# Leakware-Ransomware-Hybrid Attacks

hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

Security Lab October 23, 2020


## Summary: Leakware-Ransomware Hybrids

Since December 2019, ransomware operators have been using leakware/ransomware hybrid attacks more and more often. These attacks combine the classic ransomware attack with a leakware attack. In a classic ransomware attack, the victim's data is encrypted and is only decrypted back after the victim pays a ransom fee to the ransomware operators. In a leakware attack, the data is stolen, and the victim is blackmailed with the data being published publicly unless he pays a certain fee. In a leakware/ransomware hybrid attack, the data is first stolen, then encrypted. Then the victim is first asked to pay the ransom for decryption. If the victim declines to pay the ransom, the attackers threaten him to release the stolen data publicly. In some cases, business partners and/or customers of the victim are also contacted and informed of the impending data release to put even more pressure on the victim.

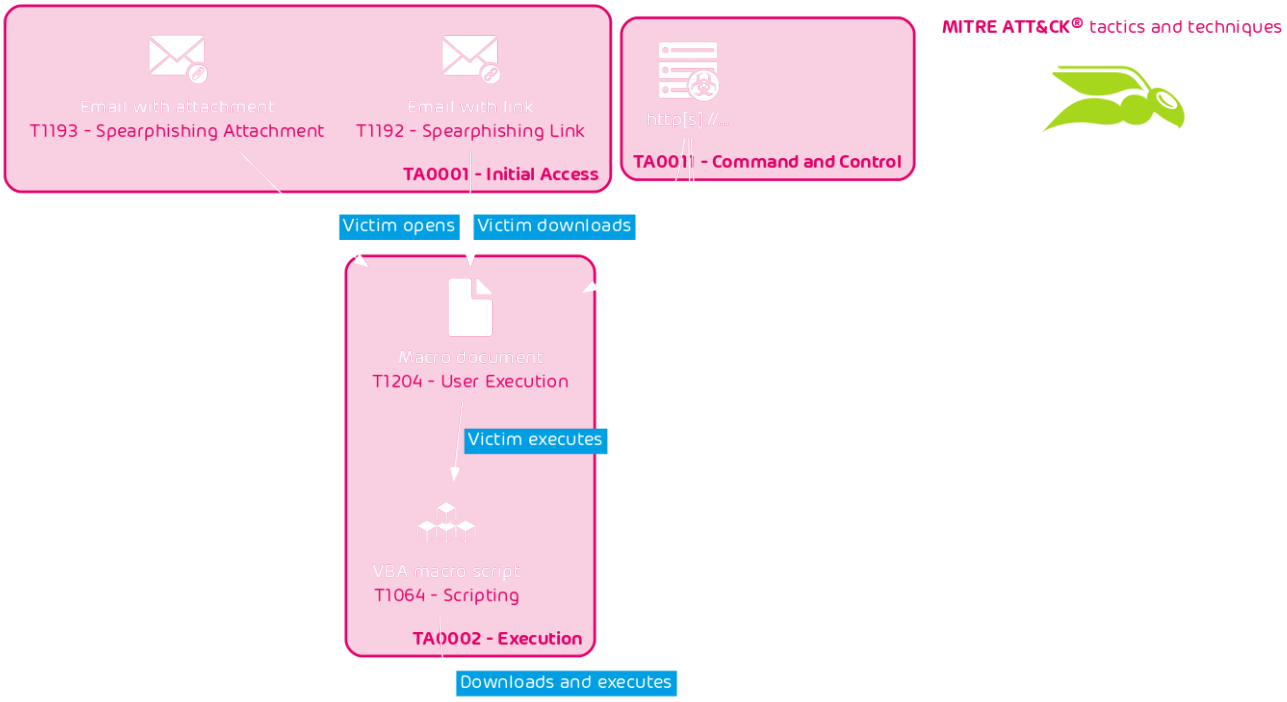
In this article we outline how these leakware/ransomware hybrid attacks work, how they differ from classic ransomware attacks, and how you can protect yourself against them.

## Background: What is Ransomware?

With the rise of crypto currencies, ransomware has become popular for cybercriminals. While ransomware existed before crypto currencies, the logistics of the ransom transfer were greatly simplified by crypto currencies.

According to ID Ransomware, a free service to identify ransomware, there exist 928 different pieces of ransomware[1].

Ransomware is often distributed and deployed by other malware. A popular attack vector is email. A typical infection chain of a ransomware attack is the following:

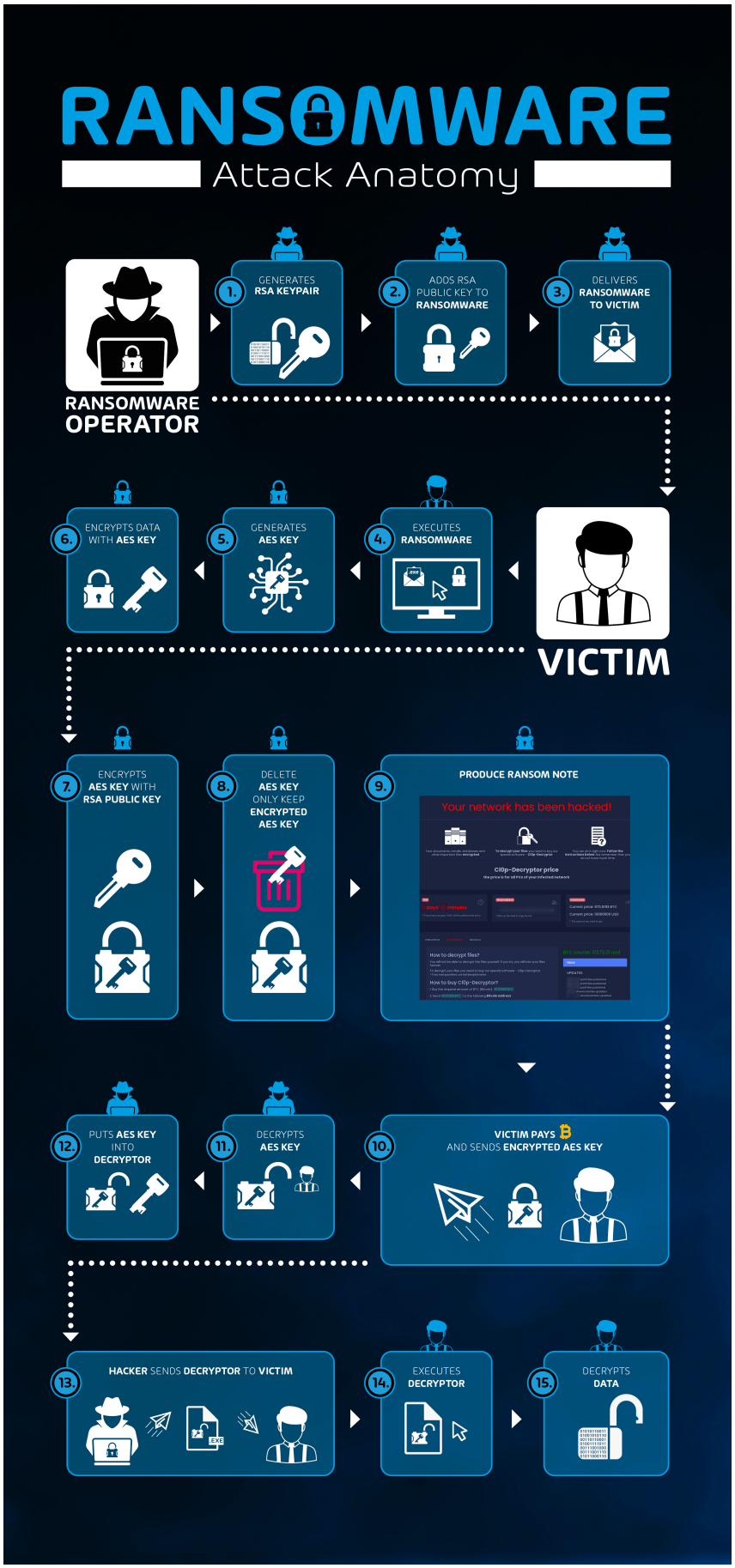



Actors behind ransomware are financially motivated. Their ransomware encrypts the victim's data. The attackers will only decrypt the data if the victim pays a ransom.

