Q3 Ransomware Landscape Report

October 2022

Cyberint

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Q3 of 2022 has provided us with many interesting insights into the ransomware industry.

Instead of fairly wide distribution of victims between the various ransomware groups, we saw consistency from Lockbit3.0, as they remain the number one group with 37% of all ransomware attacks this quarter, an increase of 5% since the previous quarter, whereas they participated in "only" 29% of the ransomware incidents (Figure 1).

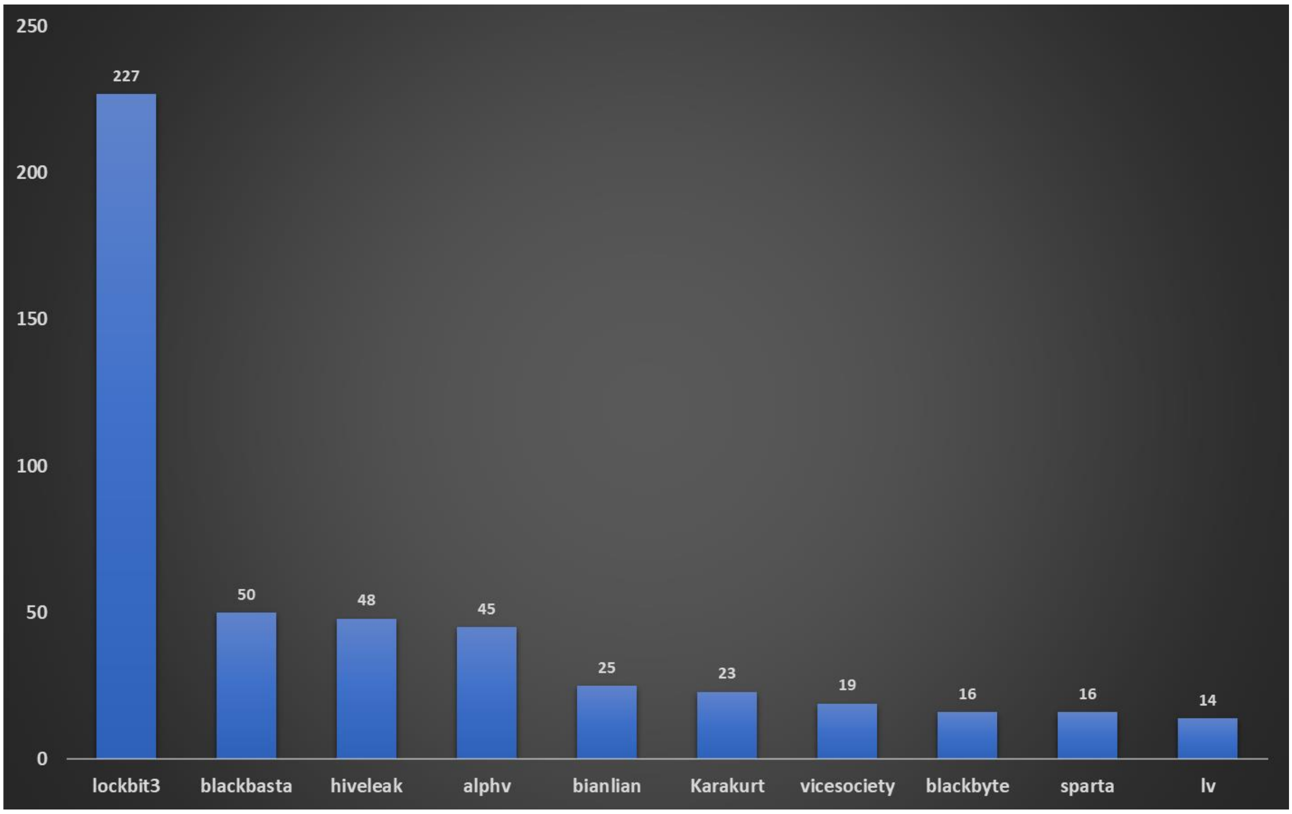


Figure 1: Top 10 ransomware families

The shutting down of Conti, which was responsible for 14% of last Q's incidents, did not result in the establishment of a new group, but rather led to a somewhat equal distribution of their share of the pie between all of the remaining groups.

USA remains the most targeted region followed by the UK, France, Spain and Germany, which were equally targeted (Figure 2).

