Akamai

State of the Internet
Volume 09 | Issue 04

Ransomware on the Move

EMEA Snapshot

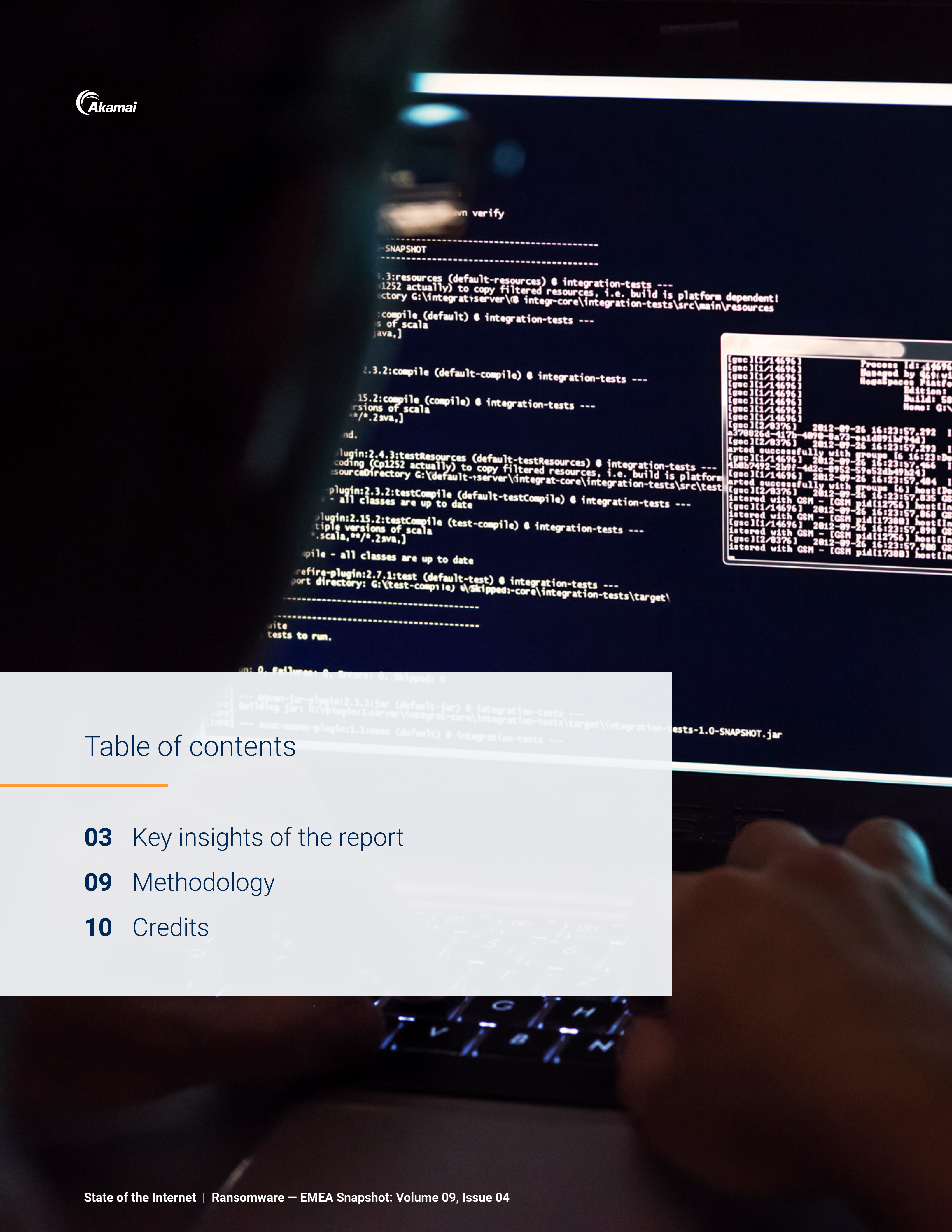


Table of contents

Key insights of the report

The EMEA Snapshot is a companion piece to our larger ransomware SOTI report, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days (available in English only). Please refer to that report for detailed analyses of ransomware groups' attack trends, methodology, and techniques; a description of the stages of attacks and the corresponding solutions and recommendations to safeguard your organization; and our research methodologies.

