ALLURE SECURITY

Trends in Scams Targeting Regional Banks & Their Customers Online

TexasBankersAssociation

Sam Bakken
DIRECTOR OF PRODUCT MARKETING
ALLURE SECURITY

June 20, 2024

AGENDA

1. Trends in Online Scams Targeting Regional Banks
2. Examples of Recent Schemes
3. Brand Protection 101: Online Brand Audit
4. The Problem With Traditional Approaches
5. FI Case Study: A Modern Approach to Brand Protection

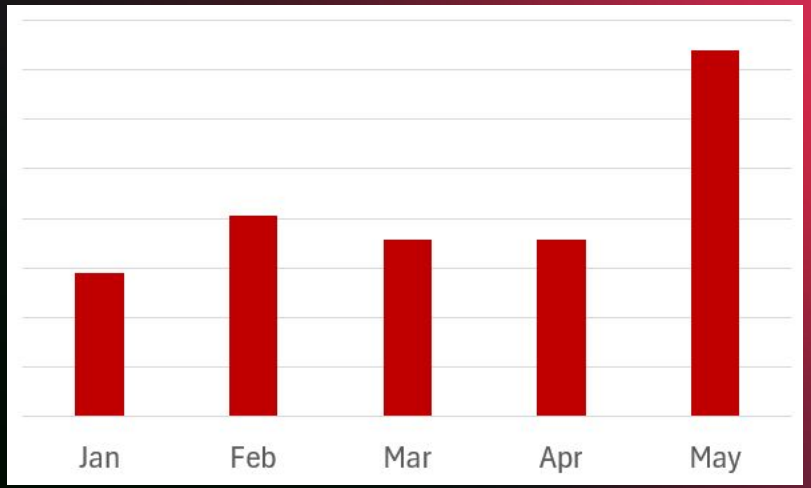
TRENDS IN ONLINE IMPERSONATIONS

Targeting Regional Banks

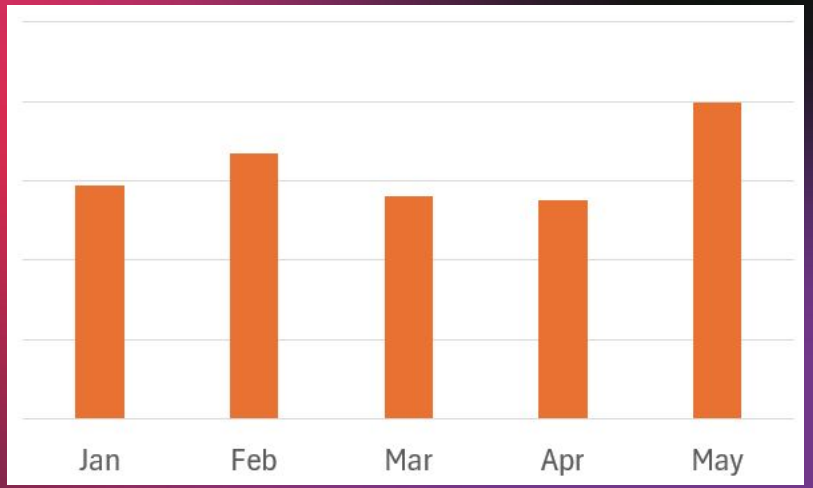
ALLURE SECURITY

Regional Bank Impersonations Detected Jan. - May 2024

Impersonations

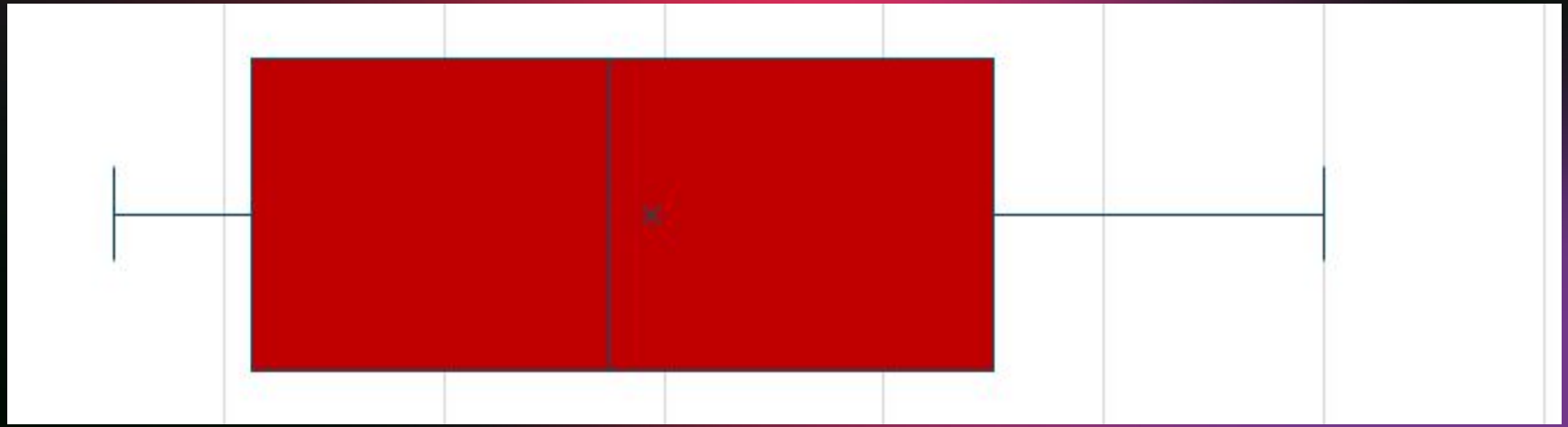


