Breaking the Bank: How NodeZero® Secured a Financial Giant in 14 Hours

Use Case About NodeZero® for Financial Services

NodeZero® delivers unmatched value to financial services organizations by identifying exploitable vulnerabilities, prioritizing critical risks, and providing actionable remediation guidance. By emulating real-world attacks, NodeZero enables organizations to secure sensitive data, maintain compliance, and proactively strengthen their defenses against evolving threats – all in hours, not weeks or longer.

Example Financial Services Company

In under 14 hours, NodeZero exposed critical vulnerabilities, including three domain compromise attack paths, and revealed systemic issues like weak access controls and poor endpoint security. Its actionable insights enabled swift remediation, showcasing NodeZero's power to help financial institutions strengthen their defenses proactively.

Use case details:

On Monday, May 6, 2024, a large financial service company conducted their first autonomous internal pentest using NodeZero. The pentest lasted 13 hours and 36 minutes before it was completed.

In that period of time, NodeZero identified 586 critical impacts during the pentest. Out of the critical impacts, three of the impacts resulted in Domain Compromise.

HORIZON3.ai
~~TRUST~~ BUT VERIFY

The domain and host compromise summary:

Domain Compromise: NodeZero compromised the domain administrator accounts.

Host Compromise: NodeZero compromised credentials with remote code execution capability that led to host compromise on one device, then it compromised another 47 hosts due to this weakness.

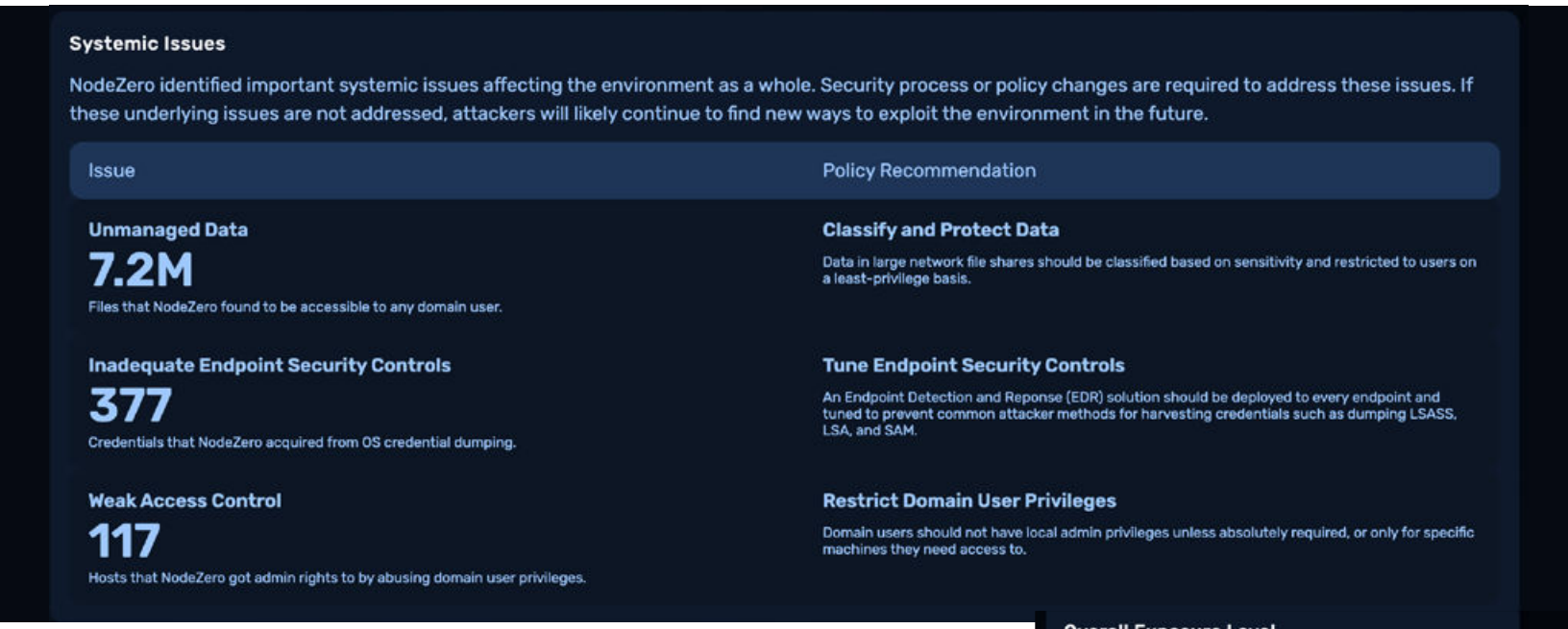
Host Compromise: NodeZero compromised credentials with local admin privileges that led to host compromise on one device, then it compromised 115 other hosts.

