horizontal line

**Plus971 Cybersecurity**

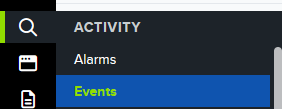
Investigative Report Using AlienVault

**7th August 2023**

**CRITERIA OF SEARCH:** Hostname Erika 07 August 2023 12 PM - 1:30 PM - DXB

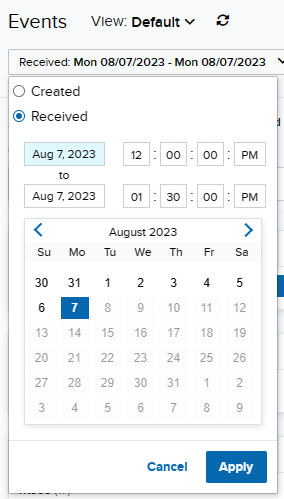
1. **Searchapp.exe made some outbound connections:** 
   1. **To what IPs were these outbound connections made to?** 
      1. **ANSWER:**

2.16.158.89(3)

192.229.221.95(2)

204.79.197.222(2)

13.107.3.254(1)

13.107.42.254(1)

13.107.6.254(1)

131.253.33.254(1)

144.2.14.25(1)

152.199.21.118(1)

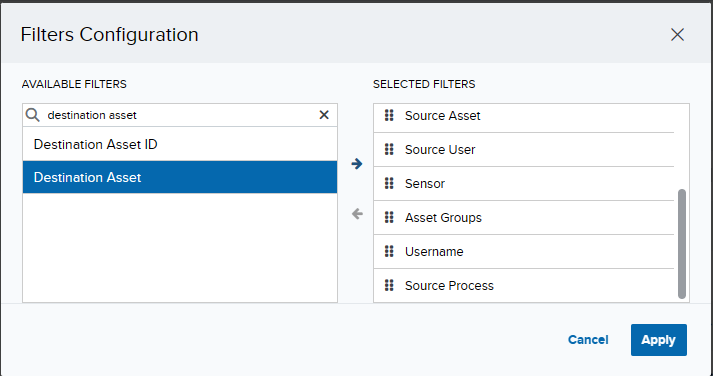
2.16.158.66(1)

204.79.197.254(1)

23.200.218.169(1)

51.104.34.11(1)

* + 1. **STEPS:**

1. First navigate to the events section under the Activity section.
2. Set the dates and times in this filter.
3. Apply the following filters:  
   Event name : outbound connection, Source asset: erika, source process: SearchApp.exe
4. 
5. We then get 16 records. And now while we can count them I found a filter that lists each unique destination ip and how many times it was used.
   1. Click configure filters in the left search and filters panel
   2. Then type “destination asset” in available filters
   3. 
   4. Hit the blue right arrow then hit apply
   5. After the page refreshes, scroll down to the destination asset filter and then copy all the records.
   6. 

**B. Is this activity suspicious? Please explain.**

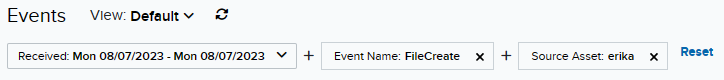
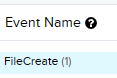
I would classify the behavior within the time frame suspicious as the application contacts multiple servers within the span of a minute, typically a website/app can have multiple CDNs or web servers around the world for load balancing or quicker response times however the application typically connects to one of these servers, however here it connects to servers in the UAE, Singapore the US etc.., thus warranting suspicion.