Overview

Ransomware continues to wreak havoc on organizations and claim more victims as adversaries continue to evolve and shift their attack techniques, introduce new extortion methods, take advantage of an expanding attack surface, and capitalize on security budget constraints. The impact of these dangerous trends is reflected in the ransomware groups that dominate the landscape and in their growing success. In EMEA, this is exemplified by an 18% growth in victim companies between Q4 2021 and Q4 2022, with a leap of 77% in the victim count year-over-year when comparing Q1 2022 with Q1 2023.

In this EMEA Snapshot, we share additional insights for better defense and risk management of this growing concern, including:

- During the period of October 2021 through May 2023, LockBit dominated the ransomware scene with CL0P rising as it aggressively exploited vulnerabilities. A shift in attack techniques, from phishing to the rampant abuse of zero-day and one-day vulnerabilities, led to the leap in victim counts.

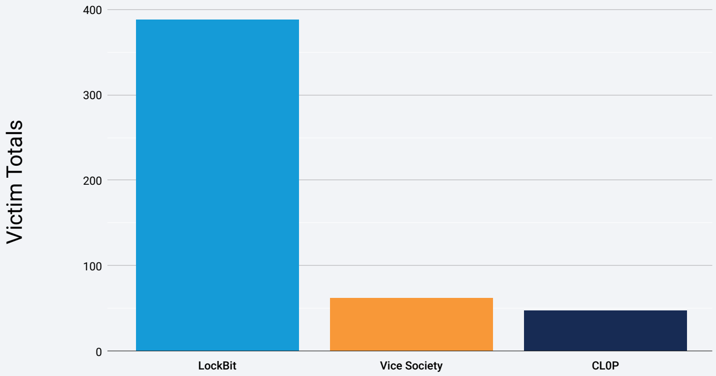
- Consistent with findings worldwide, manufacturing was the vertical with the highest number of victim organizations, followed by business services.

- The majority of ransomware victims were smaller organizations with revenue of up to US$50 million. However, the very largest organizations were also under attack.

LockBit dominates ransomware group activity

Despite a rising awareness of ransomware and an abundance of tools and best practices available to combat this threat, growth in victim companies in EMEA increased 18% between Q4 2021 and Q4 2022, with a leap of 77% in the victim count year-over-year when comparing Q1 2022 with Q1 2023. Consistent with data findings in our global report, between the period of October 1, 2021, and May 31, 2023, LockBit was responsible for the majority of attacks on victims, accounting for 45% of attacks in EMEA. However, in EMEA, Vice Society displaces ALPHV as the second most active group; CL0P is still third (EMEA Figure 1).

EMEA: Top 3 Ransomware Groups by Victim Count
October 1, 2021 – May 31, 2023



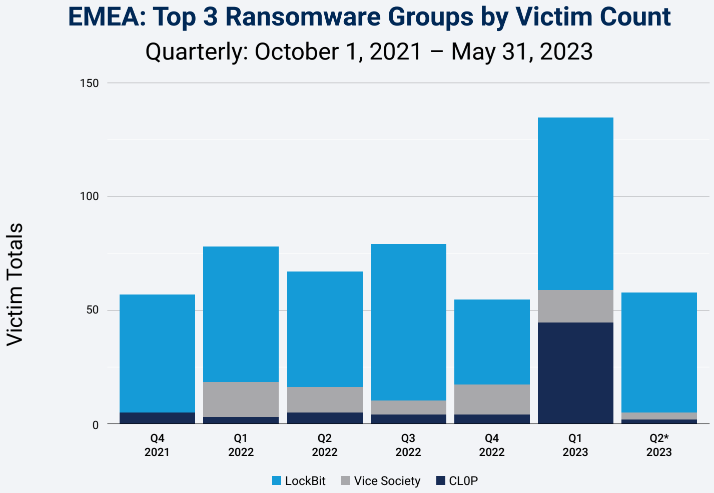
EMEA Fig. 1: The majority of the victim organizations of ransomware attacks in EMEA were hit by LockBit, Vice Society, and CL0P

