01 // 10 // 2022

TLP:WHITE

2021 RANSOMWARE BULLETIN: RECENT PAST AND NEAR FUTURE OF CYBER EXTORSIONS

www.cluster25.io

@cluster25_io

DuskRise

CONTENTS

EXECUTIVE SUMMARY

C25 analyzed the major trends of ransomware threat in 2021, reporting statistics, evolutions and forecasts for 2022.

01 INTRODUCTION

The year 2021 saw the ransomware threat on the rise and a succession of related events that also involved issues relating to the national security of large countries. To date, it is not possible to talk about ransomware without mentioning the **Colonial Pipeline** case. For a few days in May 2021, a ransomware attack conducted against this company raised awareness on how an attack that is conducted in the digital world can also have serious effects on the physical one, impacting millions of people. This could be a direct consequence of a significant increase in the sophistication and procedures adopted by many threat actors who are active in this area, which have recently been posing serious threats to the economy, security, and even the privacy of citizens of many Countries. In May 2021, for example, information about 520 patients at **Health Service Executive** (a publicly funded healthcare system in the **Republic of Ireland**) has been published after a ransomware attack carried out by the threat group known as "Conti".

02 MAJOR RANSOMWARE TRENDS IN 2021

The increase in the number of ransomware incidents in 2021 is partly to be attributed to the growth of a business model in the criminal underground called **R-a-a-S** (Ransomware-as-a-Service). In this model, in a very simplistic way, those who develop the ransomware rent their product to other criminals. The advantage for the latter is to be able to exclusively concentrate on the operations while others (the developers) take care of the maintenance and development of the malware components. This model also allowed those who did not have specific technical knowledge to be able to use very effective pieces of malware during attacks. The direct consequence has been that the number of potential threats and the degree of danger individually associated with them have grown exponentially. In addition to the **R-a-a-S** models, as already stated in rapid growth, other trends associated with this type of threat have emerged in the course of 2021. These latter have contributed to the significant raise in the perceived risk of ransomware cartels and have made headlines for gaining a foothold in attacks against major targets. Basically speaking, the attackers understood that adopting certain practices could not only allow them to have greater chances in

attempts to compromise a single target, but that they could be able to impact multiple one with a single operation. Another growing trend in 2021, indeed, is the so-called **Supply Chain Attack**. A clear example of this type of event is certainly the attack against the service provider **Kaseya**, in which approximately **1,500** of its customers were affected in a supply-chain attack perpetrated by **ReVil** gang. In this incident a top-tier Russian-speaking ransomware cartel used two flaws in software from Florida-based **Kaseya** to compromise about 50 MSP (Managed Services Providers) that were using its products. MSPs represents an efficient vehicle for malicious code because they have access to many of their customers' networks. Finally, the practices of **Double Extortion** have substantially spread and have been steadily adopted by various criminal groups and, with good reason, must be included in the major trends of 2021 regarding the world of ransomware. However, in addition to what has gone into the news, the past year has also seen many attacks targeting small and medium-sized enterprises, which explain their percentage of the total ransomware victims being the highest. *Figure 1* shows a graph relating to the percentages of attacks compared to the size of companies affected by ransomware in 2021:

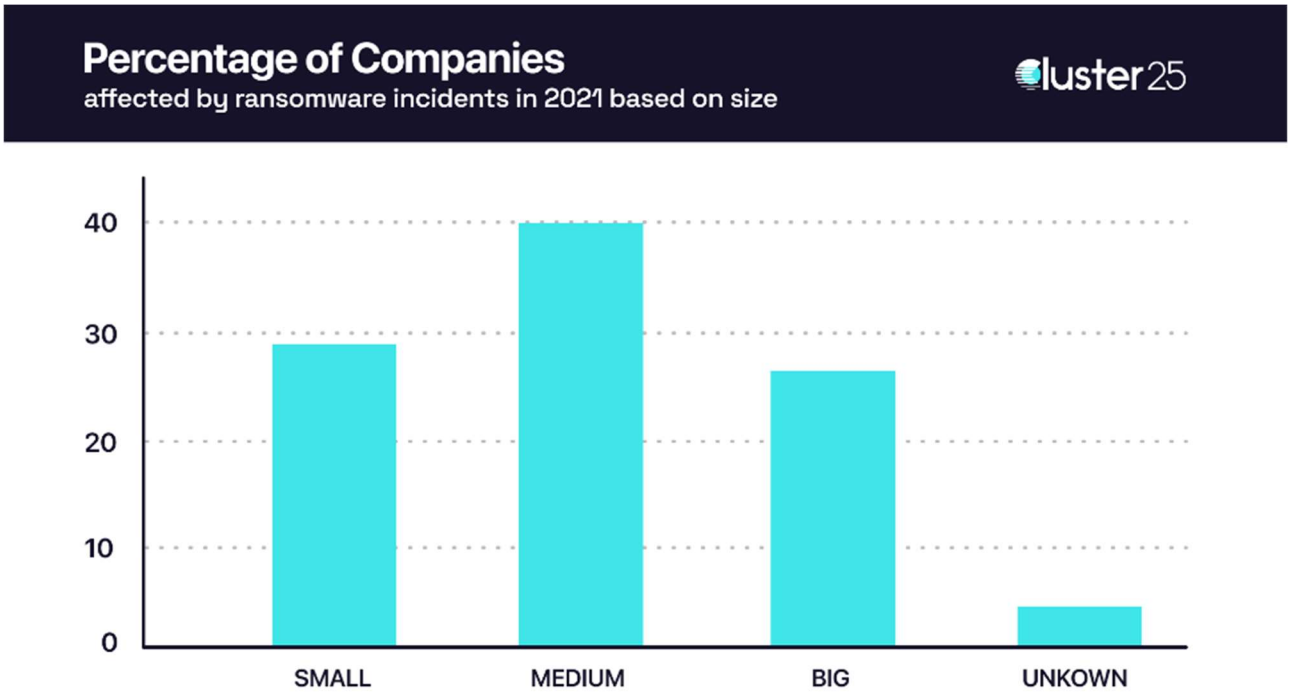

Figure 1 – Percentage of ransomware incidents by company size

03 DISTRIBUTION AND CHOICE OF VICTIMS

In regards to the choice of victims, it was possible to observe an increase in the execution of more targeted and specific operations compared to the recent past. Like many legal businesses, ransomware cartels are driven by economic profit; for the purpose of increase this latter as much as possible, many cartels are willing to spend a lot of time and knowledge in compromising a single target (even if well defended and controlled) if there are the conditions for very high ransom requests and high probability that these will be paid. In this case, critical infrastructures are the targets that we could consider most profitable, as they are tendentially intolerant to accepting the block of their activities and often, also supported by governments, can count on good financial resources. A clear and major example of a critical infrastructure ransomware attack in 2021 was certainly the one carried out against **Colonial Pipeline**. This company operates one of the largest refined product pipelines in the United States and, in May 2021, was the victim of an incident attributed to **Darkside** by security experts, a Russian-based cybercriminal group that provides a **R-a-a-S**. The attack hit the company hard, hindering its normal operations and resulting in record price hikes and gasoline shortages. The **Covid-19** pandemic has also substantially raised the criticality levels of some sectors, such as healthcare and medical research, on which many threat actors have seen the opportunity to ask for rather high ransoms. On June 14, 2021, **Humber River Hospital** in Ontario had to shut down its systems to prevent and mitigate a ransomware attack. As a direct consequence, staff no longer had access to electronic patient records and diagnostic test results, resulting in longer wait times in the emergency department. In addition, the hospital had to cancel various services and redirect ambulances to other hospitals. In Italy, on September 12, a ransomware attack against the **San Giovanni Addolorata** hospital - one of the largest in Rome - caused difficulties in carrying out normal service activities. In addition to damage to activities and services, attacks on healthcare infrastructures also give cybercriminals the advantage of acquiring patient health data. The threat of publishing personal data of patients often represents a strong lever for criminals to push, for the aim of increasing the likeliness of having the ransom paid. Even in the face of the ransom payment, however, the victims have no guarantee that such data will later be shared with third parties following auctions or private negotiations. Keeping in mind that

