INTEL471

Leading Ransomware Variants

TLP:CLEAR

Q3 2022

Key findings

- Intel 471 observed 455 ransomware attacks during the third quarter (Q3) of 2022, a decrease of 72 attacks recorded from the second quarter (Q2) of 2022.
- The most prevalent ransomware variants in descending order were LockBit 3.0, Black Basta, Hive and ALPHV aka ALPHV-ng, BlackCat.
- The most-impacted sectors, in descending order, were consumer and industrial products; manufacturing; professional services and consulting; real estate; public; technology, media and telecommunications; energy, resources and agriculture; life sciences and health care; financial services and nonprofit.
- The most-impacted regions, in descending order, were North America, Europe, Asia, South America, Oceania, Africa and the Middle East.
- The dissolution of the Conti group likely impacted the overall quantity of breaches as well as placement of most impactful ransomware variants for Q3 2022.

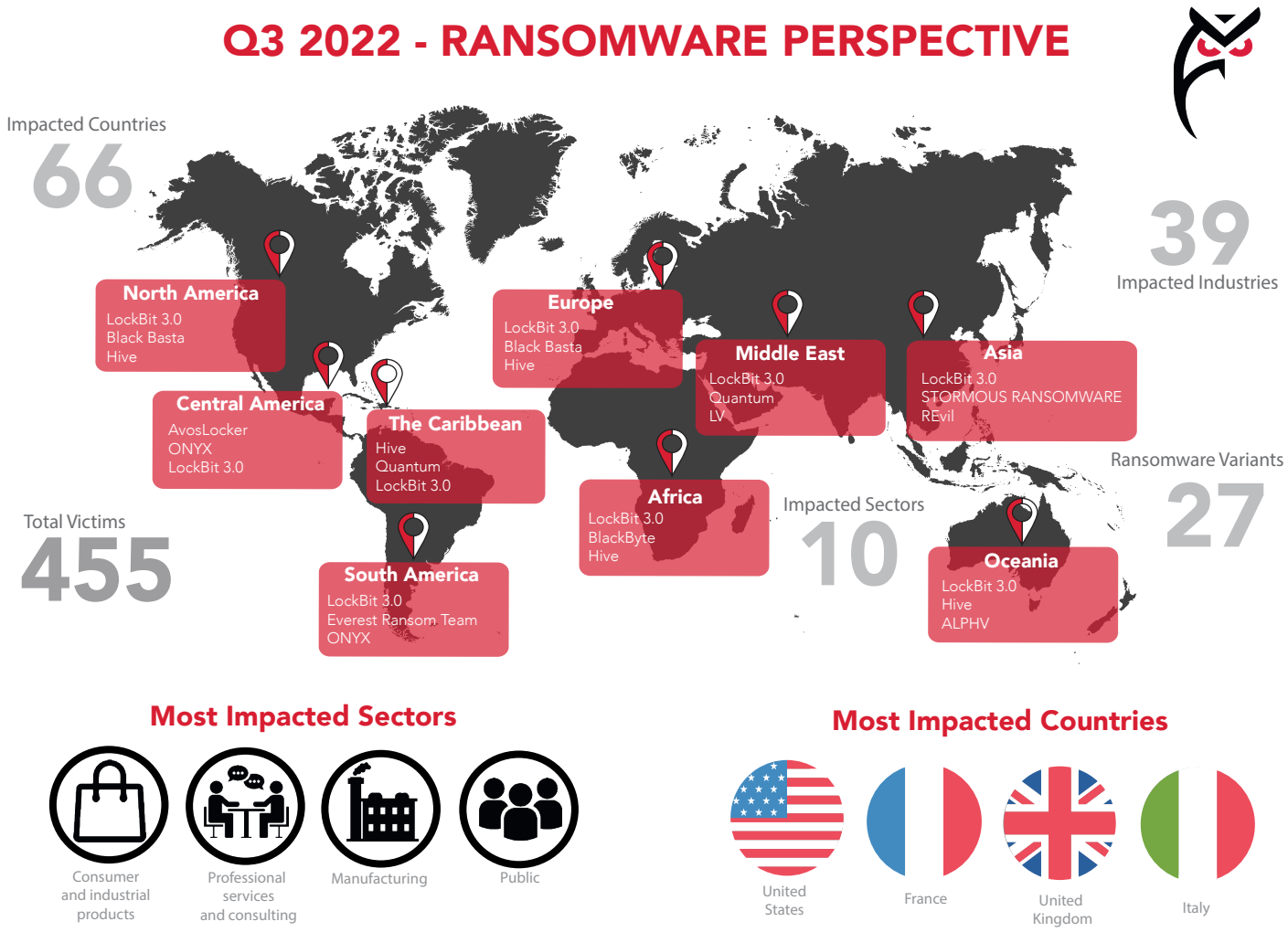

Figure 1: Ransomware statistics for Q3 2022

Overview

Intel 471 reported 27 ransomware variants were used to conduct 455 attacks from July 2022 to September 2022, a decrease of 38 attacks from the second quarter of 2022 and 134 from the first quarter of 2022. The most prevalent ransomware strain this quarter was LockBit 3.0, which was responsible for 42.2% of all reported incidents. This was followed by Black Basta at 11%, Hive at 9.23% and ALPHV at 6.6%. Other reported variants each accounted for 4.62% or less of the total number of observed ransomware attacks. The daily average of reported LockBit breaches was two - the same trend we observed from the ransomware group in the third and fourth quarters of 2021 and the first and second quarters of 2022.

In June 2022, we observed the Conti ransomware group's payment site and victim name-and-shame blog went down. The group allegedly terminated its operation due to mounting law enforcement pressure and public scrutiny. This likely impacted the overall quantity of breaches for the third quarter of 2022 compared to the previous two quarters by decreasing the total number of breaches and allowing other variants to appear in the top four or move up in the rankings.

Each recorded ransomware event was sourced from Intel 471 Spot Reports or Breach Alerts, which listed impacted entities and domains when available and were tagged with a country, industry, region and sector that align with our General Intelligence Requirement (GIR) framework. Our analysis in this review is based on ransomware variant-related events specifically observed and recorded by Intel 471.

