



LOOKINGGLASS

WHITE PAPER

THE PROFESSIONALIZATION OF RANSOMWARE

HOW RANSOMWARE GROUPS ARE ADOPTING BUSINESS



TABLE OF CONTENTS

Executive Summary	3
Introduction	4
The Most Active Ransomware Groups	5
Ransomware’s Most Targeted Countries	8
Top Industry Sectors Facing Ransomware Attacks	10
Major Ransomware Threat Groups	12
Ransomware-as-a-Service (RaaS)	17
A Possible Ransomware Future	17



EXECUTIVE SUMMARY

Organized crime groups have developed new ways of monetizing ransomware beyond encryption, including double and triple extortion. More than that, however, is that ransomware groups have grown in sophistication and business acumen. The rise in attacks has also been accompanied by an increasingly professional threat actor community – largely replacing the loosely affiliated groups of the past. Many of these malicious actors operate almost exactly like legitimate corporations with a full financial motivation for their activities.

The most active ransomware groups in the first half of 2022 have been LockBit, Conti, Alphv, Black Basta, and Vice Society. Most of the targets for these ransomware organizations were predominantly located in the United States. LookingGlass data shows that US enterprises and people continue to be a frequent high target for many of these ransomware groups.

Data also suggests that current global social, political, and economic events have significantly impacted ransomware operations in 2022. Notably, the arrests of LAPSUS\$ and REvil members and the war in Ukraine have shifted the threat actor landscape. In Q2 2022, dormant REvil servers came back online despite arrests and redirected visitors to a new data leak site. This suggests that members of the group who escaped apprehension are still carrying out ransomware activities.

Ransomware-as-a-service has been a growing issue for many businesses and nation-states as these gangs sell their software or victim information on the dark web. The Conti Leaks is perhaps the most notable event of the first quarter of 2022 that highlights how large ransomware groups are organized and how they operate. This leak led to Conti shutting down and likely rebranding into the now active Black Basta, which was one of the more prominent groups in Q2 2022.

This report explores how the professionalization of ransomware has evolved in the first half of 2022. It also examines:

- the primary threat actors involved,
- the shifts made from the capture of some members of these gangs,
- the growing issue with RaaS, and
- the possible future of ransomware operations.



INTRODUCTION

Ransomware is one of the more persistent issues in cybersecurity. Tracing its origins back to 1989 and the AIDS Trojan distributed on floppy disks, ransomware as a class of attack did not fully take off until the advent of cryptocurrency enabled anonymous and hard-to-trace transactions. CryptoLocker in 2013 marked the latest age of ransomware, enabling loosely affiliated groups or lone wolf ransomware writers to collect their ransoms more readily.

These initial ransomware gangs were at best focused on spray-and-pray tactics that emphasized trying to encrypt as many targets as possible. The barriers to entry were high as well, given that composing effective ransomware code still required extensive skill.



IN THE FIRST HALF OF 2022, LOOKINGGLASS TRACKED MORE THAN 1,100 RANSOMWARE INCIDENTS TARGETING COMPANIES WORLDWIDE

These are 1,100+ incidents that were confirmed and attributed to a known threat actor group, not necessarily all the ransomware incidents that occurred in the first six months of the year. We anticipate that number will continue to climb through the remainder of 2022. This rapidly growing trend raises many questions about what can be done to stop this new generation of cybercriminals.

What is more interesting, however, is that ransomware gangs are increasingly professionalized. Groups have started to incorporate business practices such as finance departments, human resources, and even naming employees of the month. These are not the loosely affiliated groups of the past; rather, they are highly professionalized organizations with quarterly revenue targets and even customer service teams. Since the average ransomware payment is now at [\\$812,360, according to Sophos](#), it should come as no surprise that these groups are looking to evolve and benefit from it.

In addition to serving their customers, ransomware organizations want to make profit, just like any other business. Ransomware enterprises have been known to set up payment plans and other arrangements to ensure the ransom is paid. They also want to convince victims that paying up is their best option in the first place. They even have bug bounty programs to point out errors in their code; LockBit launched the first one in June 2022 and paid out a bounty of \$50,000 to a researcher in September.

According to the [Verizon DBIR released for 2022](#), there was a 13% year-over-year increase in ransomware breaches globally last year. Outside of a few nation-state sponsored groups focused on cyberespionage, most ransomware is commonly only used to earn money for the financially motivated cybercriminals who deploy them.

The professionalization of ransomware has been fueled by sophisticated software and networks, which has made it a serious problem that threatens businesses and consumers alike. This report will examine the increasing professionalization of ransomware groups over the course of the first six months of 2022. From ransomware-as-a-service (RaaS) to bug bounties alongside sales teams and live chat, ransomware groups are emulating the organizational structure of legitimate businesses to professionalize their operations.





THE MOST ACTIVE RANSOMWARE GROUPS

Today’s ransomware involves more sophisticated tactics and measures than ever before. Ransomware actors rely on strategies such as encryption algorithms that make it nearly impossible for even law enforcement agencies to regain access to encrypted files. The skill on display in terms of ransomware development, including encryption methodologies and their ability to leverage initial access brokers, points toward signs that ransomware gangs are reaching a new level of professional acumen.

Further, “Ransomware as a Service” (RaaS) has allowed ransomware gangs to expand the ways they monetize their attacks. Rather than spend time targeting companies themselves, the creators of ransomware can offer their attacks for sale on the dark web and receive a percentage of the ransom from people who use their code. This lowers the barrier to entry for ransomware usage to those with malicious intent and minimal skill and allows ransomware gangs to make more money.



1,133 CONFIRMED AND ATTRIBUTED RANSOMWARE
ATTACKS OCCURRED IN THE FIRST SIX MONTHS OF 2022

LookingGlass analysts confirmed and attributed 1,133 ransomware attacks in the first six months of 2022. They also confirmed and attributed 207 data leaks across all active threat actor groups throughout the first six months of the year. Of the more than 1,300 incidents, the bulk came from the top 15 most active ransomware groups.