ransomware can affect anyone, from the individual to large companies, in 2021 there were some verticals that were more affected than others. The **Healthcare** sector was one of these together with the **Government** and **Education** ones. Leveraging on the pandemic, attackers took advantage of industries that have been hit the hardest, such as healthcare industries, municipalities, and educational facilities. As previously stated, criminals also saw the pandemic as an opportunity to take advantage of employees that are now working remotely on their personal devices, which often contributes to increasing the potential attack surface. Other sectors that were heavily impacted by cartels' criminal activities are those of **Services**, **Finance**, **Research**, **Technology** and **Industrial**. As far as the distribution of the threat is concerned, it can practically include any geographic region and potentially every business sector could be the victim of extortion attacks. Most victims of ransomware cartels for the year 2021 are located in the USA (40%), followed by the EMEA (32%) and Asia regions (15%) as reported in *Figure 2*:

Figure 2 - Spread of the ransomware threat on a worldwide basis

In regards to the activities of the individual criminal groups, *Figure 3* shows a cross-section of the most active in the last year based on the number of victims, with **Conti** and **LockBit 2.0** being almost equal:

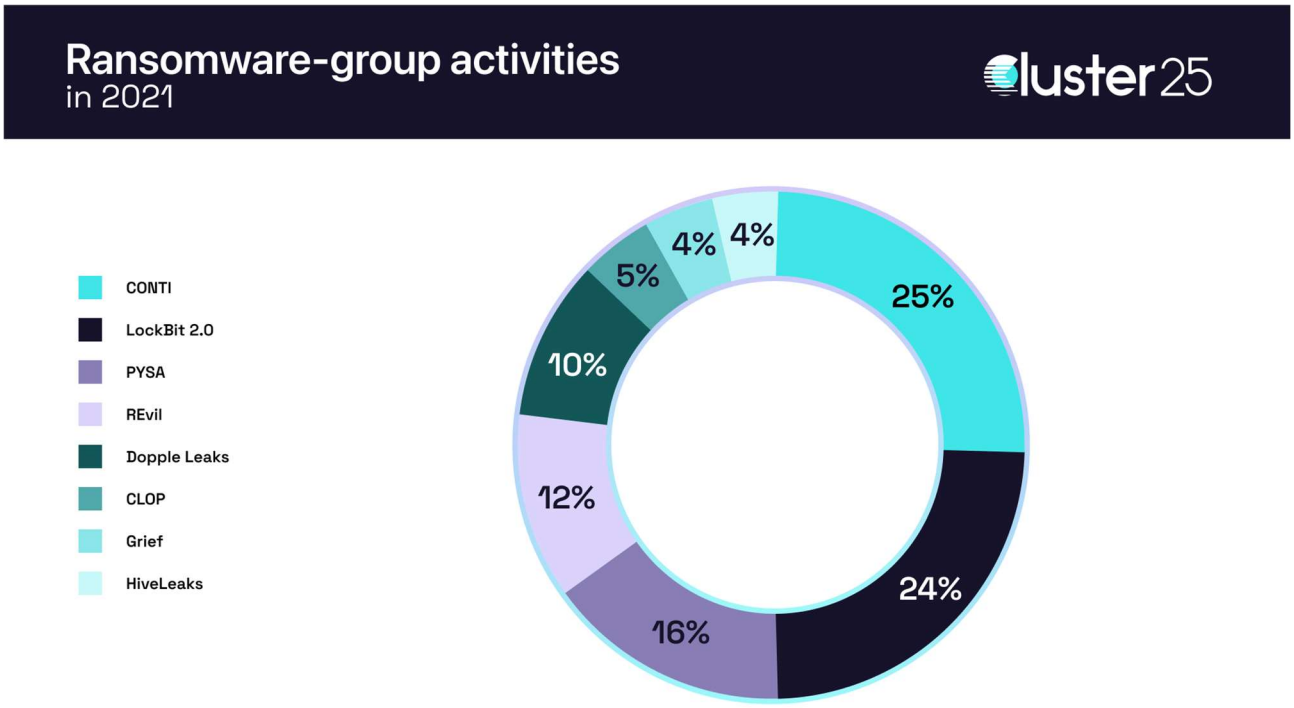

Figure 3 – Most active ransomware gangs in 2021

04 PAYMENTS

Payments of ransoms are requested in crypto currencies; essentially, this happens because the latter are difficult to trace. To date, **BitCoin** continues to be the most requested currency in ransom payments with a trend in 2021 seeing an increase in the average requested ransoms. However, it is likely that this cryptocurrency is destined to be replaced with more anonymous alternatives such as, for example, **Monero**. Anonymous cryptocurrencies allow a greater degree of stealth and

