

# DARK WEB PROFILES

THE MOST PROLIFIC RANSOMWARE  
GROUPS OF 2022





## SEARCHLIGHT. CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web threat intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

### METHODOLOGY

The threat intelligence in this report is derived from our Ransomware Search and Insights feature, which collates data from the dark web leak sites of ransomware groups. These groups are prolific and their dark web sites are constantly being updated, which means this data will change quickly. Groups also often choose not to publicize some of their attacks, either because the victim has paid the ransom or because they do not want to draw attention to certain activity. The purpose of this report is to demonstrate what insights can be derived from the dark web, but this data should always be used in correlation with other threat intelligence.

The data used in this report is reflective of the ransomware groups' dark web presence as of December 9th 2022.



## CONTENTS

<b>4</b>	<b>INTRODUCTION</b>
<b>5</b>	<b>ACTIONING DARK WEB INTELLIGENCE</b>
<b>8</b>	<b>DARK WEB PROFILES</b>
<b>8</b>	LOCKBIT
<b>10</b>	CONTI
<b>12</b>	BLACKCAT
<b>14</b>	<b>RANSOMWARE IN 2023</b>
<b>16</b>	<b>ABOUT RANSOMWARE SEARCH AND INSIGHTS</b>
<b>16</b>	<b>ABOUT CERBERUS</b>

## INTRODUCTION

WHAT CAN A NEW  
RANSOMWARE REPORT TELL  
YOU THAT YOU HAVEN'T  
HEARD BEFORE?

WOULD YOU LIKE TO SEE  
HOW RANSOMWARE  
GROUPS OPERATE ON  
THE DARK WEB?

Ransomware has been the “top trend” in cybersecurity for many years now and, while that might give the impression that the threat is static, it is actually continuously developing. Techniques and tactics change, monetization models develop, and groups appear, disband, and emerge again with new branding. Even looking back on the past 12 months, there are new factors that were not at play this time last year.

The most obvious is the impact of the war in Ukraine, which has crystalized the geo-politics of the ransomware world. Many groups that we have always known to be Russia-affiliated are now explicitly acting in the interest of the Russian state, and ransomware attacks are often being deployed with a dual purpose of undermining Ukrainian allies while also collecting ransom. Sometimes, there is no opportunity for the victim to pay the ransom at all, the attack is purely destructive not financial in motivation.

At the same time, the ransomware-as-a-service (RaaS) model has increased in prominence, further commoditizing the ransomware market, lowering the barrier of entry for new threat actors, and leading to more attacks than ever before.



It is noteworthy that this year's three most prolific ransomware gangs - profiled below - are all RaaS groups, so in fact the attacks are being undertaken by their affiliates rather than the threat actors themselves. They just get a cut of the spoils.

On a more positive note, we have also seen successful disruption of ransomware groups by law enforcement this year. Actors associated with the likes of REvil and LockBit have been arrested over the last 12 months, and Conti - which was at the time the most prolific ransomware group - was forced to disband after attracting too much attention to itself.

## DARK WEB INTELLIGENCE

Organizations have to keep track of these changes so they are protecting against current and emerging threats, rather than the attack techniques of the past. Gathering intelligence on groups in as real-time as possible gives them the best chance to effectively threat model for a ransomware attack, prepare their defenses, and mitigate their risk.

This is where the dark web - and this report - comes in. The dark web is the best source of intelligence on what ransomware groups are doing right now. There is no delay for the incident response report to come out, it is live information on their current actions. Whilst it doesn't cover the hands on keyboard side of activities, it can provide some light as to changes in targeting, potential vulnerabilities being exploited, how credentials are sourced etc.

In this report, we look at the three most prolific groups in 2022 to demonstrate just a fraction of what can be gleaned about ransomware operators from dark web intelligence, and how cybersecurity practitioners can practically action this data. This threat intelligence is derived from the [Ransomware Search and Insights module of our dark web investigation product, Cerberus](#). This feature automatically collates intelligence on ransomware groups from the dark web to help our customers get a more accurate picture of the ransomware landscape. It is our latest initiative to give law enforcement and enterprises the upper hand in combating dark web threats.

### DR. GARETH OWENSON

CTO and Co-Founder  
Searchlight Cyber

# ACTIONING DARK WEB INTELLIGENCE

The elemental purpose of intelligence is to ask - and get answers to - specific questions you have on a topic. When we talk about Cybercrime Intelligence and its loving parent Cyber Threat Intelligence, it's important to understand what questions can be asked.

This report is going to give some highlights of our ransomware data collection, some examples of the questions that we have asked of our data set, and different ways in which your organization could interrogate it too.

## THE FUNDAMENTALS OF THREAT MODELING

It is worth recapping some fundamentals before getting into specifics around this data. Firstly, and perhaps most straightforwardly, whether your organization should be worried about ransomware?

That's obviously a yes... isn't it? But to fully understand the specific threat of ransomware to your organization you should invest time into creating a threat model.

Threat modeling is an exercise that should be top of the pile in terms of your intelligence requirements. From a very high level a threat model gives you an idea of:

- Which groups/actors might be targeting you.
- Which groups/actors are opportunistic.
- What groups/actors might be trying to achieve.
- What methods they use throughout the attack.
- Event types that might trigger an attack.
- And more...

All of this data is useful in guiding priorities from a defensive and alerting perspective. One key aspect of threat modeling is learning from the past, and the dataset we are talking about in this report plays into understanding that historical view.

Threat modeling isn't a one and done exercise - attackers change what they are doing, new actors join the party, and some actors aren't ever seen again. For these reasons, it is an ongoing requirement.

How often it is done will be determined by each individual organization but at a minimum it should be conducted annually. Having a source of data that collates and breaks down knowledge of ransomware groups is a huge time saver, and live updates can alert you to a change in actor behavior, providing a timely update for your threat model.