Brands Impersonated



Analysis of Rogue Mobile Apps Detected per Regional Bank

Minimum	Median	Maximum
1	5.5	12



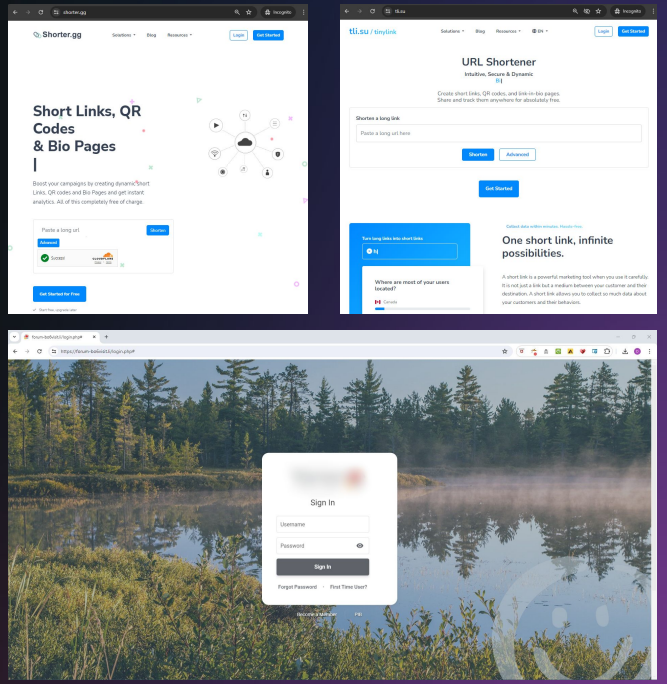
RECENT SCHEMES

Targeting Regional Banks

ALLURE SECURITY

FRAUDSTERS USING THEIR OWN URL SHORTENERS TO EVADE DETECTION

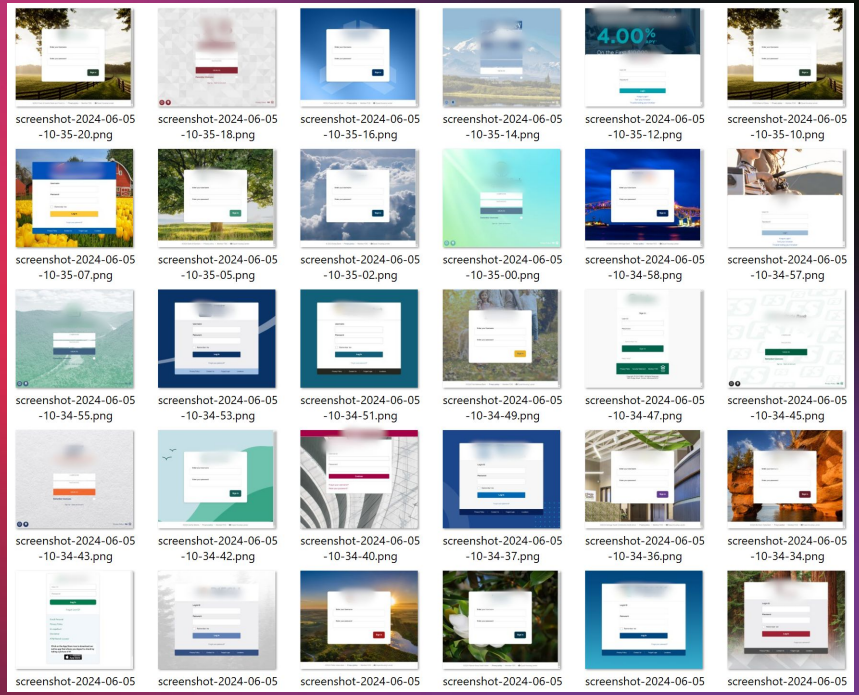
- **SMS phishing messages sent to credit union members in late May**
- **Used shortened URLs with domains including kn8[.]site, kv6[.]site, dx2[.]site, and dx5[.]site**
- **More mature link shorteners use vetting to prevent phishing**
- **Threat actors create their own link shorteners to evade vetting while still disguising links**