Ransom demands can range from a few hundred Euro for decrypting a single computer, over several thousand for computers of a small business, up to millions for large corporations and/or government entities. The largest publicly known ransom to ever be paid amounted to $4.5M. It was paid by the U.S. travel management company CWT[2].

## Classic Ransomware

The interaction and information flow of a classical ransomware case is as follows:


RANSOMWARE
Attack Anatomy
RANSOMWARE OPERATOR
1. GENERATES RSA KEYPAIR
2. ADDS RSA PUBLIC KEY TO RANSOMWARE
3. DELIVERS RANSOMWARE TO VICTIM
4. EXECUTES RANSOMWARE
5. GENERATES AES KEY
6. ENCRYPTS DATA WITH AES KEY
VICTIM
7. ENCRYPTS AES KEY WITH RSA PUBLIC KEY
8. DELETE AES KEY ONLY KEEP ENCRYPTED AES KEY
9. PRODUCE RANSOM NOTE
Your network has been hacked!
ClOp-Decryptor price
How to decrypt files?
How to buy ClOp-Decryptor?
10. VICTIM PAYS ₿ AND SENDS ENCRYPTED AES KEY
11. DECRYPTS AES KEY
12. PUTS AES KEY INTO DECRYPTOR
13. HACKER SENDS DECRYPTOR TO VICTIM
14. EXECUTES DECRYPTOR
15. DECRYPTS DATA

## New Leakware/Ransomware Hybrid

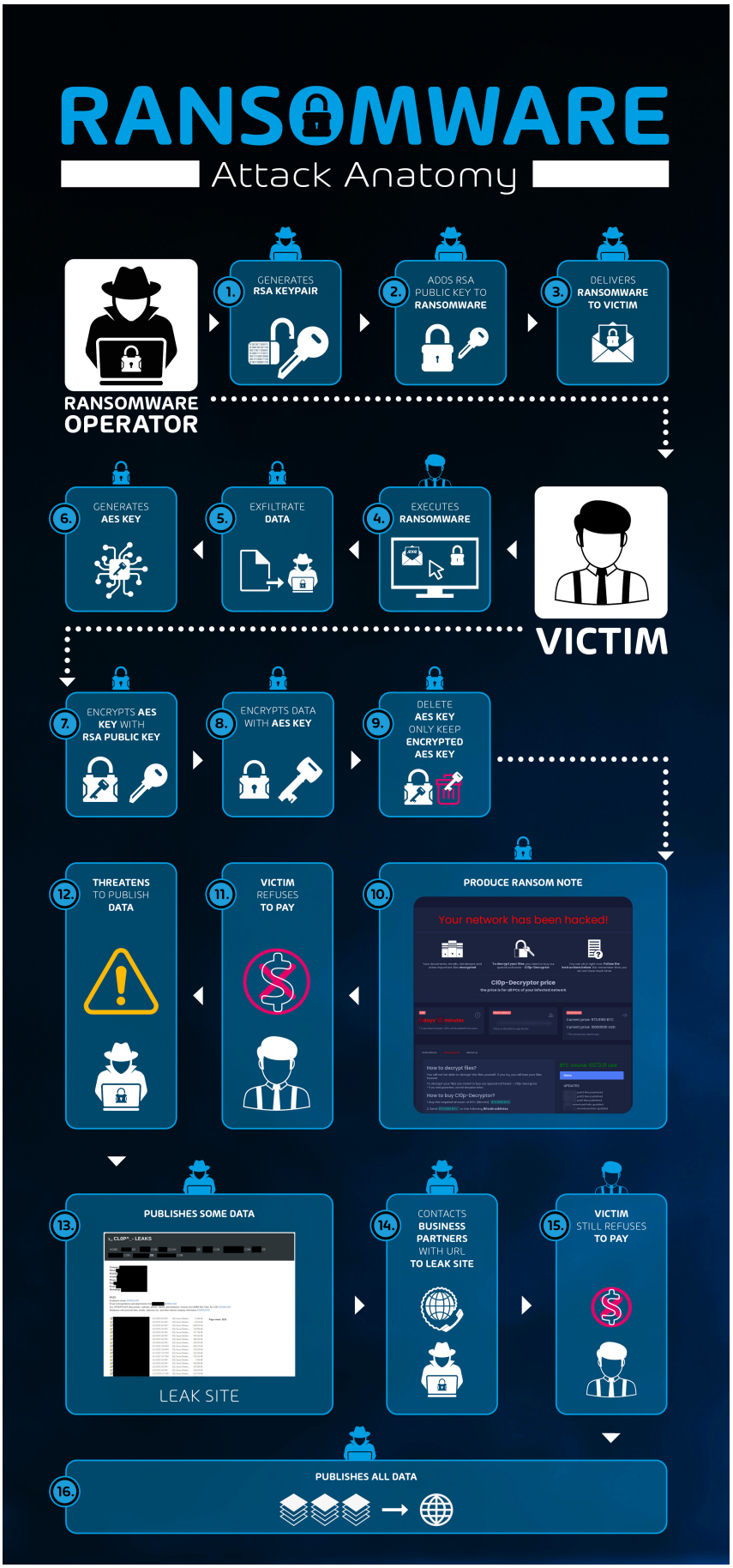
Since December 2019, actors behind the Maze ransomware operation began combining a previous attack known as leakware with ransomware.

In a leakware attack, data of the victim is stolen, and the attackers threaten to publish the data if the victim does not pay a ransom. Leakware is therefore the opposite to ransomware. Instead of denying the victim access to the data, access to the data is granted to everyone in case the victim does not pay.

This new leakware/ransomware hybrid scheme combines both leakware and ransomware. To this end, before encrypting the victim's data via ransomware, the data is exfiltrated to the ransomware operators, who then threaten to publish the data if the victim refuses to pay the ransom.

In addition, some ransomware operators will contact the victim's business partners or customers, whose data is often among the data to be published. The operators behind the Clop ransomware are notorious for doing this. This is used to further increase pressure on the victim to pay the ransom.

