

KOVRR

Cyber Decisions. Financially Quantified.


The Ransomware Threat Landscape H1-23

GUY PROPPER
HEAD OF DATA

JULY 2023

www.kovrr.com

Introduction



In this comprehensive report, Kovrr collected and analyzed data on all known ransomware attacks reported during the first two quarters of 2023. The data was collected from multiple sources, all aggregated and updated regularly in Kovrr's Threat Intelligence Database. The database includes data on many different types of cyber incidents, but this report includes only data on ransomware attacks, excluding data on any other type of attacks.

The ransomware groups covered in this report all operate as a RaaS (Ransomware as a Service), a business model through which the ransomware binary and operation are sold or leased to operators, called affiliates. This means that a ransomware operation is composed of many different individuals, with separate roles, and the extortion profits are divided between them. Some individuals are responsible for initial access to the targets, others to lateral movement to interesting and profitable areas in the victim network, while others are responsible for the ransomware infection itself, and others negotiate with the victim after infection.

Summary

These are the main insights from the collected data:

-32% ATTACKS

There is a 32% drop in attack amounts in H1-23 compared to H2-22. It is important to note that this drop can also be due to delayed reporting of cyber incidents by attacked companies.



The most targeted industry is the Services industry, while companies with a revenue of \$10M-\$50M are the most common targets.

262 DAYS - AVERAGE LIFESPAN

The average lifespan of a ransomware group is 262 days, while the median is 167 days. In an average month, 18.3 different ransomware groups are active.

The top ten most active groups observed during the first half of 2023 are AvosLocker, Bianlian, BlackBasta, BlackCat, Clop, Lockbit 3.0, MedusaLocker, Play, Royal, and ViceSociety. All 10 actors accounted for 87% of attacks during this period, while the top 3 groups (Lockbit 3.0, BlackCat, and Clop) accounted for 53% of all claimed attacks during this period.

Data Collection Methods and Possible Biases

The data for this research was collected from Kovrr's Threat Intelligence Database, that collects data from multiple sources, and includes information on different types of cyber incidents. Specifically for this report, data was collected mainly from ransomware leak sites, public filings of attacked companies, and news reports on ransomware attacks. The data from ransomware leak sites was collected mainly from Double Extortion (<https://doubleextortion.com>), a data source providing up to date information from ransomware leak sites. The rest of the data was collected using proprietary sources and methods.

This data was then combined with additional sources to collect company business information and is limited to ransomware attacks that occurred and were reported in the first two quarters of 2023, between January 1st 2023 and June 31st 2023.

There are several possible biases in the data that may affect the results presented in the report.

Data collection for this research relied either on a company filing a notification on a ransomware attack, or a ransomware group uploading information about a victim. Therefore, in the case that a company decided not to file a notice of a ransomware attack, for example due to not being legally required to do so, it will not be included in our data. This means that companies located in countries that require data breach notifications, such as companies in the United States or the European Union, are expected to have a higher representation in our data. This is also true for companies in more regulated industries, such as healthcare.

Regarding data retrieved from ransom group sites, there may be cases where an attacker did not upload data on the attack victim, as the victim paid the ransom, or for other reasons. This means that some victims that have quickly paid ransoms following an attack might not appear in our data.

Additionally, we have previously researched and written about delayed reporting of cyber events by attacked companies (<https://www.kovrr.com/reports/2022-seems-to-be-on-target-for-the-lowest-year-of-reported-breaches-by-large-us-corporations>). This might cause our data for 2023, and especially for May and June, to be lacking, as some incidents that have occurred have not yet been reported.

Main Observed Trends

Number of Attacks in H1-23

The chart shows the number of attacks in the first half of 2023



It can be seen that there is a significant drop (32%) in the total number of attacks observed in the first half of this year compared to the second half of last year. When the data from the first halves of the previous two years is taken into account, the amount of ransomware attacks has remained relatively constant between these periods. Additionally, in the previous two years, more attacks have been reported, or have occurred, in the second half of the year compared to the first half. Though this could be a random pattern, one possible reason for it might be the holidays of Thanksgiving and Christmas, that occur during the second half of the year, and always cause a spike in cyber attacks.

! One last item of note and worth repetition, is that there is a known delay in reporting cyber incidents. This might cause the number of known attacks in the first half of 2023 to currently be lower, however, this can change in several months, as additional incidents are reported.

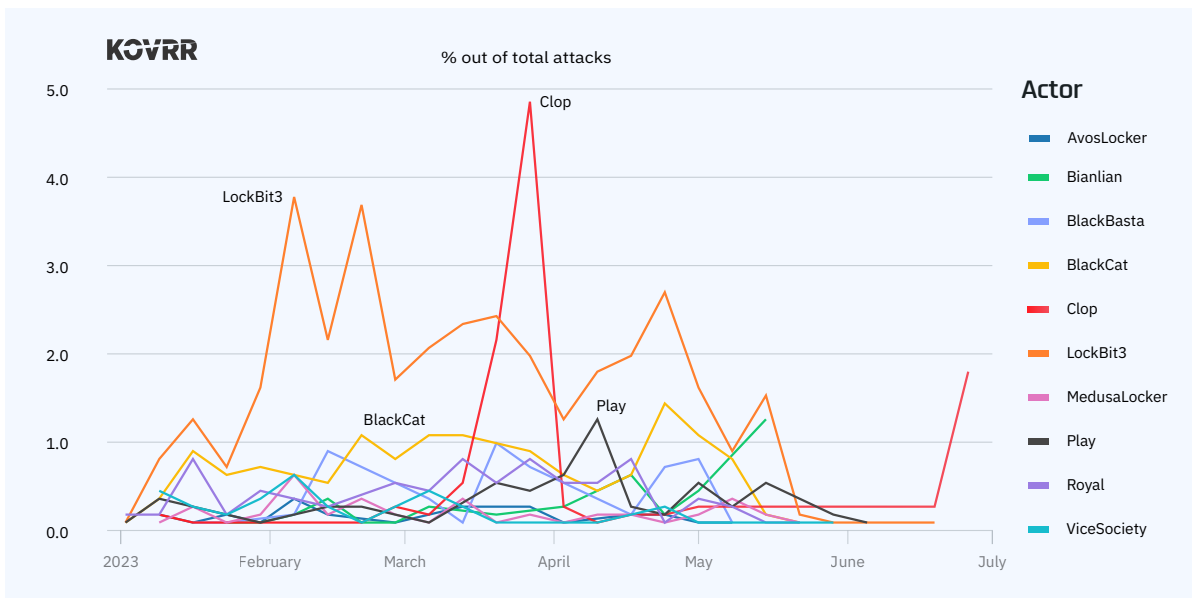
Identifying The Most Active Groups

The data analyzed in this report uncovered several interesting trends, regarding both the ransomware activity in the first half of the year, and the type of targets preferred by the most active ransomware attack groups.

