SOCRadar®
Your Eyes Beyond

RANSOMWARE

Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

January 2023: UK's Royal Mail Targeted by LockBit

- The UK's national postal service, Royal Mail, was targeted by the LockBit group. Ransom was requested, but Royal Mail refused to pay.

February 2023: ESXiArgs Ransomware

- An attack, leaving numerous VMware ESXi servers encrypted, occurred through the RCE vulnerability CVE-2021-21974 in VMware ESXi servers.

April 2023: NCR Ransomware Attack by ALPHV Blackcat

- NCR, a financial services firm, was hit by ALPHV Blackcat ransomware, which disrupted payment processing systems.

May 2023: CL0P Ransomware Exploits MOVEit Vulnerability

- Hundreds of companies were impacted after the CL0P ransomware gang exploited a known SQL injection vulnerability in the MOVEit Transfer software.

June 2023: Taiwan Semiconductor Manufacturing Company Targeted by LockBit

- Taiwan Semiconductor Manufacturing Company, the world's biggest chipmaker, appeared on the website of LockBit 3.0.

August 2023: Rhysida on an attack spree

- The Rhysida group targeted many organizations in Europe and the Middle East. Critical infrastructure such as power plants, hospitals, and public institutions were attacked.

September 2023: Vegas Hit

- MGM and Caesars Entertainment were targeted by Scattered Spider / ALPHV, resulting in tens of millions in losses.

September 2023: Sony Got Hit Twice

- RansomedVC alleged they had breached the company's systems and threatened to sell the stolen data, but their claims were overstated.
- Sony was listed on the website of the Cl0p ransomware group after they exploited a 0-day in MOVEit Secure Managed File Transfer Software.

October-November 2023: LockBit Targeted Boeing

- In late October 2023, LockBit announced an attack on Boeing and threatened to publish data if the ransom was not paid by November 2, which Boeing refused to pay.

December 2023: ALPHV Blackcat infrastructure seized by law enforcement

- The ALPHV Blackcat ransomware group lost control over its infrastructure thanks to a joint operation by the U.S. Department of Justice, the FBI, Europol, and law enforcement agencies of several European states.

February 2024: Change Healthcare Attack

- UnitedHealth Group has confirmed a cyberattack on its Change Healthcare unit. The ALPHV Blackcat ransomware group is allegedly responsible for the attack.

May 2024: LockBit Revealed

- The person behind the LockBit ransomware was revealed by law enforcement and identified as an individual named Dmitry Yuryevich Khoroshev (Дмитрий Юрьевич Хорошев) from Russia.

Top Takeaways

The majority of the ransomware news were **target announcements (81,4%)**. The rest (18,6%) were from threat actors leaking sensitive data from those organizations that refuse to pay.

According to our data, the most active ransomware groups were **LockBit 3.0** for 17,6%, **Cl0p** for 9,14%, and **Play ransomware** responsible for 8,56% of all the attacks.

Last year, the top 3 countries targeted by ransomware groups were the **United States**, which had 65,14%, the **United Kingdom**, which had 8,64%, and **Canada**, which had 5,01% of the attacks.

The Manufacturing sector was targeted the most with approximately 14% of the attacks. **The Professional, Scientific and Technical services** sector was the second with 11% of the attacks. On the third place we have the **Information sector**, the target of approximately 7% of ransomware attacks.

An **increase in ransomware attacks** can be seen from the beginning of 2023 to the end of the year. But with the start of 2024, attacks gained momentum and increased in numbers significantly.

Most of the ransomware attacks occurred in **February 2024**.

