Advanced Threat Hunting and Compromise Assessment

Steven Cronk, Saarthik Tannan, and Lin Nhat Nguyen

Sponsor: Booz Allen Hamilton

Subject Matter Expert: Rod Wetsel

Booz | Allen | Hamilton

GEORGE MASON UNIVERSITY

Date: 5/2/2019

Introduction

- Most organizations detect a data breach by an adversary too late
- It is important to identify adversary activity at the initial compromise stage in order to contain the activity, develop threat indicators and reduce dwell time
- Threat hunting involves a proactive approach instead of a reactive approach
- The general steps of threat hunting include generating a hypothesis, analyzing the evidence, removing the threat, and a compromise report
- There are many indicators of compromise (IOC) and indicators of attack (IOA) that threat hunters look for
- An environment was not provided so we configured a lab system and implemented an attack against it

Objectives

- Perform a compromise assessment using threat hunting techniques against the configured lab system
- Utilize threat hunting techniques to perform host analysis
- Analyze the configured lab system for IOCs
- Compromise assessment report with mitigation strategies

Source: https://www.bankinfosecurity.com/webinars/effective-cyber-threat-hunting-requires-actor-incident-centric-approach-w-1254

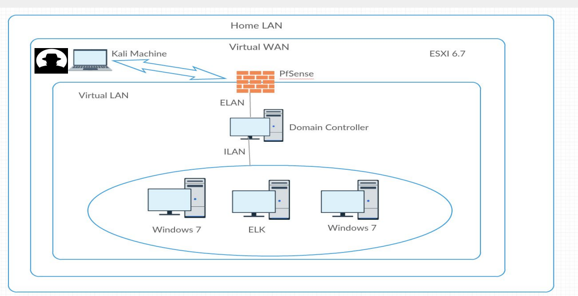


Fig 1. Network Diagram of Environment

- The attack scenario involves an adversary who dumps hashes from a compromised system account management (SAM) database and uses the hash and Metasploit PsExec module to move laterally in a network
- It is assumed that the attacker conducted a phishing attack to steal the credentials of a user's SAM database account. Once the attacker logs into the database he or she gets the hash of the administrator's password which is used in the attack

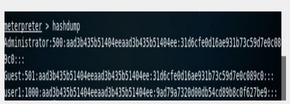


Fig 2. Using Hash to Gain Access to Admin Account

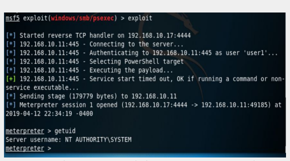


Fig 3. Metasploit PsExec Executed on Victim Machine

Methods

How Metasploit PsExec works:

- The main things the attacker does to the victim system, using the module, are the following:
  - 1. Uses the hash of the administrator password to login to his or her account, typically obtained through a separate phishing attack
  - 2. The attacker connects to the Windows Admin$ share and checks whether PowerShell (used to execute code) is installed. Administrative shares are created by Windows when multiple computers are connected to a network; these shares are hidden on the hard drive. It is used to allow administrators to access other computers and make modifications
  - 3. Creates a pipe named "NTSVCS", which allows commands to be sent to the victim system, to be able to send commands to PowerShell later on
  - 4. Modifies the Registry by adding a Key which is used for a new service
  - 5. Installs a new service called "Stager"
  - 6. Deploys malicious service "Stager" to Admin$ and launches PowerShell to execute it; this malicious service is used to execute malicious code intended to achieve the attacker's objectives
  - 7. Once an attacker has executed malicious code, he or she disables the new service and modifies the registry by deleting the key. The attacker does this to hide his or her traces

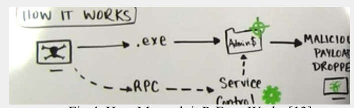


Fig 4. How Metasploit PsExec Works [13]

Log Manangement Flatform

- We used ELK Stack Elasticsearch, Logstash and Kibana (ELK stack) to hunt for compromises.
  - **Elasticsearch**: responsible for indexing data and providing the data. It is responsible for data operations. Because of its ability to allow real-time access to high volumes of a variety of data, it is a good platform to use for security analytics
  - **Logstash** works with some inputs to do some filtering of the data it receives and outputs this to Elasticsearch. Data that Logstash receives will be handled as events. The events could be log file entries, chat messages, etc. It can read multiple logs and then have multiple outputs of these logs
  - **Kibana**: a web interface that allows for the visualizations of data from Elasticsearch
  - **Beats**: Collect data on the endpoints with sysmon and winlogbeats and sends this to logstash
- Hunting Techniques utilized were searching and grouping

