THREATWATCH360

See Risk, Secure Instantly

THREATWATCH360
See Risk, Secure Instantly

Your brand is under attack and no one tells you until it's too late.

Your brand is being impersonated — through fake websites, social profiles, emails, and apps — targeting your customers without your knowledge. These attacks erode trust, steal data, and cost you money. Most companies realize it only after the damage is done. Brand impersonation isn't a rare event — it's a daily threat.

Fake websites, Fake apps, Fake mail domains

They've copied your logo, cloned your website, and are sending emails to your customers — and they have no idea it's a scam.

Customers are being scammed in your name.

They trust the attacker, thinking it's you. When the fraud is exposed, your brand takes the hit — not the scammer.

Employee credentials are leaking.

From dark web dumps to open databases, attackers get inside access — and use it to go deeper into your organization.

Most companies find out too late.

By the time you detect it, the damage is done. Rebuilding trust, reputation, and security costs far more than prevention.

THREATWATCH360
See Risk, Secure Instantly

The ThreatWatch360 dashboard puts real-time threats and instant action at your fingertips all in one place.

The ThreatWatch360 dashboard gives you full visibility into phishing attacks, leaked credentials, rogue apps, and impersonation threats all in one place. Monitor, prioritize, and act faster with real-time insights and instant takedown control, designed for speed, clarity, and security.

THREATWATCH360
See Risk, Secure Instantly

Solutions

See threats as they happen, stop them instantly, and stay in control all from one unified platform.

Anti-Phishing

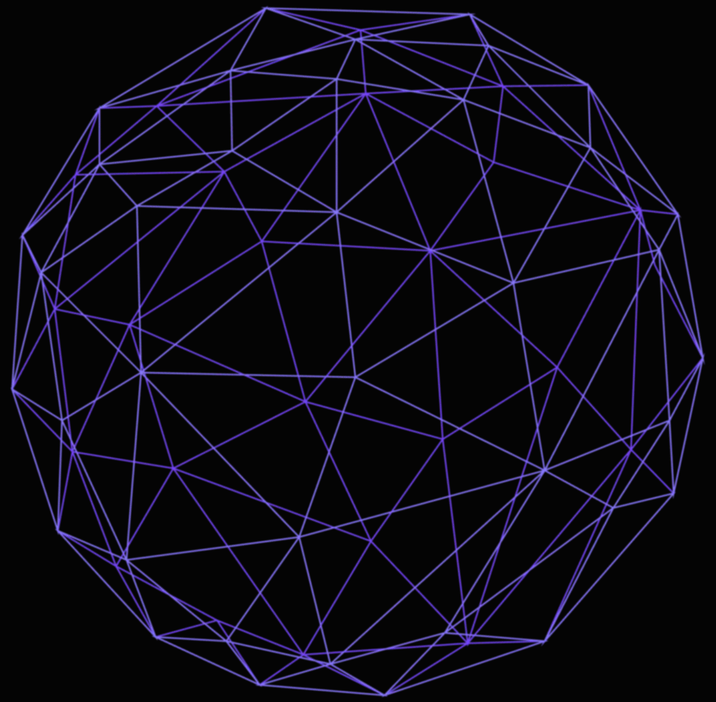
Phishing attacks cause over 60% of breaches, using fake logins, emails, and spoofed domains to steal credentials or money.

Anti-Rogue

Rogue apps and browser extensions mimic your brand, harvest user data, and often bypass app store checks.

BreachEye

Credential stuffing and dark web leaks are rising fast, leading to identity theft and unauthorized access.



Takedown-as-a-Service

Most brands don't have a takedown system, allowing fake domains and impersonators to stay active longer.