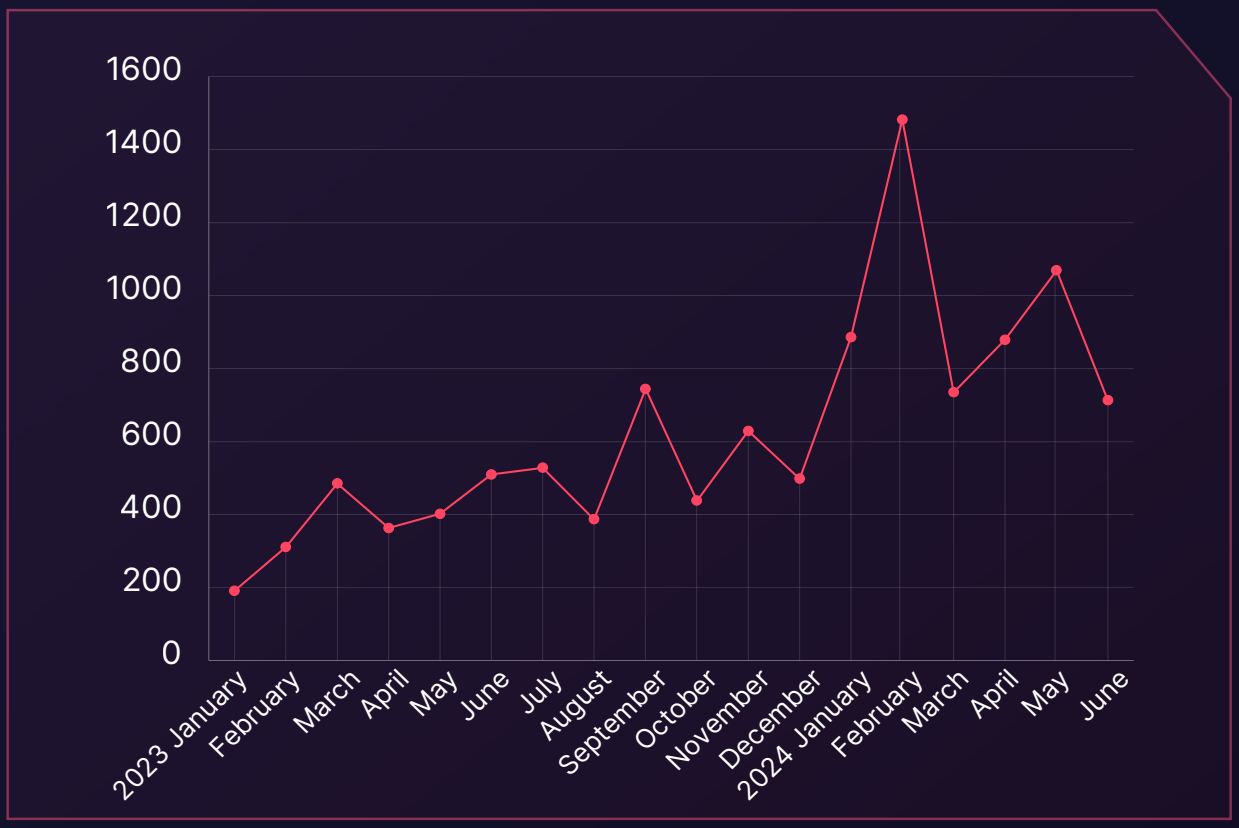
Technical Details

An Outlook to the Ransomware Threat Landscape

Ransomware attacks present substantial risks to organizations, often resulting in severe outcomes like major data loss and the disclosure of confidential information.

In this chapter, we will provide a general overview of the ransomware threat landscape, examine payment data, and identify the most active threat actors in the ransomware world.

Ransomware Activity

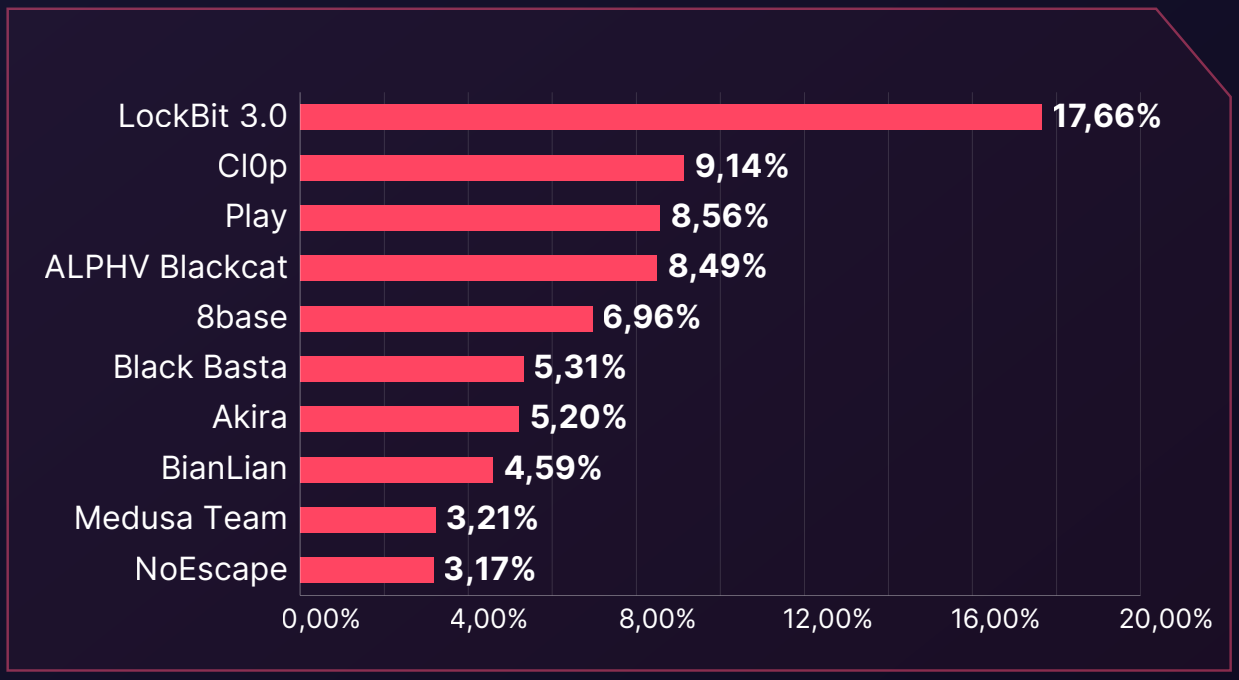


Looking at the trend in ransomware activity starting from the previous year, we see an increase in the number of attacks towards the end of 2023 with a peak during September 2023. With the beginning of 2024, we saw an acceleration. Even though there is a certain decrease with the beginning of the second quarter of 2024, there is a rise in the amount of ransomware incidents compared to previous year.

Ransomware Payment Ratio

The majority of the posts published on the dark web are the victims of ransomware attacks. If the demanded ransom is not paid, the threat actors share the alleged leak and try to damage the target organizations. However, the majority of the data these threat actors leak are not related to their alleged attack. A lot of threat actors also announce fake victims to seem more dangerous than they actually are.