The graph below shows the activity of the top 10 most active ransomware groups for the first half of 2023.

The names of the top ten groups are:

AvosLocker **BlackBasta** **BlackCat**
MedusaLocker **Lockbit 3.0** **MedusaLocker**
Clop **Play** **Bianlian** **Royal**



Out of these 10 actors, the top 3 most active groups for this time period are Lockbit 3.0, BlackCat, and Clop. Among them, these 3 groups accounted for 53% of all claimed attacks during this period. All 10 actors accounted for 87% of attacks during this period, with the remaining 13% divided between 31 other actors. The preferred victims for each attack group will be reviewed later, but in the meantime it is interesting to point out several data points:

1 Attack peaks

There are several large peaks of attacks in the graph - for Lockbit in February, and Clop in March and June. While the Lockbit peak in February is not attributed to any specific factor (apart from a general high attack rate for the group), the Clop peak in March is due to the exploitation of a vulnerability in Fortra's GoAnywhere software, which led to dozens of attacks by Clop on infected organizations, and the peak in June is due to the exploitation of a vulnerability in the MoveIT file transfer software. In general, ransomware groups have "picked up" several high profile vulnerabilities during the year, and exploited them very heavily, before organizations have the opportunity to patch them and close the window of opportunity. This is discussed further below.

2

Attack timing

Most attacks occurred during March (29%) and April (24%). In May, attacks decreased significantly, and only made up 10% of the data. However, the decrease might be due to delayed publication or reporting of attacks.

3

The chart compares the activity of the top five actors in H1-23, with their activity in the second half of 2022. It can be seen that Lockbit has kept continuously high activity in the first half of this year, performing a third of all attacks seen so far. The other top groups increased their activity from last year, with the most notable increase seen in the activity of the Clop attack group. After having a very small number of attacks in the second half of last year, they have risen to become one of the most active ransomware groups.

Actor	% of observed attacks H12023	% of observed attacks H22022
Lockbit	31.5%	39%
BlackCat	13%	8.5%
Clop	8%	<0.5%
Royal	7%	3%
Play	6%	1.5%

4

Vulnerabilities in open source tools

As mentioned above, several zero-day and one-day vulnerabilities have been extensively exploited by ransomware groups, that tried to attack victims quickly before the vulnerabilities were patched. Some examples of exploits are:

a

A vulnerability in Fortra's GoAnywhere software, tracked as CVE-2023-0669, led to the Clop peak, and to a smaller BlackCat peak, in March

b

A vulnerability in the MoveIT file transfer software, tracked as CVE-2023-34362, led to multiple Clop attacks in May. For more details:

<https://www.kovrr.com/blog-post/moveit-file-transfer-zero-day-c-ompromises-multiple-organizations>.

c

Vulnerabilities in PaperCut, tagged as CVE-2023-27350 and CVE-2023-27351, were exploited by Clop and Lockbit, leading to a peak in attacks from the middle of April until the beginning of May.

5

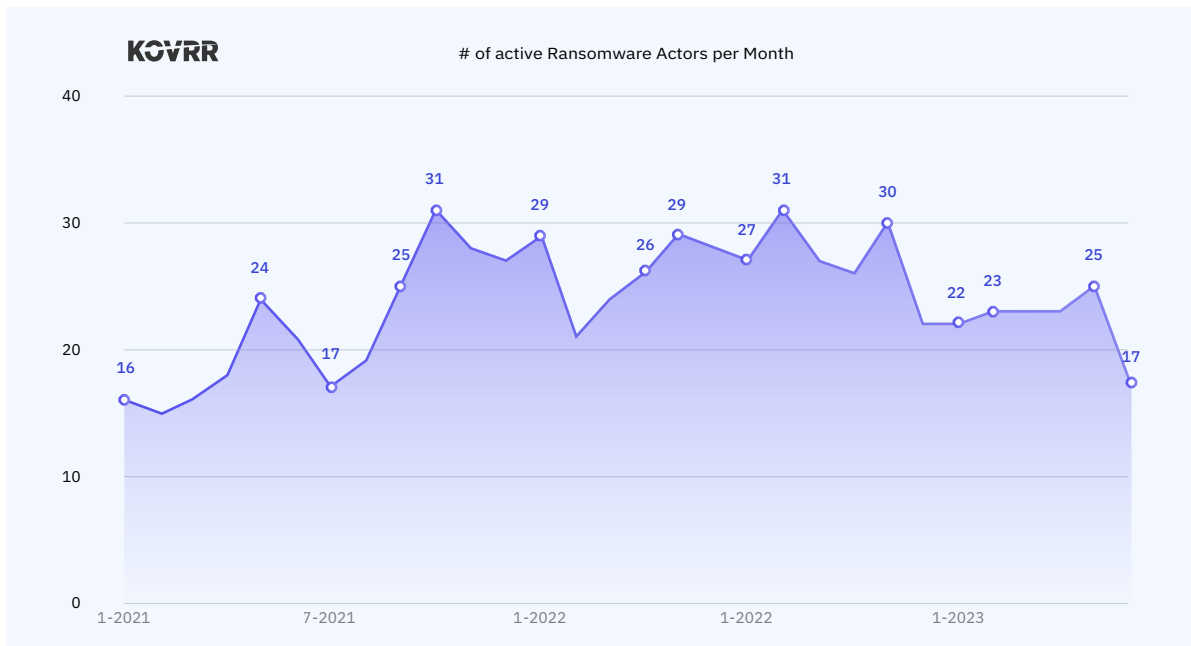
8Base

This is a new ransomware group that has attracted significant attention recently. From our data, 8Base was the second most active group for June, after Clop. The group attacked several companies, mainly located in the United States and Brazil, predominantly in the Business Services sector.

The Lifespan of Ransomware Groups

After reviewing the most active ransomware groups of the first half of 2023, it is worth taking a look at the overall lifecycle of ransomware groups, to understand what is their average life-span.

To understand this, we first checked how many ransomware attack groups were active (meaning actively posting on ransomware leak sites), since January 2021. The results are presented in the graph below.



Generally, it can be seen that from the second half of 2021, the number of currently active ransomware groups grew slightly, compared to before that period.