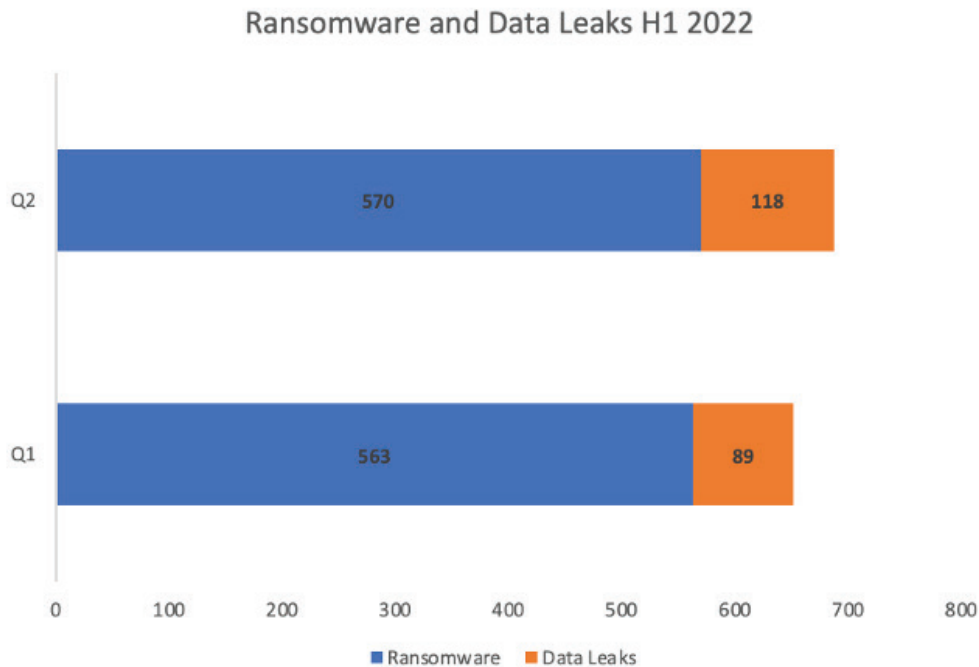


Figure 1. Ransomware and Data Leaks H1 2022





THE MOST ACTIVE RANSOMWARE GROUPS (CONTINUED)

The total number of ransomware attacks that LookingGlass analysts confirmed spanned 26 ransomware groups, with some shift in the number of groups active throughout the first six months of the year. The biggest change in group activity was with Conti in the second quarter, who disbanded operations. REvil Reborn also appeared as a new group in the second quarter, taking up the mantle of REvil and redirecting to a new data leak site. LookingGlass analysts identified these active groups based on detailed research on several data leak sites, confirming the details of the more than 1,100 ransomware attacks throughout the first six months of the year. The below chart shows the top 15 most active groups throughout the period of January to June 2022.

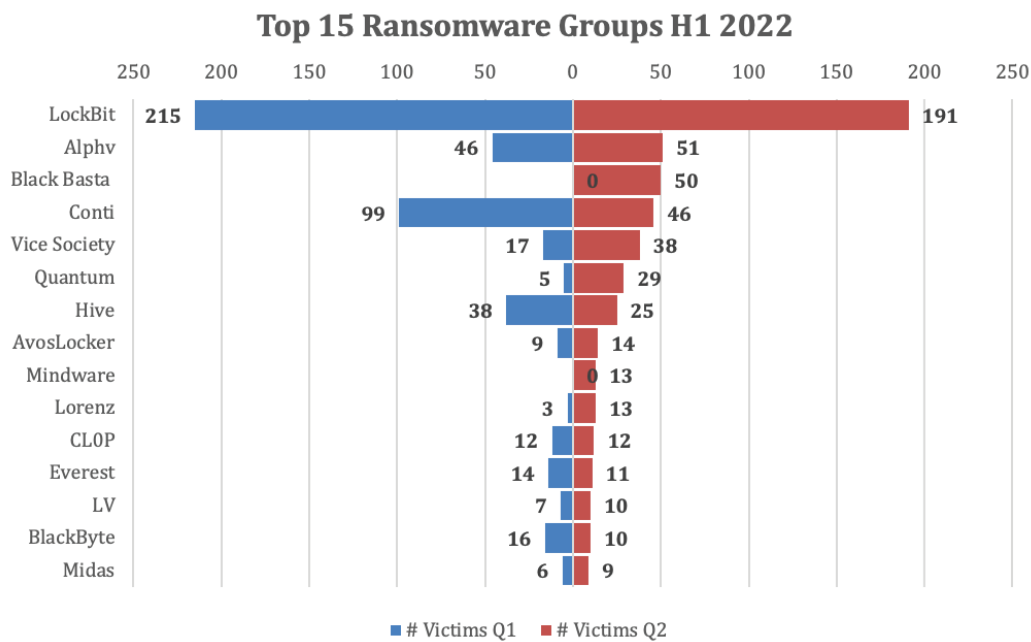


Figure 2. Most Active Ransomware Groups H1 2022a

LockBit was by far the most active ransomware group in the first half of the year. The group targeted 215 victims in Q1 2022 and 191 victims in Q2 2022 across all industries and geographies. Conti took second place in Q1 with 99 victims; they dropped to fourth place in Q2 when they disbanded following Conti Leaks. Alphv took third place in Q1 with 46 victims and took second place in Q2 with an 11% increase to 51 victims. Hive (38 victims) and Vice Society (17 victims) rounded out the top five most active groups in Q1. The chart below details the most active groups throughout the first six months of the year.



THE MOST ACTIVE RANSOMWARE GROUPS (CONTINUED)

