Read more: Boosty | TG

Abstract – The analysis of the ransomware trends for the 4th quarter of 2023 aims to understand the multifaceted threat landscape associated with ransomware.

Delving into the specifics, we intend to reveal the nuances of ransomware operations, including the identification of the dominant groups of ransomware, their target sectors and the geographical distribution of attacks.

Furthermore, the analysis will highlight significant trends, such as the surge in ransomware incidents, the evolution of extortion tactics, and the implications of these developments on cybersecurity strategies.

This knowledge will be useful for both technical and strategic security professionals, offering information that can guide the development of reliable protection mechanisms, inform risk management decisions and, ultimately, increase the resilience of organizations to the ever-present threat of ransomware.

The significance of this analysis extends beyond mere academic interest; it equips security practitioners with actionable intelligence, enabling them to anticipate and counteract the sophisticated strategies employed by ransomware operators.

I. Introduction

In Q4 2023, the most common types of ransomware attacks were primarily carried out by three groups: LockBit 3.0, Clop Ransomware, and ALPHV/BlackCat ransomware.

LockBit 3.0 remained the most active ransomware group, claiming an average of around 23 victims per week. Other prominent groups included Clop Ransomware and ALPHV/BlackCat ransomware. Notable incidents included LockBit's attack on Royal Mail and the shutdown of Hive Ransomware.

The Quarterly Threat Report by Air IT highlighted that ransomware attacks, phishing, and insider threats continued to pose significant risks, with a surge in data volume and global connectivity widening vulnerabilities. The report from ISACA's State of Cyber Security for 2023 indicated that 48% of organizations experienced a rise in cyber attacks in Q4 2023.

TechTarget's report on ransomware trends heading into 2024 suggested that supply chain attacks and the exploitation of cloud and VPN infrastructure would continue to be key trends. The report also mentioned that since 2020, more than 130 different ransomware strains have been detected, with the GandCrab family being the most prevalent.

The environmental services industry faced an unprecedented surge in DDoS attacks, with a 61,839% increase in attack traffic year-over-year, as reported by Cloudflare. This surge was associated with the COP 28 event and highlighted the growing intersection between environmental issues and cyber threats.

Trend Micro's report on ransomware in the first half of 2023 showed that LockBit, BlackCat, and Clop were the top RaaS groups, with a significant increase in the number of victim organizations compared to the last half of 2022.

Check Point Research described 2023 as the year of mega ransomware attacks, with a shift in tactics from encryption to leveraging stolen data for extortion. The education/research sector was the most impacted by ransomware attacks in 2023.

II. Affected Industries

In Q4 2023, the industries most affected by ransomware attacks were the business services sector, education/research sector, and the retail/wholesale sector.

The business services sector was the most targeted sector. The United States, being the most targeted country, likely contributed to the high number of attacks on this sector.

The education/research sector was also heavily impacted by ransomware attacks, accounting for 22% of all attacks in 2023, according to Check Point Research.

The retail/wholesale sector experienced a significant 22% spike in attacks weekly compared to 2022, as reported by Check Point Research.

Other industries that were notably affected include the IT, healthcare, and manufacturing sectors, which were the most targeted sectors in terms of ransomware file detections in the first half of 2023, according to Trend Micro. The report from TechTarget also listed several industries as top targets, including construction and property, central and federal government, media, entertainment and leisure, local and state government, energy and utilities infrastructure, distribution and transport, financial services, and business, professional and legal services.

III. Takeaways from Ransomware Q4

- **Record Number of Victims**: The year 2023 marked the most successful year for ransomware groups in history, with a total of 4,368 victims, which is a 55.5% increase from the previous year. The fourth quarter alone saw 1,386 victims

- **Dominant Ransomware Groups**: LockBit 3.0 remained the most active ransomware group, claiming an average of around 23 victims per week. Clop Ransomware and ALPHV/BlackCat ransomware were also prominent, with 104 and 81 victims respectively
- **High-Profile Incidents**: Notable incidents included LockBit's attack on Royal Mail and the shutdown of Hive Ransomware
- **Industry Impact**: The business services sector, education/research sector, and the retail/wholesale sector were among the most affected by ransomware
- **Geographical Focus**: The United States was the most targeted country, followed by the UK and Canada
- **Trends in Attack Techniques**: There was a shift in tactics from encryption to leveraging stolen data for extortion, with attackers focusing more on data theft and extortion campaigns that did not necessarily involve data encryption
- **Ransomware Strains**: Since 2020, more than 130 different ransomware strains have been detected, with the GandCrab family being the most prevalent
- **Increased Response from Governments and Vendors**: There has been an increased response from government and technology vendors to help stem the tide of ransomware attacks
- **Ransomware as a Service (RaaS)**: RaaS remains a key driver for the ongoing frequency of attacks, with groups like LockBit operating under this model
- **Extortion Tactics**: Double and triple extortion attacks have become more prevalent and potentially more impactful and costly for affected companies
- **Supply Chain Attacks**: Supply chain attacks have become an established part of the ransomware threat landscape, extending the impact of attacks beyond single victims

IV. Ransomware Payments

In Q4 2023, the most common payment methods used in ransomware attacks continued to be cryptocurrencies, with Bitcoin being the most prevalent. Bitcoin accounted for approximately 98% of ransomware payments due to its perceived anonymity and ease of use. However, there were early indications that more privacy-focused digital currencies, such as Monero, were growing in popularity as the payment method of choice for cybercriminals. This shift was due to the increasing ease of detecting the flow and sources of Bitcoin.

