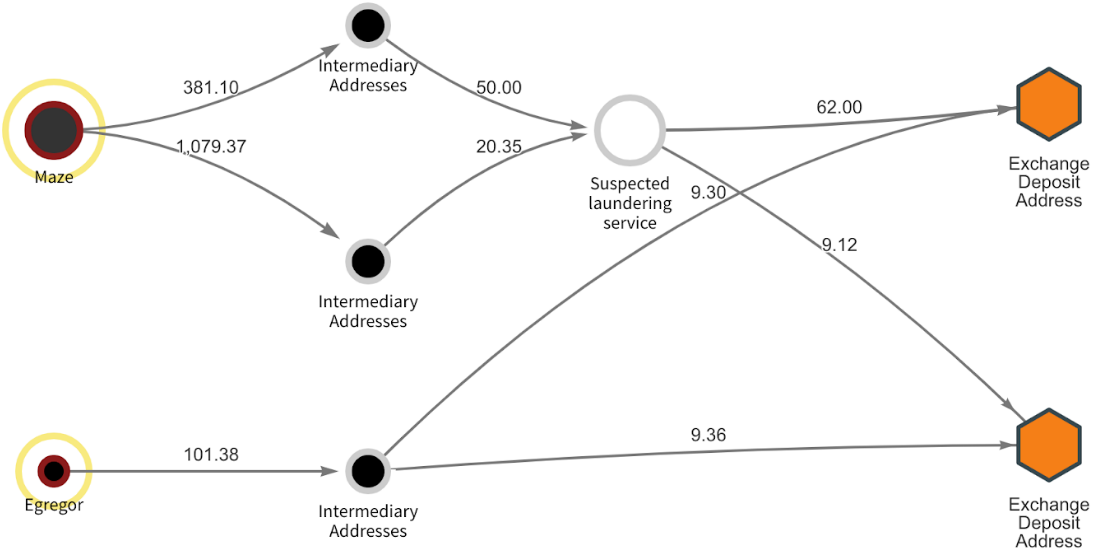
In this case, however, we see that the Maze affiliate also sent funds — roughly 9.55 Bitcoin worth over $90,000 — via an intermediary wallet to an address labeled "Suspected SunCrypt admin," which we've identified as part of a wallet that has consolidated funds related to a few different SunCrypt attacks. This suggests that the Maze affiliate is also an affiliate for SunCrypt, or possibly involved with SunCrypt in another way.

Another Reactor graph shows links between the Egregor and Doppelpaymer ransomware strains.



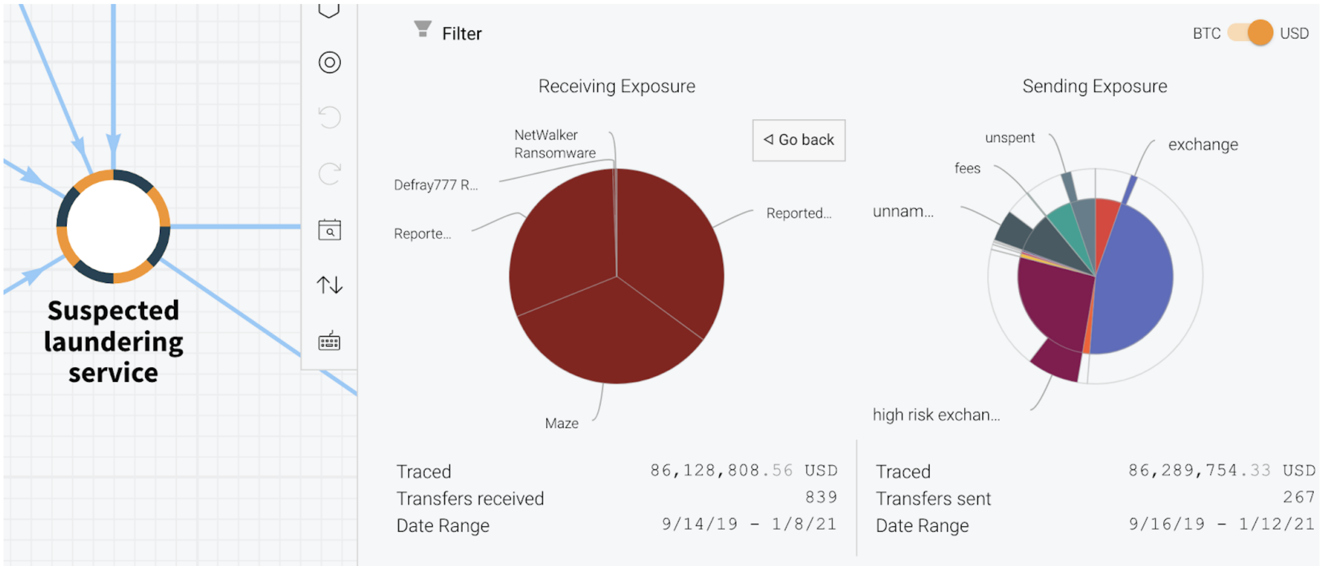
In this case, we see that an Egregor wallet sent roughly 78.9 BTC worth approximately $850,000 to a suspected Doppelpaymer administrator wallet. Though we can't know for sure, we believe that this is another example of affiliate overlap. Our hypothesis is that the Egregor-labeled wallet is an affiliate for both strains sending funds to the Doppelpaymer administrators.