## CAPABILITY, OPPORTUNITY, AND INTENT

So you've got your threat model done, it is being updated on the regular, and ransomware groups make up a portion of it. You have answered the "obvious" question, so now what? This is where things get fun (your definition of fun may vary wildly from mine). What actually constitutes a threat? This Venn diagram shows three abstract components that, combined, form a fully fledged threat.



### CAPABILITY

Ransomware operators' capabilities (the "how" they do it) are often well documented, which means you can take steps to thwart those actions if you have a good understanding of which group is likely to target you.

### HOSTILE INTENT

Their intent (or motive) is usually financial, but there are nuances within that. For example, Cuba ransomware is less prolific than some groups, choosing to focus on a small number of victims to garner larger payments. The STOP group is the opposite, operating at scale for smaller demands. Either way, perceived intent can be extrapolated from historical data on ransomware groups.

### OPPORTUNITY

Understanding ransomware group tactics also provides us with clues on what to look for online that would constitute an opportunity for them to execute their attack. For example, many gangs rely on phishing attacks or stolen credentials to get a foothold on the network. Marketplaces where these transactions take place typically give ambiguous details about

the credentials being sold, such as location, industry vertical, profit, and employee size. However, if your organization fits the description, you can identify that there may be a live opportunity for a ransomware group looking to attack you.

## THE VALUE OF DARK WEB INTELLIGENCE

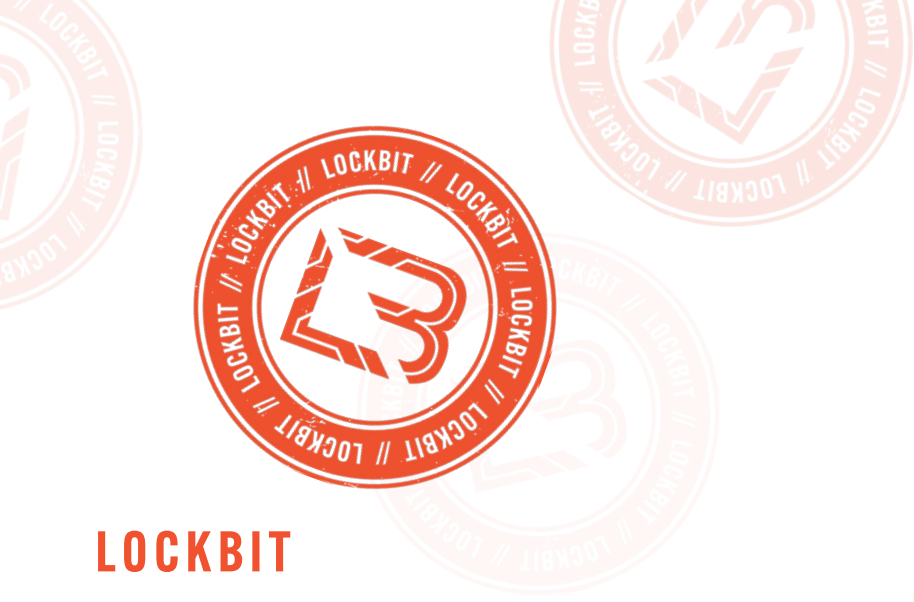
While insight into how ransomware groups operate on the dark web is illuminating, threat intelligence is only as valuable as the actions that you take on it.

Dark web intelligence is powerful because it gives you first mover advantage - early indicators about which group might be targeting your network and how they might be looking to gain initial access. Used properly, it can help you identify attacks earlier in the Cyber Kill Chain, giving you valuable time and knowledge to increase your chances of mitigating a ransomware attack.

### JIM SIMPSON

Director of Threat Intelligence  
Searchlight Cyber





# LOCKBIT

## OVERVIEW

LockBit is a RaaS operation that targets organizations across a broad range of industries and regions. Since the closure of Conti, it has become the most prolific RaaS operation, accounting for almost a third of all of the ransomware attacks that we track on our Cerberus platform.

Originally dubbed ABCD, LockBit has developed several improved versions of its malware, the most recent being LockBit 3.0. It is thought to be part of the LockerGoga and MegaCortex ransomware family due to its self-propagating and targeted attacks. In addition to targeting Windows machines, LockBit also has a Linux version.

LockBit uses double extortion tactics to incentivize its victims to pay the demanded ransom; as well as encrypting an organization's data, it also exfiltrates and threatens to release the data on its dark web leaks site after a specified "countdown" period (see Figure 2).

On its latest leak site, LockBit 3.0, there are options on some victims' listings to either extend the countdown timer by 24 hours, "destroy" the stolen data, or download the stolen data, for varying price points.

As demonstrated in the screenshots in Figure 3 and 4, LockBit actively engages with its affiliates over dark web forums, promoting its attacks, and investing effort into its branding.

Most notably, this year the group offered money in exchange for people tattooing themselves with the LockBit logo, which was taken up by some enthusiastic followers (Figure 5).

## FIRST ACTIVE

September 2019

## TOTAL LISTED VICTIMS

1248

## NOTABLE VICTIMS

Accenture  
Continental  
Advanced

## KNOWN FORUM PRESENCE

Xss forum  
Exploit forum  
Xss forum  
Exploit forum

## VICTIMOLOGY

LockBit targets industries indiscriminately, with victims in sectors from public sector, to energy, to tech.

Those in the capital goods, professional services, and consumer industries are most at risk - as these sectors count the highest number of LockBit's victims.

However, as LockBit is so prolific, no industry should consider itself "safe". Even industries that rank mid-table for LockBit (such as Transport, with 45 listed victims on its leak site) are more at risk from LockBit than any industry is from BlackCat (who have no more than 30 victims in any industry sector).