Most Active Ransomware Groups



According to our data, the most active ransomware groups are LockBit 3.0 with 17,6% of the attacks, Cl0p with 9,14% of the attacks, and Play ransomware with 8,56% of all the attacks. For an overview of these threat actors, you can check the following summaries. For more detailed information, you can visit our blog.

Lockbit 3.0 Ransomware Group

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

You can visit our blog post for more detailed information about the Lockbit 3.0 Ransomware Group.

Cl0p Ransomware Group

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey
Target Sectors:	IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication
Attack Type:	Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Exploitation for Privilege Escalation:	T1068
Exfiltration Over C2 Channel:	T1041

Cl0p, a member of the well-known Cryptomix ransomware family, is a dangerous file-encrypting malware that intentionally exploits vulnerable systems and encrypts saved files with the ".Clop" extension. The name of the threat actor comes from the Russian word "klop," which means "bed bug," a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of Cl0p is the string "Don't Worry C|0P" found in the ransom notes.

On June 16, 2021, in a coordinated international effort involving law enforcement agencies from various countries, authorities arrested numerous individuals suspected of affiliation with the Cl0p ransomware gang. Despite this operation, the ransomware group grabbed attention a few days later by releasing data acquired from new victims.

You can visit our blog post for more detailed information about the Cl0p Ransomware Group.

Play Ransomware Group

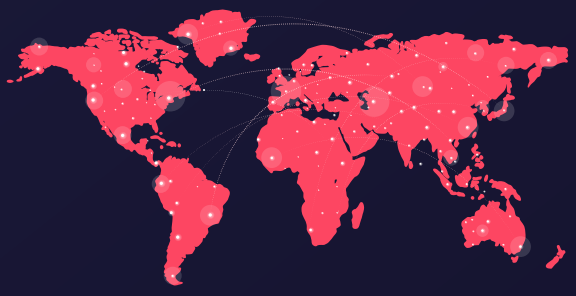
-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	Latin America, India, Hungary, Spain, Netherlands, United States
Target Sectors:	Manufacturing, Education, Real Estate, Technology, Transportation, Healthcare
Attack Type:	Compromised Valid Accounts, LOLBins, Ransomware, Data Exfiltration

-TTPs-

Process Injection:	T1055
Input Capture:	T1068
Proxy:	T1090

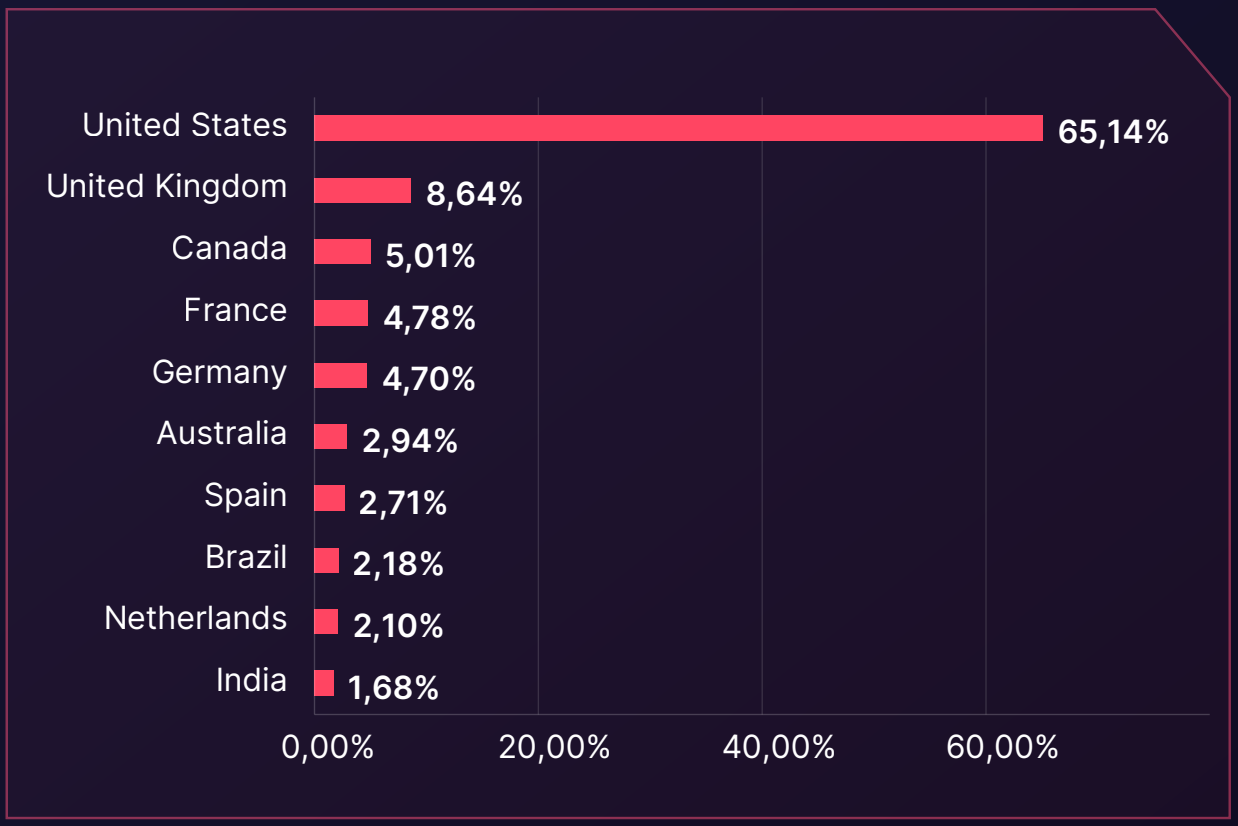
> Researchers have uncovered a significant development as Play Ransomware transitions to a Ransomware-as-a-Service (RaaS) model. A recent in-depth analysis, based on various Play ransomware attacks, reveals a striking uniformity in tactics and procedures across different sectors, indicating the use of predefined playbooks or instructions, possibly supplied by a RaaS kit.
>
> Play Ransomware also uses double extortion against its victims. They can archive the breached data with WinRAR and then upload it to file-sharing sites.
>
> You can visit our blog post for more detailed information about Play Ransomware.



