SITUATION

your investigation. All investigation findings belong in the sec

This is Alexander from the IT Security Team, reporting a potential security breach impacting one of our client's infrastructures.

An Analyst from our Security operations center had evidence of a remote intrusion attempt on 12/06/2017 involving AT-USA infrastructure and captured a PCAP of the suspicious activity.

This suspicious activity is impacting the network infrastructure belonging to a long-time client, AT-USA.

I believe by analyzing the captured PCAP I would be able to confirm or disconfirm if the activity was malicious.

I believe by analyzing the captured PCAP I would be able to confirm or disconfirm if the activity was remotely generated or not.

I believe by analyzing the log data within a SIEM, I would be able to corroborate my initial conclusion with additional facts on whether the activity was malicious.

I believe I would be able to determine if any devices in the client's network were compromised by analyzing the log data with a SIEM (Splunk)

This investigation has no relationship to any other previous or ongoing investigation that I am aware of.

BACKGROUND

Date of incident: 12/06/2017

Local Time at which the incident occurred: 18:34:24 GMT - 18: 35: 33 GMT

I am tasked by Virgil to assess whether the attack is malicious by scrutinizing the PCAP, and then validating these preliminary conclusions through an analysis of log data in the SIEM.

I have been provided with PCAP and SIEM logs as the sources for this investigation.

The SIEM log was captured on 12/06/2017 from 1800GMT - 1900 GMT

The PCAP was captured on 12/06/2017 and spans from 18: 34:19. 90- 18:35:47.90 GMT

ASSESSMENT

investigation.

The notion that the incident was a remote intrusion activity came up not torue after the investigation. The investigation revealed that the attack originated internally and not externally.

There was a brute-force attack where an attacker, LAB-Kali (10.5.10.105) (made several attempts to log into WordPress instance account on the server LAB-Web02 (10.5.20.16) using Hydra technology.

12/06/2017 6:14:43 - 6:18:58   First cluster of Brute Force activity <LAB-Kali.at.USA.co> 10.5.10.105 uses Hydra to Brute-Force the authentication form from wp-login.php account hosted by LAB-Web02

LAB-kali' is the attacking device because it is the device where a malicious entity is performing actions intended to compromise or exploit vulnerabilities in another device or system. This device could be running software tools designed for penetration testing and cyber-attacks, such as Kali Linux, hence the 'kali' in its host name. Kali Linux comes with numerous built-in tools that can be used for purposes like password cracking, network scanning, and vulnerability exploitation.

'LAB-Web02', on the other hand, is the web server hosting a WordPress instance. WordPress is a widely used content management system that allows users to build and manage websites. In this scenario, 'LAB-Web02' is the target of the attack being carried out by 'LAB-kali'.

12/06/2017 6:15:07 LAB-Kali (10.5.10.105) made the first successful authentication: unknown credentials

12/06/2017 6:27 - 6:36PM the second cluster of Brute-Force activity by LAB-Kali was unleashed on LAB-Web02 to access the authentication credentials of its WordPress instance account

12/06/2017 6:34:45 LAB-Kali (10.5.10.105) made second successful authentication: credentials given by Wireshark as user id == admin, pwd == Winter2017wp@dmin

12/06/2017 6:46 - 6: 51 PM The third cluster of Brute-force attacked from LAB-Kali.at.USA.co on LAB-Web02 to authenticate the login credentials of the WordPress login account was recorded.

12/06/2017 6:47:02 LAB-Kali (10.5.10.105) made third successful authentication into the WordPress login account: unknow credentials

12/06/2017 6:50:01 LAB-Kali (10.5.10.105) made the fourth successful authentication; credentials unknown.

During the incident, the primary security breach was a brute-force attack. An attacker (WEB.Kali.at.USA.co) aimed to access the authentication details of AT-USA's WordPress instance hosted on the LAB-Web02 server. In simpler terms, the attacker was attempting to "break into" the system by trying all password combinations until they found the right one.

This occurred on 12/06/20.

Our analysis pinpointed the attack's origin to a host server, LAB.Kali.at.USA.co, with an IP address of "10.5.10.105", which utilized Hydra to initiate the Brute-force attack.

The attacker (LAB-Kali) specifically targeted AT-USA's WordPress instance on the LAB-Web02 server, IP "10.5.20.16". This server was primarily attacked, facing numerous login attempts by the assailant.

Here's a breakdown of the attack sequence:

- 6:14:43 - 6:18:58: Initial brute-force activity. LAB-Kali.at.USA.co (IP 10.5.10.105) employed Hydra to brute-force wp-login.php on LAB-W02.
- 12/06/2017 6:15:07: LAB-Kali's first successful login; exact credentials remain unidentified.
- 12/06/2017 6:27 - 6:36PM: LAB-Kali initiated a second brute-force wave on LAB-Web02.
- 12/06/2017 6:34:45: LAB-Kali's second successful entry used credentials: Username - "admin", Password - "Winter2017wp@dmin".
- 12/06/2017 6:46 - 6:51PM: LAB-Kali launched a third brute-force attempt on LAB-Web02.
- 12/06/2017 6:47:02: LAB-Kali's third successful login, but credentials remain unknown.
- 12/06/2017 6:50:01: LAB-Kali's fourth successful entry; credentials are still unidentified.

