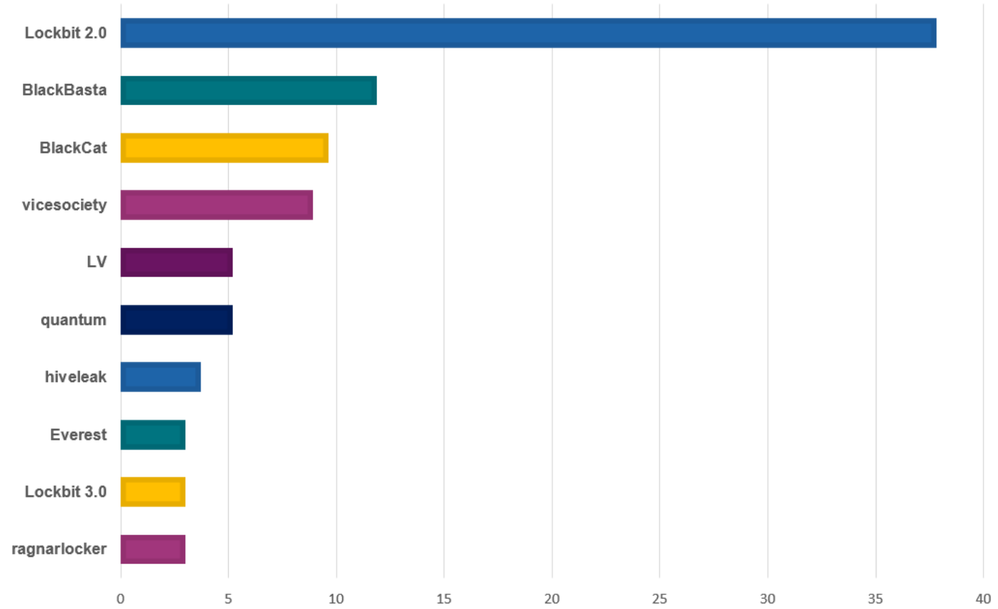
Monthly Threat Pulse
June 2022

We are continuing to track ransomware groups operating the hack and leak double extortion tactic, this is achieved by actively monitoring the leak sites used by each ransomware group and scraping victim details as they are released.

By recording this data and classifying the victims by sector, we can derive additional insights such as, which sectors are being targeted this last month, and how do these insights compare to previous months?