anonymity and are less subject to those tracking technologies that law enforcement agencies use to track money transactions by exploiting the "*open-to-read*" nature of the BitCoin blockchain. To mitigate this problem, cartels often use exchangers that do not comply with control standards, crypto currencies mixers and techniques for obfuscating transactions. For example, **LockBit,** one of the top-tier ransomware gang, has been observed to use **CoinJoin** to make money flow tracking activities more difficult. CoinJoin is an untrustful method for combining multiple BitCoin payments from multiple spenders into a single transaction, to make it difficult for external parties to determine which spender paid which recipient or recipients; gangs use BitCoin mixers as well, like **Blender dot io**. BitCoin can also be converted into other cryptocurrencies such as **Monero** and **ZCash** at a later stage. Despite these strategies, the tracking of cryptocurrency movements remains a particularly useful practice to extend the degree of visibility in the operations of criminal cartels. This practice can often lead to evidence suggesting unexpected relationships such as that of an affiliate operating simultaneously for two cartels. As shown in *Figure 3*, a single BTC address of an affiliate receives money from different wallets associated with two different ransomware groups, **Conti** and **DarkSide,** in the first quarter of 2021, suggesting that it was working for both criminal cartels at the same time:

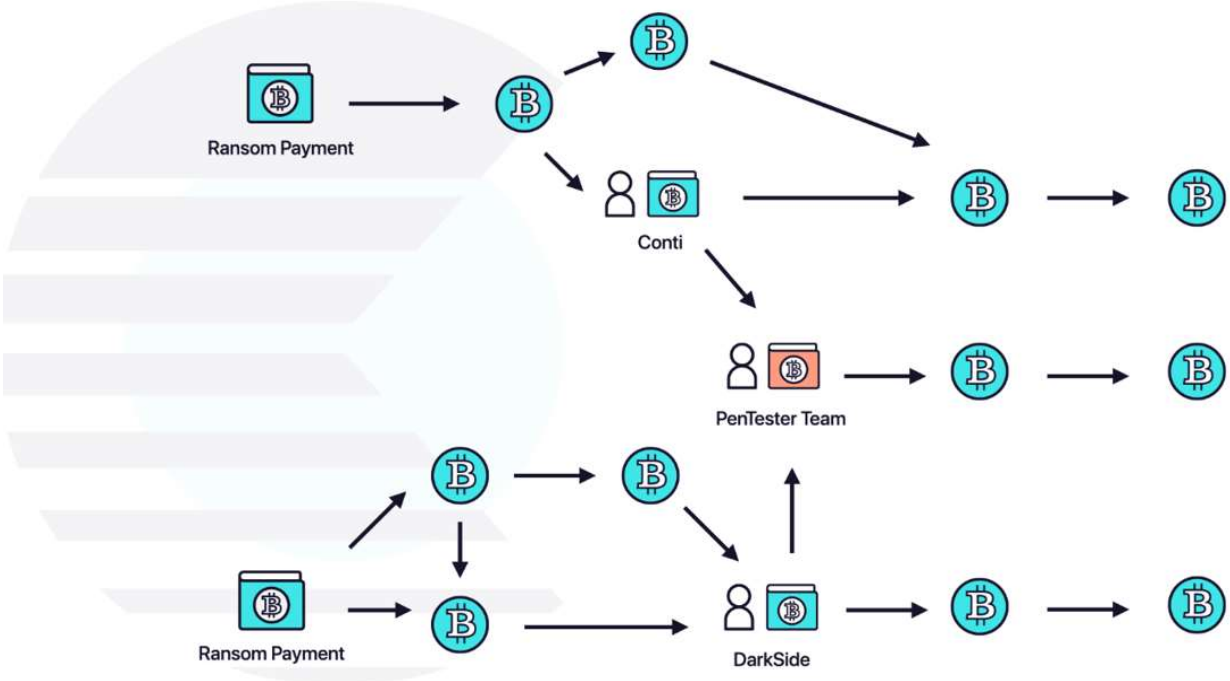

Figure 3 - Relationships between BitCoin payment addresses

05 GOVERNMENT, APT AND ECRIME

In the past, it was possible to observe operations carried out by *state-sponsored* groups who intentionally disguised their real intentions by simulating the operations of ransomware gangs motivated by financial gain. Already in 2020 **Iran's Islamic Revolutionary Guard Corps** (IRGC) carried out a campaign of ransomware attacks through an Iranian outsourcing company, mimicking the TTPs (Tactics, Techniques and Procedures) of a financially motivated ransomware gang in order to avoid the campaign being attributed to an institution of the State and to maintain a "plausible denial" for its actions. In regards to this, it is easy to predict that the hypothesis of mimicking the actions of ransomware groups will be taken into consideration and adopted by other state-sponsored groups as well. Coming to the potential interactions between government institutions and criminal groups, the **United States Department of the Treasury** has recently declared that the **Federal Security Service** (FSB) of Russia supports and mobilizes cybercriminals, including **EvilCorp** (aka **GoldDrake**), allowing them to launch ransomware attacks and phishing campaigns. Such statements suggest an interaction between the Russian intelligence services and, at least, part of the criminal landscape that pertains to the world of ransomware which could explain, at least in part, why some of the major ransomware groups are Russian-based and why they are prevented, both via technicalities and formal rules of adherence to the cartels, from attacking targets of **Commonwealth of Independent