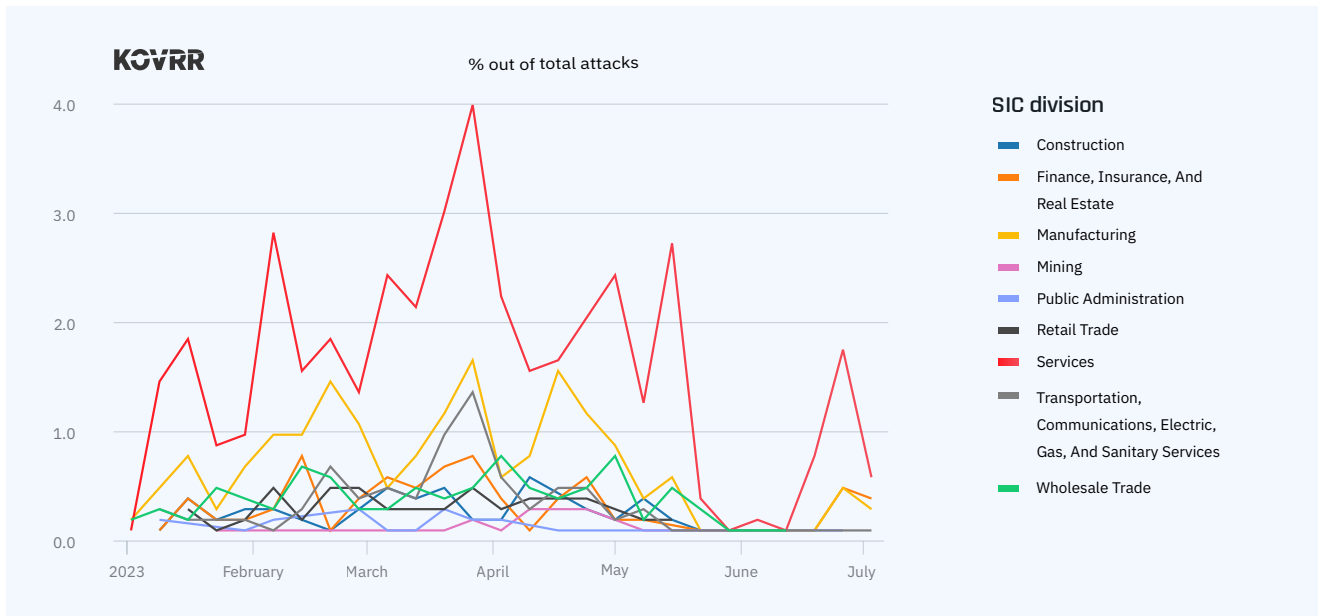
Overall, on average 18.3 actors were active per month during the entire time period. In addition, the average lifespan per actor is 262 days, while the median is 167 days. We also checked the number of active days for the current most active actors, and the data is shown in the table below. It can be seen that all of the top actors' lifespans are longer than the median, with most also having lifespans which are much longer than the average actor.

Actor	# of Days Active
Clop	964
BlackCat	535
AvosLocker	663
Bianlian	303
BlackBasta	807
Lockbit 3.0	367
MedusaLocker	635
Play	224
Royal	224
ViceSociety	723

The Most Targeted Sectors

As part of the analysis, we also identified the sectors that are most commonly targeted by the different groups. Sectors are identified by their SIC division. (<https://www.osha.gov/data/sic-manual>)

The chart below shows the distribution of SIC divisions targeted over time in the first half of 2023.



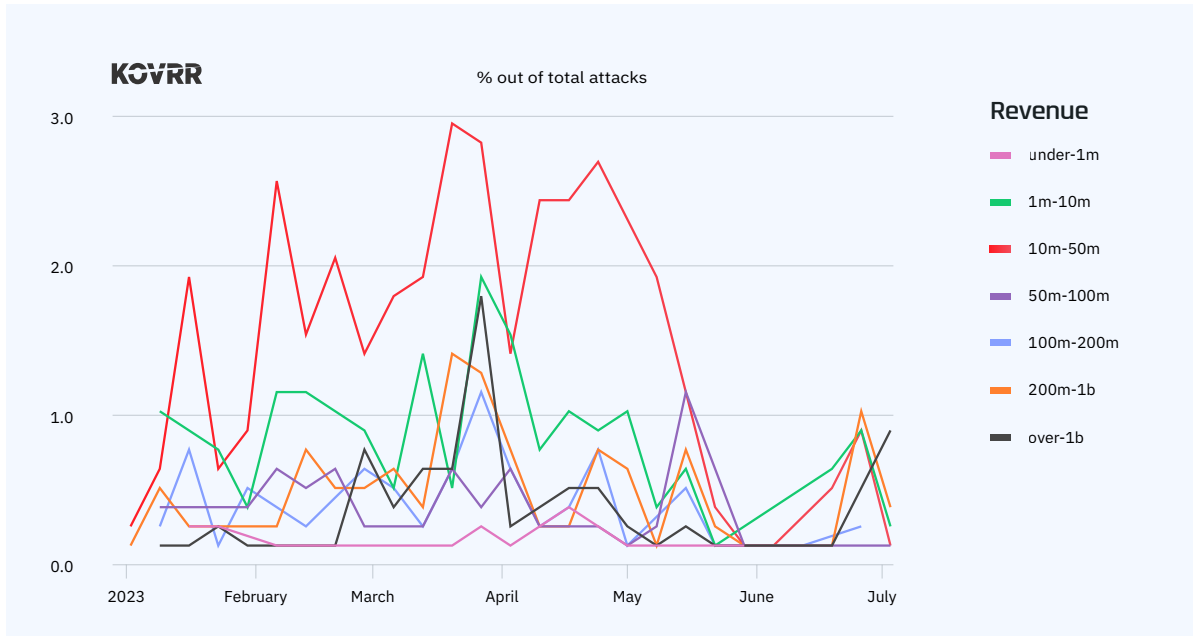
It can be seen that over the entire period, the top targeted SIC divisions are Services (42% of attacks), Manufacturing (18%), and Wholesale Trade (8.5%), which is closely followed by Transportation, Communications, Electric, Gas, And Sanitary Services (8.3%), and Finance, Insurance, And Real Estate (8%). Within the Services division, the top targeted SIC major groups are: Business Services (13% of attacks), Educational Services (8%), Engineering, Accounting, Research, Management, And Related Services (6.5%), closely followed by Health Services (5%) and Wholesale Trade-Durable Goods (5%).

From the data, it is clear that ransomware actors have a preference to attack companies that provide services. Service providers are a preferred target for ransomware actors for several reasons. Firstly, these companies provide services that are relied on by third parties, they store a significant amount of third party data, that will harm them if exposed, and they require as little downtime to their services as possible, making them an easy target for attackers wishing to cause denial of service. In addition, many of these companies maintain a large portion of their infrastructure online, and require external remote access to these online resources. Remote access is one of the attack methods most favored and exploited by ransomware groups, as remote access can in many cases provide a wide and simple initial access point to an organization.

Another interesting data point is the peak in attacks targeting companies in the Services division at the end of March, due to the high amount of attacks conducted by the Clop group, through exploitation of a vulnerability in Fortra's GoAnywhere software.

Victim Company Sizes

Kovrr also analyzed the revenue ranges of targeted companies, and the different revenue ranges targeted over time can be seen in the graph below.



