A BLACK KITE RESEARCH REPORT

RANSOMWARE THREAT LANDSCAPE REPORT

RANSOMWARE RESURGENCE

EMERGING TRENDS, THREAT ACTORS, AND CYBERSECURITY STRATEGIES

EXECUTIVE SUMMARY

PREPARED BY
Black Kite Research

HEAD OF RESEARCH
Ferhat Dikbiyik

A BLACK KITE RESEARCH REPORT

Among all cyber threats, ransomware groups continue to evolve into formidable adversaries, causing significant financial and operational disruptions.

This Ransomware Threat Landscape: Ransomware Resurgence 2023 report examines the evolving landscape of ransomware attacks from **April 1, 2022, to March 31, 2023.** The analysis includes **2,708 ransomware victims** whose names were publicized by ransomware groups on their underground blogs. The report delves into the targeted industries, countries, and ransomware groups involved in these attacks, as well as the victims' Ransomware Susceptibility Index™ (RSI™) values.

Although the overall number of ransomware attacks did not increase significantly until 2023, a resurgence in February and March 2023 was observed, with new ransomware gangs emerging and established players executing mass-ransomware attacks. The top targeted industries during this period were Manufacturing, Professional, Scientific, and Technical Services, and Educational Services. The United States remained the top targeted country, followed by the UK, Germany, Canada, and France.

KEY TAKEAWAYS

- Ransomware attacks resurged in early 2023, with new players such as Royal, BianLian, and Play ransomware gangs joining the field and major players like LockBit and Clop executing mass-ransomware attacks.
- The top targeted industries were **Manufacturing (19.5%),** Professional, Scientific, and Technical Services (15.3%), and Educational Services (6.1%).
- The **United States** was the top targeted country, accounting for **43%** of victim organizations, followed by the UK (5.7%) and Germany (4.4%).
- Ransomware groups tended to target companies with annual revenues of around **$50M to $60M,** with third-party vendors often being targeted for client information extortion.
- The top ransomware groups during the analysis period included **LockBit (29%),** AlphaVM (BlackCat) (8.6%), and Black Basta (7.2%).
- **Encryption-less ransomware** is on the rise, underscoring the importance of data protection and regulatory compliance in addition to addressing business interruption risks posed by traditional encryption-based attacks.
- Over **70%** of ransomware victims had an RSI™ value above the high-risk threshold **(0.4)**, indicating their susceptibility to ransomware attacks.
- Common ransomware indicators among victims included poor email configuration, recent credential leaks, public remote access ports, out-of-date systems, and IP addresses with botnet activity.

BY UNDERSTANDING THESE KEY INSIGHTS, ORGANIZATIONS CAN BETTER PREPARE AND DEFEND AGAINST THE EVER-EVOLVING THREAT OF RANSOMWARE ATTACKS.

NAVIGATING THE RANSOMWARE LANDSCAPE IN 2023

The dynamic and often unpredictable nature of cyber threats poses a constant challenge for organizations worldwide. Among these threats, ransomware groups continue to evolve into formidable adversaries, causing significant financial and operational disruptions. In recent years, ransomware groups have adapted their tactics, honed their targeting methodologies, and exploited vulnerabilities in third-party vendors to maximize their profits.

These groups have taken on the characteristics of a tech company, adopting a mentality geared towards expanding their illicit businesses. This rapid evolution of cybercriminals creates a challenging and uneven playing field for cybersecurity professionals tasked with defending organizations against ransomware attacks.

This report aims to provide valuable insights into the current state of ransomware attacks and equip cybersecurity professionals with crucial information to combat these resourceful adversaries.

Through a detailed analysis of 2,708 ransomware victims publicized by ransomware groups between April 1, 2022, and March 31, 2023, we have identified key trends, targeted industries, and countries, as well as the prominent ransomware groups behind these attacks. Additionally, we delve into the Ransomware Susceptibility Index™ (RSI™), a parameter developed by Black Kite, which computes the likelihood of an organization experiencing a ransomware attack.

By understanding the complexities of the ransomware landscape in 2023, recognizing the patterns of these cybercriminals, and acknowledging the challenges faced by cybersecurity professionals, organizations can make informed decisions about their cybersecurity strategies, invest in the right defenses, and ultimately reduce their susceptibility to ransomware attacks.

We hope that the information, statistics, and insights provided in this report will empower and aid cybersecurity professionals in their ongoing battle against cybercrime.

RANSOMWARE ATTACK TRENDS:
A YEAR OF UPS AND DOWNS

Throughout 2022, ransomware attacks experienced a period of relative stagnation as several major ransomware groups were shut down, and various external factors contributed to a decrease in attack frequency:

- International sanctions due to the Russian invasion of Ukraine, hindering ransom money movement and resource investment in Western countries.
- Increased pressure from law enforcement and successful joint operations against ransomware groups in 2021 and 2022, leading to heightened caution among cyber criminals.
- A general lack of ransom coverage in cyber insurance policies, discouraging ransom payments.
- The knowledge that paying a ransom does not guarantee the threat actor will refrain from publishing sensitive records, leaving organizations vulnerable to regulatory fines regardless of payment.

However, the ransomware landscape experienced a notable uptick in February and March of 2023:

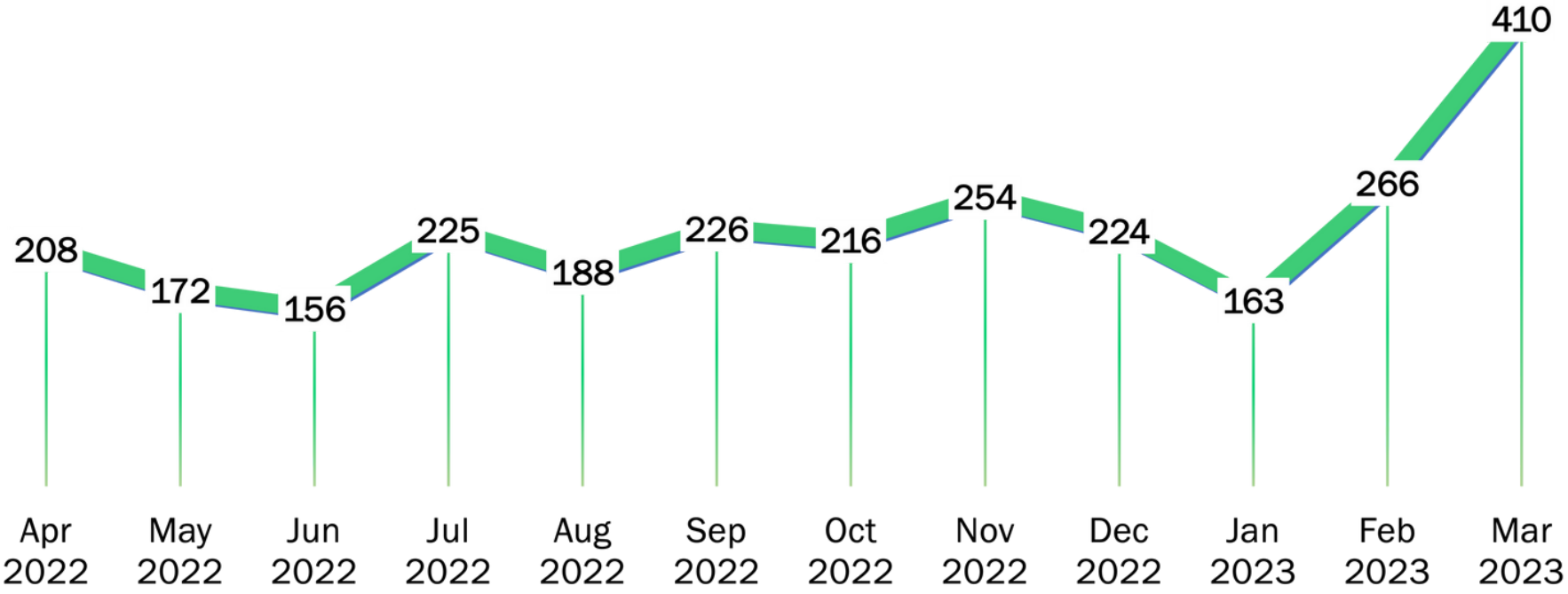
- Emergence of new ransomware gangs such as Royal, BianLian, and Play, with some like Karakurt and BianLian adopting encryption-less tactics.
- Mass ransomware attacks executed by major players like LockBit and Clop.

The number of ransomware victims announced in March 2023 was nearly double that of April 2022 and **1.6 times higher** than the peak month in 2022, signaling a dramatic increase in ransomware activity.

The following chart (Chart 1) visually illustrates the fluctuating pattern of ransomware attacks over the year, emphasizing the significant rise in recent months. This trend underscores the importance of remaining vigilant in the face of an ever-evolving threat landscape and adapting cybersecurity strategies accordingly.

NUMBER OF VICTIMS ANNOUNCED BY RANSOMWARE GROUPS

CHART 1



INDUSTRY INSIGHTS: RANSOMWARE GROUPS' FOCUS AND EVOLVING LANDSCAPE

Our analysis reveals the distribution of ransomware victims across various industries*, shedding light on the areas of focus for cybercriminals and the evolving threat landscape. (Chart 2)

Based on these findings, we can provide the following insights:

- **Manufacturing and Professional, Scientific, and Technical Services** together account for **nearly 35%** of all ransomware victims, making these industries particularly attractive targets for cybercriminals. This could be attributed to the wealth of valuable intellectual property and sensitive data held by organizations in these sectors.

- **Educational Services, Retail Trade, and Health Care and Social Assistance** together represent **around 17%** of ransomware victims. Organizations in these industries often hold sensitive personal information, making them lucrative targets for ransomware groups seeking to extort money.

- Industries such as Wholesale Trade, Finance and Insurance, and Public Administration make up a smaller portion of total ransomware victims, but still require close attention. The finance sector, for example, faces inherent risks due to the high value of financial data they possess, while public administration entities may be targeted for political reasons or to disrupt essential services.

