LOCKDATA Auction – Another leak marketplace showing the recent shift of ransomware operators

telekom.com/en/blog/group/article/lockdata-auction-631300

Blog.Telekom

07-14-2021
Nils Stünkel

5 Comments

- Share Share
  Two clicks for more data privacy: click here to activate the button and send your recommendation. Data will be transfered as soon as the activation occurs.

- Print
- Read out

By now policy makers all over the world identify ransomware as a significant threat to our digital society. In the aftermath of the Colonial Pipeline Attack in May 2021 that caused widespread gasoline shortages in several US states, ransomware was more discussed than ever. President Biden recently requested Russian President Putin to crack down on ransomware operations and the U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism. This caused panic in the ransomware underground with some underground forums banning advertisements for ransomware operations.

LOCKDATA Auction shows the recent shift of ransomware operators. (Bild von Gerd Altmann auf Pixabay)

The ransomware underground is constantly innovating and finding new ways to operate. One of these recent innovations is the rise of stolen data marketplaces. Instead of using the double extortion approach, i.e. encrypting the infrastructure and threatening to release stolen data, former ransomware gangs shift to data-theft extortion operations only. One reason for this might be to evade the measures that authorities are now putting in place due to events like the Colonial Pipeline Attack. Two examples for such marketplaces are Marketo and File Leaks.

In this blog post, Thomas Barabosch and I will talk about another leak site that Deutsche Telekom Security recently encountered: LOCKDATA Auction. We will describe what LOCKDATA Auction is and give insights into a CryLock ransomware case where the CryLock affiliate worked with this portal. And, of course we provide analysis resources for CryLock ransomware including YARA rules at our Github repository.

The Incident Response Team at Deutsche Telekom Security GmbH can quickly investigate and help you remediate ongoing ransomware intrusions. For more information, please contact: DFIR@telekom.de.

What is LOCKDATA Auction?

LOCKDATA Auction is a Darknet portal that Deutsche Telekom Security is aware of since May 2021. Figure 1 depicts the main page of LOCKDATA Auction. It appears to offer various auctions of stolen data from victims worldwide. The country of origin of the victims is always annotated, e.g. Saudi Arabia or USA. Auctions appear to be open for more than one month in some cases.

Figure 1: LOCKDATA Auction victim listing.

The registration for auctions is described as invite-only (see Figure 2). Underground marketplace operators frequently use reputation based or referral systems to better protect their identities from investigators and shield their communication methods from outsiders.

Figure 2: Registration for auctions is invite-only.

But, to our surprise, when we looked through the page code to learn how invites worked under the hood, we discovered that the “Sign up” and “Sign in” functions were completely non-functional.
Usually, when a user tries to log into a webpage, the user’s browser will have to check in with the server and verify that their credentials are correct. This page doesn’t do that at all - it will always just display a message like “Error: Login or password entered incorrectly” or “Error: Wrong invite code!” immediately when “Sign in” or “Sign up” is clicked.

Figure 3: The code responsible for the “Sign up” and “Sign in” forms.

So, what does this mean? Most likely, since the portal is fairly new, functionality might still be in development. Another hypothesis is that the site merely serves as a menacing mockup of an online auction site, to coerce victims into paying the ransom. During our investigation, we have observed a ransomware operator change victim information on the auction site on the fly, which proves they have direct access to LOCKDATA Auction.

Auctions have a start price (ranging from $50 000 to $500 000), a minimum deposit (ranging from $0 to $50 000 dollars), and a blitz price (up to $1 500 000). The website shows the top bet for active auctions as well. In some cases, the top bet is less than the starting price. There is a link to preview data, which however was broken in most cases (as of time of writing). The descriptions of the victims and data sets is comprehensive. Data set sizes range from 50 GB to 2 TB. Figure 3 shows an example of an active auction.

Figure 4: An active auction on LOCKDATA Auction.

Successfully concluded auctions are still listed on the website. Their download link is “locked” but there is still a button to contact the seller. Figure 4 depicts an example of a finished auction. In this case, supposedly $40 000 were paid for 2 terabytes of personal data of a North American public entity.

Figure 5: A completed auction on LOCKDATA Auction.

Who offers leaks on LOCKDATA Auction?

Deutsche Telekom Security was involved in a LOCKDATA Auction case. In this occasion, the threat actor utilized the CryLock ransomware to encrypt the victim’s environment.

CryLock is a ransomware from the Russian cybercrime underground. It follows a Ransomware-as-a-Service (RaaS) model, where “partners” (or “affiliates”) acquire the ransomware to deploy it in victim environments. The first reference to this ransomware was in 2014. Back then, it was publicly known as Crykal. A take-down of its infrastructure took place in 2018, resulting in a decryptor being published. In 2020, Crykal was rebranded under the name CryLock.

