NC STATE

Samuel Carter <swcarter@ncsu.edu>

Query in Crowdstrike to determine machines that might be affected.

1 message

Jeremiah Jackson <jeremiah.jackson@dpi.nc.gov> Fri, Jul 19, 2024 at 10:56 AM
To: "ncdpidtldirectors@googlegroups.com" <ncdpidtldirectors@googlegroups.com>
Cc: "list@ncet.net" <list@ncet.net>

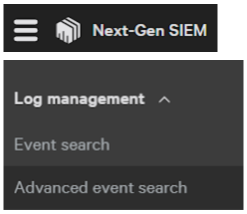
Hello Everyone,

Below is how to query your CrowdStrike Falcon Console to see devices that might be affected. This shows the devices that received the bad update and have not checked in to CrowdStrike within the last 4 hours.

Attached is the query info. If you cannot open the txt file. You can also get the query at this google doc.

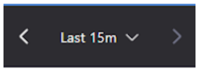
Login to CrowdStrike Falcon Online
https://falcon.crowdstrike.com/login/

Once logged in
Click the Three Lines upper left corner
and Choose Next-Gen SIEM - Advanced Event Search



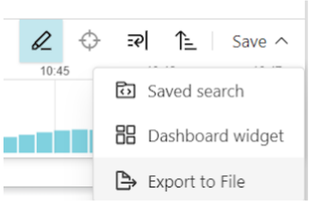
Once there open the attached TXT file and copy the contents.
Paste the contents in the Search Box

Find the box that says Last 15 minutes
Click the Drop Down and choose Last 12 hours.



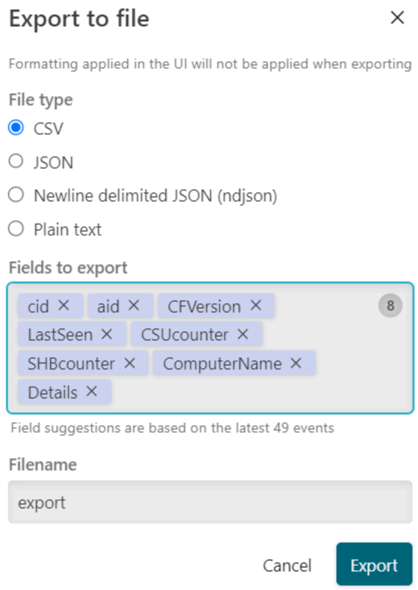
Then Click Run on the right
In the details column of this search you will either see "OK" or "Check"
This query shows all devices that received the bad update but have not been online in the last 4 hours.
Those are the devices you need to check on.

To export this list.
Click the "SAVE" button on the right of the results.
Choose Export to File



Once the new window pops up.
Add the following fields: (Capitalization Matters)
ComputerName & Details

Give the file a name and click Export



Export to file ✕

Formatting applied in the UI will not be applied when exporting

File type

● CSV
○ JSON
○ Newline delimited JSON (ndjson)
○ Plain text

Fields to export

cid ✕ aid ✕ CFVersion ✕ LastSeen ✕ CSUcounter ✕ SHBcounter ✕ ComputerName ✕ Details ✕ 8

Field suggestions are based on the latest 49 events

Filename

export

Cancel Export

Jeremiah Jackson
Chief Information Security Officer
Office of Risk Management and Cybersecurity
NC Department of Public Instruction
P: (828) 283-0022
jeremiah.jackson@dpi.nc.gov
Follow us: Facebook, Twitter, Instagram, and YouTube

North Carolina Department of
PUBLIC INSTRUCTION

Visit us on the web at https://dpi.nc.gov . All e-mail correspondence to and from this address is subject to the North Carolina Public Records Law, which may result in monitoring and disclosure to third parties, including law enforcement.

--
You received this message because you are subscribed to the Google Groups "NCDPI Digital Teaching and Learning - Directors Group" group.
To unsubscribe from this group and stop receiving emails from it, send an email to ncdpidtldirectors+unsubscribe@

googlegroups.com.
To view this discussion on the web visit https://groups.google.com/d/msgid/ncdpidtldirectors/SA2PR03MB58171C0D53264E9A0F2E8CE1BEAD2%40SA2PR03MB5817.namprd03.prod.outlook.com.

CS-EndpointQuery.txt
3K