FUTURE OF DIGITAL SECURITY

2023 RTF Global Ransomware Incident Map: Attacks Increase by 73%, Big Game Hunting Appears to Surge

By Taylor Grossman, Trevaughn Smith on September 26, 2024

Introduction

In 2021, the Ransomware Task Force (RTF) released 48 recommendations that together formed a public-private, unified, whole-of-society approach to tackling the threat of ransomware. Access to accurate, comprehensive data plays a key role in many of these recommendations: without a clear understanding of the entities, payments, sectors, countries, and tactics, techniques, and procedures involved, we struggle to effectively reduce the threat.

The RTF's establishment marked important progress towards achieving a better understanding of the ecosystem and supporting public and private stakeholders with information to drive policy recommendations. Now in its fourth year, the RTF continues to collect data and insights from task force members, including from law enforcement, government, and security professionals.

The 2023 RTF Global Ransomware Incident Map presents the task force's annual map of ransomware incidents and identifies ransomware trends worldwide. We noted in last year's map that the decline in ransomware incidents in 2022 was likely temporary due to several factors, most notably law enforcement action and the invasion of Ukraine. Indeed, starting in January 2023, we began to see the number of incidents increase, a trend that our data indicates ultimately resulted in a 73% year-over-year increase in attacks from 2022 to 2023. This piece examines data from eCrime.ch, a site that compiles messages on data leak sites as its primary source of ransomware incident tracking. We explore in greater detail in the Data and Methodology section the benefits and limitations of this approach.

We argue that this significant rise illustrates a shift in tactics to big game hunting—targeting high-value organizations or entities with ransomware attacks—and use this as an opportunity to analyze one of the largest incidents of the year: CL0P's exploitation of the MOVEit vulnerability. Because ransomware activity continues to trend in the wrong direction, we reiterate our call for an increased focus on deterrence and disruptive efforts as articulated in the April 2024 RTF progress report. Available evidence suggests that government and industry actions taken in 2023 were not enough to significantly reduce the profitability of the ransomware model.