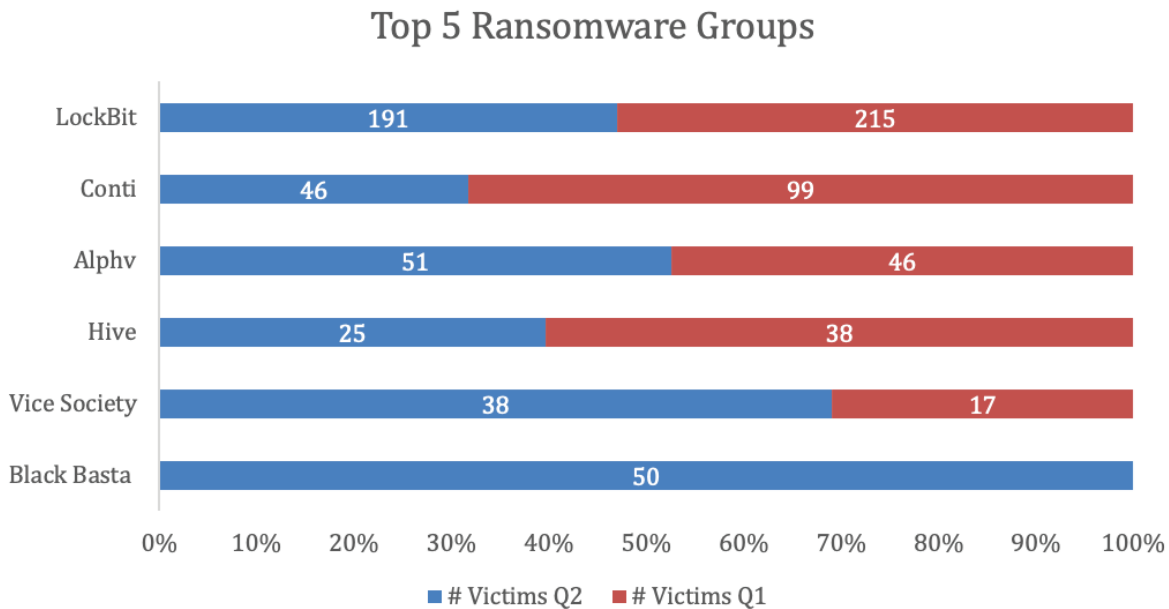


Figure 3. Top 5 Most Active Ransomware Groups

Roughly the same groups were active in the same volume throughout the first six months of the year. The primary change was the emergence of Black Basta in the second quarter. This group quickly became one of the most active throughout the period from April to June. Black Basta is said to be composed of former Conti and REvil members, which is indicative of the reality that shutting down or disbanding specific gangs does little to quash the volume of ransomware attacks. Vice Society rounded out the top five active groups of Q2; they more than doubled their victims from the first quarter targeting 38 victims in their efforts.

LockBit likely retained their title as the most active in part due to their neutrality in the conflict between Russia and Ukraine. Conti's stated allegiance to the Russian government, and the resulting leak of their chat logs in Q1, probably played a role in their decision to wind down operations. Despite this, they remained active throughout the first six months of the year.



MORE THAN A THIRD OF ALL RANSOMWARE ATTACKS IN H1 WERE ATTRIBUTED TO LOCKBIT

LookingGlass also tracked several prominent data leak sites throughout the first half of the year. These data leak sites often publicize their victims as well as the type of data they possess, making it valuable for organizations to monitor these sites as well as the activity of ransomware gangs. By either self-monitoring these leak sites, or partnering with organizations who already do, enterprises can gain a window into what type of data has been truly exfiltrated from their systems. The chart below shows the most active data leak sites in the first six months of the year.





THE MOST ACTIVE RANSOMWARE GROUPS (CONTINUED)

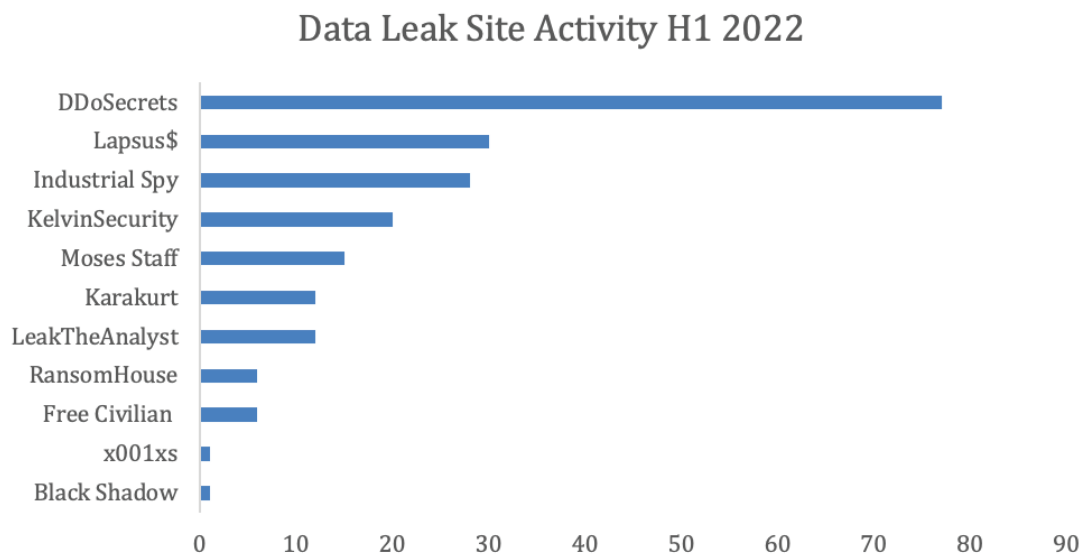


Figure 4. The most active data leak sites in H1 2022

Karakurt, which is believed to be a data extortion arm of Conti, listed 30 victims on their site in Q1 2022. DDoSecrets, billed as a nonprofit collective, was the most active throughout the first six months of the year. The bulk of DDoSecrets targets were in Russia, and their activity picked up in terms of data leaks following the Russian invasion of Ukraine in February. Many of the leaks came in partnership with the Anonymous hacking group, who very publicly declared their opposition to Russia following the invasion. The LAPSUS\$ hacking group was the second most active data leak operation in the first half of 2022. They posted some high-profile victims before several of its members were arrested for their activities.

Despite these shifts in the landscape, these leak sites are nevertheless important components to the ransomware ecosystem. Each leak site is typically partnered with a specific operation and monitoring them may provide insight into who the ransomware group has targeted and what data they exfiltrate.

RANSOMWARE'S MOST TARGETED COUNTRIES

Ransomware gangs have historically focused their efforts on certain geographies. In the case of some nation-state sponsored groups, that targeting is informed by what the government of their home country views as their threats. This can often include attacks on critical infrastructure, such as the [Colonial Pipeline ransomware attack](#) in May 2021.

Of the 1,133 ransomware attacks that LookingGlass analysts confirmed in the first half of 2022, more than half (52%) were against targets in the United States. This is a total of 433 confirmed attacks attributed to specific threat actor groups. The number of attacks against targets in the United States is more than 4x higher than the United Kingdom, which was the second most-targeted country at 73 attacks. The United States by far received most of the attention from ransomware groups that we tracked.