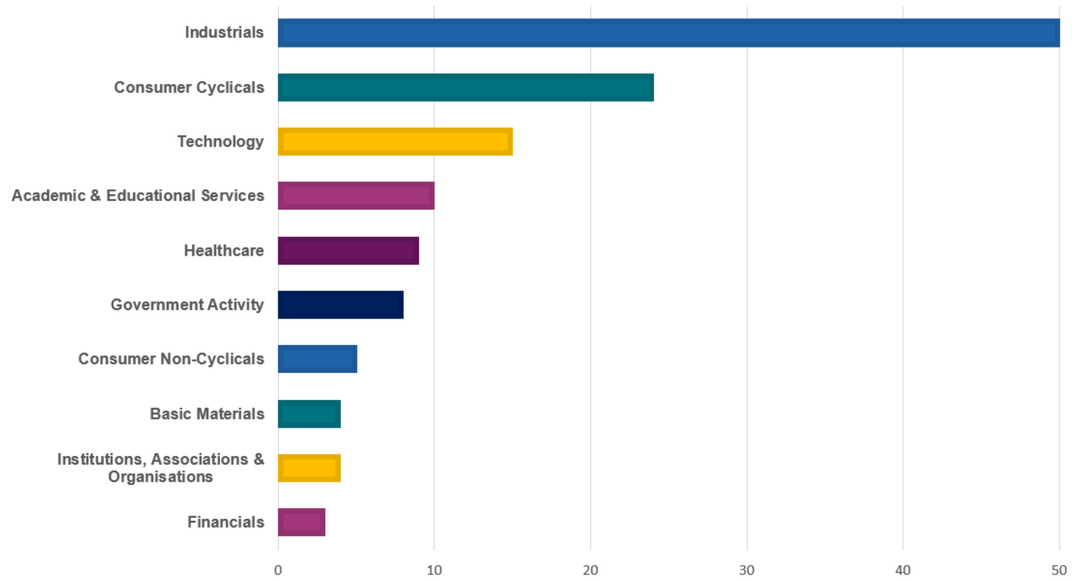
Key data

Number of Victims by Group in June 2022

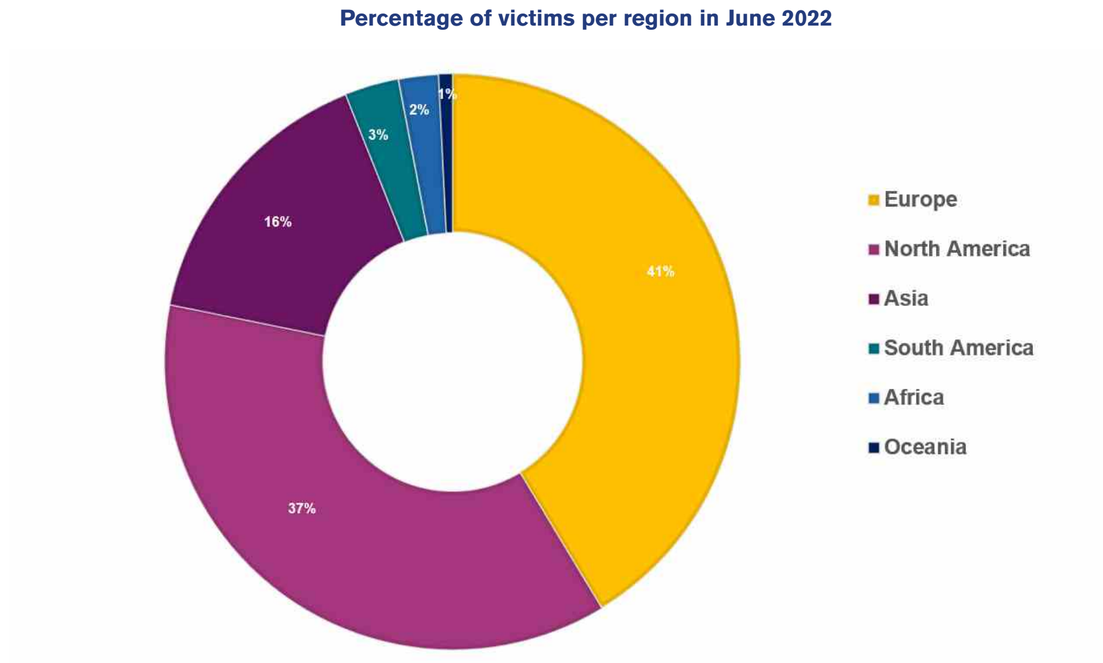


Key data

No. of Victims by Sector in June 2022



Key data



Analyst comments

This June we observed a total of 135 ransomware attacks, a significant drop in incidents from May (236), representing a 42% percentage decrease.

With almost half the number of attacks, several reasons may be at play. Since May, a number of changes have occurred to the dominant threat actors within the cybercrime landscape.

Last month, we discussed the rebranding of our second most prominent ransomware strain, Conti, which has likely impacted the number of incidents as the threat actors behind re-establish themselves.

Likewise, LockBit2.0 has evolved, developing its new ransomware strain LockBit3.0 and enhancing capabilities.

Looking back at 2021, only a small variation in the number of ransomware attacks was identified between May (224) and June (219).

Whilst a larger drop was observed between June (219) and July (159), it appears that the summer months of 2021 did not experience as greater decrease as we are witnessing now.

As such, whilst seasonal variation may affect the statistics this June, it is more likely that the changes we have observed to our key ransomware variants (Conti and LockBit2.0), are responsible.