The interaction and information flow of the new leakware/ransomware hybrid is as follows:


RANSOMWARE
Attack Anatomy
RANSOMWARE OPERATOR
1. GENERATES RSA KEYPAIR
2. ADDS RSA PUBLIC KEY TO RANSOMWARE
3. DELIVERS RANSOMWARE TO VICTIM
VICTIM
4. EXECUTES RANSOMWARE
5. EXFILTRATE DATA
6. GENERATES AES KEY
7. ENCRYPTS AES KEY WITH RSA PUBLIC KEY
8. ENCRYPTS DATA WITH AES KEY
9. DELETE AES KEY ONLY KEEP ENCRYPTED AES KEY
10. PRODUCE RANSOM NOTE
Your network has been hacked!
11. VICTIM REFUSES TO PAY
12. THREATENS TO PUBLISH DATA
13. PUBLISHES SOME DATA
LEAK SITE
14. CONTACTS BUSINESS PARTNERS WITH URL TO LEAK SITE
15. VICTIM STILL REFUSES TO PAY
16. PUBLISHES ALL DATA

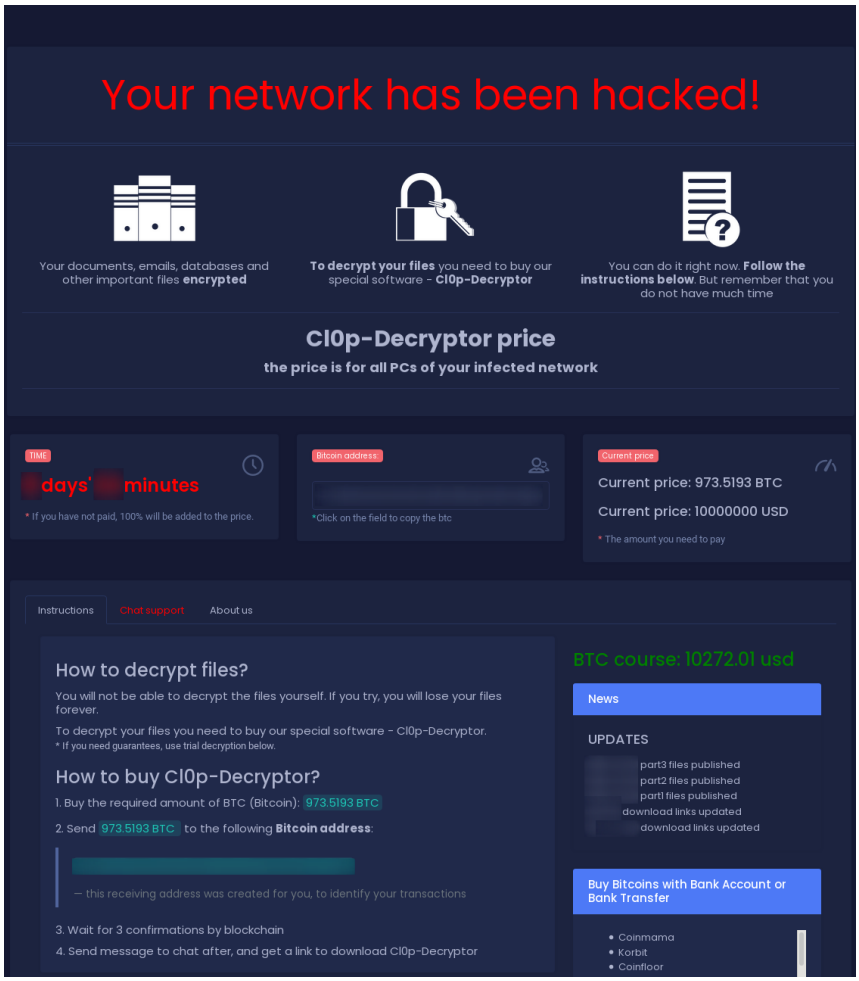
The problem for the victims is that, even if they pay the ransom, there is no guarantee the leaked data will be deleted – only the promise of criminals. The leaked data could be sold in the underground economy, used in future attacks, and even used to extort the same victim again with the same data at a later point in time.

## Clop Ransomware as Example

Using the Clop ransomware as an example, we outline how a leakware/ransomware hybrid attack unfolds.

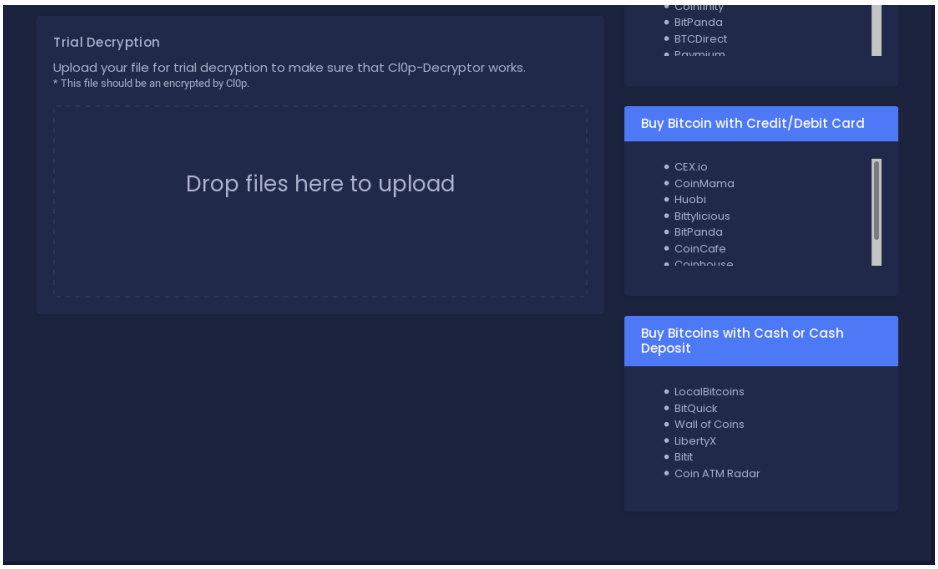
The Clop ransomware is operated by a threat actor commonly referred to as TA505. Hornetsecurity has reported on these activities previously[3]. Initial access takes place via a malicious email. TA505 does big-game hunting, i.e., they specifically target large corporations with high revenues. If a recipient opens the email and follows the instructions, which in most cases involve downloading a malicious document and allowing the document to execute macros, the recipient becomes a victim. The macro code in the document then downloads a remote administration trojan (RAT). This RAT gives the attackers remote access to the victim's computer. The RAT is then used to move laterally within the victim's company network and gather additional information. In addition, other tools (such as those from the Cobalt Strike framework) are often deployed to obtain domain admin rights. Valuable data is then exfiltrated. From victim data which was published in the past, we know that this data usually contains the complete shared drives of the infected company. Eventually, the Clop ransomware is deployed company-wide to encrypt and incapacitate as many systems as possible so the disruption to the company is maximized.

Then, the operators of the Clop ransomware send the victim to a ransom note website hosted via a Tor hidden service. This ransom note website includes details on the ransom and how to pay it.