RANSOMWARE'S MOST TARGETED COUNTRIES (CONTINUED)

The United States being the primary target of ransomware groups makes some sense for financially motivated gangs. The United States has the world’s largest GDP at \$24 trillion, and as such is a more financially rich target. In fact, six of the top 10 countries that experienced ransomware attacks in our dataset are within the top 10 countries in terms of GDP amounts. These include the United Kingdom, Germany, Italy, France, and Canada in addition to the United States.

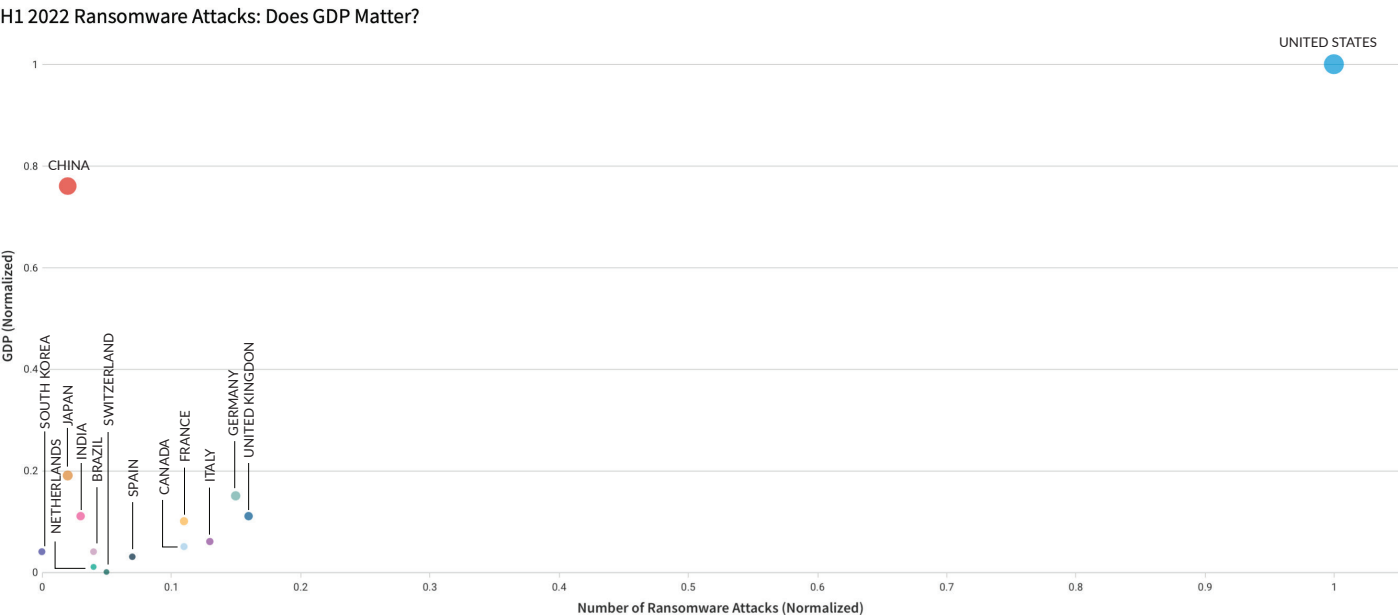


Figure 5. Ransomware Attacks vs. Global

In this comparative, you will notice that China, Japan, and India did not make the top 10 in terms of the confirmed and attributed ransomware attacks that LookingGlass analysts found. This does not mean that Chinese organizations did not experience ransomware in the first half of 2022; only that they were not the primary targets within our dataset. China and Japan both experienced 12 of the confirmed and attributed ransomware attacks in the first six months of the year, as shown in the table of the top 20 targeted nations globally.





RANSOMWARE'S MOST TARGETED COUNTRIES (CONTINUED)

Country	Q2	Q1	Ransomware Attacks H1
United States	215	218	433
United Kingdom	32	41	73
Germany	39	28	67
Italy	25	33	58
Canada	28	22	50
France	23	27	50
Spain	14	18	32
Switzerland	10	13	23
Brazil	10	11	21
Netherlands	9	10	19
Mexico	10	6	16
Austria	7	7	14
India	6	8	14
Argentina	5	8	13
Australia	13	0	13
Thailand	11	2	13
China	8	4	12
Japan	8	4	12
Belgium	8	3	11
Hong Kong	3	7	10

India, the third most populous nation worldwide and the sixth largest economy, similarly had fewer than 15 confirmed ransomware attacks based on our research. We've also broken out Hong Kong from China because of its special political status. You'll note that the bulk of the top 20 nations are in Europe or the Americas, with only a few entrants in the Asia Pacific region. Ultimately, the key point to understand is that countries with stronger economies tend to be – but are not necessarily – more highly targeted by ransomware gangs.

Table 1. Top 20 Countries Targeted by Ransomware

TOP INDUSTRY SECTORS FACING RANSOMWARE ATTACKS

Ransomware groups have historically tended to attack financial services organizations out of the correctly held belief that you'd typically want to attack where the money is. They have also often attacked organizations that have a low tolerance for downtime, as those organizations tend to be more likely to pay ransoms to restore their access. If ransomware groups can infringe on the confidentiality, system integrity, and availability of targeted systems, they will likely succeed at their goals.



ATTACKS AGAINST GOVERNMENT AND PUBLIC SECTOR ORGS ROSE 60% BETWEEN Q1 AND Q2

So far in 2022, ransomware gangs primarily targeted two sectors: manufacturing and industrial products (103 victims in Q1; 86 in Q2) and professional services (91 in Q1; 93 in Q2). In Q1, the next four sectors targeted by ransomware groups were financial services, technology, engineering and construction, and healthcare and life sciences. In Q2, engineering and construction became the third most targeted sector, along with healthcare and life sciences. The consumer and retail industry moved into the top 5 targeted sectors in Q2, replacing financial services and technology. Notably, there was also a 60% increase in government and public sector organizations, with targets between Q1 and Q2 growing from 25 to 40 victims.