The attacker; LAB-Kali achieved his goal, compromising the WordPress account by obtaining its credentials on four distinct occasions. They gained access using the following credentials: Username - "admin", Password - "Winter2017wp@dmin".

Our research discovered that the attacker repeatedly succeeded in accessing AT-USA's WordPress account on the LAB-Web02 server for the same purpose: to obtain login details.

Certain vulnerabilities in the WordPress account allowed the attacker unauthorized access. This weak point was the main entryway for the attacker.

The attacker executed multiple brute-force assaults on the WordPress account, consistently obtaining authentication details.

Our findings highlight that brute-force was the consistent technique across all successful breaches. This suggests the attacker's keen interest in accessing the WordPress admin account.

1. Internal Host Name: LAB-Web02(10.5.20.16): This was the webserver the attacker repeatedly tried to log into by Brute-Force method

2. Internal Hostname: Lab.Kali.at-usa.co. Located at (10.5.10.105): Attacker's hostname and IP

After repeated login attempts the username and password of the WordPress admin login form was authenticated successfully by the Hydra attacker (10.5.10.106) showing brute-force attack thereby compromising the WordPress instance account.

After the investigation it was deduced that there was no external host in this incident, rather the attacker was an internal player.

This incident was severe in that the login credentials of our client's WordPress instance account had been accessed by an attacker.

The Administrative privileges to LAB-Web02 server seemed to be of particular interest to the attacker. However, it is unknown if any relevant documents were stolen from the server per this investigation other than the WordPress account credentials.

It is not known as of now. However, LAB-Web02 server might contain important information such as employee account information, company files belonging to AT-USA, our client

There is no evidence to support the claim that anything of value might have been stolen or exfiltrated during the incident except the login credentials.

At the moment it seems the threat has been contained because we are not seeing the repetition of the same event in the server since the last WordPress instance login was completed.

At this time there is no evidence to support the claim that immediate mitigation measures have been put in place

RECOMMENDATION

INCIDENT RESPONSETRIAGE

1. I recommend that the LAB-Web02 be disconnected, forensically imaged and examined and be reset to a good state to prevent further potential attack.

2. The attacker's device with the hostname Lab.kali.at-usa.co (10.5.10.105) should be quarantined for further digital analysis.

3. All user credentials associated with the WordPress site should be reset

4. Existing account holders should be verified to ensure that they are rightful owners of their respective accounts

5.The webmaster WordPress login account password should be reset.

6. The compromised server should be singled out for additional analysis.

7. Additional logs should be gathered from any of the devices involved in the attack, particularly the authentication logs from the WordPress instance hosted on LAB-Web02. This will help in determining which other user credentials were also compromised.

8. The attacker's device should be singled out for additional analysis. We will want to know if any confidential data was transferred from the server

1. The employee who owns the device, Lab.kali.at-usa.co (10.5.10.105) will have to answers question based on the attack

2. The LAB-Web02 administrator will have to answer questions about the attack and explain to us whether the WordPress site has any information of value to the attacker.

These individuals could help us to understand the motive and purpose of the attack.

AT-USA Management should be notified

Employees whose accounts are going to be reset should be notified as well.

PREVENTION OF FUTURE INCIDENTS OF THIS TYPE

1. I recommend all users create complex and unique passwords. For instance, must include lower and uppercase letters as well as numbers and special characters

2. I recommend the implementation of account lockout policies. After a certain number of failed login attempts, the account should be either temporarily locked or the user should be forced to wait a longer period between each login attempt.

3. I also recommend the company should adopt Two-Factor Authentication policies for all users

4. I recommend the use of firewall rules, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to detect and block repeated login attempts from the same IP address.

The company should consider a policy to Monitor failed login attempts and set up alerts for multiple failed login attempts in a short period of time. This can help you quickly detect and respond to brute force attacks.

TECHNICAL APPENDIX

An attacker operating from the host Lab.Kali.at-usa.co (IP address 10.5.10.105) initiated a brute force attack on our server LAB-Web02 (IP address 10.5.20.16) in an attempt to obtain login credentials to a WordPress account, employing the tool Hydra.

The first cluster of this brute force activity was observed on 12/06/2017, between 6:14:43 and 6:18:58. The attacking device with IP 10.5.10.105 was seen using Hydra to force the authentication credentials of a wp-login.php account on the LAB-Web02 server.

At 6:15:07 on the same day, the attacker from 10.5.10.105 was able to achieve the first successful authentication, though the credentials used remain unknown.

At 6:34:45, a second successful authentication was made by the attacker. The credentials were identified by Wireshark as: User ID - admin, Password - Winter2017wp@dmin.

The attacker made a third successful entry into the WordPress login account at 6:47:02, but again, the credentials remain unknown.

Finally, at 6:50:01, the attacker from 10.5.10.105 made the fourth successful authentication, with the specific credentials remaining unknown.