Security, and Data Breach Analysis, FBI Association

Phantom Productions Data Breach Incident: Ensuring Your Security

Law Enforcement Related: Scroll To The Bottom

Dear valued members of the Phantom Productions community,

We understand the utmost importance of your online security, and it is with a serious and diligent approach that we address the recent data breach incident concerning our web store, store.phantom-productions.net, where we provide FiveM assets. We want to assure you that we are actively taking all necessary measures to mitigate the situation and secure our systems moving forward.

Immediate Action Taken:

In response to the breach, we have been working tirelessly to safeguard all other Phantom Productions assets. We have taken the precaution of fully wiping our server and associated services, while continuously monitoring and diagnosing the extent of the breach. We are also in the process of compiling comprehensive documentation about the breach to ensure transparency and accountability.

Along with the measures previously mentioned, we are taking comprehensive steps to address both our internal and publicly facing platforms, such as Phantom Hosting databases and Phantom Productions staff databases. While these databases were not compromised, we consider it essential to enhance their security posture even more. Consequently, we will be changing all passwords and cryptographic keys associated with these platforms. Furthermore, as an added layer of protection, we will be mandating password resets for all clients using these services. We emphasize that these measures are proactive and precautionary, aimed at ensuring the sanctity of your data and our systems.

We want to assure you that every available measure is being taken to uphold the security and integrity of Phantom Productions across the board. Our commitment to providing a safe and secure environment for our community remains steadfast.

Our Commitment to Security:

At Phantom Productions, security stands as a paramount concern, and we are wholly dedicated to the protection of both your data and our services. We recognize the gravity of the situation

and want to assure you that we are dedicating significant resources to address and rectify the breach.

Known Affected Data:

As part of the breach's impact, the following information has been identified as compromised:

- DiscordID: Your unique Discord account ID.
- Banned Status: Indicating if you were banned from our store.
- Name: Your Discord name.
- Discriminator: Your Discord tag.
- Avatar: Your Discord avatar.
- Banner: Account banner (inactive).
- Email: Your Discord email.
- Join Date: Date of joining our community.
- Payment Data: Transaction IDs of past purchases (no readable payment data) no card information was stored or leaked.
- Order History: Any orders you have placed in the past on the website.

Password Security:

While no passwords were released in the breach, we feel it is crucial to emphasize that Phantom Productions does not store passwords. Nonetheless, as a precautionary measure, we strongly recommend that you reset your Discord password and any other password linked to your email.

Affected Users:

The breach specifically impacts those who have logged into our store using a Discord account.

Insight into Our Store's Security:

It is important to note that our store's architecture incorporated encryption, preventing Phantom Productions from making any modifications. The store's original creator encrypted the platform, ensuring that updates and code evaluations were solely conducted by the original developer. While this structure added an extra layer of security, it also posed challenges in terms of monitoring and assessing the code for potential vulnerabilities.

Transparency and Communication:

We understand that this incident is unsettling, and we are committed to keeping you informed throughout this process. Our aim is to provide transparent communication as we continue to assess the situation, enhance our security measures, and share updates regarding our progress.

Your Confidence Matters:

We want to reiterate that your confidence in Phantom Productions matters to us. Rest assured, we are leveraging all available resources to rectify the breach, bolster our security, and ensure that such incidents do not recur in the future.

How did this happen?

Breach Timeline and Attack Vector:

Sometime yesterday, an unauthorized attacker, more commonly referred to as a hacker, managed to gain illicit access to our primary database. This breach exploited a previously unknown MYSQL vulnerability within our store's architecture. This vulnerability provided the attacker with remote access to the database, allowing them root-level control. Despite having comprehensive security measures in place, the attacker successfully bypassed our database's built-in protections through a remote connection and SQL injection attack.

Vulnerability Source and Assumptions:

It's important to clarify that we purchased the store from an external company, and this store is encrypted, preventing us from making code modifications or vulnerability assessments. Regrettably, we erroneously assumed that this encrypted store was inherently secure. The breach exposed a gap in our diligence, as we were unable to scrutinize the underlying code for potential vulnerabilities.