The top targeted company sizes are: \$10M-\$50M (39%), \$1M-\$10M (20%), and \$200M-\$1B (12%). It is clear from the data that ransomware actors prefer to attack smaller companies, with only 8% of attacked companies having a revenue of over \$1B, and 70% of attacked companies having revenue below \$100M. This preference might be due to several reasons:

- 1 Smaller companies have a smaller workforces and a smaller budget. This means that in many cases they invest smaller amounts in cyber security and lack employees with cyber security expertise.
- 2 In recent years government and law enforcement agencies have become increasingly involved in ransomware attacks. Some attacks against very large companies, such as the attack against Colonial Pipeline in May 2021, have led to quick and aggressive law enforcement activity against the attacker. Attacking smaller companies, while possibly promising lower rewards, also poses a lower risk for ransomware groups, as they are less likely to be persecuted due to a single attack.

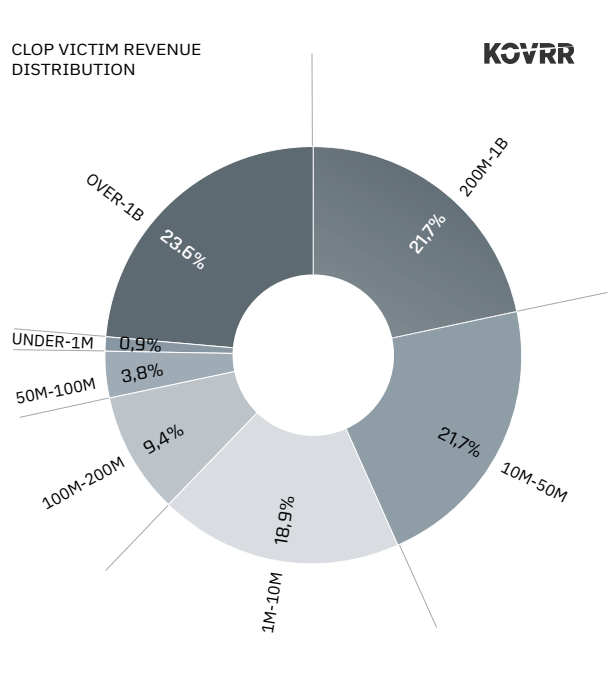
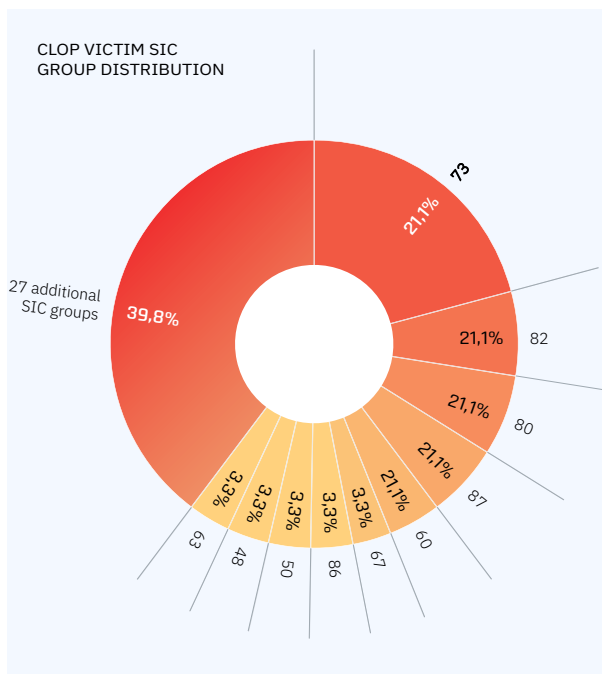
One more date point to note is there was a great rise in the proportion of large companies attacked in June. This is most probably due to the vulnerability in the MoveIT file transfer software, exploited by Clop to attack several very large companies.

Profiling the Top Ten Actors of H1-2023

The next section contains a detailed breakdown of the activity of the ten most active ransomware groups during the first half of 2023. We provide data on the top industries, company sizes, and company countries attacked by each group, along with a short overview of the attack group

In this section, the targeted industries are provided by division to SIC Major Groups, instead of SIC Divisions, as these provide higher granularity and help to show the preferred targets of each ransomware group.

Cllop



Summary

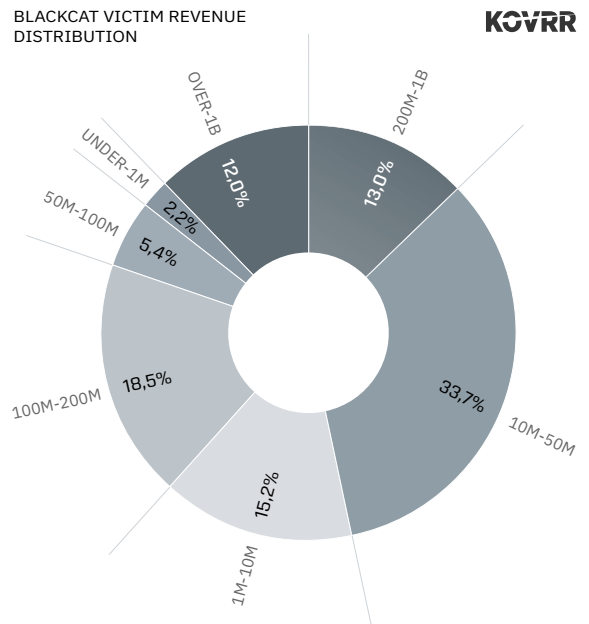
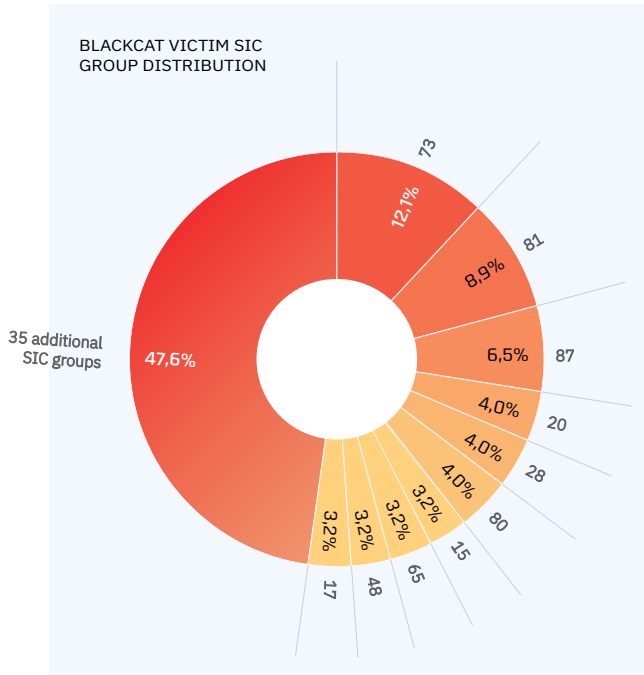
Cllop ransomware first appeared in 2019, and has since then been involved in several high profile attacks, including most recently the widespread attack exploiting vulnerabilities in the MoveIT file transfer software

<https://www.kovrr.com/blog-post/moveit-file-transfer-zero-day-compromises-multiple-organizations>

Main findings

In the time period studied, Cllop has mainly targeted companies in the Business Services sector (SIC group 73), followed by companies in the Educational Services sector (SIC group 82). Cllop favors attacking either very small companies, with between \$1M-\$50M in revenue, or very large companies, with over \$1B in revenue.