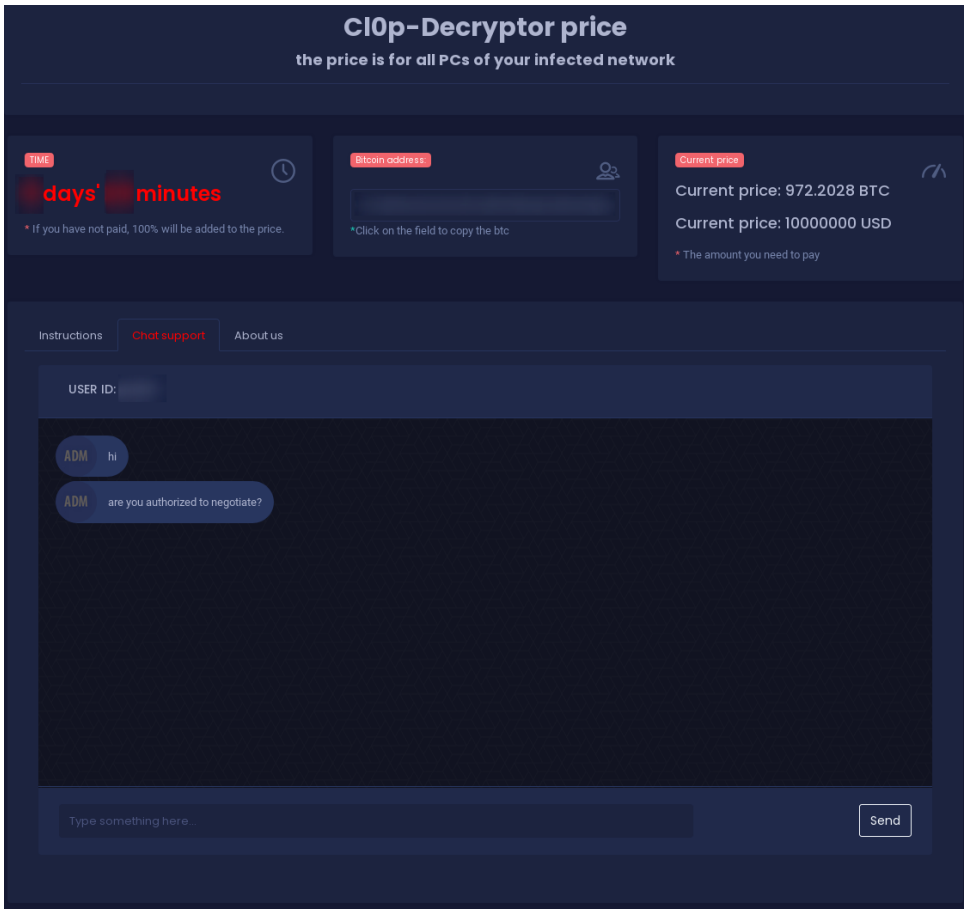



Depending on the company size and estimated revenue, the demanded ransom is often in the millions. Again, TA505 does big-game hunting, i.e., they will only target large corporations with high revenues. The ransom note website also features a timer and a threat that if the ransom is not paid in time, the price will be doubled.

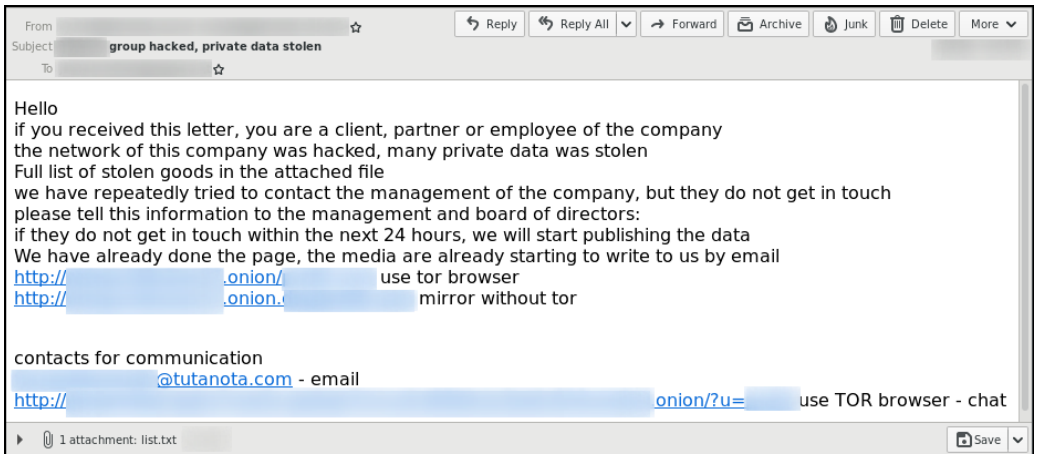
To proof to the victim that files can be decrypted, the ransom note site also offers a “Trial Decryption”.




The ransom note site also features a support chat. Those chats are often used to negotiate the ransom, payment rates or deadline extensions.

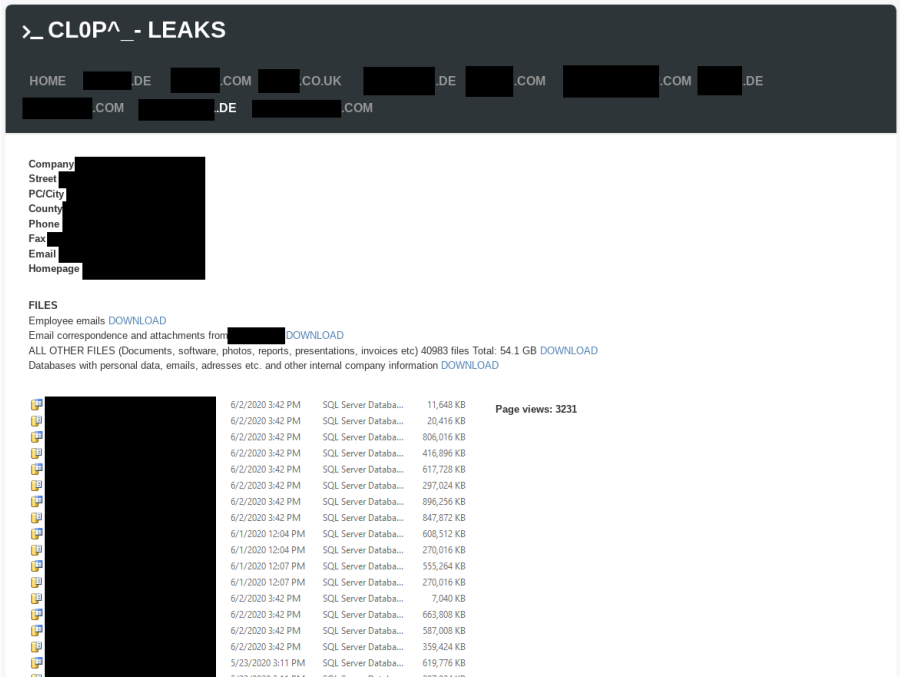



If a victim refuses to pay or does not enter negotiations, the ransomware operators start sending out mass-email notifications to the victim's business partners and/or customers. Here is one example of such a notification email sent out by the Clop ransomware operators:



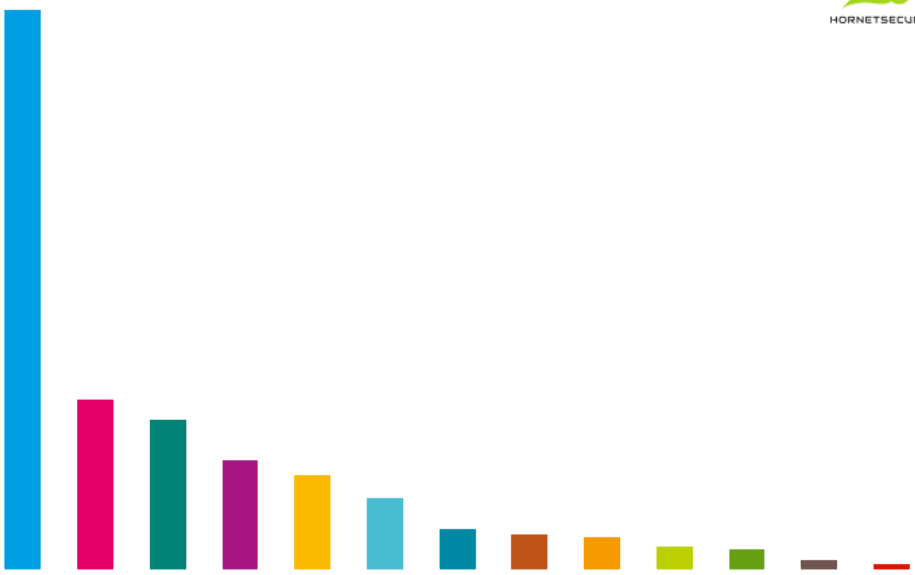

The attached `list.txt` file contains a list of the Windows domains and their corresponding network shares from which the Clop ransomware operators have exfiltrated data. The links in the notification email point to the subpage on the Clop's leak site where the stolen data is shared.

