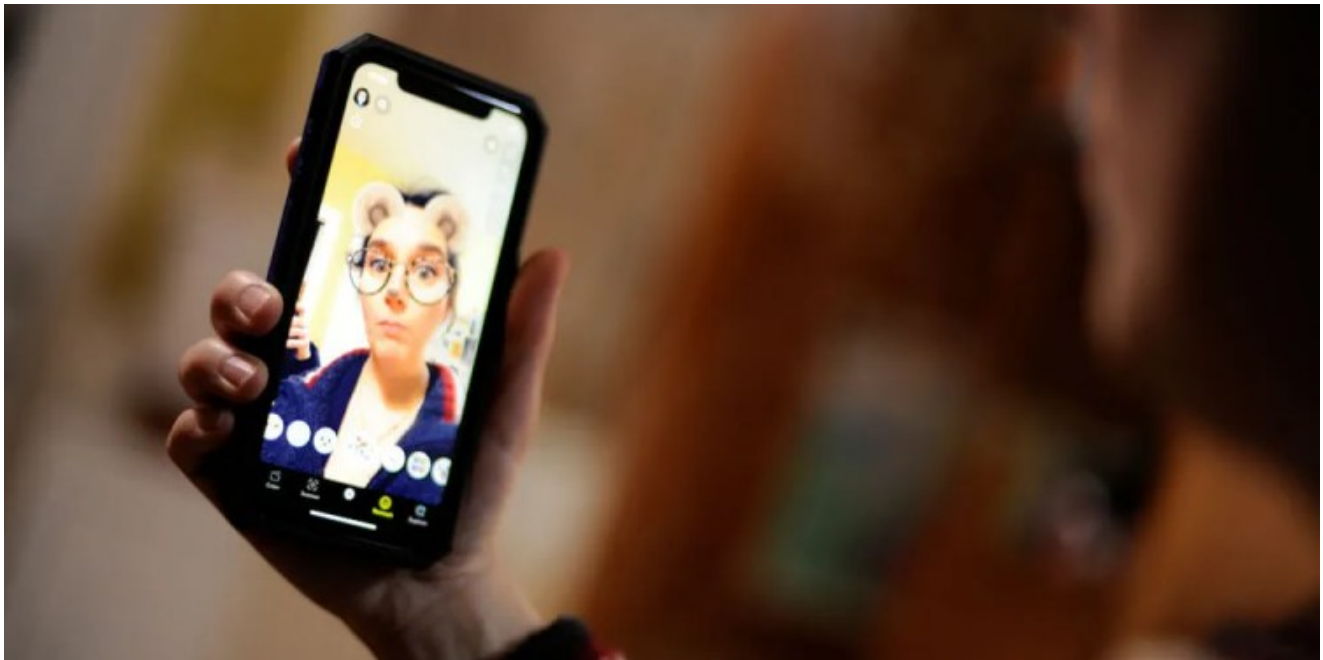


Hack Alert: SN Blackmeta Claims Cyberattack on Snapchat Over Explicit Content and Alleged Political Bias!

theycyberexpress.com/sn-blackmeta-claim-snapchat-cyberattack/

June 12, 2024



The notorious hacker group SN Blackmeta has allegedly claimed responsibility for a cyberattack on Snapchat's infrastructure. The Snapchat cyberattack has reportedly led to disruptions in service in specific regions and the disabling of login and account creation features within the app.

In a post attributed to SN Blackmeta, the threat actor outlined their motives for the cyberattack on Snapchat, citing reasons such as their opposition to the content promoted by the social media platform, which they claim includes pornography and undermines moral values.

Additionally, the group accuses the application of supporting Israel while opposing efforts in support of Palestine. These grievances, according to SN Blackmeta, prompted them to target Snapchat as a means to "test their strength."

Decoding the Snapchat Cyberattack by SN Blackmeta

The terminal window displays a list of URLs, including various endpoints for Snapchat and related services. To the right, a network diagram shows a central server connected to multiple clients, with IP addresses and port numbers listed.

reported

The most common problem reported about Snapchat, with 48% of all reports, was: **send message**.

Problem	Percentage
Send Message	48%
Login	38%
Receive Message	14%

Location of their report to see if other people in your area are having similar problem!