BlackCat



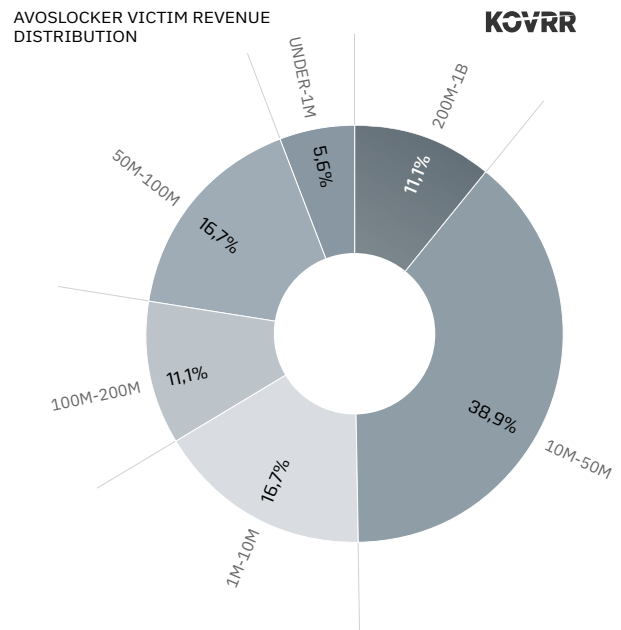
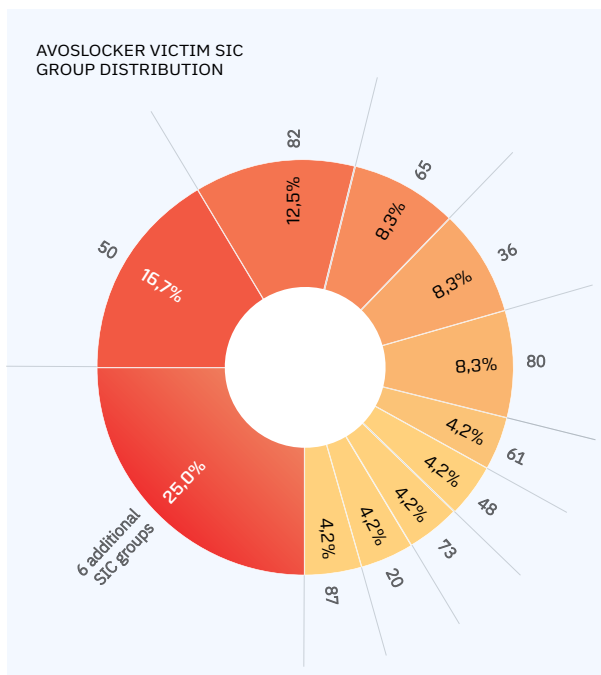
Summary

BlackCat ransomware, AKA AlphV or AlphVM, is a ransomware group that first appeared in November 2021. The ransomware, written in the Rust language, is a RaaS (ransomware as a service) operation, splitting profits between multiple affiliates that conduct different stages of the attack. The group has been involved in high-profile attacks against German oil companies, and a European government.

Main findings

In the time period studied, BlackCat has mainly targeted companies in the Business Services sector, followed by companies in the Legal Services sector. Additionally, BlackCat mainly attacks smaller companies, with a revenue range of \$10M-\$50M.

AvosLocker



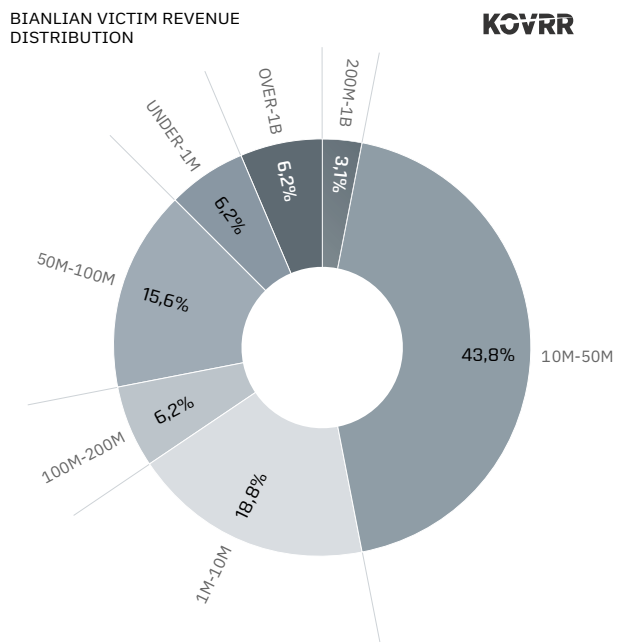
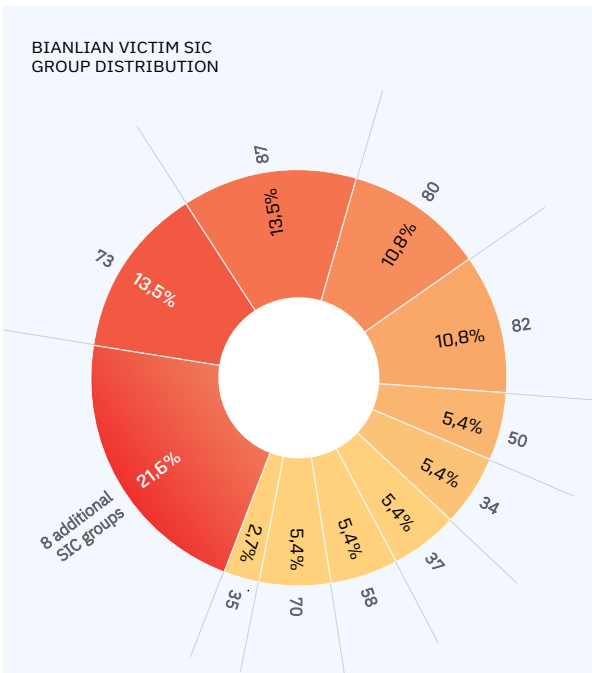
Summary

Avoslocker is another RaaS operation first spotted in July 2021. The ransomware, which has had several versions released since its initial appearance, has been involved in several attacks on US-based healthcare companies, such as CHRISTUS Health.

Main findings

In the first half of 2023, Avoslocker mainly targeted companies in the Wholesale Trade sector, followed by companies in the Educational Services sector. In addition, the group clearly prefers targeting smaller companies, with a vast majority of the targets having a revenue between \$1M-\$50M.

