INFERMAL Study Findings

Jonathan Zuck

Overview

The report investigates the factors influencing the registration of malicious domains, particularly those used for phishing. It analyzes various features related to domain registration, proactive verification, and reactive security practices.

INFERMAL seems to aim at validating previously anecdotal claims regarding the prevalence of DNS abuse linked to factors such as cost, payment methods, and registration methods. **The report does not offer solutions**; instead, it simply confirms how these factors influence certain rates of DNS abuse. Additionally, it does not discuss the commercial realities associated with domain sales.

Conclusion: The report highlights the importance of economic incentives, proactive verification, and stringent restrictions in mitigating domain abuse. It provides valuable insights for registrars and policymakers to develop effective anti-abuse strategies.

Key Findings

Economic Incentives

- **Lower Registration Fees**: Each dollar reduction in registration fees corresponds to a 49% increase in malicious domains.
- **Free Services**: The availability of free services, such as web hosting, drives an 88% surge in phishing activities.
- **Discounts**: Discounts on domain registrations are associated with a significant increase in malicious registrations.

Proactive Measures

- **Stringent Restrictions**: Implementing stringent restrictions can reduce abuse by 63%.
- **API Access**: Registrars providing application programming interface (API) access for domain registration or account creation experience a 401% rise in malicious domains.
- **Verification Practices**: Proactive verification of registrant information, such as email and phone validation, significantly reduces malicious registrations.

Key Findings

Reactive Measures

- **Mitigation Times:** The impact of mitigation times on reducing domain abuse is minimal. Even brief uptimes can provide attackers with valuable credentials and financial gain.

Registrar and TLD Preferences

- **Concentration of Abuse:** Malicious registrations are not uniformly distributed and tend to be concentrated in certain registrars and TLDs.
- **Registrar Practices:** Registrars offering lower prices and free services are more likely to attract malicious registrations.