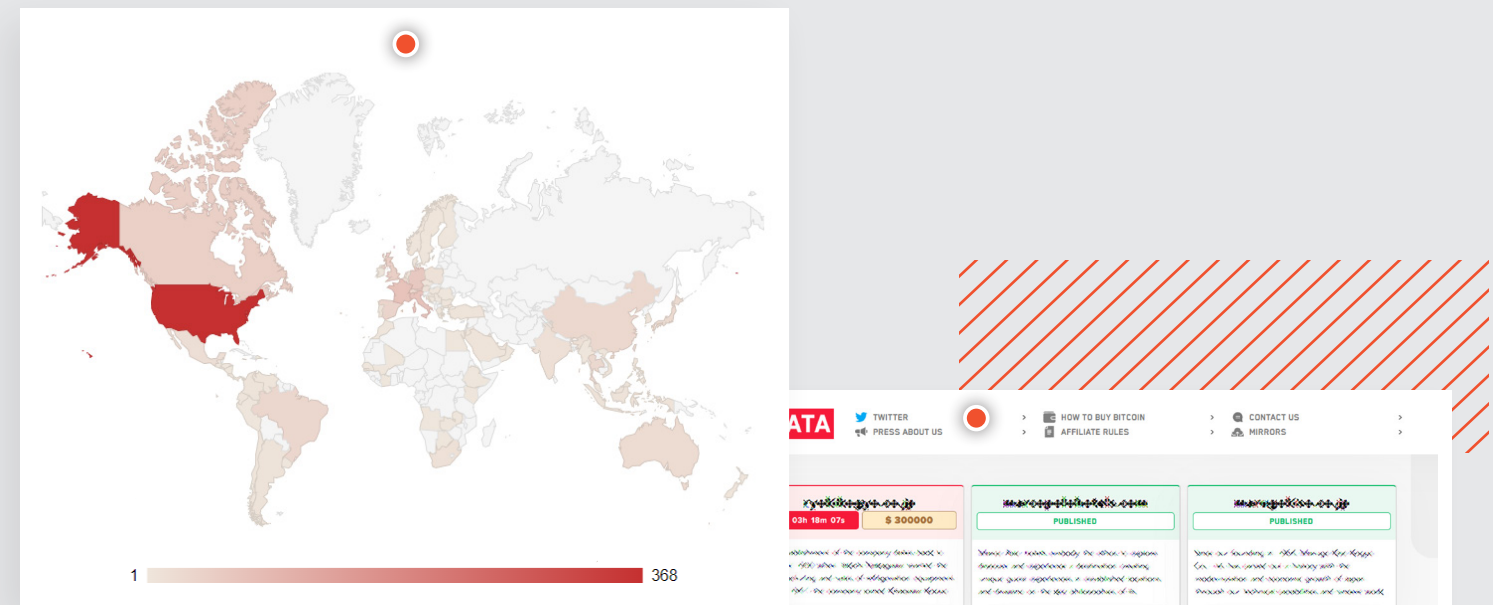


FIGURE 1: A HEAT MAP SHOWING THE DISTRIBUTION OF THE VICTIMS LISTED ON LOCKBIT'S LEAK SITE, BY GEOGRAPHY.

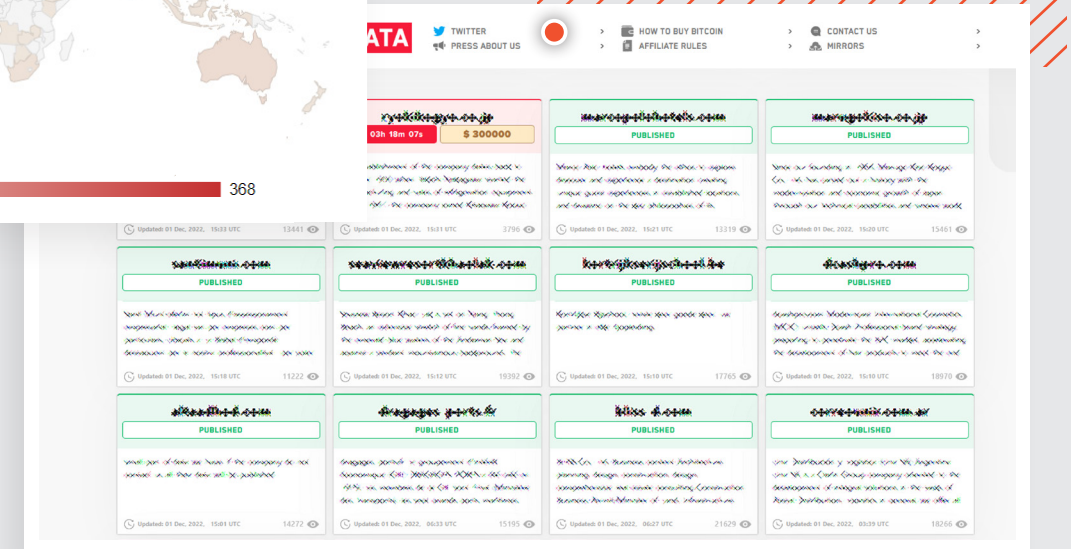


FIGURE 2: LOCKBIT'S DARK WEB LEAK SITE.

