Cyberint

Impactful Intelligence

RANSOMWARE RECAP 2022

January 2023

TABLE OF CONTENTS

EXECUTIVE SUMMARY

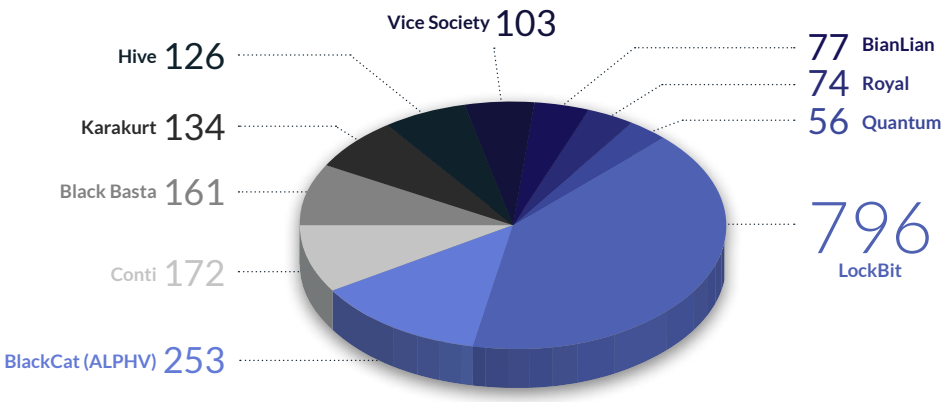
2022 brought with it many crazy stories that we'll be talking about for years to come, as the ransomware industry continued growing and introduced us to many new groups.

The year's big story was the rise to power of LockBit3.0, which dominated the entire industry following the disappearance of Conti after the ContiLeaks incident.

Although a lot of new ransomware emerged in 2022, including BlackBasta, Royal and BianLian, none could match LockBit3.0's abilities to claim the massive 796 victims, not too far from what LockBit and Conti combined in 2021 (Figure 1).

Figure 1 //

TOP 10
RANSOMWARE FAMILIES



Overall, in 2022 the ransomware industry claimed 2,809 victims, a decline of only 36 victims compared to 2845 victims in 2021.

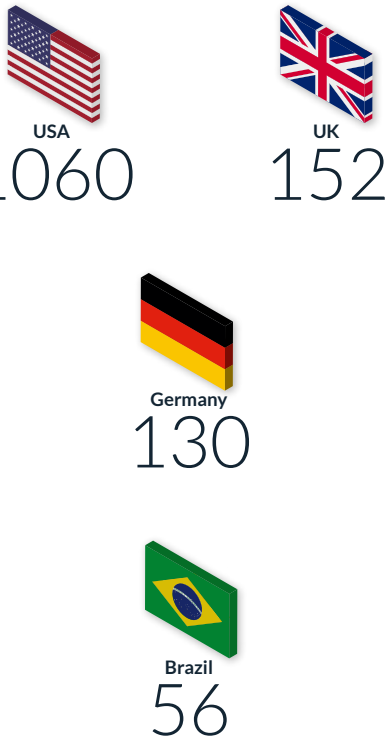
Although LockBit3.0 is currently the leading ransomware group, we should all fear and be on the look-out for, other groups that also made major impacts this year.

RANSOMWARE INDUSTRY STATS

The ransomware industry stats draw an interesting picture compared to last year. When it comes to the most targeted regions of the world, there are no real surprises as the US is still in the lead with 1060 victims, a decline of almost 300 victims since last year, followed by the UK, Canada and Germany (Figure 2).