Bianlian



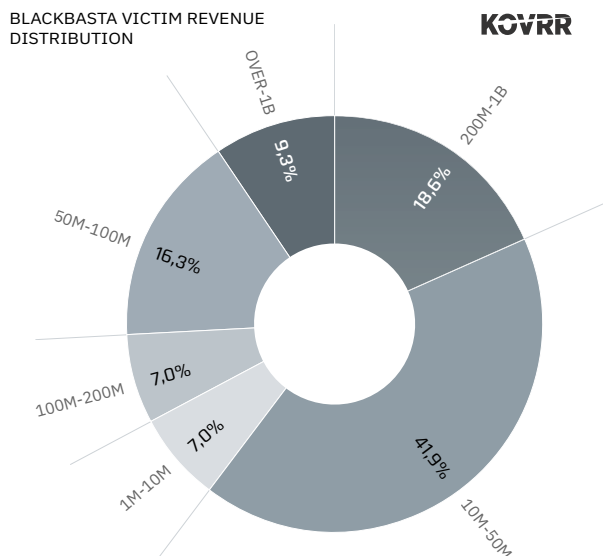
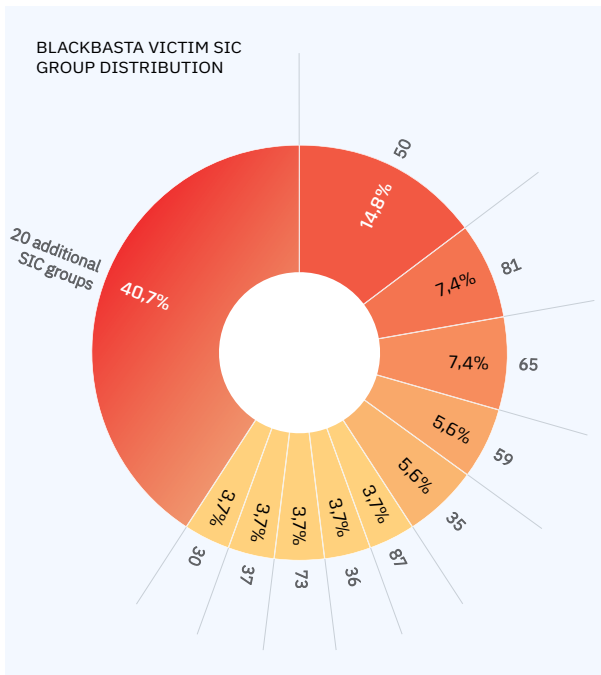
Summary

Bianlian is a ransomware operation that first surfaced in June 2022. The group, started off with a double extortion ransomware model (meaning that the data was both encrypted and stolen, and would be decrypted and not published in demand for a ransom), however, has switched to a data-theft only attack in January 2023

(<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a>), no longer encrypting data in attacked organizations.

Main findings

In the period studied, Bianlian mainly targeted companies from the Engineering, Accounting, Research, Management, And Related Services sector (SIC group 87), and companies in the Business Services sector. Bianlian also mainly targets smaller companies, with most targets having a revenue range of \$1M-\$50M



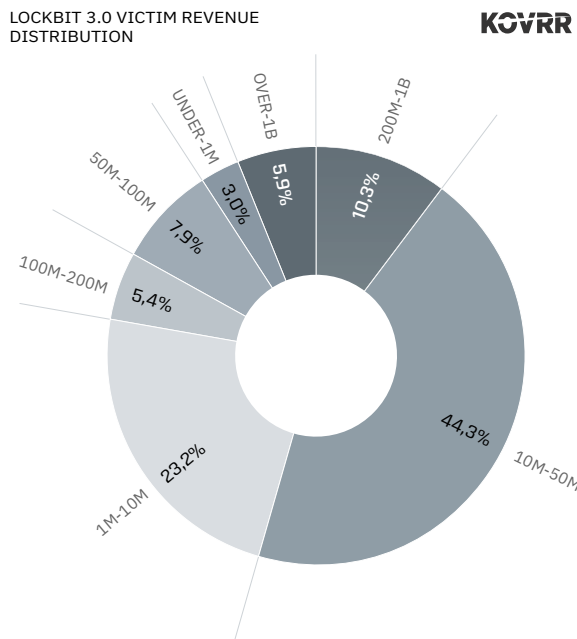
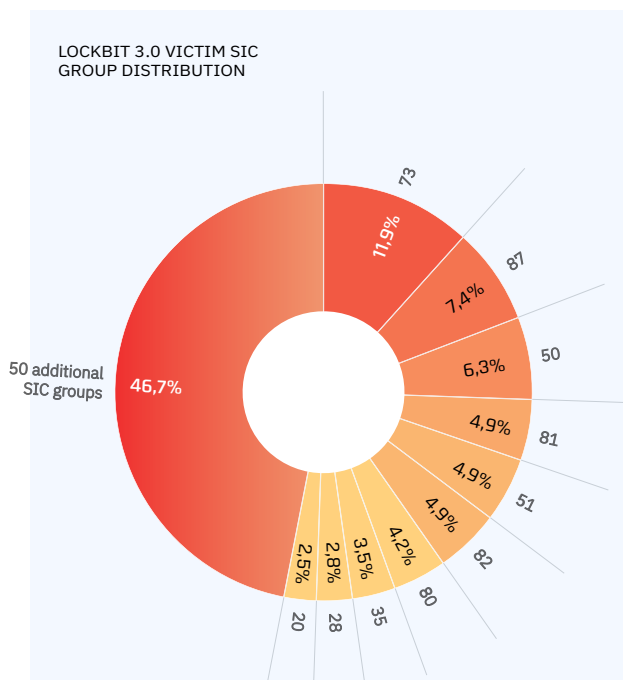
Summary

The Blackbasta ransomware group first appeared in early 2022, and operates using a RaaS model of double extortion in order to attack victims and extort them. The ransomware group attacked numerous victims shortly after its first appearance, including a high-profile attack on the American Dental Association (ADA)

Main findings

In the covered time period, Blackbasta mainly targeted companies in the Wholesale Trade sector, followed by companies in the Real Estate and Legal Services sectors. Like many other ransomware operators, the group mainly targets smaller companies, with a revenue range of \$10M-\$50M. This is followed by larger companies, with a revenue of \$200M-\$1B.