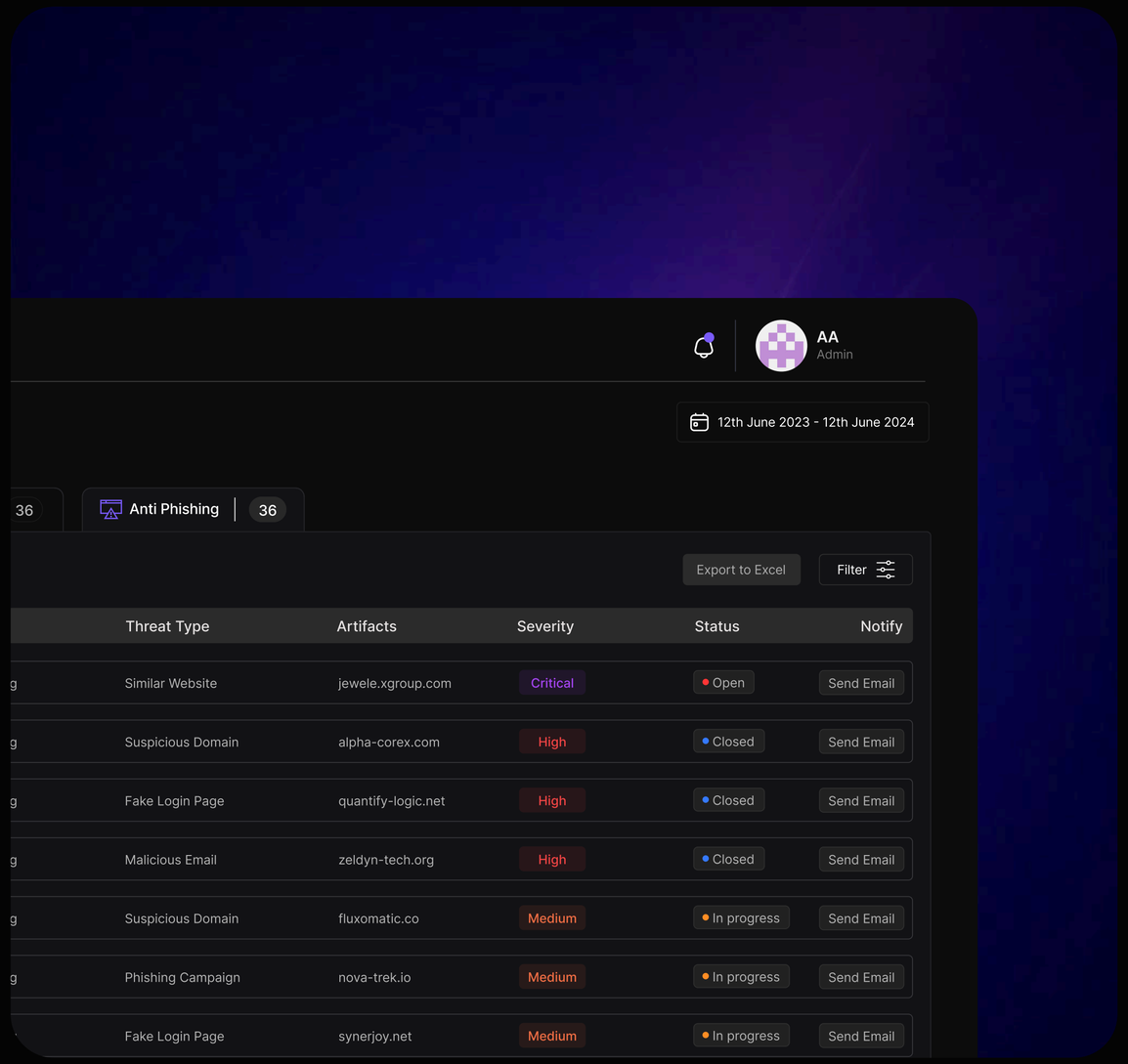
Early-Warning

Early Warning detects suspicious domain registrations and impersonation infrastructure flagging threats before phishing pages are created or fraud attacks are launched.

Social Media

Fake social profiles and cloned brand pages run scams, phishing campaigns, and damage your reputation.

THREATWATCH360
See Risk, Secure Instantly



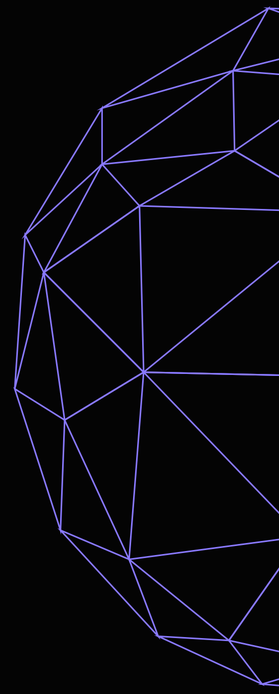
Anti-Phishing

Protect Your Brand from Phishing Attacks
Instantly Detect and Neutralize Threats

01 Instantly detect phishing attacks.

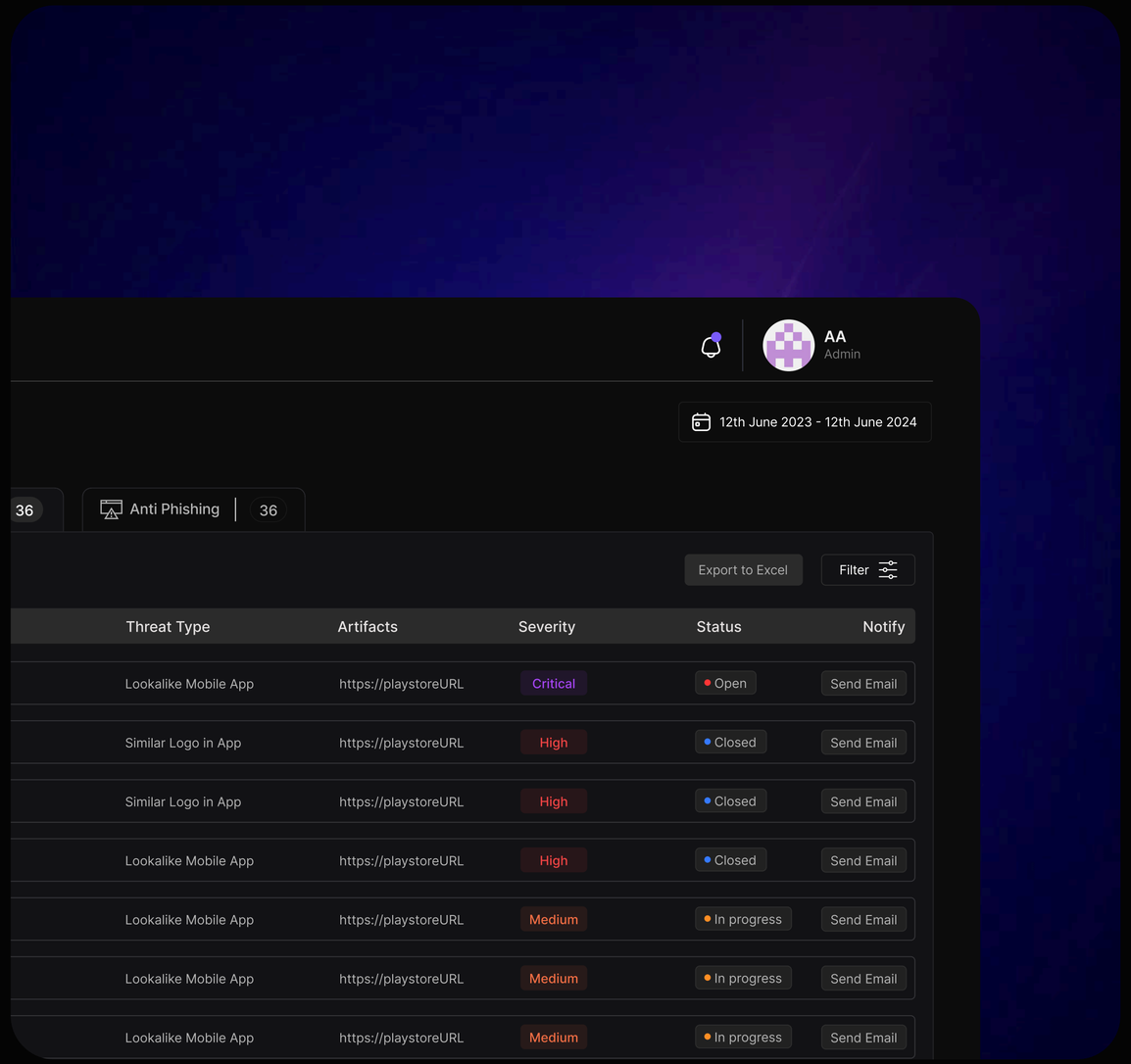
02 Receive actionable alerts with detailed threat insights.