The Clop ransomware leak site is titled "CL0P^_- LEAKS". It currently lists 13 victims. Here is an example of a leaked data view:



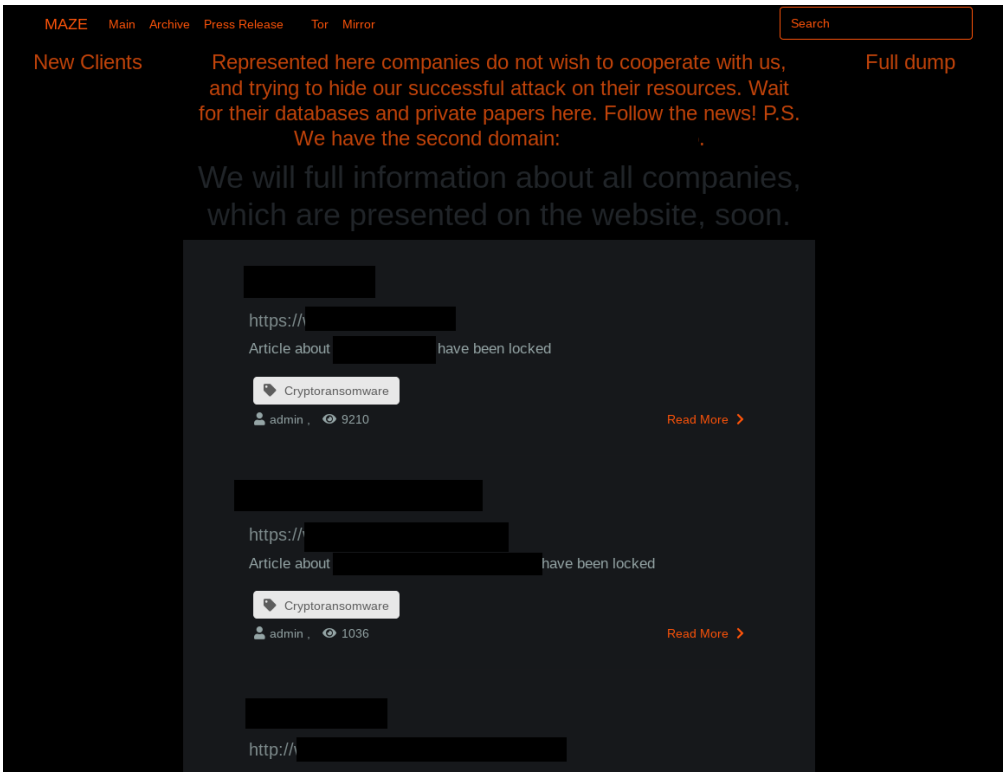

## List of Leak Sites

Currently, there exist leak sites for 13 different ransomware operations. The distribution of victims among each leak site can be seen in the following plot:



## Maze

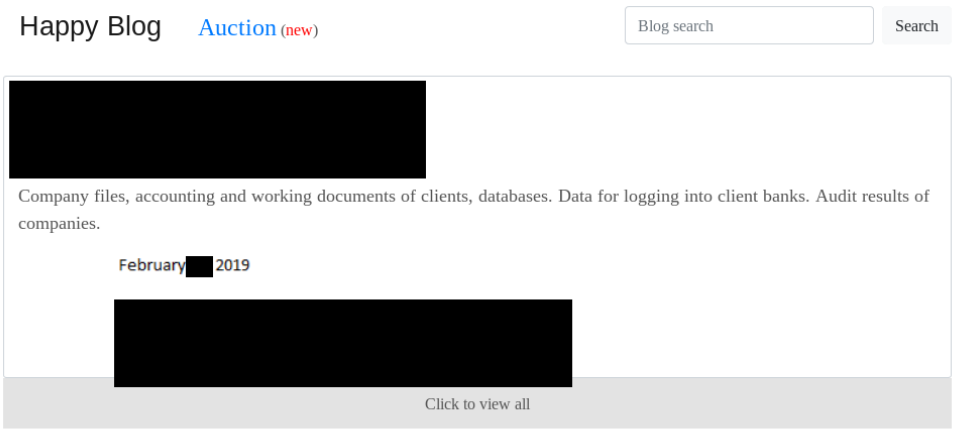
With 220 victims, the leak site of the Maze ransomware is the one with highest number of victims. Apparently, the operators behind the Maze ransomware have so many potential victims that they have formed the so-called Maze Cartel, in which the help other ransomware operations for a share of the profits.

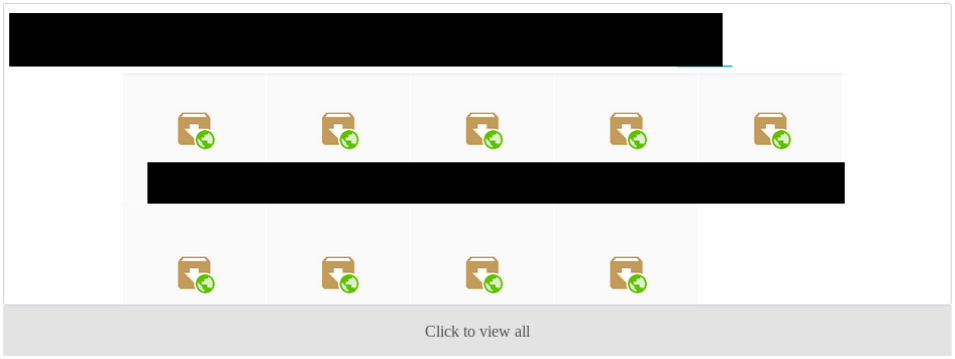



Interestingly, the Maze leak site is among the leak sites that are also acessible via the clear web and not just via a hidden service.