Moving forward, it will be interesting to see how this impacts the threat landscape in the coming months, i.e. an increase in attacks.

Sectors

Three key sectors remain at the forefront of threat actor targeting; Industrials, 50 incidents (37%), Consumer Cyclicals, 24 incidents (18%) and Technology, 15 incidents (11%).

Given the overall decrease of 42% between May and June, a substantial reduction in attack numbers was expected for these sectors from their figures in May; Industrials 73, Consumer Cyclicals 53, and Technology 29.

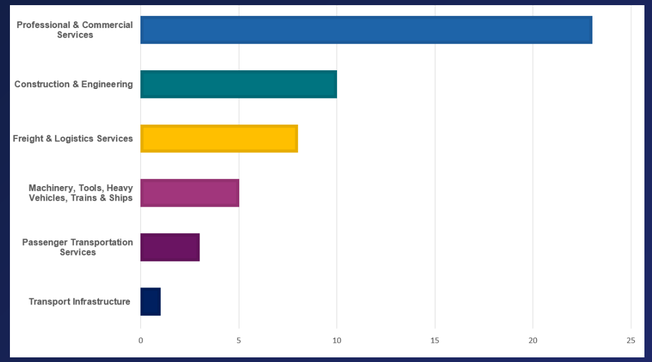
Interestingly however, Industrials reflects the least amount of change, with a decrease of only 30%, re-stating its position as a highly attractive and vulnerable target.

Industrials

Products and services within the Industrials Sector form part of many supply chains meaning that any interference will lead to widespread and costly disruption.

Much of the sector is characterised by operational technologies (OT) and legacy systems newly converged with internet technology (IT).

As many of these networks are not segmented, the possibility for lateral movement across IT and OT infrastructure increases threats to production and safety.



No. of Ransomware Victims for the Industrials Industries

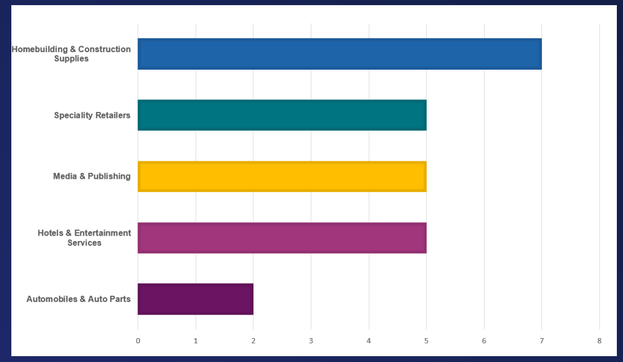
Ransomware actors exploit these weaknesses to pressurise organisations into payment.

Analysis of the industries within revealed Professional and Commercial Services (23 incidents) and Construction and Engineering (10 incidents) as most targeted.

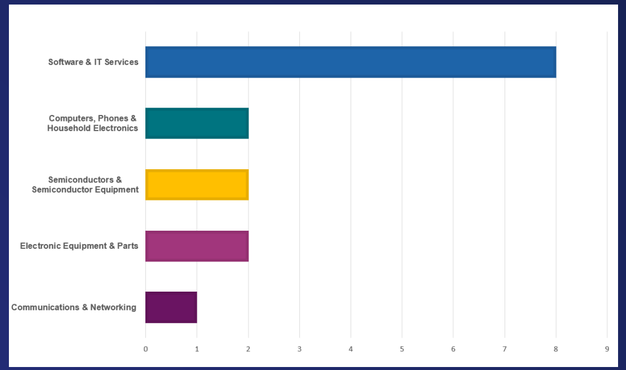
This is consistent with the targeting patterns we have observed over the previous months and should encourage organisations within to strengthen their cybersecurity posture.

Professional and Commercial Services, whilst less associated with OT systems, accounts for many company types which likely results in a greater number of attacks.