TOP INDUSTRY SECTORS FACING RANSOMWARE ATTACKS (CONTINUED)

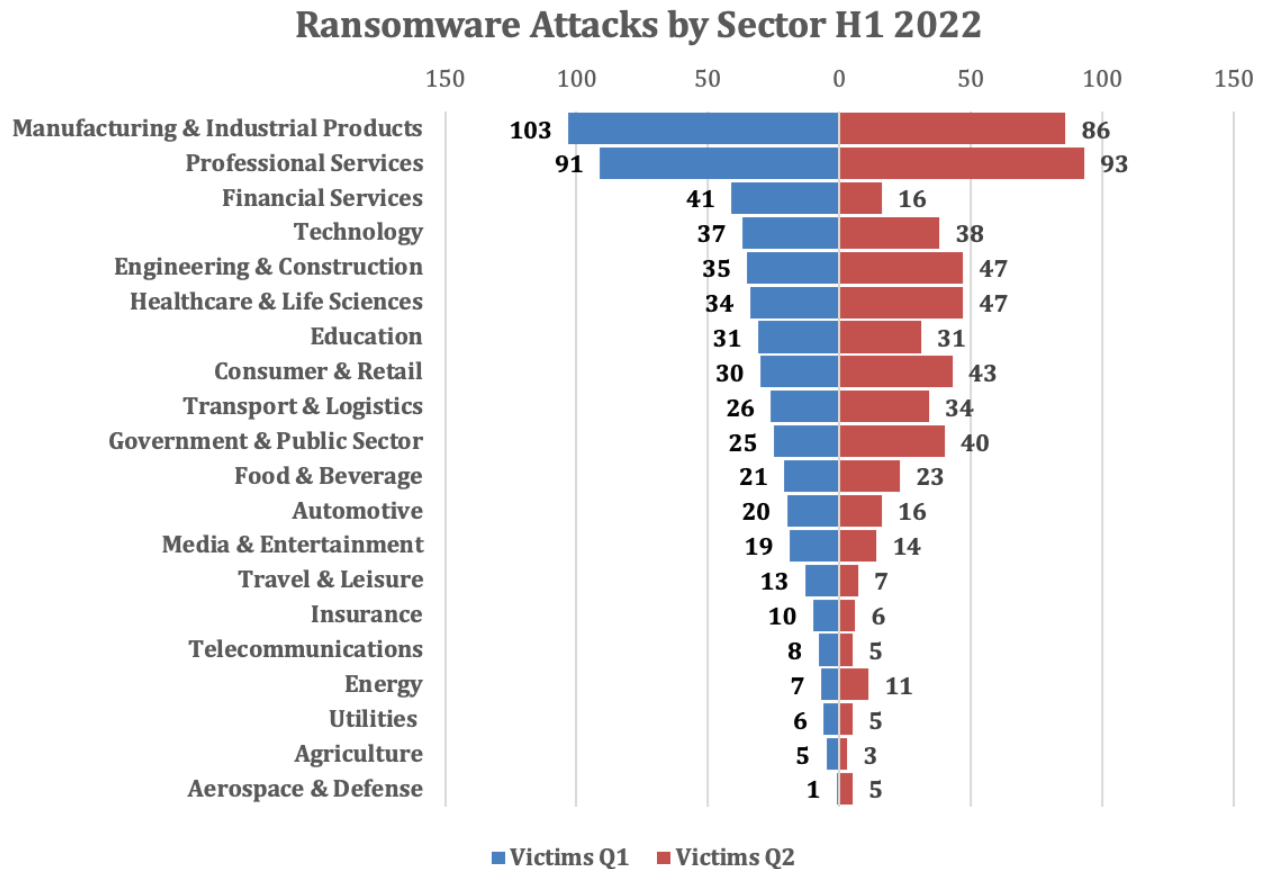


Figure 6. Sectors Targeted by Ransomware Mid-Year

The attacks on financial services organizations follow the historical trendline of ransomware groups taking aim at the monetary system. Manufacturing & Industrial Products organizations are also often an attractive target; disrupting those companies often has downstream impacts on the supply chain. Similarly, professional services firms could allow ransomware gangs to gain access to customer data and opportunities to encrypt other systems through managed services providers. It is thus professional services firms who are likely starting places for supply chain attacks. Traditionally, these companies are under-resourced in terms of cyber defense; once an attacker gains access, they can likely hop to their real target via a supply chain relationship. [This was how the 2014 Target breach occurred](#), in fact.



MAJOR RANSOMWARE THREAT GROUPS

Ransomware as a threat class is not a monolithic entity. There are numerous groups that have their own ransomware or license the code of other, more talented ransomware gangs. Despite this, there are a few prominent ransomware gangs that conduct most of the attacks or have the largest affiliate networks in the underground.



26 RANSOMWARE FAMILIES WERE ACTIVE IN Q1 2022

Among the numerous attacks done on multiple sectors of businesses in early 2022, there are several prevalent ransomware threat groups. As previously stated, we observed 26 ransomware families active in Q1 2022 and 25 ransomware families active in Q2 2022. Of the families observed, LockBit and Conti were the most dominant ransomware groups that posed the greatest threat to organizations in the first half of 2022.

LOCKBIT

LockBit is one of the oldest ransomware groups. They have been operational since at least 2019, without rebranding to avoid its members being identified. They were the most active ransomware group by far in the first half of 2022. LockBit is among the most famous ransomware gangs as well; they are often in the news claiming responsibility for attacks. That they have been able to avoid rebranding is a positive sign for their relative longevity. The chart below details the sectors they most commonly targeted in the first half of 2022.