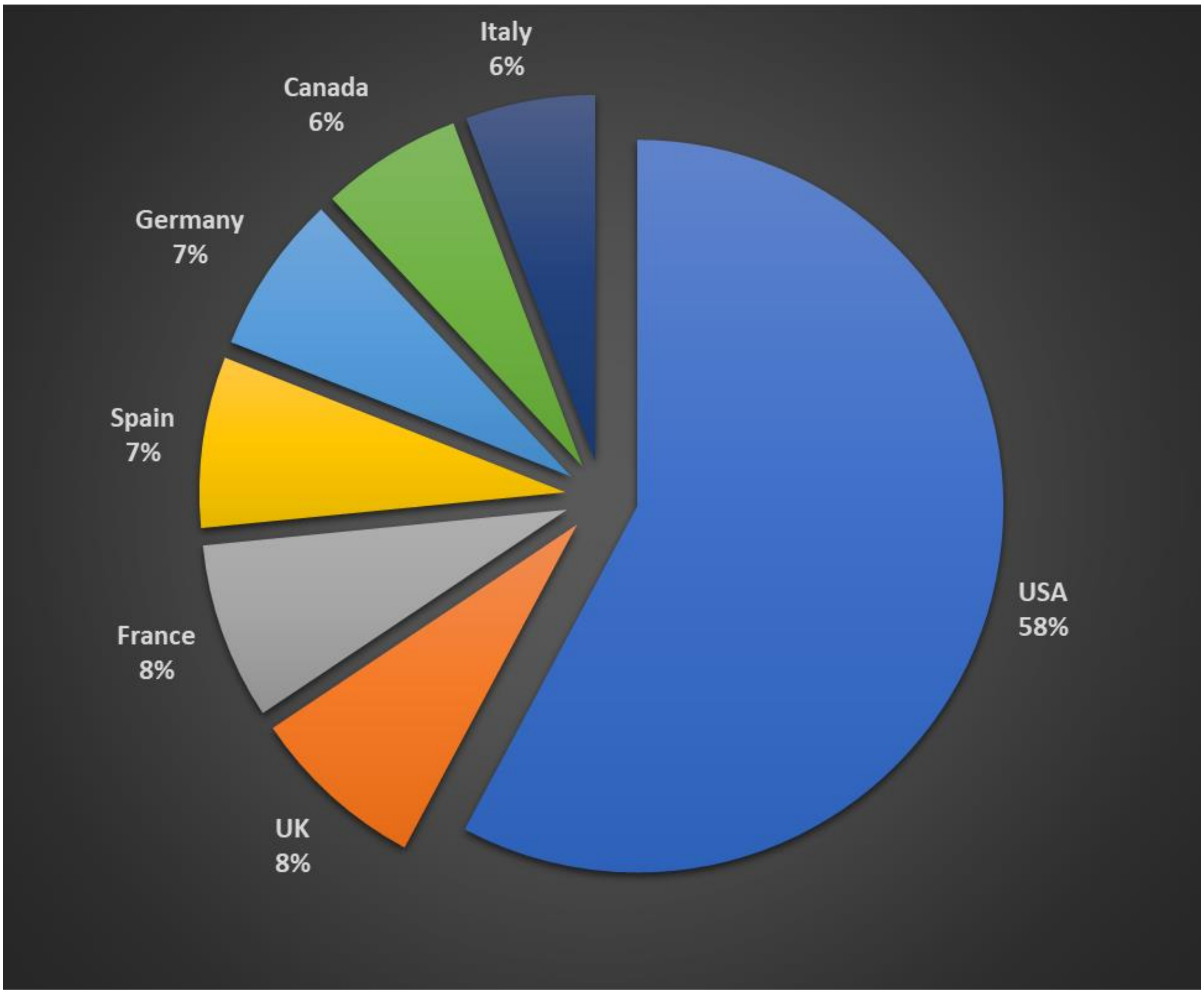


Figure 2: Ransomware incidents distribution by country

Although it seems like the ransomware industry is owned by one family, we did see some new groups, and promising newcomers have emerged such as BianLian, IceFire, Sparta and the notorious Bl00dy gang.

The most interesting piece of data we were able to find this quarter is that even though we have seen over 85 new ransomware families being introduced to the industry, the number of documented victims is lower by 15% since Q2 and by around 30% compared to Q1.

In this report, we will cover the ransomware trends in targeted sectors and countries, along with the most important cases we have witnessed where ransomware groups were the attackers, but sometimes the victims as well, and how the newcomers will play a part in the future.

Q3 NOTABLE EVENTS AND DEVELOPMENTS

LOCKBIT3.0 BACK IN SHAPE

Q2 was a “slow” quarter for Lockbit3.0 with 204 incidents. As the group was mainly focusing on expanding and investing time and effort in their infrastructure, their victim count was relatively low. Q3, however, was a totally different story. They participated in an interview in July that claimed that they were announcing Lockbit3.0 updates and promised to strike hard in the near future. Promised and delivered. In Q3, the group was responsible for at least 227 incidents.

PR INVESTMENTS

Lockbit3.0 is not just a ransomware group, they want to remind all of us that they are “the” ransomware group. In order to do so, they believe that being the number one group is not enough. So they also invested in becoming somewhat of a celebrity in the underground community, with PR and other gimmicks that their followers were more than happy to be part of.

INTERVIEWS

Although Lockbit3.0 doesn’t operate any Twitter or Telegram accounts like other threat groups, they do look to spread their message using other communication channels.

At the beginning of the quarter, a Lockbit3.0 member gave an interview to a cyber security magazine, talking freely about their exploits, describing the structure of the group, giving some success rate stats, and sharing their plans for the future.

TATTOO CAMPAIGN

Another Lockbit3.0 PR stunt was their tattoo campaign. The group offered $1000 to anyone getting a tattoo of their logo. As expected, a massive number of followers declared they would, or had already had a Lockbit tattoo done (Figure 3). In light of the massive response, the group had to publish another announcement that they were limiting the offer (Figure 4).