Screenshots of Suspicious URL Shortener Web Pages and Credit Union Impersonation

SCOURGE OF PHISHING KIT NESTS

- **Scourge of phishing kit nests targeting multiple FIs started in May**
- **Ready-made phishing page templates**
- **212 FIs targeted: regional banks & CUs**
- **10+ phishing nests detected a day**
- **Up to 40 phishing pages in any nest**
- **Impervious to typo-based detection**
- **Typical automated scanners can't find them**



Screenshots of 30 different credit unions and regional banks impersonated within one single phishing kit nest found June 5, 2024

FRAUD VIA ROGUE MOBILE APPS

Growing portion of fraud:
5 percent of fraud attacks traced to rogue mobile apps

Adversaries inject malicious code into cloned apps

Older app versions lack latest security features

Mostly Android apps, rogue iOS apps will grow w/ new March 2024 EU rules

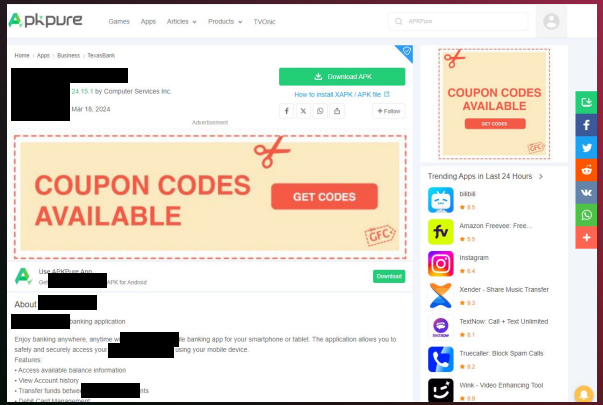
> ***Threat actors will weaponize our mobile banking app, put it on some third-party site and then send an email with a link to it.***
>
> ***It's something I hadn't heard of before.***

VP Cybersecurity
Medium-Sized Financial Institution

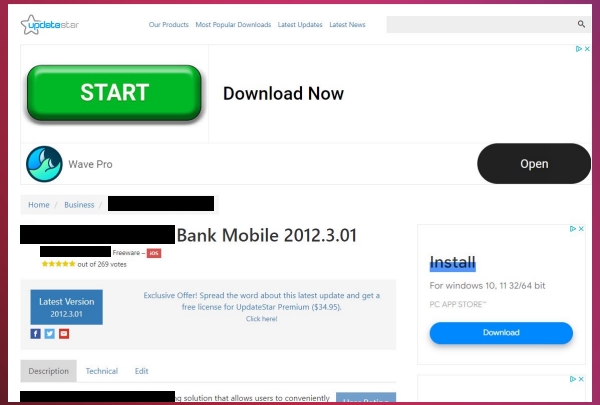
"Ramp Up Protections as Mobile Fraud Grows" The Financial Brand
https://thefinancialbrand.com/news/digital-banking/mobile-banking-trends/banks-must-ramp-up-against-multiplying-fraud-actors-173185/