03 Launch rapid takedown actions directly from the dashboard.



With ThreatWatch360's Anti-Phishing dashboard, you get real-time visibility into phishing sites, lookalike domains, and fake online stores targeting your brand.

THREATWATCH360
See Risk, Secure Instantly



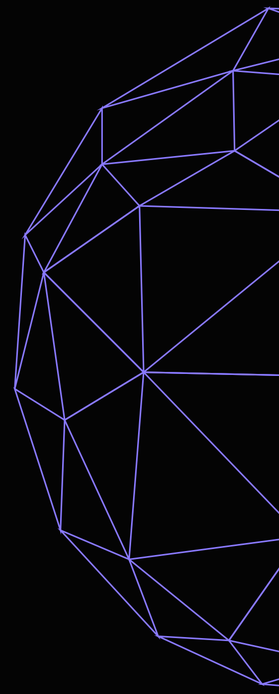
Anti-Rogue

Eliminate Rogue Apps and Secure Your Digital Presence

01 Instantly spot fake or copycat apps.

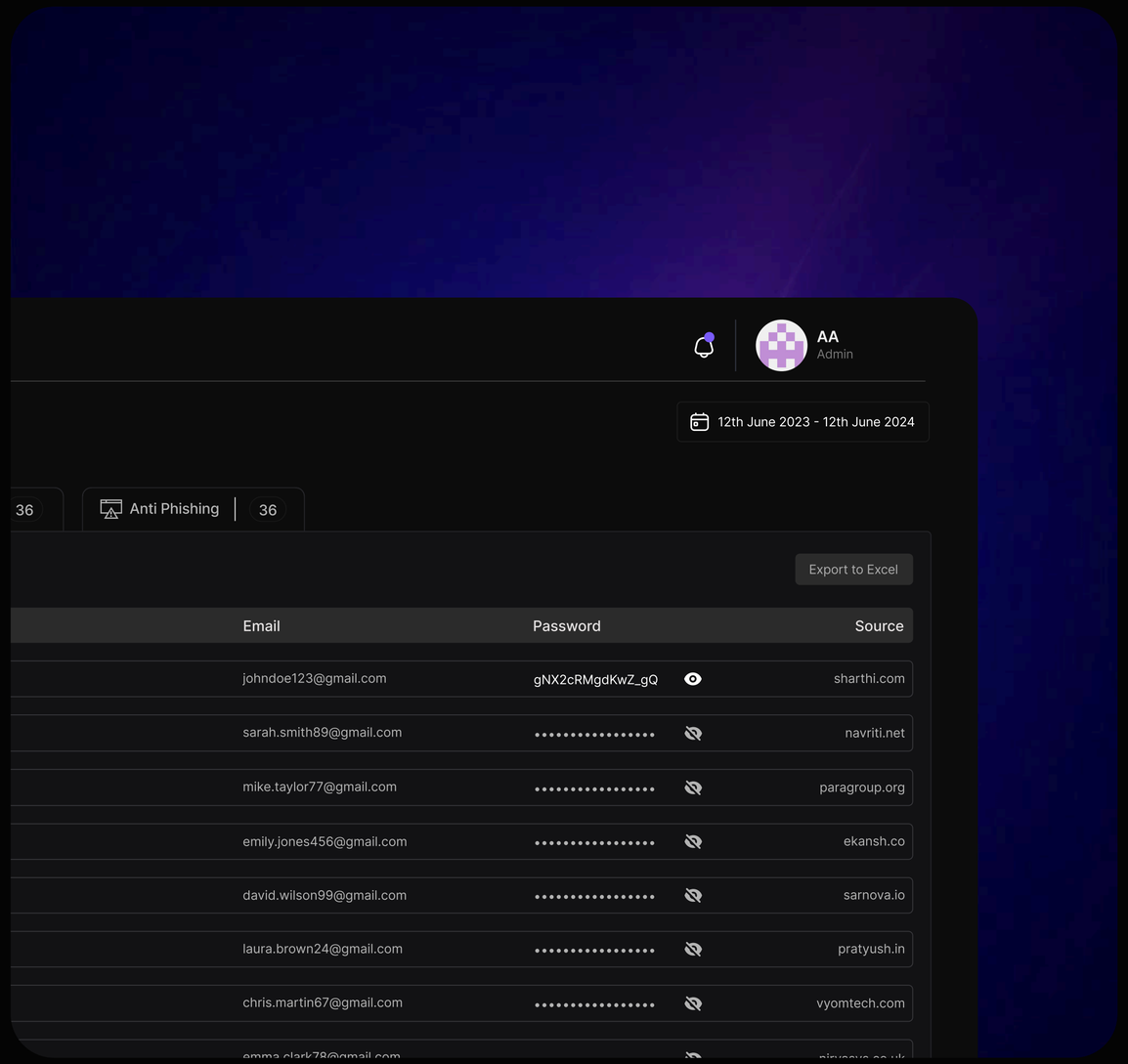
02 Initiate takedowns directly through the platform.

03 Get alerts for app icon, name, and keyword hijacking attempts.



ThreatWatch360's Anti-Rogue dashboard continuously monitors global app stores and third-party platforms for unauthorized apps imitating your brand.