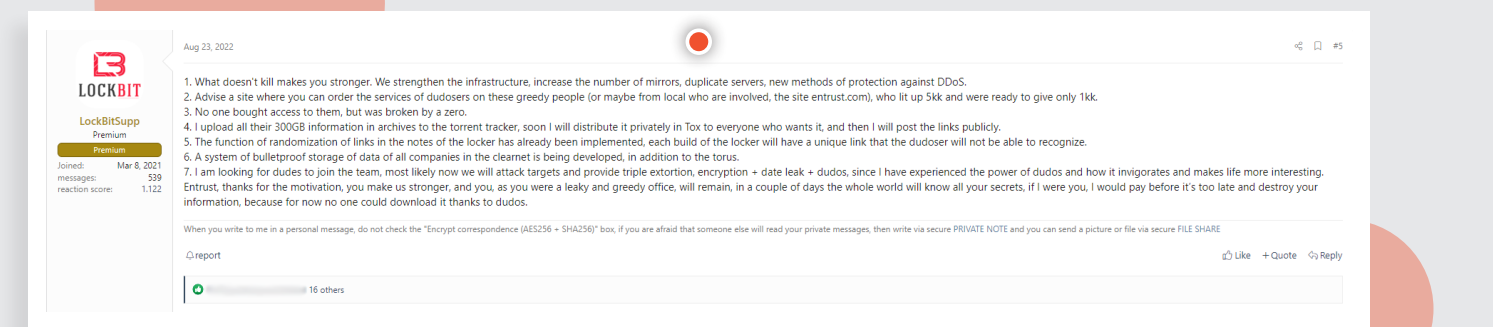


FIGURE 3: ASSOCIATED LOCKBIT ACCOUNT POSTS ON THE XSS DARK WEB FORUM ABOUT ITS ATTACK ON ENTRUST.

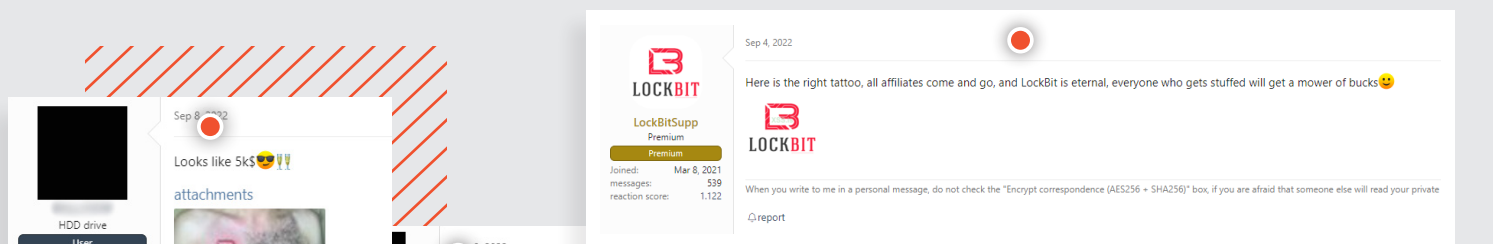


FIGURE 4: LOCKBIT OFFERS MONEY TO PEOPLE WHO TATTOO THEMSELVES WITH ITS LOGO.

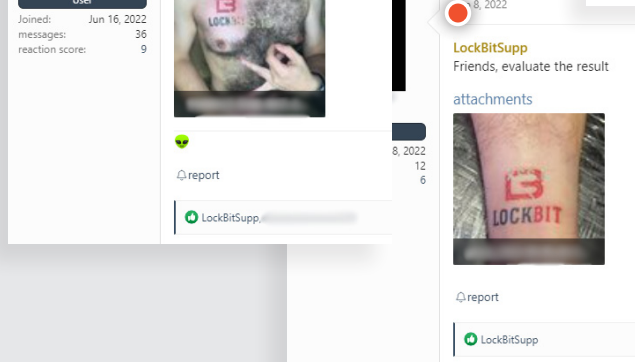


FIGURE 5: USERS POST PICTURES OF THEIR LOCKBIT TATTOOS ON A DARK WEB FORUM.

# CONTI



## OVERVIEW

Conti was, until its closure in June 2022, the most prolific RaaS group, thought to have compromised more than 1000 victims worldwide (although they listed just under 900 on their leaks site).

It is believed to have been managed by a group of Russian cybercriminals known as Wizard Spider, who also administered Ryuk ransomware.

Notable features of Conti ransomware and its operation include deletion of Volume Shadow copies of files, disabling security products that may identify it as ransomware, and its use of trojans TrickBot and BazarLoader to compromise networks with backdoor access, usually delivered via phishing emails. Like LockBit, Conti also used double extortion tactics, threatening to release victim data on its dark web leaks site (see Figure 7).

In early 2022, Conti's internal chats and ransomware source code were leaked by a Twitter user called ContiLeaks. The identity of the actor behind the leak is unclear, with some suspecting a disgruntled group member, while others blame a Ukrainian cybersecurity researcher retaliating against the group's public statement of support for Russia's invasion of Ukraine (see Figure 8).

Conti's dark web leaks site went offline in June 2022. It is strongly suspected that group members joined other RaaS operations such as BlackBasta and BlackByte, or refocused their efforts into groups thought to be subsidiaries of the primary Conti operation, such as Karakurt.

## FIRST ACTIVE

July 2020

## LAST ACTIVE

June 7, 2022

## TOTAL LISTED VICTIMS

877

## NOTABLE VICTIMS

The Costa Rican Government  
The Irish Health Service Executive  
JVCKenwood

## KNOWN FORUM PRESENCE

Exploit forum  
Rutor forum

## VICTIMOLOGY

Like LockBit, Conti attacked organizations across all industries. Also like LockBit, companies working in capital goods, professional services, or consumer products and services were most likely to be targeted. This trend across the two most prolific ransomware groups of all time speaks to the risk profile of these industries.

Conti was perhaps most famous for its attacks on government and critical national infrastructure organizations, with public sector institutions, healthcare, transport, and minerals making up a high proportion of the victims on its leak site.