Date	Problem	Location
Jan 10, 2024, 1:04:04	Login	United States
Jan 10, 2024, 12:01:04	Send Message	United Kingdom
Jan 11, 2024, 11:48:29	Login	United Kingdom
Jan 11, 2024, 10:24:29	Send Message	United Kingdom

The Great Leader Darkmeta writes

- 1) Checking the "blueprints" of the SnapChat Application
- 2) Currently, we announce an attack on the company behind the Snapchat application


Reason: We do not need a reason to target this American application, which generally promotes pornography and destroys all moral values, in addition to encouraging sexual deviance. The application fully supports the state of Israel and opposes any campaigns that benefit Palestine or spread awareness about the Palestinian cause.

we have decided to test our strength on it today.

Source: X

The claimed Snapchat cyberattack has allegedly resulted in service disruptions in certain countries and the temporary incapacitation of key features within the Snapchat application.

Despite SN Blackmeta's claims, Snapchat has not yet released an official statement about the incident, leaving the details of the cyberattack unconfirmed. The Cyber Express has reached out to the company, and we are currently awaiting their response.

 **The Great Leader Darkmeta writes**

🔴 Checking the "blueprints" of the SnapChat Application 📱

🔴 Currently, we announce an attack on the company behind the Snapchat application

Reason: We do not need a reason to target this American application, which generally promotes pornography and destroys all moral values, in addition to encouraging sexual deviance. The application fully supports the state of Israel and opposes any campaigns that benefit Palestine or spread awareness about the Palestinian cause.

we have decided to test our strength on it today.

Results of the attack:

- 1. Service disruptions in certain countries.
- 2. Disabling login and account creation systems in the application.

📱 حاليًا، نعلن عن هجوم على شركة تطبيق سناب شات 📱

السبب: لا نحتاج إلى سبب لمهاجمة هذا التطبيق الأمريكي الذي يعمل بشكل عام على نشر الإباحية وتدمير كل المفاهيم الأخلاقية، بالإضافة إلى تشجيعه على الشذوذ الجنسي. التطبيق يدعم بشكل كامل دولة إسرائيل ويعارض أي حملات تعود بالنفع لفلسطين أو نشر قضية فلسطين.

لذلك، قررنا اليوم تجربة قوتنا عليه

نتائج الهجوم:

- 1. إيقاف الخدمات في بعض الدول
- 2. تعطيل تسجيل الدخول وإنشاء الحسابات في التطبيق

🗡️

✅ The duration of this attack is over. This mission was a complete success for us, and as of now, we have received confirmation of the attack.

We are fire we are Death

#Darkmeta

📱 202 🗡️ 82 ⚡ 77 ❤️ 52 🔥 24 😈 1 🏆 1

👁️ 826 08:38

Source: X

Interestingly, this isn't the first time SN Blackmeta has made headlines for their cyber activities.

In the past few days alone, the group has launched attacks on various targets, including the Social Security Administration (SSA) website and Microsoft's OneDrive. These attacks aim to disrupt services and hinder user access, demonstrating the group's proficiency in executing cyber warfare.

The recent surge in cyberattacks by SN Blackmeta comes amidst a backdrop of escalating tensions in the digital world. Other hacktivist groups have also been active, targeting prominent organizations and government entities with coordinated attacks.

Previous Cybersecurity Challenges

The current Snapchat cyberattack is not the first time that the Snap INC-owned platform has faced cybersecurity challenges. The most recent controversy with Snapchat was reported by Vice in May 2019 wherein researchers discovered that Snapchat employees were misusing their access privileges to spy on users. This breach of trust raised concerns about user privacy and data security within the platform.

Between January 2014 and February 2018, Snapchat faced a series of cybersecurity challenges. In July 2017, a phishing attack compromised over 55,000 accounts by luring users to a fake login page. The attackers then published stolen credentials, granting unauthorized access.

In February 2016, a phishing scam targeted Snapchat employees, resulting in the disclosure of payroll information. The October 2014 incident involved a third-party app hack, leaking 200,000 explicit images. Though Snapchat denied system compromise, blame was placed on the app providers.

In January 2014, a security vulnerability led to the exposure of 4.6 million user details, despite Snapchat's claim of addressing the issue promptly. As for the current Snapchat cyberattack claim, this is an ongoing story and The Cyber Express will be closely monitoring the situation. We'll update this post once we have more information on the alleged cyberattack on the social media platform or any official confirmation from Snap INC.

Media Disclaimer: This report is based on internal and external research obtained through various means. The information provided is for reference purposes only, and users bear full responsibility for their reliance on it. The Cyber Express assumes no liability for the accuracy or consequences of using this information.

© 2022 - 2024 The Cyber Express by Cyble. All Rights Reserved