Construction and Engineering by contrast contributes to manufacturing processes and these have been highly targeted by ransomware across 2021 and into 2022.



No. of Ransomware Victims for the Consumer Cyclicals Industries



No. of Ransomware Victims for the Technology Industries

Consumer cyclicals

The Consumer Cyclicals Sector continues to rank in second place (24 incidents). Responsible for the provision of widely consumed, non-essential goods within society, disruption to products and services used in everyday life provides an attractive target as organisations seek to restore business operations.

This June, the most targeted industry concerned Homebuilding and Construction Supplies with 7 incidents (29%). Whilst organisations within should reinforce their cyber security posture, industry targeting often fluctuates as such, it is best practice for all within the sector to ensure strong cyber hygiene.

Technology

Technology Sector remains third most targeted with 15 incidents in June, with a particular interest in the Software and IT Services industry accounting for 8 incident (53%).

Notably, the industry is likely to form part of many supply chains for which disruption would be catastrophic to the immediate victim and partner organisations. Looking ahead, we except these three sectors to remain highly targeted, in line with the targeting pattern observed over the last 5 months.

Threat Actors

Our top two prevalent threat actors in June continue to be LockBit and Black Basta. LockBit's total attacks decreased from 95 in May to 55 in June a 42% drop in activity, possibly attributed to the fact that they are transitioning into their LockBit 3.0 variant. Black Basta attacks decreased from 17-16, representing a minimal 6% decrease in their activity. Finally, BlackCat's total attacks fell from 15 – 13 (13%) which is again, a rather inconsequential drop in activity.

In June, only 1 incident was observed by Conti, a 94% decrease in activity since May (17 attacks). This can be attributed to their disbanding and abandoning of their previous alias as they branch out and integrate themselves with other, smaller groups.

Going forward, it is likely that we will see a proportionate increase in activity from some of the smaller groups due to the assistance of Conti members

LockBit 2.0/3.0

Although there is a general decrease in overall activity in the ransomware threat landscape, LockBit continue to be at the forefront in June 2022.

LockBit's total attacks did decrease from 95 in May 2022 to 55 in June 2022 (marking a 42% decrease) but this is still 244% more than the group in second place (BlackBasta) highlighting that they are still the most prominent entity within the ransomware threat landscape.

NCC Group attributes this decrease in activity to their transition into LockBit 3.0 (Or LockBit Black, as they dubbed it themselves), as only 4 of their attacks published under their new alias took place in June.

We expect to see LockBit's activity to increase to their former prevalence if not surpass it, as they employ their new variant and take advantage of their new extortion tactics and bug **bounty scheme.**

Running parallel with previous months, LockBit's most targeted sectors were Industrials with 25/55 of all of their attacks in June 2022 (45%), Consumer Cyclicals with 9/55 (16%) and Technology with 6/55 (11%).

This shows that, although they are going through a transitionary period, they are maintaining their same breadth of targets.

Consequently, organisations operating within these sectors should consider the threat that LockBit historically presented, as well as the new threats that their new extortion tactics bring to the surface; discussed in our threat actor spotlight later on.

To focus in further on LockBit's victims, their top 3 most targeted industries were Professional & Commercial Services with 14/55 of all attacks (25%), Freight & Logistics Services with 6/55 (11%), and finally Government Activity with 5/55 (9%).

These stats do slightly differ from the previous month, when their most targeted industries were Professional & Commercial Services, Speciality Retailers, and Hotels and Entertainment Services.

As classifying attacks by industries is very granular, it is interesting to see that Professional & Commercial Services remains at the top of their priorities, likely due to the vast quantities of PII these organisations store related to various consultancy work.

Black Basta

Black Basta's activity in June 2022 has remained consistent with May 2022, with only a small decrease in attacks; from 17 – 16, representing a 6% decrease.

This stability in their attack frequency could be attributed to the fact that after Conti's dissolution, the members are thought to have joined Black Basta's ransomware operation, giving them the experience and technical ability to feature in the top players in the ransomware threat landscape.