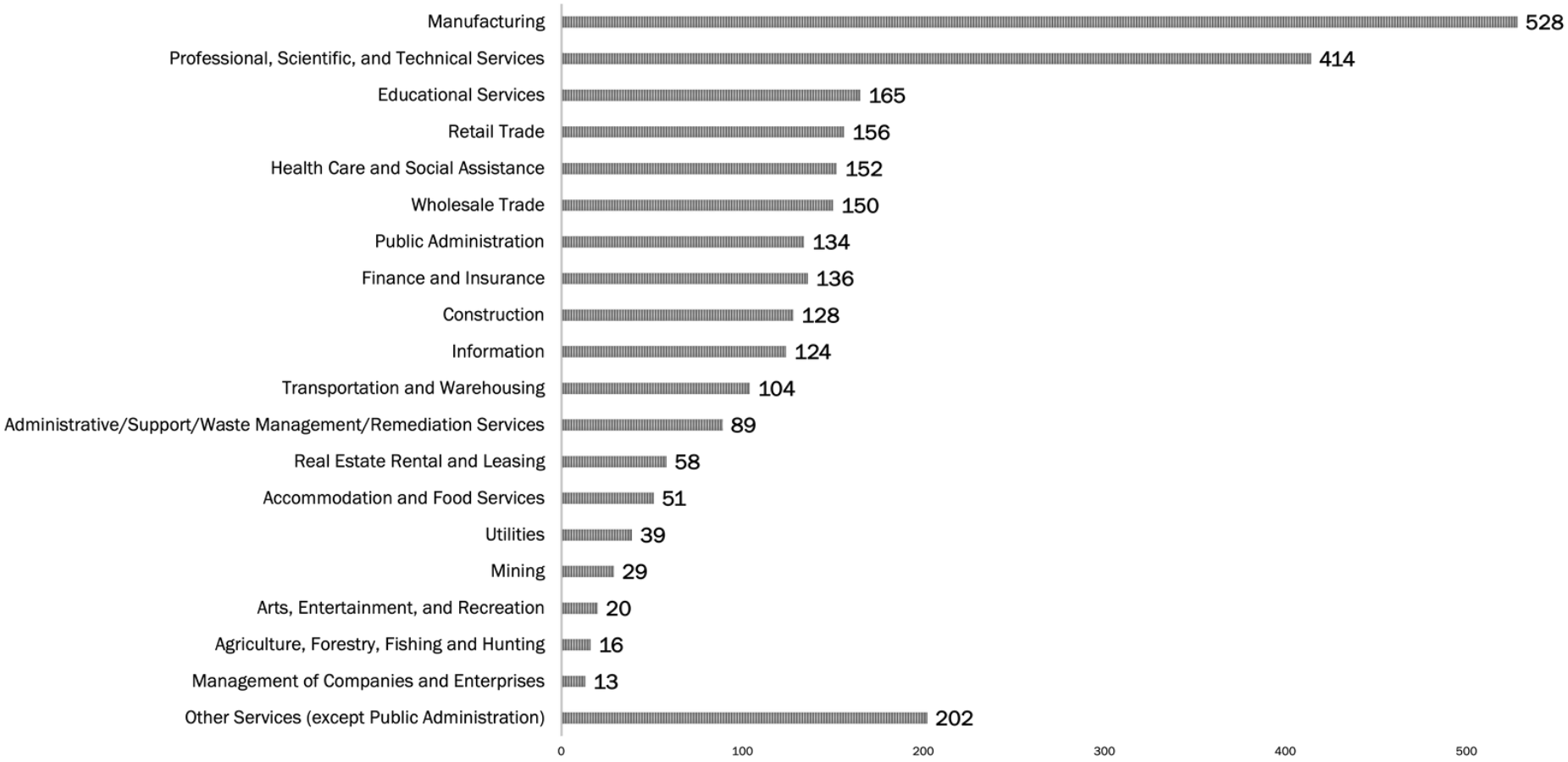
*We use the North American Industry Classification System (NAICS) codes for industry classifications in this analysis.

Additionally, our trend analysis (Chart 3) indicates that (1) Educational Services, (2) Wholesale Trade, and (3) Administrative, Support, Waste Management, and Remediation Services are emerging as trending industries for ransomware attacks. This suggests that ransomware groups are expanding their focus and adapting their tactics to exploit vulnerabilities in a broader range of sectors.

Based on these insights, organizations should assess their industry's risk profile and tailor their cybersecurity strategies accordingly. Being aware of the specific vulnerabilities and motivations behind targeting certain industries can help organizations better prepare for and mitigate the risks associated with ransomware attacks.

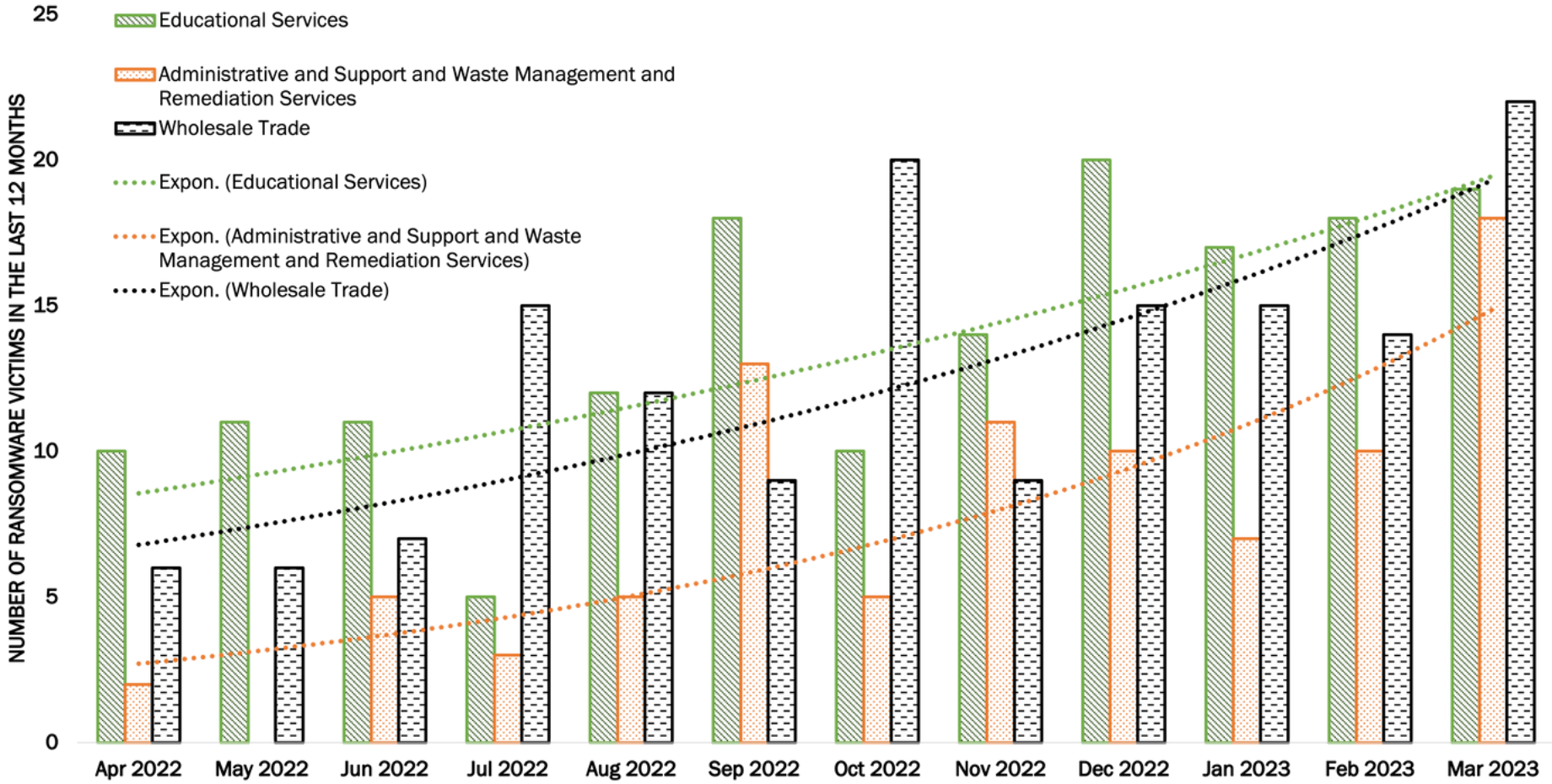
NUMBER OF RANSOMWARE VICTIMS IN THE LAST 12 MONTHS BY INDUSTRY

CHART 2



TRENDING INDUSTRIES IN RANSOMWARE

CHART 3

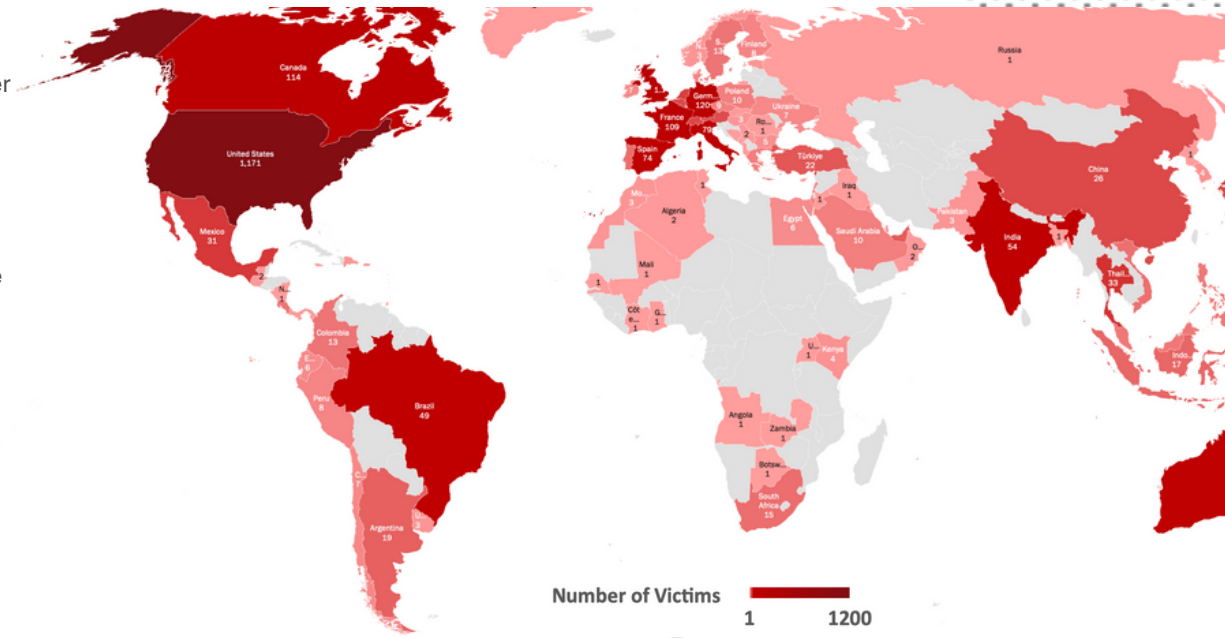


GEOGRAPHIC HOTSPOTS:
RANSOMWARE ATTACKS ACROSS THE GLOBE

Our analysis of the geographic distribution of ransomware victims (Chart 4) reveals key insights regarding the countries most heavily targeted by ransomware groups. Here are some important observations:

- The **United States leads as the top targeted country**, accounting for a staggering **43%** of all victim organizations. The prominence of US-based victims could be attributed to the country's wealth, a large number of organizations with valuable data, or the potential for larger ransom payouts.
- **European countries** also experienced a significant number of attacks, with the UK, Germany, France, Italy, and Spain together making up around **20%** of total victims. This highlights that ransomware groups are actively targeting organizations across Europe, capitalizing on the region's economic importance and interconnected industries.
- Other countries such as Canada, Australia, India, and Brazil are not immune to the threat, with each experiencing a smaller but still notable percentage of ransomware attacks.
- The remaining attacks are distributed across 111 different countries, with less than 35 victims per country. This demonstrates the global reach of ransomware groups and the need for organizations in all regions to prioritize cybersecurity.

Understanding the geographic distribution of ransomware attacks can provide valuable insights for organizations looking to strengthen their defenses against this evolving threat. By recognizing the countries and regions most heavily targeted, organizations can assess their risk profile based on their location and implement appropriate security measures to counter potential ransomware attacks.



NUMBER OF RANSOMWARE VICTIMS IN THE LAST 12 MONTHS BY COUNTRY

CHART 4

RANSOMWARE TARGETS:
REVENUE PROFILE AND RELUCTANCE TO ATTACK LARGE ORGANIZATIONS

Our analysis of ransomware victims' annual revenue distribution (Chart 5), along with factors that influence ransomware groups' targeting decisions, reveals insightful patterns about the types of organizations frequently targeted. Here are some key findings:

- Ransomware groups often target companies with annual revenues of around **$50M to $60M**, as they may have the financial resources to pay ransoms but potentially lack the robust security measures of larger corporations.
- Large organizations with high annual revenues (e.g., more than $100B) are targeted less frequently.
- Smaller organizations with lower revenues are targeted as third-party vendors, allowing ransomware groups to obtain valuable client information for extortion purposes, such as the LockBit ransomware group's alleged attack on a small CNC/Laser cutting vendor to obtain SpaceX engineering drawings.
- According to our Third-Party Breach Report published in January 2023, **ransomware ranks as the second most common root cause of data breaches caused by third parties.**

OPINION: HEAD OF RESEARCH, FERHAT DIKBIYIK

WHY ARE RANSOMWARE GROUPS RELUCTANT TO TARGET VERY LARGE ORGANIZATIONS?

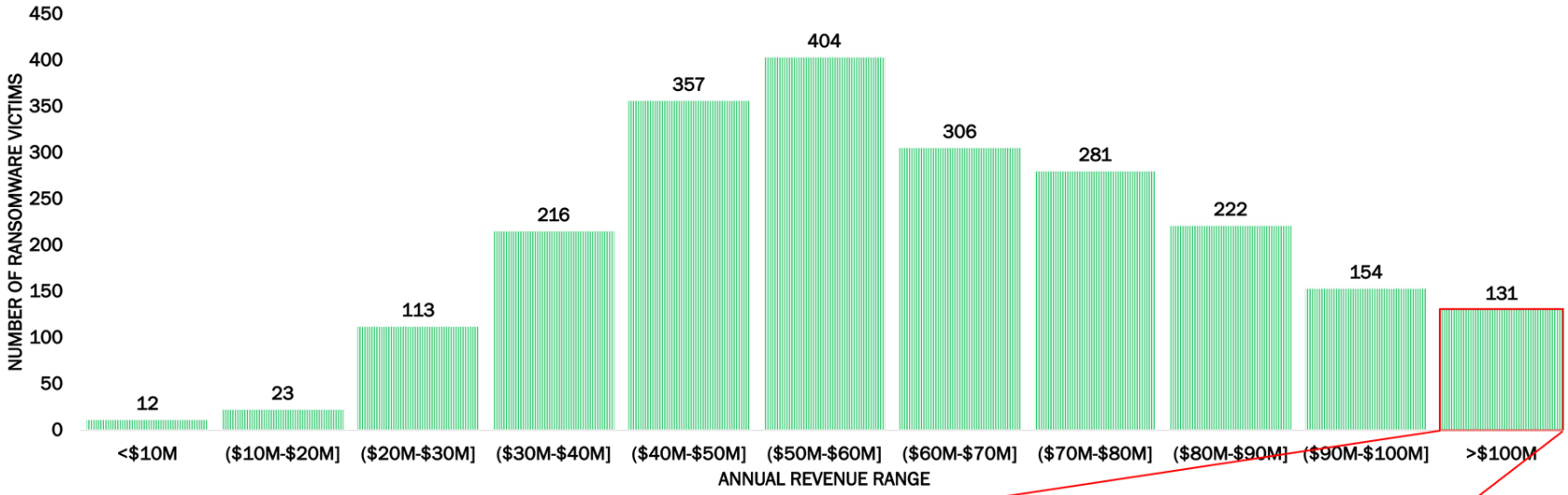
Ransomware groups are often reluctant to target large organizations for several reasons. Large organizations have extensive security infrastructure and resources to combat ransomware threats, but this is not the only reason for the reluctance of ransomware groups.

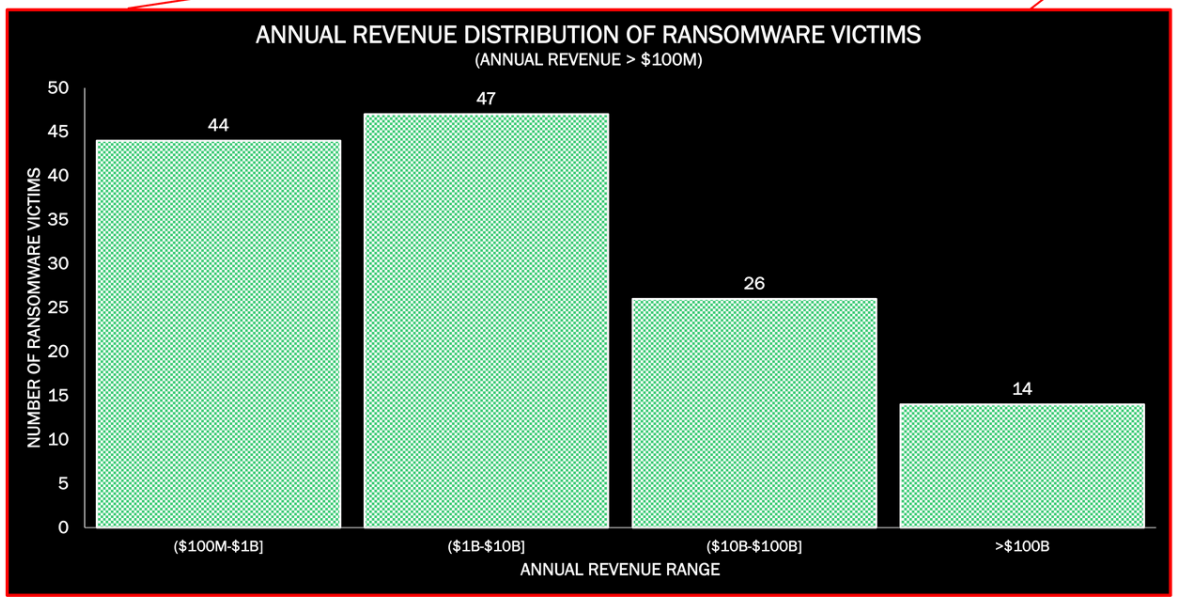
- Ransomware groups may avoid targeting large organizations to prevent significant disruptions that could draw nationwide attention, unwanted publicity, and increased likelihood of a strong law enforcement response.
- High-profile attacks on large organizations, such as Lapsus$ targeting Nvidia with political motivations, are exceptions rather than the norm, as they can draw unwanted attention and prompt stronger countermeasures.
- Unintended consequences, like the Stormous and LockBit ransomware group's recent attack on a hospital's IT system, may lead to apologies from ransomware groups to avoid further scrutiny.
- The Colonial Pipeline attack by the DarkSide ransomware group serves as a cautionary tale, reinforcing the tendency of ransomware groups to avoid targeting large organizations and causing significant disruptions.

Ransomware groups often target smaller organizations or third-party vendors to minimize the risks of attracting unwanted attention and law enforcement responses. By understanding ransomware groups' motivations and reluctance to target large organizations, we can better prepare and protect against the threat landscape.