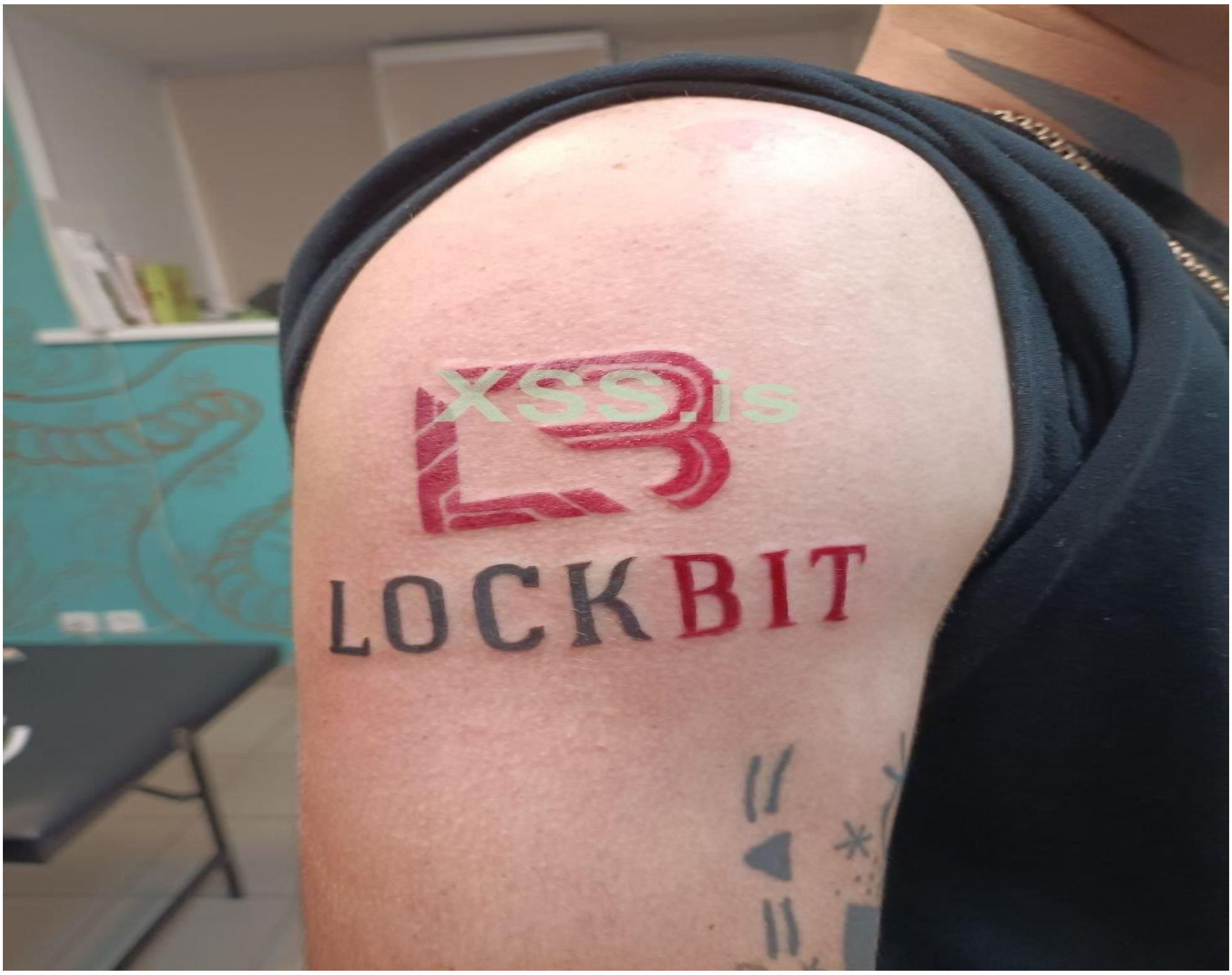
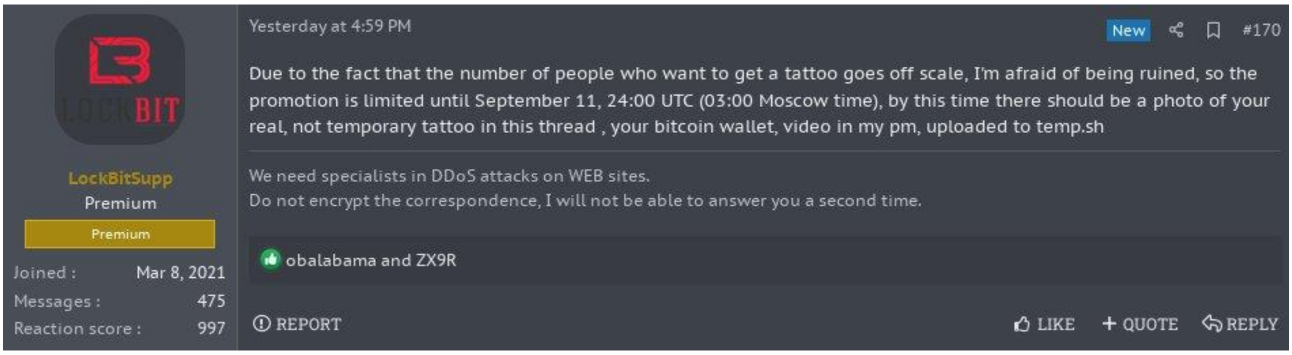


