I. Introduction

According to different reports the year 2023 is considered the most successful year for ransomware groups in history, with a total of 4,368 victims, marking a rise of over 55.5% since the previous year. Q2 and Q3 alone claimed more victims than the entirety of 2022, with 2,903 victims. In Q2 2023, there was a significant increase of 67% in ransomware cases compared to the previous quarter, with ransomware groups compromising 1,386 victims worldwide.

Below, we will analyze in detail the public materials on ransomware for the third quarter of 2023, delving into various aspects of the current situation, changing trends in attacks, industries and the geography of the phenomenon. The materials make it possible not only to assess the quantitative factors of incidents, but also to provide a qualitative synthesis of these tactics used by attackers and the consequences for cybersecurity strategies in the future. The purpose of the analysis is to provide readers with useful information and a deeper understanding of the phenomenon of ransomware in its current form and its trajectory in the field of cybersecurity

II. 2023 Ransomware Overview

- **Ransomware Attacks Increase**: The number of known attacks, where the victim did not pay a ransom, was 457 in November alone; the total number of attacks recorded was 1,900, and the undisclosed attacks were a massive 1,815 in the first six months of the year. The number of ransomware-related posts was 4,082, with an average of 371.1 posts per month.
- **Ransomware Attacks on Healthcare Sector**: with a 278% increase in ransomware attacks on the health sector over the past four years. The large breaches reported in 2023 affected over 88 million individuals, a 60% increase from the previous year.
- **Ransomware Gangs**: Several ransomware gangs were shut down in 2023, including Hive, RansomedVC, and ALPHV. However, new and evolving players such as Hunters International, Dragon Force, and WereWolves emerged.
- **Ransomware Payment**: The average enterprise ransom payment exceeded $100,000, with a $5.3 million average demand. However, 80% of organizations have a "Do-Not-Pay" policy on ransomware, and only 41% of organizations attacked last year paid the ransom.
- **Ransomware Insurance**: 77% of organizations found out that ransomware is specifically excluded from their security insurance. Insurance companies are catching on, with 74% seeing their premiums increase, 43% seeing increased deductibles, and 10% seeing their coverage benefits reduced.
- **Ransomware Targets**: manufacturing sector emerged as a prime target for 48 distinct ransomware groups In United States.
- **High-Profile Attacks**: High-profile attacks were carried out on Toyota, Boeing, and more using a Citrix Bleed vulnerability (CVE-2023-4966).
- **Ransomware as a Service (RaaS)**: The proliferation of RaaS was a notable trend in 2023, simplifying the execution of ransomware attacks for cybercriminals.
- **Prominent Ransomware Groups**: Groups such as CL0P played a major role in the spike of ransomware activity in 2023, with CL0P exploiting the file transfer software and impacting over 130 victims.
- **Ransomware Success**: The year 2023 is noted as the most successful year for ransomware groups historically, with a total of 4,368 victims, which is a 55.5% increase from the previous year. The second and third quarters of 2023 alone surpassed the total number of victims in 2022, with 2,903 victims.
- **Q2 2023 Ransomware Surge**: There was a 67% increase in ransomware cases in Q2 2023 compared to the previous quarter, with 1,386 victims globally. Leading ransomware groups during this period were LockBit3.0, ALPHV, and Cl0p.
- **MOVEit Campaign**: The MOVEit campaign was singled out as the most successful of the year, underscoring the significance of supply chain attacks and the need for robust version control and attack surface understanding. The United States was the primary target, with approximately 64% of the cases.
- **Record-Breaking Q3 2023**: Q3 2023 was the most successful quarter ever for ransomware, with the industry heavily impacted by the exploitation of critical vulnerabilities. The rise of new ransomware groups and families contributed to this growth.
- **Continued Growth Despite Law Enforcement**: Despite global law enforcement efforts to combat ransomware, the industry is expanding rapidly.

III. Highlight on MOVEit Campaign

MOVEit Campaign refers to a significant cybersecurity incident that occurred in 2023, involving the exploitation of a zero-day vulnerability in the MOVEit file transfer software developed by Progress Software. The campaign was orchestrated by the Clop ransomware group, which used the vulnerability to steal data from numerous organizations across various sectors, including government, finance, and healthcare.