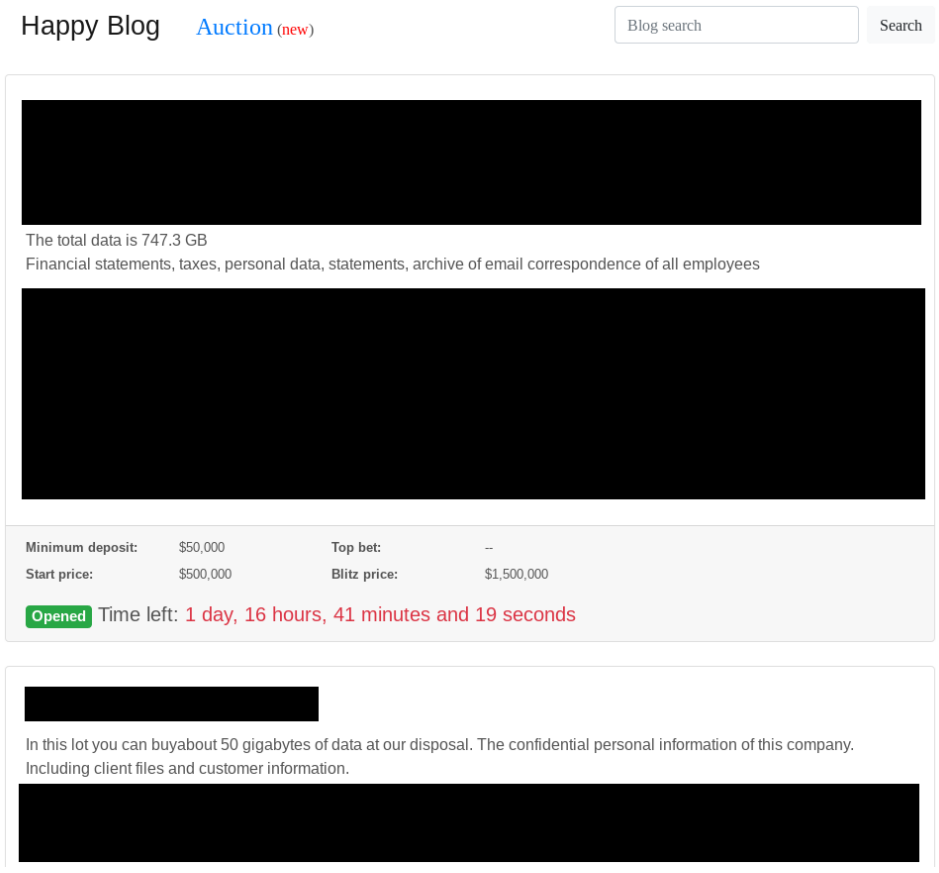
## REvil / Sodinokibi

The second most dominant ransomware with a leak site is REvil. Their site, called “Happy Blog”, contains data from 67 victims.



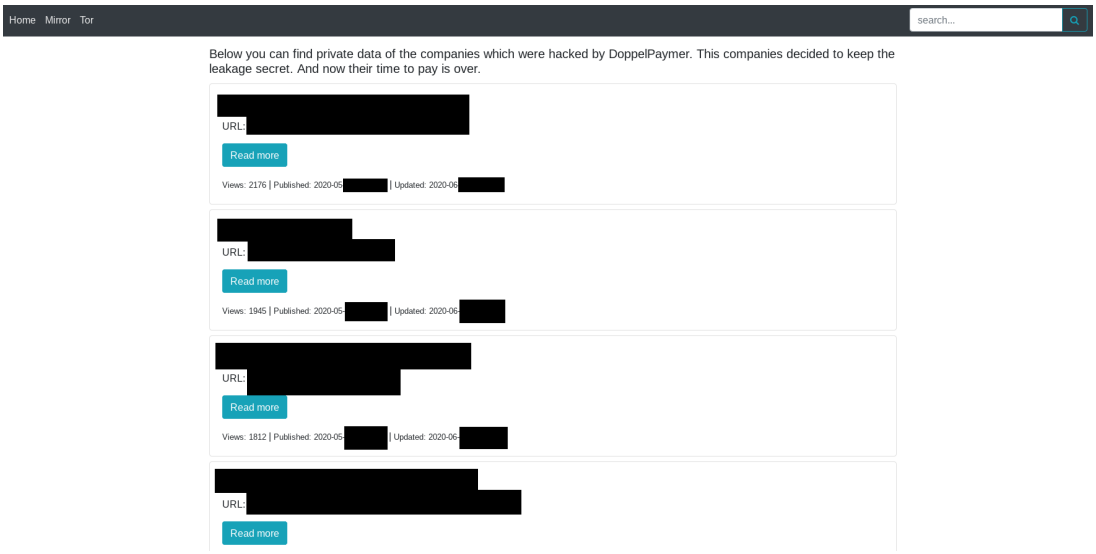

In June 2020, the actors behind the REvil ransomware also started to “auction” stolen data:



However, the auction site doesn't contain any information on how to bid. It is likely just another mechanism to gain media attention and scare companies into paying the attackers.

## DoppelPaymer

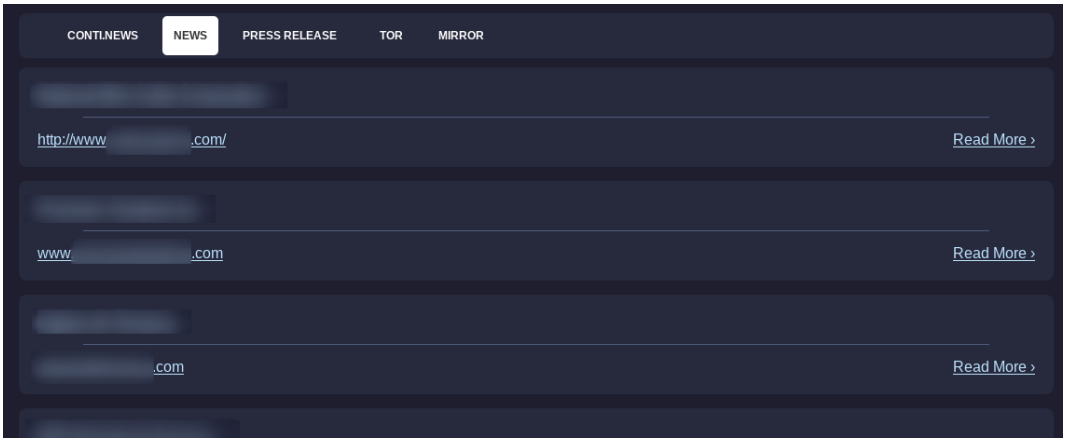
With data from 59 victims, the "Doppel leaks" leak site of the DoppelPaymer ransomware comes in on third place.




The site is also accessible via a clear web domain.

## Conti

The "Conti News" leak site of the new Conti ransomware already has data from 43 victims. From all current available information, the Conti ransomware seems to be the successor to the notorious Ryuk ransomware.

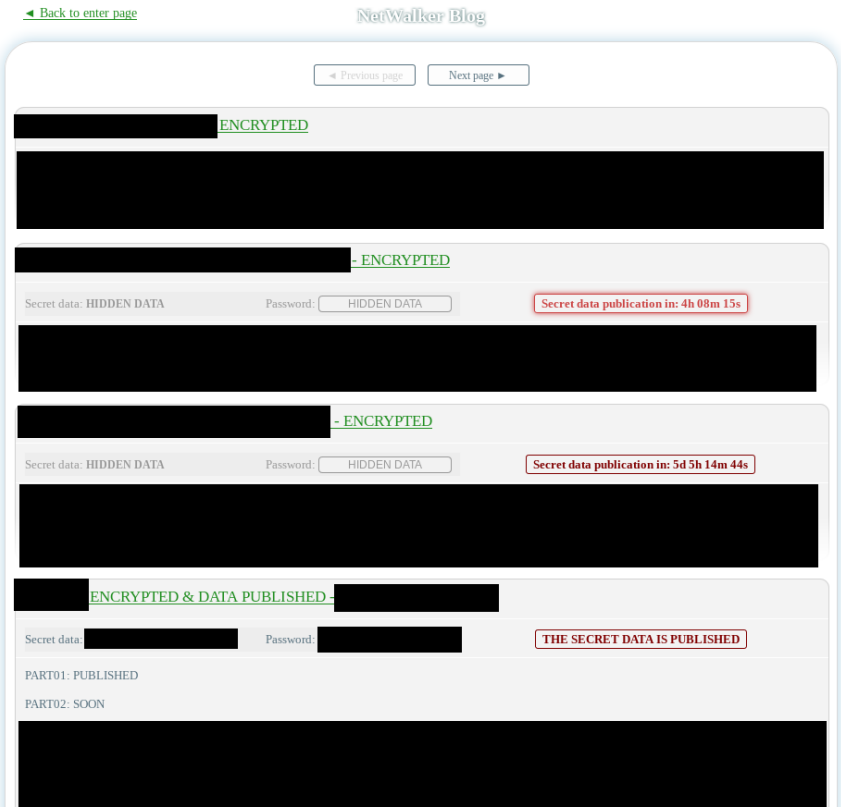



The site is also accessible via a clear web domain.