Figure 3: Lockbit's fan publishing his tattoo



Joined : Mar 8, 2021
Messages : 475
Reaction score : 997

Yesterday at 4:59 PM

Due to the fact that the number of people who want to get a tattoo goes off scale, I'm afraid of being ruined, so the promotion is limited until September 11, 24:00 UTC (03:00 Moscow time), by this time there should be a photo of your real, not temporary tattoo in this thread , your bitcoin wallet, video in my pm, uploaded to temp.sh

We need specialists in DDoS attacks on WEB sites.
Do not encrypt the correspondence, I will not be able to answer you a second time.

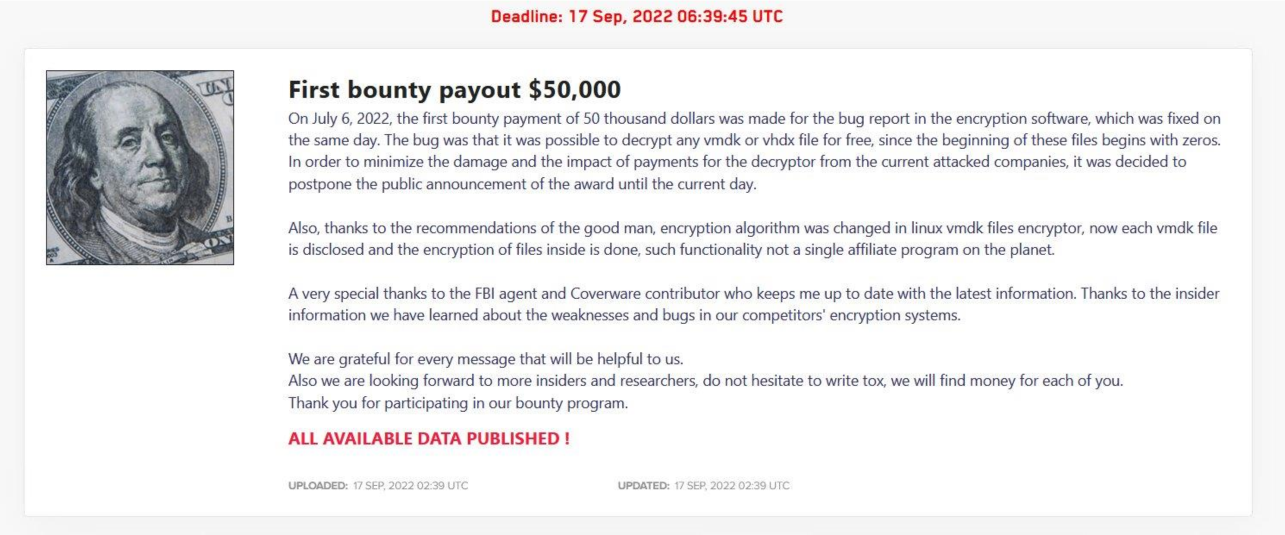
obalabama and ZX9R

Figure 4: Lockbit's announcement about limiting the tattoo campaign

BUG BOUNTY PROGRAM

Lockbit3.0 is always looking to show how confident they are in their product. One way was by offering a bug bounty program to anyone finding vulnerabilities in their servers.

As expected, the bug bounty program has drawn the attention of many followers and researchers, who have risen to the challenge, leading to over $50,000 bounty paid to pen testers, the group claims (Figure 5).



Deadline: 17 Sep, 2022 06:39:45 UTC

First bounty payout $50,000

On July 6, 2022, the first bounty payment of 50 thousand dollars was made for the bug report in the encryption software, which was fixed on the same day. The bug was that it was possible to decrypt any vmdk or vhdx file for free, since the beginning of these files begins with zeros. In order to minimize the damage and the impact of payments for the decryptor from the current attacked companies, it was decided to postpone the public announcement of the award until the current day.

Also, thanks to the recommendations of the good man, encryption algorithm was changed in linux vmdk files encryptor, now each vmdk file is disclosed and the encryption of files inside is done, such functionality not a single affiliate program on the planet.

A very special thanks to the FBI agent and Coverware contributor who keeps me up to date with the latest information. Thanks to the insider information we have learned about the weaknesses and bugs in our competitors' encryption systems.

We are grateful for every message that will be helpful to us.
Also we are looking forward to more insiders and researchers, do not hesitate to write tox, we will find money for each of you.
Thank you for participating in our bounty program.