Figure 2 //

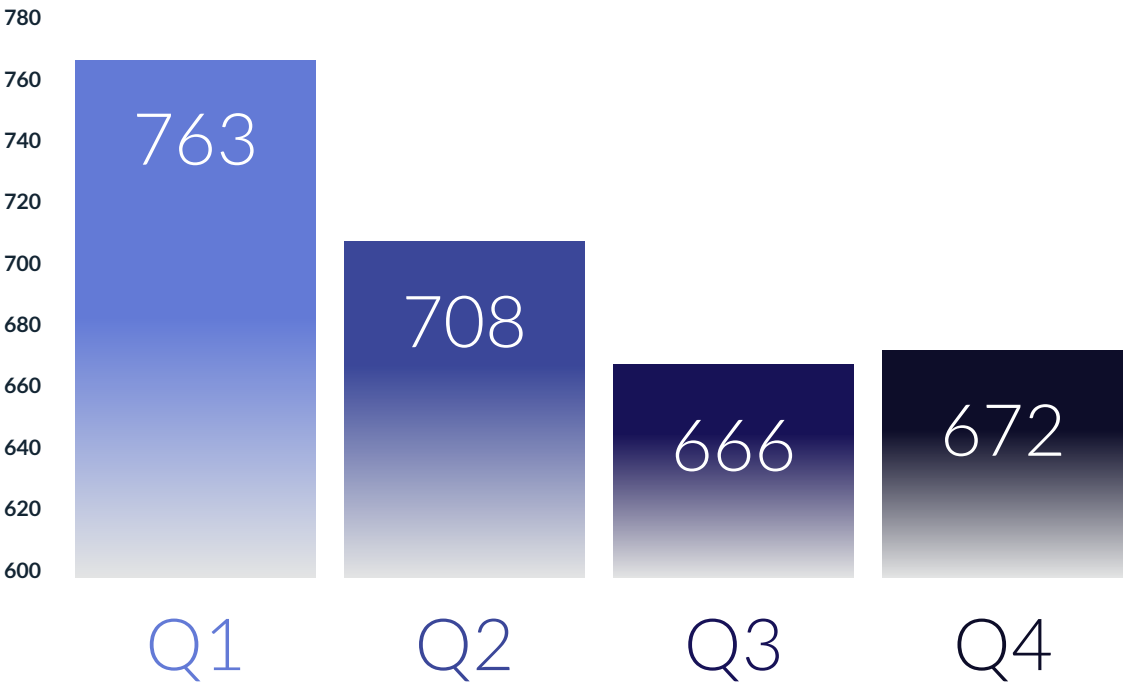
TOP 10
TARGETED COUNTRIES



In addition, the ransomware industry suffered inconsistency throughout the year when it comes to victims count (Figure 3).

Figure 3 //

VICTIMS COUNT
PER Q



Q1 was most successful, seemingly continuing on from the success of the previous year. Conti was still around and along with LockBit's development, both groups led the ransomware industry.

After the beginning of the Russia-Ukraine conflict and the ContiLeaks incidents, the ransomware industry was plagued with inconsistency as the only group that acted as a major threat was LockBit that soon took over the industry.

This turning point mainly impacted Q2 and Q3, while Q4 seems to have experienced a bit of an increase, probably due to the new and promising groups established in Q3 and Q4 such as Royal and BlackBasta.

2022 TOP INCIDENTS

As mentioned, 2022 provided us with many stories and events to talk about and to learn from, from ContiLeaks to the return of REvil and the short appearance of LAPSU$.

Here are some notable incidents that shaped the ransomware industry this year.

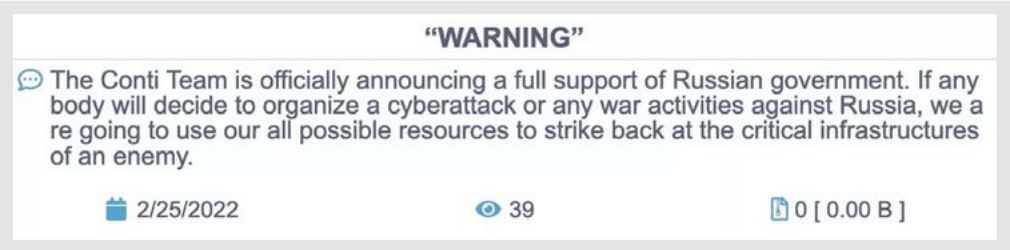
CONTI LEAKS

The most impactful case, which changed the face of the entire industry was, without a doubt, the ContiLeaks incident.

As the Russia-Ukraine conflict developed, we saw many ransomware groups in particular, and hacking groups in general, taking sides and going at each other. Conti could have picked a side or stayed silent. As we suspected, Conti chose to side with Russia (Figure 4), and this was the turning point for the group that used to be the most dominant in history.

Figure 4 //

CONTI'S ANNOUNCEMENT THAT THEY WERE SIDING WITH RUSSIA



A few hours after the announcement, an alleged security researcher (presumably a former member of the team), who unfortunately for Conti, was Ukrainian, decided to expose the group and leak every shred of information he was able to leak. Leaks of threat groups are not a new phenomenon, but this case was different both because of the group and the content of the leak.