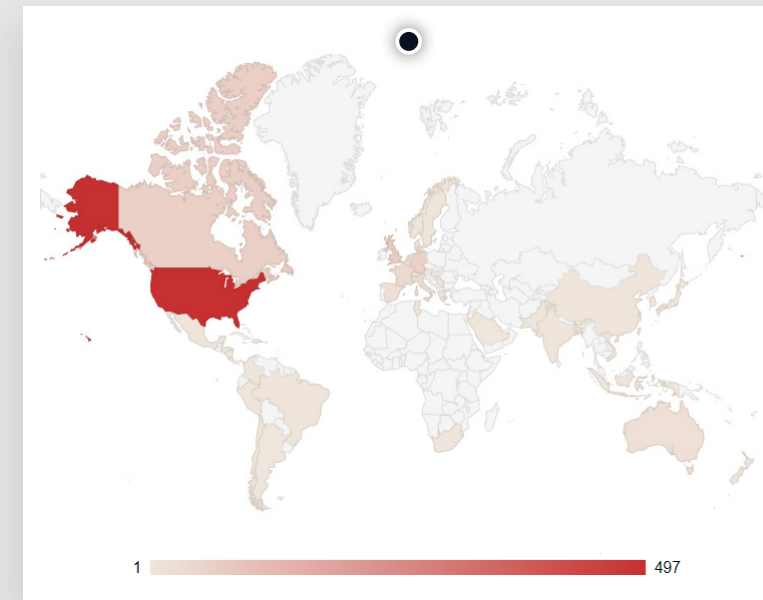


FIGURE 6: A HEATMAP SHOWING THE DISTRIBUTION OF THE VICTIMS LISTED ON CONTI'S LEAK SITE, BY GEOGRAPHY.

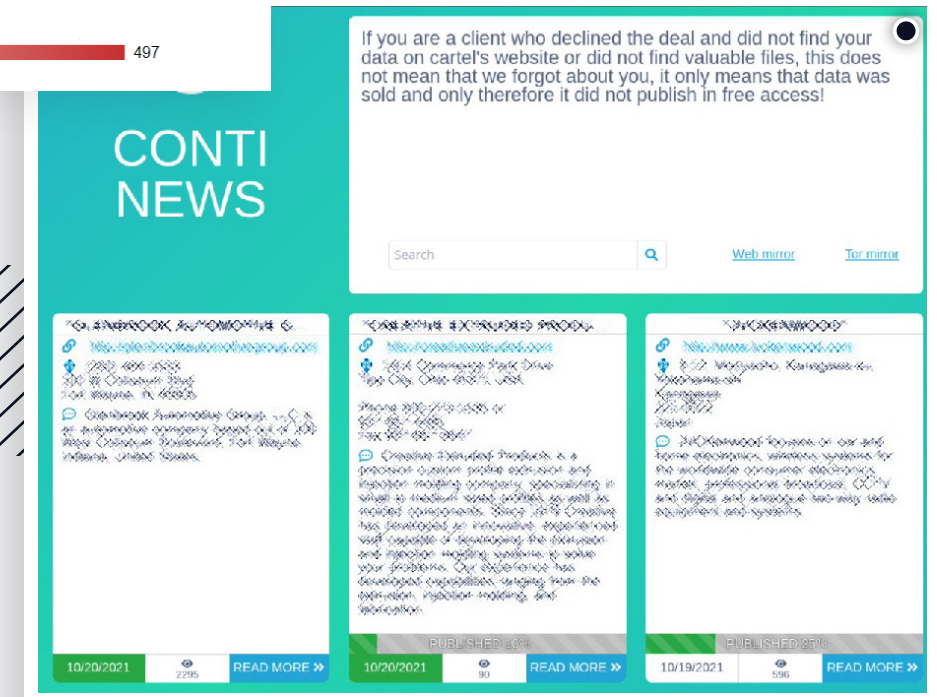


FIGURE 7: CONTI'S LEAK SITE, WHICH IS NO LONGER IN OPERATION.

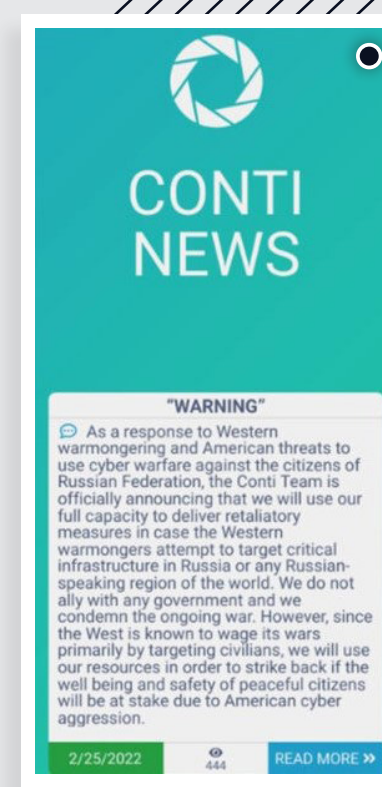


FIGURE 8: CONTI'S POST IN SUPPORT OF THE RUSSIAN GOVERNMENT, FOLLOWING THE DECLARATION OF WAR IN UKRAINE.

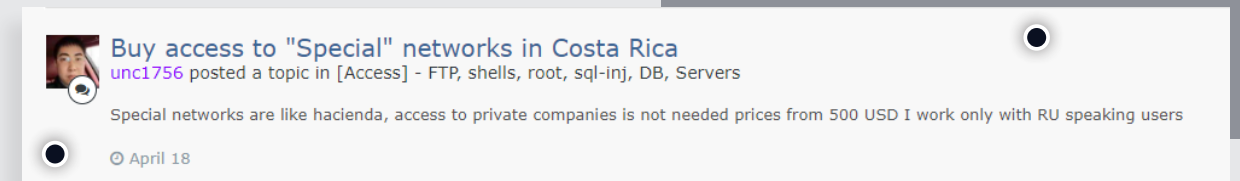


FIGURE 9: A USER AFFILIATED WITH CONTI OFFERS ACCESS TO COSTA RICA ON THE DARK WEB FORUM EXPLOIT.





