KOVRR
Cyber Risk Modeling

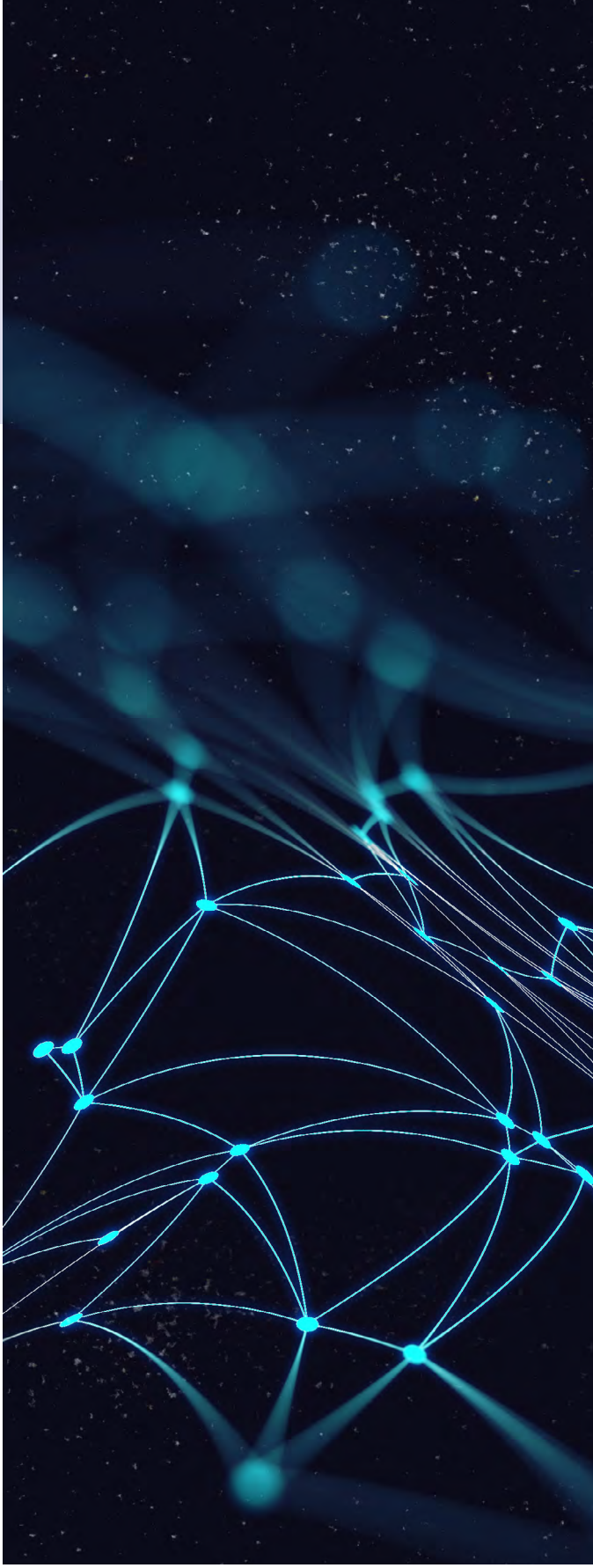
www.kovrr.com

Key Drivers of Rise of Ransomware in 2020

FEBRUARY 2021

KOVRR
Cyber Risk Modeling

Key Drivers of Rise of Ransomware in 2020: Ransomware-as-a-Service and Double Extortion



Ransomware has been a known method for cyber attacks for more than 30 years and has significantly evolved within this timespan.[1] The growth in the number of ransomware attacks in 2020 has marked a pivotal milestone in the ransomware evolution. According to a Check Point study, *Global Surges in Ransomware Attacks*,[2] in Q3 2020 the daily average of ransomware attacks has increased by 50%, and has specifically increased by 98.1% in the United States. Additionally, the average amount of money requested by attackers in Q3 2020 increased by 178% compared to Q4 of 2019.[3] Supporting this trend, Coalition's *Cyber Insurance Claims Report* stated that more than 40% of the cyber incident claims in Q1 and Q2 2020 were due to ransomware attacks.[4]

Taking into account these statistics, Kovrr has conducted research that included monitoring the activity of trending threats actors, the attacks they were involved with and the victims of these operations through 2020. The research included data from various proprietary and third party data sources including leaked data from the dark web. The research revealed that ransomware attacks have evolved in the following two areas:

1. Methodology - unlike ransomware attacks witnessed in the past, the last half year of 2020 was characterized by adoption of a new attack method which includes - stealing the company's data along with encrypting the attacked company's data. This practice is also known as "Double Extortion" because the attacker not only encrypts the data but also threatens to publish the company's stolen data.