Country Analysis

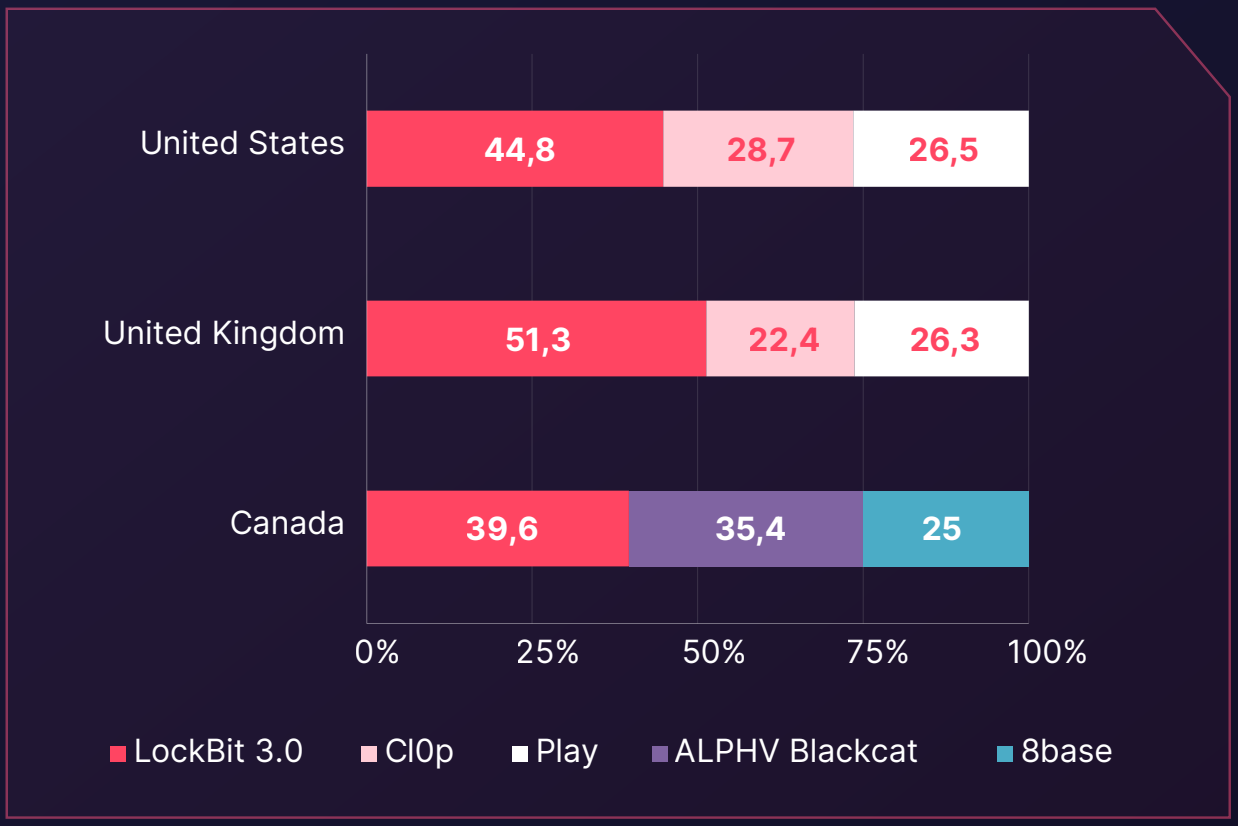
Examining ransomware attacks by country can provide insights into the incentives of the threat actors. Although these attacks are primarily financially motivated rather than ideologically driven, mapping them can help us identify the movements of these threat actors and determine which states are at risk.

Top 10 Countries Targeted by Ransomware Groups



Last year, the top 3 countries targeted by ransomware groups were the United States, which suffered 65,14% of the attacks. The United Kingdom experienced 8,64%, and Canada experienced 5,01% of the attacks.