Lockbit 3.0



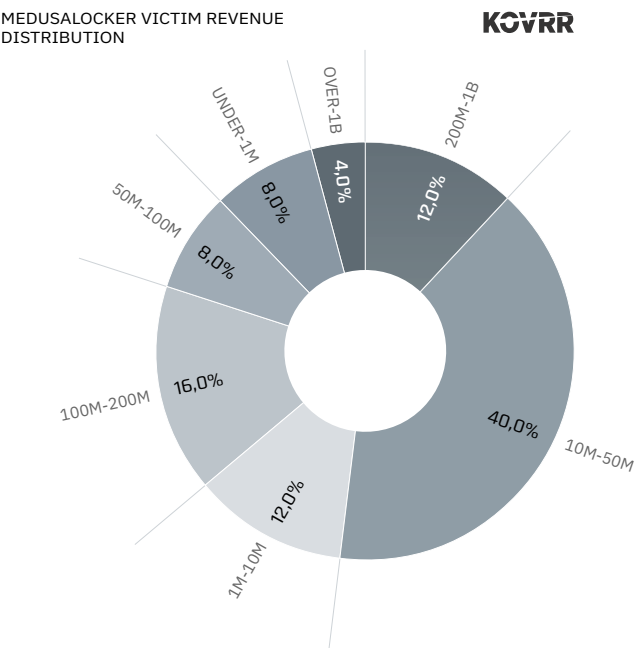
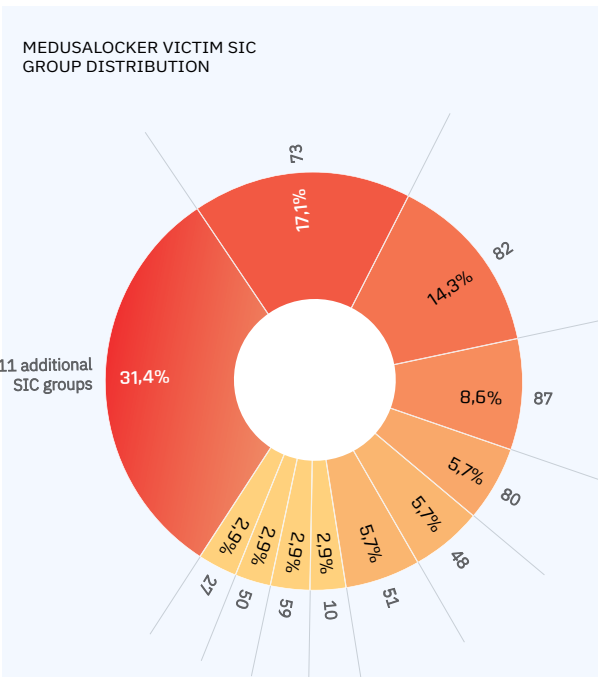
Summary

Lockbit is the most active ransomware group in the studied time period, and was also the most active group in the second half of 2022. Lockbit is a highly sophisticated RaaS group which first started operating in January 2020, releasing several new versions over time. Lockbit has abused multiple open-source and freeware tools, such as TeamViewer and FileZilla in order to attack hundreds of organizations worldwide

Main findings

Lockbit targets companies from numerous industries (in the studied time period attacks were observed against 60 SIC groups), with the main targets coming from the Business Services and Engineering, Accounting, Research, Management, And Related Services sectors. The group primarily attacks smaller companies, with a revenue range of \$1M-\$50M.

MedusaLocker



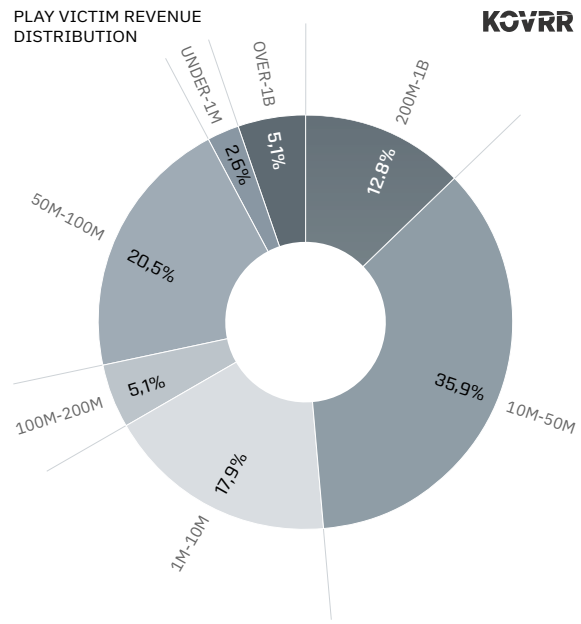
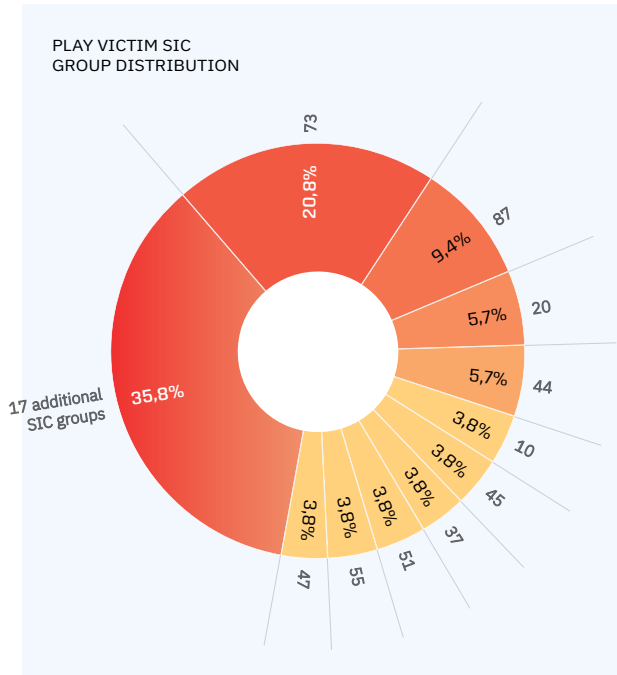
Summary

MedusaLocker is a ransomware group first observed in late 2019. Like most other prominent ransomware groups, the group operates using a RaaS model. To attack, the group relies predominantly on vulnerabilities in remote desktop protocol (RDP), to access victims' networks, in order to both encrypt and steal data.

Main findings

In the first half of 2023, MedusaLocker mainly targeted companies in the Business Services sector, followed by companies in the Educational Services sector. The group prefers to target smaller companies, with a revenue range of \$10M-\$50M.