States** (CIS) countries. Following the US-Russia summit in June 2021, criminal groups **DarkSide** and **REvil** (which were responsible for a series of ransomware attacks against **Colonial Pipeline**, **JBS USA** and **Kaseya**) have taken down their infrastructure and services and formally ceased their activities. By September 2021, however, the **BlackMatter** group resurfaced as successor to several groups including **DarkSide** and **REvil** had resurfaced and resumed their malicious activities. However, **REvil** was dismantled in October 2021 when its infrastructure was compromised as part of an operation carried out by the United States.

05 CONCLUSIONS

C25 asserts with a good degree of confidence that, in the near future, the scale and the sophistication of attacks will grow further as they are still particularly lucrative for criminal gangs. Ransomware operators will continue to pose a serious threat to the national security and the economy of many Countries. It is also probably possible to expect further increases in the average of ransom requests, which already highly increased in 2021 especially by the top-tier groups that will continue to target particularly lucrative sectors. As a matter of fact, these groups will probably be very interested in carrying out operations against targets included in the jurisdictions of the United States, United Kingdom or the EU, which are part of one of the critical sectors and have revenues of at least 5M USD. However, it is also foreseeable that there will be groups that will continue to focus on small and medium-sized companies that are known to invest less in cyber-security and which will therefore require less effort and skills to be compromised. Considering the nature of **R-a-a-S** and the difficulty in prosecuting ransomware operators, it is highly possible that this business model will continue to grow in 2022. Further evolutions of extortion methods for the current year could involve however a new business model in which companies, through a subscription, pay in order to avoid becoming potential targets of ransomware campaigns. Finally, cyber-criminals will almost certainly continue to use crypto-currencies to facilitate their operations. For this reason, with a view to greater international collaboration between countries, increasing the levels of pressure and supervision on exchangers that do not report suspicious transactions could effectively support the fight against ransomware phenomenon.

ABOUT CLUSTER25

Cluster25 is the internal Cyber Intelligence Research and Adversary Hunting Unit at DuskRise Inc. Cluster25 experts are specialized in hunting and collecting cyber threats, analysis, reverse-engineering and adversary hunting practices. Cluster25 independently designs and develops technologies aimed at the classification and categorization of malicious artifacts as well as for their correlation with known threat groups. Relying on extensive visibility into the digital threat landscape, it overcomes the usual limitations of services based on *ex-post* threat observation by providing real predictive and proactive intelligence services.

Visit us at **cluster25.io**

Contact us at **threatintel@cluster25.io**