Incident Report: Brute Force Attack 2024-05-13 #1

Globe Sistemas - Av. Libertador Jardin America

Report Overview

As an analyst for **globesistemas.com** , which provides systems analysis and cybersecurity services, an attacker has decided to lure users to a fake website with malware.

The threat actor executed a brute-force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they hit on the correct one.

Once they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file when visiting the website. After integrating the malware, the attacker changed the password for the administrative account.

When customers downloaded the file, they were redirected to a fake version of the website containing the malware.

Hours after the attack, several customers sent emails to **globesistemas.com 's support service** . They complained that the company's website had prompted them to download a file to access their user account.

Customers reported that after running the file, the website address changed and their personal computers began to run slower.

In response to this incident, the website owner tries to access the admin panel but is unsuccessful, so he contacts the website hosting provider. All cybersecurity analysts were tasked with investigating this security incident.

To address the incident, you create an isolated environment to observe the suspicious behavior of the website.

Run the tcpdump network protocol analyzer, and then type the URL of the website, **globesistemas.com** .

As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then notice that your browser redirects you to a different URL, **globalsistemas.com ,** which contains the malware.

The logs show the following process

1. The browser initiates a DNS request: It requests the IP address of the URL **globesistemas.com** from the DNS server.
2. The DNS responds with the correct IP address.
3. The browser initiates an HTTP request: It requests the **globesistemas.com web page** using the IP address sent by the DNS server.
4. The browser initiates the malware download.
5. The browser initiates a DNS request for **globalsistemas.com** .
6. The DNS server responds with the IP address of **globalsistemas.com**
7. The browser initiates an HTTP request to the IP address of **globalsistemas.com**

A senior analyst confirms that the website has been compromised. The analyst checks the website's source code.

They noticed that javascript code has been added to encourage website visitors to download an executable file. Analysis of the downloaded file found a script that redirects visitors' browsers from **globesistemas.com to globalsistemas.com.**

The cybersecurity team reports that the web server was hit by a brute force attack. The disgruntled attacker was able to guess the password easily because the admin password was still the default password. In addition, there were no controls in place to prevent a brute force attack.

The job involves documenting the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. It should also recommend a security action to be taken to prevent brute force attacks in the future.

| **Part 1: Identify the network protocol involved in the incident** |
| --- |
| The protocol involved in the incident is Hypertext Transfer Protocol (HTTP). Since the problem was with access to the **globesistemas.com web server** , we know that web page requests to web servers involve http traffic.  **globesistemas.com** website , the corresponding tcpdump log file showed the use of the http protocol when contacting the file. It is observed that the malicious file is transported to users' computers using the HTTP protocol at the application layer. |

The main goal of this activity was to identify the network protocol used in the incident. The first line of the report announces the response to that step.

The protocol involved was determined using the information presented in the scenario, the DNS and HTTP record, and the knowledge you learned about the TCP/IP model in this course:

* The tcpdump log shows that a request is sent to the DNS server to resolve the IP address of the URL **globesistemas.com** . The DNS server responds with the correct IP address. The browser uses this to direct users to the correct website.
* The scenario states that when the website loads, a feature on the website prompts users to download a file to access free recipes.

Both the scenario and the logs indicate that this activity occurs over the HTTP protocol, which you learned earlier is part of the application layer of the TCP/IP model.

Review the "How to Read the tcpdump Traffic Log" article linked in Step 2 of the activity for an explanation of the evidence found in the log.

* After the user downloads and executes the file, logs show that the user's browser sends a new request to the DNS server to retrieve the IP address of a different URL: **globalsistemas.com** .

The DNS server sends the IP address to the users browser and the users are redirected to this new website via HTTP.

| **Part 2: Documenting the incident** |
| --- |
| **Summary of events and issues identified when the incident was first reported**  Several customers contacted the website's support service and said that when they visited the website, they were asked to download and run a file containing access to new recipes.  Since then, their personal computers have been running slowly. The website owner tried to log in to the web server but noticed that his account was locked.  **Description of the testing activities involved in the investigation of this event**  The cybersecurity analyst used a sandbox environment to open the website without affecting the company's network.  The analyst then ran tcpdump to capture the network traffic packets produced when interacting with the website.  **globalsistemas.com** website .  **Job description for analysis**  The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address of the yummyrecipesforme.com website.  Once the connection to the website was established via the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic when the browser requested a new IP address for the URL **globalsistemas.com** .  Network traffic was then redirected to the new IP address of the **globalsistemas.com website** .  **Conclusion from the senior cybersecurity analyst and the incident management team on the root cause of the attack**  The senior cybersecurity professional analyzed the source code of the websites and the downloaded file. He discovered that an attacker had manipulated the website to add code that prompted users to download a malicious file disguised as a free software update.  Since the website owner stated that he was locked out of his admin account, the team believes that the attacker used a brute force attack to access the account and change the admin password.  Execution of the malicious file compromised end-users' computers. |

| **Part 3: Recommend a solution to address brute force attacks** |
| --- |
| One security measure the team plans to implement to protect against brute force attacks is to disallow the use of old passwords.  Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it is important that we prevent old passwords, such as default passwords, from being used to reset the password.  Another backup measure is to require longer passwords. Passwords of 15 characters or more offer greater protection against brute force attacks.  Finally, another useful solution is to implement two-factor authentication (2FA). 2FA requires authentication using a password and also confirming a one-time passcode (OTP) sent to your email or phone.  Once the user confirms his identity through his login credentials and OTP, he will gain access to the system.  Any malicious actor attempting a brute force attack will likely not gain access to the system because it requires additional authentication. |