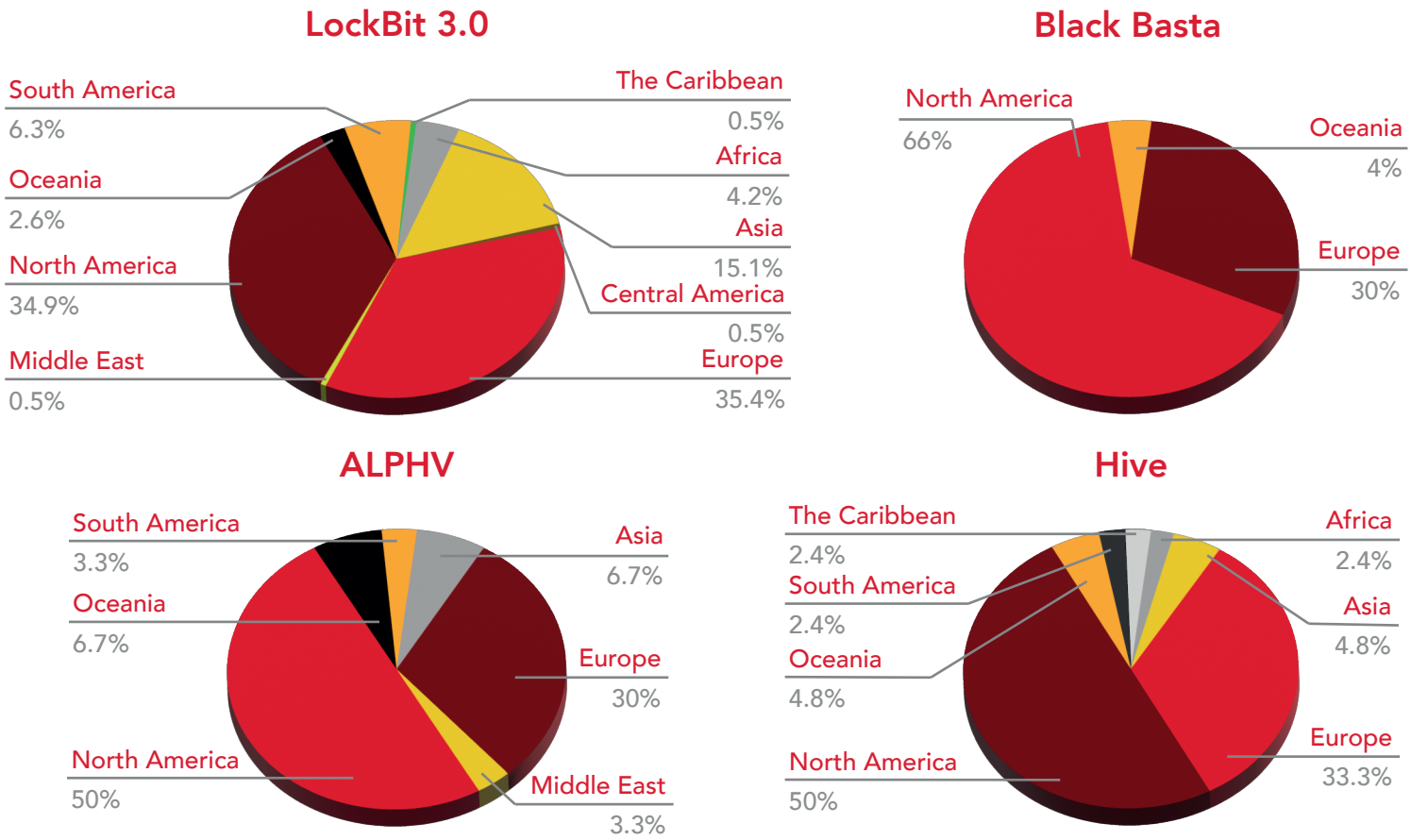

Figure 2: The graphs depict the percentage of variant-specific events per impacted region for the top four most active ransomware services in the third quarter of 2022.

LockBit 3.0

The LockBit 3.0 ransomware continued to be the most prominent variant in the third quarter of 2022 at 192 ransomware breaches, highlighting its continued dominance. The countries most impacted by LockBit 3.0 in descending order were the U.S. at 31.25%, France at 14.1%, Italy at 4.7%, Taiwan at 4.2% and Canada at 3.65%. The LockBit 3.0 ransomware impacted another 37 countries, but each amounted to less than 2.6% of the total number of ransomware events associated with this variant.

The sectors most impacted by LockBit 3.0 were professional services and consulting and manufacturing at 18.75%, followed by consumer and industrial products at 17.19%, real estate at 10.94%, public at 9.4% and energy, resources and agriculture at 8.34%. We observed a slight decrease in the number of attacks that impacted organizations in the consumer and industrial products sector from the second quarter of 2022. However, analysis of Intel 471 recorded breach events indicated the LockBit 3.0 operators remained relatively consistent in targeting this sector over time.

The LockBit 3.0 variant first was announced in the second quarter of 2022. The actor **LockBit** aka **LockBitSupp** claimed version 3.0 of the ransomware-as-a-service (RaaS) included an updated data leak blog, a bug-bounty program and new functionality in the ransomware. The variant impacted a relatively consistent number of organizations, down just 4.7% from the previous quarter.

LockBit security breach

