Second Zerologon attacker seen exploiting internet honeypot

By Kevin Beaumont

Published: 2020-10-16 · Archived: 2026-04-05 15:35:45 UTC

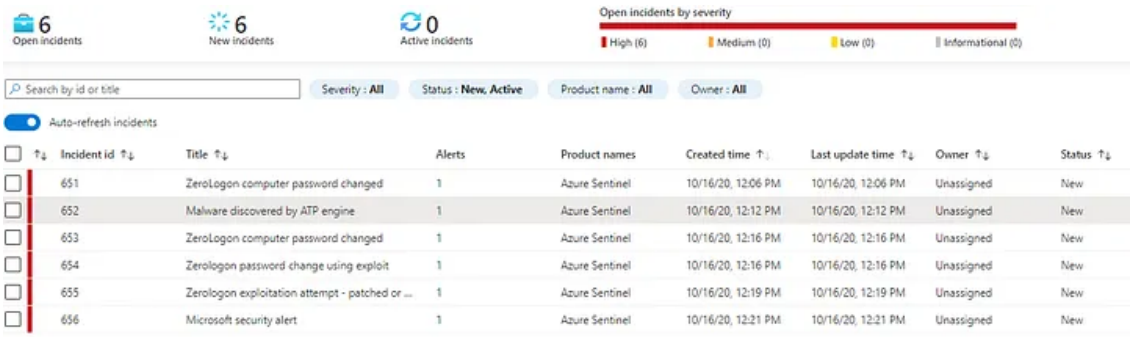
About three weeks I detected an attacker exploiting Zerologon on my personal honeypot:

There is more activity today, which shows proof of attackers using Zerologon for remote code execution on random internet endpoints.

At 11:01UTC, IP address 124.70.137.246 arrived in BluePot and tried exploiting Zerologon.

Azure Sentinel tipped me off:

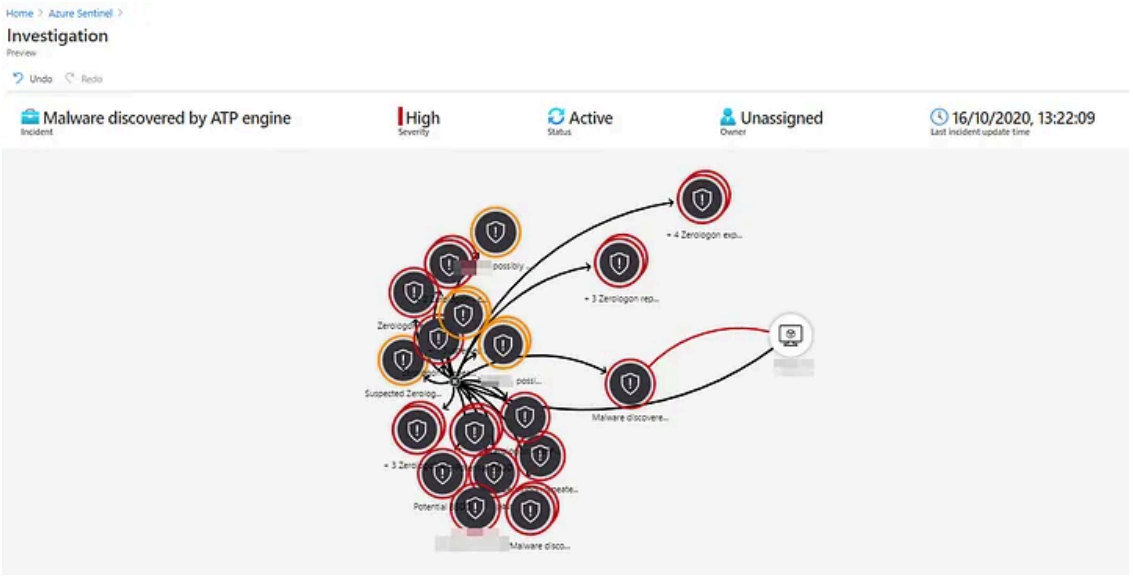
Press enter or click to view image in full size



Incident id	Title	Alerts	Product names	Created time	Last update time	Owner	Status
651	ZeroLogon computer password changed	1	Azure Sentinel	10/16/20, 12:06 PM	10/16/20, 12:06 PM	Unassigned	New
652	Malware discovered by ATP engine	1	Azure Sentinel	10/16/20, 12:12 PM	10/16/20, 12:12 PM	Unassigned	New
653	ZeroLogon computer password changed	1	Azure Sentinel	10/16/20, 12:16 PM	10/16/20, 12:16 PM	Unassigned	New
654	Zerologon password change using exploit	1	Azure Sentinel	10/16/20, 12:16 PM	10/16/20, 12:16 PM	Unassigned	New
655	Zerologon exploitation attempt - patched or ...	1	Azure Sentinel	10/16/20, 12:19 PM	10/16/20, 12:19 PM	Unassigned	New
656	Microsoft security alert	1	Azure Sentinel	10/16/20, 12:21 PM	10/16/20, 12:21 PM	Unassigned	New

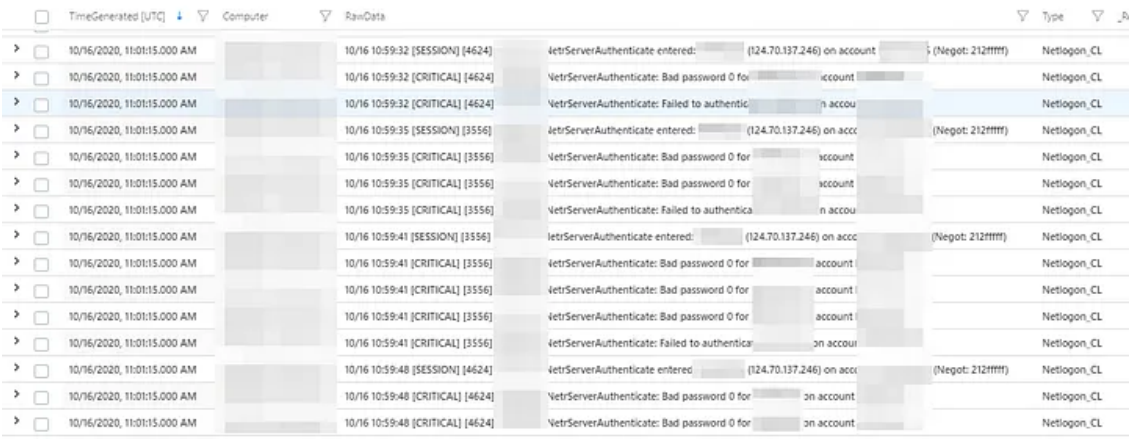
(times in UK time, i.e. UTC+1).

Press enter or click to view image in full size



Upon examining logs we can see the problems:

Press enter or click to view image in full size



That is an IP in Huawei Cloud Service, according to Shodan:

Source: https://doublepulsar.com/second-zerologon-attacker-seen-exploiting-internet-honeypot-c7fb074451ef