2. Ransomware as - a - service (RaaS) - a method that recently became popular, which enables potential attackers to purchase already existing ransomware and use it for their desired purposes.

Kovrr has researched 16 active 'double extortion' ransomware attack campaigns in the last year. Of the campaigns studied, 75% use social engineering (phishing emails) to propagate, while 25% of them involve exploiting a vulnerability in remote access software.

1. https://www.welivesecurity.com/2015/09/18/evolution-ransomware-pc-cyborg-service-sale/
2. https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/
3. https://atlasvpn.com/blog/average-ransom-payout-jumped-178-in-a-year
4. https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf

In order to fully understand the effect of the ransomware campaigns, Kovrr applied the CRA-Zones framework to better analyze and report findings of the research. CRA-Zones are an easy to use open framework to measure and understand cyber risk exposure that focus on the minimal elements needed to describe cyber risk accumulation. Elements of the CRA-Zones include location, industry, and entity size. Applying the CRA-Zones framework to the ransomware campaign research found the top 5 CRA-Zones exposed were:

- **US_NY_I_S** [United States_New York_Services_Small Company]
- **GB_I_S** [Great Britain_Services_Small Company]
- **CA_I_S** [Canada_Services_Small Company]
- **CA_E_S** [Canada_Transportation & Communications_Small Company]
- **US_CA_I_S** [United States_California_Services_Small Company]

Most of the attacked companies are located in the U.S. (more than 50% of the targets), followed by Canada, the United Kingdom, Germany and France. Within the U.S., the main states affected were California, Texas, Florida and New York. The industries to which most of the attacked companies belong to are Services (20% of the services category is attributed to educational services), Transportation and Communication, and Manufacturing.

These findings have a significant impact on the cyber insurance market both in terms of rising claim numbers and entity of the amount claimed. The increase in attacks is more concentrated in particular combinations of location, industry, and entity size (CRA-Zones), meaning certain CRA-Zones are more susceptible to an attack than others. This paper addresses new ransomware trend characteristics by providing an overview of two major ransomware campaigns encountered in the research; provides examples of ways in which a portfolio can be influenced as a result of the wide adoption of these trends; and finally discusses ways insurance companies can reduce their ransomware losses.

State of the Threat Landscape

Research consisted of collecting data about the operation of 16 ransomware campaigns using the Double Extortion method, mostly for closed web sources, with the option to purchase RaaS. Two major-recent campaigns from this list are **Avaddon** and **Nefilim**. These campaigns were selected because they are new entrants in the "top 10" market share of ransomware campaigns[5] and each uses different attack methods.

Avaddon

The Avaddon ransomware campaign was first spotted in June 2020, and propagated through social engineering, spreading via phishing emails with a malicious attachment. After clicking and opening the attachment, malicious code is executed and the affected users see that their system desktop's wallpaper has been automatically changed to an image that states that all the files have been encrypted and refers to the ransom note. The ransomware also leaks the data to an external server and the attackers threaten to publish the attacked company's proprietary data to a dedicated leaked data site. Analysis shows that the majority of those most recently targeted by Avaddon, fall into the category of small - medium companies (SMBs) located in the United States. American Bank Systems (ABS), a provider of compliance services for banks and financial institutions, as well as EFCO, a construction company, both located in the U.S., are examples of companies attacked by Avaddon ransomware and both suffered from proprietary data leakage, including customers' information.