Finally, the Reactor graph below shows what we believe is an instance of Maze and Egregor administrators using the same money laundering infrastructure.



Both strains' victim payments' wallets have sent funds to two deposit addresses at a prominent cryptocurrency exchange via intermediary wallets. Based on their transaction patterns, we believe that both deposit addresses belong to over-the-counter (OTC) brokers who specialize in helping ransomware operators and other cybercriminals trade illicitly-gained cryptocurrency for cash. In the case of Maze, those funds first flow through another suspected money laundering service before reaching the OTC addresses — it's unclear whether Maze receives cash from that service or from the OTCs themselves, and it's also possible that the OTC broker and those running the laundering service are one in the same.

While this doesn't suggest that Maze and Egregor share the same administrators or affiliates, it's still an important potential lead for law enforcement. Cryptocurrency-related crime isn't worthwhile if there's no way to convert ill-gotten funds into cash. By going after bad actors like the money laundering service or corrupt OTC brokers on the graph above — the latter of whom, again, operate on a large, well-known exchange — law enforcement could significantly hamper the ability of Maze and Egregor to operate profitably without actually catching the strains' administrators or affiliates. It's not just those specific ransomware strains either.



Traced 86,128,808.56 USD
Transfers received 839
Date Range 9/14/19 - 1/8/21

Traced 86,289,754.33 USD
Transfers sent 267
Date Range 9/16/19 - 1/12/21

The suspected laundering service has also received funds from the Doppelpaymer, WastedLocker, and Netwalker ransomware strains, taking in nearly $2.9 million worth of cryptocurrency from the category as a whole. Likewise, it's received nearly $650,000 worth of cryptocurrency from darknet markets such as Hydra and FEShop. The two OTC broker addresses on the graph have similar criminal exposure as well.

What does this mean for ransomware?

While we can't say for sure that Maze, Egregor, SunCrypt, or Doppelpaymer have the same administrators, we can say with relative certainty that some of them have affiliates in common. We also know that Maze and Egregor rely on the same OTC brokers to convert cryptocurrency into cash, though they interact with those brokers in different ways.

Regardless of the exact depth and nature of these connections, the evidence suggests that the ransomware world is smaller than one may initially think given the number of unique strains currently operating. This information can be a force multiplier for law enforcement. If they can identify and act against groups controlling multiple ransomware strains, or against OTCs enabling multiple ransomware strains to cash out their earnings, then they'll be able to halt or impact the operations of several strains with one takedown.

This blog is an excerpt from the Chainalysis 2021 Crypto Crime Report. Click here to download the whole thing!