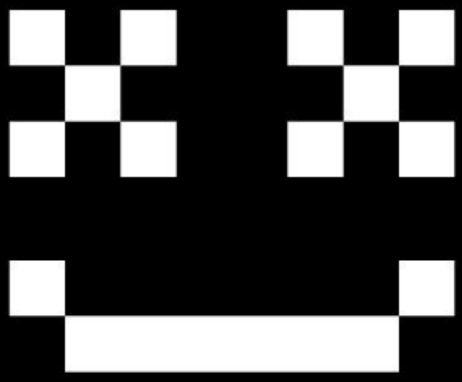
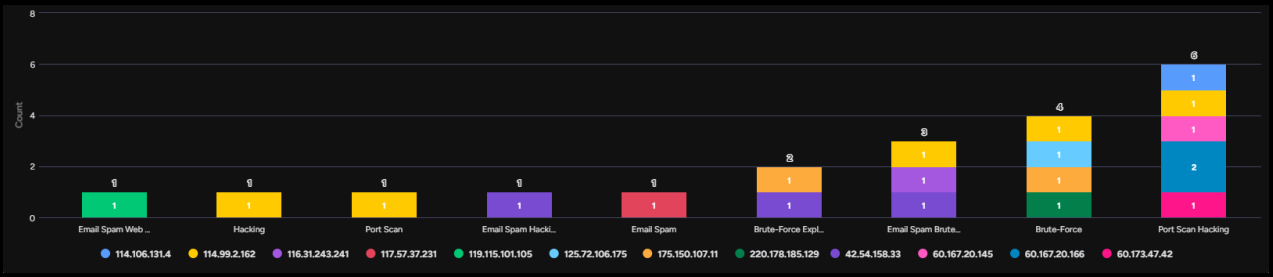
DEADPXLZ CyberSec Summary



2023

1. External Email Analysis:

Last year S³ actively monitored and investigated malicious emails received/rejected by the PXLZ team. Several potential threats were identified upon closer examination and tailored recommendations made by S³ were promptly implemented to prevent and reduce future attacks against the DEADPXLZ ecosystem.



Top three attack vectors identified:

- **Port Scan Attacks** - Port scan hacking involves the unauthorized probing of a computer system's ports to identify open ports and services, aiming to discover vulnerabilities for potential exploitation.

- **Brute Force Attacks** - Brute force is a trial-and-error method used in hacking and cryptography, systematically attempting all possible combinations to crack passwords, encryption, or authentication mechanisms.

- **Email Spam Brute Force Attacks** - Email spam brute force is a targeted attack on email accounts, where attackers systematically try different username and password combinations to gain unauthorized access, often employed in conjunction with spam campaigns for malicious activities.

The implementation of a strict DMARC policy and phishing awareness training has been instrumental in greatly reducing DEADPXLZ external attack surface. To date, phishing remains one of the most prominent attack vectors for malicious actors within the crypto-sphere and often leave developers and their corresponding communities rekt. Cardano-based projects have been somewhat insulated from these types of attacks for quite some time, however with the rise in popularity of Cardano these attacks remain imminent and ever-increasing. Additionally, our research continues to conclude that many developers nor their teams within the space take phishing-based threats seriously. DEADPXLZ continues to excel on this front and has diligently worked with S³ over the past year to protect the DEADPXLZ brand and maintain their community's trust via:

- **External Email Analysis** – Analyzing/correlating and rejecting emails based on their malicious nature and origins. An 85% drop in malicious emails received was observed after implementation.

- **Phishing Simulations & Training** – DEADPXLZ developer(s) and team members are subjected to several simulated phishing campaigns to increase both user awareness and overall security posture.

2. External/Web Application Analysis:

S³ continues to observe (large) Cardano Stakepools/DEXs/Projects to be misconfigured, unpatched, and potentially vulnerable to malicious attacks. Our research continues to yield owners of these vulnerable systems remain unaware or indifferent to the importance of sound security controls, patch management, & risk mitigation strategies. Though some of the vulnerabilities identified may not be actively exploited, they simply remain a ticking timebomb for the communities involved.

- **External/Web Application Analysis** – DEADPXLZ continues to exceed the standards of best practices in remediating external vulnerabilities identified by S³ and remains one of the best secured stakepools on Cardano. Critical items such as the Express Stack Trace (OWASP - Improper Error Handling) vulnerability observed in early 2023 were remediated immediately upon the disclosure of sensitive information via verbose error message(s). S³ acknowledges all critical vulnerabilities identified to have been promptly addressed and remediated in a timely manner by the DEADPXLZ team.

2. Incident Response:

On October 11th, 2023 the DEADPXLZ team and S³ observed a user abusing webhook permissions and impersonating an admin. The attacker proceeded to share a malicious Ethereum-based wallet drainer link within the server. Impact was found to be extremely limited and did not affect or compromise any DEADPXLZ admin accounts due to the swift actions taken by the team. The user was banned immediately and a takedown of malicious website pxlz[.]ink escalated by S³ was completed within 24hrs. It should be noted: “No single approach can provide complete protection against all attacks.” However, incorporating an incident response plan and a security team can greatly aid in reducing the impact of the attack amongst the broader community.

- **Discord Incident Response** – This incident was thoroughly investigated and remediated by both DEADPXLZ & the S³ security team. Webhook permissions were promptly disabled and the abuse method was promptly shared with the greater community. DEADPXLZ developer remained transparent through the entire investigation process and supplied all necessary logs needed by S³. As a result, S³ was able to quickly provide a transparent response to the DEADPXLZ community, thus maintaining trust.