ALLURE SECURITY

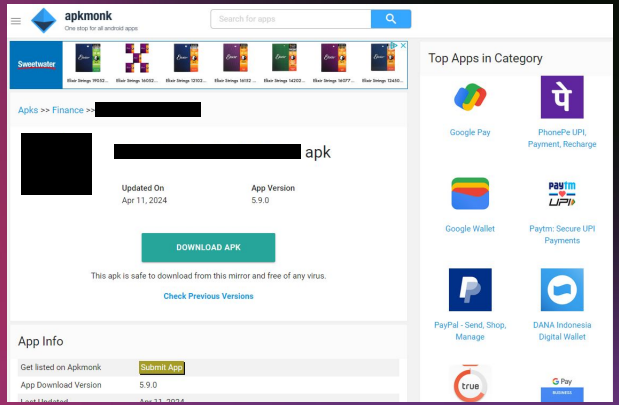
ROGUE MOBILE REGIONAL BANK APPS



apkpure.com
3 mos. out of date
17 versions back to Oct 2016

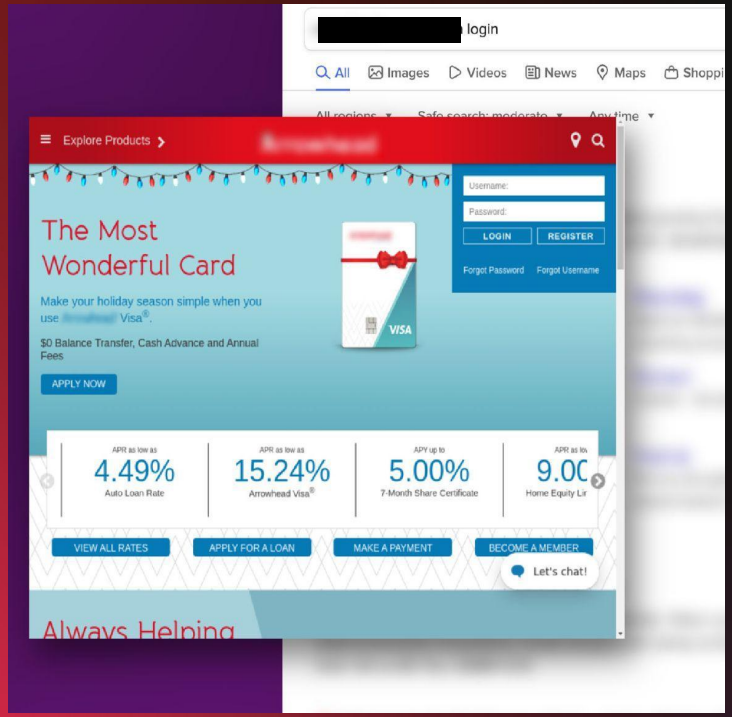


updatestar.com
12 yrs, 23 mos. out of date
For iOS



apkmonk.com
Current version
7 versions back to Dec 2021

SEARCH ENGINE POISONING: ORGANIC



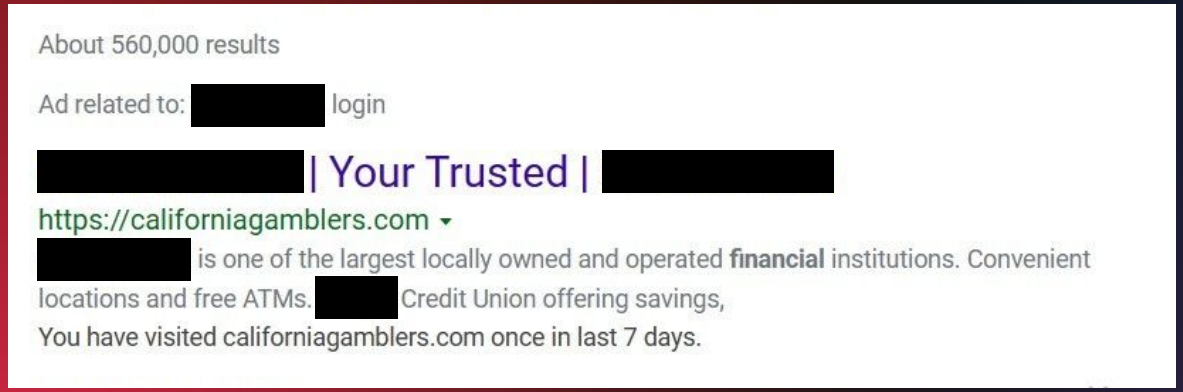
Search for "[financial institution] login"