Nefilim

The Nefilim ransomware was first detected in March 2020 and distributed through Remote Desktop Protocol (RDP) by exploiting vulnerabilities. As mentioned, along with encrypting the attacked companies data, Nefilim also steals company data. The stolen data leakage begins weeks before the files are encrypted and the ransomware is requested. After the ransom payment is requested, the attackers threaten the attacked company to publish their stolen data, if they do not pay the ransom. Compared to Avaddon, the composition of the attacked companies' size is more diverse, although most of them are large companies, while nearly 50% of the attacked companies are in the manufacturing industry. Toll Group, a giant Australian transportation company, and Luxottica Group, an Italian eyewear conglomerate and the largest company in the global eyewear industry, are two examples of companies who fell victims to Nefilim ransomware. The attacks led to shutdowns on different levels and both companies' proprietary data was stolen and published by the attackers.

5. https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

The Impact on the Insurance Industry: Changes in the Portfolio Expected Risk

The combination of the two trends, RaaS and Double Extortion, has a significant influence on a given portfolio's expected loss. In the case of these two ransomware trends, the parameters that contribute to expected loss calculations, **the probability that a loss will occur** and **the cost of the loss**, have increased.

Effects on Frequency

In the past, attackers had to be capable of building their own ransomware. With the RaaS model, they have easy access for the tools needed to propagate an attack. This means attackers can be less sophisticated and the barrier to entry has become lower. As a result, the group of potential attackers has grown and accordingly, the number of attacked companies has grown as well. As the RaaS trend increases, the number of attacks continues to grow and therefore the probability that a company will be attacked in a given portfolio (the probability that a loss will occur) also increases.

Cost Components Impacted by Ransomware

Cyber events are unique and complex, and by nature can cause different types of losses which can be broken down by a diverse list of cost drivers. In order to estimate the financial damage an event can cause, **'cost components'** are used to map the types of losses derived from a cyber event. Kovrr's platform allows for customization of cost drivers by allowing users to configure cost components by the type of event and coverage. A "conventional" ransomware attack (which encrypts the attacked company's data without leaking it) leads to several cost components being triggered. In a scenario that the company has paid the ransom, cost components can include:

- **Extortion Payment** -depending on the jurisdiction, insurance carriers will reimburse the amount of money paid as a ransom.
- **Lost Income** - results of business interruption caused by the encryption process which prevented access to the attacked company's systems and data. Lost income may be higher due to a longer period of time in which system accessibility was limited.
- **Recovery Expenses** - refers to the cost of restoring data and getting the systems to full recovery after an attack or failure.
- **Forensics Expenses** - necessary expenses incurred by the attacked company to investigate the source of the security vulnerabilities that enabled the attack for the purpose of preventing a future security breach.

Therefore, until recently, attacked companies that had backups of their sensitive data, could dramatically reduce the damage caused by ransomware. Double Extortion changes the rules. In today's threat landscape, due to attackers performing a ransomware attack and stealing the company's sensitive data, attacked companies are worried that their data will be published, and therefore backing up the company's data is no longer a sufficient mitigation strategy. This change in the potential damage gives the attackers leverage while requesting the ransom payment and accordingly, gives the attacked companies an extra incentive to pay the ransom. Thus, as mentioned above, the average payment demanded by attackers increased and it can be assumed that the number of successful attacks will increase as well as the numbers of filed claims. Moreover, in cases in which the company doesn't pay or the attacker publishes the data despite the ransom being paid,[6] the ransomware attack becomes de facto, a data breach event, and therefore adds a significant number of cost components.

6. https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

Examples of these additional potential costs include:

- **Notifications Costs** - costs incurred through notifying customers, regulators and other required authorities of a data breach.
- **Monitoring** - monitoring services for identity theft or credit card fraud that has to be supplied to individuals whose data was stolen in a breach.
- **Regulatory Fines and Legal Expenses** - due to third party's claims whose private data was stolen.
- **Data Recovery and PR Repairment** - costs and expenses of a public relations firm or consultant, crisis management firm or law firm which an insured may engage with in order to prevent or limit adverse effects of any negative publicity which has arisen from any covered claim or inquiry.

What can insurance companies do to reduce their ransomware losses?