In September 2022, the LockBit ransomware version 3 builder was leaked via Twitter social media. The actor **LockBitSupp** claimed the files were leaked by a disgruntled coder. The incident rippled through the underground community and sparked an active discussion on the XSS forum. Actors revealed details about the LockBit RaaS program, including real-world identity information of the ransomware developer. Details included legitimate organizations the individual worked for, property owned, government and military service involvement, familial status and previous ransomware group affiliations.

An actor stated this was the "end of the LockBit era." However, **LockBitSupp** claimed the RaaS operation was not impacted by the breach, likely in an attempt to save face and preserve the reputation of the ransomware group. This incident has the potential to further decrease the amount of LockBit breaches in the fourth quarter of 2022. The syndicate likely will need to focus attention on modifying the ransomware's code and the groups' tactics, techniques and procedures (TTPs), as well as implementing more operational security (OPSEC) measures. It is likely actors may use the LockBit source code as foundation to build other ransomware programs.

Black Basta

The Black Basta ransomware compromised 50 organizations in the third quarter of 2022. The Black Basta affiliate program's portfolio primarily includes highly profitable organizations. The sectors Black Basta ransomware impacted the most this quarter were consumer and industrial products at 19%; professional services and consulting, technology, media and telecommunications and manufacturing at 16.67% each; life sciences and health care at 11.9%; and energy, resources and agriculture at 9.52%. Entities that fell within the other three sectors accounted for less than 4.76% of all Black Basta ransomware breach instances.