Ransomware Group Breakdown of the Top 3 Target Countries

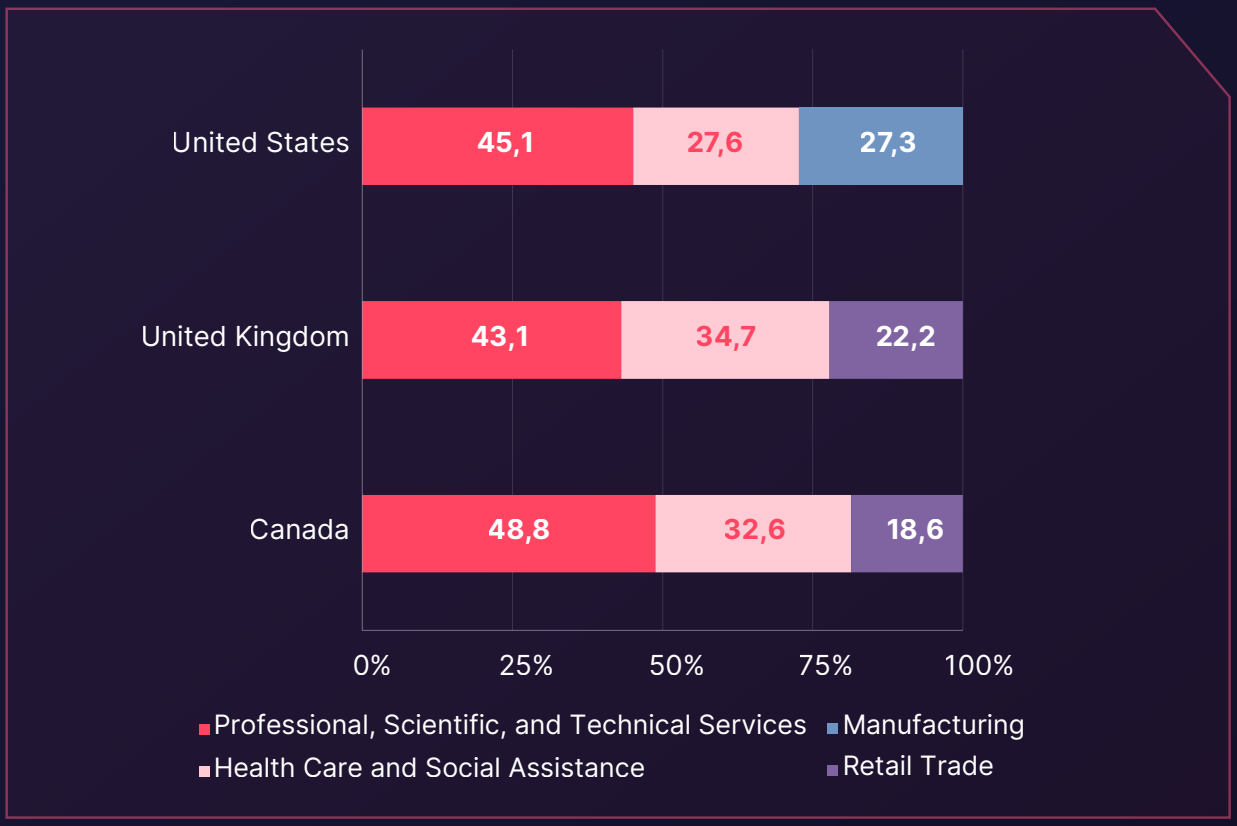


When we analyze the most prominent targets for each country in that list, we see that LockBit 3.0 plays a huge role, especially in the United Kingdom, by being responsible for around %51 of the ransomware attacks towards the UK targets.

Cl0p ransomware is the second threat actor for the US and the UK while ALPHV Blackcat is the second most active threat actor attacking the Canadian organizations.

In third place, the Play ransomware is the most troublesome group targeting the US and UK, while 8base is the third most active threat actor harming Canadian institutions.

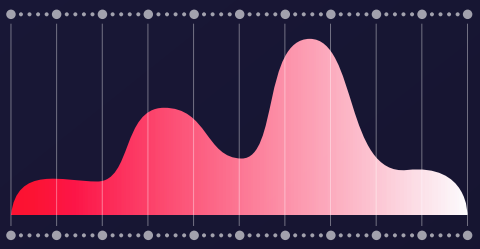
Industry Breakdown of the Top 3 Target Countries



When we look at the industries targeted in the most attacked countries, we see that Professional, Scientific, and Technical Services are the leading group that is being targeted by ransomware attacks in all three states.

Afterward, companies in the Manufacturing sector became the second most targeted institutions.