# BLACKCAT

## OVERVIEW

BlackCat, also known as ALPHV or Noberus, is also a RaaS group. Its operators include developers and money launderers who originated from DarkSide, the ransomware group most infamous for the Colonial Pipeline attack, which disbanded in 2021.

BlackCat is noteworthy for being one of the first ransomware families to be written in Rust, a relatively modern programming language. This makes the malware harder to reverse engineer and defend against. Like LockBit, BlackCat has a Windows and Linux version.

It has also been reported that BlackCat lets its affiliates keep a larger share of the profits than other RaaS platforms, which may explain how the group has managed to make it into the top three most active groups in 2022.

Like LockBit and Conti, BlackCat also uses double extortion but, arguably, goes a step further than other groups in applying pressure on its victims through its “general collection” (Figure 12).

As explained by a BlackCat affiliate in Figure 13, the general collection is a searchable database of leaked data from victims who don’t pay their ransom, optimized to make it easier for cybercriminals to find a particular company’s stolen files. At one point, this collection was even available on the clear web, leaving BlackCat’s victims even more exposed.

## FIRST ACTIVE

November 2021

## TOTAL LISTED VICTIMS

215

## NOTABLE VICTIMS

Gestore dei Servizi Energetici SpA (GSE)

Creos Luxembourg S.A

NJVC

## KNOWN FORUM PRESENCE

Exploit forum

Xss forum

## VICTIMOLOGY

BlackCat also has a broad spread of victims across industries but we can identify trends.

Companies that specialize in consumer products, services, and retail are the most targeted, followed by professional services, software and services, and - once again - capital goods.

Health and public sector organizations also make up a large proportion of its victims.

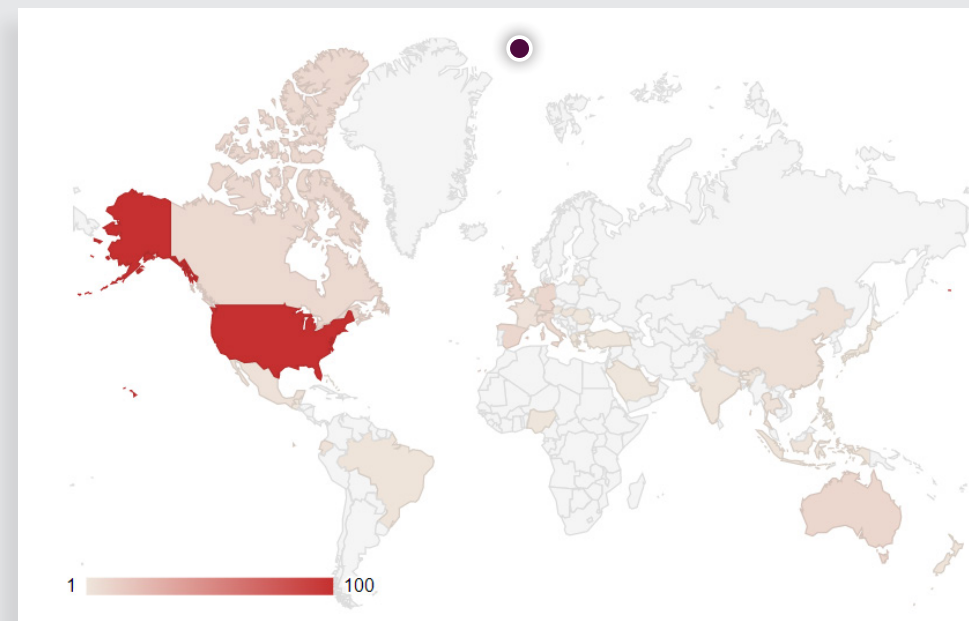


FIGURE 10: A HEATMAP SHOWING THE DISTRIBUTION OF THE VICTIMS LISTED ON BLACKCAT'S DARK WEB LEAK SITE BY GEOGRAPHY.

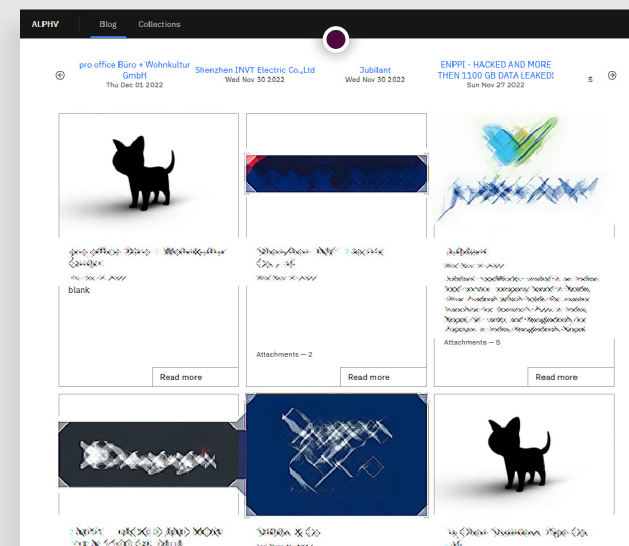


FIGURE 11: BLACKCAT'S DARK WEB LEAK SITE.