The U.S. was the most-impacted country at 62% of all reported Black Basta attacks, followed by Germany at 18%. The other six countries with organizations Black Basta compromised accounted for less than 4.34% of all breaches in the third quarter of 2022. There was a large jump from 17.1% to 62% for U.S. impact of breaches from the second to third quarter of 2022. The variant also went from impacting 11 different countries to eight during this time. It is possible actors deploying Black Basta focused their efforts on targeting organizations based in the U.S. instead of a wider array of nations.

The Black Basta variant became the second most observed variant this quarter, which is where the Conti variant stood in the second quarter of 2022. We previously reported with a low to moderate degree of confidence the Black Basta RaaS was launched by the actor **tramp**, a Conti ransomware affiliate. The actor likely continued to use Conti's TTPs to operate the Black Basta ransomware following Conti's dissolution.

Hive

The Hive ransomware variant returned to the top four most observed variants this quarter since the first quarter of 2022. It was the fourth most deployed variant in the first quarter and the sixth most deployed in the second quarter of 2022. The number of breaches the ransomware group conducted each quarter remained relatively stable from the first to second to third quarter of 2022 at 41, 32 and 42, respectively. The fluctuation in its place likely is due to other groups demonstrating more or less activity in their own operations.

Countries most impacted by Hive from July 2022 to September 2022 included the U.S. at 47.2% and the U.K. at 14.3%. The Hive variant impacted 13 other countries that accounted for 4.8% or less of the total countries affiliated with the variant.

In August 2022, an alleged operator of the Hive ransomware revealed they used phishing emails as an initial attack vector. The actor allegedly leads a team of network hackers that targets businesses of all sizes in Australia, Canada, the U.K. and the U.S. Actors deploying the Hive ransomware often leveraged phishing campaigns to provide initial access and distribute their malware. Most of these phishing campaigns are drafted in the English language, which narrows the target set but allows actors to refine their product and tailor social-engineering campaigns to a focused audience. This likely reduces resource expenditure and increases the chance of success.

The most-targeted sectors by the Hive ransomware variant were consumer and industrial products at 19.1%, followed by professional services and consulting, technology, media and telecommunications and manufacturing at 16.67% each. The group also breached the life sciences and health care sector at 11.9% and the energy, resources and agriculture sector at 9.5%. Other sectors accounted for 4.76% or less of ransomware events associated with Hive.

ALPHV

The ALPHV ransomware variant was observed breaching 30 organizations in the third quarter of 2022, down from 35 breaches in the second quarter. The sectors most impacted by ALPHV were real estate and professional services and consulting at 26.67% each, consumer and industrial products at 16.67% and technology, media and telecommunications and manufacturing at 10% each. Other sectors accounted for 6.67% or less of total ALPHV breaches for the third quarter of 2022. The ALPHV ransomware variant also was the fourth most impactful to the Middle East based on observed incidents.

In September 2022, the alleged leader of the ALPHV RaaS affiliate program claimed the group targeted many airports, fuel pipeline operators, gas stations, oil refineries and other systems of critical infrastructure since the launch of the program.

The ALPHV ransomware group continues to leverage vulnerabilities and obtain exploits to impact large companies. In September 2022, the operator or operators behind the ALPHV RaaS affiliate program claimed to compromise the Virginia, U.S.-based information technology (IT) company NJVC LLC, the Turkey-based multibrand consumer products manufacturer Hayat Holding and the Canada-based transportation company The Checker Transportation Group.

Summary

Ransomware attacks observed in the third quarter of 2022 indicated the variants collectively targeted 111 organizations in July 2022, 162 in August 2022 and 182 in September 2022. The LockBit variant has remained the most impactful ransomware service with 192 attacks for the fourth consecutive quarter since the third quarter of 2021.

Following LockBit 3.0, 50 attacks were associated with Black Basta, 42 with Hive and 30 with ALPHV. Other ransomware variants observed conducting multiple ransomware attacks this quarter in descending order were AvosLocker, Vice Society, STORMOUS RANSOMWARE, RansomHouse, Quantum and LV, each accounting for 32 or fewer breaches.