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 17 SEP, 2022 02:39 UTC UPDATED: 17 SEP, 2022 02:39 UTC

Figure 5: Lockbit's announcement of the first bounty payout

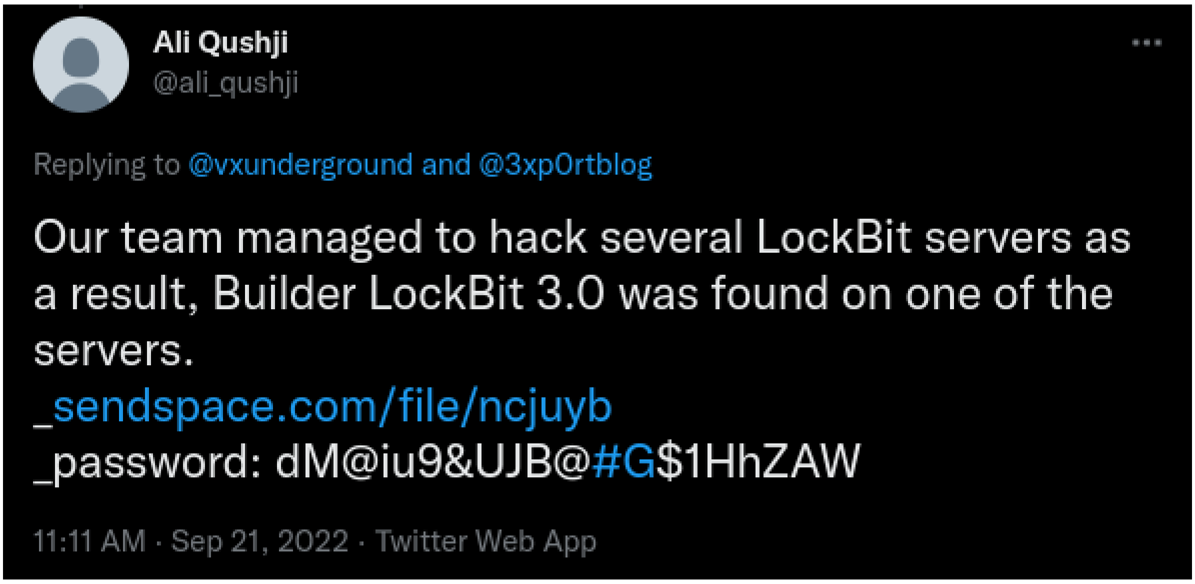
LOCKBIT3.0 LEAK

The confidence and arrogance of this notorious group gained them many followers, but a lot of enemies as well.

Ever since Conti's leaks, Lockbit claimed the ransomware throne without any intention of relinquishing it anytime soon.

Although business seems to be thriving for the ransomware group, an unknown threat actor, named Ali Quashji claimed that his group was able to compromise Lockbit's servers and leaked the builder and keygen module of the group.

As the announcement was published on a dedicated Twitter account (Figure 6), many security researchers and cyber security figures from the community tried to validate the leak, and if it was the actual Lockbit products.



Ali Qushji
@ali_qushji

Replying to @vxunderground and @3xp0rtblog

Our team managed to hack several LockBit servers as a result, Builder LockBit 3.0 was found on one of the servers.
_sendspace.com/file/ncjuyb
_password: dM@iu9&UJB@#G$1HhZAW

11:11 AM · Sep 21, 2022 · Twitter Web App

Figure 6: Ali Quashji Tweeting about the leak

Eventually, it was confirmed that the published items are in fact used by Lockbit, although many community figures decided not to publish these tools to prevent others from using them for sinister ends.

As we all wait and see if this incident will have the “Conti effect” that will lead to Lockbit’s inevitable end, the group claimed that Ali Qushji was a contractor who did some jobs for them and participated in developing these tools. This is an important piece of information because it proves that no servers were compromised, which means that we are not expected to see massive leaks other than what has already been leaked.

As much as we would like to see this group fall, just as Conti did, this is not a similar situation, and this incident will not lead to the fall of the ransomware ruler.

BL00DY GANG USES LOCKBIT3.0’S TOOLS

As much as many security figures tried to prevent these tools from getting into the wrong hands, one can only do so much, and, as expected, it didn’t take too long for other threat groups to utilize these tools in their own campaigns.

