SOCRadar®
Your Eyes Beyond

CHALLENGE
Impersonated
Landing Page

SOLUTION
Dark Web Monitoring
Takedown

CUSTOMER STORIES

STOLEN DATA via DECEPTIVE LANDING PAGES UNCOVERED on TELEGRAM

REGION
Europe

INDUSTRY
Banking & Finance

CHALLENGE
Phishing and
impersonation

SOLUTION
Detecting stolen assets & take
down, Telegram monitoring

One of SOCRadar's customers, a bank in Europe, faced a sophisticated **phishing campaign** with impersonated **landing pages.** The threat actors aimed to steal **customer credentials** by using various social engineering tactics that directed them to fake landing pages and to sell the credentials in a private Telegram channel.

Thanks to SOCRadar's **monitoring capabilities** that cover **Telegram channels** in addition to underground hacker forums, our analyst team identified a channel where the bank's exposed data was being offered for sale. This discovery served as the catalyst, prompting us to launch a comprehensive **investigation.** Subsequently, the analysts identified **impersonated landing pages** that mimicked the bank's legitimate website. These deceptive sites were designed to lure bank customers into providing their sensitive financial information.

Leveraging its dark web and Telegram monitoring capabilities and the subsequent identification of the impersonated landing pages, SOCRadar swiftly **informed the affected customer** and orchestrated a **takedown** operation to neutralize the threat posed by these **counterfeit sites.**

In light of this intervention, the bank was made acutely aware of the extent and specifics of the compromised data, enabling proactive measures to thwart additional breaches and safeguard their clientele.

Impersonated domains and fake landing pages represent a serious **danger** to the finance industry due to its potential to result in major **financial losses,** compromise sensitive data, and harm financial institutions' reputations.

Why is this important?

Telegram has evolved to a platform that may replace dark web forums where **stolen data** has been **exchanged.** Heightened **privacy** in this app appeals to **cybercriminal** factions. Many groups have turned to private Telegram channels to **broker deals** involving stolen credentials and other illicit data.

Telegram's unique combination of cross-platform accessibility, cloud-based storage, and synchronization capabilities make it a **hotbed for clandestine data trading** and many other activities of cyber threat actors. Given its burgeoning significance in the cybercrime ecosystem, security teams cannot afford to overlook Telegram and must **prioritize its surveillance.**

SOCRadar®
Your Eyes Beyond

CHALLENGE
Impersonated
Landing Page

SOLUTION
Dark Web Monitoring
Takedown

CUSTOMER STORIES

Impersonated domains and deceptive landing pages represent a grave and growing threat to banks and other financial institutions. At the heart of this menace is the art of deception, where cybercriminals design sites to **mirror the authentic web interfaces** of trusted financial bodies. Unsuspecting clients, unable to discern these well-crafted facades from the genuine platforms, may inadvertently divulge sensitive personal and financial data.

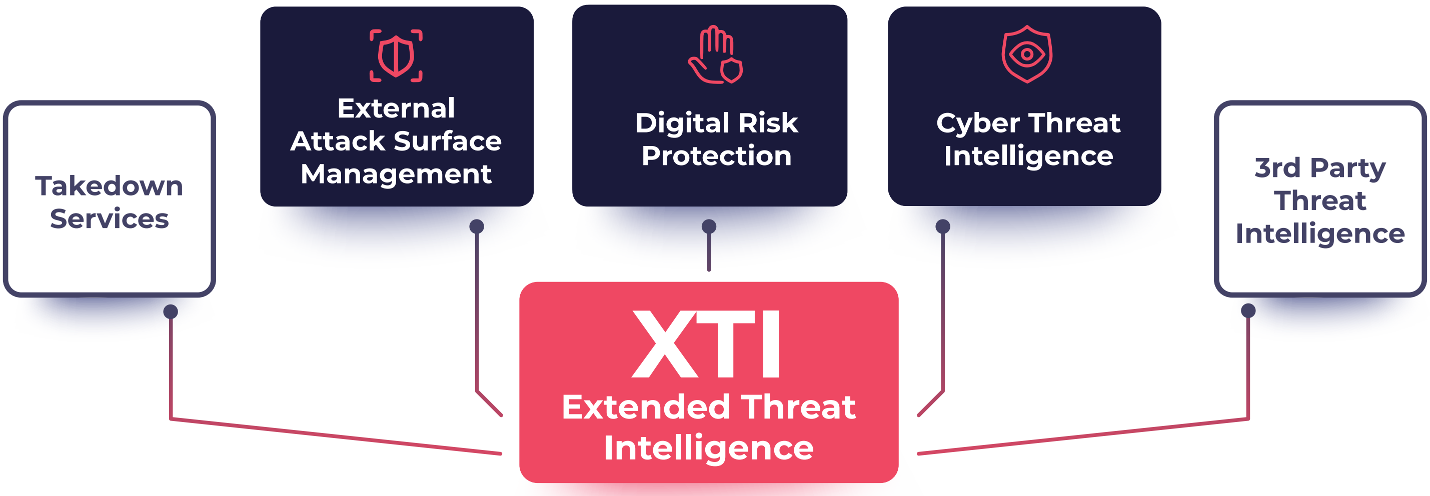
This not only jeopardizes individual accounts, potentially leading to **fraudulent transactions** and **identity theft,** but also undermines the institution's **reputation** for security and reliability. The ramifications of such breaches extend beyond immediate financial losses; they erode customer trust, a cornerstone for any financial institution.

In an era where digital interactions are paramount, ensuring the integrity and authenticity of online platforms is not merely about asset protection, but also about preserving the very credibility and trustworthiness of the institution in question.

1 The credentials of a bank’s customers were stolen by threat actors leveraging an impersonated landing page and listed for sale on a private Telegram channel.

2 Through the 24/7 and automated dark web monitoring capability, SOCRadar detected the sale announcement on Telegram and ran a comprehensive investigation that led to the impersonated landing page.

3 SOCRadar informed the affected customer (The bank) to implement proactive measures and initiated the takedown process against the fake web page.


Takedown Services
External Attack Surface Management
Digital Risk Protection
Cyber Threat Intelligence
3rd Party Threat Intelligence
XTI
Extended Threat Intelligence