Play



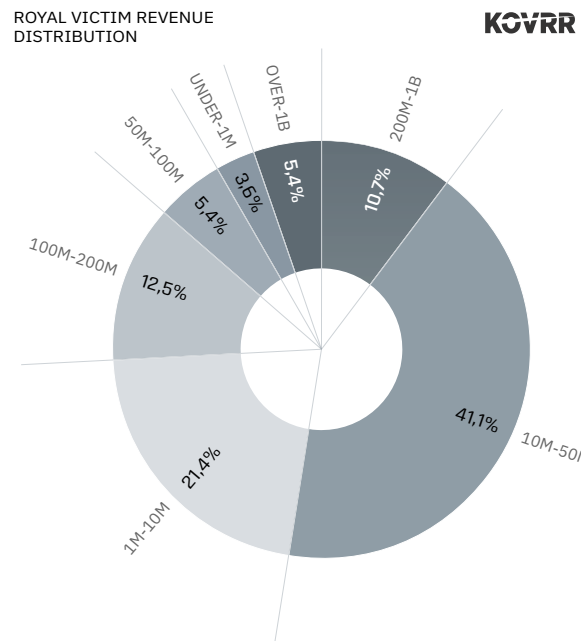
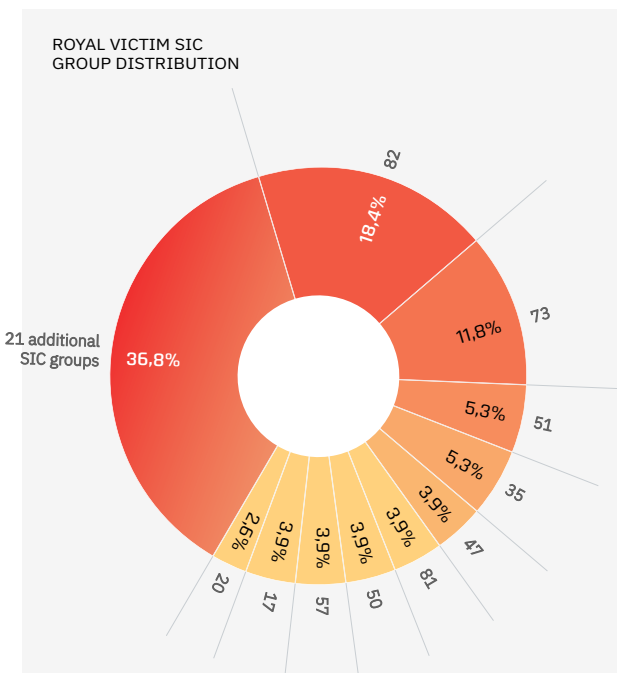
Summary

Play ransomware was first seen in June 2022. Since first appearing in the landscape, the group has targeted several dozen victims, with one of the most high-profile attacks targeting the cloud computing company Rackspace.

Main findings

The group mainly targets companies in the Business Services sector, followed by companies in the Engineering, Accounting, Research, Management, And Related Services sector. Play prefers targeting small companies, with a revenue range of \$10M-\$50M, however, it also often targets slightly larger companies, with a revenue range of \$50M-\$100M.

Royal



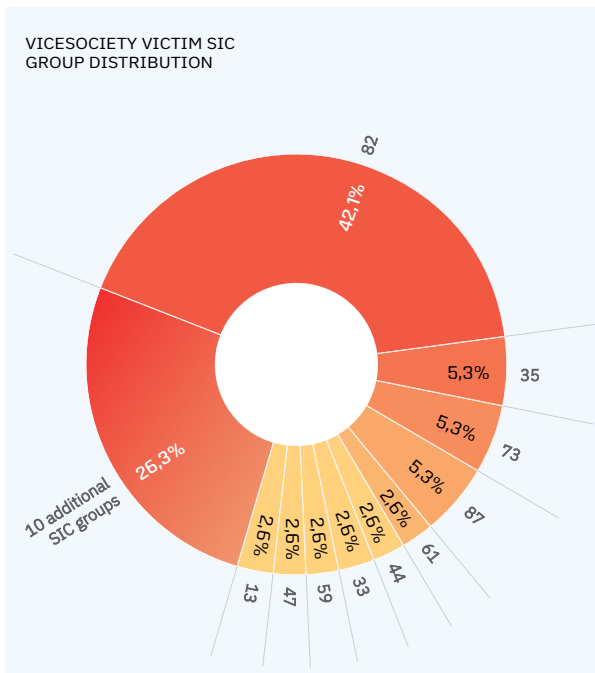
Summary

Royal ransomware first appeared around the third quarter of 2022. Royal gains access to victim networks mainly through phishing attempts, and following a successful attack, usually demands large ransoms, in excess of \$1M. One of the group's high profile targets was the City of Dallas.

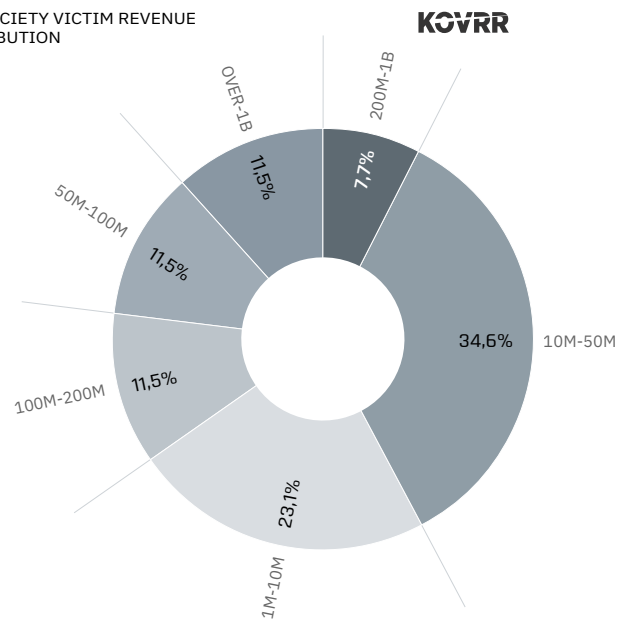
Main findings

Royal mainly targets companies from the Educational Services sector, followed by companies from the Business Services sector. The group attacks small companies, with a revenue range of \$1M-\$50M

ViceSociety



VICESOCIETY VICTIM REVENUE DISTRIBUTION



Summary

ViceSociety was first spotted attacking victims in the summer of 2021. Unlike other ransomware groups, ViceSociety has used several existing ransomware variants to perform the attack - so far using the HelloKitty and Zeppelin ransomware strains.

Main findings

The group primarily targets companies from the Educational Services sector, with most of the groups attack efforts focusing on that sector. In addition, the group usually targets small companies, with a revenue range of between \$1M-\$50M.



GUY PROPPER is the Head of Data at Kovrr and has extensive expertise in reverse engineering, malware research, and threat actor analysis. Prior to that, Guy was the head of the Threat Intelligence and Deep Learning Group at Deep Instinct, and participated as a speaker in Defcon 26. Guy has over ten years of cyber security experience, and holds a B.Sc. in Biology and Cognitive Science from the Hebrew University in Jerusalem.

KOVRR is a leading cyber risk quantification (CRQ) technology and solutions provider enabling global enterprises and (re)insurers to financially quantify cyber risk on demand.

Kovrr's technology enables decision makers to seamlessly drive actionable cyber risk management decisions. CISOs trust Kovrr's platform for planning their cybersecurity budgets, communicating risk to board of directors, prioritizing for new initiatives, buying cyber insurance, reporting to regulators and more.

Learn more about how Kovrr can help your revamp your cyber risk management program with its CRQ technology today by reaching out to contact@kovrr.com