THREATWATCH360
See Risk, Secure Instantly



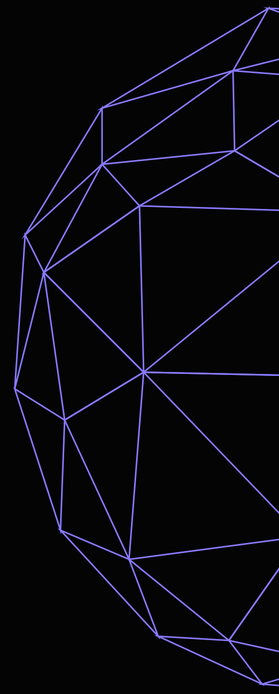
BreachEye

Proactive Credential Monitoring — Stop Breaches Before They Start

01 Get instant alerts for compromised employee credentials.

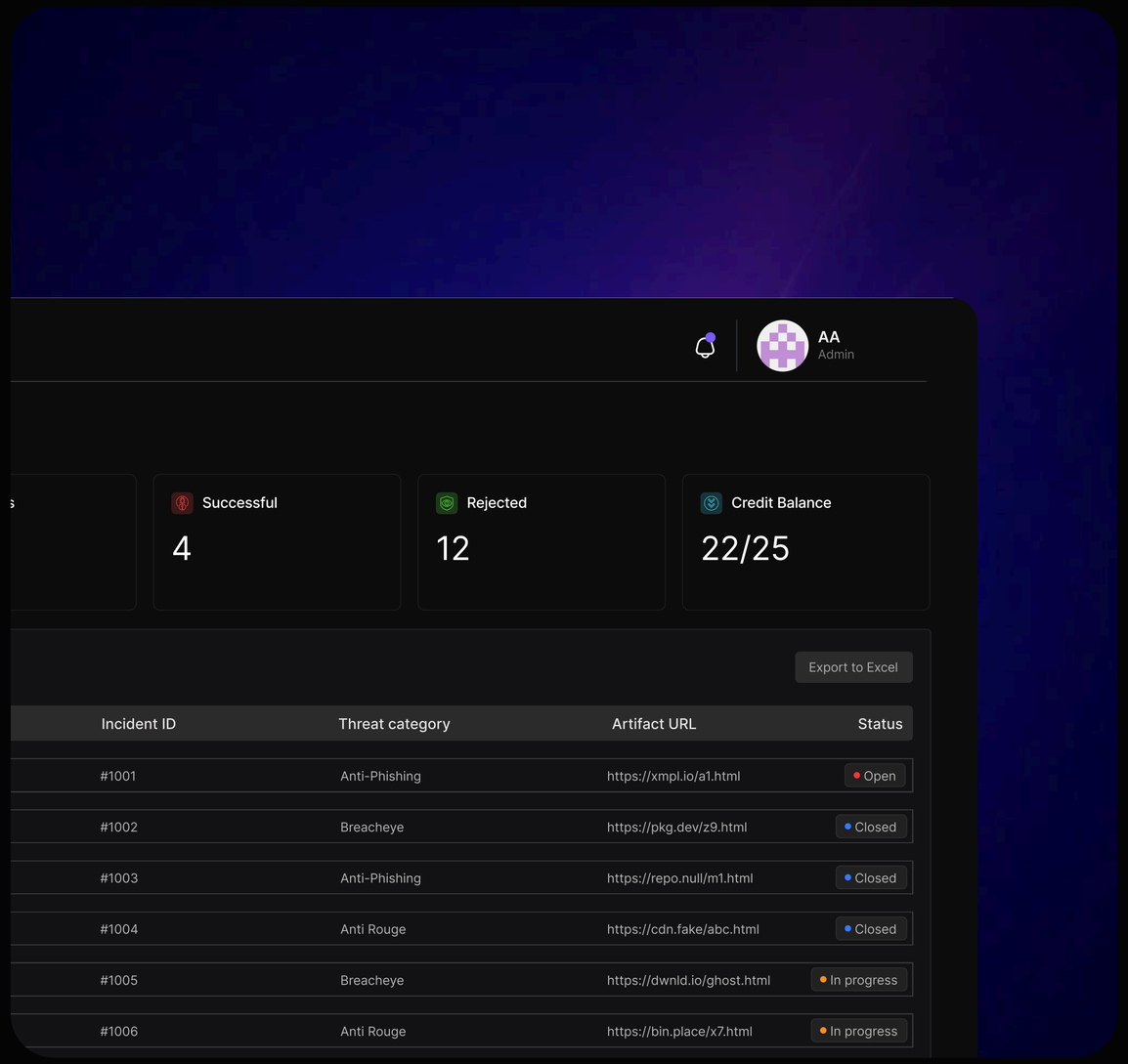
02 Monitor data leaks, illegal listings, and unauthorized repository exposures.

03 Assess breach impact and prioritize high-risk accounts.



Through the BreachEye dashboard, ThreatWatch360 monitors the deep web, dark web, and public repositories to detect exposed credentials linked to your domains.