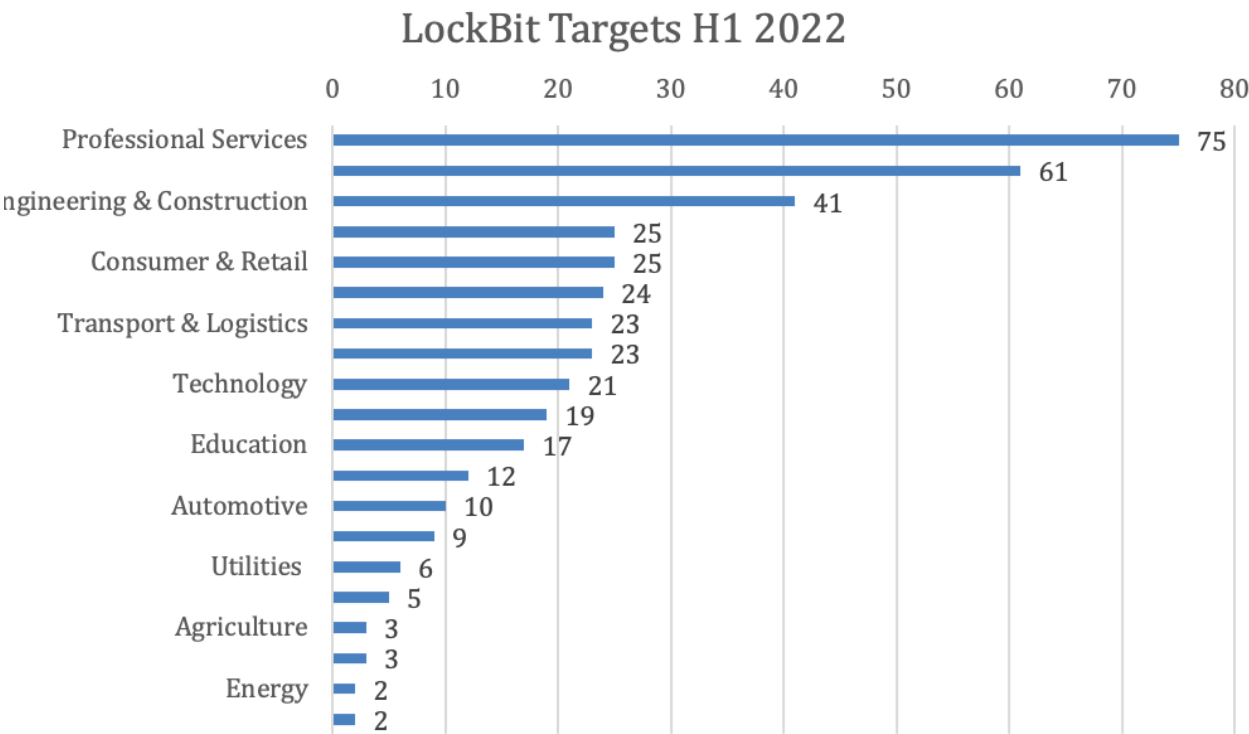


Figure 7. Sectors Targeted by LockBit H1 2022





LOCKBIT (CONTINUED)

According to our data, LockBit most frequently targeted the professional services sector in the first half of 2022, with that industry enduring 75 of their cyberattacks or about 19% of their total 406 targets. LockBit also targeted the manufacturing and industrial products sector with about 15% of their cyberattacks. Some of the other industries LockBit frequently targeted included financial services, engineering and construction, technology, government and public sector, and education.

Professional services as a category makes some sense for LockBit. It includes service providers like Managed Security Service Providers as well as other organizations who focus on staff augmentation for a host of industries. As supply chains become a common vector for ransomware, LockBit compromising this type of firm theoretically provides them access to many other organizations.

LockBit’s focus on financial services declined throughout the first half of the year. They targeted 21 financial firms in Q1, but only four in Q2. That was the largest single decline in a targeted sector, and there does not appear to be a logic for the decline. The largest growth in attacks was in the Consumer & Retail sector, which saw 7 attacks in Q1 but 18 in Q2. This could be indicative of a slight change in targeting strategy for LockBit but could also be unrelated.

In terms of geography, LockBit followed the trend of targeting companies located within the United States as their primary target. This was the largest victim group, with 32% (68 victims being US-based). The second largest targeted countries were followed by Italy, the UK, and France.

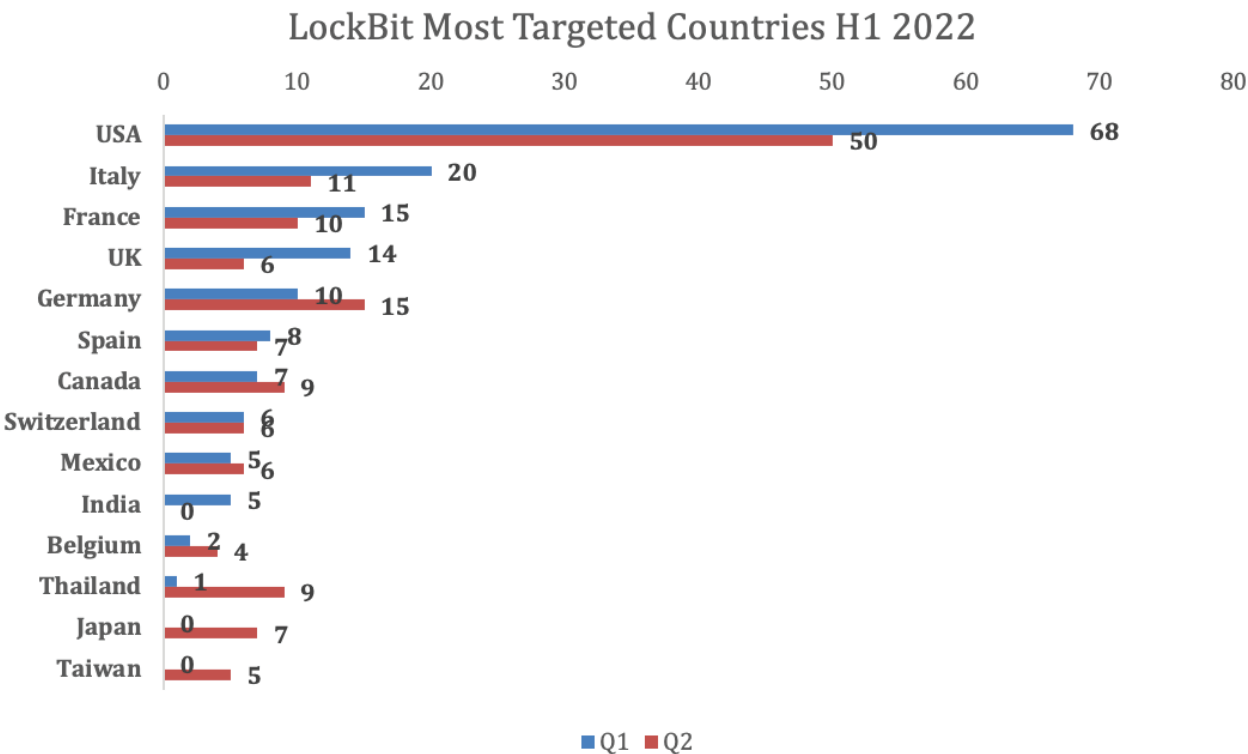


Figure 8. Top Countries Targeted by LockBit Ransomware Mid-Year 2022





LOCKBIT (CONTINUED)

Another possible reason for the decline is the release of LockBit 3.0, which occurred in June 2022. The new version of the ransomware strain introduced updated features, as well as the launch of their bug bounty program. This bug bounty program offers payment for reporting vulnerabilities and bugs in LockBit's ransomware and data leak site, TOX, and TOR. It was released with the intention to pay hackers to protect their operations further from risks in general, especially if it could harm their operations. LockBit 3.0 also started packaging its victim data and included a searchable company function in Q2.