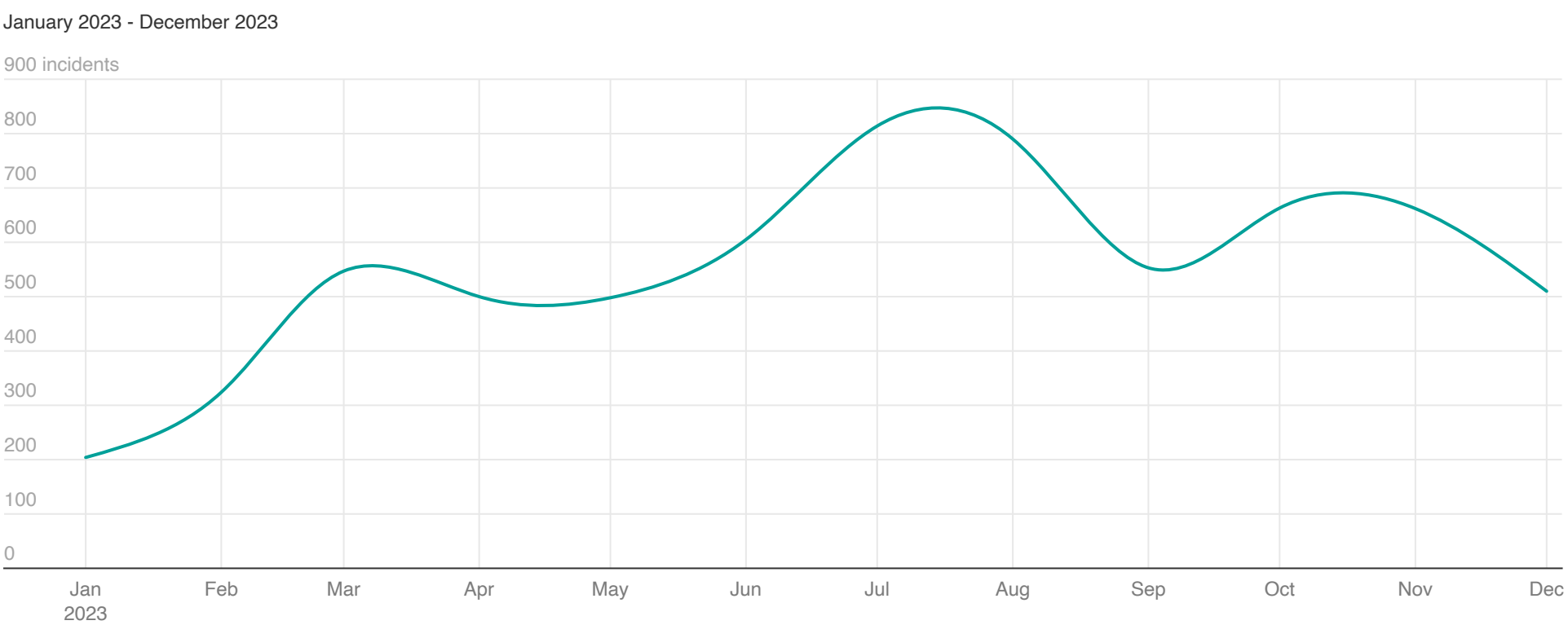


Chart: Institute for Security and Technology • Source: ecrime.ch • Created with Datawrapper

In 2023, the data shows 6,670 ransomware incidents, a 73% year-over-year increase from 2022. This increase is consistent with other recently published findings, which demonstrate an overall increase in ransomware activity and illicit cryptocurrency payments. The FBI Internet Crime Center (IC3), for example, reported over 2,825 complaints from the American public alone. According to Chainalysis, ransomware payments broke a new record, totaling over $1 billion in 2023.

In addition to the rise in overall ransomware activity, the data also reflects increases resulting from several large and high-profile ransomware attacks, such as CL0P's GoAnywhere MOVEit exploits, which alone contributed to approximately 666 incidents in 2023. We believe that this is the likely cause of the spike in incidents from June 2023 to July 2023 in the above graph.

Ransomware Incidents By Sector

Ransomware Incidents by Sector

January 2023 to December 2023

Sector	# of incidents	% change from 2022
Construction	231	49.03%
Hospitals and Health Care	177	98.88%
IT Services and IT Consulting	164	112.99%
Financial Services	147	149.15%
Law Practice	146	108.57%
Higher Education	119	105.17%
Government Administration	117	44.44%
Real Estate	103	71.67%
Software Development	95	331.82%

Note: This graph does not reflect incomplete entries in the dataset.

Table: Institute for Security and Technology • Source: ecrime.ch • Created with Datawrapper

In 2023, ransomware actors targeted construction, hospitals and healthcare, IT services and consulting, financial services, and law practices, as well as myriad other industries. The data shows a year-over-year increase in incidents in a majority of sectors compared to 2022, which is in line with the overall increased ransomware activity observed throughout the year. Like last year, our data indicates that the construction and hospitals and healthcare sectors continue to be the top two sectors with the most incidents worldwide.

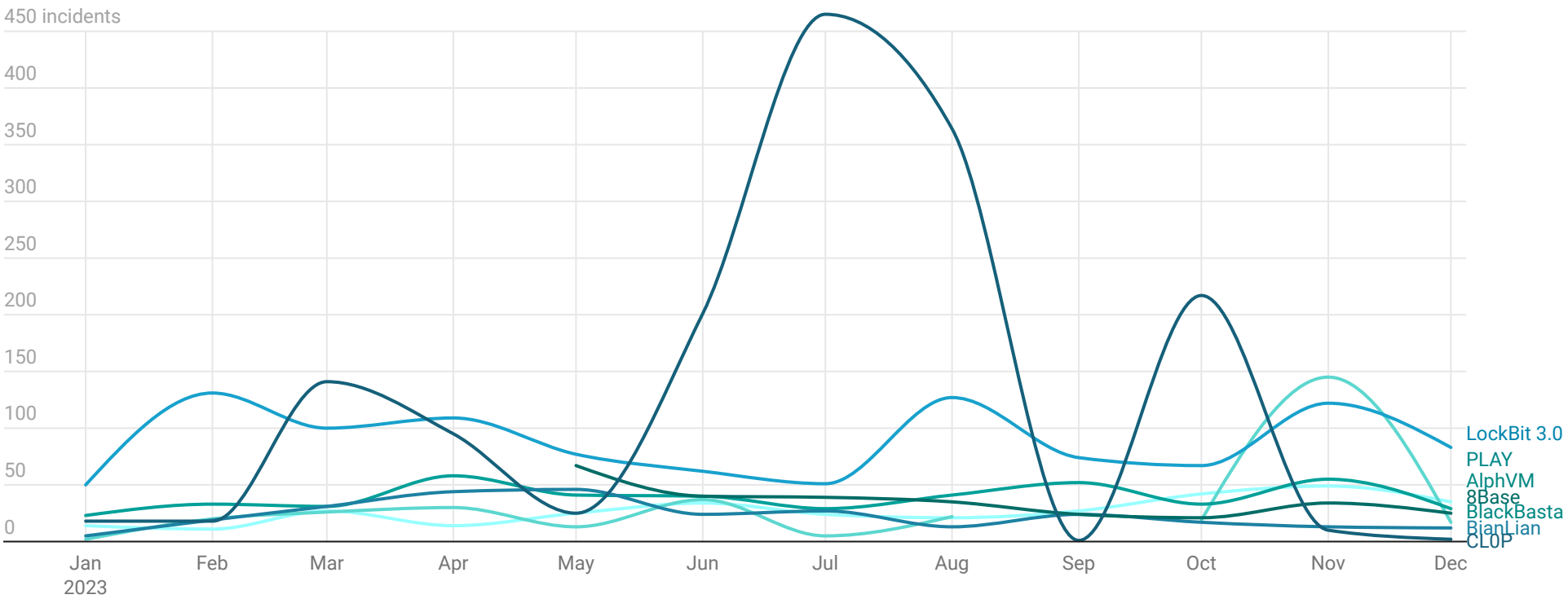
services incidents, and a 113% increase in IT services and IT consulting incidents.

