Origins and Adversaries, Pt. 2

crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/

The CrowdStrike Intel Team October 6, 2020

As data leak extortion swiftly became the new norm for big game hunting (BGH) ransomware operators since late 2019, various criminal adversaries began innovating in this area. This includes collaboration between ransomware groups, auctioning leaked data and demanding not just one ransom for the ransomware decryptor but also a second ransom to ensure stolen data is deleted.

The first part of this two-part blog series explored the origins of ransomware, BGH and extortion and introduced some of the criminal adversaries that are currently dominating the data leak extortion ecosystem. This blog explores operators of *Ako* (a fork of *MedusaLocker*) demanding two ransoms from victims, PINCHY SPIDER's auctioning of stolen data and TWISTED SPIDER's creation of the self-named "Maze Cartel."

Twice the Price: Ako Operators Demand Separate Ransoms

In May 2020, CrowdStrike® Intelligence observed an update to the *Ako* ransomware portal. Similar to many other ransomware operators, the threat actors added a link to their dedicated leak site (DLS), as shown in Figure 1. What makes this DLS interesting is an indication that

the threat actors were likely issuing two ransom demands: one for the victim to obtain the decryption key and a second to delete the exfiltrated data from the DLS.

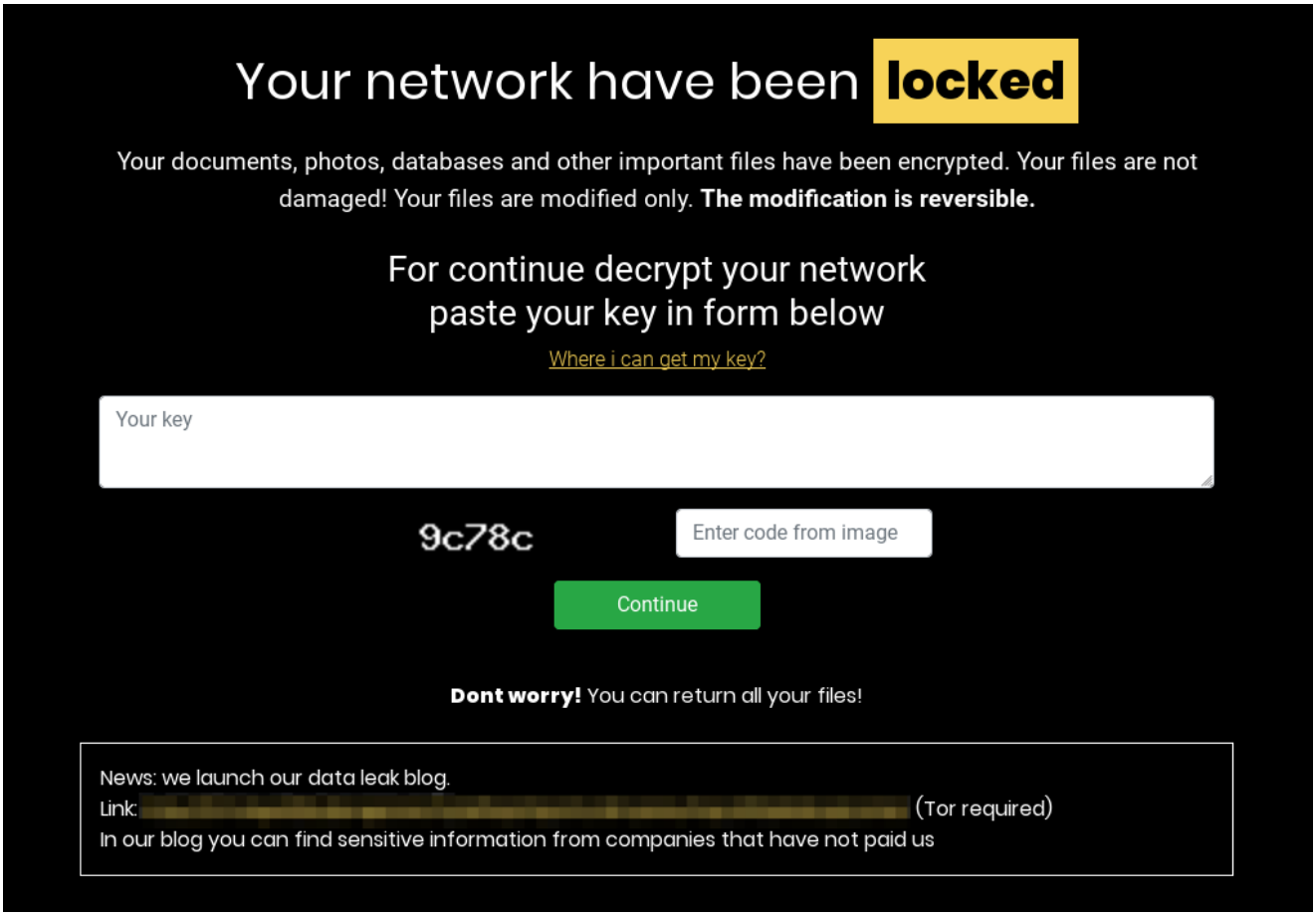

Figure 1. Updated *Ako* ransom portal

One of the threat actor posts (involving a U.S.-based engineering company) included the following comment:

Got only payment for decrypt – 350,000$
Payment for delete stolen files was not received.

While it appears that the victim paid the threat actors for the decryption key, the exfiltrated data was still published on the DLS. This inclusion of a ransom demand for the exfiltrated data is not yet commonly seen across ransomware families.

Going Once, Twice — Sold!

On June 2, 2020, CrowdStrike Intelligence observed PINCHY SPIDER introduce a new auction feature to their *REvil* DLS. This feature allows users to bid for leak data or purchase the data immediately for a specified "Blitz Price." Payments are only accepted in Monero (XMR) cryptocurrency. These auctions are listed in a specific section of the DLS, which provides a list of available and previously expired auctions. Each auction title corresponds to the company the data has been exfiltrated from and contains a countdown timer providing

the time remaining before the auction expires (Figure 2). Once the auction expires, PINCHY SPIDER typically provides a link to the company's data, which can be downloaded from a public file distribution website.

In order to place a bid or pay the provided Blitz Price, the bidder is required to register for a particular leak auction. When a leak auction title is clicked, it takes the bidder to a detailed page containing "Login" and "Registration" buttons, as shown in Figure 2.

