Information Security Incident Report Form

|  |
| --- |
| Name: Bhargav Gosai |
| Email address: bgosai2001@gmail.com |
| Telephone/Mobile number: |
| Date of report: |
| Incident detection date: |
| Has the incident been resolved (yes/no): yes |
| Organization name and address: |
| Incident Overview |
| **Location of incident (site)**  The incident occurred on User database of Steam and affected users worldwide. |
| **Nature of Incident (select all that apply)**   1. **Suspicious system and network activities** 2. **Compromise of sensitive information** 3. **Unauthorized access or attempts to access a system** 4. Emails with suspicious attachments or links 5. Denial of service attacks 6. Suspected tampering of electronic devices 7. Malware infection    * Cryptlocker    * Coin miner    * Remote access trojan    * Credential harvesting malware    * Botnet    * Other malware (describe) 8. Reconnaissance (scanning/probing) 9. Social engineering 10. **Account compromise** |
| **Incident Severity**   1. None/Negligible (suspicious activity only) 2. Minor (Impacts single computer, non-privileged account) 3. Moderate (Impacts part of the organization’s infrastructure) 4. **High (impact’s organization’s entire infrastructure/privileged accounts)** 5. Very High (has impact beyond the organization) |
| **How did the organization become aware of the incident?**  The owner and operator of Steam, Valve, found out about an intrusion while investigating a security breach of a discussion forum. Upon further investigating they uncovered that attackers had used login details from forum to get access into database. |
| **Provide a general description of the incident:**  On November 6, 2011, Valve’ online gaming platform steam was attacked by hackers to steal user credentials such as ID and credit card details. Valve forum offline instantly and said it was down due maintenance but few days later posted a message about getting hit. Investigation revealed that the intrusion went past beyond just steam forums and username, hashed passwords, game purchases, email addresses and encrypted credit card information were compromised. |

|  |
| --- |
| Incident Report |
| **Incident Impact (select all that apply)**   1. **Loss of access to services** 2. Loss of productivity 3. Loss of reputation 4. **Loss of revenue** 5. Propagation to other networks 6. **Unauthorized disclosure of data/information** 7. **Unauthorized modification of data/information** 8. Unknown/Other (please describe) |
| **What steps were taken to investigate the nature and severity of the incident?**  **Notification of users**: All Steam users were immediately emailed about the security vulnerability and asked to change their passwords by Valve Corporation. Users were also urged by the organization to keep an eye on any fraudulent charges on their credit card statements.  **Engagement of a third-party forensics firm:** A third-party forensics company named CrowdStrike was hired by Valve Corporation to perform an investigation into the kind and scope of the security breach. The company thoroughly investigated the Steam user database and other relevant systems to identify the attack's origin and consequences.  **Analysis of the attack:** The third-party forensics organization investigated the attack to identify the technique the hacker used to gain access to the Steam system.After completing the investigation, they found that hackers accessed the steam database, which contains sensitive information about the user. This includes names of users, hashed passwords, and credit card data in encrypted form.  **Coordination with law enforcement:** Valve Corporation collaborated completely with the law enforcement organizations, that includes FBI, they will investigate the attack and identify who was responsible behind this attack. So, we will provide information to law enforcement organization and helping them with the attack’s investigation.  **Communication with impacted parties:** To keep impacted parties informed of the progress of the investigation and any further measures being taken to address the incident, Valve Corporation was constantly communicating with them. Affected parties included users and credit card companies. Additionally, the organization provided concerned consumers access to free credit monitoring services. |
| **What systems were impacted?**   * IP addresses of affected systems: * FQDN of affected systems: * Role of affected systems (Domain controller/DNS/DHCP/Web Server): * Operating systems of affected systems: * Patch level of affected systems: * Security software on affected systems: * Physical location of affected systems: * Additional details:   Company has not disclosed any of given details. |
| **Which applications were impacted?**  The Steam platform, a digital distribution platform for video games and related content, was the main application hit by the 2011 Steam attack. The Steam platform's user database was the focus of the attack, which exposed millions of users' user names, hashed passwords, and encrypted credit card information. Steam Client was impacted as the main application used for purchasing game from steam store.  Moreover, Steam Community was also impacted where users can interact with each other and also join groups and share contents to other users. Steam Cloud was also affected and it is the place where user save their game, user generated data, another confidential data on steam servers. So, they can access it from any device in which the steam is installed. |
| **What unauthorized data access occurred?**  **Usernames and passwords:** The attackers were successful in getting their hands on user login data, including usernames and hashed passwords.  **Encrypted credit card information**: They also gained access to the encrypted credit card information of the Steam users, while the encryption provided a certain level of security to the data. But the attacker might have been able to decrypt the data and use it for some malicious purpose.  **Billing Address**: While accessing the accounts, the hacker also has access to the billing address of the user’s account.  **Purchase History:** The attackers were able to view what games and other content users had bought on the Steam platform since they had access to the customers' purchase histories. |
| **Which privileged user accounts were impacted?**  The exact details of privileged user accounts that were impacted in 2011 steam attack were not publicly disclosed. However, as per the reports it states that the attackers hack the steam user database, which contains confidential data of the users such as usernames, email addresses, salted and hashed passwords, encrypted credit card details. It is expected that the hack compromised certain privileged user accounts, including those of Steam administrators or developers. |

