KOVRR

Report

Ransomware In Transportation

A Deep Dive into Cybersecurity Threats and Trends

Ransomware attacks have become a significant cybersecurity issue, causing severe financial loss and reputational damage for those affected. The use of sophisticated techniques and various delivery channels, such as phishing emails and software vulnerabilities, have made these attacks more challenging to prevent. This report provides a short synopsis of data and statistics from Kovrr's cyber incident database spanning the previous three years.

Maritime

The maritime industry involves all activities related to sea transportation, including the operation, maintenance, and management of ships and other vessels. It encompasses both commercial and military maritime activities, such as cargo and passenger shipping, offshore oil and gas exploration, and naval operations. The maritime industry is critical to global trade, supporting the movement of goods and commodities around the world. The industry is also subject to international regulations, ensuring safety, security, and environmental protection. Advancements in technology and increasing concerns about sustainability are shaping the future of the maritime industry.

Main ransomware actors 2020-2022:

1. LockBit

LockBit is a ransomware gang that emerged in 2019. They use advanced techniques to encrypt files and demand large ransoms. LockBit has targeted various organizations globally and is known to steal sensitive data and threaten to release it if the ransom is not paid. The group is believed to operate from Russia and is linked to other cybercriminal organizations in the region.

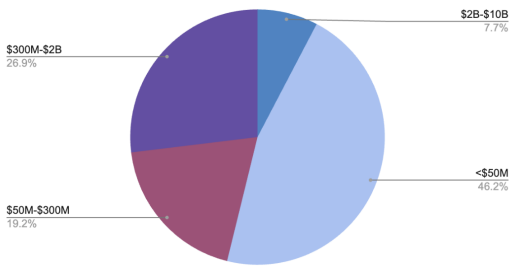
2. REvil (Sodinokibi)

Revil is a prominent ransomware group that has been active since 2019. They are infamous for their sophisticated attacks on high-profile organizations, including celebrities and large corporations. The group is known for their double-extortion tactics. Revil is believed to be a Russian-speaking group, and their ransom demands are usually in the seven-figure range. The group has also been linked to other cybercriminal organizations and is known for their use of zero-day exploits to bypass security measures.

3. Mespinoza (Pysa)

Mespinoza is a relatively new ransomware gang that appeared in 2020. They are known for their targeted attacks on high-profile organizations and their use of double-extortion tactics. Mespinoza's ransom demands are usually in the six-figure range, and they threaten to release sensitive data if the ransom is not paid. The group is believed to be based in Eastern Europe and has targeted industries such as healthcare and education.

Dist. of Company Revenue Range According to the Amount of Ransomware Attacks



© 2023 Kovrr. All rights reserved.

Aviation

The aviation industry encompasses all activities related to air transportation, including the design, manufacture, operation, and maintenance of aircrafts. It includes both commercial and military aviation, as well as the infrastructure and regulations that support air travel. The aviation industry has a significant impact on global commerce and tourism, facilitating the movement of people and goods around the world. The industry is highly regulated to ensure safety and security, and technological advancements continue to shape the future of air transportation.

Main ransomware actors 2020-2022:

1. LockBit

LockBit is a ransomware gang that emerged in 2019. They use advanced techniques to encrypt files and demand large ransoms. LockBit has targeted various organizations globally and is known to steal sensitive data and threaten to release it if the ransom is not paid. The group is believed to operate from Russia and is linked to other cybercriminal organizations in the region. They were also main actors in the Maritime industry.

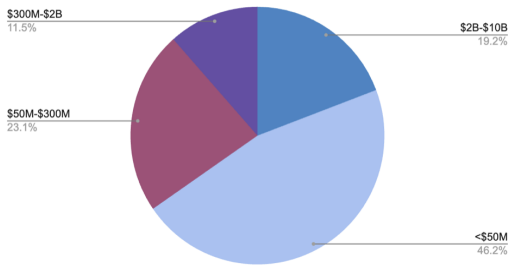
2. Avaddon

Avaddon is another relatively new ransomware gang that appeared in early 2020. They use advanced double-extortion tactics, targeting various industries and operating as a Ransomware-as-a-Service. Avaddon's ransom demands are usually high, and is believed to be based in Russia or Eastern Europe.