The security researcher opened a Twitter account named ContiLeaks, which is where he published, piece by piece, a massive amount of information about the group, including crypto-wallet addresses, personal conversations from the past 2 years of all members of the group, the source code of all the tools Conti used and developed, faces and pictures of the members, and more.

This leak was so extensive, that we could draw a clear picture of the key members, day-to-day operations, how the organization was built (Figure 5), government relationships and how many members Conti included, which was an astonishing number of around 300 members.

Figure 5 //

CONTI'S ORGANIZATION STRUCTURE

Overall, Conti made nearly $3 billion throughout 2020 and 2021, and gave us a clear estimate of how much a ransomware industry-leading group could earn from their campaigns.

Immediately after the leaks, we were able to see via the last conversations in Conti's chat server that the decision was made to go off the grid for some time. It seems that the key members of the group made efforts to ensure that all relevant files were deleted, all links shared within the conversations were dead, and all servers used for the organization's infrastructure were down.

A few weeks later Conti returned with some new victims, but something was different when it came to how the group managed its Onion page, the victim profiles they chose to target, and other behavior patterns that didn't seem typical to the Conti we all knew in the past two years. The operators seemed less mature and a bit impulsive in their actions and statements.

It was clear that two things were going to happen from that point on - Conti was slowly dying and could disappear in the subsequent months and LockBit would become the most popular and successful ransomware group in the industry - which eventually happened.

Currently, there is much speculation about where the operators are now, what are they up to, and which of the new groups that emerged after Conti is a rebrand, but it seems that there are no precise answers to those questions just yet.

LOCKBIT3.0'S RISE TO POWER

As mentioned, LockBit took advantage of the opportunity and claimed first place in the ransomware industry after Conti's death, in a year full of interesting activities.

LOCKBIT3.0 INTERVIEWS

Unlike other threat groups, LockBit3.0 doesn't operate any Twitter accounts. Nevertheless, they do look to promote themselves in other channels.

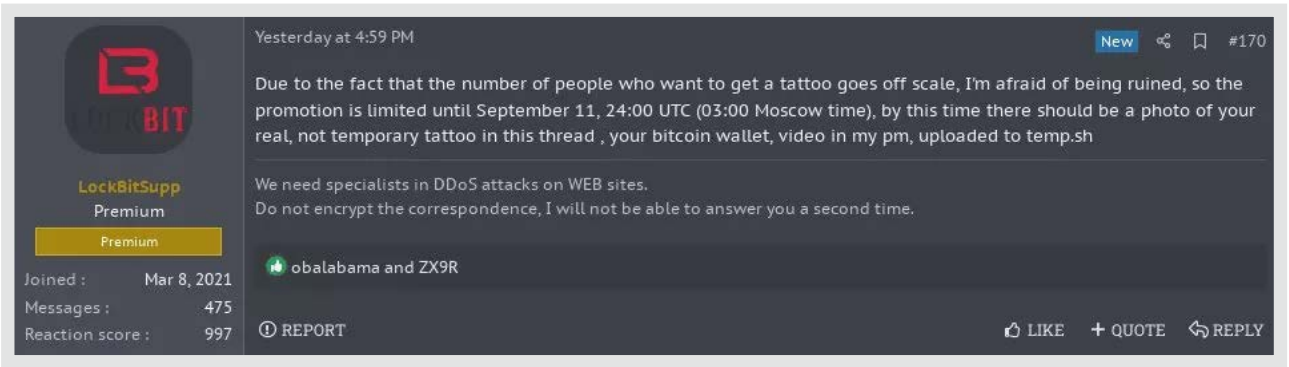
LockBit3.0 members gave two interviews in 2022 to a cyber security magazine and the popular VX-Underground community. They talked freely about their exploits, describing the structure of the group, giving some success rate stats, and sharing their plans for the future along with money laundering techniques, their origins, and much more.

TATTOO CAMPAIGN

Another LockBit3.0 PR effort this year 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. In light of the massive response, the group had to publish another announcement that they were limiting the offer (Figure 6).

Figure 6 //

LOCKBIT3.0 TATTOO CAMPAIGN'S & ANNOUNCEMENT



The reputation of the group was somewhat damaged by this campaign because some fans of the group claimed they had tattoos done of the group but did not receive any payment.