MORE THAN A THIRD OF LOCKBIT'S VICTIMS WERE BASED IN THE UNITED STATES

According to [Darkfeed.io](https://darkfeed.io), the first payout of the new bug bounty program was completed on July 6th, 2022, in the amount of \$50,000. The bug that was uncovered made it possible to decrypt any vmdk or vhdx file for free, given the beginning of these files begins with zeros. In order to minimize the damage and the impact of payments for the decryptor from currently affected companies, the encryption algorithm was changed in the Linux vmdk files encryptor. This bounty helped the gang close the gap to continue conducting their malicious activities.



CONTI

Conti is another influential ransomware group that was highly active in the first quarter of 2022. The Conti group uses malware to block access to computer data until a ransom is paid. They became even more famous in February because of a few things: they voiced support for the Russian government in its invasion of Ukraine, and someone leaked their internal information it what became known as “the Conti Leaks.”

Following the Conti Leaks, it was confirmed that Conti conducts its operations much the same as a traditional business. Their operations include an HR team, customer service representatives, regular salaried employees, and even research and development. These leaks occurred four days after Conti announced its full support of the Russian government as they invaded Ukraine in February. This announcement made Conti unique among ransomware gangs, as many avoid explicit statements of support for any government.

In terms of their industry targeting, 27% of the organizations targeted by Conti in Q1 2022 are in the manufacturing and industrial products sector. The additional sectors also targeted included professional services at 13% of their ransomware attacks and the consumer and retail industry as being the target of 9% of their efforts. Most of Conti’s targets were from the USA, with 41% of their victims. German companies comprised 12% of their attacks and the UK was targeted 10% of the time to round out the top three countries targeted by this group.

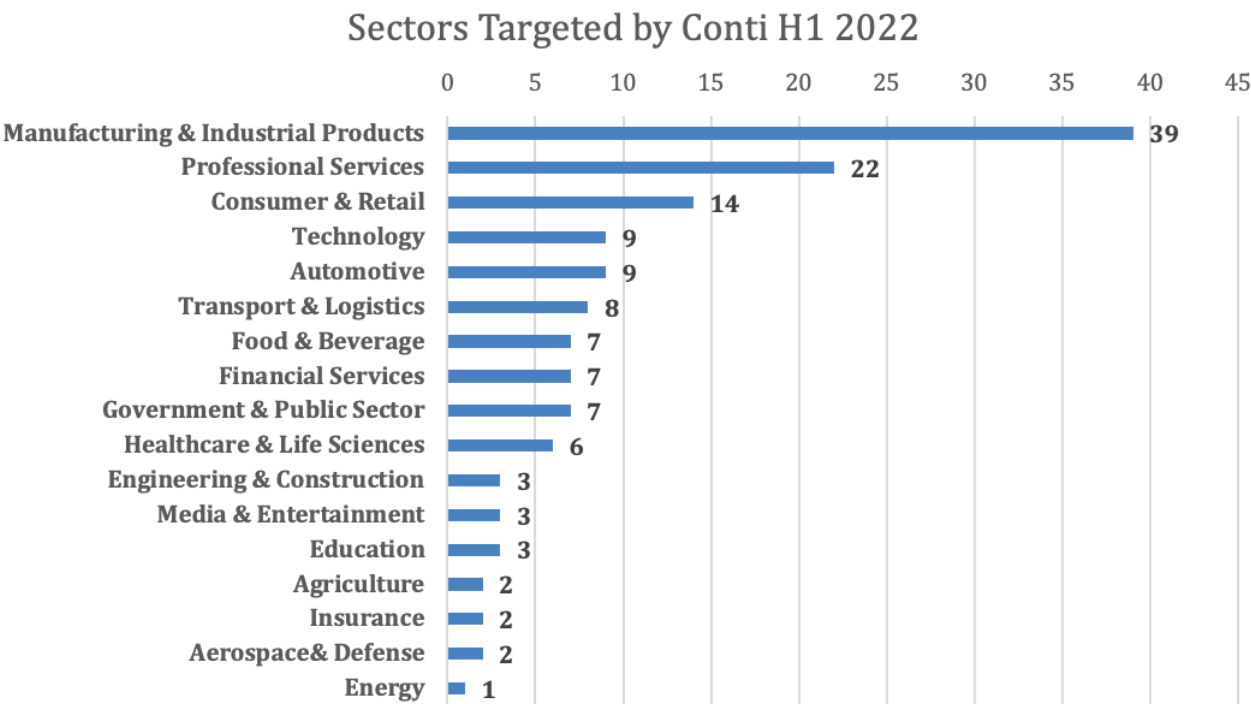


Figure 9. Sectors Targeted by Conti H1 2022





CONTI (CONTINUED)

While Conti was still one of the most active ransomware groups in Q2, they had about half the number of victims compared to Q1. This was due in part because Conti shut down operations, took its infrastructure offline, and team leaders advised the group was disbanding in May of 2022.