After Maze, Conti is currently the ransomware with the fastest growing victim count, sometimes increasing in up to 10 new victims per day. Here, it is worth noticing that only victims who refuse to pay the ransom are published on the leak sites.

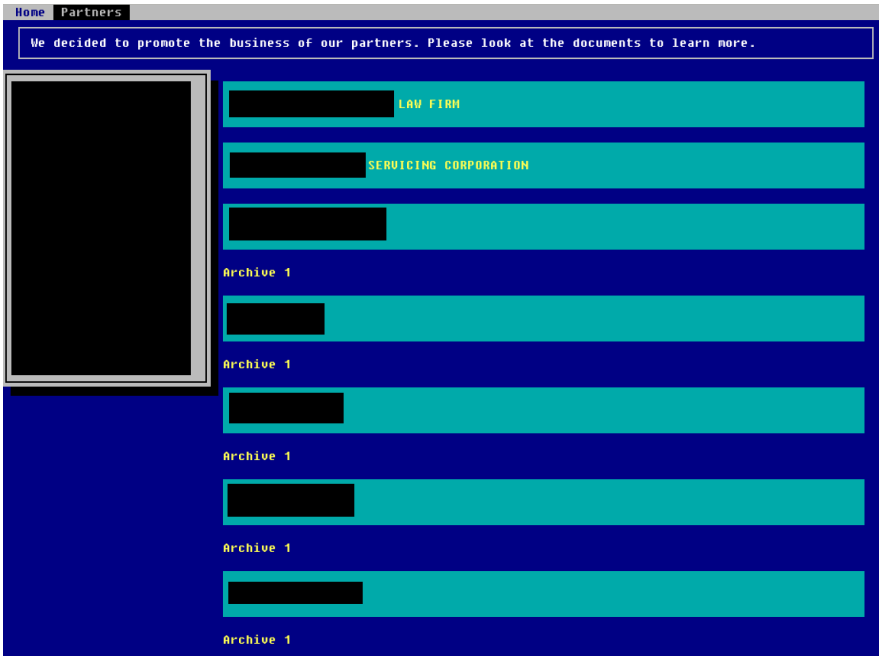
## NetWalker

Data from 37 victims of the NetWalker ransomware has been published on their leak site titled “NetWalker Blog”.



## Mespinoza / Pysa

The Mespinoza ransomware, also known as Pysa, has titled their leak site “Pysa’s Partners”. It features data from 28 victims.




## Nephilim

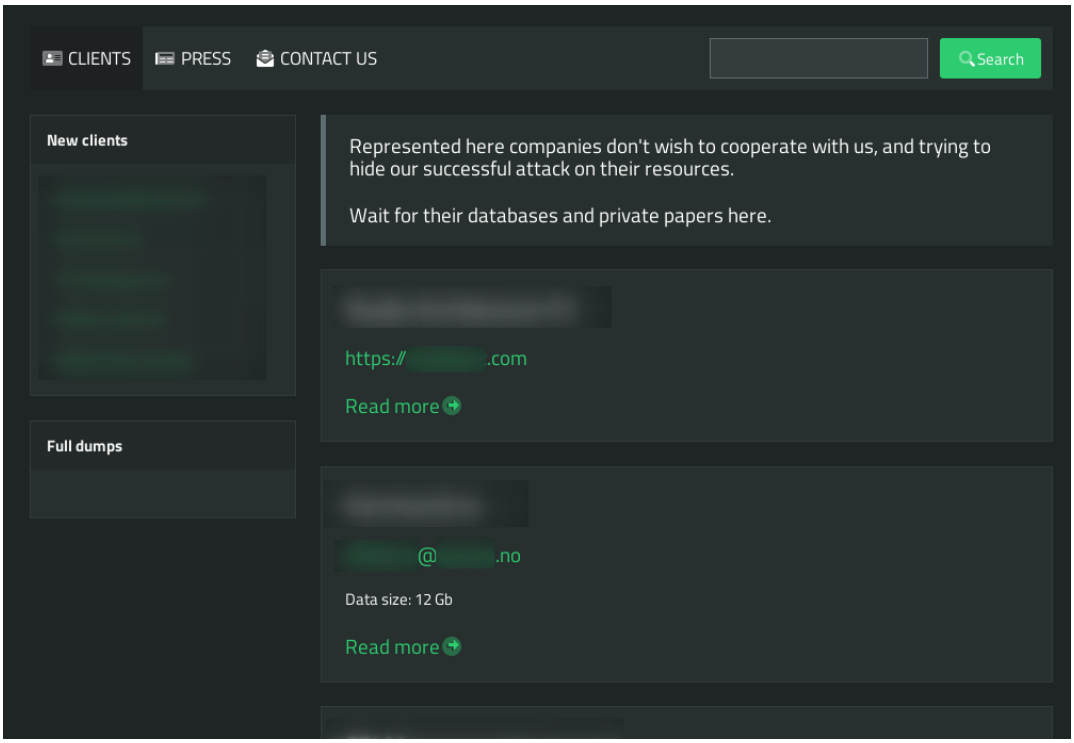
The leak site of the Nephilim ransomware, called “Corporate Leaks”, contains data from 16 victims.

## RagnarLocker

The leak site of the RagnarLocker ransomware is titled “RAGNAR LEAKS NEWS”. It features data from 14 victims.

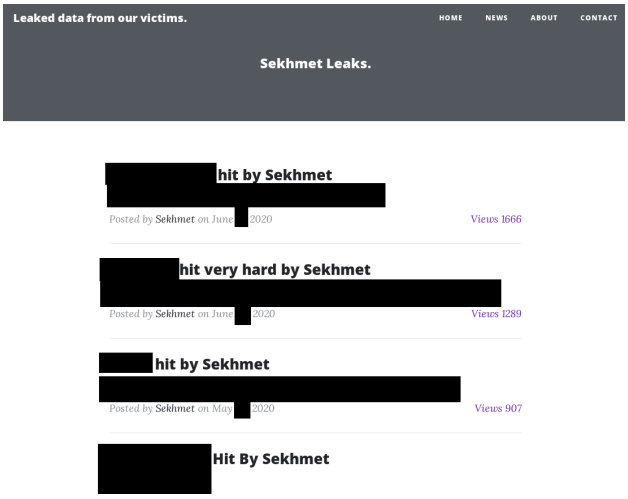

## SunCrypt

The leak site of the SunCrypt ransomware is simply titled “News”. However, researchers were able to contact the operators of the site and confirm that the leak site is associated with the SunCrypt ransomware. The leak site features data from 9 victims.