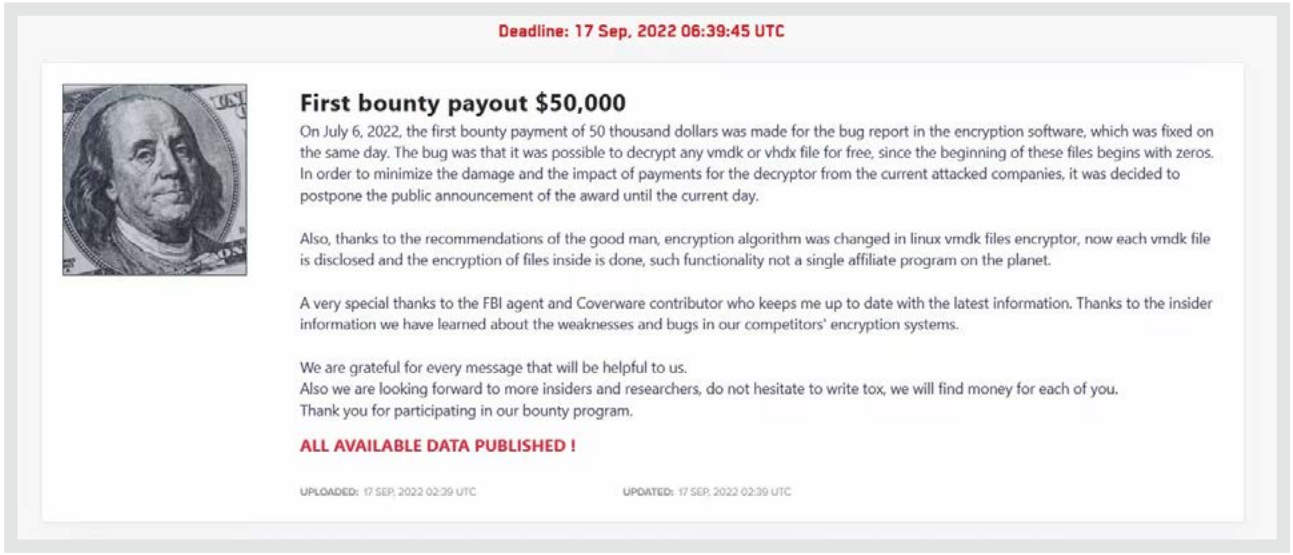
BUG BOUNTY PROGRAM

This wasn't the first time that LockBit3.0 demonstrated its arrogance, and their next move was not surprising. The group offered a bug bounty program to anyone finding vulnerabilities in their servers.

As expected, the program drew the attention of many followers and researchers. The group claimed that they already paid the first bounty of $50,000 in July 2022 (Figure 7).

Figure 7 //

LOCKBIT3.0'S BOUNTY PAYOUT ANNOUNCEMENT



THE ARREST & RETURN OF REVIL

2022 started with one major event as the REvil ransomware group was arrested. While this major RaaS group had been dying for almost a year, on January 14, Russian law enforcement put the final nail in its coffin by arresting the last of REvil's operators (Figure 8).

Figure 8 //

REVIL ARREST

Although the arrest was important, and mostly political, many people claim that this arrest was mostly a PR stunt on the part of the law authorities at the expense of a dying group, and that the arrest was carried out way later than it should have been.

Although REvil was a symbol in the ransomware industry and was one of the most popular groups, at the time of the arrest, it made little to no impact on the ransomware industry.

Several months after the Russia-Ukraine conflict began, the REvil Onion site came back online, and since then, the group has claimed very few victims. Some speculation suggests that REvil operators, or at least the ones who do not matter anymore, were released and resumed their old habits.

It is important to note that the group is still active under the name of REvil2.0, although it is far removed from the REvil that wreaked havoc a few years ago.

LAPSU$ - A LOT OF DAMAGE WITH LITTLE TALENT

Lastly, Lapsus was a group that taught us a valuable lesson and showed us the harsh truth - you no longer have to be skilled to cause damage.

Although Lapsus commenced its operations in December 2021, they made their greatest impact in 2022, compromising major organizations such as NVIDIA, Vodafone, Samsung Microsoft, LG and Okta.

The Lapsus group kept things simple and had some unique characteristics, whether it was their leak channel, the way they chose their victims, or initial infection methods.