NCC Group suspects this number will gradually increase as we progress towards the second half of 2022, as the group begins to utilise their new operators and develop a rhythm, being a relatively new group to begin with.

It will be interesting to see how Black Basta evolve and whether they will become one of the consistent top players in the ransomware threat landscape in Conti's stead.

Black Basta's targeting in June is largely focused on Industrials with 10 of their 16 attacks being within this sector (63% of their attacks).

In joint place for their second-most targeted sectors are Consumer Cyclicals and Technology with 2 attacks each (13%) and, finally, in joint third place, are Basic Materials and Financials with 1 attack each (6%). This targeting aligns with many threat actors in the landscape, including the late Conti, whose targeting had become more sporadic as they approached their end. NCC Group expect to see this targeting pattern to continue with larger figures in each sector as Black Basta develop.

In terms of industries, Black Basta's targeting is currently very diverse with Construction & Engineering slightly in the lead with 3 of their 16 attacks (19%). This is followed by Freight & Logistics and Machinery, Tools, Heavy Vehicles, Trains & Ships with 2 (13%). Finally, their third-most targeted industries were Banking Services, Chemicals, Communications & Networking, Media & Publishing, Software & IT Services, Specialty Retailers, and Transport Infrastructure with 1 attack each (6%). Black Basta is one of the few threat actors we have seen that have no victims in the highly targeted Professional & Commercial Services industry, implying that they may bring a new dynamic to the threat landscape as they mature.

BlackCat

Like Black Basta, Black Cat's activity has remained fairly consistent from May 2022 to June 2022 with a decrease of only 2 attacks from 15 – 13 (marking a 13% decrease). Though, these figures are still a sizeable drop from those that they exhibited from February – April, which averaged at around 22 attacks each. It has been reported that families such as Conti have begun utilising the BlackCat ransomware strain , but perhaps following their parting, they have put most of their focus on other ransomware offerings such as the aforementioned Black Basta, resulting in a diminished presence from BlackCat.

BlackCat's sectoral targeting reveals some interesting insights that, again differentiate from the usual trend of Industrials, Consumer Cyclicals and Technology. Their most targeted sector is still Industrials with 4 of their 13 attacks (31%). Conversely however, their second most targeted sector is Academic and Educational Services with 3 of their 13 attacks (23%).

Finally, their third most targeted sector is Consumer Cyclicals with 2 of their 13 attacks (15%). NCC Group will continue to monitor BlackCat going forward to see if a trend in targeting Academic & Educational Services develops.

Finally, BlackCat's industry targeting, like Black Basta's, is noticeably diverse with an emphasis on Schools, Colleges & Universities, which accounted for 3 of their 13 attacks (23%). Their second-most targeted industry was Professional & Commercial Services with 2 attacks (15%). Finally, in joint last place are Electric Utilities & IPPs, Food & Tobacco, Government Activity, Hotel & Entertainment Services, Machinery, Tools, Heavy Vehicles, Trains & Ships, Media & Publishing, Passenger Transportation Services and Software & IT Services with 1 attack each (8%). The diversity of these targets perhaps shows that BlackCat are more opportunistic in their approach, with little focus on the exact nature of the organisations that they are compromising.

Regions

In June, Europe received the highest number of victims with 56 incidents (41%), North America 49, (36%), Asia 21 (15%), Africa 4 (3%), South America 4(3%) and Oceania 1 (1%).

In May, we noted that the number of European attacks overtook North America, although this was only by a very minor difference. In June, whilst the difference again remains small, for the second month in a row Europe remains the most targeted region.

It remains to be seen whether this shift means threat actors are increasingly focused on European organisations, and if so, what this means for prevention.

Many reasons may explain this shift, for example, 35.71% of victims in Europe were targeted by LockBit2.0/3.0, as such, higher numbers may simply reflect threat actor preference. Likewise, greater opportunities for successful exploitation, vulnerabilities to target or number of active threat actors could be at play.