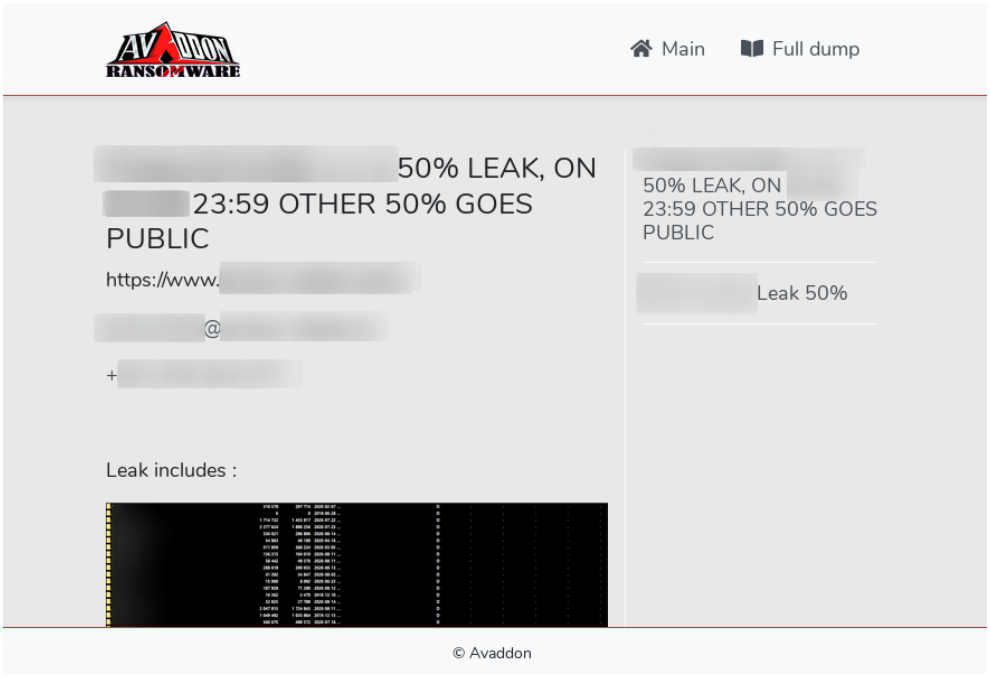

## Sekhmet

The Sekhmet ransomware leak site, titled “Sekhmet Leaks.” is only available via a clear web address. It currently features data from 8 victims.



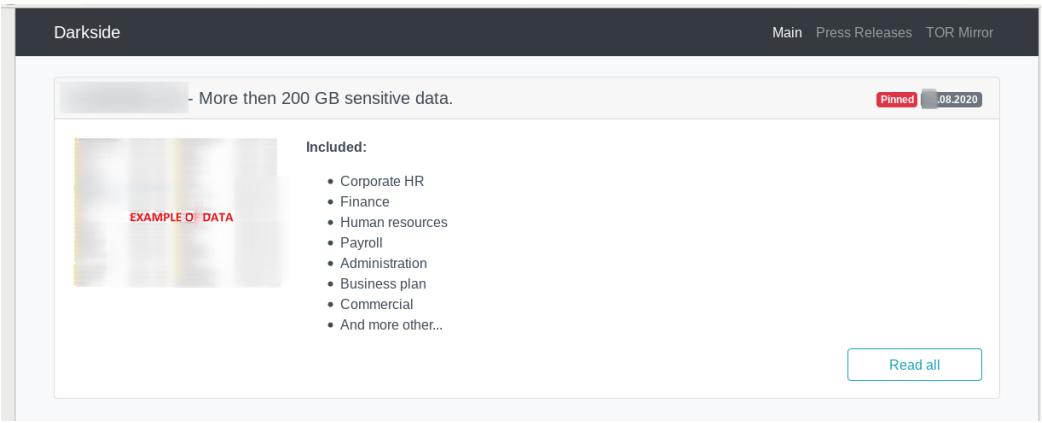

## Avaddon

In the first Avaddon campaign observed by Hornetsecurity[4], no data was exfiltrated. The campaign distributed Avaddon via the Phorpiex botnet, and the encryption of the victims was fully automated. The campaign was hence not targeted at high-value victims for which a leak would be worthwhile. However, Avaddon has since been used in different campaigns and their leak site, titled “Avaddon Info”, has currently data from 4 victims.



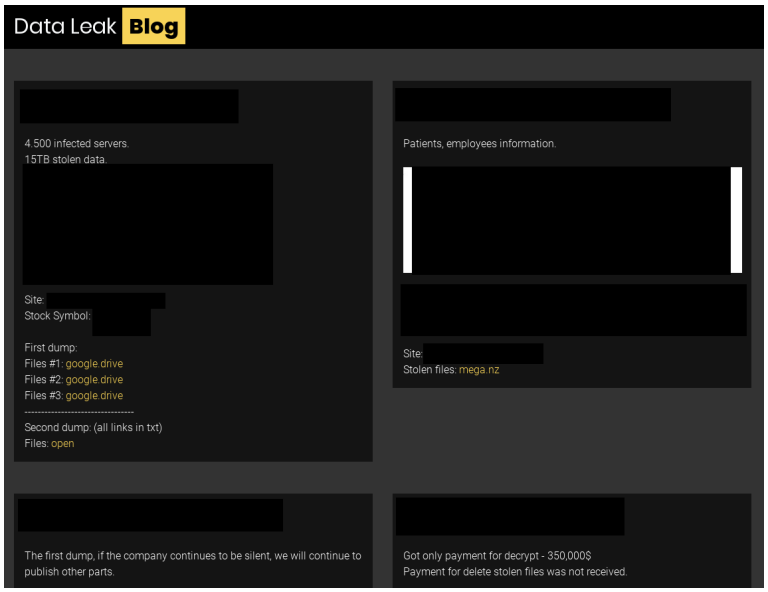

## Darkside

A very recent leak site is the “Darkside” leak site of the Darkside ransomware. It has data from 2 victims.




## MedusaLocker / AKO

The MedusaLocker ransomware also had a leak site, which at one point featured data from 7 victims.




However, currently the site only contains a “coming soon” message without any published contents of victims. It seems the site is currently being restructured.

### Nemty

The Nemty ransomware also used to have a leak site. The site was also reachable via a clear web domain. However, the site is currently not reachable anymore.

### ProLock

Hornetsecurity previously has analyzed the ProLock ransomware, which also claims to “have gathered […] sensitive data” and “would share it in case [the victims] refuse to pay”[5]. However, no ProLock leak site has appeared yet.

## Conclusion and Remediation

The new leakware/ransomware hybrid attacks make malware infections more dangerous to businesses than ever before. While good backups helped against classic ransomware attacks, they do not provide any protection against private and/or confidential data being forcefully leaked to the public. The broad announcement of the data leak to business partners and customers will cause further damages and loss of reputation to victims as business partners and customers, but also competitors get unlimited access to internal documents, such as contracts, pricing, research and development findings, etc.

In general, the only protection against these leakware/ransomware hybrid attacks is to invest in effective IT security. With regards to email, Hornetsecurity’s Spam Protection Service and Hornetsecurity’s Advanced Threat Protection protect against leakware/ransomware hybrid attacks using email as their initial infection vector in the same way they protect against

classic ransomware attacks using this access vector: by fending off these attacks at the very beginning of the attack chain before the attackers can even obtain initial access to your systems.

## References

### Further information:

More about Ransomware on the Hornetsecurity Knowledgebase.