NVIDIA INCIDENT

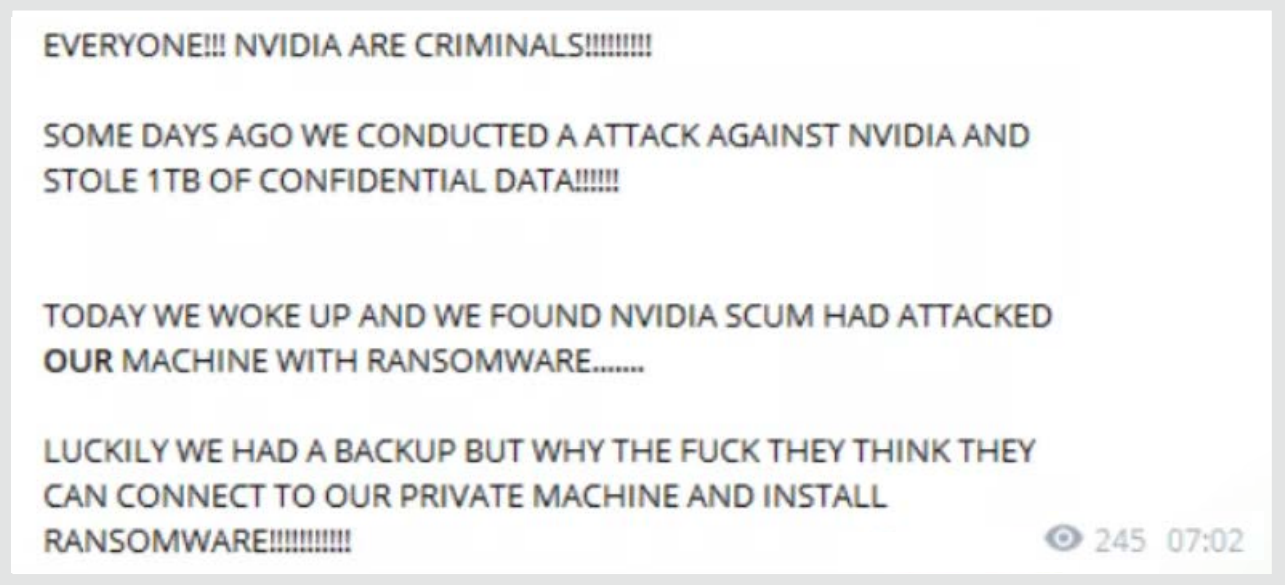
One of the group's most popular cases was the NVIDIA incident. While the whole world, including the cyber world, was focused on the first days of the Russia-Ukraine conflict, Lapsus launched a campaign against tech giant NVIDIA.

On February 28, the group shared an announcement on their Telegram group that NVIDIA had been hacked. The official announcement shared that Lapsus had gained access to NVIDIA's infrastructure for a week and reached the most sensitive data. The group also exfiltrated 1TB of information including schematics, drivers, firmware, SDKs, documentation and Fast Logic Controller (Falcon).

The odd detail in this story was Lapsus' claim that NVIDIA attacked its servers in return (Figure 9).

Figure 9 //

LAPSUS ACCUSATIONS AGAINST NVIDIA



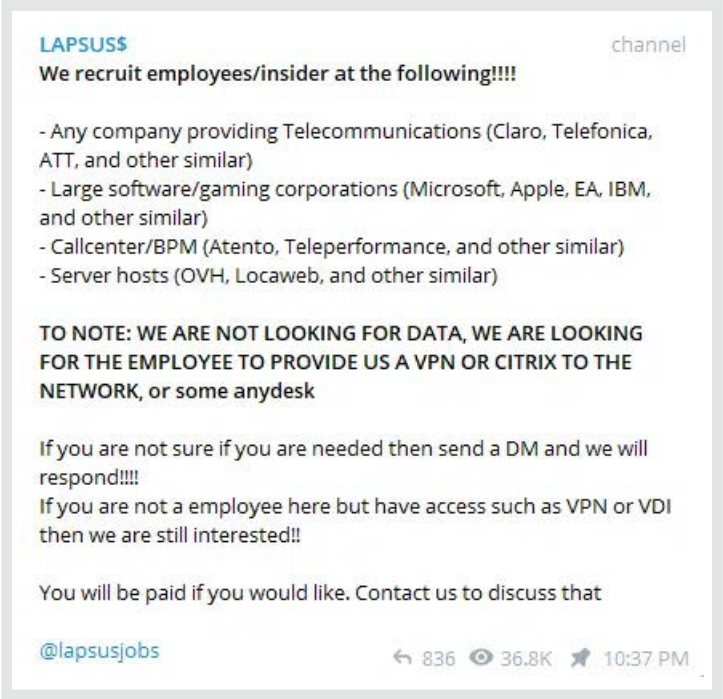
INFECTION METHODS

The Lapsus saga was short but impactful. The Latin American ransomware group taught us a lot about the insider threat that might be the most devastating point of failure, even for the most fortified organizations.