Many variables will influence the threat landscape as such it is important for organisations irrespective of their geographic location to consistently ensure strong cybersecurity.

We will need to observe a larger gap between North American and European targeting to decipher whether this is a clear shift.

Threat actor spotlight:

LockBit 3.0 aka LockBit Black

June 2022 saw another threat actor reincarnation, the retirement of LockBit 2.0 and subsequent birth of LockBit 3.0.

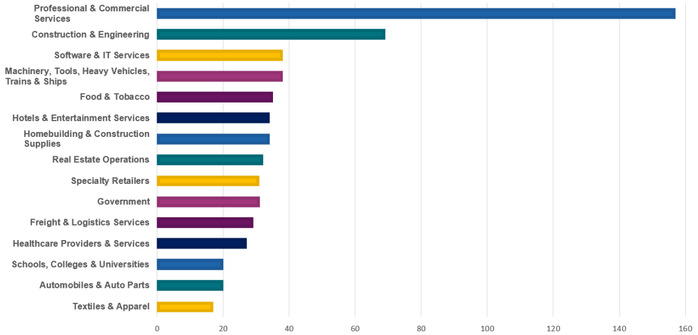
The group will be referred to generally as LockBit throughout this report.

NCC Group started tracking LockBit 2.0 in July 2021 and saw it quickly become an unstoppable ransomware force, stacking up tens of victim's month on month.

The reasoning behind the new strain is unclear, however, researchers have identified similarities with previous variants of the BlackMatter/DarkSide ransomware, possibly explaining the new naming convention by the group; LockBit Black.

Analysis has shown similarities to be so close that automated analysis platforms have been excused for mistaking the new LockBit Black strain for a BlackMatter variant.

In the 12 months leading up to the date of this report, NCC Group recorded 854 LockBit victims across 56 industry categories. With NCC's category of Professional & Commercial Services identified as the most targeted industry by the LockBit 2.0 strain (the top 15 industries can be seen within the below graph). Recent indications suggest that LockBit 3.0 is on a trajectory to - at the very least - meet these numbers, if not soar past them.



Top 15 most targeted industries for LockBit in the last 12 months

Expanding their reach

As well as the new strain of ransomware now in operation, and with a number of successful compromises already achieved since its launch, the gang have also offered a wide range of services and financial incentives for others to help them.

The first being a bug bounty program, offering remuneration of $1,000 to $1 million for bugs such as XSS vulnerabilities, MySQL injections, and weaknesses that can enable webshell deployment in websites, but ultimately, they request the details of any vulnerability that will assist them in their objectives.

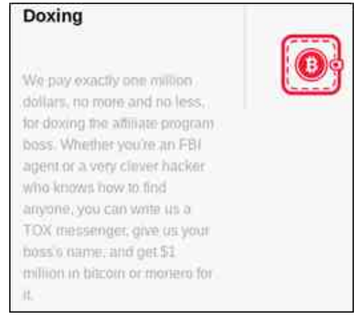
The group are also particularly interested in the assistance of researchers identifying vulnerabilities in their own tools, such as the encryption routine used in their locker which could be exploited to produce a decryption solution, and the TOX messaging platform used by group.

The group, however, did not stop there, with notorious 'LockBitSupp' member of the group declaring that $1M would be given to the individual who can expose their details.

This announcement was supported on the LockBit 3.0 website as detailed on their bug-bounty page.

Bug Bounty

LockBitSupp



Doxing

Percentage rate of affiliate program is 20% of the ransom, if you think that this is too much and because of this you are working with another affiliate program or using your personal software, then you should not deny yourself the pleasure of working with us, just increase the amount of ransom by 20% and be happy.
You receive payments from companies to your personal wallets in any convenient currency and only then transfer the share to our affiliate program.
However, for ransom amounts over $500 thousand, you give the attacked company 2 wallets for payment - one is yours, to which the company will transfer 80%, and the second is ours for 20%, thus we will be protected from scam on your part.

