Hafnium Exchange Vuln Detection - KQL - Pastebin.com

1. let networkEvent = DeviceNetworkEvents
2. | where ActionType == "InboundConnectionAccepted" and InitiatingProcessFileName =~ "System"
3. | extend netTimestamp = Timestamp
4. | project DeviceId, DeviceName, netTimestamp, RemoteIP, RemotePort; //Grab a table of all accepted inbound connections, projecting the Timestamp for further manipulation
5. let shellWrite = DeviceFileEvents
6. | where ActionType == "FileCreated" and FolderPath has "inetpub" and FileName has_any (".php", ".jsp", ".js", ".aspx", ".asmx", ".asax", ".cfm", ".shtml")
7. | project DeviceName, DeviceId, Timestamp, FileName, FolderPath; //Grab a table of all created files in inetpub, with a file extension ending in ".php", ".jsp", ".js", ".aspx", ".asmx", ".asax", ".cfm", ".shtml". Projecting timestamp for further manipulation
8. DeviceFileEvents
9. | where (FileName =~ "applicationHost.config" or FileName =~ "administration.config") and FolderPath contains "inetpub" //Grab all instances of updates to the IIS applicationHost.config or administration.config
10. | join shellWrite on DeviceName, DeviceId
11. | join networkEvent on DeviceId, DeviceName
12. | extend time_diff = datetime_diff('second',Timestamp,Timestamp1) //create a time differential column for shellWrite and config update
13. | extend netTimeDiff = datetime_diff('second',Timestamp1,netTimestamp) //create a time differential column for networkEvent and the shellWrite
14. | where (time_diff <= 60 and time_diff >= 0) and (netTimeDiff <= 10 and netTimeDiff >= 0) //differential filtering for networkEvent and shellWrite

---