Unlike most ransomware groups, Lapsus mainly focused on recruiting employees who can be bribed to disclose their credentials (Figure 10), or buying leaked credentials from other threat actors or access brokers.

Figure 10 //

LAPSUS RECRUITMENT ANNOUNCEMENT



THE DEATH OF LAPSUS

As mentioned, Lapsus didn't last long. Poor OpSec led to the arrest of several individuals linked to the group and eventually, the group closed its Telegram channel. We haven't witnessed any new campaigns of a group that identified as Lapsus for some months.

MIXING BUSINESS WITH POLITICS

One of the main cybersecurity lessons that the Russia-Ukraine conflict taught us is that in these kinds of extreme cases, not all groups are able to maintain their "Business only" attitude.

One of the more unpredictable phenomena that occurred during the conflict was the involvement of threat groups and ransomware groups siding with either Russia or Ukraine.

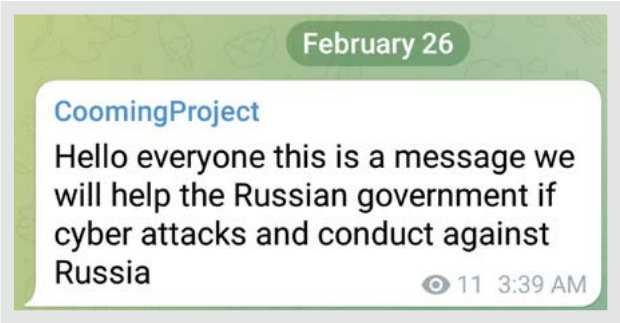
As mentioned, Conti also was one of the groups that sided with Russia and paid a big price for it. But they are not the only ones.

COOMINGPROJECT

CoomingProject was a French threat group that announced that it would retaliate if Russia became a target of cyber-attacks (Figure 11).

Figure 11 //

COOMINGPROJECT ANNOUNCEMENT OF SUPPORTING RUSSIA



CoomingProject came to the forefront as a result of the conflict, which was also why they were arrested. Their announcement caught the attention of AgainstTheWest, a threat group siding with Ukraine, which was able to compromise CoomingProject and fully leak all the information about its members to the local French police. And CoomingProject disappeared entirely.

BELARUSIAN CYBER PARTISANS

The Belarusian Cyber Partisans made real history as one of the first to use political ransomware before and after the beginning of the conflict.

One of their most popular campaigns was ransoming the Belarusian Railway. The group was able to compromise the railway that was used by the Russian government to transport supplies, military equipment and troops to the Ukrainian border. After gaining control of the railway, they were able to create massive delays and even complete shut downs of valuable supplies during the warfare.

The ransom they demanded in this campaign was the release of over 50 political prisoners from the Russian government. Throughout the first days of the conflict, the group kept giving live updates of their actions on their official Telegram channel (Figure 12).