This upward trajectory suggests that cyber criminals still stand to profit from the Ransomware-as-a-Service (RaaS) model. As reflected by this data set, disruptive actions appear to be generally tactical and temporary. However, as we noted in our 2024 RTF progress report, governments have stepped up efforts in recent months, the effects of which are likely not visible in our data thus far.

Ransomware Incidents By Group

Timeline of Incidents by Ransomware Group

January 2023 to December 2023



Note: This graph does not reflect incomplete entries in the dataset.

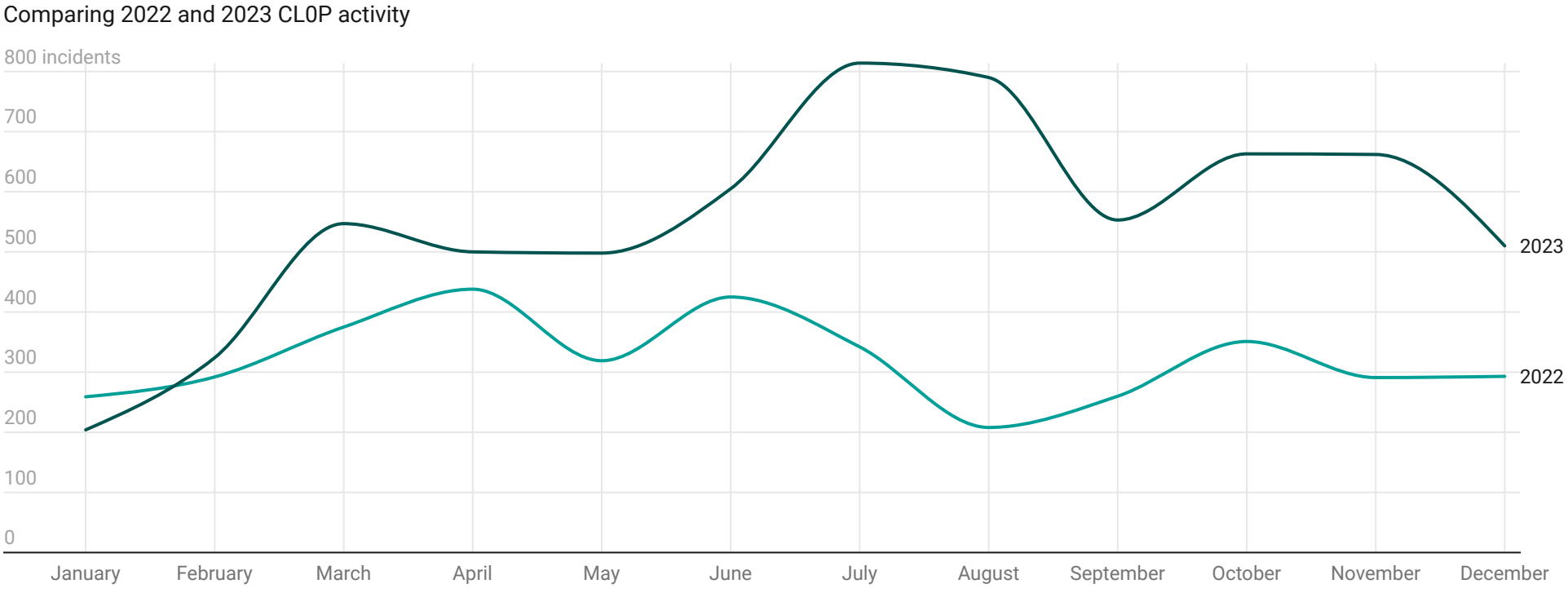
Chart: Institute for Security and Technology • Source: ecrime.ch • Created with Datawrapper