3. Maze

Maze is a notorious ransomware gang that has been active since 2019. They are known for their aggressive tactics, which include stealing sensitive data before encrypting it and threatening to release it publicly if the ransom is not paid. Maze has targeted a wide range of industries, including healthcare, government, and finance. Maze has been linked to other cybercriminal organizations and is believed to be based in Russia. It is believed that the group is no longer active, as of today.

Dist. of Company Revenue Range According to the Amount of Ransomware Attacks



© 2023 Kovrr. All rights reserved.

(Ground) Transportation

The ground transportation industry encompasses all activities related to land transportation, including the operation, maintenance, and management of vehicles and infrastructure. It includes various modes of transportation, such as cars, buses, trains, and trucks. The industry plays a crucial role in facilitating the movement of people and goods, supporting commerce, tourism, and daily life. The ground transportation industry is subject to various regulations and safety standards, and technological advancements are shaping the future of transportation, including the development of autonomous vehicles and alternative energy sources.

Main ransomware actors 2020-2022:

1. LockBit

LockBit is a ransomware gang that emerged in 2019. They use advanced techniques to encrypt files and demand large ransoms. LockBit has targeted various organizations globally and is known to steal sensitive data and threaten to release it if the ransom is not paid. The group is believed to operate from Russia and is linked to other cybercriminal organizations in the region. They were also main actors in the Maritime industry.

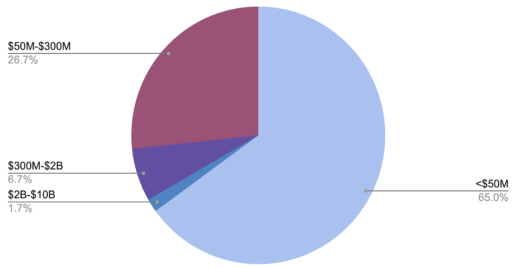
2. Conti

Conti is a ransomware gang that emerged in 2020. They use sophisticated techniques to steal data and demand large ransoms. Conti is linked to other cybercriminal organizations and operates out of Russia. They're known for their use of double-extortion tactics and have targeted various industries, constantly evolving their tactics to remain a major threat.

3. REvil (Sodinokibi)

Revil is a prominent ransomware group that has been active since 2019. They are infamous for their sophisticated attacks on high-profile organizations, including celebrities and large corporations. The group is known for their double-extortion tactics. Revil is believed to be a Russian-speaking group, and their ransom demands are usually in the seven-figure range. The group has also been linked to other cybercriminal organizations and is known for their use of zero-day exploits to bypass security measures.

Dist. of Company Revenue Range According to the Amount of Ransomware Attacks:



© 2023 Kovrr. All rights reserved.

Concluding thoughts

The three industries exhibit a similar pattern when it comes to attacks in terms of revenue range.This can be attributed to the insufficient security measures implemented by smaller businesses against ransomware attacks, resulting in a higher likelihood of paying the ransom. Furthermore, small enterprises are common across industries, which could explain their prevalence as the primary targets.

LockBit is considered to be one of the most prominent ransomware groups in the current cyber threat landscape. The group is known for their sophisticated attack methods and extensive network of affiliates, who help distribute their malware and carry out attacks on high-profile targets. Therefore, it is not surprising that we see it at the top of the list of attackers of all transportation industries.

Ransomware attacks pose a severe threat to the transportation industry, which relies heavily on data and technology to ensure safe and efficient operations. A successful attack can disrupt critical systems, such as traffic management and logistics, leading to significant disruptions in the supply chain and affecting the movement of goods and people. The transportation industry is also responsible for the safety of passengers, and a ransomware attack on critical systems could compromise the safety of the traveling public. Additionally, the transportation industry collects and stores sensitive data, such as personal information and trade secrets, making it an attractive target for cybercriminals seeking to profit from stolen data. Given the industry's importance and interconnectedness to other sectors, a ransomware attack on the transportation industry could have far-reaching consequences, affecting the economy and public safety.

Liri Shirav

Cyber Data Analyst & Engineer

© 2023 Kovrr. All rights reserved.