Result directs to malicious URL

Results differ by search engine, location, etc,

ALLURE SECURITY

SEARCH ENGINE POISONING: PAID



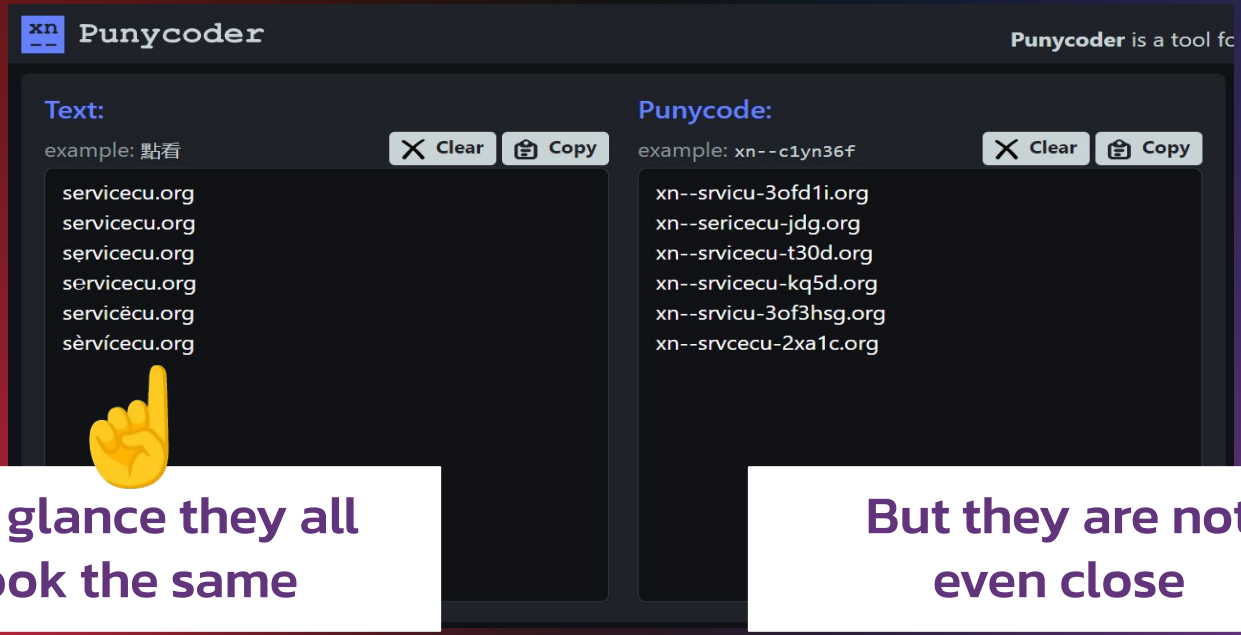
Ad displays upon search for "[financial institution] login" (note irrelevant URL)

