Splunk 3: Protecting VSI from Future Attacks

(Recommendations)

Scenario

Previously was setted a SOC and monitored attacks from JobeCorp. Now, you will need to design mitigation strategies to protect VSI from future attacks.

You are tasked with using your findings to suggest mitigation strategies.

Windows Server Attack

This is a public-facing windows server that VSI employees access.

Fact 1

- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.

  If the objective of JobeCorp is to compromise the availability of VSI systems through generating lock-out time for accounts, we suggest migrating to a multifactor authentication.

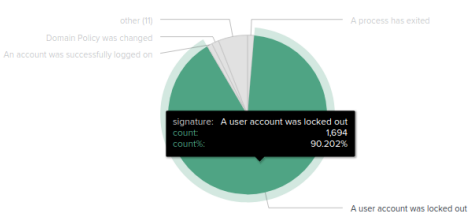
  Users mitigation

  The account **user_a** has 1694 events for “locked out account” representing 90% of its activity. We suggest lowering the number of the threshold for account reset alerts.

  More important is the activity detected from the account **user_k** who reached 2021 attempts to reset an account password representing 95% of its activity. This could mean that the account is compromised and has been used to escalate and expand the access to other users. We recommend freezing this account to analyze, clean and confirm its safety before activating with a new strong password.

  Moreover, we recommend changing passwords to new strong passwords. At least 8 characters long, and should include at least one capital letter, symbol, number and Lowercase letter. We suggest the password does not contain related-to-the-user words, or even the use of a password manager approved by the company.

  For the company **global mitigations**, we recommend increasing the lock-time of accounts every time it reaches the number threshold’s failed attempt, increasing the requirement for strong passwords(At least 8 characters long, and should include at least one capital letter, symbol, number, and Lowercase letter), and creating a company password manager. Likewise, we recommend the implementation of a security awareness plan. The current phase of the attack implies a previous reconnaissance involving a social engineering attack on the employees. Employees, mostly, are the weakest point of failure.



Fact 2

- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

  If the objective of JobeCorp is to compromise the availability of VSI systems through generating lock-out time for accounts, we suggest migrating to a multifactor authentication.

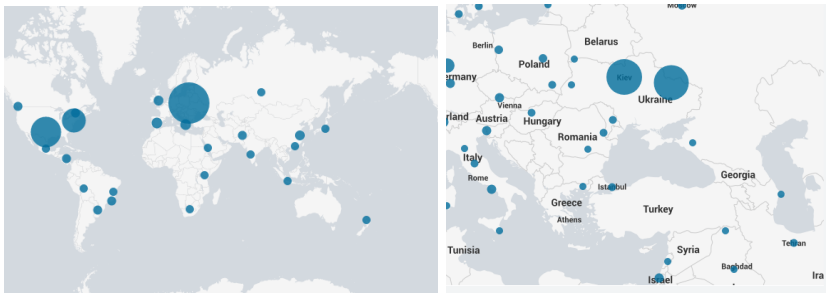
Apache Webserver Attack:

Fact 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.

  Block all incoming HTTP traffic where the source IP comes from the country of Ukraine

- Provide a screenshot of the geographic map that justifies why you created this rule.



Fact 2

- VSI has insider information that JobeCorp will launch the same web server attack but use a different IP each time in order to avoid being stopped by the rule you just created.

- What other rules can you create to protect VSI from attacks against your webserver?

  Block all incoming POST request to the /VSI_Account_logon/php folder Where the IP comes from the country of Ukraine