THREATWATCH360
See Risk, Secure Instantly



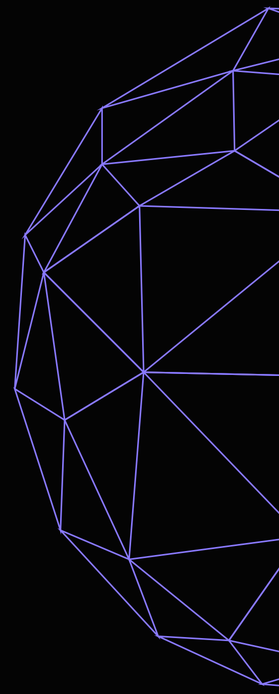
Takedown As A Service

Swift Threat Removal to Protect Your Digital Assets

01 Submit and track takedown requests instantly.

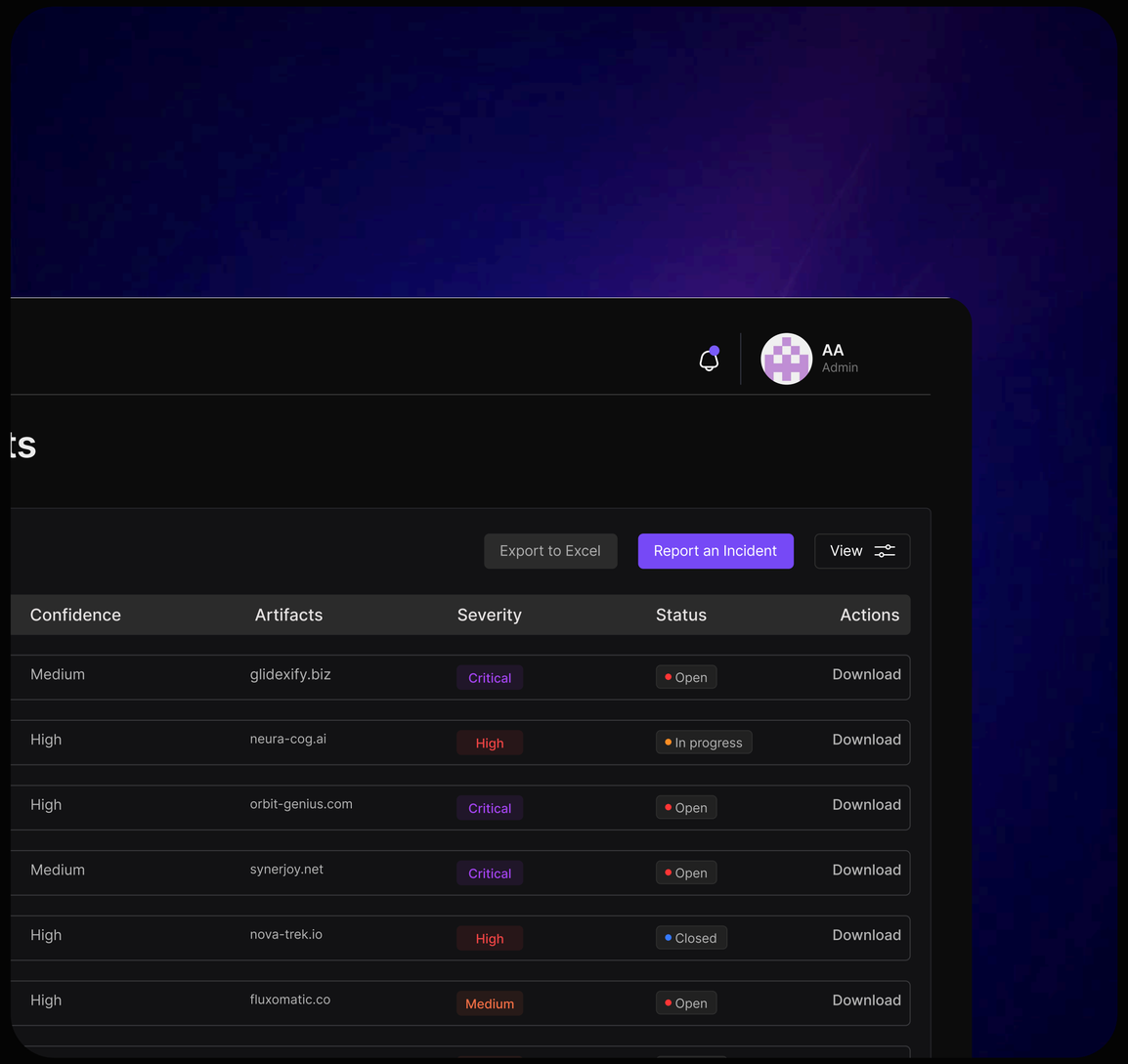
02 Disrupt attacker infrastructure at scale.

03 Get full visibility through status updates, resolution tracking, and detailed reports.



ThreatWatch360's Takedown dashboard automates the removal of malicious domains, fake apps, and harmful content across the internet.

THREATWATCH360
See Risk, Secure Instantly



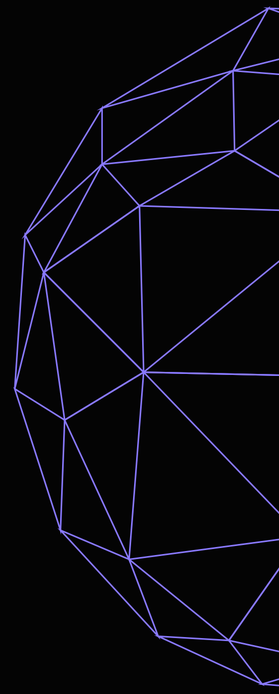
Early Warning

Detect Threats Before They Become Attacks

01 Identify potential phishing and impersonation threats early.

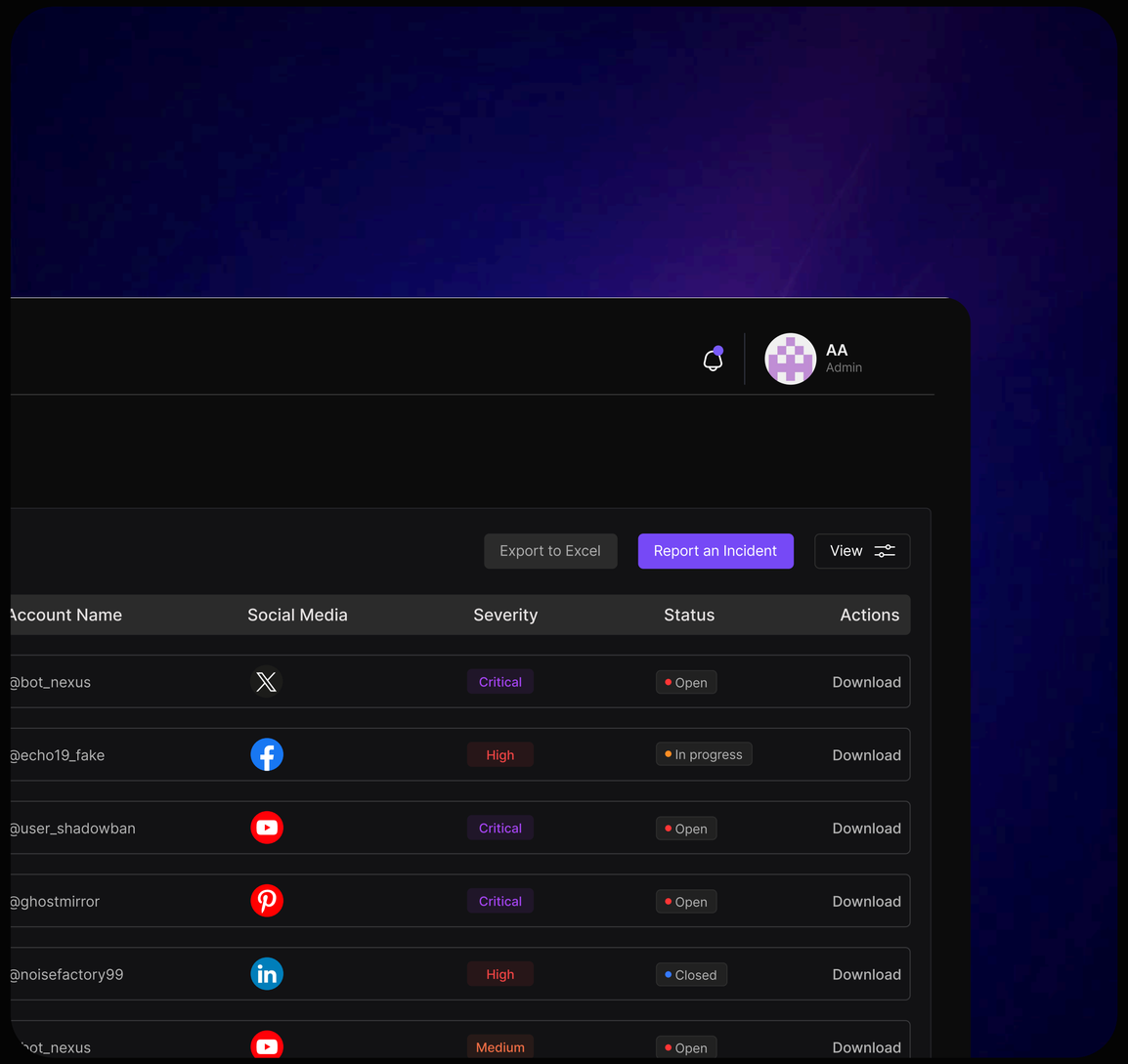
02 Monitor newly registered domains linked to your brand.