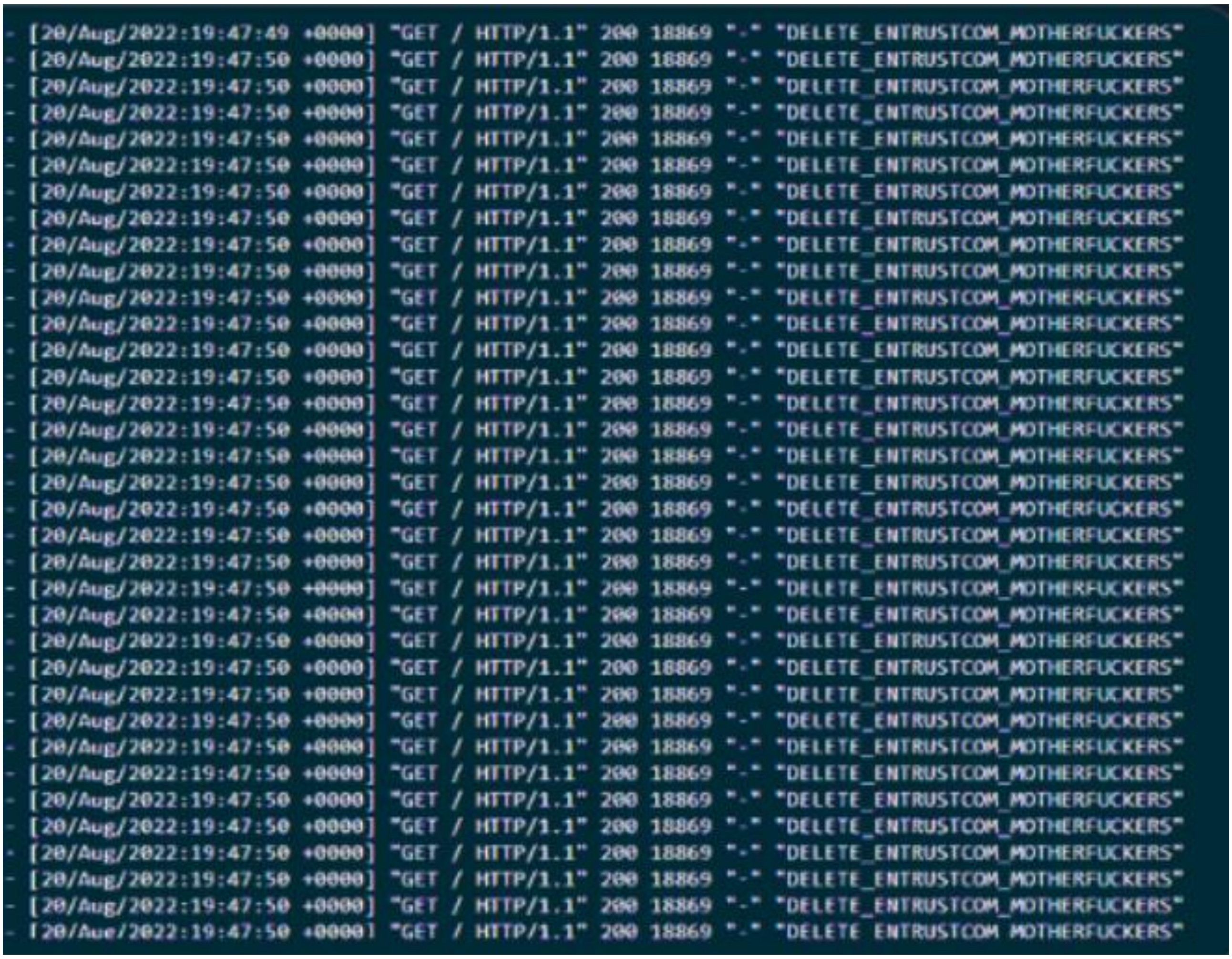
Bl00dy gang, a new group that emerged in September, is already responsible for several campaigns during their short existence. In the last several campaigns, the group was witnessed using the leaked Lockbit3.0’s builder against several organizations.

Given the simplicity and the customization options for whoever is using this builder, it is fairly predictable that Bl00dy gang might be the first, but certainly not the last to use it. New ransomware groups tend to utilize leaked builders instead of developing their own. We have witnessed this several times in Babuk and Conti leaks in the past, and this time is no different.

NEGOTIATION IN THE FORM OF DDOS

In the ransomware industry, negotiation usually includes both sides agreeing or disagreeing on the ransom payment, and that's about it. This quarter, however, we have been made aware of peculiar incidents where negotiations went south in the most extreme way.

One of LockBit3.0's many victims this quarter was Entrust, a company that provides software and hardware services to the financial sector. After relatively short negotiation talks, it seems like both sides could not find common ground and LockBit reported that they suffered a DDoS attempt from Entrust - a peculiar choice of action by Entrust. But when people from the community were skeptical about the authenticity of the claim, LockBit provided proof of their servers logs (Figure 7) displaying the DDoS requests contained the content "DELETE_ENTRUSTCOM_MOTHERFUCKERS".

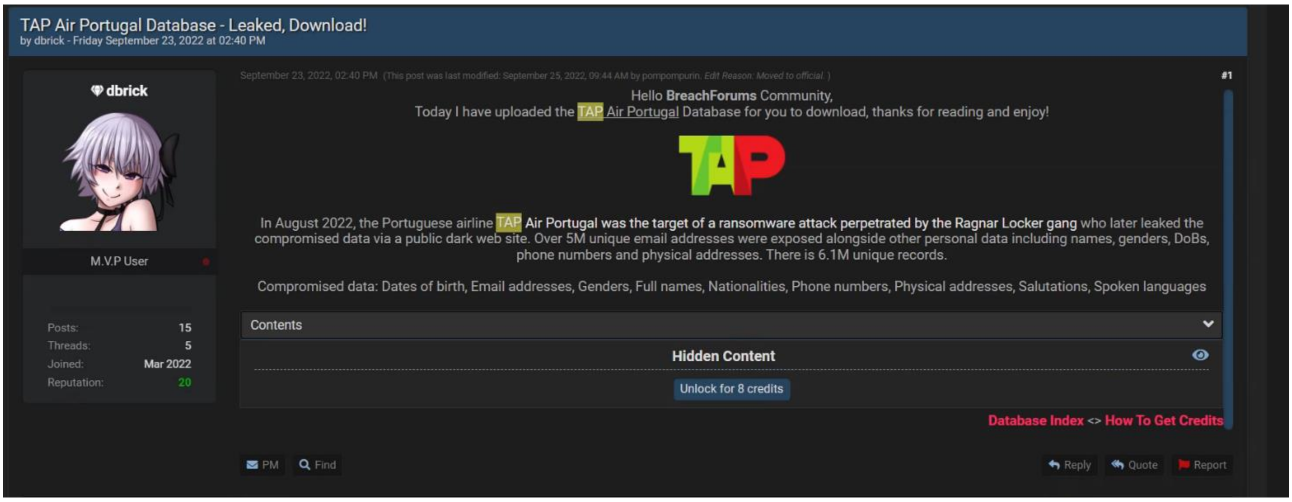


```
- [20/Aug/2022:19:47:49 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
- [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
```