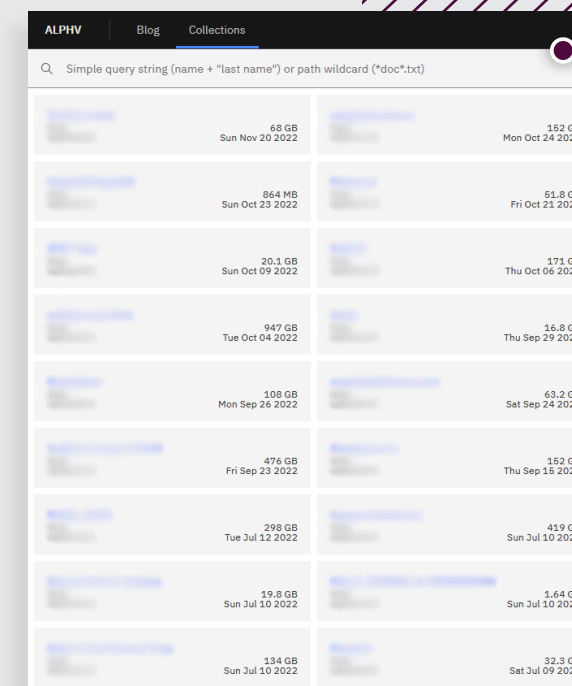


FIGURE 13: BLACKCAT'S "GENERAL COLLECTION" OF LEAKED DATA, AVAILABLE ON ITS UNION SITE FOR USERS TO SEARCH.

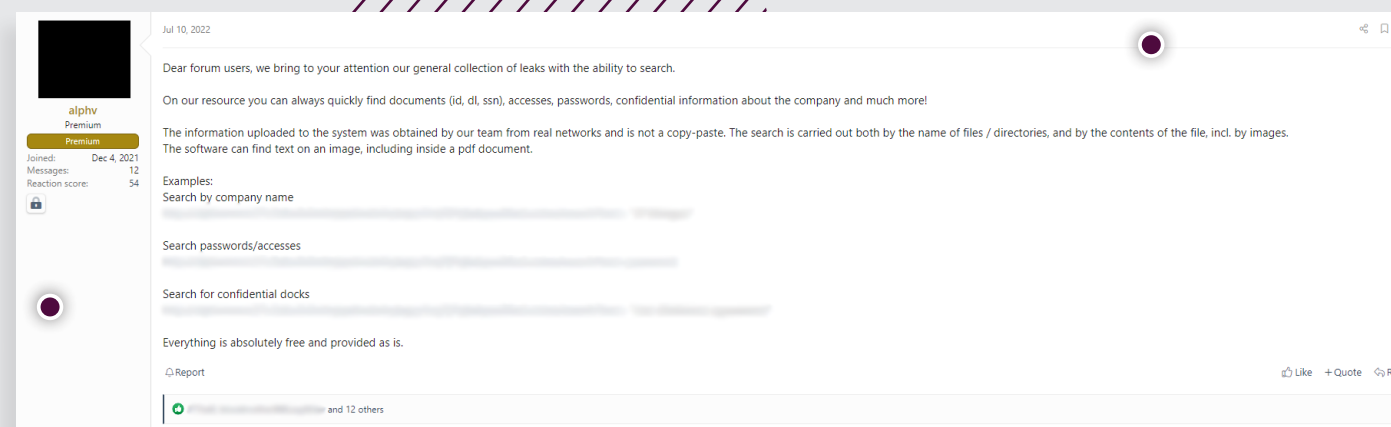


FIGURE 12: A BLACKCAT AFFILIATE PROMOTES THE "GENERAL COLLECTION" ON THE DARK WEB FORUM XSS.



## RANSOMWARE IN 2023

For years, security professionals have made the prediction that ransomware will continue to be one of the greatest challenges facing organizations. Dark web intelligence allows us to dig deeper into trends that inform our defenses for the year ahead. In 2023 we can expect:

### CONTINUED DOMINATION OF RAAS

It is no surprise that the three most prolific groups of 2022 are RaaS operators, or that they all conduct double extortion attacks. These commercial models have been proven to work for ransomware actors, and until that stops being the case (or something even more effective comes along) this trend will continue. RaaS operations will likely become even more sophisticated, as groups continue to “professionalize” and develop new ransomware kits in competition with each other to attract affiliates. This will continue to lower the bar of entry for new actors, as RaaS becomes easier to use and deploy, which will only be counterbalanced by the increased risk of being caught by law enforcement (see point three below).

### INCREASED GLOBAL POLARIZATION

We also can't be shocked by the presence of Russian-speaking threat actors in the three most prolific groups of this year. As we discussed in the introduction, the war in Ukraine has hardened the digital frontier between the west and Russia, with many ransomware operators - if not explicitly acting as part of the effort - at least taking advantage of the Russian state's leniency on groups targeting organizations in the territories of Ukraine's allies.

We have even seen signs of threat actors outside of Russia migrating their infrastructure to the region, to take advantage of the perceived protection of the state. This also influences groups' tactics, with some groups breaking with wider ransomware trends by focusing on destruction over extortion, giving organizations even less time and opportunity to salvage their data.



### INTERNATIONAL COLLABORATION AGAINST RANSOMWARE

In turn, we can expect to see a harder response from nations against ransomware groups. It is likely that in the next year we will see the beginnings of tougher legislation to force organizations to better prepare for ransomware threats. We will also see law enforcement agencies clamp down on ransomware operators and infrastructure that falls within their jurisdictions. The key element to both of these strategies is international collaboration. One government's legislation or unilateral law enforcement efforts aren't going to be enough to stop ransomware groups. Ransomware is a global problem, so it needs a globally coordinated solution. The problem here is that rogue states like Russia, for example, let groups act with impunity as long as they don't cross certain lines. As long as this continues, RaaS operators will have a safe haven. The West may try to use diplomatic means to encourage rogue states to fall in line but, equally, ransomware is a way for certain governments to get funding that offsets the negative impact of sanctions, which creates an incentive for them not to cooperate.