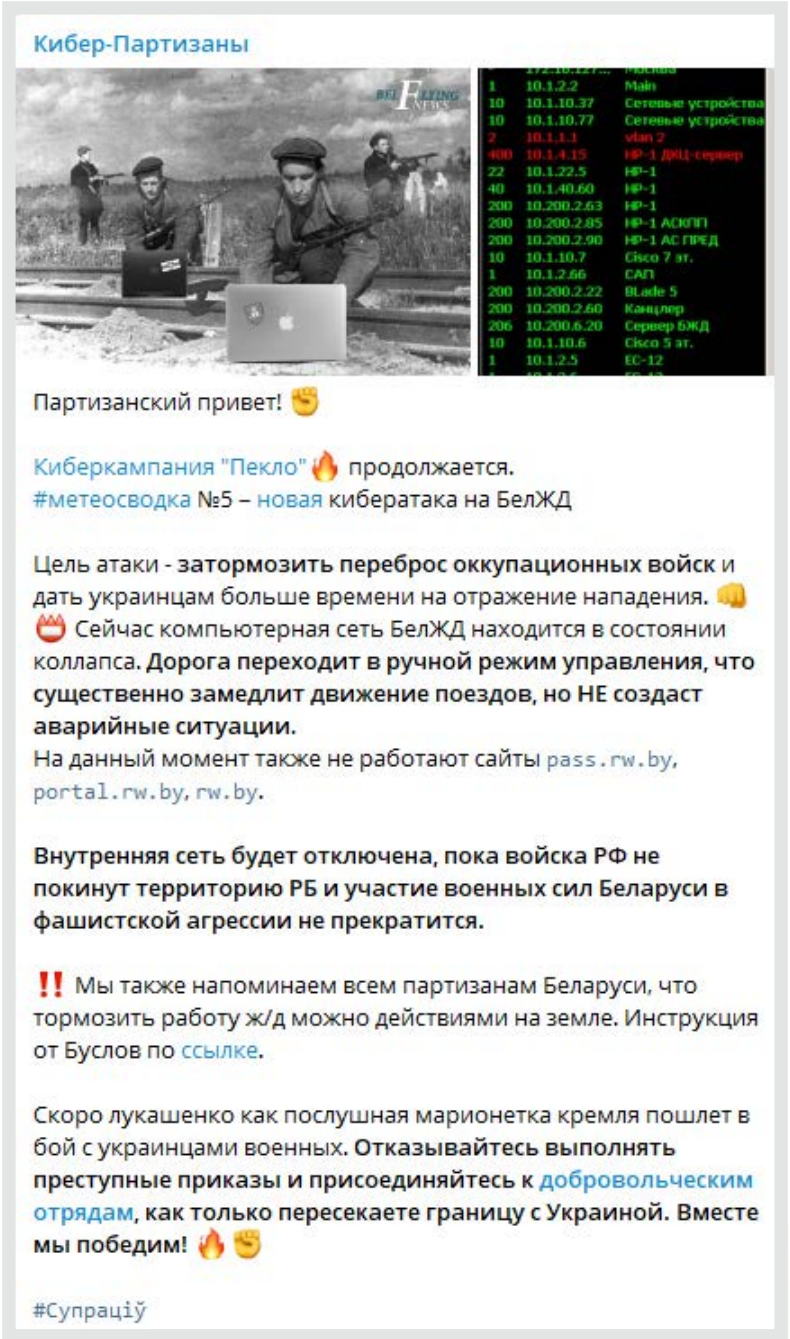


Figure 12 //

BELARUSIAN CYBER PARTISANS UPDATES ON THEIR TELEGRAM CHANNEL

LOCKBIT3.0 - BUSINESS COMES FIRST

Contrary to most threat groups, LockBit3.0, (previously LockBit2.0), handled the situation differently and didn't make any irrational decisions. With great anticipation from the cyber security community, LockBit3.0 published its announcement with one simple message - Business comes first (Figure 13).

Figure 13 //

LOCKBIT3.0 ANNOUNCING THEY ARE NOT TAKING SIDES

```
Many people ask us, will our international community of post-paid pentesters, threaten the west on
critical infrastructure in response to cyber aggression against Russia?
Our community consists of many nationalities of the world, most of our pentesters are from the CIS
including Russians and Ukrainians, but we also have Americans, Englishmen, Chinese, French, Arabs,
Jews, and many others in our team. Our programmers developers live permanently around the world in
China, the United States, Canada, Russia and Switzerland. Our servers are located in the Netherlands
and the Seychelles, we are all simple and peaceful people, we are all Earthlings.
For us it is just business and we are all apolitical. We are only interested in money for our
harmless and useful work.  All we do is provide paid training to system administrators around the
world on how to properly set up a corporate network. We will never, under any circumstances, take
part in cyber-attacks on critical infrastructures of any country in the world or engage in any
international conflicts.
```

The group claimed they consist of many types of individuals from all over the world and they only care about succeeding in business. In order to do so, they have to keep away from politics, which ultimately seemed to work very well for them.

NEWCOMERS TURNING INTO BIG LEAGUERS

BLACKBASTA

BlackBasta is a fairly unique and interesting group that emerged in the ransomware industry in mid-early 2022. The Russia-based ransomware group really shined over the past six months as it was able to claim 145 victims - a number that seems subpar compared to the explosive numbers LockBit achieved this year, but is still impactful for one single ransomware family.

CONTI RELATIONS?

As the group seemed to remain consistent since their emergence, some speculation from the cybersecurity community claimed that they are the rebrand of the Conti members who left the group after the ContiLeak incident.