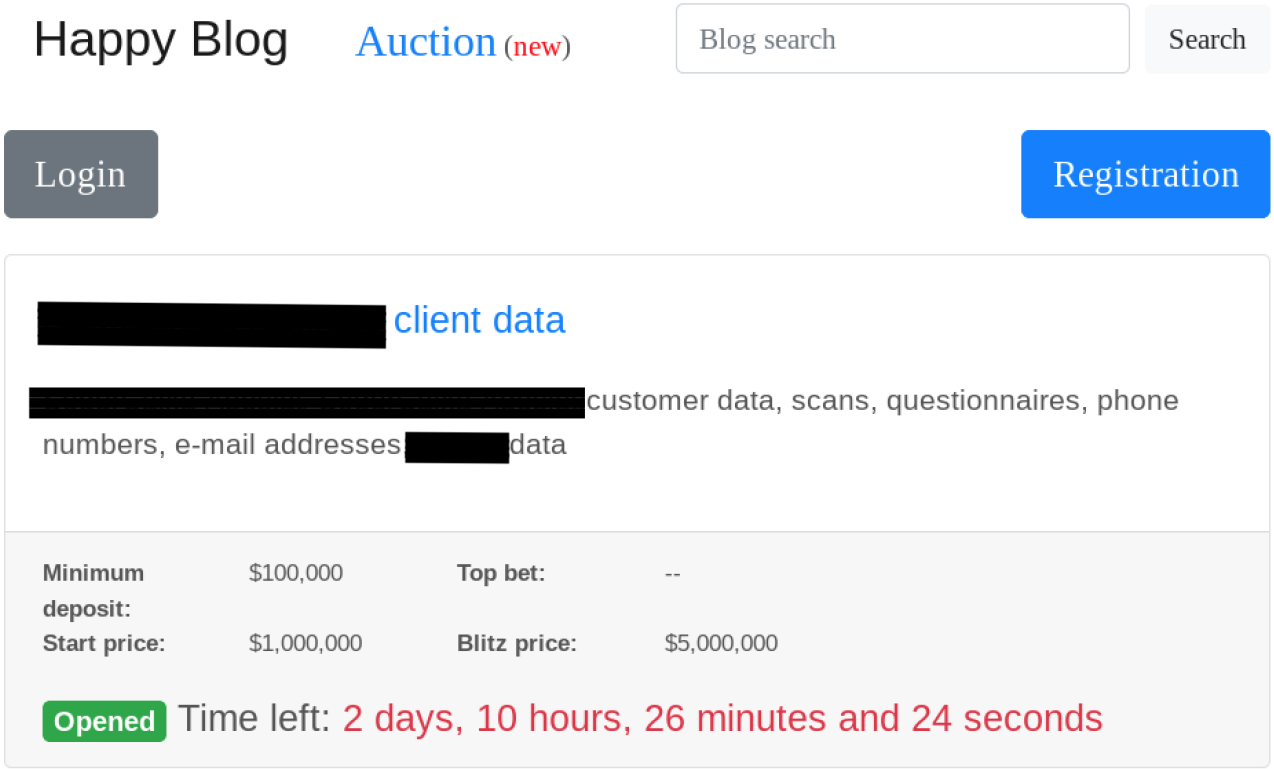

Figure 2. Detailed leak auction page

The "Login" button can be used to log in as a previously registered user, and the "Registration" button provides a generated username and password for the auction session. Once the bidder is authenticated for a particular auction, the resulting page displays auction deposit amounts, starting auction price, ending auction price, an XMR address to send transactions to, a listing of transactions to that address, and the time left until the auction expires, as shown in Figure 3.