03 Take preemptive action with predictive threat insights.



ThreatWatch360's Early Warning dashboard provides proactive intelligence on suspicious domain registrations, typo domains, and phishing infrastructure setups.

THREATWATCH360
See Risk, Secure Instantly



Social Media Intel

Monitor, Detect, and Act on Social Media Threats

01 Detect unauthorized use of your brand on social media.

02 Get alerts for fake profiles, phishing posts, and scam ads.

03 Initiate takedown requests to remove harmful content fast.

ThreatWatch360's Social Media Intel dashboard offers real-time monitoring of fake accounts, scam campaigns, and reputational risks across major platforms.

THREATWATCH360
See Risk, Secure Instantly

Here’s how we go from detection to takedown without delay.

Most cybersecurity tools end with detection, pushing the problem back to your team. ThreatWatch360 changes the game by detecting threats early and actively taking them down so you don’t just know about the problem, you see it solved.

01. Onboarding (Digital Asset Mapping)

We begin by collecting all digital assets linked to your brand. Official websites, app links, email domains, brand-specific keywords (e.g., product or brand names), logos, product visuals, social media profiles, and public executive accounts, to enable effective monitoring for misuse or impersonation.

02. Data Collection & Threat Hunting

We continuously scan the internet using intelligence gathering techniques to detect threats like fake websites, rogue apps, impersonation profiles, and phishing content targeting your digital presence.

03. Threat Categorization

Each detected incident is categorized. Such as similar website, fake job postings, lookalike mail domains, or unauthorized social media profiles, email credential breach, to ensure structured response and effective threat management.

THREATWATCH360
See Risk, Secure Instantly

06. Takedown Assistance

When a validated threat is found, clients can initiate a takedown via the dashboard. Our team then works with domain registrars, hosting providers, platforms, and legal bodies to remove or block the malicious content.

05. Intelligence Alerting & Reporting

Confirmed incidents are filtered to remove false positives and displayed on your dashboard with full context and confidence ratings.

04. Threat Analysis & Prioritization

Our system automatically detects threats, which are then reviewed by expert analysts to assess the impact, ensuring each incident is accurately prioritized for response.

THREATWATCH360
See Risk, Secure Instantly

Other tools just detect ThreatWatch360 actually solves the problem.

Most cybersecurity tools end with detection, pushing the problem back to your team. ThreatWatch360 changes the game by detecting threats early and actively taking them down so you don't just know about the problem, you see it solved.

Feature	Others	ThreatWatch360
Threat Alerts Only	✓	✓
Unified Threat Dashboard	✗	✓
Dedicated Analyst Escalation	✗	✓
Flexible, Affordable Pricing	✗	✓

THREATWATCH360
See Risk, Secure Instantly

Pick A Plan That Fits Your Business We've Made It Simple.

From startups to enterprises, our plans are designed to match your security needs—simple, scalable, and built to keep you protected at every stage.

Plan Name	Essential Monitor	Enterprise Shield
Best For	Best For Small Teams Or Growing Businesses	Best For Large Organizations With Complex Needs
Takedown As A Service	✓ Unlimited	✓ Unlimited
User Dashboard	✓	✓
Export Reports	✓	✓
Monthly Reports	✗	✓
Executive Reporting	✗	✓
Alert Notifications	✓	✓
Dedicated Analysts	✗	✓
Business Reviews	✗	✓
VIP Support	✗	✓