Quarterly analysis

When we look at victim counts by ransomware group (EMEA Figure 2), LockBit remains prevalent, and the consistent presence of Vice Society likely goes hand-in-hand with education being one of the top industries targeted by ransomware in EMEA (shown later in EMEA Figure 3) as Vice Society is a ransomware-as-a-service offering that disproportionately targets the education sector. However, consistent with global data trends, CL0P is rising in the EMEA ransomware landscape and its spike in Q1 2023 can be attributed to its exploitation of a variety of zero-day vulnerabilities as a point of entry. A shift in attack techniques over the past six months, from phishing to the rampant abuse of vulnerabilities, is leading to the leap in victim counts. That said, only partial data was available for Q2 2023* at the time of this report. As of May 31, 2023, CL0P activity returned to the level

**Q2 2023 is not a full quarter as the data has a May 31, 2023, cutoff.*

we saw in 2022. Although we cannot say definitively what the quarter will ultimately reveal, it is important to note that in June 2023 CL0P published the names of more victim companies in EMEA as a result of the exploitation of the MOVEit vulnerability, so the victim count will likely rise.



EMEA Fig. 2: A comparison of quarterly victim counts among the top three ransomware groups in EMEA: LockBit, Vice Society, and CL0P

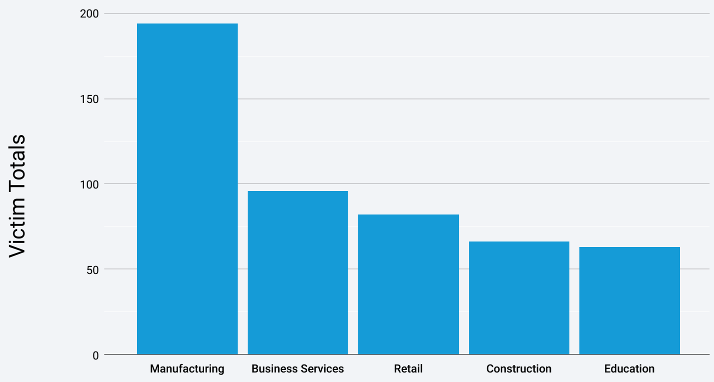
Critical industries at risk

The top five critical industries at risk of a ransomware attack in EMEA are manufacturing, business services, retail, construction, and education (EMEA Figure 3). This corresponds to the same top five industries worldwide, and is also consistent with the 2022 global ransomware report, in which manufacturing and business services held the top two positions. During that time they were victimized by Conti ransomware. After Conti's disappearance, LockBit filled the spot that Conti left. We also see significant overlap with the top five affected industries in our previous DNS report, Attack Superhighway: A Deep Dive on Malicious DNS Traffic, reflecting a clear link between malicious command and control (C2) traffic and ransomware attacks.

**Q2 2023 is not a full quarter as the data has a May 31, 2023, cutoff.*

EMEA: Top 5 Industries by Ransomware Group Victim Count

October 1, 2021 – May 31, 2023



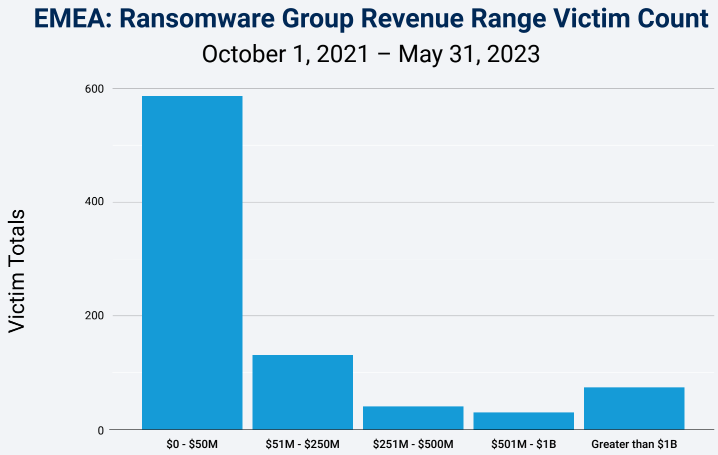
EMEA Fig. 3: Manufacturing is the vertical with the highest number of victim organizations in ransomware attacks in EMEA

It is also important to note that LockBit is the most prevalent ransomware in each of the four top industries in EMEA, accounting for 45.9% of attacks in manufacturing, 45.4% in business services, 45.1% in retail, and 53.6% in construction. Education is the exception: Vice Society is responsible for the most attacks (36.5%) and LockBit accounts for 22.2% of attacks.