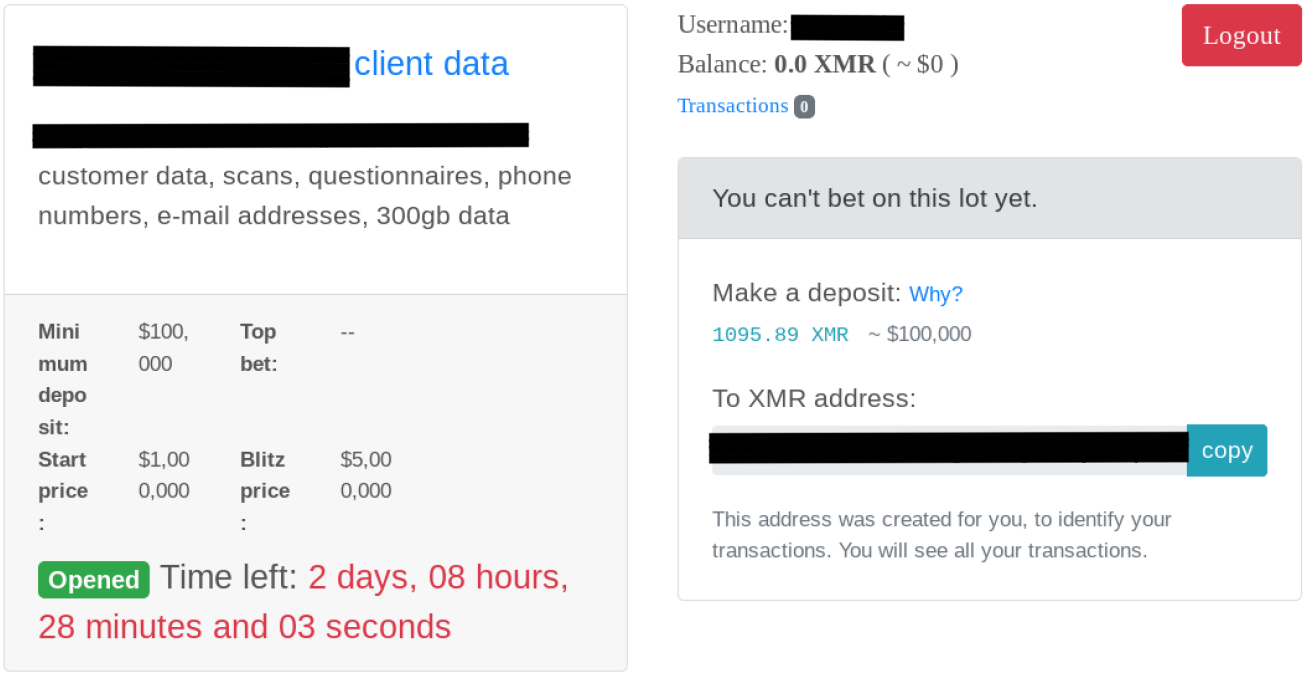

Figure 3. Registered user leak auction page

A minimum deposit needs to be made to the provided XMR address in order to make a bid. If the bidder is outbid, then the deposit is returned to the original bidder. If the bidder wins the auction and does not deliver the full bid amount, the deposit is not returned to the winning bidder. This protects PINCHY SPIDER from fraudulent bids, while providing confidence to legitimate bidders that they will have their money returned upon losing a bid. In theory, PINCHY SPIDER could refrain from returning bids, but this would break the trust of bidders in the future, thus hindering this avenue as an income stream.

At the time of this writing, CrowdStrike Intelligence had not observed any of the auctions initiated by PINCHY SPIDER result in payments. If users are not willing to bid on leaked information, this business model will not suffice as an income stream. Additionally, PINCHY SPIDER's willingness to release the information after the auction has expired, which effectively provides the data for free, may have a negative impact on the business model if those seeking the information are willing to have the information go public prior to accessing it.

Enter the Labyrinth: Maze Cartel Encourages Criminal Collaboration

In June 2020, TWISTED SPIDER, the threat actor operating *Maze* ransomware, introduced a new twist to their ransomware operations by announcing the creation of the "Maze Cartel" — a collaboration between certain ransomware operators that results in victims' exfiltrated information being hosted on multiple DLSs, as shown in Figure 4.

