Dark Web Profile: SpaceBears

Published: 2024-06-20 · Archived: 2026-04-05 14:25:10 UTC

Recent history could be termed the Age of Ransomware in the realm of cybercrime. However, threat actors have discovered a way to profit without the need for malware development or sophisticated methods. SpaceBears is a new participant in the **Data Broker trend**, which has gained momentum particularly due to major crackdowns on ransomware groups by security forces.

Depiction of SpaceBears, Image created with Bing AI

Who is SpaceBears

SpaceBears threat actor card

It's been said amongst the cybersecurity community that the SpaceBears, a ransomware group believed to be based in Moscow, Russia, has recently taken credit for several high-profile cyberattacks, demonstrating their advanced tactics in the cyber threat landscape. However, we did not encounter any advanced techniques, traces or indicators of ransomware.

Main page of SpaceBears' Data Leak Site (DLS)

When you enter the Data Leak Site (DLS), you see the following text: *"This page contains a list of companies whose clients and business partners entrusted them with their confidential data, but these companies leaked data. The data may contain confidential information such as login credentials, intellectual property, personal and financial data, etc."*

As we discussed in another blog post, such groups follow an extortion strategy by reaching insurance companies and worrying the organization's customers in order to earn income from the data they obtain.

You can visit our relevant blog post to learn the Modus Operandi of Data Broker groups.

What to do section in the DLS

The group provides instructions for DLS visitors on what to do if they believe their data has been compromised. They claim that upon receiving payment, the publication will be removed, the obtained data will be deleted from their servers, and a decryption tool will be provided for the alleged **"encrypted"** files. Additionally, they even offer guidance on how to prevent similar attacks in the future.

Victimology

SpaceBears currently has 8 organizations listed in its DLS, most of which are medium/small sized organizations.

When we look at the countries in which the organizations are located through their domain addresses, there are 2 US, Portugal, Canada, Germany, Norway, Morocco and Singapore each containing one victim.

When looked at on a sectoral basis, we see Manufacturing, small technology solutions organizations and a Healthcare-related company.

Latest victim announcements from SpaceBears

When we look at the sharing formats of a victim, in addition to company related information, the number of views, publication date and the content of the leaked database are also written.

Leaked data was being hosted on a file sharing service

They do not host allegedly leaked data on their own servers, but share it through file sharing services accessible on the clear web; Of course, this results in the file being deleted in a short time.

In addition, this situation seems to be an indicator of insufficient technical capacities of the group, but even dangers that seem small for now can lead to big problems in the future. A leaked credential could lead to a bigger attack in the future.

Conclusion

In summary, this preliminary research on SpaceBears highlights their emergence in the Data Broker trend amidst the ongoing crackdown on ransomware groups. While they claim responsibility for several cyberattacks and operate a Data Leak Site listing compromised organizations, the group's methods and infrastructure suggest a reliance on basic extortion strategies rather than sophisticated malware tactics.

Their use of external file-sharing services for hosting leaked data indicates potential limitations in their technical capabilities. However, even seemingly minor threats can escalate, underscoring the importance of continued vigilance and proactive cybersecurity measures. This report may be expanded in the future as new developments and incidents unfold.

Mitigation Strategy: Data Protection Focus

Given the tactics employed by SpaceBears and many other Data Broker groups, organizations must adopt a mitigation strategy centered around **data protection**. Here's a comprehensive approach to mitigate the risks posed by SpaceBears and similar threat actors.

Data Classification and Encryption

- **Develop and enforce data classification policies:** Identify and categorize sensitive information, such as customer data, financial records, and intellectual property.

- **Encrypt sensitive data:** Use strong encryption algorithms to secure data both at rest and in transit, preventing unauthorized access and protecting against data theft.

Access Control and Principle of Least Privilege (PoLP)

- **Implement stringent access controls:** Restrict data access based on the principle of least privilege, ensuring that employees only have access to data essential for their roles.
- **Regularly review and update access permissions:** Minimize the risk of insider threats and unauthorized access to sensitive data.

Network Segmentation and Monitoring

- **Segment networks:** Create isolated zones to limit the spread of potential breaches, reducing the impact of a successful attack.
- **Deploy robust network monitoring tools:** Use Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) solutions to detect and respond to suspicious activities indicative of data exfiltration attempts.

Employee Training and Awareness

- **Conduct regular cybersecurity training sessions:** Educate employees about phishing attacks, social engineering tactics, and the importance of data protection.
- **Foster a culture of security awareness:** Encourage employees to report suspicious activities promptly and follow best practices for data security.

Incident Response Plan

- **Develop a comprehensive incident response plan:** Tailor it specifically to address data breaches and extortion attempts by threat actors like SpaceBears.
- **Define clear protocols:** Establish incident escalation procedures, communication methods, legal considerations, and coordination with law enforcement agencies.

Backup and Recovery

- **Implement a reliable backup and recovery strategy:** Ensure data availability and continuity in the event of a ransomware attack or data breach.
- **Regularly test backup systems:** Verify their effectiveness in restoring critical data and minimizing downtime.

Vendor and Third-Party Risk Management

- **Evaluate the security posture of vendors and third-party partners:** Ensure they adhere to strict security standards and undergo regular security assessments.
- **Establish contractual agreements:** Include security requirements and responsibilities to mitigate third-party risks effectively.

By implementing these proactive measures, organizations can strengthen their defenses against data extortion threats posed by groups like SpaceBears. Regular monitoring, testing, and refinement of these strategies are essential to adapt to evolving cyber threats and protect sensitive data effectively.

SOCRadar: Enhancing Data Breach Detection and Mitigation

SOCRadar presents an indispensable solution for detecting and addressing data leaks and credential compromises, bolstering your organization's resilience against cyber threats. Through continuous monitoring of both surface and dark web sources, SOCRadar swiftly detects any exposure of sensitive information, including employee emails, customer login credentials, and financial data such as credit card numbers.

Key Use Cases of SOCRadar in Data Breach Scenarios

- **Early Threat Detection:** SOCRadar enables early detection of potential data breaches by actively scanning web sources for any signs of compromised data or unauthorized access attempts.
- **Real-time Alerting:** The platform provides real-time alerts and notifications for critical security incidents, allowing your security team to respond promptly and mitigate risks effectively.

An example of SOCRadar's alerts

- **Threat Intelligence:** SOCRadar offers comprehensive threat intelligence, including contextual information about threat actors, attack vectors, and potential impact, empowering your organization to make informed decisions and prioritize response efforts.
- **Intellectual Property Protection:** SOCRadar safeguards your intellectual property by monitoring for unauthorized access or exposure, preventing data theft and preserving the integrity of your proprietary information.
- **Resource Optimization:** Through intelligent prioritization of security incidents, SOCRadar helps your team allocate resources efficiently, focusing on critical areas that require immediate attention and mitigation.