## EVOLUTION OF GROUPS

The rise and fall of Conti is just one demonstration of the capricious nature of the ransomware landscape. Groups are ephemeral and, often, interconnected. While it hasn't been the focus of this report, you may have noticed the crossover of threat actors between existing and historic groups. Other researchers have demonstrated that Conti actors have gone on to join other groups, including BlackBasta and BlackByte. While it is impossible to predict which group will rank as the most prolific this time next year, we can highlight three groups that will undoubtedly be prominent as we go into the year ahead:

## GROUPS TO WATCH

VICESOCIETY	AVOSLOCKER	HIVE
 <p>ViceSociety is a ransomware/data extortion operation that targets organizations primarily in the education sector.</p> <p>While files encrypted by the group sometimes bear a .v-s0ciety or .v-society extension, Vice Society is not believed to deploy any proprietary ransomware of its own. Instead, it has been observed using variants of ransomware payloads such as HelloKitty, FiveHands, Zepellin, MountLocker, and BlackCat.</p> <p>Vice Society threatens double extortion via its leak site but, in some cases, doesn't deploy any ransomware onto a victim's systems, opting instead for a pure exfiltrate-and-extort operation.</p>	 <p>AvosLocker is another RaaS operation that is particularly active against organizations in North America.</p> <p>It threatens double extortion via its leak site but tends to go for smaller targets than the likes of LockBit and BlackCat.</p> <p>A representative of AvosLocker is regularly observed bidding in auctions for initial access to compromised corporate networks on a popular Russian cybercrime forum.</p> <p>In addition to targeting Windows machines, AvosLocker also has a Linux version.</p>	 <p>Hive is a RaaS operation that particularly focuses on the energy and healthcare sectors.</p> <p>Its ransomware is designed to be used by novice RaaS affiliates and has gone through several evolutions.</p> <p>Around the time a researcher created a free decryptor for one version of the Hive payload, a new iteration was released revealing a switch from GoLang programming language to the relatively faster and harder-to-analyze Rust, as well as a more evasive encryption method.</p> <p>Hive targets Linux as well as Windows machines.</p>

# ABOUT RANSOMWARE SEARCH AND INSIGHTS

[Ransomware Search and Insights](#) is a new strategic enhancement to our dark web investigation platform, Cerberus. It automatically collates data from known ransomware groups to help organizations and law enforcement agencies to investigate, track, and gather intelligence on live ransomware activity. This means that patterns in ransomware group tactics, incidents, and victimology can be observed in real-time, helping analysts to bolster their threat intelligence, and gain the upper hand on ransomware groups.

## RANSOMWARE SEARCH AND INSIGHTS ALLOWS YOU TO:



Better understand a ransomware group's tactics, victimology, and leak activity.



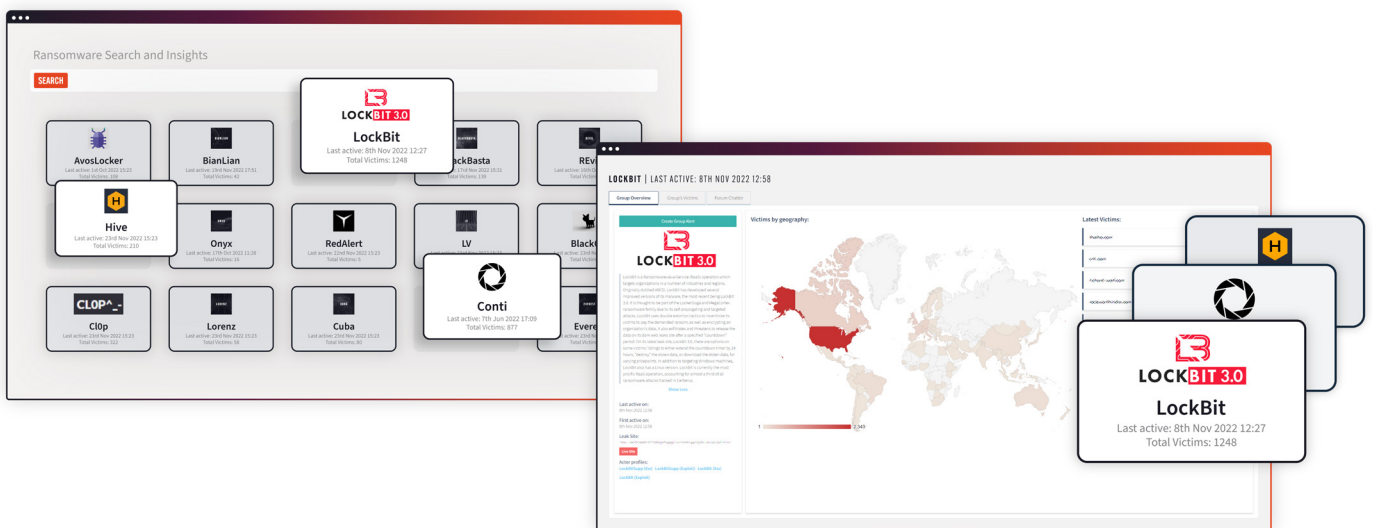
Track known group members on the dark web.



Reduce time spent manually researching each threat group.



Identify the groups that are most relevant to you, based on their victim profiles.



# ABOUT CERBERUS

Cerberus uses proprietary techniques developed by world-leading researchers to deliver the most comprehensive dark web dataset on the market, providing access to intelligence that was previously unobtainable. Interrogate more than 15 years of data from marketplaces, forums, and leak sites with new deep and dark web activity updated live. [Ransomware Search and Insights](#) is available as a feature of Cerberus.



VISIT [WWW.SLCYBER.IO](http://WWW.SLCYBER.IO) TO FIND  
OUT MORE OR BOOK A DEMO NOW.

**SEARCHLIGHT.  
CYBER** 

VISIT [WWW.SLCYBER.IO](http://WWW.SLCYBER.IO) TO FIND  
OUT MORE OR BOOK A DEMO NOW.

**UK HEADQUARTERS**

Suite 63, Pure Offices,  
1 Port Way, Port Solent,  
Portsmouth PO6 4TY  
United Kingdom

**US HEADQUARTERS**

900 16th Street NW,  
Suite 450, Washington,  
DC 20006  
United States