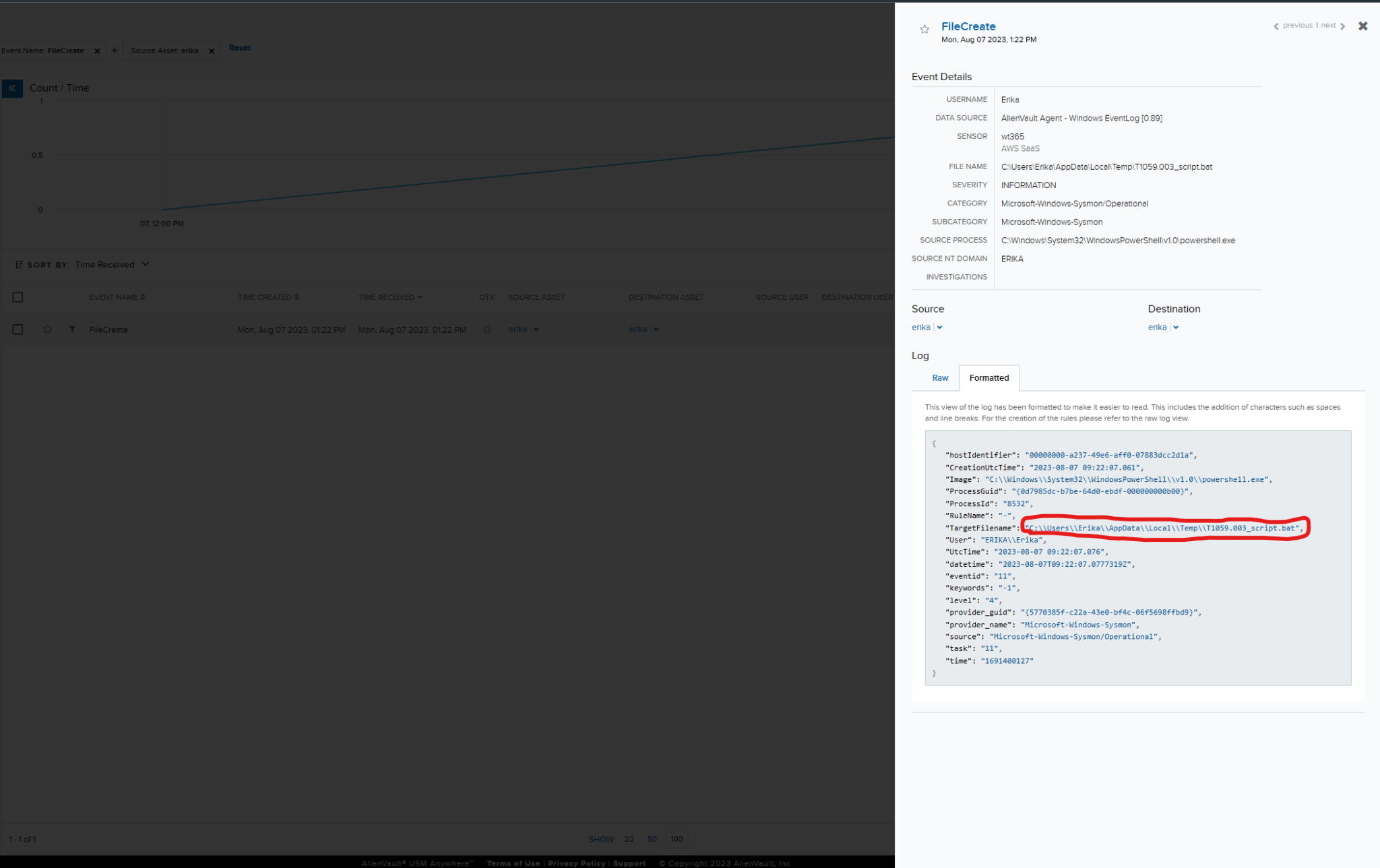
**2. A file was created during this time:**