Ransomware Variant Leaders Q2 2022 vs. Q3 2022 position			
Strain		Ranking	
		Q2	Q3
LockBit 3.0	⟺	1	1
Black Basta	⬆	3	2
Hive	⬆	Not in top	3
ALPHV	⟺	4	4

Table 1: The table depicts the change in ransomware variant ranks by number of attacks from the second quarter of 2022 to the third quarter of 2022.
**Note: These rankings are for illustrative purposes only and the assessment is made from Intel 471 data only.*

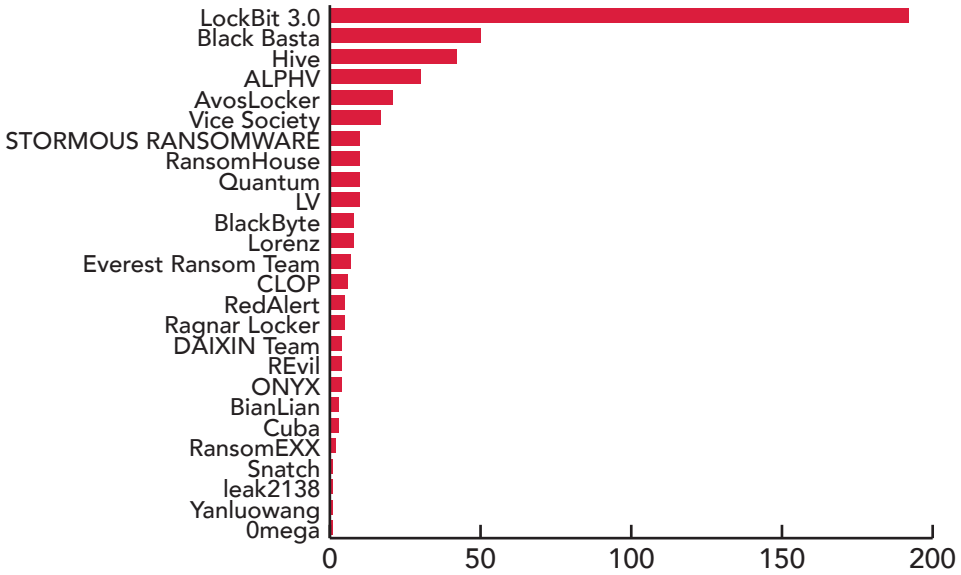

Figure 3: The graph depicts the total number of ransomware events per variant in the third quarter of 2022.

Attacks impacting the consumer and industrial products sector in the third quarter of 2022 decreased by 14% from the second quarter of 2022. It continued to be the most impacted sector this quarter, as it was in both the second and first quarters of 2022. The second most-impacted sector from July 2022 to September 2022 was professional services and consulting, followed by manufacturing. These sectors also were in the top four most impacted sectors in the third and fourth quarters of 2021, the first quarter of 2022 and the second quarter of 2022. This indicates there was no significant difference in the primary impacted sectors over the course of 2021 and 2022 thus far.