Figure 7: Lockbit's proof of Entrust's DDoS attack

Although we can't know for sure whether Entrust initiated or hired someone to perform the DDoS, this is still an unusual event.

Another unique incident occurred as RagnarLocker compromised TAP Air Portugal (Figure 8). To their surprise, TAP Air demonstrated that they are no pushovers and retaliated with a DDoS attack on RagnarLocker's servers.



TAP Air Portugal Database - Leaked, Download!
by dbrick - Friday September 23, 2022 at 02:40 PM

dbrick

M.V.P User

Posts:	15
Threads:	5
Joined:	Mar 2022
Reputation:	20

September 23, 2022, 02:40 PM (This post was last modified: September 25, 2022, 09:44 AM by pompompurin. *Edit Reason: Moved to official.*) #1

Hello **BreachForums** Community,
Today I have uploaded the TAP Air Portugal Database for you to download, thanks for reading and enjoy!

In August 2022, the Portuguese airline TAP **Air Portugal was the target of a ransomware attack perpetrated by the Ragnar Locker gang** who later leaked the compromised data via a public dark web site. Over 5M unique email addresses were exposed alongside other personal data including names, genders, DoBs, phone numbers and physical addresses. There is 6.1M unique records.

Compromised data: Dates of birth, Email addresses, Genders, Full names, Nationalities, Phone numbers, Physical addresses, Salutations, Spoken languages

Figure 8: RagnarLocker's announcement of TAP Air Portugal attack

In addition to RagnarLocker and Lockbit3.0, other groups including LV, Everest, Hive, BianLian, Quantum, Yanluwang and other were documented as being victims of various DDoS attacks.

INTERMITTENT ENCRYPTION

The cat and mouse game between ransomware groups and security vendors push both sides to think of new creative ways to achieve their goals. Usually, the result is that the ransomware groups show us new techniques and TTPs we haven't seen before.

Blackcat/ALPHV and BlackBasta provided us with a new encryption technique. After discovering that security vendors were able to identify their encryption module, these decided to improve their encryption mechanism to handle each file separately. BlackBasta is basing their new encryption module on file size where for files under 704 bytes they encrypt the whole file, for files that are less than 4KB they encrypt every 64 bytes and skip 192 bytes. For larger files, they encrypt 64 bytes but skip 128 bytes.

Blackcat uses a similar mechanism but they also provide configuration for the user to decide the form of byte-skipping patterns.

Using this technique, the encrypted files are still unreadable/corrupted on the one hand, but on the other hand, the process is quick and undetectable.

It is important to understand that all these small changes seem insignificant when it comes to the development of the module, but it could take weeks or even months until the security vendors identify and expand their products' capabilities to identify and protect against this technique.

In addition, like many other businesses, it is highly likely that other ransomware groups will copy this mechanism for their campaigns in one form or another.

NEWCOMERS

During Q3 2022, the Cyberint Research team identified over 85 new ransomware groups. Given the competitive and sophisticated skills threat group require in order to succeed in this field, obviously not all of them will become the next Lockbit3.0, but here are a few worth mentioning that we expect to see more of.

BIANLIAN

BianLian is a new ransomware group that emerged in mid-July and are looking to make a name for themselves.

The group has already managed to compromise at least 21 victims, mainly targeting North America. Given the strong start for the ransomware group, evidence suggests they have invested a lot in strengthening their C&C servers infrastructures and are currently looking to build a better technical foundation.

What makes BianLian versatile is their cross-platform support, which means they are able to target all kinds of assets in the victim's environment. Their main product is written in GoLang, which more and more threat groups are using for developing their malware (not necessarily ransomware).

Previous campaigns suggest that the group is looking to compromise front-facing instances such as the SonicWall VPN and Microsoft Exchange Server.

The group's operational flow usually involves leveraging access they've gained through installing a Web shell or Ngrok payload. In addition, the group regularly utilizes living off-the-land techniques to achieve lateral movement and monitor network activities.

When it comes to staying undetected in the encryption phase, BianLian uses the relatively new technique used by many other groups. Like others, BianLian often executes the encryption module in Windows Safe Mode, which allows the module to run silently and remain undetected by the various security vendors. The pre-encryption phase includes deleting snapshots and backup files.