ANNUAL REVENUE DISTRIBUTION OF RANSOMWARE VICTIMS

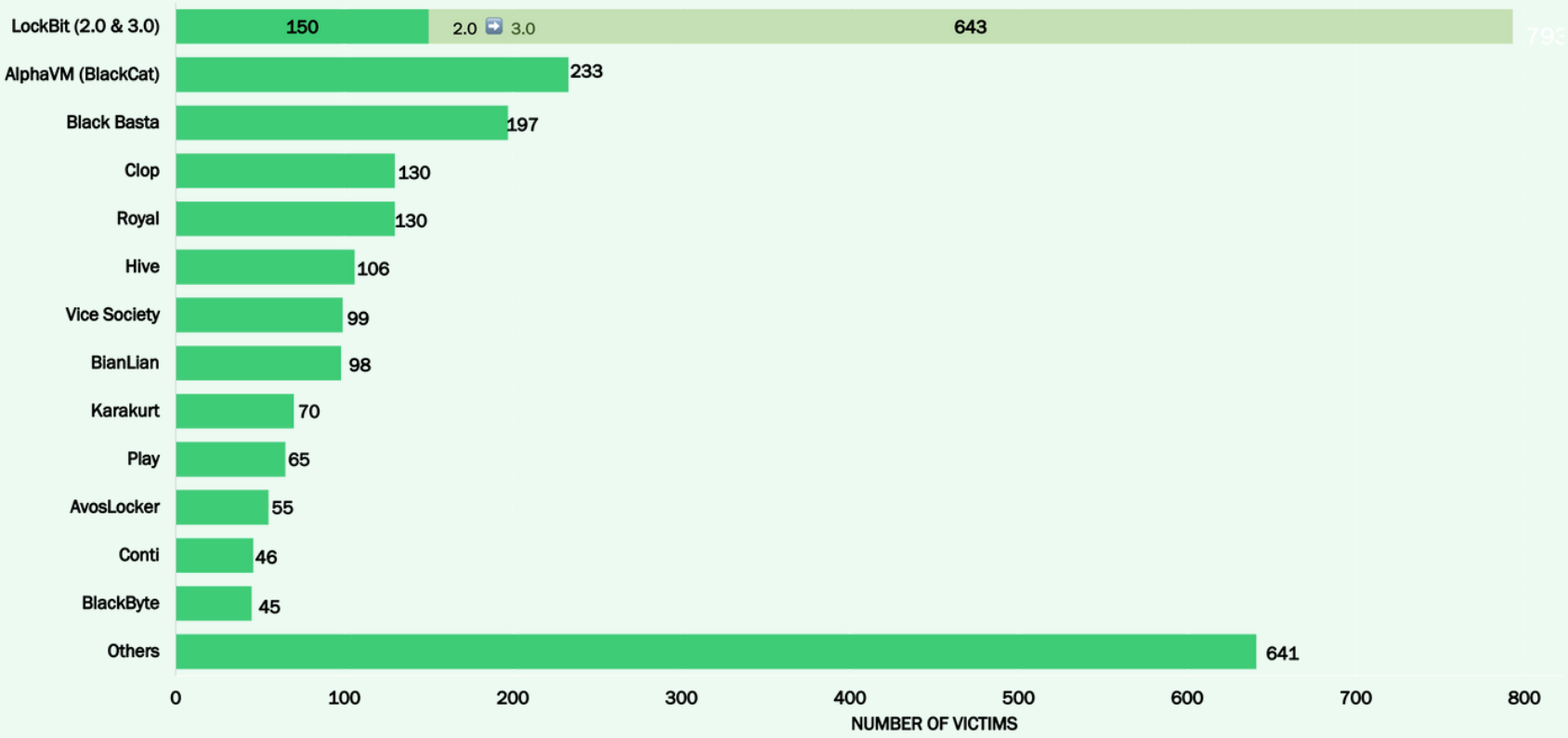
CHART 5





TOP 13 RANSOMWARE GROUPS AND KEY EVENTS:
A 12-MONTH ANALYSIS

Our analysis of the top ransomware groups and their activities over the past 12 months sheds light on the changing threat landscape and reveals important events that have shaped the ransomware ecosystem.



ONE: LOCKBIT (2.0 & 3.0)

LOCKBIT'S DOMINANCE, TARGET PREFERENCES, AND TTPS

LockBit ransomware group, responsible for **29% of attacks** during this period, remains the top ransomware group. Its transition from LockBit 2.0 to LockBit 3.0 in June-July 2022 highlights its ongoing evolution and expansion.

The group mainly targets companies with annual revenues between $40M and $80M, accounting for 60% of its victims. They primarily focus on organizations in the US and Europe, across 75 different countries. Manufacturing and Professional, Scientific, and Technical Services are the top industries targeted, comprising 21% and 19% of its victims, respectively.

LockBit's main TTPs include:

- Exploiting software vulnerabilities using exploit kits, such as unauthenticated remote command execution vulnerabilities in F5's BIG-IP, remote code execution vulnerabilities in Microsoft Exchange Server, vulnerabilities in the Windows Print Spooler service, and vulnerabilities in the Windows Server Message Block (SMB) protocol.
- Utilizing phishing emails to deliver the ransomware payload.
- Employing Remote Desktop Protocol (RDP) to gain access to victims' computers.

LockBit's sophistication and organization are evident through its dedicated teams of hackers and operators responsible for ransomware development, deployment, and negotiation with victims. The group views ransom demands as payments for their "post-paid services" and sees itself as a business rather than a criminal operation*.

In a record-breaking incident this year, LockBit demanded an $80 million ransom from the UK's largest shipping organization. After the ransom was rejected, the group leaked files and negotiation chat history, showcasing their determination and ruthlessness.

*This is a statement based on an interview with the leader of the LockBit group and published negotiation chats.

TWO: ALPHAVM (BLACKCAT)

RUNNER-UP

Responsible for **8.6% of attacks, AlphaVM (BlackCat)**, also known as AlphaV, LPHV, ALPHV-ng, or Noberus, ranks as the second most active ransomware group over the past 12 months. Emerging in November 2021, BlackCat is an apparent descendant of the BlackMatter (a possible rebrand of DarkSide) ransomware group.

BlackCat possesses the knowledge to exploit various vulnerabilities, including a privilege escalation vulnerability in older versions of Microsoft Windows, an SQL injection vulnerability in SonicWall Secure Remote Access devices, and critical vulnerabilities known as ProxyShell in Microsoft Exchange Server.

According to our analysis, 55% of BlackCat's victims are U.S. organizations, with the full victim list spanning 44 different countries. The group primarily targets Professional, Scientific, and Technical Services (27% of its victims) and Manufacturing (12%). Over half of its victims report annual revenues between $40M and $70M.

THREE: BLACK BASTA

KEY STATS AND TACTICS

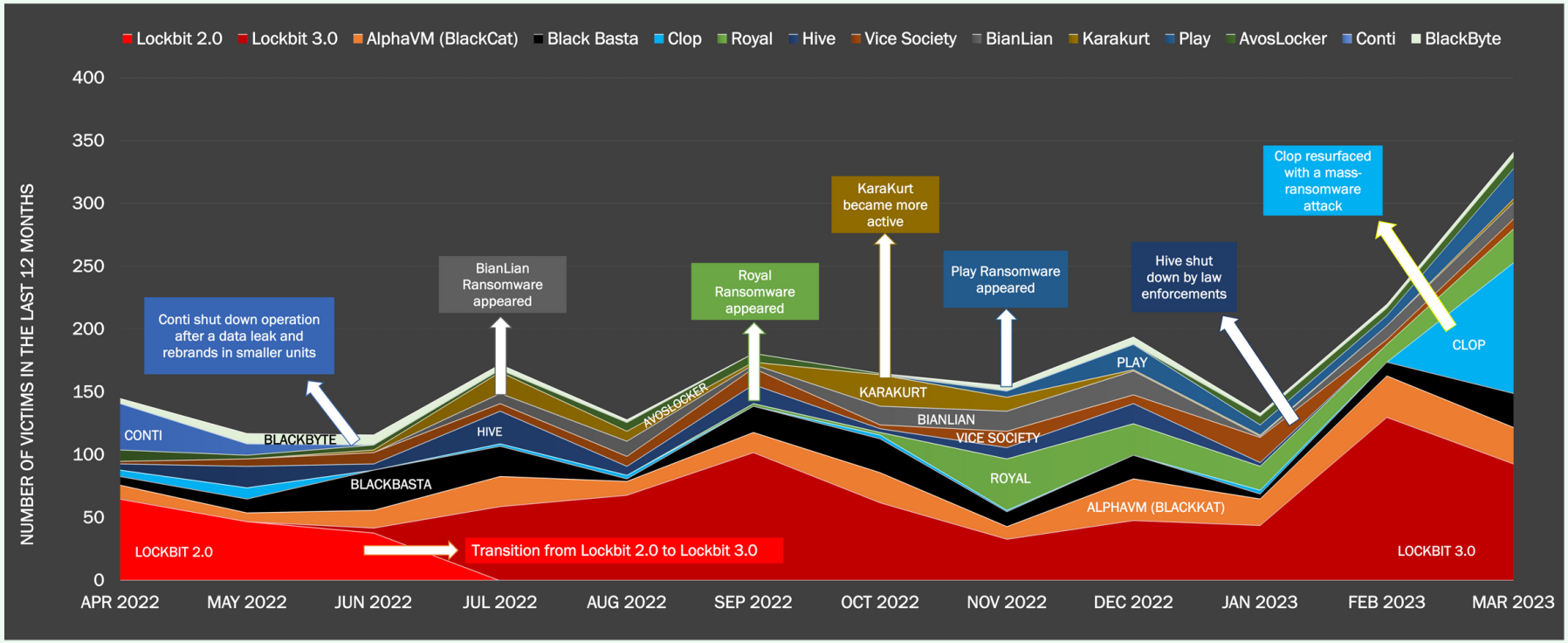
Black Basta, a ransomware-as-a-service (RaaS) group responsible for **7.2% of attacks,** emerged in early 2022. The group employs double-extortion tactics and tools like the Qakbot trojan and PrintNightmare vulnerability.

Notably, the American Dental Association fell victim to an attack, with its stolen data later appearing on Black Basta's leak site. Black Basta has also developed a Linux build of its ransomware capable of encrypting VMware ESXi virtual machines.

The group's activities are concentrated within 15 countries, with 67% of victims in the U.S. and 31% in Europe. Manufacturing (39%) and Retail Trade (16%) are the most targeted industries, and 60% of its victims report annual revenues between $40M and $70M.