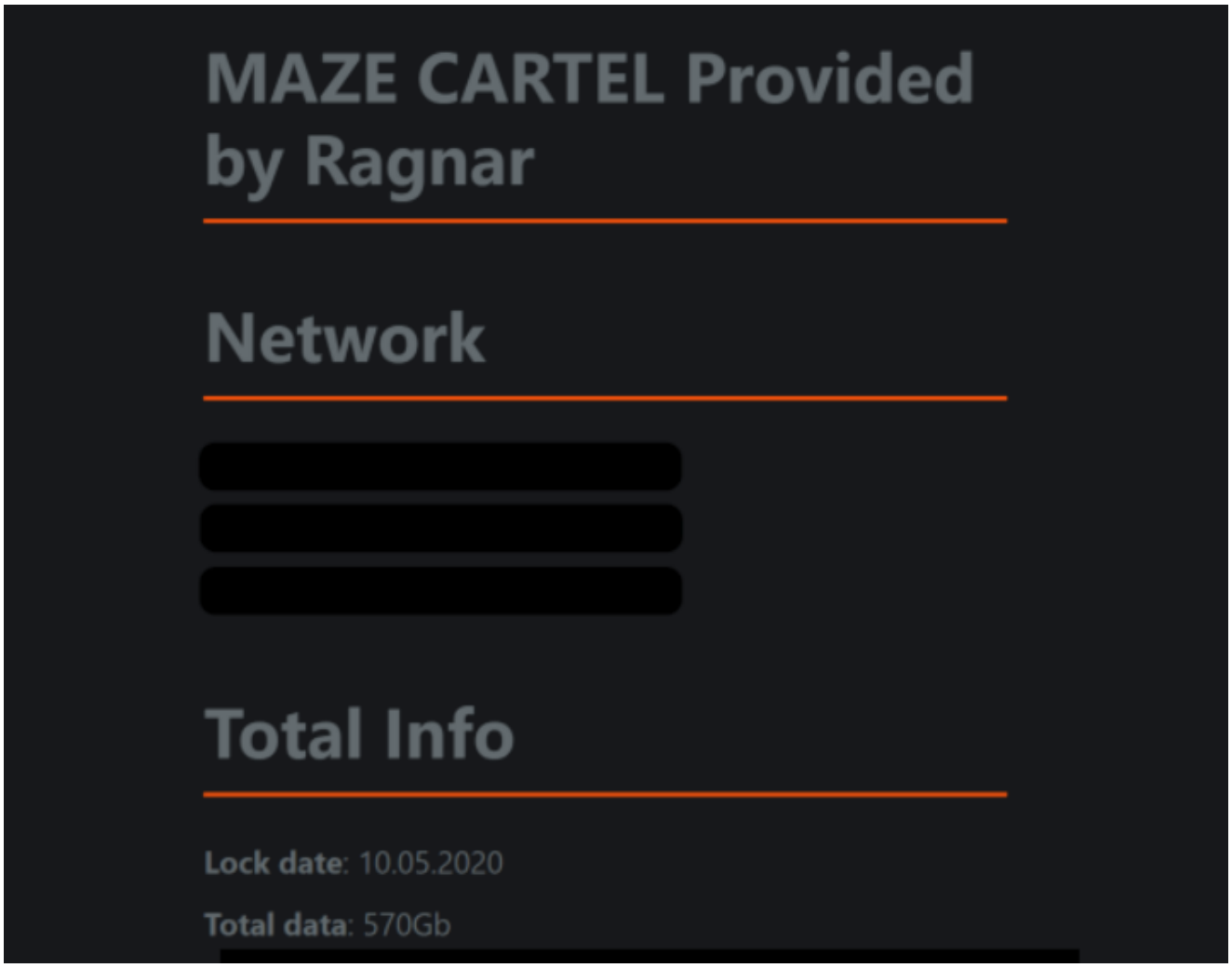

Figure 4. Screenshot of TWISTED SPIDER's DLS implicating the Maze Cartel

To date, the Maze Cartel is confirmed to consist of TWISTED SPIDER, VIKING SPIDER (the operators of *Ragnar Locker*) and the operators of *LockBit*. Data-sharing activity observed by CrowdStrike Intelligence is displayed in Table 1.

Victim	Ransomware Variant Involved	Data Hosted By (and Date)
U.S.-based engineering company	*LockBit*	TWISTED SPIDER (June 1)
U.S.-based media and marketing company	VIKING SPIDER's *Ragnar Locker*	TWISTED SPIDER (June 8)
U.S.-based engineering company	TWISTED SPIDER's *Maze*	TWISTED SPIDER (June 5) VIKING SPIDER (June 11)

Table 1. Maze Cartel data-sharing activity to date

In August 2020, operators of *SunCrypt* ransomware claimed they were a new addition to the Maze Cartel — the claim was refuted by TWISTED SPIDER. Duplication of a Norway-based victim's details on both the TWISTED SPIDER DLS and *SunCrypt* DLS contributed to theories the adversaries were collaborating, though the data was also available on criminal forums at the time it appeared on *SunCrypt's* DLS.