You personally communicate with the attacked companies and decide yourself how much money to take for your invaluable pentest work, which should surely be generously paid.

Return on Investment

Victims and Ransoms

Categories of targets to attack:
It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.
The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.
It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

LockBit Affiliate Rules

Ransomware as a Service (RaaS)

LockBit remains an affiliate driven organisation and actively recruits from its website, among other places. The group offer their affiliates in the region of 20% of the ransom paid, with recent victims facing ransoms from anywhere between $4000USD and $15M USD.

Initial research in relation to these victims indicates that company size and/or turnover are indeed decisive factors when the group determine the ransom amount.

The LockBit site also provides helpful information to would-be affiliates wishing to join their program. However, the group appears to be very aware of the resulting impact if their ransomware strain is used to target critical national infrastructure. Moreover, the group highlights that any post-Soviet countries are forbidden fruit.

Payment Coercion

Once the ransomware is triggered on the victim machine, one of the first things the user will notice is the modification of the ransomed files to that which shows the group's infamous logo. The desktop background is changed via the registry, and ransom note deployed.

Files Encrypted by LockBit Black

```
LockBit 3.0 the world's fastest and most stable ransomware from 2019

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites.
Keep in mind that once your data appears on our leak site, it could be bought by your
competitors at any second, so don't hesitate for a long time.
The sooner you pay the ransom, the sooner your company will be safe.
```

Purchased by Competitors

```
>>>>> What are the dangers of leaking your company's data.
First of all, you will receive fines from the government such as the GDRP and many others, you can be sued
by customers of your firm for leaking information that was confidential.
Your leaked data will be used by all the hackers on the planet for various unpleasant things.
For example, social engineering, your employees' personal data can be used to re-infiltrate your company.
Bank details and passports can be used to create bank accounts and online wallets through which criminal money will be laundered.
On another vacation trip, you will have to explain to the FBI where you got millions of dollars worth of stolen cryptocurrency transferred
through your accounts on cryptocurrency exchanges. Your personal information could be used to make loans or buy appliances.
You would later have to prove in court that it wasn't you who took out the loan and pay off someone else's loan.
Your competitors may use the stolen information to steal technology or to improve their processes, your working methods,
suppliers, investors, sponsors, employees, it will all be in the public domain.
You won't be happy if your competitors lure your employees to other firms offering better wages,
will you? Your competitors will use your information against you.
For example, look for tax violations in the financial documents or any other violations, so you have to close your firm.
According to statistics, two thirds of small and medium-sized companies close within half a year after a data breach.
You will have to find and fix the vulnerabilities in your network, work with the customers affected by data leaks.
All of these are very costly procedures that can exceed the cost of a ransomware buyout by a factor of hundreds.
It's much easier, cheaper and faster to pay us the ransom.
Well and most importantly, you will suffer a reputational loss, you have been building your company for many years,
and now your reputation will be destroyed.

Read more about the GDRP legislation::
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr.eu/what-is
```

Ransom Note GDPR

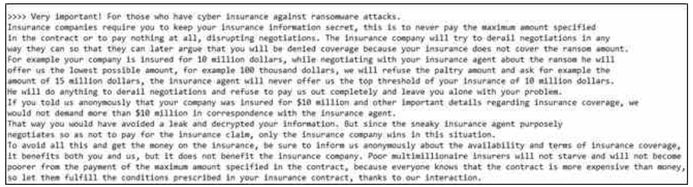
LockBit doesn't fail to fully exploit the first opportunity for payment coercion either; the ransom note. The group details a number of – arguably very strong - reasons as to why the victim should pay up without stalling.

As we can see from the following screenshots of the ransom note, that the first argument for quick payment is that competitors may attempt to buy their sensitive data.

The group describes how the stolen data will be abused by other hackers, and the impact on the victim's reputation. Additionally, the group use GDPR as a driver for quick payment.

