

DOMAIN INTELLIGENCE LOG

Evidence ID: DOMAIN-2024-11-13

Source: WHOIS / DNS / SSL Lookup

Status: Player-facing

[2024-11-15 00:18:44] DOMAIN_LOOKUP_STARTED

Target Domain: disc0rd-alert.com

[2024-11-15 00:18:45] WHOIS_RESULT

Domain: disc0rd-alert.com

Registrar: Namecheap

Created: 2024-11-13 09:14:22 UTC

Status: Active

[2024-11-15 00:18:45] DOMAIN_AGE_CHECK

Domain Age: Approximately 36 hours before the attack

Risk Indicator: RECENTLY_REGISTERED_DOMAIN

[2024-11-15 00:18:46] REGISTRANT_CHECK

Registrant Name: REDACTED

Registrant Organization: REDACTED

Privacy Service: Privacy Guard

Risk Indicator: OWNER_IDENTITY_HIDDEN

[2024-11-15 00:18:47] DNS_CHECK

Name Server 1: ns1.sharedhost-99.net

Hosting Pattern: Shared hosting infrastructure

Risk Indicator: LOW_TRUST_HOSTING

[2024-11-15 00:18:48] SSL_CERTIFICATE_CHECK

SSL Provider: Let's Encrypt

Certificate Type: Free SSL certificate

Certificate Status: Valid

Risk Indicator: FREE_CERTIFICATE_USED

[2024-11-15 00:18:49] ANALYSIS_SUMMARY

The domain disc0rd-alert.com was created shortly before the attack and uses a look-alike spelling of a trusted service name. The registrant identity is hidden behind privacy protection, and the domain points to shared hosting name servers.

[2024-11-15 00:18:50] FINAL_ASSESSMENT

Classification: SUSPICIOUS

Possible Use: Phishing / Account credential theft

Recommended Action: Compare with email header evidence and login activity logs.