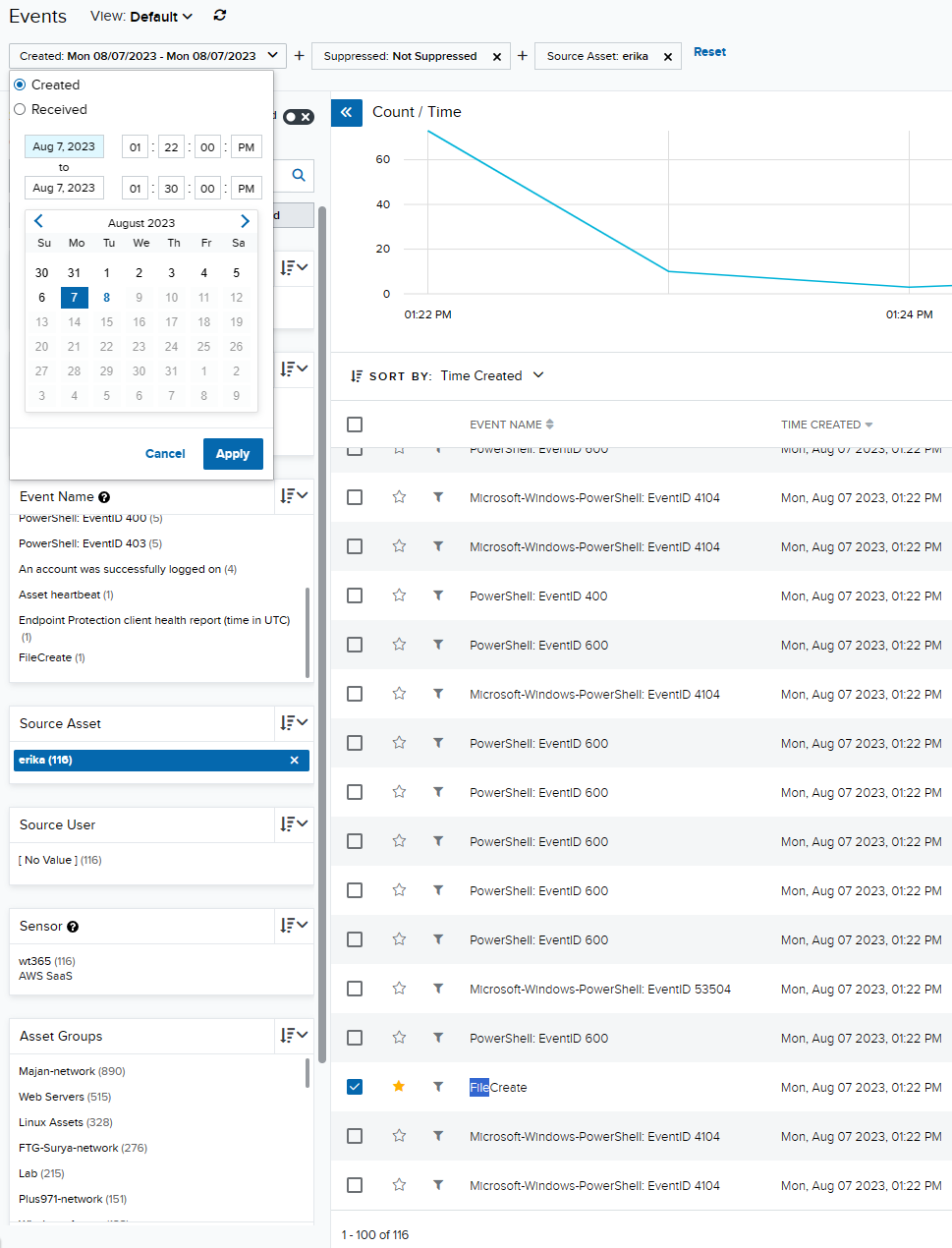
**a. What is the name of the file?**

**ANSWER**: T1059.003\_script.bat

**STEPS:**

1. Keeping the same time frame as before we remove the following filters:
   1. Event.name and source process
   2. 
   3. In the event name filter scroll until you find the file created event, of which there is only 1.
   4. Further expanding the event we can see the file name in the log.

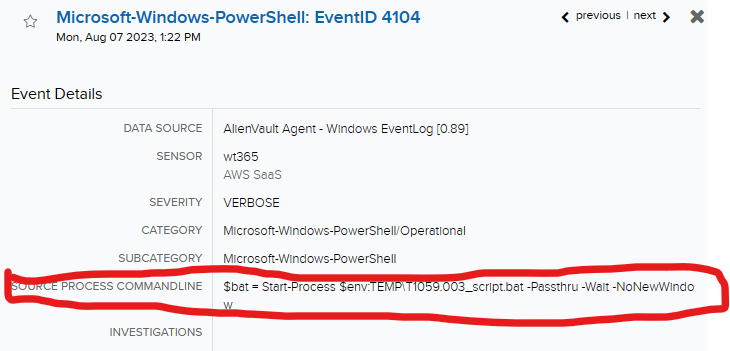


**b. This file was started and then stored inside a variable, what is the name of the variable?**

**ANSWER**:

$bat

**STEPS**:

1. We see the time of the event occurs at 1:22 PM so we filter from 1:22 - 1:30
2. Then we find the file create event and look at the logs after
3. Sort the events by time received from smallest to largest
4. Then keep looking at all the events
5. Until you reach the file create then favorite it as a reference point as the answer will be in an event after this.
6. And here we can see that the start-process command along with the file path listed in the question
7. 

**c. What was this variable utilized for? Provide a detailed explanation.**

**ANSWER:**

Storing the command that will be used when it needs to be run?

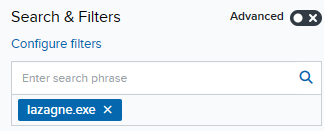
**3. A process is being executed on the target system.**

**a. What lazagne.exe is utilized for?**

**ANSWER**:

| [CSOC - 032022,Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries](https://otx.alienvault.com/pulse/6226df0cb6b7b2aee29d37f5?utm_source=USMA&utm_campaign=meta&utm_medium=events) |
| --- |

**STEPS**:

1. I Removed all filters except source asset: erika
2. Using the search phrase box i typed in “lazagne.exe” and hit enter
3. 
4. The was only 1 event and upon opening it i saw:
5. 