Depending on the gravity of the GDPR failure, less severe infringements can result "in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher" as noted on the GDPR site.

Interestingly, the group provides guidance in relation to their cyber insurance. Encouraging victims to share information around the level of insurance coverage they hold, and ultimately not to feel sorry for 'multimillionaire insurers'.



```
>>>> Very important! For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret, this is to never pay the maximum amount specified
in the contract or to pay nothing at all, disrupting negotiations. The insurance company will try to derail negotiations in any
way they can so that they can later argue that you will be denied coverage because your insurance does not cover the ransom amount.
For example your company is insured for 10 million dollars, while negotiating with your insurance agent about the ransom he will
offer us the lowest possible amount, for example 100 thousand dollars, we will refuse the paltry amount and ask for example the
amount of 15 million dollars, the insurance agent will never offer us the top threshold of your insurance of 10 million dollars.
He will do anything to derail negotiations and refuse to pay us out completely and leave you alone with your problem.
If you told us anonymously that your company was insured for $10 million and other important details regarding insurance coverage, we
would not demand more than $10 million in correspondence with the insurance agent.
That way you would have avoided a leak and decrypted your information. But since the sneaky insurance agent purposely
negotiates so as not to pay for the insurance claim, only the insurance company wins in this situation.
To avoid all this and get the money on the insurance, be sure to inform us anonymously about the availability and terms of insurance coverage,
it benefits both you and us, but it does not benefit the insurance company. Poor multimillionaire insurers will not starve and will not become
poorer from the payment of the maximum amount specified in the contract, because everyone knows that the contract is more expensive than money,
so let them fulfill the conditions prescribed in your insurance contract, thanks to our interaction.
```

Cyber Insurance

Unaffiliated Affiliates

Research by Mandiant indicated that one of the affiliate groups seen to be utilising LockBit ransomware is Evil Corp, in an effort to evade sanctions imposed by the Office of Foreign Assets Control (OFAC) in the **US**.

OFAC also refer to Evil Corp as Dridex Gang linked to Moscow, Russia, and **Moldova**.

The adoption of a RaaS solution may offer a multitude of benefits to the group, not just the ability to evade sanctions by the US, but a better return on investment when considering how less time spent developing and maintaining tooling can be focused on reconnaissance and targeting.

Going Forward

LockBit have proven themselves to be a capable and effective adversary on the cyber security battleground. However, with increased exposure comes unwanted attention, and by welcoming BlackMatter and Evil Corp into the fold as well, this will inevitably have an impact on the group.

After BlackMater's Colonial Pipeline attack, the US government offered $10M for information leading to the identification or location of the BlackMatter **team**.

If we also take into consideration the sanctions imposed on Evil Corp and the financial reward declared for information leading to the conviction of the group's leader, the governmental interest in LockBit will increase.

State run and commercial cyber security agencies across continents will be developing and sharing intelligence in relation to these groups, waiting for the slightest slip-up in both cyber and real-world OpSec.

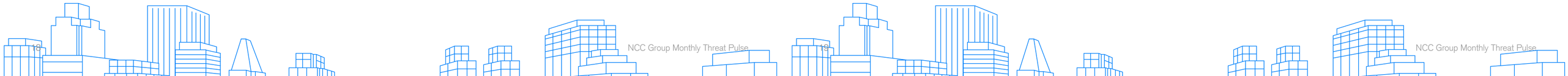
These groups are inevitably aware of their wanted status, although remaining in their silos and working in cooperation is going to be a difficult task to manage without making mistakes.

LockBit, the world is watching.

About the NCC Group Monthly Threat Pulse

NCC Group 's Strategic Threat Intelligence Practice gathers data on ransomware data leaks on the dark web in real time to get regular insights into who are the most recent ransomware victims.

By recording this data and classifying the victims by sector, the team is able to derive additional insights highlighting the sectors that have been targeted, and how current ransomware threats compare to previous months.



19 NCC Group Monthly Threat Pulse