Once speculation became mainstream, Conti, in its last days, responded aggressively on their Onion page as part of its “For Peru” campaign (Figure 14), claiming there is no link between the two groups. might see several innovations and shortened times between new malware variants given this technology.

Figure 14 //

CONTI ANNOUNCING BLACKBASTA HAS NO RELATIONS TO THEM

BIANLIAN

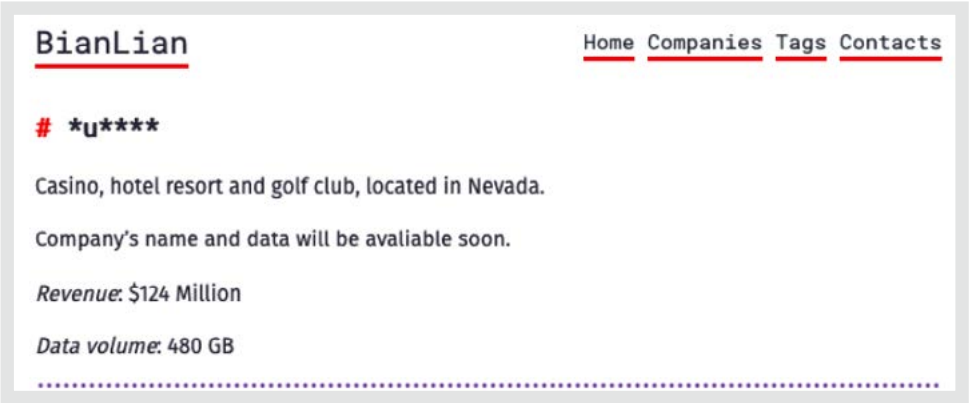
When summarizing 2022's newcomers, we had to include BianLian, another ransomware family that we observed, as it started strong and claimed 62 victims in five months of operation.

We found that their victims were mostly from the North American region.

Some speculations suggest that BianLian is currently investing most of its time and efforts in establishing a solid infrastructure foundation that it can work with and deploy its C&Cs properly while still being able to compromise new victims every week.

Figure 15 //

VICTIM'S ANNOUNCEMENT ON BIANLIAN'S ONION PAGE



What makes BianLian versatile is its 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 to develop their malware (not necessarily ransomware), given the fact that it is more complex to analyze.

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

When it comes to staying undetected in the encryption phase, BianLian uses a familiar 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.

ROYAL

One of the fiercest and most determined ransomware groups that emerged in 2022 is most definitely Royal. One cannot write about the new groups in the ransomware industry without mentioning them.

The group stormed into the ransomware industry at the beginning of November and in December already claimed 49 victims - a rate that is even higher than LockBit3.0.

The Royal ransomware family is very new to the industry but has already made a significant mark and might be a real challenger to all ransomware families with this performance - even to LockBit.

Like many others, Royal maintains an Onion page, which is where they publish their new victims (Figure 16).

Figure 16 //

VICTIM ANNOUNCEMENT ON ROYAL'S ONION PAGE

Although not much is known about the group as it is still young and still growing, like BlackBasta and BianLian, speculation has it that Royal is also a descendant of the notorious Conti group, as they are the only ones who claim numbers of victims similar to Conti. Having said that, as of publication, they have only been operating for one month, and they might turn out to be a solid ransomware group, but still far off Conti or LockBit's level.

ROOM TO GROW

When we look back at 2021, new ransomware groups such as AvosLocker emerged without claiming a high number of victims, but still were able to become an impactful threat that we had to consider very seriously in our attack surface. BianLian, BlackBasta, and Royal are in a similar position to what AvosLocker was in 2021, and they might also become dominant players that represent a new age in the ransomware industry and represent a new challenge to LockBit3.0.

CONCLUSIONS

The ransomware industry is on a cusp of an extremely important era, as the Conti family disappeared, and LockBit3.0 became the number one team, maybe in the history of the ransomware industry.

2022 showed us the adaptability of LockBit3.0 and its ability to take advantage of any opportunity.

In addition, in 2022 we discovered several new groups that are most likely to survive and thrive in the future, challenging LockBit3.0 as they develop and fully establish themselves.

Overall, the ransomware industry is currently creating a new generation of ransomware groups that most likely will fill the void Conti left, especially if members of these groups might be ex-Conti members.

Cyberint

CONTACT US

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

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

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

USA – TX
Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

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

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

JAPAN
Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.