NUMBER OF RANSOMWARE VICTIMS

WITH THE TIMELINE OF THREAT ACTORS



FOUR: CLOP

RESURFACE WITH MASS-RANSOMWARE ATTACKS

Clop ransomware group, responsible for **4.8% of attacks,** has been active since at least 2019. The group resurfaced in March 2023, launching a mass-ransomware campaign that exploited a high-severity Fortra GoAnywhere vulnerability. In March alone, they announced over 100 victims. Previously, in December 2020, they exploited an Accellion FTA zero-day vulnerability, stealing data from approximately 100 companies.

High-profile victims include energy giant Shell, supermarket chain Kroger, cybersecurity firm Qualys, and several universities worldwide. In June 2021, an international law enforcement operation, Operation Cyclone, led to the arrest of six money launderers linked to the group.

Clop focuses on hit-and-run mass-ransomware attacks, exploiting large-scale vulnerabilities without targeting specific organizations. Their use of Accellion in 2020 and GoAnywhere in 2023 vulnerabilities demonstrate their opportunistic approach, which also explains their on-and-off presence in the ransomware landscape.

FIVE: ROYAL

A NEW PLAYER IN TOWN

Initially dubbed as "Zeon" before its rebranding to "Royal" in September 2022, the **Royal** ransomware group has quickly gained traction, accounting for **4.8% of attacks.** Backed by Conti threat actors, Royal uses a mix of old and new techniques, including callback phishing and intermittent encryption.

Most of Royal's victims are U.S. companies (66%), followed by European companies (22%). The top targeted industry is Professional, Scientific, and Technical Services (23%). A majority of victims have annual revenues between $40M and $70M. The group has swiftly adapted to new tactics, developing Linux-based variants targeting ESXi servers, impacting enterprise data centers and virtualized storage.

SIX: HIVE

RISE AND FALL OF A PROMINENT RANSOMWARE GROUP

Hive ransomware group, responsible for **3.9% of attacks,** was launched in June 2021 as a Ransomware-as-a-Service operation. It quickly became one of the most active ransomware groups, extorting around $100 million from over 1,500 companies. Hive's well-known attack on Lake Charles Memorial Health System in October 2022 resulted in a data breach affecting almost 270,000 people.

In January 2023, an international law enforcement operation shut down Hive by seizing its Tor websites. Although no arrests were made, the operation secretly hacked the group's servers in July 2022, monitoring communications, intercepting decryption keys, and helping victims with free decryptors. This dealt a significant blow to a prominent player in the cybercrime space, preventing $100 million in ransom payments.

SEVEN: VICE SOCIETY

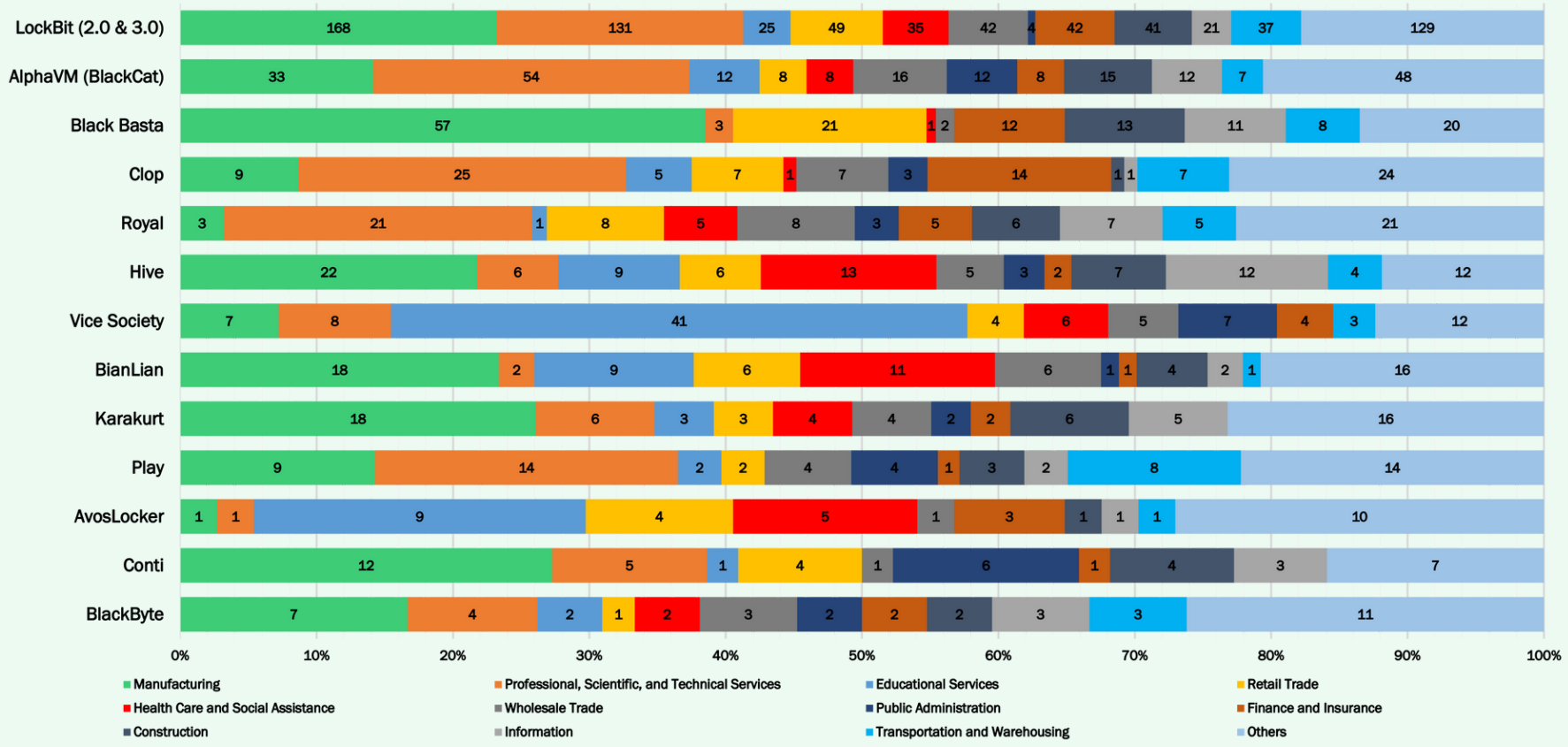
FOCUSED ON EUROPE AND EDUCATION

Accounting for **3.6% of attacks, Vice Society** stands apart from other top ransomware groups mentioned in the report, as it primarily targets European organizations and the Education sector. Initially known for exploiting the PrintNightmare vulnerability and deploying ransomware variants like Hello Kitty/Five Hands and Zeppelin, the group has since developed its custom ransomware builder and adopted more robust encryption methods. These advancements may indicate that Vice Society is preparing to launch its Ransomware-as-a-Service (RaaS) operation.

With 43% of its victims in the Education sector, Vice Society also targets Professional, Scientific, Technical Services, Manufacturing, and Public Institutions. Half of its victims are European organizations, while 32% are in the U.S.

INDUSTRY DISTRIBUTION

OF VICTIMS FOR EACH RANSOMWARE GROUP



EIGHT: BIANLIAN

SWIFT RISE AND ENCRYPTION-LESS EXTORTION

Emerging in July 2022, **BianLian** ransomware group quickly accounted for **3.6% of attacks.** The group soon shifted focus from encrypting files to an encryption-less extortion model, threatening to leak stolen data instead. BianLian commonly targets the ProxyShell vulnerability chain, SonicWall VPN devices, and remote network access solutions like Remote Desktop.

The group predominantly targets the Manufacturing (24%) and Healthcare (15%) sectors. Although victims have been reported in 18 different countries, 62% are located in the U.S., followed by 11% in Europe.

NINE: KARAKURT

DATA EXTORTION ARM OF CONTI SYNDICATE

Responsible for **2.6% of attacks, Karakurt** ransomware group increased its activity around October 2022. Like BianLian, Karakurt focuses solely on data theft and extortion, auctioning or leaking stolen data if the ransom is not paid. According to several reports, Karakurt is operationally linked to both Conti and Diavol ransomware groups.

Karakurt, active since June 2021, began actively extorting in September 2021, targeting many organizations across multiple industries within two months. While the group has targeted victims in 20 countries in the last 12 months, 62% are located in North America. Although 26% of victims are in Manufacturing, Karakurt shows no specific industry preference.

OPINION: THE RISE OF ENCRYPTION-LESS RANSOMWARE, A NEW CHAPTER IN CYBER EXTORTION

Ransomware attacks have long dominated the cybersecurity landscape. However, a new trend is emerging: encryption-less ransomware. Some ransomware groups, such as BianLian and Karakurt, have shifted their focus to holding data hostage without resorting to encryption.

Why the change in tactics? As regulatory fines on data protection increase, data breaches become an attractive target for ransomware operators. By threatening to leak sensitive data, they can pressure victims to pay the ransom, even if they have strong backup and recovery systems in place. Ransomware groups may also want to avoid causing unintended business interruption and attracting unwanted international law enforcement attention by disrupting critical infrastructure.

To address this evolving threat landscape, ransomware prevention now requires a dual approach. Organizations both ensure robust backup and recovery processes and also prioritize data protection to avoid regulatory penalties and reputational damage.

TEN: PLAY

EMERGING RANSOMWARE GROUP TARGETING EUROPE

Appearing in June 2022 and becoming more visible in November 2022, **Play** ransomware group is responsible for **2.4% of attacks.** The group has targeted numerous organizations, including the City of Oakland, Antwerp, H-Hotels, Rackspace, Arnold Clark, and A10 Networks. Play's behavior and tactics resemble those of Hive and Nokoyawa ransomware, using similar file names and paths for their tools and payloads.

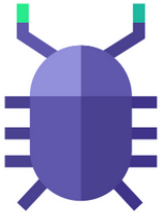
Play's infection chain includes exploiting compromised valid accounts or unpatched Fortinet SSL VPN vulnerabilities to access organizational networks. By the end of December 2022, Play was observed exploiting two ProxyNotShell vulnerabilities in Microsoft Exchange for initial access. Notably, Play has announced more victims in Europe than the U.S., with 52% of victims located in Europe.