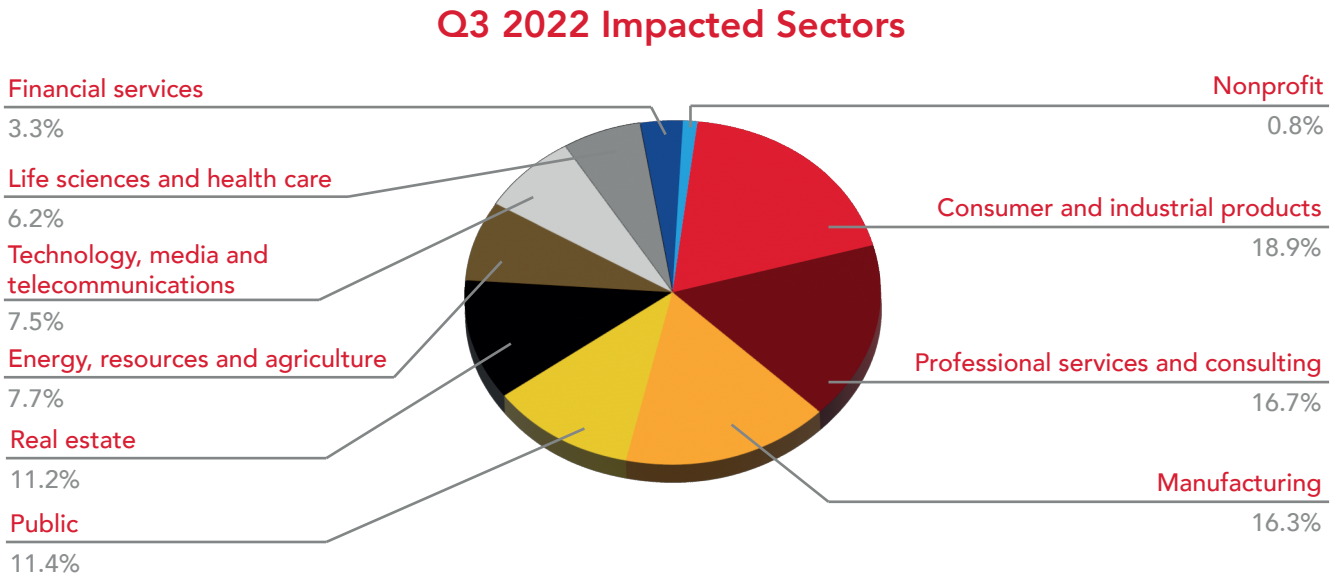

Figure 4: The chart depicts the breakdown of sectors and percentage of ransomware attacks observed in the third quarter of 2022.

The most-impacted region in the third quarter of 2022 was North America, amounting to 43.07% of all reported attacks. This was followed by Europe at 33.19%, Asia at 10.9% and South America at 4.18%. The number of entities impacted in these regions did not change the leading placement from the previous quarter, with the percentage impact per region remaining near constant. This likely will not change for the fourth quarter of 2022.

Ransomware Attacks per Sector Q3 2022 vs. Q2 2022	
Consumer and industrial products	↓ Down 30
Professional services and consulting	↑ Up 14
Manufacturing	↓ Down 15
Public	↓ Down 5
Real estate	↓ Down 10
Energy, resources and agriculture	↓ Down 1
Technology, media and telecommunications	↑ Up 2
Life sciences and health care	↓ Down 4
Financial services	↓ Down 4
Nonprofit	↓ Down 8

Table 2: The table depicts the change in ransomware attacks per sector from the second quarter of 2022 to the third quarter of 2022.
**Note: These rankings are for illustrative purposes only and the assessment is made from Intel 471 data only.*

Some ransomware groups maintained their pervasiveness in the third quarter of 2022, including LockBit 3.0, Black Basta, Hive, ALPHV, AvosLocker, Vice Society and STORMOUS RANSOMWARE. Although we observed many similarities from the previous quarter, there also were some notable differences. Significant increases for ransomware deployments were observed for the RansomHouse, Everest Ransom Team and RedAlert variants. We also observed the number of attacks associated with some ransomware variants decrease. The Cuba ransomware decreased from 19 attacks in the first quarter of 2022 to eight in the second and three in the third. This trend may continue toward the end of the year. Some variants went from being observed in the second quarter of 2022 to completely disappearing in the third quarter, including Conti, Haron, SunCrypt and Dark Angels.

We also observed the launch of several new RaaS affiliate programs. In late June 2022, an actor offered the MONSTER RaaS on an underground forum. In June 2022, another actor **chaos_exe** advertised the Solidbit RaaS affiliate program on a cybercrime forum. Lastly, in September 2022, the actor **BN28** advertised the Garyk RaaS affiliate program on a cybercrime forum. It is possible these groups will continue to operate in the fourth quarter of 2022.

Since the beginning of August 2022, we reported 21 breaches by the BianLian RaaS operator or operators. In July 2022, the RaaS claimed the compromise of the India-based engineering company ISGEC Heavy Engineering Ltd. with an annual revenue of US $734 million. In September 2022, the group claimed the compromise of and threatened to release data allegedly stolen from the Florida, U.S.-based furniture retailer Baer's Furniture Co. Inc. with an annual revenue of US $171 million. Due to its high level of activity toward the end of the third quarter, it is likely the group will impact more organizations in the fourth quarter of 2022. Intel 471 will continue to monitor the activity of this and other ransomware groups and report on their activity in the next quarter.

Observations from this report should be seen as an overview of activity highlighted across individual breach events that were correlated to a specific ransomware strain. They are not categorized at the service operator or affiliate level, which would be difficult to ascertain based on information available in breach notifications.