As we saw in 2022, the profitability of the RaaS model continues to motivate ransomware actors to shift allegiances, form new groups, or iterate existing variants. In 2023, the two most active ransomware groups, LockBit and CL0P, pursued two different styles of operations as reflected in the eCrime data. While CL0P perpetrated one of—if not the most–serious ransomware incidents of the year, the group's activity is concentrated in June and July 2023. LockBit, meanwhile, showed a more consistent pattern of activity.

CLOP's Rise & MOVEit Exploit

CL0P Gang Activity Timeline

Comparing 2022 and 2023 CL0P activity



Note: This graph does not reflect incomplete entries in the dataset.

Chart: Institute for Security and Technology • Source: ecrime.ch • Created with Datawrapper

deal with the aftermath: organizations issued data breach notifications in August and September 2024, and courts will likely be adjudicating class-action lawsuits for years to come.

MOVEit marks CL0P's third known use of zero-day vulnerabilities. (In January 2021, CL0P used multiple zero-day vulnerabilities to gain unauthorized access to Accellion, now known as Kiteworks, a legacy file transfer appliance. In February 2023, CL0P again used a zero-day to compromise GoAnywhere, a managed file transfer software.) Such incidents tend to attract significant attention because of their relative novelty and impact. However, it is unclear if CL0P recognized how common these file transfer softwares were across industries, or if the group simply exploited the vulnerabilities as a matter of convenience or opportunity.

Importantly, zero-days are nowhere near the most common method ransomware actors use to exploit remote access applications. Akira and Snatch employed known vulnerabilities in VPN appliances to establish initial access to targets. According to eCrime, Akira executed at least 200 ransomware incidents from March to December 2023, while Snatch was less prolific but still active over the course of the year. Zero-days often receive the most attention, but other methods of attack are still very profitable.
Altogether, these groups' recent successes may incentivize other ransomware actors to shift to using remote exploit vulnerabilities to compromise important systems found across industries. Incidents like these could also signal a shift by certain ransomware gangs to big game hunting tactics: using ransomware to target high-profile, high-value organizations to maximize potential payouts.

Evolving Ransomware Group Methods: LockBit and 8Base

While CL0P's major exploits contributed to a temporary surge in ransomware activity, LockBit continued to stand out as the most "stable" ransomware group last year. The group launched a consistent number of ransomware attacks across 2023, often overshadowing CL0P during their points of downtime. By continuously adapting their existing RaaS model to attract affiliates, leverage new vulnerabilities, and improve their malicious software, LockBit has been able to maintain this consistency where other ransomware groups have faltered.

LockBit's Royal Mail ransomware attack in early 2023 made international headlines, potentially driving additional business to the group and its affiliates within the RaaS ecosystem. Royal Mail is a private British mail courier responsible for servicing all 32 million United Kingdom addresses, six days a week. The ransomware attack resulted in major delays for Royal Mail customers and forced the company to temporarily stop processing new international shipments for over a month. After an initial ask of $80 million, LockBit demanded a $70 million ransom for the decryption keys and to prevent the group from leaking stolen data on the dark web. Royal Mail refused, ultimately spending almost £10 million in recovery costs after the attack. Lockbit then released chat logs of the entire negotiation between the group and Royal Mail.

At the same time, many ransomware groups still rely on traditional, relatively unsophisticated means such as phishing to execute an attack. 8Base is a good example of the profitability of such a model. 8Base, who portray themselves as "'simple penetration testers'" to trick victims into paying their ransom demand, emerged in March 2022. The group typically relies on phishing attacks to compromise systems, delivering a ransom note that pretends to offer help to their victims. In May 2023, 8Base moved to a double-extortion ransomware model and created their own data leak site. (While 8Base was likely active before this time, eCrime data only notes their presence after May 2023, which is when they created their data leak site.)