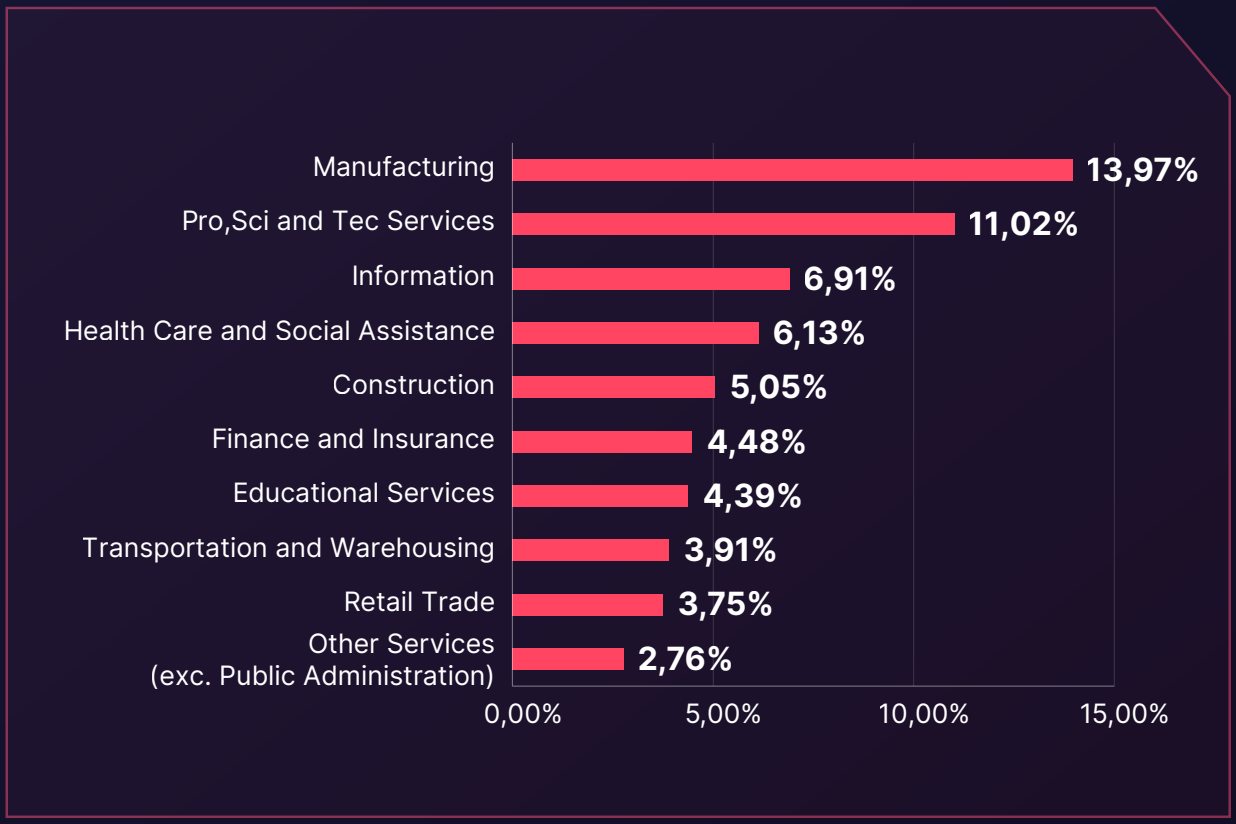
In third place, Healthcare for the United States and Retail Trade for the UK and Canada are the most targeted sectors.



Industry Analysis

Ransomware attacks are primarily financially motivated. Analyzing data by industry can help identify which sectors are more targeted by these groups. This allows organizations to focus their resources on specific vulnerabilities rather than using broad solutions to address the extensive ransomware threat landscape.

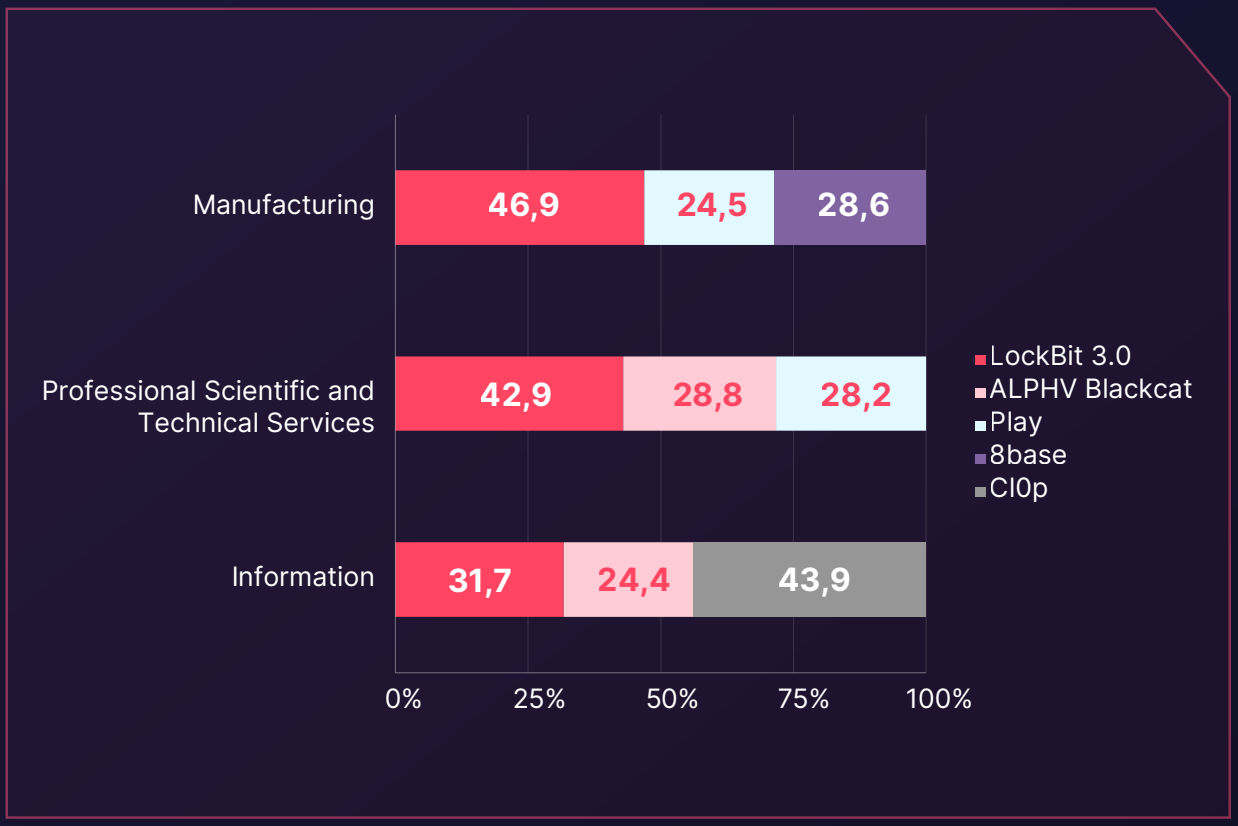
Ransomware Attacks - Distribution by Industries



When we look at the ransomware attacks from the industry perspective, we can see that Manufacturing with approximately 14% of the attacks, is the most targeted sector, followed by Professional, Scientific, and Technical Services with 11% of the attacks. In the third place we have the Information sector with approximately 7% of ransomware attacks.

