Incident Reporting Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| **I am:**  the effected entity ☑ reporting incident affecting other entity | | | | |
| **Contact Information of the Reporter** | | | | |
| Name & Role/Title |  Individual ☑ Organization | | | |
| Organization name (if any) | CatchPhish | | | |
| Contact No. | 8779959071 | | Email: | catchphish@gmail.com |
| Address: | Kj Somaiya college of engineering | | | |
| **Basic Incident Details** | | | | |
| Affected entity  (if not same as reporting entity above) | | Union bank of India | | |
| Incident Type | | | | |
| Targeted scanning/probing of critical  Data Breach Attacks or malicious/suspicious activities  networks/systems  Data Leak affecting systems/ servers/ networks/  Compromise of critical systems/information Attacks on Internet of Things (IoT) devices software/ applications related to Big Data,  Unauthorised access of IT systems/data and associated systems, networks Block chain, virtual assets, virtual asset  Defacement or intrusion into the website software, servers exchanges, custodian wallets, Robotics, 3D  Malicious code attacks Attacks or incident affecting Digital and 4D Printing, additive manufacturing,  Attack on servers such as Database, Mail and DNS Payment systems Drones  and network devices such as Routers Attacks through Malicious mobile Apps Attacks or malicious/ suspicious activities  ☑Identity Theft, spoofing and phishing attacks Fake mobile Apps affecting systems/ servers/software/   DoS/DDoS attacks  Unauthorised access to social media applications related to Artificial Intelligence  Attacks on Critical infrastructure, SCADA and accounts and Machine Learning operational technology systems and Wireless Attacks or malicious/ suspicious activities  Other (Please Specify)  networks affecting Cloud computing ----------------------------------------------------------  Attacks on Application such as E-Governance, E- systems/servers/software/applications  Commerce etc. ---------------------------------------------------------- | | | | |
| Is the affected system/network critical to the organization’s mission? (Yes / No). (Brief details.) | | Yes | | |
| Basic Information of Affected System (Provide information that is readily available.) | | Domain/URL: http://loginkucoin-elog.webflow.io IP Address: 172.64.151.8, 104.18.36.248 Operating System:Unknown (Hosting Server Details Not Available) Make/ Model/Cloud details: Hosted by MarkMonitor, Inc. Affected Application details (If any): Potential phishing website at loginkucoin-elog.webflow.io Location of affected system (including City, Region & Country): San Francisco, California, US  Network and name of ISP: MarkMonitor, Inc., IP: 172.64.151.8, 104.18.36.248 | | |
| Brief description of Incident: A potential phishing website was detected at loginkucoin-elog.webflow.io. Risk Score: 43.62/10 (Confidence: Medium). The site was created on 08/05/2013 07:50 UTC.   Risk Analysis: - Brand Impersonation: The domain name 'loginkucoin-elog.webflow.io' is suspicious. The official KuCoin domain should be kucoin.com or a legitimate subdomain. This implies an attempt to impersonate the legitimate KuCoin login page. - Login Form Illegitimacy: There is no actual login form in the provided HTML. This suggests that the page is incomplete or a preliminary setup for a phishing attack. The lack of a form, combined with the domain name, heightens the suspicion. - Social Engineering: The title and description attempt to mimic the official KuCoin login page. Phrases like '(Official Site)®' and 'Sign In to Your Account™' are used to create a sense of legitimacy and urgency, encouraging users to enter their credentials on a potentially fake page. - Domain Hosted on Webflow: While Webflow is a legitimate platform, it's commonly used for quick website creation, making it easier for attackers to set up phishing sites. Hosting a critical service like a login page on a generic Webflow domain is unusual for a large company like KuCoin.  The domain is registered with MarkMonitor, Inc.. VirusTotal scan shows 21 engines flagged this domain as malicious out of 94 total engines. Immediate intervention is recommended to prevent potential data theft and financial fraud. | | Occurrence date & time (dd/mm/yyyy hh:mm): 08/05/2013 07:50 UTC Detection date & time (dd/mm/yyyy hh:mm): 15/03/2025 19:58 UTC | | |
| **Note:** (i) This form provides general guidance in terms of information which could be relevant to the incident.   1. It is not mandatory to fill and/or sign this form. Incidents may also be reported by providing relevant information in the communication itself or in any other readable form. 2. Reporting entity may, if desired, also provide relevant information other than mentioned in this form. | | | | |
| **Mail/Fax incident reports to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at:** [**incide**](mailto:incident@cert-in.org.in)[**nt@cert-in.org.in**](mailto:nt@cert-in.org.in) | | | | |