HORIZON3.ai

CASE STUDY

FROM REACTIVE TO REAL-TIME:

Using Iranian Tradecraft to Eliminate a Critical AD Risk

Iranian state-aligned threat groups are increasingly targeting identity systems as the fastest path to enterprise compromise.

A leading global manufacturer wanted to understand their exposure: could an adversary using Iranian tradecraft covertly take control of their Active Directory environment?

To answer this, they used Horizon3.ai's NodeZero® to run an autonomous pentest modeled on real-world attacker behavior.

Discovery:
Zerologon Exposure

Within hours, NodeZero identified Zerologon (CVE-2020-1472) on a critical domain controller, a flaw that enables full domain compromise.

This attack path aligns with how Iranian groups like MuddyWater and Magic Hound operate, using credential abuse and native tools to escalate privileges and move laterally without detection.

For the organization, this represented a direct path to its most critical systems.

Response:
Immediate Fix + Retest

Teams mobilized immediately to:

- Patch the domain controller
- Harden affected systems
- Verify no additional exposure

But remediation alone was not enough.

They re-ran the same NodeZero test using the same adversary techniques to validate the fix.

Result:
Attack Path Closed in just over 24 Hours

Within ~ 24 hours:

- Zerologon was no longer exploitable
- The domain compromise path was eliminated
- Adversary techniques associated with Iranian groups were no longer viable for domain compromise

This was validated, not assumed.

The Impact: Why This Matters Now

As Iranian threat activity continues to escalate, organizations can no longer rely on assumed security or point-in-time fixes, especially in identity systems. This engagement proved that:

- Critical exposures can be identified and remediated quickly
- Security effectiveness must be validated, not inferred
- Continuous adversarial testing is essential against nation-state tradecraft

Takeaway

With NodeZero, the organization:

1. **Found a critical identity weakness**
2. **Fixed it rapidly**
3. **Proved it was eliminated**

All in under a little over one day.

In a threat landscape shaped by nation-state actors, continuous validation, not assumptions, is what defines real security.