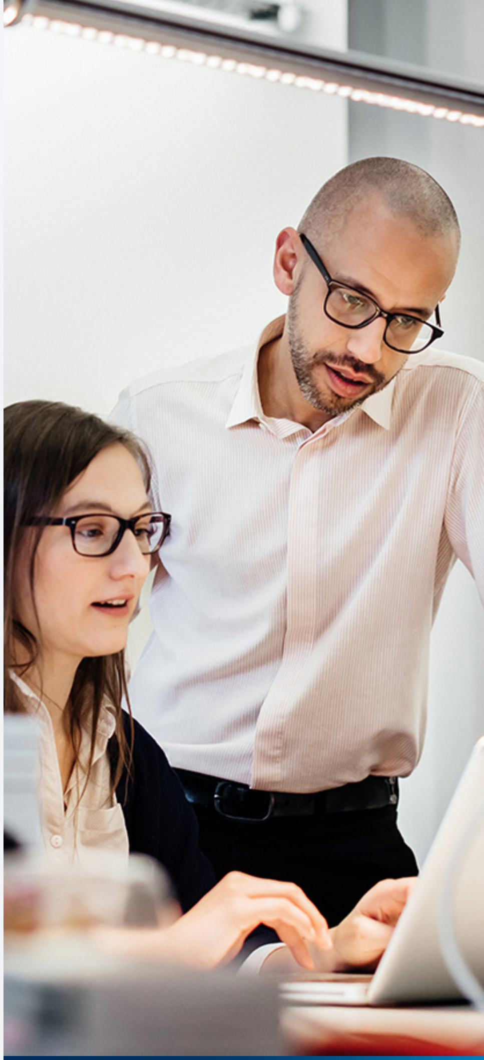
> Every organization, regardless of company size or revenue, is at risk of ransomware attacks.

Ransomware groups focus on ROI

Every organization, regardless of company size or revenue, is at risk of ransomware attacks. However, mirroring the worldwide trend, the data shows that attackers are successful in launching attacks against smaller organizations in EMEA (EMEA Figure 4). We surmise that smaller companies have limited security resources to combat the hazards of ransomware, which makes them more vulnerable and easier to infiltrate, and they have the capacity to pay the ransom. However, the largest enterprises are also under attack, with research showing the higher the revenue of the affected organization, the bigger the ransom payment.



EMEA Fig. 4: The majority of ransomware victims in EMEA are in organizations with reported revenue of up to US$50 million