The weaknesses found:

H3-2021-0043: LSA Dump affecting a certain host. The weakness was leveraged in 101 attack paths leading to Domain Compromise, Host Compromise, and 3 other impacts.

H3-2021-0044: LSASS Dump affecting a certain host and 602 other hosts. The weakness was leveraged in 386 attack paths leading to Domain Compromise, Host Compromise, and 3 other impacts.

H3-2021-0042: SAM Dump affecting a certain host and 91 other hosts. The weakness was leveraged in 92 attack paths leading to Host Compromise and Sensitive Data Exposure.



The systemic issues discovered:

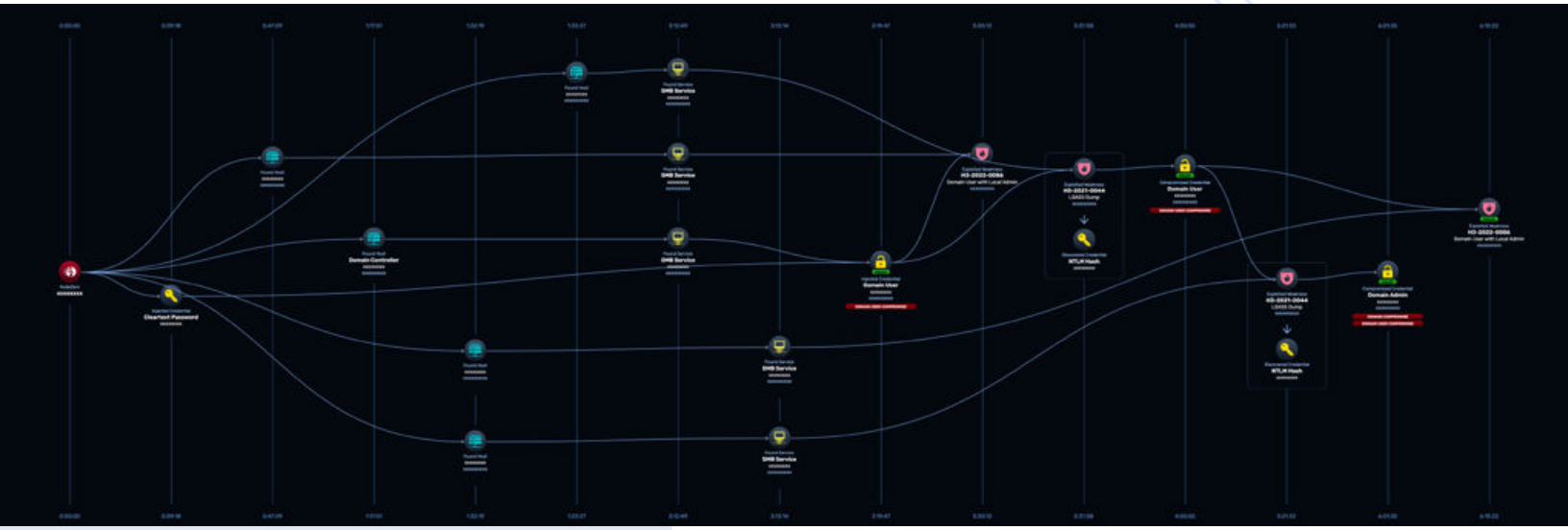
Unmanaged Data: NodeZero found 7,239,986 files to be accessible to any domain user.

Inadequate Endpoint Security Controls: NodeZero acquired 377 credentials from OS credential dumping.

Weak Access Control: NodeZero obtained admin rights to 117 hosts by abusing domain user privileges.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

The attack path that led to domain and user compromise:



STATE OF THE INDUSTRY

In the Financial Services industry in just the third quarter of 2024,

141
Breaches

impacted over

16
Million Victims

The final outcome:

Using the remediation guidance NodeZero provided, the financial services organization has remediated the issues, and at this time, NodeZero cannot obtain domain and/or user compromise using the same attack paths it previously discovered.

Conclusion:

With NodeZero, financial services organizations can confidently defend against sophisticated cyber threats by transforming their security posture in record time.
By uncovering and remediating vulnerabilities that matter most, NodeZero empowers organizations to safeguard sensitive data, meet regulatory requirements, and protect their reputation – ensuring resilience in an ever-evolving threat landscape.

 @Horizon3ai info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST BUT~~ VERIFY