Also in August 2020, details of two victims were duplicated on both TWISTED SPIDER's DLS and WIZARD SPIDER's *Conti* DLS, resulting in theories that WIZARD SPIDER is a new addition to the Maze Cartel. However, TWISTED SPIDER made no reference to the inclusion of WIZARD SPIDER, and the duplication is potentially the result of the victims facing two intrusions by separate ransomware actors, or data being sold by WIZARD SPIDER to other threat actors.

The exact nature of the collaboration between Maze Cartel's members is unconfirmed; it is unknown if the actors actively participate in the same operations. Some of the actors share similar tactics, techniques and procedures (TTPs), including an initial aversion to targeting frontline healthcare facilities during the COVID-19 pandemic, and there are indications that adversaries are emulating successful techniques demonstrated by other members of the cartel[1]. The Maze Cartel creates benefits for the adversaries involved, and potential pitfalls for victims. Less-established operators can host data on a more-established DLS, reducing the risk of the data being taken offline by a public hosting provider. TWISTED SPIDER's reputation as a prolific ransomware operator arguably bolsters the reputation of the newer operators and could encourage the victim to pay the ransom demand. A yet-to-be-seen but realistic threat is that victims whose data is hosted in multiple locations could face negotiations with multiple ransomware operators, potentially increasing the price of the ransom to ensure the data's removal and destruction.

Conclusion

Collaboration between eCrime operators is not uncommon — for example, WIZARD SPIDER has a historically profitable arrangement involving the distribution of *TrickBot* by MUMMY SPIDER in *Emotet* spam campaigns. However, the apparent collaboration between members of the Maze Cartel is more unusual and has the potential to alter the TTPs used in the ransomware threat landscape. Collaboration between operators may also place additional pressure on the victim to meet the ransom demand, as the stolen data has gained increased publicity and has already been shared at least once. To date, the collaboration appears to focus on data sharing, but should the collaboration escalate into combined or consecutive ransomware operations, then the fallout and impact on victims could become significantly higher.

The auctioning of victim data enables the monetization of exfiltrated data when victims are not willing to pay ransoms, while incentivizing the original victims to pay the ransom amount in order to prevent the information from going public. Double ransoms potentially increase

the amount of money a ransomware operator can collect, but should the operators demand the ransoms separately, victims may be more willing to pay for the deletion of data where receiving decryptors is not a concern. As eCrime adversaries seek to further monetize their efforts, these trends will likely continue, with the auctioning of data occurring regardless of whether or not the original ransom is paid.

The collaboration between Maze Cartel members and the auction feature on PINCHY SPIDER's DLS may be combined in the future. It is possible that a criminal marketplace may be created for ransomware operators to sell or auction data, share techniques and even sell access to victims if they don't have the time or capability to conduct such operations. CrowdStrike Intelligence has previously observed actors selling access to organizations on criminal underground forums. However, these advertisements do not appear to be restricted to ransomware operations and could instead enable espionage and other nefarious activity.

These evolutions in data leak extortion techniques demonstrate the drive of these criminal actors to capitalize on their capabilities and increase monetization wherever possible. The overall trend of exfiltrating, selling and outright leaking victim data will likely continue as long as organizations are willing to pay ransoms. These tactics enable criminal actors to capitalize on their efforts, even when companies have procedures in place to recover their data and are able to remove the actors from their environments.

Currently, the best protection against ransomware-related data leaks is prevention. Security solutions such as the CrowdStrike Falcon® endpoint protection platform come with many preventive features to protect against threats like those outlined in this blog series. With features that include machine learning, behavioral preventions and executable quarantining, the Falcon platform has proven to be highly effective at stopping ransomware and other common techniques criminal organizations employ.

This blog was written by CrowdStrike Intelligence analysts Zoe Shewell, Josh Reynolds, Sean Wilson and Molly Lane.

1. https[:]//news.sophos[.]com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

Additional Resources

- *Read the first blog in this two-part series: "Double Trouble: Ransomware with Data Leak Extortion, Part 1."*
- *Download the CrowdStrike 2020 Global Threat Report.*
- *To learn more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*