CryLock is written in Delphi, so obfuscations are nearly non-existent. There is a check whether or not the victim is located in a CIS (Commonwealth of Independent States) country, which is a common check for malware families from Russia and other CIS states. The ransomware encrypts files using a combination of RSA and a custom symmetric algorithm. After encryption, it drops a file called “how_to_decrypt.hta” as seen in Figure 5. The key takeaway is that the victim must contact the ransomware affiliate using the provided email address and a unique victim ID. This is the general course of action that CryLock affiliates follow.

Figure 6: how_to_decrypt.hta shows information to the victim.

However, in this particular case the modus operandi was slightly different. We observed how the threat actor utilized a Batch file to also add a legal notice to show on startup of the encrypted systems. This legal notice stated the following:

“Your system has been tested for security by the CryLOCK Ramsoware team and has failed. We specialize in file encryption and are also involved in industrial (also economic or corporate) espionage. We don't care about your files and what you do, nothing personal - it's just business. We recommend contacting us, as your confidential files have been stolen and will be sold to interested people if you do not pay for their removal or decryption of the files. One of the email for communication: [REDACTED]@[REDACTED].com Do not use corporate email for communication, in most cases your letters will not reach us. Our auction of information and confidential files, hosted in Tor [REDACTED].onion or http://[REDACTED].”

In their notice, the threat actor refers to the “CryLOCK Ramsoware [sic] team”. In addition to the aforementioned email address for communication purposes, they also provide the link to LOCKDATA Auction.

“Search Keys” Utility

The notice also contained an additional (shortened) Internet link. This link resolved to a cloud hosting provider (see Figure 7), where the “Search_keys_CryLOCK_3.0.exe” tool could be downloaded.

The page also contained a wallpaper of a part of the legal notice quoted above. Again, the same typo can be seen here. At this point, we are not sure whether this is an unintended typo or a stylization of the word “ransomware”. There were several communication channels mentioned: two email addresses and the TOR link to LOCKDATA Auction. One email address refers to CryLock and one to the auctioneer who was responsible for the auction on LOCKDATA Auction.

Figure 7: CryLock tool hosted at cloud hosting provider.

The tool “Search_keys_CryLOCK_3.0.exe” (see Figure 7) itself is rather interesting. This Delphi 7 utility can scan local disks as well as network storage for files that CryLock encrypted. It supposedly will also identify which generation of encryption mode was used on the files. Furthermore, it can kill CryLock related processes (e.g. mshta.exe, which shows the ransom note).

Figure 8: CryLock Delphi Tool Search_keys_CryLOCK_3.0.exe.

Access Brokering

Nowadays, ransomware is teamwork. Administrator access to systems is gained and sold by specialized hackers, sometimes for as low as $10. When an access path changes hands, we typically observe a change in the way the attack is carried out.

In this case, we discovered that the initial compromise of the victim's environment had been supported by a very distinct set of attacker infrastructure, tools, and mannerisms. The exact same behavior was observed in an entirely different case that occurred around the same time, but where another RaaS was used. This indicates that the actor using those tools may breach different victims and then either trade the access to one or more other group(s) or deploy different last stage payloads themselves.

Conclusion

LOCKDATA Auction is a new player in the field of darknet marketplaces. At this time, the site lacks basic functionality one would expect from an online auction site but is likely to grow over time.

At this point, it is not 100% clear whether LOCKDATA Auction is exclusive to CryLock affiliates or open to other ransomware operations as well, even though the similarity in branding between CryLock and LOCKDATA is striking. The attackers state with typos that the CryLock ransomware team attacked a victim's environment, which may suggest a group of people working together more closely than in a typical RaaS affiliate model. On the other side, the link to LOCKDATA Auction was not directly provided in the ransom note. It was shown to the victim only through a pre-login "legal notice" in Windows. Also, separate email addresses are listed for communication: one CryLock-related and one for the auctioneer at LOCKDATA Auction.

The ransomware landscape is innovating at a fast pace. Reactions of nation-states due to recent events like the Colonial Pipeline Attack in May 2021 are just increasing the velocity. One recent trend are stolen data (or leak) marketplaces like LOCKDATA Auction. These marketplaces offer threat actors a way to publish and monetize stolen data as leverage for their data-theft extortions.

Appendix A: IOCs

IOC	Description
e89135d80017e9da16b187ebe0a9de64	Search_keys_CryLOCK_3.0.exe
58a65f8e2075fd8ea32cd2a0384de10c	Sample "how_to_decrypt.hta"

3139ca1821331314c95816b92fe24c29	Sample CryLock 2.3.0.0

On topicBleepingComputer: Data leak marketplaces aim to take over the extortion economy
Reuters: Exclusive: U.S. to give ransomware hacks similar priority as terrorism