15.02.2024 – 11:54 Uhr

Horizon3.ai Unveils Phishing Impact Testing to Help Organizations Understand the Impact of Phished Credentials

Horizon3.ai Unveils Phishing Impact Testing to Help Organizations Understand the Impact of Phished Credentials

Empowering Decision-Makers with Precise Insights into Phishing Consequences and Recovery Strategies

San Francisco, February 15th, 2024 –Horizon3.ai, a pioneer in autonomous security solutions, today announced the launch of its first-to-market Phishing Impact test capability within NodeZero™. This new capability marks a significant advancement in penetration testing, addressing a critical gap in understanding the real-world implications of phished credentials.

Horizon3.ai Co-Founder and CEO Snehal Antani said: "Phishing is the most common type of cyberattack. Today there are over 1.35 million unique phishing sites detected worldwide. Every day, IT and security teams leverage sophisticated, state-of-the-art security training and in-house phishing tests to raise security awareness and identify susceptible human targets, yet every day, new attacks succeed because humans are naturally responsive, and attacks are increasingly sophisticated. Our Phishing Impact test is first-to-market and gives you the ammunition required to drive meaningful improvements to reduce the credential attack surface of your organization."

Business leaders often dismiss the threat of entry-level employees who click on malicious links, leading to frustration by IT and security organizations. The Phishing Impact test delivered by NodeZero can help those IT and security teams accurately convey the "blast radius" of those phished credentials, proving that sensitive data was indeed at risk.

"The NodeZero Phishing Impact test is the natural complement to supplement phishing tools such as KnowBe4, Proofpoint, InfosecIQ, Mimecast, and in-house initiatives, and it represents the next step in responsible cybersecurity diligence," said Stephen Gates, Principal Security SME at Horizon3.ai. "Organizations can now prove the end-to-end impact when an intern's credentials were phished during a training exercise."

By adding a few lines of JavaScript code provided by NodeZero to phishing pages created using popular testing tools, organizations can automatically channel captured credentials into an active NodeZero penetration test. This test then utilizes those phished credentials in conjunction with exploitable security weaknesses discovered by NodeZero as part of its attack against the network.

The outcome is a comprehensive report detailing the impact of each phished credential, offering organizations unprecedented insights into their security posture. This not only enhances their understanding of potential threats but also drives effective improvements to safeguard their systems against real-world attacks.

"We tested the new capability that NodeZero brings to the table against a small group of people who we call our 'clickers,' and three users entered their valid credentials. NodeZero then used those credentials during its internal pentests, and the results were enlightening, to say the least. We do plan to incorporate this solution into our phishing program going forward. We love the perspective of using credentials to see what different users can access, and the integration with KnowBe4 was very easy to implement," said an Information Security Analyst for a large U.S. retail chain.

"I was super excited about the Phishing Impact test in NodeZero. It's the exact thing we've been missing and will, no doubt, be eye-opening for our users and executive team," said a Database Administrator for a public services organization.

Horizon3.ai's Phishing Impact test with NodeZero is a first-of-its-kind tool, equipping organizations with the knowledge and resources to proactively address vulnerabilities in their cybersecurity defenses.

Easily Interoperates With Popular Phishing Awareness Solutions

The NodeZero Phishing Impact test is resource-light: it's easily conducted by IT and security team members by simply adding a few lines of JavaScript generated by NodeZero to their phishing page. Credentials of users "hooked by the lure" are automatically injected into a running NodeZero pentest via the JavaScript copied into the phishing page.

With legitimate credentials in hand, this type of testing reveals if an attacker would next be able to:

- Find and gain access to your private data stores
- Gain admin access to other hosts in your network
- Move laterally to compromise your cloud environments
- Elevate their privileges and take over your domains
- Exploit unpatched vulnerabilities in your internal systems
- Achieve even more

The Phishing Impact test is conducted with Horizon3.ai's secure methods that ensure clear text credentials are not maintained outside of the test's ephemeral infrastructure.

Each phished credential is added to the NodeZero platform as a “Notable Event” with a timestamp. Testers see the running list of credentials being tested in the Credentials window in the NodeZero UI.

Helps Security Teams Access Policies and Responses, Prioritize Systemic Issues

In addition to revealing to users the potential gravity of being phished, NodeZero Phishing Impact testing helps security teams assess their defenses. Learning that a phished employee could lead to domain compromise can inspire security teams to tighten their least privilege controls.

See a demonstration of a Phishing Impact test.

Sign up for a free trial of NodeZero. [check]

About Horizon3.ai

The NodeZero™ platform empowers organizations to continuously find, fix, and verify exploitable attack surfaces. It is the flagship product of Horizon3.ai, founded in 2019 by former industry and U.S. National Security veterans. Our mission is to help organizations see their networks through the eyes of the attacker and proactively fix problems that truly matter, improve the effectiveness of their security initiatives, and ensure that they are prepared to respond to real cyberattacks.

Follow Horizon3.ai on LinkedIn and on X, formerly known as Twitter.

Contact: Horizon3.AI Europe GmbH,
Sebastian-Kneipp-Straße 41, 60439 Frankfurt am Main, Germany,
Web: www.horizon3.ai

PR-agency: euromarcom public relations GmbH,
Muehlhohle 2, 65205 Wiesbaden, Germany,
Tel.: +49 611 973150, E-Mail: team@euromarcom.de,
Web: www.euromarcom.de

- - - -