THREATWATCH360
See Risk, Secure Instantly

Need Quick Action? We Give Unlimited Takedowns

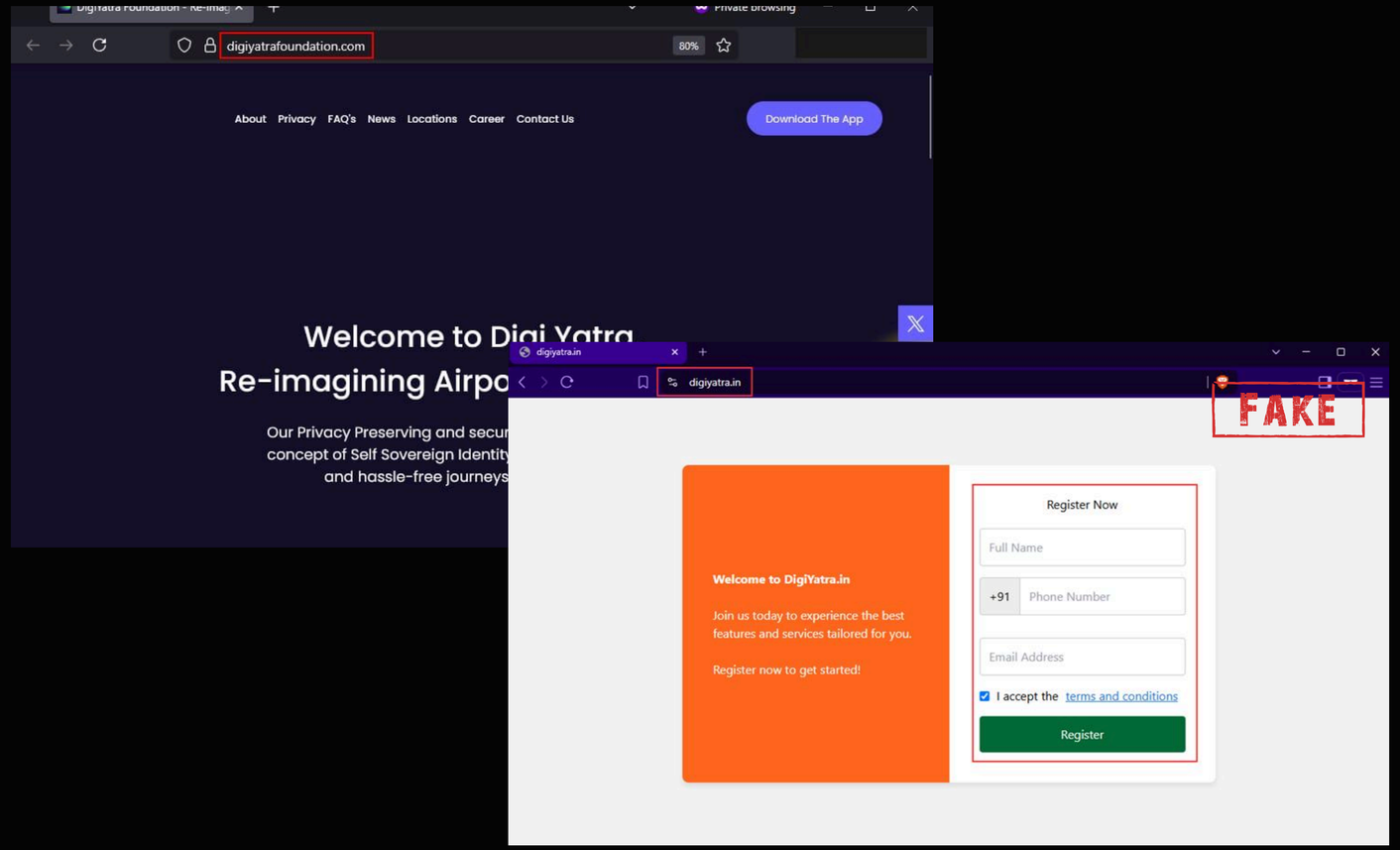
At TW360, we believe brand protection should be fast, flexible, and always within reach. That's why we offer unlimited takedown support without any mandatory subscription. Whether it's one threat or a hundred, you get the same powerful takedown action without limits and without the pressure of recurring commitments. We're built for businesses that want results, not red tape.

From impersonation sites and fake social accounts to counterfeit products and domain abuse, digital threats are constant and unpredictable. Our model gives you freedom: tackle every incident with full force, whenever it appears. Pay only for what you need, when you need it while still enjoying enterprise-grade response, 24/7 monitoring, and real-time resolution. No subscription. Just protection on your terms.

THREATWATCH360
See Risk, Secure Instantly

Our takedown solutions have delivered consistent, measurable results.

Case Study 1: Government and Ministry of Civil Aviation Initiative (Digiyatra Foundation)



Fake DigiYatra Website Targeting Indian Flyers

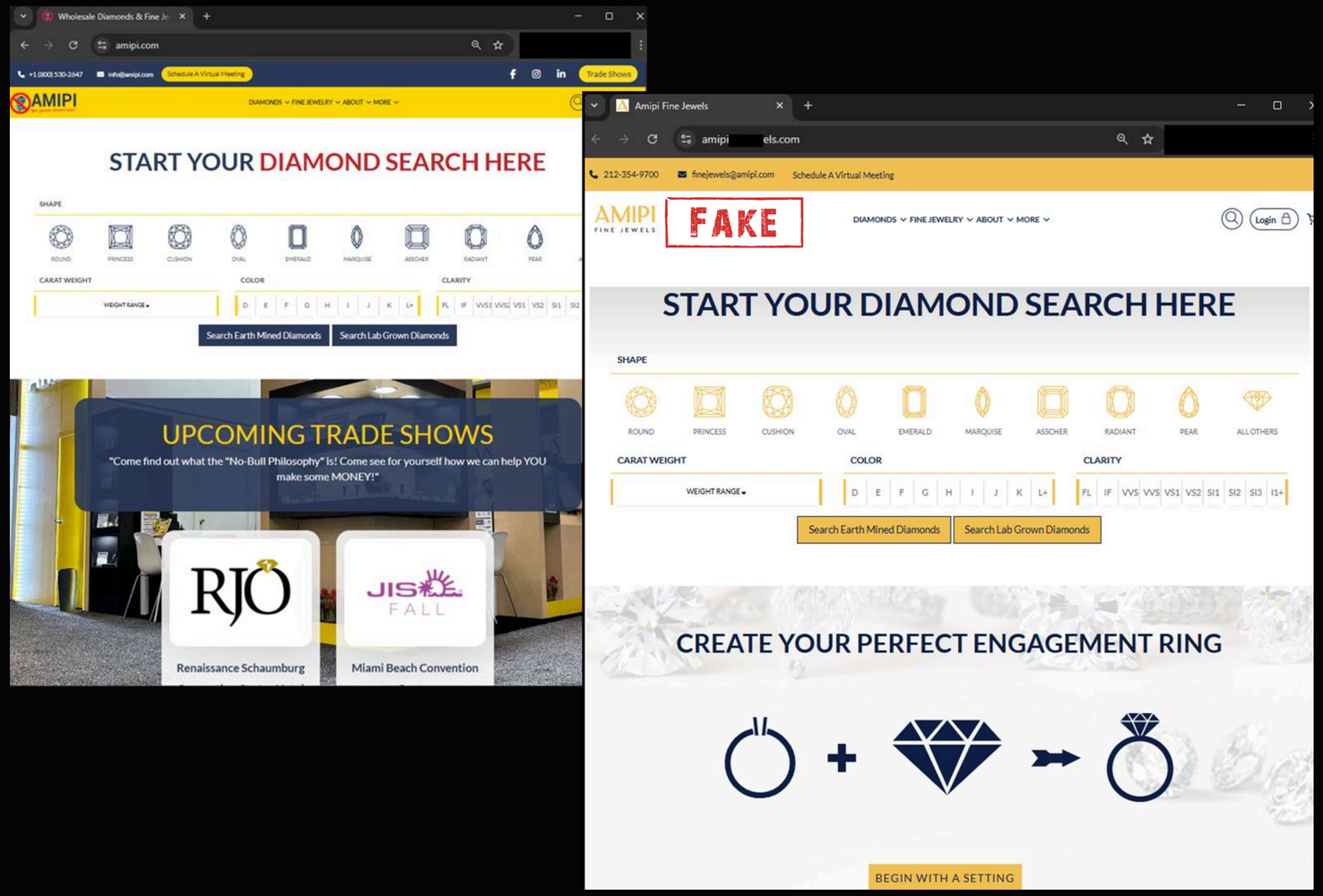
ThreatWatch360 detected a phishing website impersonating the official DigiYatra platform, aimed at stealing Aadhaar, OTP, and travel details. The fake domain had a valid SSL certificate and was indexed on Google, making it appear to be legitimate.