|  |
| --- |
| **Which unprivileged user accounts were impacted?**  There has not been any official release regarding which user accounts were impacted. |
| **Which third parties were impacted (Vendors/Contractors/Partners)**  According to claims made public, the 2011 Steam attack did not specifically target any vendors, contractors, or partners. However, it's possible that some of the hacked data may contain details about third-party organizations who were doing business with Valve Corporation or Steam. It's also possible that some of the users who were affected by the breach had connections with other businesses or services outside the company. So, it was unclear that which third parties’ vendors, contractors or partners were affected or not. |
| Sensitivity of Compromised Data (select all that apply)   1. **Confidential/Sensitive data** 2. Non-sensitive data 3. Publicly available data 4. **Financial data** 5. **Personally identifiable information (PII)** 6. **Intellectual property** 7. Critical infrastructure/key resources 8. Other (describe) |
| **What would the consequences be of the data that was accessed in an unauthorized manner becoming public?**  If the information gained through an illegal data breach at Steam is made public, there can be serious implications If personally identifiable information (PII) about customers such as names, addresses, email addresses, phone numbers, and payment card information in the compromised data, customers may suffer identity theft, fraud, and financial losses.  The release of sensitive company data, that includes trade secrets or proprietary information, could damage Steam's reputation as a market leader and result in financial losses for the business. The public release of information regarding vulnerabilities in Steam's systems or software could also put other businesses at risk who use comparable systems or software, and that leads to increase in cyberattacks and data breaches.  Additionally, data theft and unauthorized access could negatively impact Steam's reputation and destroy customer and partner trust. If it is determined that the company didn't properly safeguard customer data, it may potentially be subject to regulatory penalties and legal action. |
| **What is the time frame of the incident?**  Suspected initial date/time of compromise:  November 2011  Detection date/time: 6 November  Incident remediation date/time: [10 November](http://forums.steampowered.com/forums/) |
| How did the breach occur? (Select all that apply)   1. DDoS 2. Malware 3. Misconfiguration 4. Phishing 5. **Vulnerability exploit** 6. Unknown |
| **Suspected perpetrators:**   1. Insider 2. Former staff 3. Other 4. **Unknown** |
| **Estimated total cost incurred: (Cost to contain incident, restore systems, notify stakeholders)**  No information revealed regarding this by the company. |
| **What steps have been taken to remediate the cause of and vulnerabilities related to the incident?**  **Password Reset:** Valve urged all the users to change their password that were potentially affected by the breach. This was done to prevent the unauthorized access to the user steam account and to make sure that data is safeguarded.  **Security Audit:** They go through a thorough investigation of the system to identify and address the location from where the breach occurs. So, they can quickly fix the vulnerabilities.  **Improved security measures**: They implemented various security measures like two-factor authentication, for account access and reset all the passwords. They also updated their security protocols and collaborated with the law enforcement agencies to investigate the attack and identify the culprit behind it.  **Improved Communication:** Valve took efforts to increase transparency on their security policies and to better communicate with users about security-related issues. They also requested all the users to continuously monitor their credit card statements if they find any suspicious notify the company. |
| **What additional controls should be in place to prevent the incident reoccurring?**  **Regular vulnerability assessments and penetration testing:** This can be helpful in identifying vulnerabilities in the system and can be resolved before attackers try to attack them.  **Security awareness training for employees:** Providing training to the employees regularly this will help them to identify unusual activity and report it, such as phishing emails, and prevent unintended data breaches.  **Implementing multi-factor authentication:** It will help to prevent unauthorized access to the sensitive systems and data even if the attacker gets the login credentials.  **Improving network segmentation:** The impact of a potential breach can be reduced and lateral attacker movement within the network can be prevented with improved network segmentation**.**  **Implementing a comprehensive incident response plan:** A comprehensive incident response strategy can lessen the effects of a cyberattack and reduce the amount of interruption. |
| **Do any authorities need to be notified about the details of the incident?**  Since credit card information was also compromised, the organization should notify payment card network, law enforcement, government regulators and every individual affected by the breach. |
| **Additional impact information:**  About 35 million user accounts were impacted by the attack, which revealed usernames, passwords, email addresses, billing addresses, and encrypted credit card information.  Valve suffered significant financial losses as a result of the attack, including the expense of fixing the problem and a loss of customer trust. |

**CONCLUSION:**

In conclusion, the 2011 Steam breach was a significant data breach that affected 35 million users. An unauthorized user accesses the steam user database, which contained usernames, email addresses, encrypted passwords, and payment card information. There was a weakness found in the steam as a result that led to the attack. Both privileged and non-privileged user accounts were affected by the assault. Private information, such as financial information and personally identifiable information, both were disclosed and the suspected attackers were not identified. To prevent this incident in future additional features were added in the organization like regular assessment, reviewing and updating the systems with the latest technologies, implementing stronger access controls. They should also implement incident response and notifying the users if necessary. The Steam attack provides an illustration of the importance of maintaining strong safety measures and the potential consequences of a breach of information.