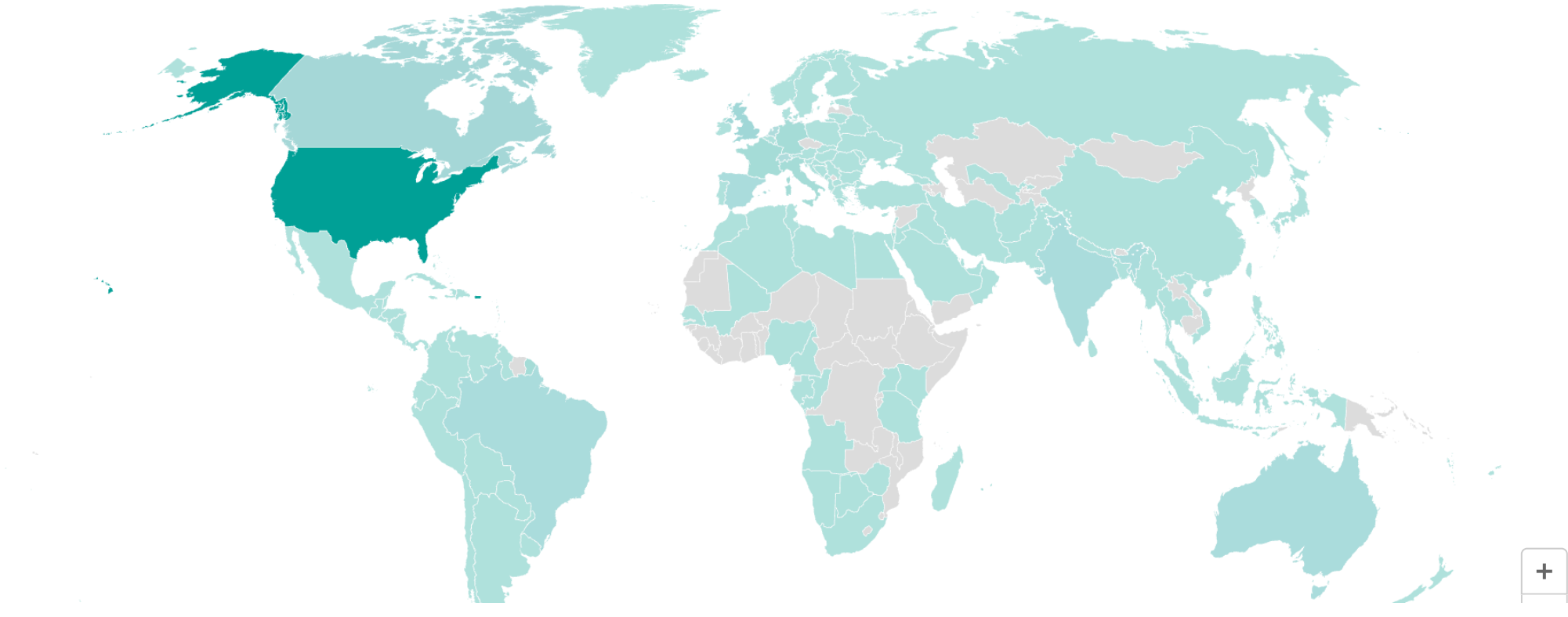
Global Ransomware Incidents

Global Ransomware Incidents by Country

January 2023 - December 2023

# of incidents

1 4,892



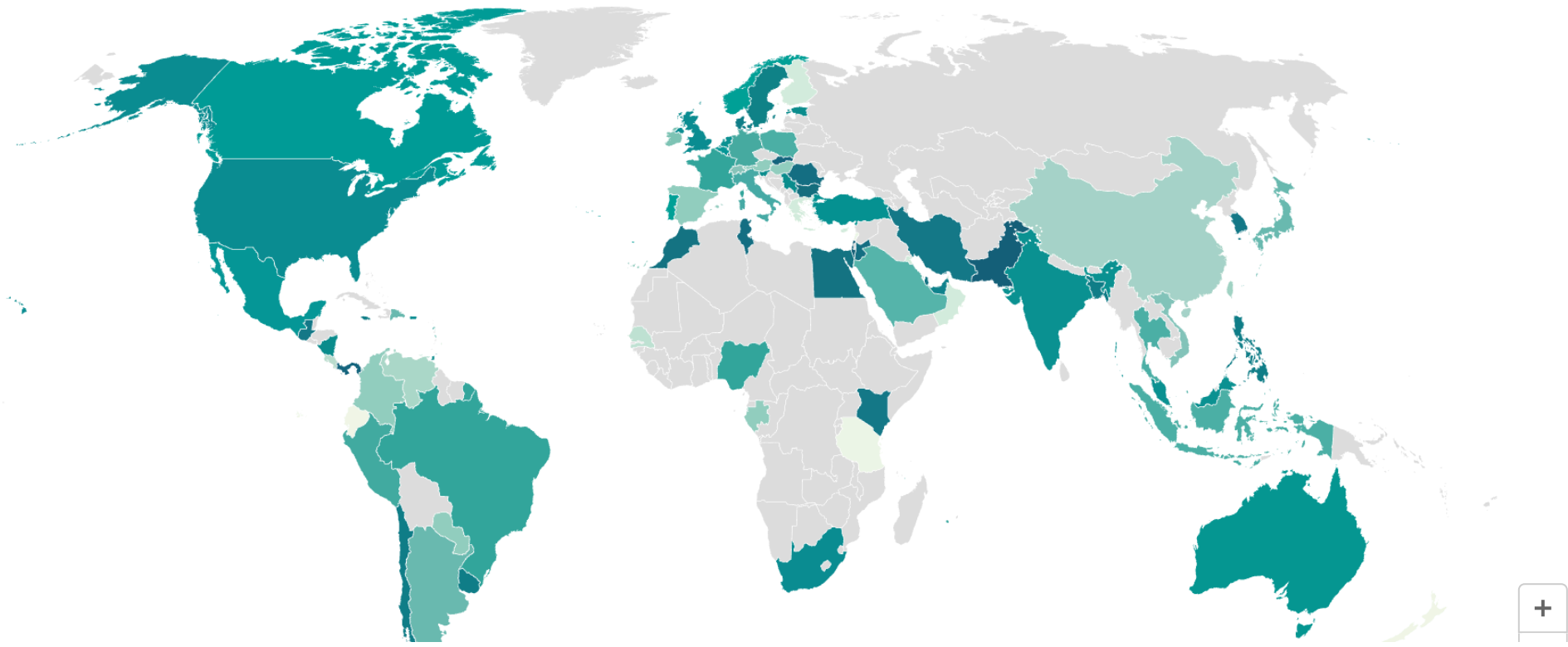
IST Institute for SECURITY + TECHNOLOGY

Global Ransomware Incidents: Year-Over-Year Change

January 2023 - December 2023

% change in # of incidents

−71.0% 500.0%



Mapping the year-over-year change globally tells us a different story. The data shows the greatest increase in ransomware activity in South Asia, specifically around Iran, Pakistan, and India. However, with a small number of incidents to begin with, the percent change