Scientific Method & Cybersecurity Event Analysis
Brandi Keough
Overview

- My background
- Scientific approach to cybersecurity
- Scientific Method
- Scientific Method related to cybersecurity
- Examples
- Summary
- Q&A
About Me

- Mother to one year old son, Oliver
- UNCC- double major Chemistry and Criminal Justice
- Found love for cybersecurity along the way
- Utica College- Class of 2016
- Information Security Analyst Novant Health- 3 years
- Network+, Security+, GCIH
Reoccurring Theme

Chemistry

Chemicals

Scientific Method

Problem
Hypothesis
Constants
Variables
Testing
Analysis
Labs
Reports

Cybersecurity

Computers

Prezi
Observation

→ Ask Question

→ Hypothesis

→ Experiment

Accept Hypothesis or Reject Hypothesis
Scientific Method

- Focused thought process
- Helps keep main goal in mind
- Even if you go down a path with experiment that didn't work, can take direct path back to main goal
Observation

SIEM alert for Brute Force Logons from one user account to internal server

Accept or Reject

Accept
User had not logged off of server after password was changed; the server was still trying to authenticate using the user's old credentials

Question

Why is user account failing logons?

Experiment

Check date user last changed password
Check last logoff from server

Hypothesis

User changed password recently and has cached credentials on server
Observation

SIEM alert for Brute Force Logons from one user account to internal server
Question

Why is user account failing logons?
Hypothesis

User changed password recently and has cached credentials on server
Experiment

Check date user last changed password

Check last logoff from server
Accept or Reject

Accept

User had not logged off of server after password was changed the server was still trying to authenticate using the user's old credentials
Observation

SMB alert for multiple devices showing malware infection.

Question

What is causing the malware outbreak?

Question

What is the AV alert?

Question

What is triggering the AV alert?

Question

What can be done about AV alert?

Hypothesis

Infected file on file share

Hypothesis

One website hosting malicious content

Hypothesis

Different malicious sites

Hypothesis

New AV signature

Hypothesis

Something in common on websites

Hypothesis

Wordpress plugin vulnerable to spyware

Hypothesis

Web browsing denied by AV policy

Experiment

Check file causing AV alert

Experiment

Check to see if some website

Experiment

Check reputation of websites

Experiment

Check threat database for AV signature

Experiment

Look for similarity of all websites being visited

Experiment

Wordpress plugin vulnerability Google search

Experiment

All web browsing is a file with URL string

Accept or Reject

Reject

Accept or Reject

Reject

Accept or Reject

Accept

Accept or Reject

Accept

Accept or Reject

Accept

Accept or Reject

Accept
Observation

SIEM alert for multiple devices showing malware infection
Question

What is causing the malware outbreak?
Hypothesis

Infected file on file share
Experiment

Check file causing AV alert
Accept or Reject

Reject
Hypothesis

One website hosting malicious content
Experiment

Check to see if same website
Accept or Reject

Reject
Hypothesis

Different malicious sites
Experiment

Check reputation of websites
Accept or Reject

Reject
What is the AV alert?
Hypothesis

New AV signature
Experiment

Check threat database for AV signature
Accept or Reject

Accept
Question

What is triggering AV alert?
Hypothesis

Something in common on websites
Experiment

Look for similarity of all websites being visited (/wp-content/plugins)
Accept or Reject

Accept
Hypothesis

WordPress plugin is vulnerable to spyware
Experiment

WordPress plugin vulnerability Google search
Accept or Reject

Accept
Question

What can be done about AV alert?
Hypothesis

Web browsing denied by AV policy
All web browsing to sites with URL string (/wp-content/plugins) that were triggered for AV alert was being denied by AV policy for spyware.
Accept or Reject

Accept

AV alert was being triggered due to new AV signature for spyware, users were web browsing to sites that were hosting vulnerable WordPress plugins. Web browsing was being denied for AV policy for spyware and only remediation is for sites to update vulnerable WordPress plugins.
Questions?
Resources

Google Images

https://www.google.com/search?q=corn+maze+entrance&rlz=1C1GGRV_enUS791US791&pws=0&tbm=isch&source=iu&ictx=1&fir=_Sva5enRLo7hkM%253A%252CveEb5jU68kxgcM%252C&usg=AI4_-kQC9YZiHy5dMxO04mUmePsTS51qxg&sa=X&ved=2ahUKEvjojlykmPrdAhWqr1kKHQBBBngQ9QEwAHoECAUQBA&safe=active&ssui=on#imgrc=_Sva5enRLo7hkM:

https://www.google.com/search?rlz=1C1GGRV_enUS791US791&pws=0&biw=1920&bih=1009&tbm=isch&so=1&ei=NQ-9W7_RCMXz5gLTrb_YCw&q=north+carolina+and+south+carolina+corn+maze&oq=north+carolina+and+south+carolina+corn+maze&gs_l=img.3...30699.37458..37519...0.0.0.0......39....1.gws-wiz-img._xqZxKWDMOQ&safe=active&ssui=on#imgrc=psfbMAInBEN6kM:

https://science.howstuffworks.com/innovation/scientific-experiments/scientific-method6.htm