Clicking the ad directs the visitor to the malicious site

ALLURE SECURITY

ADVERSARIES RELY LESS ON TYPOS

TYPOSQUAT-BASED DETECTION MISSES UP TO 94%



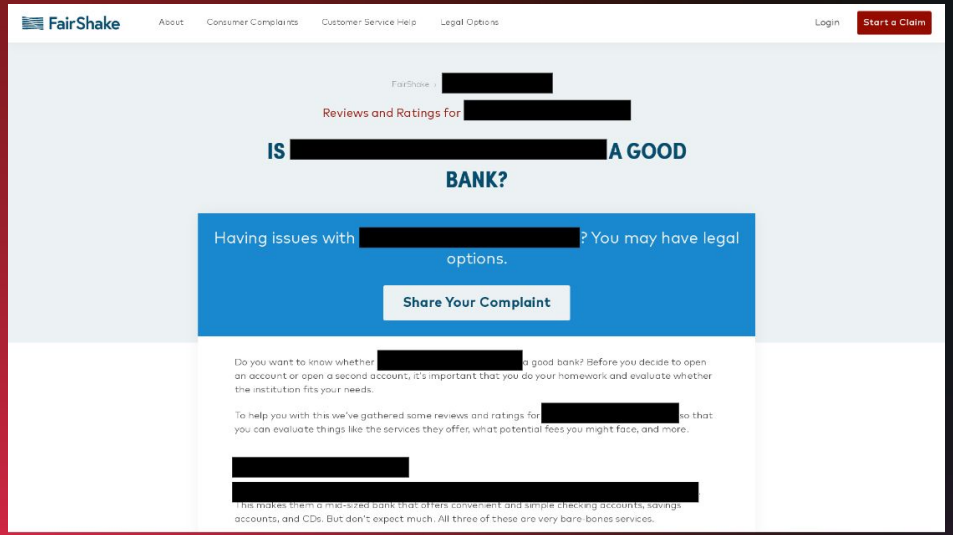
At a glance they all look the same

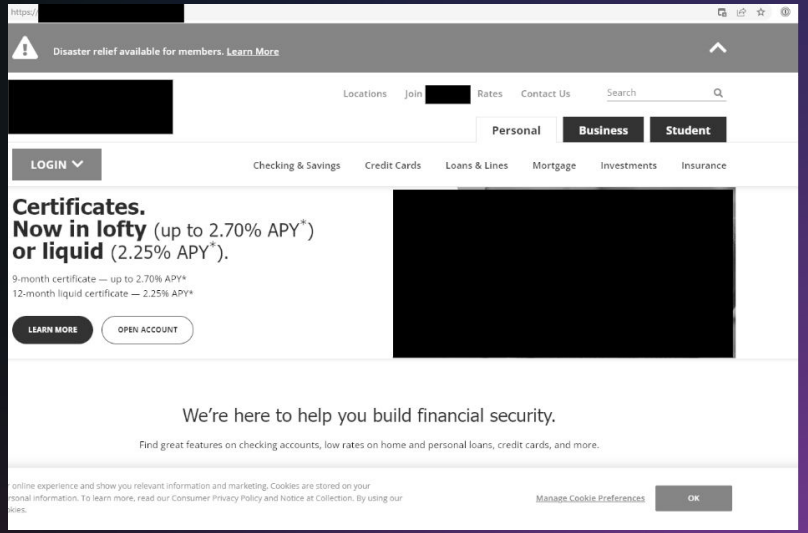
But they are not even close

ALLURE SECURITY

LAYERS OF IMPERSONATION

MEASURES TO EVADE DETECTION





ALLURE SECURITY

BRAND PROTECTION 101:
BRAND AUDIT

For Regional Banks

ALLURE SECURITY

BRAND AUDIT PLAN

TRADEMARKS / COPYRIGHT

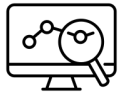
Check your registrations

MOBILE APP DISTRIBUTION

Clarify approved app stores

WEB SITE INVENTORY

Build inventory of owned sites



ONLINE BRAND MONITORING

How will you spot fakes?

3RD PARTY PROPERTIES

Identify 3rd-parties' use of your brand

COLLECTING REPORTED FAKES

Who will collect reports?

SOCIAL MEDIA ACCOUNTS

Claim your brand accounts

INCIDENT RESPONSE PLAN

Who responds and how?

ALLURE SECURITY

THE PROBLEM WITH TRADITIONAL APPROACHES

ALLURE SECURITY

THE PROBLEM WITH OLD FASHIONED APPROACHES

69% of attacks can't be detected by domain monitoring
The old way misses most scams

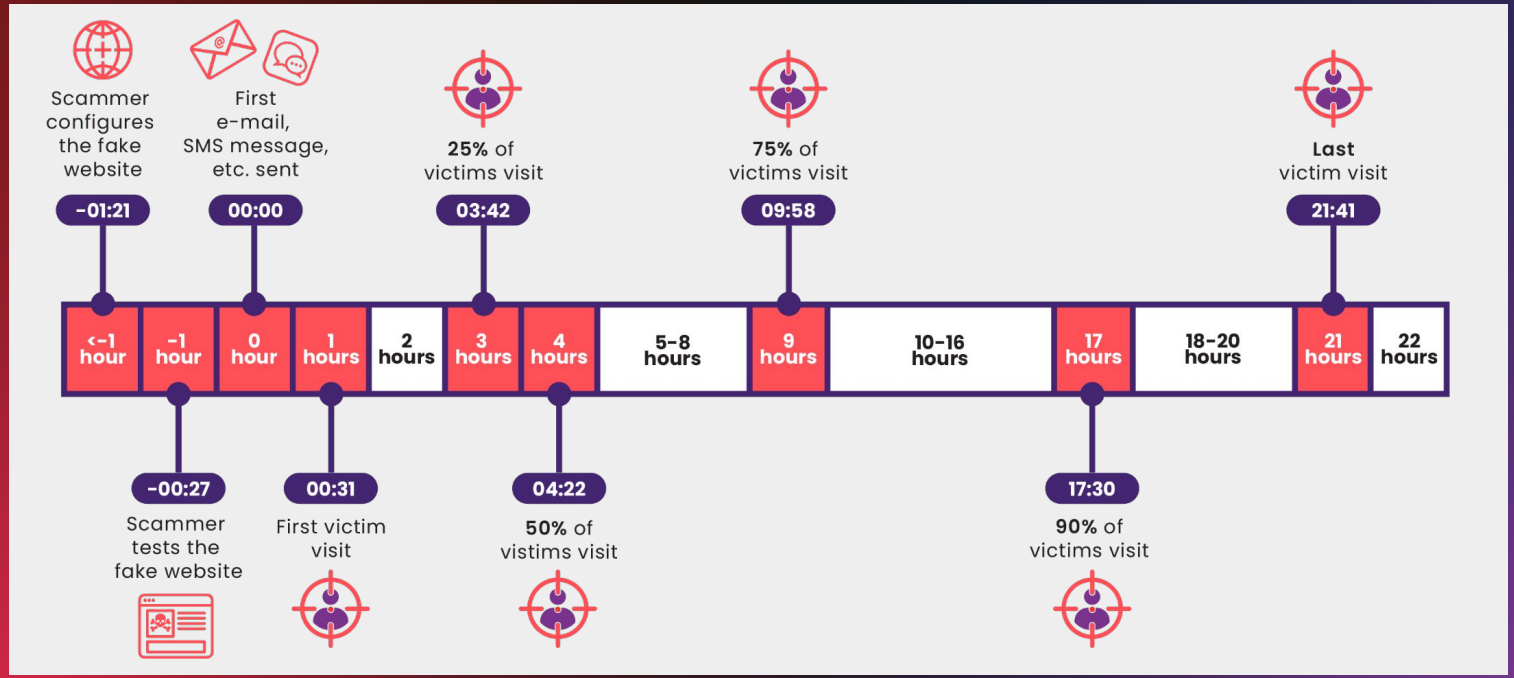
75% of victims visit a scam site during the first 10 hours
The old way is too slow to help