Here are the key points:

- **The Vulnerability and Exploitation**: The vulnerability, tracked as CVE-2023-34362, affected both on-premises and cloud-based versions of MOVEit. It was first disclosed by Progress on May 31, 2023, and a patch was issued shortly after. The vulnerability was related to SQL injection, a common entry point into applications that enables data manipulation or database access.
- **The Perpetrators**: The Clop ransomware group was responsible for the attacks and they were also linked to the GoAnywhere and PaperCut incidents earlier in the same year.
- **The Impact**: The campaign had a significant impact, affecting over 1,062 organizations and approximately 65,435,641 individuals by the end of August 2023. The victims spanned a range of industries and included both private entities and public sector organizations.
- **The Response**: Progress Software responded promptly to the discovery of the vulnerability, issuing a patch and advising customers to apply it immediately. However, the victim count continued to grow months later, suggesting that many organizations were likely breached in the first few days and weeks of the campaign.
- **The Aftermath**: The MOVEit campaign highlighted the importance of proactive cybersecurity and vulnerability management. It also underscored the potential damage that can be caused by supply chain cyber-attacks, as many organizations were compromised not because they used MOVEit directly, but because they employed third-party contractors or subcontractors who did.

IV. Geographical Impact

Key points related to geographical impact:

- **Global Spread of Ransomware**: Cybercriminals expanded their geographical reach in 2023, taking proven malware tools to new countries and regions.
- **Countries Most Affected**: The United States was the most affected country, with the highest number of breached accounts. Other countries significantly impacted by ransomware attacks included the United Kingdom and Canada, Mozambique, Angola, and Ghana.
- **Ransomware by Industry**: Ransomware attacks affected some verticals more than others. The top targets by industry included education, construction and property, central and federal government, media, entertainment and leisure, and local and state government.
- **Ransomware Trends**: New ransomware groups like Rhysida, BianLian, IceFire, Sparta, and Bl00dy emerged, underscoring the evolving nature of the industry.

V. Q3 2023: A Record Quarter

Here are the key findings into the surge in ransomware activity during the third quarter of 2023:

- **Record-Breaking Ransomware Activity**: The third quarter of 2023 witnessed a significant surge in ransomware activity, with global ransomware attack frequency up by 11% over Q2 and 95% year-over-year (YoY).
- **Ransomware Victims**: The number of ransomware victims in 2023 has already surpassed what was observed for 2021 and 2022.
- **Emerging Ransomware Groups**: New ransomware groups such as MalasLocker, 8base, and Nokoyawa gained attention in Q3 2023. In their first quarter of operations, these groups collectively claimed a total of 305 victims.
- **Ransomware by Industry**: Ransomware attacks affected some sectors more than others. The sectors hardest hit by the record-breaking spike in ransomware attack frequency included law practices, government agencies, manufacturing, oil and gas, transportation, logistics, and storage sectors.
- **Future Trends**: Based on the activity at the end of Q3 and early Q4, it is expected that the numbers will surpass anything witnessed in previous years

VI. Outlook for 2024

The trends for Q3 2023 suggest that ransomware will remain a significant threat in 2024, and organizations will need to adapt and strengthen their cybersecurity measures to protect against these evolving risks:

- **Continued Growth of Ransomware**: the ransomware industry will reach new heights in 2024, continuing to deliver a high number of victims as promising newcomers establish their presence
- **Supply Chain Attacks**: Ransomware groups are expected to take advantage of and compromise supply chain infrastructures while still sticking to traditional methods such as exploiting old leaked credentials and using social engineering techniques
- **Ransomware Trends**: The ransomware industry is expected to evolve with new groups and tactics emerging.
- **Law Enforcement and Industry Efforts**: Efforts by law enforcement and the cybersecurity industry to

combat ransomware will likely continue, with a focus on shutting down major cybercrime groups and preventing attacks

- **Ransomware Insurance**: As ransomware attacks increase, the role of insurance in cybersecurity will become more critical, with organizations needing to navigate the complexities of coverage for ransomware incidents
- **Technological Developments**: The cybersecurity landscape will continue to evolve, with a shift towards more comprehensive defense strategies that include prevention, detection, remediation, and forensics
- **Global Impact**: The geographical impact of ransomware is expected to remain significant, with cybercriminals continuing to target a wide range of countries and industries
- **Ransomware Variants**: The emergence of new ransomware strains and the continued activity of existing ones will likely persist, posing ongoing challenges for cybersecurity defenses

VII. Conclusion

Conclusion underscore the importance of robust cybersecurity measures and the need for continuous vigilance and adaptation in the face of evolving ransomware threats:

- **Ransomware Attacks in 2023**: The year 2023 was a record-breaking year for the ransomware industry, with a significant increase in the number of attacks. The most targeted sector was the business services sector, followed by the retail and manufacturing sectors
- **Ransomware Industry Growth**: Despite the efforts of law enforcement, the ransomware industry continued to grow rapidly. New groups emerged, and existing groups like LockBit3.0, ALPHV, and Cl0p caused severe damage to organizations worldwide
- **Law Enforcement Efforts**: Law enforcement authorities worldwide have been working to stop the growth of the ransomware industry. They had some success in shutting down several major cybercrime groups, such as HIVE
- **Outlook for 2024**: the ransomware industry will continue to grow in 2024, with new and existing groups posing significant threats to organizations worldwide