ELEVEN: AVOSLOCKER

RAAS-FORWARD

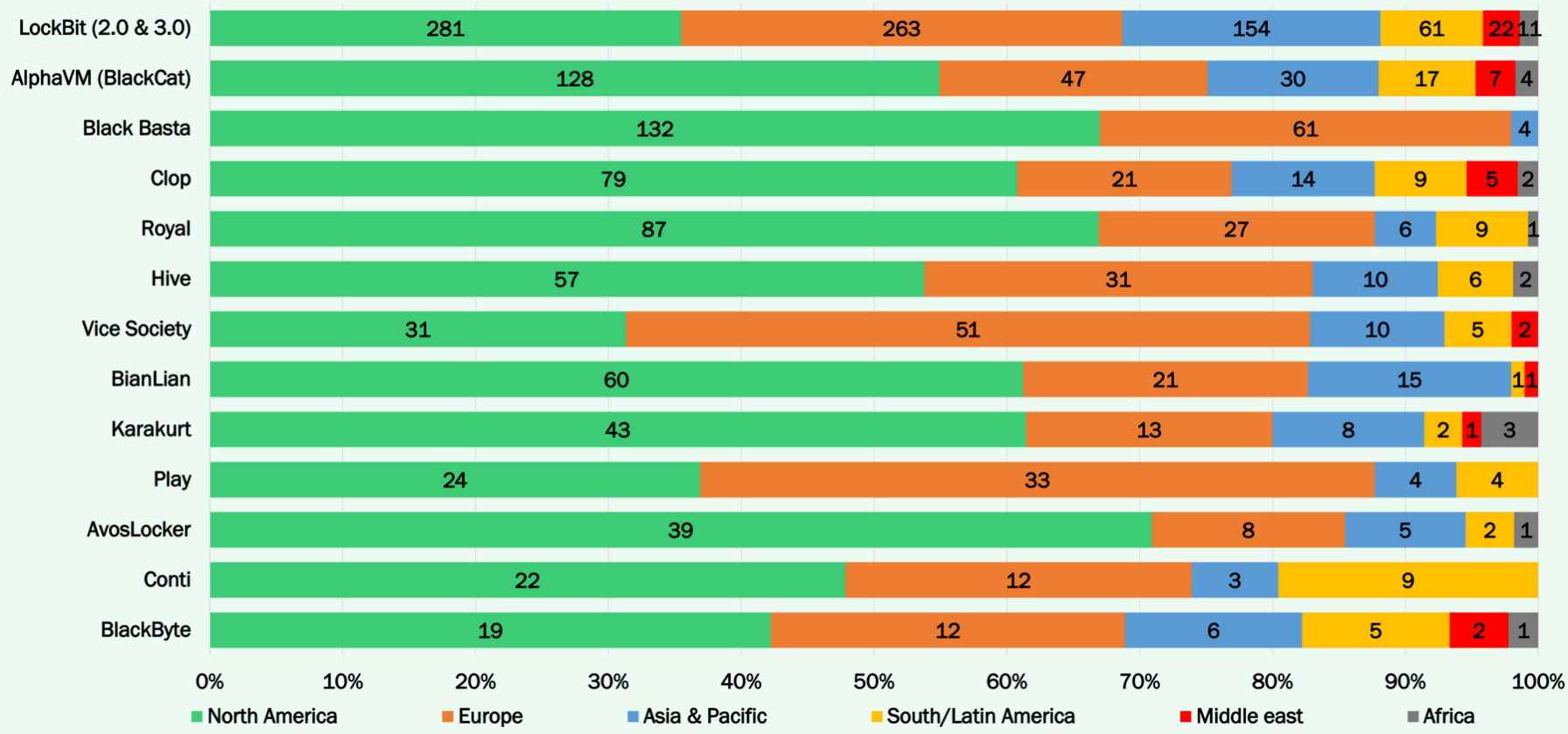
Accounting for **2.0% of attacks, AvosLocker** is an affiliate-based Ransomware-as-a-Service (RaaS) group. The FBI issued a warning in March 2022 about the group targeting victims across multiple critical infrastructure sectors in the United States, including Financial Services, Critical Manufacturing, and Government Facilities.

In June 2022, the group exploited a remote code execution (RCE) vulnerability in Atlassian Confluence Server and Data Center instances for initial access. Later, in December 2022, Kroll identified new tactics targeting backup systems used by AvosLocker-associated threat actors. They attempted to leverage vulnerabilities in Veeam Backup and Replication software (CVE-2022-26500 and CVE-2022-26501) for possible data exfiltration. AvosLocker has announced more victims in the Education sector than any other industry, with over 70% of victims located in the U.S.



REGIONAL DISTRIBUTION

OF VICTIMS FOR EACH RANSOMWARE GROUP



TWELVE: CONTI

A DISMANTLED CYBERCRIME SYNDICATE

Responsible for **1.7% of attacks, Conti** ransomware group shut down its operations in June 2022 after a data leak caused by a rival group, and rebranded into smaller units. Conti is a Russian ransomware operation, originally launched in the summer of 2020. They quickly gained notoriety for their high-profile attacks against the City of Tulsa, Broward County Public Schools, Advantech, Ireland's Health Service Executive (HSE), and the Department of Health (DoH). Over time, Conti evolved into a cybercrime syndicate, taking over the development of various malware operations, including TrickBot and BazarBackdoor.

In May 2022, Conti began shutting down its operations while leaving behind a facade of an active operation. However, the Conti brand's shutdown did not signal the end of the cybercrime syndicate. Instead, the gang members split into smaller cells that infiltrated or took over other ransomware operations, remaining loyal to the central syndicate managed by a small group of managers. By spreading members among multiple groups, the operation became more resilient against law enforcement takedowns.

Now, former Conti members are known to be involved in various ransomware gangs, including Hive, AvosLocker, BlackCat, Hello Kitty, and the revitalized Quantum operation. Additionally, some members have launched their own data extortion operations that do not encrypt data, such as Karakurt and the Bazarcall collective.

THIRTEEN: BLACKBYTE

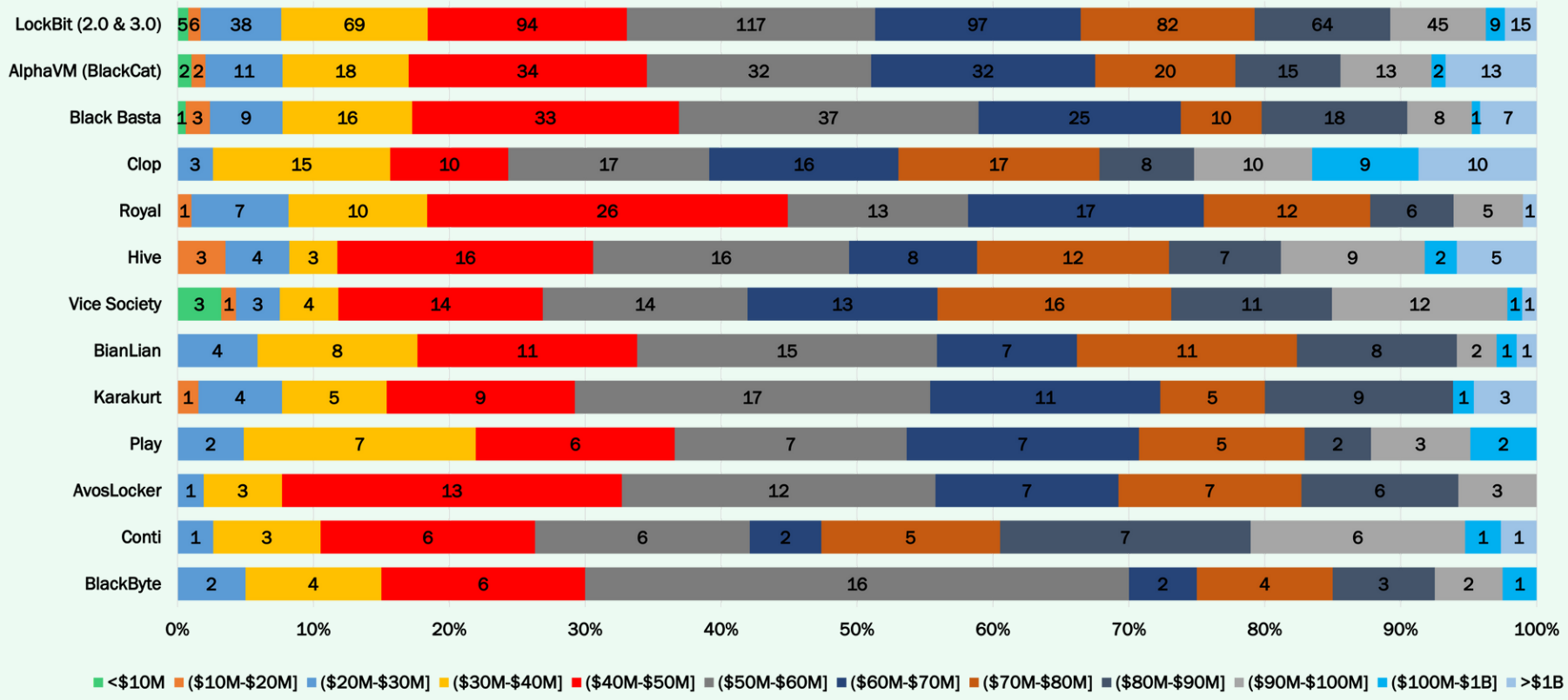
ANOTHER CONTI-RELATED GROUP

Accounting for **1.7% of attacks, BlackByte** ransomware group, like Karakurt, emerged from Conti's data extortion arm. Unlike Karakurt, the group still operates with double extortion. BlackByte ransomware group emerged in summer 2021 and has since targeted organizations across various industries, including critical infrastructure in the United States. The group's recent attacks exploit last year's ProxyShell and ProxyLogon flaw sets in Microsoft Exchange servers, using tools like AdFind, AnyDesk, NetScan, and PowerView for lateral movement.