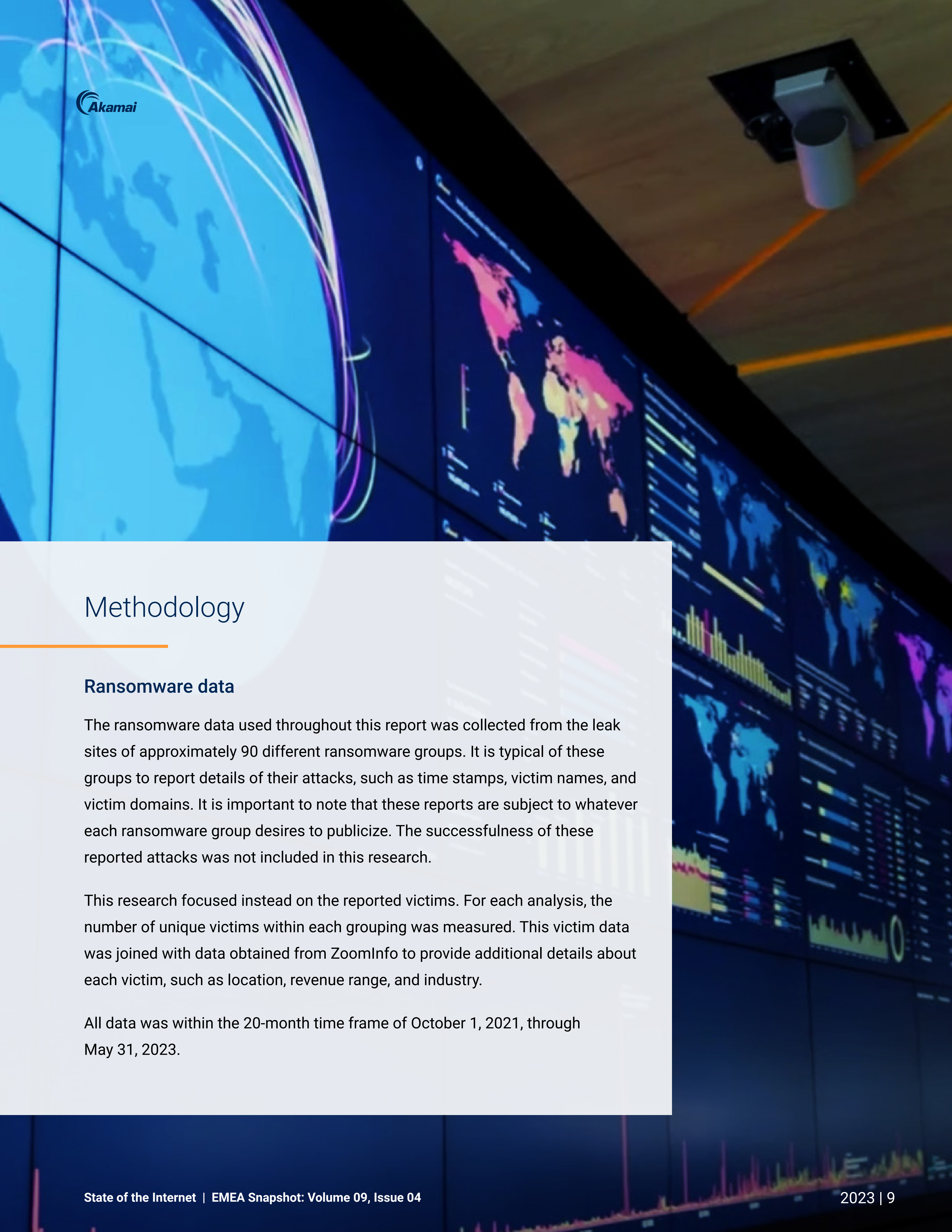


EMEA snapshot conclusion

Ransomware continues to wreak havoc on organizations. Globally and regionally, governments are forming a united front to address the threat and highlight techniques that can aid security defenders in protecting their organizations and building resilience. ENISA, the European Union Agency for Cybersecurity, issued a new Network and Information Systems Directive (NIS2) aimed at improving cybersecurity across the E.U. including new tasks such as the creation of a vulnerability registry. Outside the E.U., other countries are creating and enforcing their own controls, such as Saudi Arabia's National Cybersecurity Authority (NCA).

As regulators put initiatives and policies in place to strengthen cybersecurity standards, it is important to understand the reporting requirements in your area so that you can include them in your playbook/crisis management plan, and be aware of the opportunities you have to mitigate risk by leveraging a multilayered defense.

For more information, please refer to the global ransomware SOTI report, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days.



Methodology

Ransomware data

The ransomware data used throughout this report was collected from the leak sites of approximately 90 different ransomware groups. It is typical of these groups to report details of their attacks, such as time stamps, victim names, and victim domains. It is important to note that these reports are subject to whatever each ransomware group desires to publicize. The successfulness of these reported attacks was not included in this research.

This research focused instead on the reported victims. For each analysis, the number of unique victims within each grouping was measured. This victim data was joined with data obtained from ZoomInfo to provide additional details about each victim, such as location, revenue range, and industry.

All data was within the 20-month time frame of October 1, 2021, through May 31, 2023.

Credits

Editorial and writing

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

Review and subject matter contribution

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

Data analysis

Chelsea Tuttle

Marketing and publishing

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

More State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/ Security reports. **akamai.com/soti**

More Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports,and cybersecurity research. **akamai.com/security-research**

Akamai data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. **akamai.com/sotidata**

More on Akamai solutions

To learn more about Akamai's solutions for ransomware, visit our **Security Solutions** page.