**b. Mention the source process command line.**

**ANSWER**:

| C:\Users\Erika\AppData\Local\Temp\fc\_art\_2036630015\lazagne.exe browsers |
| --- |

**STEPS:**

1. In the same section as the previous question just a few fields above i saw:
2. 

**c. Mention the Process ID and Process GUID.**

**ANSWER**:

"ProcessGuid": "{0d7985dc-b765-64d0-22dd-000000000b00}",

"ProcessId": "10032",

**STEPS**:

1. Continuing in the same alert as the last 2 questions if we scroll down to the formatted logs we can see:
2. 

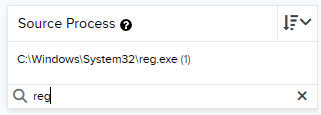
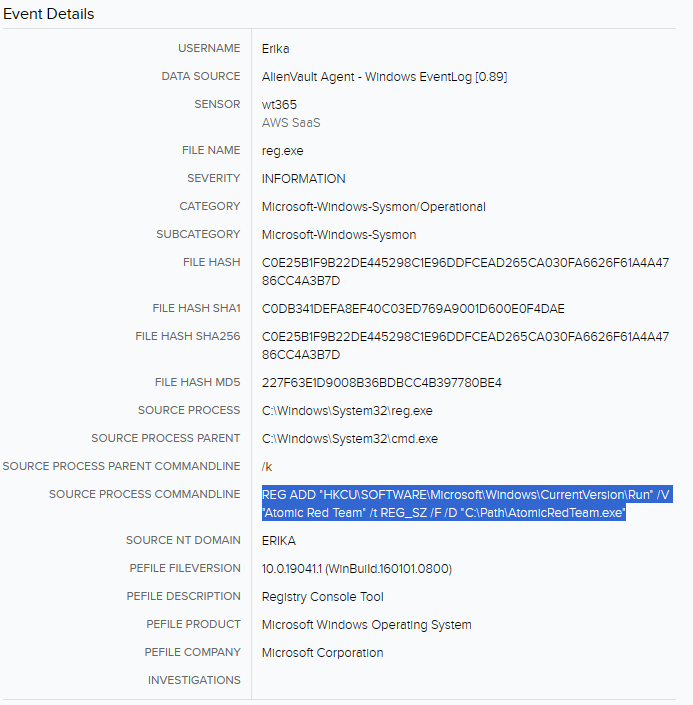
**4. Reg.exe was executed:**

**a. What was the command executed with reg.exe?**

**ANSWER**:

| REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Atomic Red Team" /t REG\_SZ /F /D "C:\Path\AtomicRedTeam.exe" |
| --- |

**STEPS**:

1. I Removed all filters except source asset: erika
2. Scroll down to the source process filter and type reg and click on C:\Windows\System32\reg.exe(1)
3. 
4. These filters yield only 1 event and upon opening it we can see the source process command line
5. 

**b. Provide reg.exe’s MD5 hash**

**ANSWER:**

227F63E1D9008B36BDBCC4B397780BE4

**STEPS:**

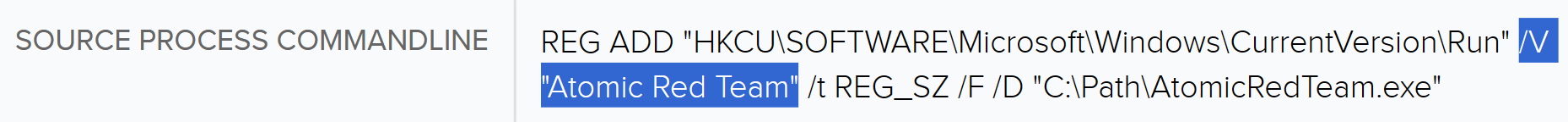
1. In the same section we can see the file hash MD5

**c. What is the name of the Registry Value being added using reg.exe?**

**ANSWER:**

"Atomic Red Team"

**STEPS:**

1. 
2. In the answer to the previous question we can see the registry that is modified, see the highlighted bit. /V indicating the value being added.

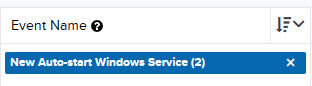
**5. A windows service was started automatically.**

**a. What was the name of this service?**

**ANSWER:**

netsvcs

**STEPS:**

1. I Removed all filters except source asset: erika
2. Looking through the event name filter i found the “New Auto-start windows service” filter
3. 
4. We find 2 records with similar info
5. Opening one of them leads to the name of the service
6. 

**b. What's the File Path for this service?**

**ANSWER:**

| %SystemRoot%\System32\qmgr.dll |
| --- |

**STEPS:**

1. In the same section we can see the file path

**c. What's the SOURCE PROCESS COMMAND LINE?**

**ANSWER:**

| C:\Windows\System32\svchost.exe -k netsvcs -p |
| --- |

**STEPS:**

1. In the same screenshot as before we see the answer.