McAfee Enterprise Security Manager Setup
For GameOver Zeus/Cryptolocker Traffic Detection

By Raj Samani, EMEA CTO McAfee, (Twitter@Raj_Samani)
and Martin DeJongh, Enterprise Technology Architect

The following guidance can be used to create an alert within McAfee Enterprise Security Manager (ESM) should any of your systems attempt to connect to the “lighthouse” IP address. McAfee ESM provides real-time visibility into all activity across systems, networks, databases, and applications. McAfee ESM provides real-time situational awareness, and this rule allows organizations to respond intelligently and efficiently in mitigating infected GameOver Zeus/Cryptolocker systems.
Create new Watchlist container with malicious external IP address for the external sinkhole system(s)

1. Open web browser and enter the URL of the McAfee ESM system (https://x.x.x.x).

2. Click on Login to load the McAfee ESM authentication GUI.

3. Enter the required McAfee ESM Authorization details and press Login button to load the ESM console.
4. Within the McAfee ESM console, select the **Watchlists** functionality (seventh icon at upper right).

5. Press the **Add button** to create a new **Watchlist**.
6. Within the Main Tab, select Static Watchlists, enter the name of the watchlist “GameOver Zeus and Cryptolocker IP List” and press the Next > button to continue.

7. Within the Values tab, select the IP address variable within the dropdown Type: field.
8. Add the specified sinkholes IP address (for example, **72.52.116.52**) within the **Values:** field and click on the **Finish** button to save the Watchlist.
9. You will see the new Watchlist entry “GameOver Zeus and Cryptolocker IP List” with a State of 1 values. Click on the OK button to close the System Properties window.
Create a custom Correlation Rule to detect a GameOver Zeus/Cryptolocker connection

Next, create a new Correlation Rule to trigger on outbound communication of Company Assets towards the external sinkhole IP address (72.52.116.52) over the specified port (4643).

1. Within the McAfee ESM Console select the Correlation functionality (third icon in upper right).
2. Within the Policy Editor window select the Default Policy > “Global Rule Correlation.” Then click on New and Correlation Rule in the upper menu list.
3. Next, create a new custom Correlation Rule with the Name: “GameOver Zeus and Cryptolocker Communication” with Severity: 80. You can enter a correlation rule description within the Description field.

4. Next, press on the icon “Show Normalization Taxonomy” (at upper right) and select the appropriate Normalization ID.
5. Within the **Normalization Taxonomy Window** select the (most) appropriate Normalization rule, for example, “Botnet (Normalization ID: 679477248).” Press the **OK** button to save the Normalization entry.
6. Next, create the required Correlation Logic within the Correlation Rule window. Drag and drop the Match Component icon within the Correlation Logic Field using the left mouse button.

7. The Match Component window opens. Press the Add button and select within the dropdown Add Filter Field the variable “Source IP,” “In.” Next click on the entry button to add a Value.
8. In the **Default Value Editor – IP Address IPv4/IPv6** window select the **Variables** tab. Next select the Variable “**Home_NET**” or/and specify within the **single value field** the corporate IP address range(s) for example (172.18.161.0/24). Press the **OK** button to save the **Source IP** entry. Again, entering multiple values is fully supported.

9. Click again on the **Add** button in the **Match Component Window** to enter an additional correlation filter variable for the **Destination IP** variable.
10. In the Add Filter Field select “Destination IP,” “In.” Next click on the entry button to add a Value.

11. Next, select the Watchlists Tab and in the overview window select the previously created Watchlist “GameOver Zeus and Cryptolocker IP List.” Press the OK button to save the Destination IP entry.
12. Click again on the **Add** button in the Match Component window to enter an additional correlation filter variable for the **Destination Port** variable.

13. In the Default Value Editor window select the **Ports tab.** Next specify within the single value field the communication port **4643**. Press the **OK** button to save the Destination Port entry.
14. Within the Match Component window now click on the **OK** button to save the added filter variables (Source IP, Destination IP, and Destination Port).
15. If the **Match Component** is set up accordingly, then click on the **OK** button in the Correlation Rule window to save the **Correlation Rule**.
16. Now you will need to enable the newly created Correlation Rule by first clicking on the value **disabled** within the Action column and then selecting the dropdown option **enabled**. After making the Rule alteration, you need to Rollout the new Correlation Policy by clicking on the **Rollout button**.

![Image of a computer screen showing the rule editor with a new rule and dropdown options for action settings and a rollout button.]

17. Finally, the ESM system will ask you if you want to **save all changes**. Click on **Yes** to roll out the newly created Correlation Rule. Check that this is directed against the **Global or Local Correlation Engine**; otherwise the new Correlation Rule will not trigger in the case of an attack or breach.

![Image of a computer screen showing a confirmation dialog box for saving changes with options for Yes and No.]
Create a custom Action Alarm for the Correlation Rule trigger “GameOver Zeus and Cryptolocker Communication”

1. After we create the Correlation Rule, we can also create a custom alert that will trigger if all variables within the Correlation Rule are met. Within the Policy Editor window, click on the “Create Alarm” button (at upper right).

2. Within the **Alarm Settings – Summary tab**, enter the Alarm name (for example, GameOver Zeus and CryptoLocker Alarm) within the Name field, specify the Alarm description within the Description Field, change the Alarm Severity to 80 and assign an **Alarm Assignee user/user group** to receive this alarm on triggering. Click on the **Devices Tab** to set up the Event Source location to trigger on.
3. Within the **Alarm Settings – Devices Tab**, select your dedicated **Advanced Correlation Engine component (ACE) >Global Rule Correlation** or select a **Receiver component >Local Rule Correlation**. Click on the **Next button** to set up the **Alert Output Actions**.

4. Finally select the required Alert Output Actions from the **Action tab**. After completion, click on the **Finish button** to save the newly created Alarm and then close the **System Properties** window. Afterward the Alarm will be armed and all preset actions will execute on triggering of the aligned “GameOver Zeus and CryptoLocker Communication” Correlation Rule.
5. Afterward, if you need to change the Output Actions, you can modify the Alarm by selecting the ESM system in the **Physical Display panel** on the left and then clicking on the **Properties button** (upper left). In the System Properties window select Alarms. Within the Alarm Option window select the **Alarm tab** and click on the **Edit button** to make the required Alarm alterations.