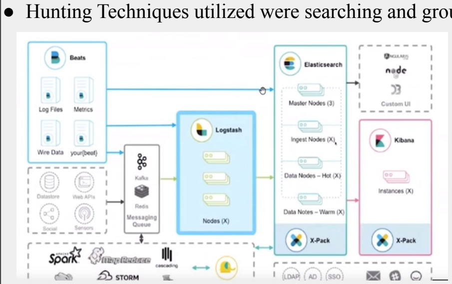
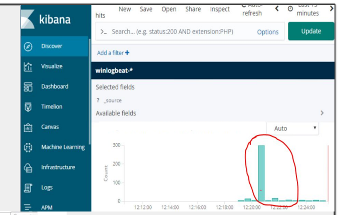


Fig 5. Low-level View of the ELK Stack [15]

Fig 6. Kibana Discover



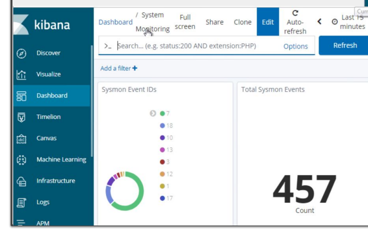


Fig 7. Kibana Dashboard

Results

- EID 3 - network connection to victim machine
- EID 4674 – a service is about to be installed, started, stopped, or modified
- EID 12 and 13 – Registry Key was created
- EID 7045 – a new service was installed on the system
- EID 1 – PowerShell executes the malicious code "Stager"
- EID 13 and 12 – the new service is disabled, and the Registry Key was deleted

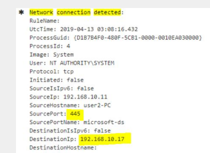


Fig 8. EID 3

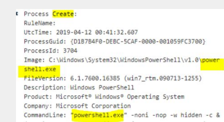


Fig 9. EID 1

Conclusion

- We collected, analyzed and discussed the threats and data that we discovered during the hunt in a remediation plan which based on the priority level of the threats.
- It is important to have a compromise specific strategy for short term and long-term containment of high priority threats.
- A compromise assessment with mitigation strategies is written

Acknowledgements

- We acknowledge the sponsor for our project who is Booz Allen Hamilton, our customer Patrick Schurr, and subject matter expert Rod Wetsel

Bibliography

[1] Roberto Rodriguez, "Chronicles of a Threat Hunter: Hunting for Remotely Executed Code via Services & Lateral Movement with Sysmon, Win Event Logs, and ELK," *Cyber Wardog Lab*, 11-Apr-2017.
[2] "Deploying and Scaling Logstash." [Online]. Available: https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html. [Accessed: 10-Apr-2019].
[3] K Hong, "ELK - Logstash, ElasticSearch, and Kibana," *BogoToBogo*. [Online]. Available: https://www.bogotobogo.com/Hadoop/ELK/ELK_ElasticSearch_Logstash_Kibana4.php. [Accessed: 10-Apr-2019].
[4] Imen Jaouani, "Establishment of a centralised log management platform with the Elastic suite," *Margo*, 14-May-2018.
[5] Ryan Nolette, "Finding Evil When Hunting for Lateral Movement," *Threat Hunting Blog*, 16-Aug-2017.
[6] "Getting started with the Elastic Stack," *Elastic*. [Online]. Available: https://www.elastic.co/guide/en/elastic-stack-get-started/7.0/get-started-elastic-stack.html. [Accessed: 10-Apr-2019].
[7] Ryan Nolette, "How Attackers Lay the Groundwork for Lateral Movement," *Threat Hunting Blog*, 08-Aug-2017.
[8] "IOCs and Artifacts," *Infosec Resources*. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/threat-hunting/iocs-and-artifacts/. [Accessed: 15-Apr-2019].
[9] "Lateral Movement Definition & Examples," *Awake Security*.
[10] Jonathan Renard, "Lateral Movement with PSExec," *ISP Blog*, 03-Mar-2017.
[11] Daniel Muñoz, "Lateral movement: A deep look into PsExec," *Context*, 04-Sep-2018. [Online]. Available: https://www.contextis.com/en/blog/lateral-movement-a-deep-look-into-psexec. [Accessed: 01-Apr-2019].
[12] David Maloney, "PSExec Demystified," *Rapid7 Blog*, 09-Mar-2013.
[13] David Maloney, *PsExec Examples: How Remote Execution Works*. 2015.
[14] "PSExec Pass the Hash," *Offensive Security*. [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/. [Accessed: 01-Apr-2019].
[15] Daniel Berman, "The Complete Guide to the ELK Stack," *Logz.io*, 20-Dec-2018.
[16] Angela Messer and Brad Medairy, "The Future of Cyber Defense… Going on the Offensive," *The Cyber Defense Review*, pp. 1–4, 2018.
[17] Saikat Basu, "What Are Administrative Shares and How to Disable Them in Windows?," *Guiding Tech*, 03-Aug-2011. [Online]. Available: https://www.guidingtech.com/7250/what-are-administrative-shares-how-to-disable-them-in-windows/. [Accessed: 15-Apr-2019].