Up to $14,700 cost of mitigating an impersonation *(est.)*
That's too much

$150,000+ cost of time (1.5 FTEs) hunting impersonations *(est.)*
Huge waste of time

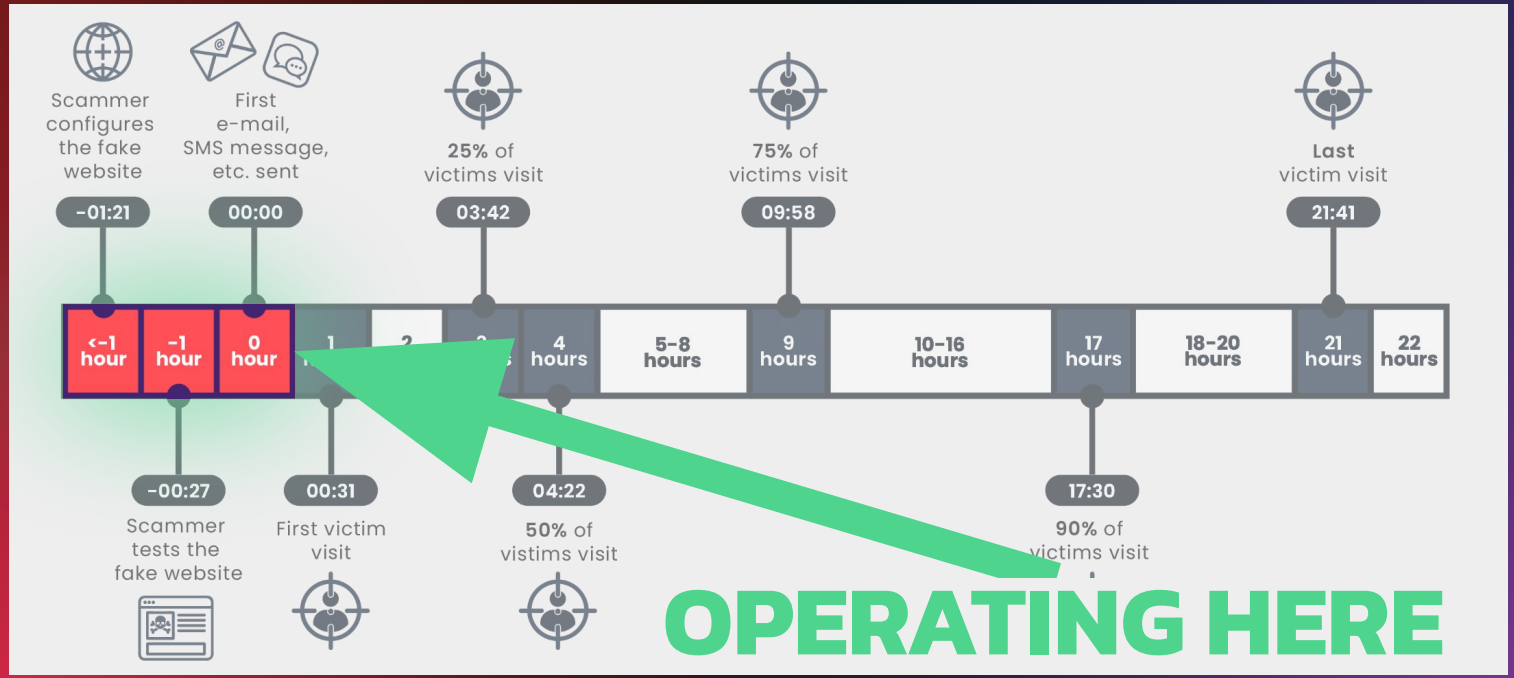
ALLURE SECURITY

BRAND IMPERSONATION TIMELINE



ALLURE SECURITY

WHAT DOES IT MEAN TO STOP SCAMS BEFORE THEY STRIKE?