BlackByte employs version 2.0 of the ransomware, which removes Kernel Notify Routines to bypass EDR protections, as revealed in an October report by Sophos. The group follows typical ransomware tactics, such as deleting volume shadow copies to prevent easy data restoration, modifying firewall settings to allow remote connections, and injecting itself into a "scvhost.exe" instance for the encryption phase. BlackByte has a broad target range, with 42% of its victims in the last 12 months located in the U.S. and 27% in Europe, spanning various industries.

ANNUAL REVENUE DISTRIBUTION

OF VICTIMS FOR EACH RANSOMWARE GROUP



IN SUMMARY

TOP RANSOMWARE GROUPS AND KEY EVENTS: A 12-MONTH ANALYSIS

In summary, the ransomware landscape remains a significant and evolving threat to organizations across industries and regions. The top ransomware groups, as discussed in the subsections above, showcase the diverse tactics, attack vectors, and targeted sectors. Despite the differences in their approaches, these groups share a common goal of causing significant disruption and financial gain.

The table provided offers a comprehensive overview of the most targeted industries, regions, and annual revenue ranges for each group, highlighting the importance of understanding the specific threats posed by these groups. Organizations need to stay informed about these evolving threats and adopt proactive cybersecurity measures to mitigate the risks associated with ransomware attacks.

Overall, it is crucial for businesses to prioritize security, continuously update and patch their systems, and invest in employee education to prevent these ransomware groups from causing further damage. As these groups continue to adapt their tactics and focus on new targets, the collaboration between organizations, cybersecurity professionals, and law enforcement will be essential in combating the growing ransomware threat.

Ransomware Group	Most Targeted Industry	Most Targeted Region	Most Targeted Annual Revenue
LockBit (2.0 & 3.0)	Manufacturing	North America	($50M-$60M]
AlphaVM (BlackCat)	Professional, Scientific, and Technical Services	North America	($40M-$50M]
Black Basta**	Manufacturing	North America	($50M-$60M]
Royal**	Professional, Scientific, and Technical Services	North America	($40M-$50M]
Hive*	Manufacturing	North America	($40M-$50M]
Vice Society	Educational Services	Europe	($70M-$80M]
BianLian**	Manufacturing	North America	($50M-$60M]
Karakurt	Manufacturing	North America	($50M-$60M]
Royal**	Professional, Scientific, and Technical Services	North America	($40M-$50M]
Play**	Professional, Scientific, and Technical Services	Europe	($30M-$40M]
AvosLocker	Educational Services, Distributed	North America	($40M-$50M]
Conti*	Manufacturing	North America	($80M-$90M]
BlackByte	Distributed	North America	($50M-$60M]

(*) Inactive
(**) Appeared in the last 12 months

RANSOMWARE INDICATORS IN VICTIMS - BLACK KITE INSIGHTS

Black Kite is a vendor risk intelligence platform that continuously monitors hundreds of thousands of companies from an outside-in hacker-perspective mindset to provide an external cyber risk assessment for organizations and their vendors.

By leveraging the insights obtained from Black Kite, we have analyzed the ransomware indicators in victims (Chart 6) to identify common vulnerabilities that ransomware groups exploit. Understanding these indicators can help organizations identify potential weaknesses and take preventive measures to protect their systems and networks against ransomware attacks.

- **Poor Email Configuration (67%):** A significant majority of victims had poor email configurations, such as missing DMARC records. This can lead to successful phishing and spear-phishing campaigns, allowing attackers to gain an initial foothold in the organization's network. Ensuring proper email configurations, including implementing DMARC, DKIM, and SPF, is essential in mitigating the risk of email-based attacks.

- **Leaked Credentials (62%):** More than half of the victims had at least one credential leaked in the 90 days preceding the attack. Leaked credentials can provide attackers with easy access to systems and networks, enabling them to bypass security controls and move laterally within the organization. Regular monitoring for leaked credentials and implementing strong password policies, multi-factor authentication, and employee education can help prevent unauthorized access.

- **Public Remote Access Ports (42%):** A significant number of victims had at least one public remote access port open. Open remote access ports can expose organizations to attacks, as cybercriminals can exploit these vulnerabilities to gain unauthorized access to systems and networks. Regularly scanning for open ports, restricting remote access to necessary personnel, and using VPNs with strong authentication can reduce the risk of unauthorized access.

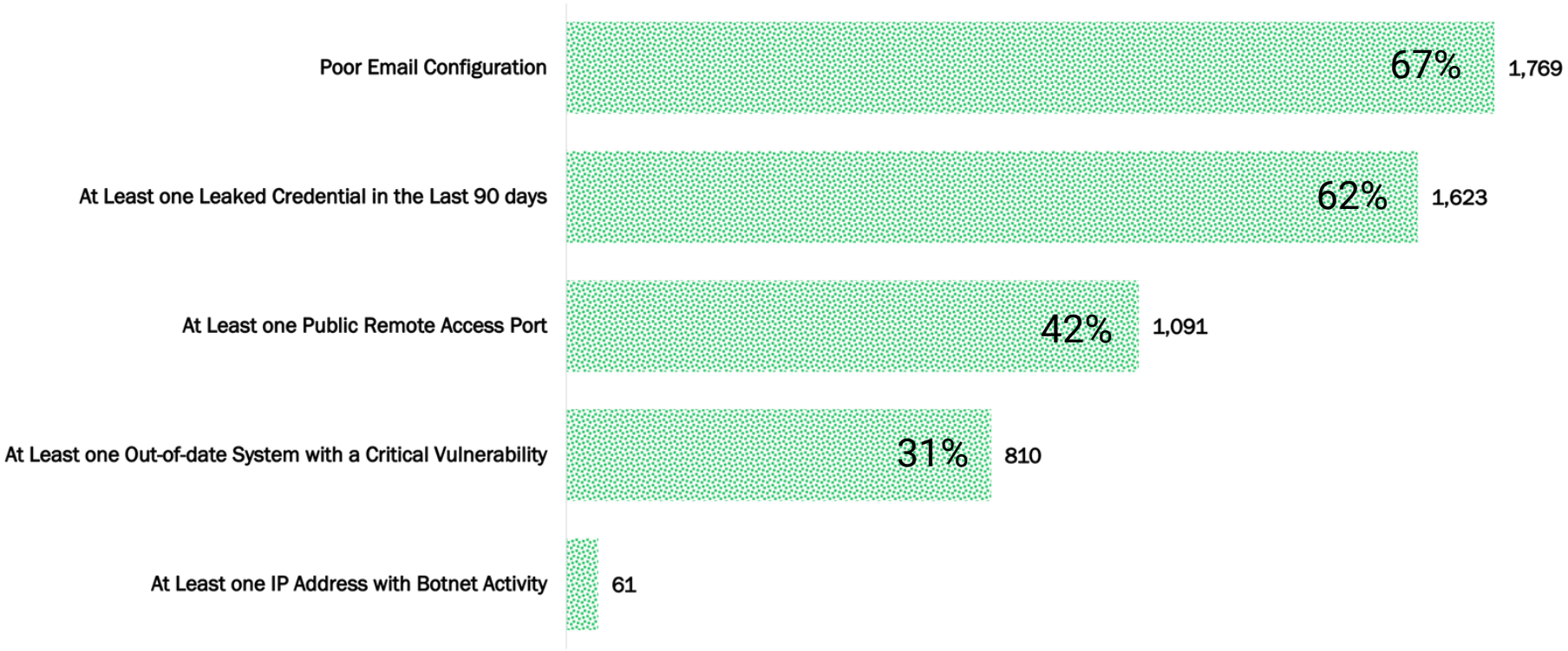
- **Out-of-date Systems (31%):** Nearly a third of the victims had publicly visible out-of-date systems with potential critical vulnerabilities. Outdated systems can be easily exploited by attackers, who take advantage of known vulnerabilities to infiltrate networks and deliver ransomware payloads. Regularly updating and patching systems, prioritizing critical vulnerabilities, and maintaining a robust vulnerability management program can help organizations stay protected against ransomware attacks.

Organizations must be aware of these ransomware indicators and take proactive measures to address the vulnerabilities. By doing so, they can significantly reduce the risk of falling victim to ransomware attacks and minimize the impact on their operations, reputation, and bottom line. It's crucial to note that many ransomware victims are also third-party vendors of other organizations.

Monitoring ransomware indicators on third parties is equally important, as it helps reduce the likelihood of being targeted by ransomware due to a compromised third-party vendor. Implementing a comprehensive third-party risk management program, including continuous monitoring of vendors' cybersecurity posture, can help organizations better understand and mitigate the risks associated with their supply chain and protect their sensitive data and systems.

RANSOMWARE INDICATORS IN VICTIMS

CHART 6



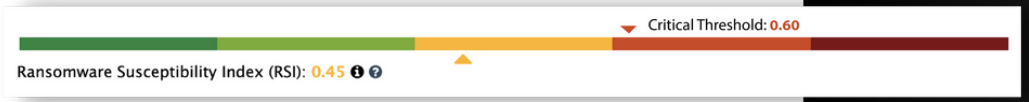
HOW SUSCEPTIBLE WERE RANSOMWARE VICTIMS BEFORE THE ATTACK?

In today's rapidly evolving threat landscape, organizations must remain vigilant against the growing risk of ransomware attacks. Black Kite's Ransomware Susceptibility Index™ (RSI™) is a valuable metric designed to assess the likelihood of an organization experiencing a ransomware attack.

By analyzing various indicators such as open critical ports, vulnerabilities with remote code execution, leaked credentials, email security, phishing/fraudulent domains, endpoint security, susceptibility following a ransomware incident, company country, company size, and company industry, RSI™ offers crucial insights into potential weaknesses and helps organizations prioritize their cybersecurity efforts.

When examining ransomware victims' RSI™ values (Chart 7), **716 received a value between 0.2 and 0.4,** 1,227 received a value between 0.4 and 0.6, 542 received a value between 0.6 and 0.8, and 138 received a value between 0.8 and 1.0. Over **70% of these victims had an RSI value above the high-risk threshold of 0.4,** with many over the critical threshold of 0.6, highlighting the importance of proactively addressing vulnerabilities.

Most victims who received low RSI values (e.g., below 0.4) are companies with very limited external-facing assets.