From the outset, it is important to consider how the evolution of ransomware and trends can cause different types of losses. Generally, ransomware has mostly affected attritional losses. This could lead to a significant deterioration of loss ratios and should be taken into consideration by insurers when deciding their pricing and reserving strategies. One solution offered by Kovrr is to quantify the impact based on CRA-Zones in order for portfolio managers and underwriting managers to quickly identify those most at risk.

Additionally, the impact on large losses needs to be taken into consideration as well. The increase in frequency and severity of losses has the potential to impact capital. At the very least it will make it more likely for aggregate limits in reinsurance programs to be used up, or aggregate attachment points to be triggered. Reinsurers need to be aware of accumulations by CRA-Zone in each of their ceded portfolios, and might need to adjust their loss expectations accordingly, especially while taking into account crippling effects of rising costs, due to double extortion ransomware.

In regard to catastrophe events, these new trends will not make a self-replicating attack more likely, however, the implications of the "double extortion" trend need to be considered. Thus far the industry has looked at "scenarios" independently. Many insurance companies have a good grasp of their potential catastrophic losses from ransomware attacks and their potential catastrophic losses from data leakage. Insurers now need to make efforts to estimate the severity of an attack with both traits and potentially consider additional scenarios that include multiple impacts which are currently modeled separately.

KOVRR
Cyber Risk Modeling

Steps that can be taken to mitigate the effects of ransomware on a portfolio

Dealing with the increase of ransomware claims and changes in the threats requires a set of decisive actions:

Identify

The starting point of any analysis should be the identification of the problem within the portfolio. This can be done following a simple pattern of aggregations by CRA-Zone. The scale of the problem will be directly proportional to the amount of policies and exposed limit that can be linked to the most vulnerable CRA-Zones as identified above. Carriers might also want to look at zones with similar traits to the ones the research has highlighted. Depending on the composition of each portfolio, "second tier" CRA-zones might provide a better metric to identify the scale of the problem. The key is gaining as much insight as possible into the hazard - the reliance of insured companies on technologies that are most vulnerable. Research from Kovrr provides evidence that companies within the same CRA-Zone tend to rely on similar technologies, and thus are subject to similar levels of risk.

Quantify

In order to define an impact on loss ratios or capital, carriers need to understand how these patterns affect frequency and severity of losses. Research shows a material increase in both frequency and severity affecting certain CRA-Zones more than others. Sections of the portfolio concentrated in these CRA-Zones are most at risk and should be identified as materially impacted. In adjusting their assumptions for pricing and reserving, insurance companies need to keep in mind three main contributing factors:

- The increase in frequency is driven by new entrants in the threat landscape, it is therefore a direct addition to assumptions made within an existing framework.
- Ransom requests are getting higher, therefore the severity of ransomware scenarios is directly increasing within an existing framework.
- The increase in severity is also due to a double extortion effect. Existing frameworks will have allowances for ransomware and data leakage, but might not account for a combination of the two. Some adjustments will need to be made to accommodate this overlap, to avoid double-counting and therefore taking over-conservative positions.

Manage

The CRA-zone framework allows exposure managers and insurance professionals to keep the risk constantly under review. Companies within the same CRA-zone tend to use similar technologies and services, and are therefore subject to similar levels of risk. Monitoring aggregations by CRA-zone enables the development of risk metrics and assumptions that are easily updated as the risk develops, leading to a more dynamic response to changes in the threat landscape.

If you're interested in understanding your company's portfolio to double extortion ransomware or ransomware-as-a-service, feel free to reach out to Kovrr to start an analysis.

The Authors

Marco Lo Giudice, PhD

Head of Pricing Models Development

Or Amir

Product and Customer Growth Manager

Yonatan Livni

Business Analyst Consultant

Contributors

Geniya Brass Gershovich, Shalom Bublil and Naomi Weisz also contributed to this report.

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers transparent, real-time data- driven insights into their affirmative and non-affirmative cyber risk exposures. The Kovrr platform is designed to help underwriters, exposure managers and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.

To learn more please contact the Kovrr team: contact@kovrr.com