Discovery and Initial Actions:

Today, upon noticing that our primary store was offline, our team immediately began investigating the matter. Led by Shane, our investigation revealed suspicious files within the store's directory that did not align with the expected contents. These files contained PHP code related to a remote authentication server. Although initially perceived as a payment processing file, the investigation swiftly shifted to the database, where we discovered files had been removed, and others were locked.

Ransom Note and Extortion Attempt:

During our thorough assessment, we identified the presence of a new table named "readme" within the database. This table contained alarming content, outlining the attacker's actions and intentions. The attacker claimed to have backed up our databases and issued a demand for payment in Bitcoin. The attacker provided a specific address and instructions for payment, coupled with a warning that our data would only be returned upon compliance. Their message included a request to contact a designated email address after payment, accompanied by server IP and transaction ID details.

Immediate Response and Ongoing Action:

In light of this breach, we want to assure you that we are taking an assertive stance to secure our systems and your data. Our initial steps involved isolating the compromised database, disconnecting any unauthorized access points, and implementing measures to prevent further

breaches. Additionally, we are collaborating with cybersecurity experts to investigate the breach, close the vulnerability, and recover our data without entertaining extortion.

Our Commitment to You:

We deeply regret any concerns or inconveniences this breach may have caused you. Please understand that your security remains our top priority, and we are committed to restoring the integrity of our services. As we move forward, we will provide you with regular updates on our progress, remediation efforts, and any necessary actions you may need to take.

We urge you to exercise vigilance and reset your associated passwords, especially if you've logged into the store using your Discord account. We are here to address your questions and concerns, and we encourage you to reach out to us here in our discord..

Our lines of communication remain open, and we encourage you to reach out to us with any questions, concerns, or suggestions you may have. We value your feedback and are here to provide the support you need.

So, what now?

Holistic Security Measures:

Our topmost priority is to ensure that every facet of Phantom Productions remains impervious to any unauthorized access. To this end, we are diligently securing all services, regardless of whether they were directly affected by the breach. This proactive stance underscores our unwavering commitment to your safety and peace of mind.

Phantom Hosting and Primary Staff Communication:

We want to emphasize that Phantom Hosting, our esteemed service designed to cater to your hosting needs, has not experienced any breaches. However, in line with our proactive strategy, we are initiating a rigorous security assessment of Phantom Hosting, bolstering its safeguards, and enhancing its resilience against potential threats. Rest assured, your hosting experience remains secure and uninterrupted.

Our primary staff communication and email system, while unaffected by the breach, also remain focal points of our security enhancement efforts. We are working diligently to fortify these platforms, implementing advanced measures to safeguard sensitive communications and secure data exchange.

Password and Key Overhaul:

We are taking a resolute step by systematically changing all passwords and connection keys across our entire infrastructure. This all-encompassing password and key overhaul aims to neutralize any potential vulnerabilities that may exist within our systems. By implementing this

far-reaching action, we are bolstering our defenses and significantly reducing the risk of unauthorized access.

Transparency and Accountability:

As part of our commitment to transparency and accountability, we will continue to provide regular updates on our security initiatives, progress, and any actions required on your part. We understand that your trust is paramount, and we are unwavering in our dedication to maintaining that trust.

Collaboration with Internet Crime Complaint Center (IC3) - The FBI:

Understanding the seriousness of the breach and the potential legal ramifications, we have initiated communication with the Internet Crime Complaint Center (IC3), an entity operated by the Federal Bureau of Investigation (FBI). Our objective is to establish a partnership with law enforcement experts who specialize in cybercrime and digital investigations. The IC3's expertise will provide invaluable insights into the breach, enhance our understanding of its origin, and contribute to the formulation of a robust remediation strategy.

Cooperation with Local Massachusetts Law Enforcement:

Furthermore, we are also actively coordinating with local law enforcement agencies within Massachusetts, where Phantom Productions is headquartered. Collaborating with local authorities ensures that we address any potential legal implications stemming from the breach. Our cooperation with Massachusetts law enforcement underscores our commitment to adhering to applicable laws and regulations while seeking justice for any potential wrongdoing.

Document Created By: Shane W - Head of Investigation – 08/017/2023