However, it is important to note that our methodology has its limits; we can only assess internet-facing assets, and we cannot account for some other ransomware attack vectors such as obtaining access information through social engineering with personal communication channels or insider threats.

It is crucial to note that many ransomware victims are also third-party vendors for other organizations. Monitoring ransomware indicators on third parties is essential to reduce the risk of being targeted by ransomware due to a third-party vendor's vulnerabilities.

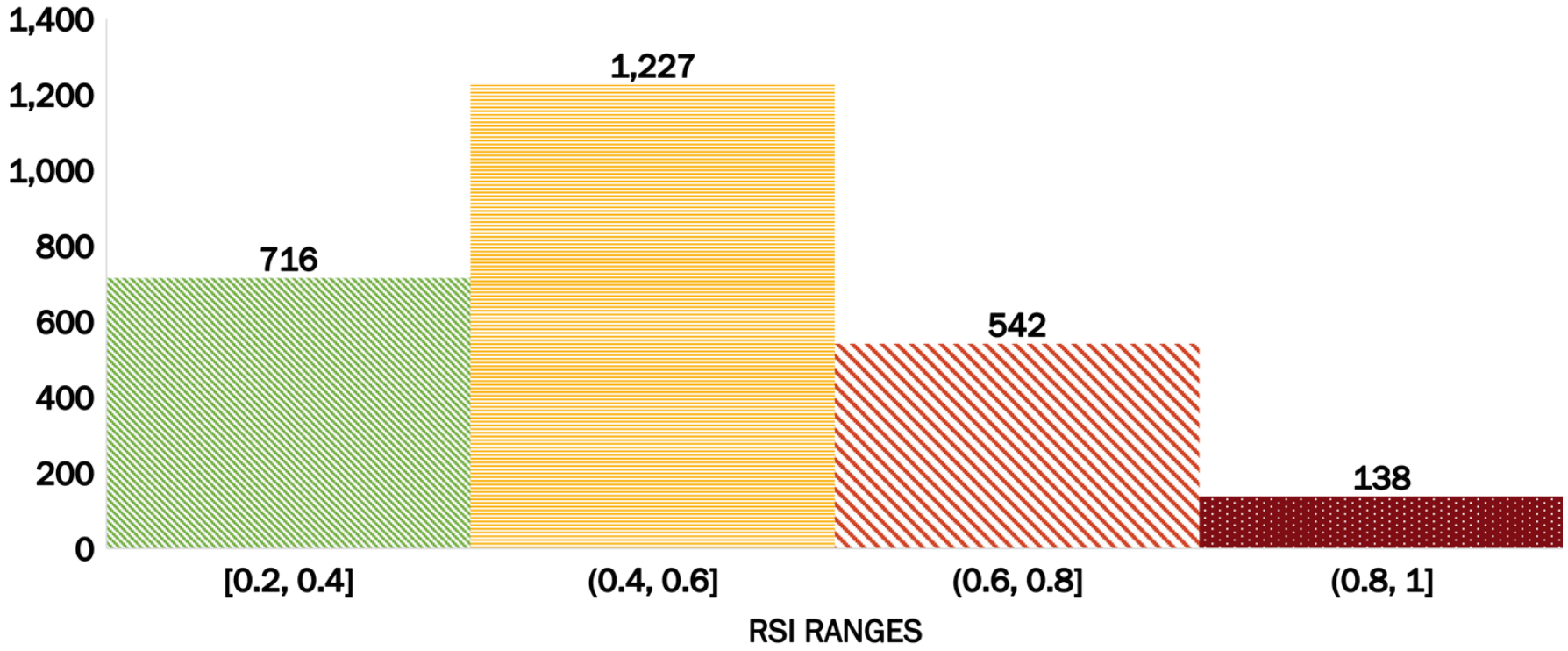
Take advantage of Black Kite's vendor risk intelligence platform and RSI™ metric to significantly reduce your organization's likelihood of falling victim to ransomware attacks, ensuring the protection of your critical data and operations. Gain valuable insights into your risk exposure and take the necessary steps to safeguard your organization against ransomware attacks. Don't leave your organization's cybersecurity to chance.

Take action now.

REQUEST A FREE RSI™ RATING

RSI™ DISTRIBUTION OF RANSOMWARE VICTIMS

CHART 7



RANSOMWARE PREVENTION AND RESPONSE:
RECOMMENDATIONS FOR ORGANIZATIONS

Ransomware attacks are evolving, and it is crucial to understand that they involve both data encryption and data breaches. Data encryption can cause significant business interruption, especially if proper backups are not in place or if recovering systems from backups takes a substantial amount of time. Furthermore, with the increasing regulatory fines for data protection breaches, data breaches can result in substantial financial penalties for companies.

Ransomware groups are well aware of this and leverage this information during negotiations. Some groups, like BianLian and Karakurt, have even shifted towards encryption-less ransomware, focusing more on holding data hostage.

With this in mind, we provide recommendations for several phases to help organizations better prepare for, respond to, and recover from ransomware attacks.

PREVENTION AND MINIMIZING RANSOMWARE RISK

INTERNAL SECURITY MEASURES FOR RANSOMWARE PREVENTION

MONITOR YOUR RANSOMWARE INDICATORS

Keep track of your ransomware indicators to avoid being on the radar of ransomware groups. Regularly check for open critical ports, leaked credentials, email security configurations, and phishing/fraudulent domains.

PATCH MANAGEMENT

Ensure all systems, applications, and software are up-to-date with the latest patches, focusing on those with known remote code execution vulnerabilities.

ENDPOINT SECURITY

Implement strong endpoint security measures, including antivirus and anti-malware software, and consider deploying advanced solutions like micro VMs to prevent malware from spreading.

NETWORK SECURITY

Restrict remote access to your network by closing unnecessary ports, using VPNs, and employing strong authentication methods like multi-factor authentication (MFA).

INCIDENT RESPONSE PLAN

Develop and maintain a comprehensive incident response plan to address potential ransomware attacks, including clear roles and responsibilities, communication protocols, and recovery strategies.

EMAIL SECURITY

Strengthen your email security by implementing SPF, DKIM, and DMARC records, and conduct regular security awareness training to educate employees on how to identify and report phishing attempts.

DATA AND SYSTEM BACKUP

Regularly back up critical data and systems to allow for quick recovery in the event of an attack. Store backups both on-site and off-site, and consider using air-gapped storage for added protection. Test your backup and recovery processes periodically to ensure their effectiveness.

By implementing these internal security measures, you can reduce the likelihood of falling victim to a ransomware attack and minimize the potential damage if an attack does occur.

MITIGATING THIRD-PARTY RANSOMWARE RISK

TO MITIGATE THE RISK OF RANSOMWARE ATTACKS DUE TO THIRD-PARTY VENDORS, ORGANIZATIONS SHOULD:

1. **Evaluate the cybersecurity posture of third-party vendors using tools like Black Kite's Ransomware Susceptibility Index™ (RSI™).**

2. **Require vendors to adhere to industry best practices and implement robust cybersecurity measures.**

3. **Perform regular audits of vendors' security practices and provide guidance for improvement if necessary.**

4. **Foster a culture of collaboration and information sharing among vendors to enhance overall cybersecurity.**

RESPONDING TO A RANSOMWARE ATTACK

IN THE EVENT OF A RANSOMWARE ATTACK, TAKING IMMEDIATE ACTION IS CRITICAL TO MITIGATE THE DAMAGE.

STEPS TO TAKE WHEN HIT BY A RANSOMWARE ATTACK INCLUDE:

1. **Isolate affected systems to prevent the spread of the ransomware.**

2. **Notify relevant authorities and stakeholders.**

3. **Engage with cybersecurity experts to assess the situation and explore potential remediation options.**

4. **Preserve evidence and document the incident for future reference and potential legal actions.**

POST-ATTACK RECOVERY

AFTER A RANSOMWARE ATTACK, IT IS CRUCIAL TO LEARN FROM THE EXPERIENCE AND STRENGTHEN YOUR ORGANIZATION'S CYBERSECURITY DEFENSES.

POST-ATTACK STEPS INCLUDE:

1. **Conduct a thorough analysis of the incident to identify root causes and vulnerabilities.**

2. **Implement recommended security measures to prevent similar attacks in the future.**

3. **Review and update your incident response plan based on the lessons learned.**

4. **Share information about the attack with relevant parties and collaborate with industry peers to improve overall cybersecurity.**

By understanding the complex nature of ransomware attacks and taking a proactive approach to prevention, response, and recovery, your organization can significantly reduce the likelihood of falling victim to ransomware and better protect its critical data and operations.

IN CONCLUSION
RANSOMWARE RISK: STAYING ONE STEP AHEAD

In this report, we've explored the current state of ransomware attacks, delving into the tactics and targets of the most notorious ransomware groups. We've discovered that organizations of all sizes and industries can fall victim to ransomware attacks, with many becoming collateral damage due to third-party vendor breaches.

Through our analysis, we've identified key ransomware indicators and demonstrated the importance of proactively monitoring and addressing them, both internally and externally. By utilizing Black Kite's Ransomware Susceptibility Index™ (RSI™) metric, organizations can better understand their susceptibility to ransomware attacks and take appropriate actions to mitigate risk.

We've provided recommendations for mitigating ransomware risk in three phases: prevention, response, and recovery. By implementing a combination of internal security measures and third-party risk management, organizations can stay off the radar of ransomware groups, protect sensitive data, and minimize the potential damage caused by ransomware attacks.

In the face of an evolving threat landscape, it's crucial to stay vigilant and continuously improve your cybersecurity posture. Black Kite's vendor risk intelligence platform offers comprehensive insights and actionable recommendations to help organizations stay one step ahead of ransomware threats. Don't wait for a ransomware attack to happen—take control of your cybersecurity today by requesting a free RSI™ score for your organization.

REQUEST A FREE RSI™ RATING

ABOUT BLACK KITE

One in four organizations suffered from a cyber attack in the last year, resulting in production, reputation, and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective.

With 500+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: technical, financial, and compliance.

CONTACT US

info@blackkite.com

800 Boylston Street, Suite 2905
Boston, MA 02199

www.blackkite.com