value can be misleading. We also observe a general increase in year-over-year ransomware incidents across North America and Latin America, and a decrease in incidents in China, likely due to underreporting.

Latin America

Ransomware Incidents: Latin America

January 2023 - December 2023

# of incidents

1 83

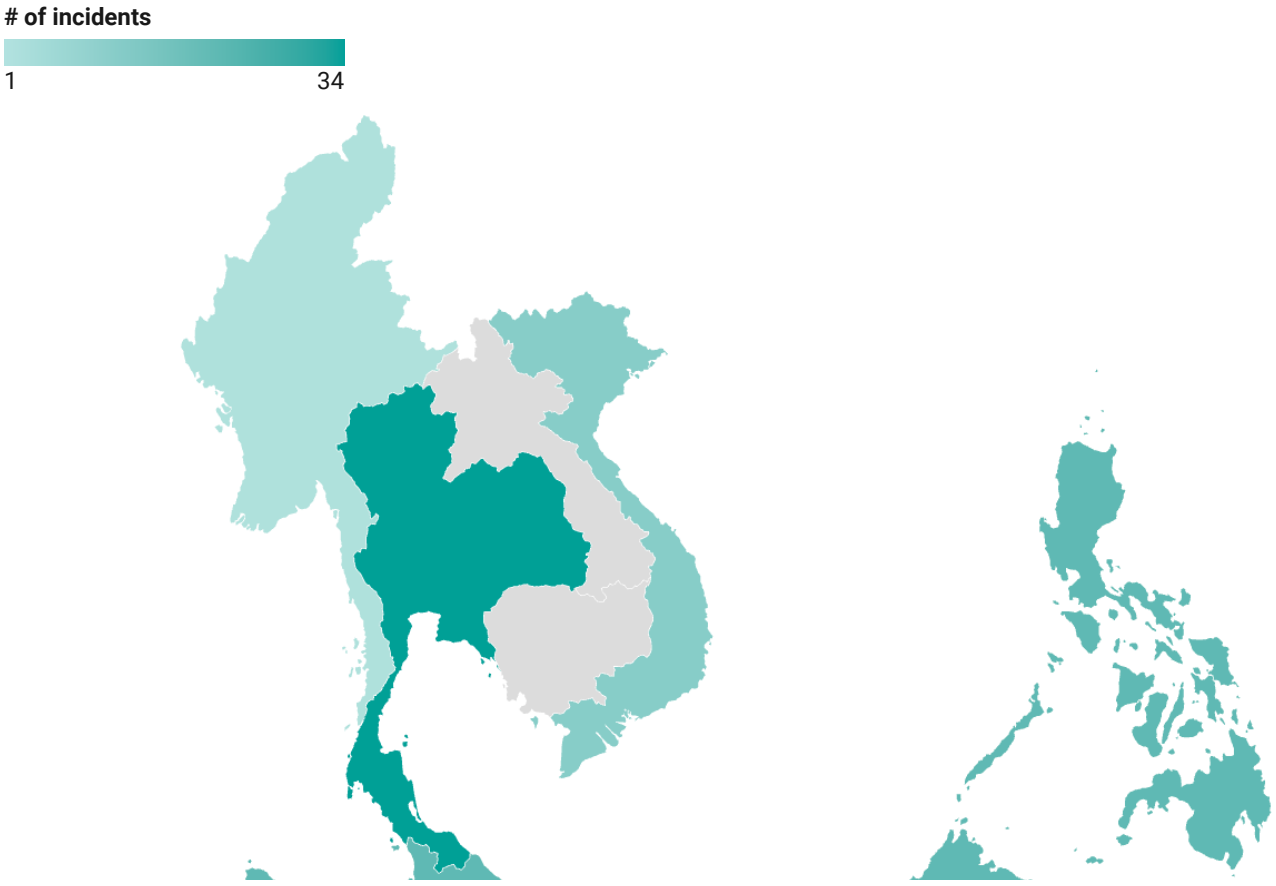
In 2023, eCrime identified 240 ransomware incidents in Latin America, a 49% increase from 2022. LockBit was responsible for the most incidents in the region (73 incidents, a 128% increase from 2022), followed by 8Base (32 incidents), and then AlphVM (25 incidents, a 53% increase from 2022).