Despite the prevalence of ransom payments, the proportion of victims who paid ransoms was decreasing. Only 37% of ransomware victims paid a ransom in Q4 2023, a record low. This decrease was attributed to improved security measures and backup continuity investments, which allowed more organizations to recover from attacks without paying ransoms.

The average ransom payment in Q4 2023 was significantly high, with the average payment being $408,643, a 58% increase from Q3 2022, and the median payment being $185,972, a 342% increase from Q3 2022. This increase in payment amounts was seen as a tactic by cybercriminals to compensate for the declining number of victims willing to pay ransoms.

V. Ransomware Entry Points

In Q4 2023, the common entry points for ransomware were:

- **Phishing Attacks**: Phishing attacks were the primary delivery method for ransomware, with 62% of successful ransomware attacks using phishing as their entry point in the victim's system. Phishing attacks rose by 173% in Q3 2023. Attackers used increasingly sophisticated social engineering techniques to trick employees into providing sensitive information
- **Exploitation of Vulnerabilities**: Vulnerabilities in software and systems were another common entry point. For instance, the ransomware group CL0P exploited GoAnywhere file transfer software. Two new ransomware strains, CACTUS and 3AM, emerged in Q4 2023, with CACTUS exploiting known vulnerabilities in VPN appliances
- **Credential Theft and Brute Force Attacks**: Credential theft was used in 44% of successful ransomware attacks, and brute force credentials, such as password guessing, were used in 17% of attacks
- **Supply Chain Attacks**: Attackers targeted third-party vendors to gain access to an organization’s network
- **Insider Threats**: Insider threats continued to pose significant risks to organizations
- **Social Engineering Attacks**: these attacks, including Business Email Compromise (BEC), were also common

VI. Ransomware Encryption methods

The encryption methods used in these attacks have evolved over time, with attackers adopting a mix of symmetric and asymmetric encryption techniques to increase the effectiveness of their attacks. In this approach, the ransomware generates two sets of keys, and a chain of encryption is used to increase the attack effectiveness.

In addition to these encryption methods, there has been a notable shift in the execution strategies of ransomware attacks. Increasingly, cybercriminals are focusing more on data theft, followed by extortion campaigns that do not necessarily involve data encryption.

VII. Ransomware Delivery methods

In Q4 2023, the most common delivery methods used in ransomware attacks were supply chain attacks, double extortion techniques, and Ransomware-as-a-Service (RaaS) operations.

Supply chain attacks became a solid technique for mature and experienced ransomware groups. In these attacks, instead of directly attacking a single victim, the attackers target third-party vendors to gain access to an organization's network.

Double extortion was another prevalent method. In this technique, attackers not only encrypt the victim's data but also threaten to leak stolen data if the ransom is not paid.

Ransomware-as-a-Service (RaaS) operations also played a significant role. In RaaS, developers create ransomware software and sell access to this tool to criminals who then spread

it among potential targets. The access is subscription-based, which is why it is called RaaS.

Phishing with malicious attachments and exploiting vulnerabilities, such as zero-day vulnerabilities, were also used as initial access methods to the target system

VIII. Vulnerabilities exploited by ransomware

In Q4 2023, ransomware attackers continued to exploit a range of vulnerabilities to compromise organizations. One of the most notable vulnerabilities exploited was a two-year-old vulnerability for which a patch had been available for around the same time. This highlights the importance of timely patch management and version control within organizations.

Additionally, attackers used a flaw in MagicLine4NX software, affecting versions before 1.0.026, to initiate their attacks. The MOVEit vulnerability was also significant, accounting for a notable percentage of victims in previous quarters, and it is likely that such vulnerabilities continued to be a target for ransomware groups.

The year 2023 also saw a surge in the use of zero-day exploits in ransomware attacks, which are vulnerabilities that are unknown to the software vendor or have no patch available at the time of the attack. This trend of exploiting zero-day vulnerabilities underscores the adaptability of cyber threat actors and the need for organizations to enhance their defenses against such evolving threats.

IX. Effective ways to prevent ransomware attacks

In Q4 2023, the most effective ways to prevent ransomware attacks were multifaceted, involving a combination of technical measures, user education, and proactive strategies:

- **Robust Data Backup**: Regularly backing up data is a crucial step in mitigating the impact of a ransomware attack. A secure, robust data backup solution can ensure that even if data is encrypted by ransomware, the organization can restore its systems without having to pay the ransom
- **Cyber Awareness Training**: Training employees to recognize and avoid potential ransomware threats, such as phishing emails and malicious attachments, can significantly reduce the risk of successful attacks
- **Patch Management**: Regularly updating and patching software can eliminate known vulnerabilities that ransomware might exploit
- **Advanced Threat Prevention**: Automated threat detection and prevention systems can identify and resolve most ransomware attacks before they cause significant damage
- **Endpoint Security**: Robust endpoint security solutions, including antivirus and anti-malware software, can detect and block ransomware threats
- **Network Segmentation**: Dividing the network into separate segments can prevent ransomware from spreading across the entire system
- **Zero Trust Security Model**: Implementing a zero-trust model, where access to resources is granted only after a user has successfully verified their identity, can reduce the attack surface against ransomware
- **Multi-factor Authentication (MFA)**: Implementing MFA can add an additional layer of security, making it more difficult for attackers to gain access to systems
- **Least Privilege Access**: Ensuring that users have the minimum levels of access necessary to perform their tasks can limit the potential damage of a ransomware attack
- **Application Whitelisting**: Allowing only approved applications to run on a system can prevent ransomware from executing