The top 10 sectors targeted by ransomware make up approximately 62% of all ransomware attacks.

Ransomware Group Breakdown of the Top 3 Target Industries



The Manufacturing industry was targeted the most by LockBit 3.0 (46,9%), ALPHV Blackcat (24,5%) and 8base (28,6%).

Professional Scientific and Technical Services were targeted most by the LockBit 3.0 (42,9%), ALPHV Blackcat (28,8%), and the Play ransomware (28,2%).

The Information sector was mostly targeted by the LockBit 3.0 (31,7%), ALPHV Blackcat (24,4%) and the Cl0p ransomware (43,9%).

Recommendations and Conclusions

Specific industries and countries as well as the most significant ransomware groups targeting them are covered in respective chapters.

This increased sophistication also impacts the importance of accurate intelligence. Taking action after following misleading information can cause serious damage to your organization. Therefore, we are providing certain recommendations here and showing you how SOCRadar's solutions can guide your organization against ransomware threats.

Key Considerations for Ransomware Negotiations

As we also pointed out in our report ransomware incidents have seen a rise in occurrence within the contemporary digital realm over recent years. The nature of this threat leads to substantial losses for businesses as they force organizations to pay substantial sums for data recovery.

Due to this nature, the importance of negotiations with threat actors has grown significantly. Navigating such negotiations can cause bigger problems if not conducted properly. Here are some recommendations from Huzeyfe Önal, CEO of SOCRadar, who also conducted million-dollar ransomware negotiations.

1. **Role Presentation:** Avoid presenting yourself as a manager or authority figure during negotiations.

2. **Extending Negotiations:** Strategically extend the negotiation timeline. This can make the ransomware group more eager to settle, potentially leading to a better deal.

3. **Verification of Claims:** Request a list of files that were compromised and verify a sample to ensure the group can actually decrypt the data, confirming their claims.

4. **Engaging Authorities:** Report the incident to local authorities before the ransomware group can leverage it as a threat. This step protects your legal standing and integrity.

5. **Price Justification:** Always ask the ransomware group to justify the ransom amount. They typically demand a ransom based on a percentage of annual revenue, allowing room for negotiation on more reasonable terms.

6. **Avoid Provocation:** Maintain a professional demeanor without making accusations that could provoke or escalate tensions.

7. **Honest Communication:** Be honest and straightforward in your communication. Avoid cliché excuses which are ineffective and could undermine the negotiation process.

8. **System Access Checks:** Confirm whether the threat actors still have access to your systems to prevent further damage or additional breaches.

9. **Pre-Negotiation Planning:** Determine your limits on operational interruptions and financial expenditure before negotiations start. This helps in making informed and strategic decisions during the negotiation process.

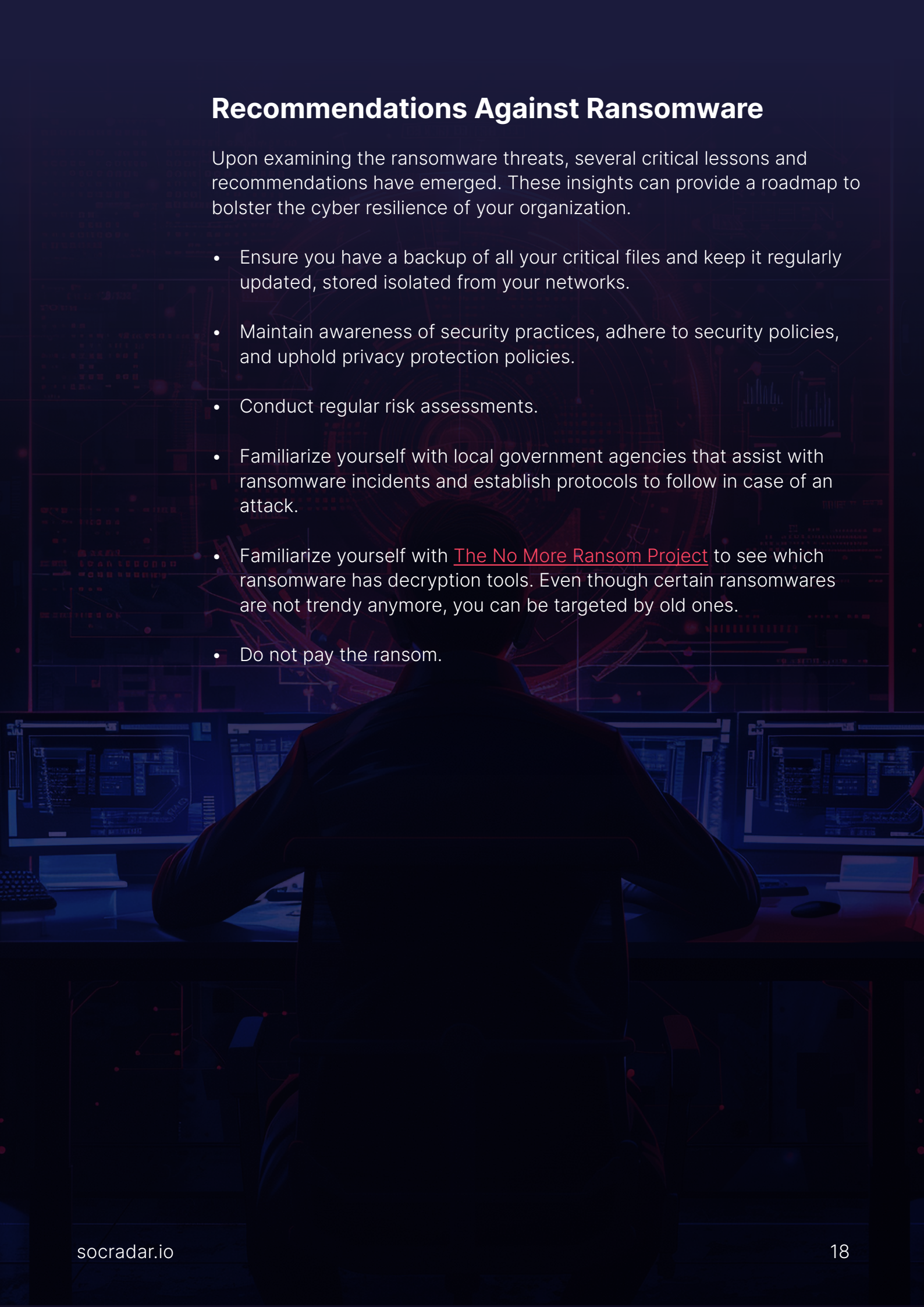
10. **Data Deletion Verification:** After any payment, ensure the data is deleted by requesting proof, such as a video, to confirm the action.