In the ransomware industry, it takes time and consistency to become a massive threat. BianLian has achieved a lot in its first three months, and if they're able to keep up with the big league's groups, they might become a solid and very threatening ransomware group in the first half of 2023.

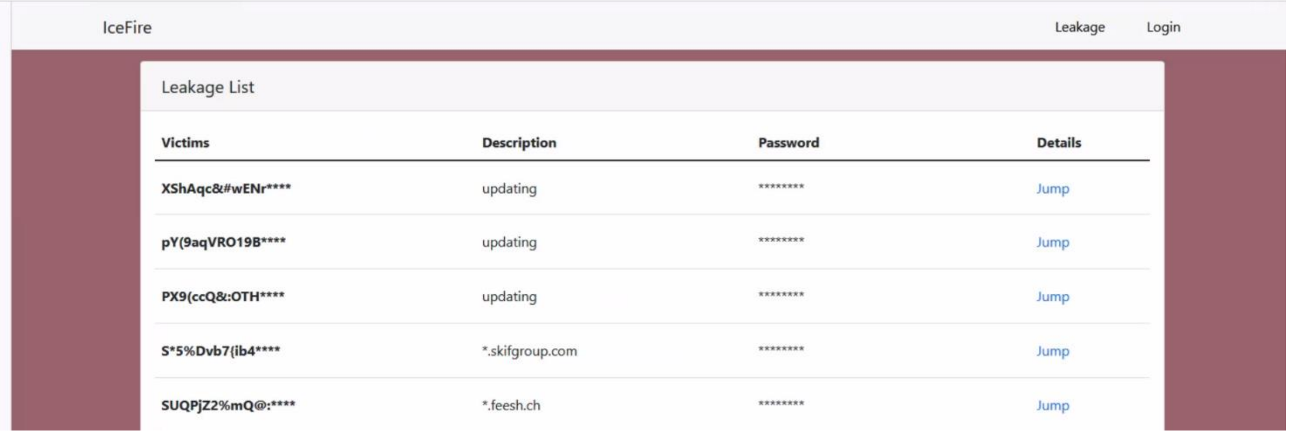
ICEFIRE

IceFire is an unusual ransomware family that has emerged this quarter, and targeted victims from less "popular" countries such as Turkey, Pakistan, and Morocco.

Of the three ransomware families we chose to highlight in this report, IceFire has claimed to compromise the highest number of victims − 46. When it comes to sectors, IceFire is also diverse, targeting a range of sectors such as finance, IT, education, and manufacturing.

This new ransomware group publishes all its victims with the "Description" tab that indicates if the victim has already paid or not.

Oddly enough, the names of the victims are published in what seems to be generated strings (Figure 9), so the only way for us to know who the actual victim is if the victim decided not to pay. In this case, the victim's domain appears in the "Description" tab mentioned.



Leakage List

Victims	Description	Password	Details
XShAqc&#wENr****	updating	********	Jump
pY(9aqVRO19B****	updating	********	Jump
PX9(ccQ&:OTH****	updating	********	Jump
S*5%Dvb7{ib4****	*.skifgroup.com	********	Jump
SUQPjZ2%mQ@:****	*.feesh.ch	********	Jump

Figure 9: IceFire Onion site

IceFire seems to be new but skilled with a lot of room to grow. They try to have their own unique style and to separate themselves from "normal ransomware groups". It seems like their skill might help them stay consistent in the industry for a while.

SPARTA

Sparta is one of the newest ransomware groups that emerged in mid-September. The group has already claimed at least 13 victims, mainly focusing on Spain.

Some speculations suggest that Sparta is a rebrand, or at least contains, former REvil members, given the basic layout of their leak site.

The group operates an onion page where they publish all of their victims. Given the fact that the group is mainly initially focusing on Spain, we can conclude that this region is where they feel most comfortable.

Like other new groups, Sparta has gained much attention in underground forums, both from the members who are advertising the group at any given opportunity and from Telegram and forum admins who talk about and promote the group.

When it comes to targeted sectors, it seems that Sparta doesn't only focus on one sector, and is looking to cover as many sectors as possible.

The group hasn't been documented in big-name campaigns so far, but in observing their product, we see that they are still at the point where they are constantly growing and developing foundations for their RaaS (Ransomware as a Service) members.

Although Sparta has less traction and "noise" around them compared to IceFire and BianLian, they have the potential to act as a solid threat actor in the ransomware industry that might not contest the "big leagues", it is still capable enough to cause some real damage to their victims.

CONCLUSIONS

During 2022, so far we have seen a consistent decline in the number of ransomware campaigns from quarter to quarter. The reason for this decline is the disappearance of the experienced groups such as Conti, REvil and PYSA, and the birth of new, inconsistent or immature groups that are still building their own legacy and foundation.

This situation leaves only one veteran, Lockbit3.0, as the group that leads the ransomware industry by a margin, and contrary to the rest of the industry, keeps on growing its victim count.

This decline provides temporary comfort given that once these fairly new groups establish themselves better professionally, we should see the numbers we are used to seeing from Q1 and even higher.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

USA - NY

Tel: +1-646-568-7813
368 9th Ave, Suite 11-108, New York, NY 10001

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

UNITED KINGDOM

Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536