



Module 12 Day 3: 04 Alert - C2 Beacon

In this activity, you will continue your role as an SOC analyst for the California Department of Motor Vehicles (DMV).

- Your organization has just experienced another, more sophisticated attack. It's a red alert that Snort has identified as an emerging threat: A C2 beacon acknowledgement attack.
- The entire network is down across the state. As long as the network is down, none of the DMV offices can issue or renew licenses and registrations, or complete driving tests.
- As part of the Computer Incident and Response Team (CIRT), you need to establish an attacker profile that includes the tactics, techniques, and procedures used by the adversary, and document all of your findings. Like a real security analyst, you may need to research other sources to answer all the questions.

Instructions

Use the following indicator of attack:

- Destination IP: 188.124.5.100
- Source IP: 192.168.3.35
- Snort Message: ET MALWARE Zbot POST Request to C2

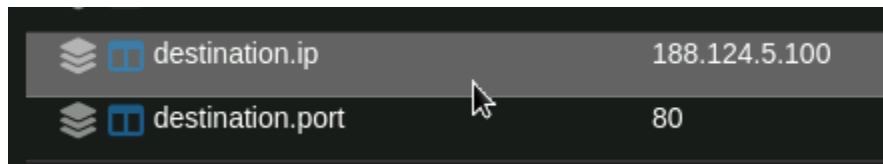
Note: You'll notice many attacks targeting the victim IP address. Please make sure to focus on the ET MALWARE Zbot POST Request to C2 attack.

Open Security Onion and look for C2 and Drilldown to see the details. Filter the results for the source IP 192.168.3.35

1. What is the rule that triggered this alert?

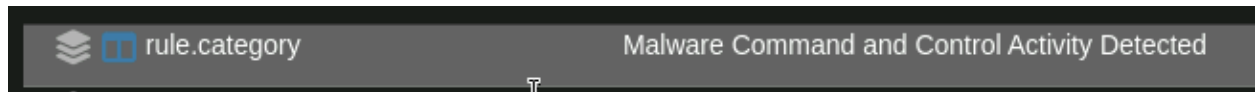
```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Zbot POST Request to C2"; flow:established,to_server; http.method; content:"POST"; http.uri; content:".php"; http.header; content:"Accept"; http.header_names; content:"[0d 0a]Accept[0d 0a]User-Agent[0d 0a]Host[0d 0a]Content-Length[0d 0a]"; depth:44; content:!"Accept-"; content:!"Content-Type[0d 0a]"; content:!"Referer[0d 0a]"; reference:md5,c86f7e024_04_08;)
```

2. According to the rule, what is the destination port?



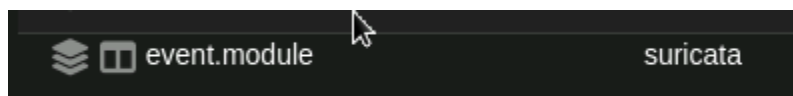
destination.ip	188.124.5.100
destination.port	80

3. Taking a closer look at the event fields, what is the rule category?



rule.category	Malware Command and Control Activity Detected
---------------	---

4. What is the event module that triggered the alert?



event.module	suricata
--------------	----------

(Use this link to answer the following questions: [A Look At The New Gameover Zeus Variant.](#))

5. What type of threat is this? **Botnet trojan**
6. Did this threat modify Windows registry keys? **yes**
7. Why does this threat modify Windows registry keys? **It does this for persistence. In order to survive reboots.**
8. What does C2 stand for and what is it? **Command and control, it's the connection between a hackers server and the infected bot.**
9. What is a sign that a computer may be under the control of a C2 server? **Suspicious network activity, performance issues, suspicious processes, unexpected behaviour.**

Bonus Questions

11. Name one of the most popular techniques an adversary uses to infect a host with a botnet. **phishing**
12. What are two ways an organization can mitigate this type of threat? **Employee awareness and an IPS, blacklisting p2p servers**
13. How far up the Cyber Kill Chain did this attack get? **All the way to action on objectives**
14. What procedure does this threat use to hide when it's discovered? **Deletes original .exe file.**
15. Why is this threat persistent? **Survives reboots by changing registry**

16. What tactic does this threat use to remain hidden and unnoticed? **To remain hidden it acts as a background process without any windows.**
17. Create a new case based off of your findings by clicking on the alert.
- Click the title and change it to Zbot Malware Discovery.
 - Scroll down and click ADD to include this event as an Observable.