With the help of these strategies, navigating the negotiations with ransomware groups will be less risky, and the potential damages can be avoided. For more in-depth analysis and additional insights, refer to the full article by Huzeyfe Önal, CEO of SOCRadar, on Medium.

Recommendations Against Ransomware

Upon examining the ransomware threats, several critical lessons and recommendations have emerged. These insights can provide a roadmap to bolster the cyber resilience of your organization.

- Ensure you have a backup of all your critical files and keep it regularly updated, stored isolated from your networks.
- Maintain awareness of security practices, adhere to security policies, and uphold privacy protection policies.
- Conduct regular risk assessments.
- Familiarize yourself with local government agencies that assist with ransomware incidents and establish protocols to follow in case of an attack.
- Familiarize yourself with The No More Ransom Project to see which ransomware has decryption tools. Even though certain ransomwares are not trendy anymore, you can be targeted by old ones.
- Do not pay the ransom.



Conclusion

The current ransomware landscape forces organizations to adopt a proactive and comprehensive cybersecurity approach. Waiting until the attack occurs is no longer a good approach, and the importance of accurate intelligence increases every day. By partnering with advanced solutions like SOCRadar, you can effectively navigate the evolving ransomware threats.

In our report, we present a detailed analysis of the biggest ransomware risks from both industry and country perspectives. The report highlights the sectors most frequently targeted by ransomware attacks, as well as the threat actors' interests and the regional differences in ransomware activity. By understanding these risks, you can better tailor your cybersecurity strategies to address the specific threats that you might face.

Utilizing SOCRadar's capabilities can give you intelligence into the operational capacity of those ransomware groups targeting your nation or industry. With the help of that kind of intelligence, you can adopt more appropriate security measures.

A deep dive focus into the threat landscape is vital for organizations. The evolving landscape of cyber threats is vast and it is impossible to allocate enough resources for every type of threat. As ransomware attacks become increasingly sophisticated, organizations must prioritize certain security measures to protect their valuable data and systems to make sure their resources are not wasted. You can check how SOCRadar can help you down below.

How can SOCRadar Help You?

Vigilance in an Evolving Cyber Threat Landscape

Organizations must keep pace with the changes in the threat landscape by adapting their security strategies. This adaptation can happen with proper guidance. By adopting a proactive approach like SOCRadar's Extended Threat Intelligence solution, organizations can gain real-time insights into emerging threats, positioning them to counteract cyber adversaries proactively.

Implementation of Multi-layered Security Measures

Given the broad spectrum of industries targeted by ransomware actors, it is essential to implement multi-layered security defenses regardless of the size or industry of your organization. Any amount can be requested as ransom and it can happen to any organization. SOCRadar supports these efforts with its proactive Threat Intelligence and monitoring services, as well as an advanced Ransomware Intelligence tool under our Operational Intelligence Module, ensuring comprehensive protection.

Consistent Guard Against Ransomware

The persistent ransomware threat underscores the need for strong defensive and responsive strategies. SOCRadar's Attack Surface Management capabilities are crucial for businesses to identify potential ransomware threats and to formulate effective countermeasures.

Continuous Employee Education and Training

The ongoing risk of phishing attacks, which is one of the most used methods by ransomware groups, makes continuous employee education and training imperative. Enhancing their ability to recognize phishing tactics and detection methods is vital. SOCRadar's Digital Risk Protection suite provides comprehensive VIP Protection and Brand Protection services, effectively addressing the challenges posed by identity-based attacks.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by **21.000+ companies** in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play

Gartner Peer Insights™ 4.8/5