ALLURE SECURITY

HOW A NORTHEAST REGIONAL STOPS PHISHING SCAMS BEFORE THEY STRIKE

ALLURE SECURITY

FI CASE STUDY: HUNTING FOR BRAND IMPERSONATIONS

BEFORE

- Customers detected fraud first
- Takedowns were slow & expensive
- Blocking & takedowns took days, increasing the number of victims
- Internal IT security, fraud & customer support staff burdened with response in addition to other priorities

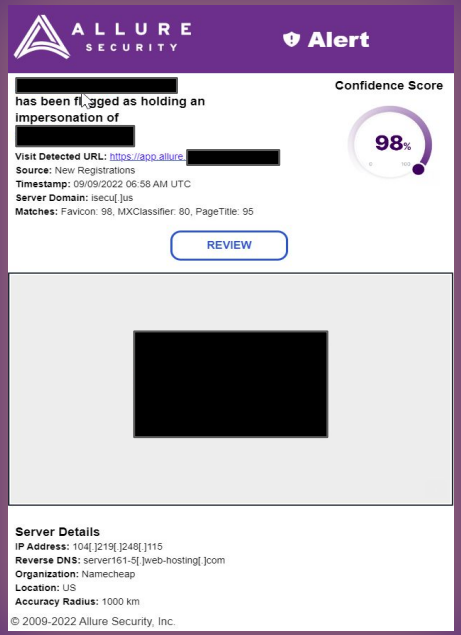
FI CASE STUDY: PROACTIVE HUNTING FOR BRAND IMPERSONATIONS

AFTER

- Scams detected within minutes of being published, pre-empting fraud & complaints
- Visibility into 10+million new & updated websites each day
- Scams blocked & taken down in minutes, before customers visit the site
- IT security, fraud & customer support staff burden eliminated, but more importantly prevented customers' credential harvesting

PROACTIVE IMPERSONATION DETECTION & RESPONSE

Actual Results



SEPT 9 06:42

Domain first observed on the Internet (DomainTools/Farsight)

SEPT 9 06:58

Alert on active impersonation attack by Allure Security

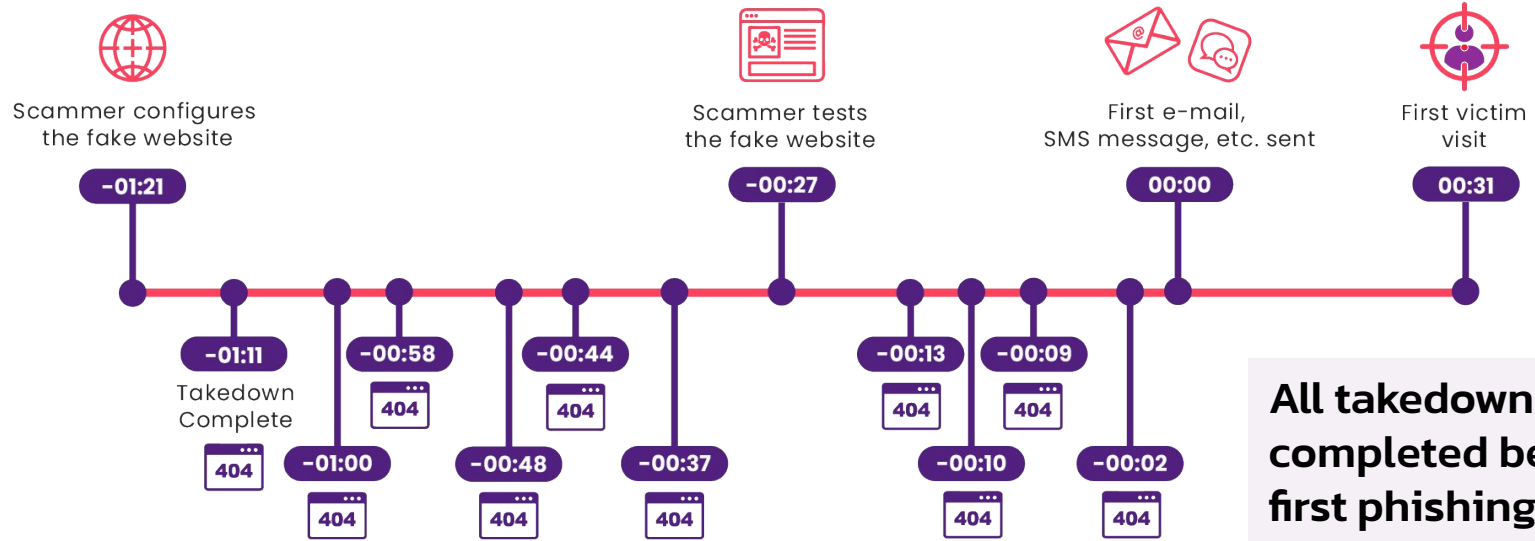
SEPT 9 07:03

Allure Security team completes site takedown

TOTAL ELAPSED TIME: 21 MINUTES

PROACTIVE DETECTION PROTECTS CUSTOMERS

Actual Performance (Sept. 1-9)



All takedowns completed before first phishing message sent

AVERAGE TIME: 40 MINUTES 54 SECONDS

ALLURE SECURITY

THANK YOU!

CONTACT

VISIT
alluresecurity.com

EMAIL
info@alluresecurity.com

CALL
877.699.8883