Brazil experienced the highest number of ransomware incidents, followed by Mexico then Argentina. Trend Micro reported that Brazil was the second most vulnerable country in cyberspace in the first half of 2023, behind the United States. LockBit and AlphVM were significantly more active in the region compared to 2022. As mentioned in last year's incident map, these numbers likely do not reflect the full extent of ransomware activity. Threat actors with a small regional footprint appear less likely to rely on public leak sites to compel payment from victims, making it more difficult for data leak site aggregators like eCrime to capture the full range of activity.

Southeast Asia

Ransomware Incidents: Southeast Asia

January 2023 - December 2023



In Southeast Asia, eCrime identified 133 ransomware incidents, a 58% year-over-year increase from 2022. Top ransomware groups include LockBit (55 incidents, a 161% increase from 2022), AlphVM (21 incidents, a 200% increase from 2022), and CL0P (6 incidents in 2023).

LockBit made headlines in May 2023 after compromising Bank Syariah Indonesia (BSI), the country's largest Islamic Bank, stealing the information of 15 million customers and employees (almost 1.5 terabytes of data) and disrupting ATM withdrawals and online banking services. LockBit leaked the stolen data and their private chats with BSI ransom negotiators, adding that they "kept a small part of the most interesting data for [themselves] for post-exploitation." LockBit's attack on BSI reflects a willingness by many ransomware groups to attack state-owned enterprises and other critical infrastructure sectors to maximize disruptions for users and increase the chances of a ransomware payment.

Hospitals & Healthcare

Timeline of Incidents in Hospitals and Healthcare Sector

January 2022 - December 2023

Note: This graph does not reflect incomplete entries in the dataset.

Chart: Institute for Security and Technology • Source: ecrime.ch • Created with Datawrapper

United States alone). However, this piece focuses on incidents as captured by data leak sites, rather than through other reporting venues.

Hospitals have traditionally emphasized data confidentiality over data availability and continuity of care. Cybersecurity has tended to lag behind. Yet hospitals cannot afford a moment of downtime both operationally and financially, making them a prime candidate for paying a ransom demand to get their systems back up and running. These entities also have highly confidential and valuable patient data that can be sold on the dark web. Ransomware attacks on healthcare facilities remain an effective opportunity for cybercriminals to make money and continue to feed profits back into the RaaS model, a key point in the RTF's research on the ransomware ecosystem.

Outlook

This year's edition of the map continues to illustrate the persistent nature of many ransomware groups. However, the scale, frequency, and complexity of incidents continue to increase as cybercriminals refine the RaaS model. The fundamental criminal effectiveness of the RaaS model has not changed, and these crimes continue to grow more profitable over time. Additional efforts must be taken in 2024 and beyond to disrupt this model.