Prior to their shutdown, two of Conti's final victim listings were Costa Rica and Peru, which was uncommon for them to list a country instead of a company. A malicious actor going by the alias of unc1756 began adding government links and data for each of these countries to their respective postings. Costa Rica had seven government entities listed on the data leak site which resulted in Costa

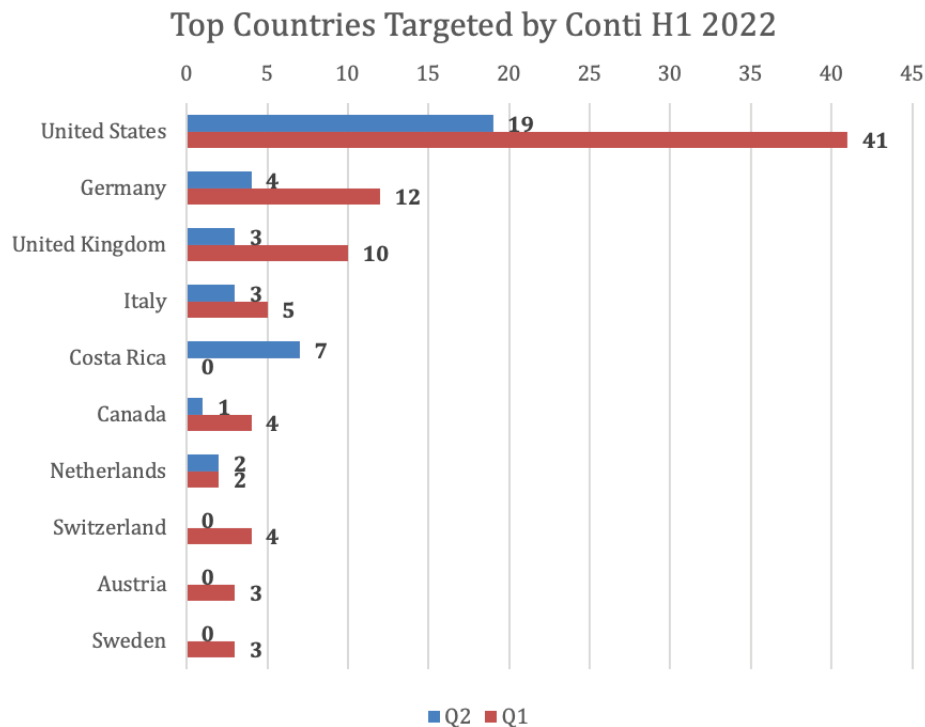


Figure 10. Top Countries Targeted by Conti Ransomware Mid-Year 2022

After Conti's shutdown, many speculated that the group might rebrand into smaller units or members would join other active ransomware groups. At the end of April, a new ransomware operation emerged called Black Basta. Some researchers believe Black Basta is Conti rebranded to avoid detection. It also appears to have some former members of REvil involved, which could have resulted following REvil's breakup.

The Black Basta group was the third most active group in the second quarter. It is possible that Conti members had a backlog of data they planned on publishing and waited for the rebrand after the chat log leaks. It is also possible that members of Conti joined the Quantum ransomware group.

Quantum posted at least three companies in Q2 that were either discussed in the chat logs or had been previously posted to Karakurt, which is believed to be Conti's data extortion division. The Quantum ransomware gang also had a large uptick in activity compared to Q1, which equaled about a 575% growth in their efforts from 5 to 29 victims. It has been suggested that the gang now has a larger group to aid their exploits and ransomware efforts.



RANSOMWARE-AS-A-SERVICE (RAAS)

Ransomware as-a-Service has also emerged as a common tactic for cybercriminals. RaaS has allowed nearly anyone with basic technical skills to become a ransomware threat actor. In the past, it was considered challenging for criminals to develop their own ransomware programs because the tools were complex and expensive. Nowadays, RaaS allows almost anyone to run their own cybercrime empire, easier and more accessible than ever before.

The RaaS model has been around for years. But recently, it has grown significantly due to increased customer and vendor demand. The customer base typically purchasing RaaS products consists of those looking for “off-the-shelf” malware that can be used in their attacks. These purchases also provide vendors access to readymade tools that allow these customers to instantly launch attacks without having diverse technical skills or knowledge about cryptography or cybersecurity best practices.



SINCE ITS INITIAL KNOWN LAUNCH IN 2016, RAAS HAS GROWN INTO A HIGHLY LUCRATIVE BUSINESS MODEL AND EXPANDED TO INCLUDE A WIDE RANGE OF MALICIOUS TOOLS—including BANKING TROJANS, SPYWARE, AND CRYPTO MINERS.

The most popular RaaS platforms are advertised on dark web forums and have thousands of registered users who pay monthly subscription fees in exchange for access to their toolkits. These services offer several benefits to would-be attackers such as:

- Establishing a framework to launch attacks
- Benefiting from other users testing and improving tooling code
- Leveraging others' servers to avoid the need to build new infrastructure.

As ransomware continues to evolve, LookingGlass anticipates RaaS will also increase in prevalence.

A POSSIBLE RANSOMWARE FUTURE

Ransomware's prevalence has grown over the past decade. In the first six months of 2022, with all the activity that LookingGlass has observed, we anticipate that the ransomware problem will continue to affect organizations of all sizes. More concerning, however, is the professionalization of ransomware gangs. Although Conti is the only gang where we have confirmation of their business practices, it stands to reason that the most successful ransomware groups likely have organized themselves in a similar fashion. It would be highly unlikely for successful groups like LockBit and others to have not organized themselves similarly.

This new, more professional ransomware structure can only mean that the problem will continue to grow in the months ahead. We anticipate the adoption of more traditional business practices as the underground economy continues to remain robust. Ransomware-as-a-Service will likely also become more prominent, and it is possible that other ransomware groups could create a bug bounty program like LockBit.

Overall, the adoption of professionalized tactics and more traditional business practices is likely to continue among financially motivated ransomware gangs. There is too much money involved in encrypting data and extorting money from enterprises and governments for this trend to abate. LookingGlass will continue to observe dark web forums and ransomware activity as these trends continue.





ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass is an intelligence company that empowers organizations to make national, industrial, and enterprise-scale decisions. With unparalleled, curated intelligence on critical assets, risks, and sectors. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect financial systems, defend critical infrastructure, and safeguard national security interests.

With insight into exposures, risks, and vulnerabilities across attack surfaces and relevant threat intelligence and analysis, LookingGlass provides a comprehensive view of cyber risk. Through the power of this intelligence, organizations make more risk-based decisions about their security. This helps mission-critical organizations reduce their mean time to detect and respond to incidents, enable cyber investigations, jumpstart threat hunt operations, and improve analyst productivity and efficiency.

Learn more at <https://lookingglasscyber.com>