As we enter the final three months of 2024, we anticipate an increase in "big game hunting" tactics by ransomware groups–most notably CL0P—as cyber criminals adapt and create new ways to further extort ransomware victims. We also note the execution of Operation Chronos, a major global disruptive operation targeting LockBit in February 2024, and look forward to unpacking the long-term effects of this operation.

We also intend to track possible ripple effects across industries following a major, public, lucrative payout. When an organization pays a large ransom, that transaction does not happen in a vacuum. For example, the same hackers targeted a number of organizations in the casino and entertainment sector in a short period of time. MGM ultimately did not pay the ransom, but only a few days prior Caesars did, which may have encouraged other groups to turn their sights on the industry. Likewise, Change Healthcare's payout in February 2024 was followed by a major rise in ransomware incidents across the sector in April. Groups may also decide to target comparable organizations and those in adjacent sectors. As 2024 draws to a close, we plan to leverage the year's data to further investigate these sector ripple effects.

As indicated by our April 2024 progress report, 24 of the 48 original recommendations proposed by the Ransomware Task Force have seen little to no action since 2021. While some RTF recommendations, such as 2.1.1 (Develop new levers for voluntary sharing of cryptocurrency payment indicators) and 2.1.3 (Incentivize voluntary information sharing between cryptocurrency entities and law enforcement) have seen some progress, they require sustained public and private sector support to maximize disruptive opportunities. Continued and coordinated efforts from both industry and government are essential for the strategic, global disruption of ransomware activity.

Data & Methodology

The 2023 Global Ransomware Incident Map, like last year's map, relies on data from eCrime.ch, which aggregates messages posted on data leak sites as the primary source of information about ransomware attacks. IST and the RTF thank Corsin Camichel and eCrime.ch for generously providing access to this critical data.

When ransomware gangs post on their respective data leak site, eCrime collects and collates this data, giving us limited but important visibility into a given breach, including how much data was exfiltrated and what type of sensitive information the data contains. Because a data leak site post typically contains information about stolen data *after* an initial ransomware attack is executed, this approach is biased towards ransomware attacks that use a double-extortion model, which involves two separate ransom demands. In double extortion, ransomware criminals first demand a payment in exchange for the decryption of the victim's data. They then demand a second payment to prevent sensitive stolen data that was exfiltrated prior to the encryption from being leaked. If the first or second ransom demand is not met, data leak sites begin to play a role in distributing this data. We also note a trend of ransomware groups that skip the encryption step of double-extortion and move directly to data extortion.

However, not every post on a data leak site is directly tied to a ransomware attack. This is due to the dual purpose nature of data leak sites, which also serve as public communication channels for ransomware groups. In February 2022, for example, Conti used their data leak site to announce their support for the Russian Government.

This increased activity on data leak sites demonstrates not only heightened ransomware group activity, but also that ransomware gangs increasingly seek to correspond with entities outside of the ransomware ecosystem. In 2022, we noted 1,355 of such incidents. These entries increased to 2,224 in 2023, a 64% year-over-year increase. Data like these help us to assess the overall activity of various ransomware gangs and to further contextualize large-scale attacks such as CL0P's MOVEit hack. Therefore, we include these incomplete entries in our overall assessment of ransomware incidents, but omit them from any sector- or country-specific analyses. We note at the bottom-left corner of each graph if this data has been removed.

The RTF is open and interested in expanding its data sources, and welcomes input from other organizations with victim data information. Many thanks to Silas Cutler and Corsin Camichel for their valuable insights and feedback.

IST Institute for SECURITY + TECHNOLOGY

Related Content

NEWS

THE NATSPECS BLOG

Back to Blog

BLUEPRINT FOR RANSOMWARE DEFENSE

Prepare, Don’t Pay: A Quick-Start Guide to Defending Against Ransomware

CRITICAL INFRASTRUCTURE

Institute for Security and Technology and Cyber Threat Alliance Submit Comments on Cyber Incident Reporting for Critical Infrastructure Act

IST Institute for SECURITY + TECHNOLOGY

FUTURE OF DIGITAL SECURITY

2022 RTF Global Ransomware Incident Map: Attacks continue worldwide, groups splinter, education sector hit hard

Copyright © 2023 - Institute for Security and Technology. All Rights Reserved.

Privacy Policy

Sign up to receive information about IST

First Name

Last Name

Organization

Your email address