Using our Early Warning and Anti-Phishing modules, the domain was flagged, analyzed, and escalated to authorities. A takedown was initiated, and public awareness was raised.

Impact: Early detection prevented data theft and brand damage, showcasing ThreatWatch360's effectiveness in protecting public-sector digital assets.

THREATWATCH360
See Risk, Secure Instantly

Case study 2: Diamond jewelry brands (Amipi Diamonds)



Fake Websites Targeting Diamond Brands at JCK Las Vegas

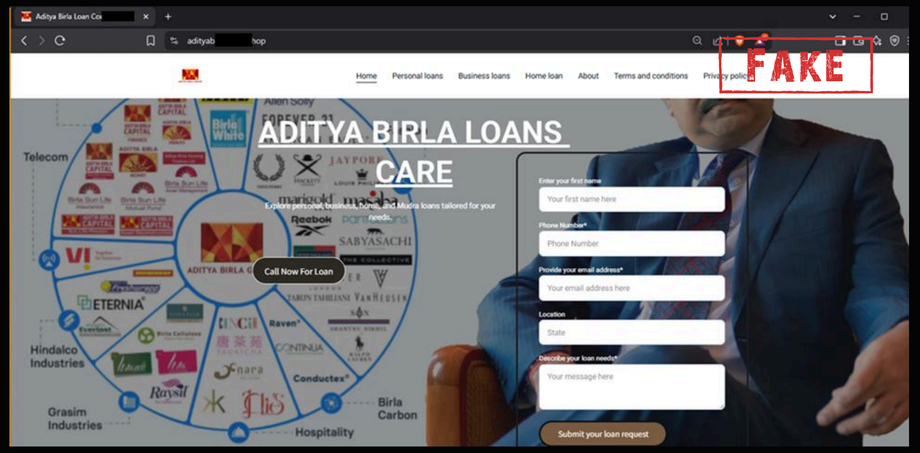
ThreatWatch360 uncovered a targeted phishing campaign during the JCK Las Vegas Jewelry Show. Threat actors created fake websites mimicking top diamond brands to steal customer leads and commit credit card frauds.

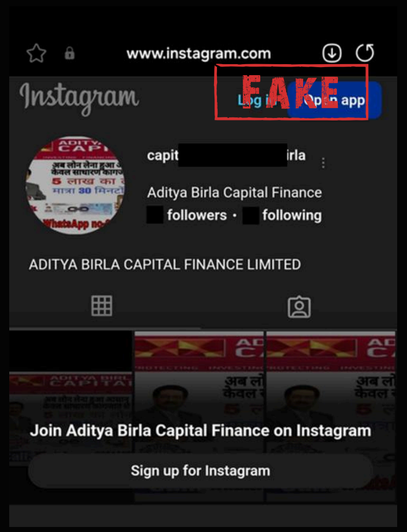
Using our Anti-Phishing and Early-Warning modules, we identified multiple lookalike domains, including one impersonating Amipi Inc, replicating branding and embedding fake purchase/contact forms.

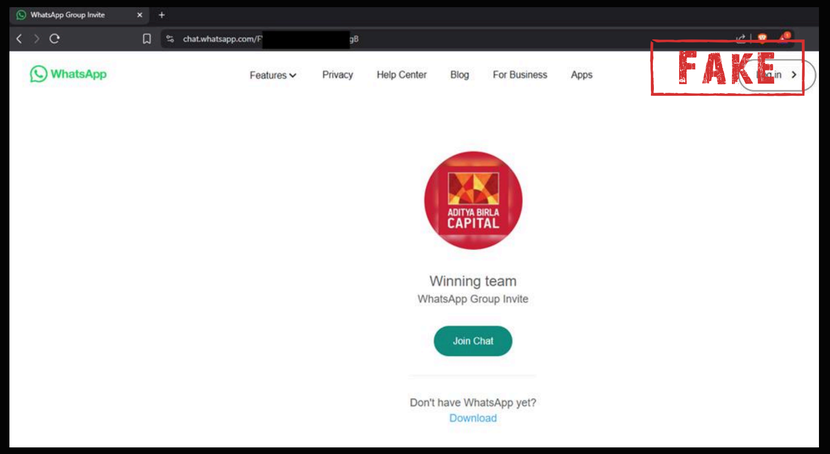
Impact: Early detection enabled immediate alerts and takedown efforts—preventing financial fraud, brand damage, and customer deception during a high-visibility event.

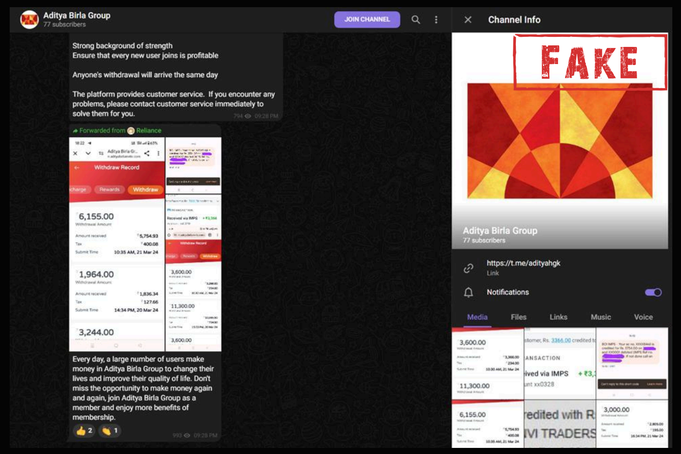
THREATWATCH360
See Risk, Secure Instantly

Case study 3: NBFC (Aditya Birla Capital)









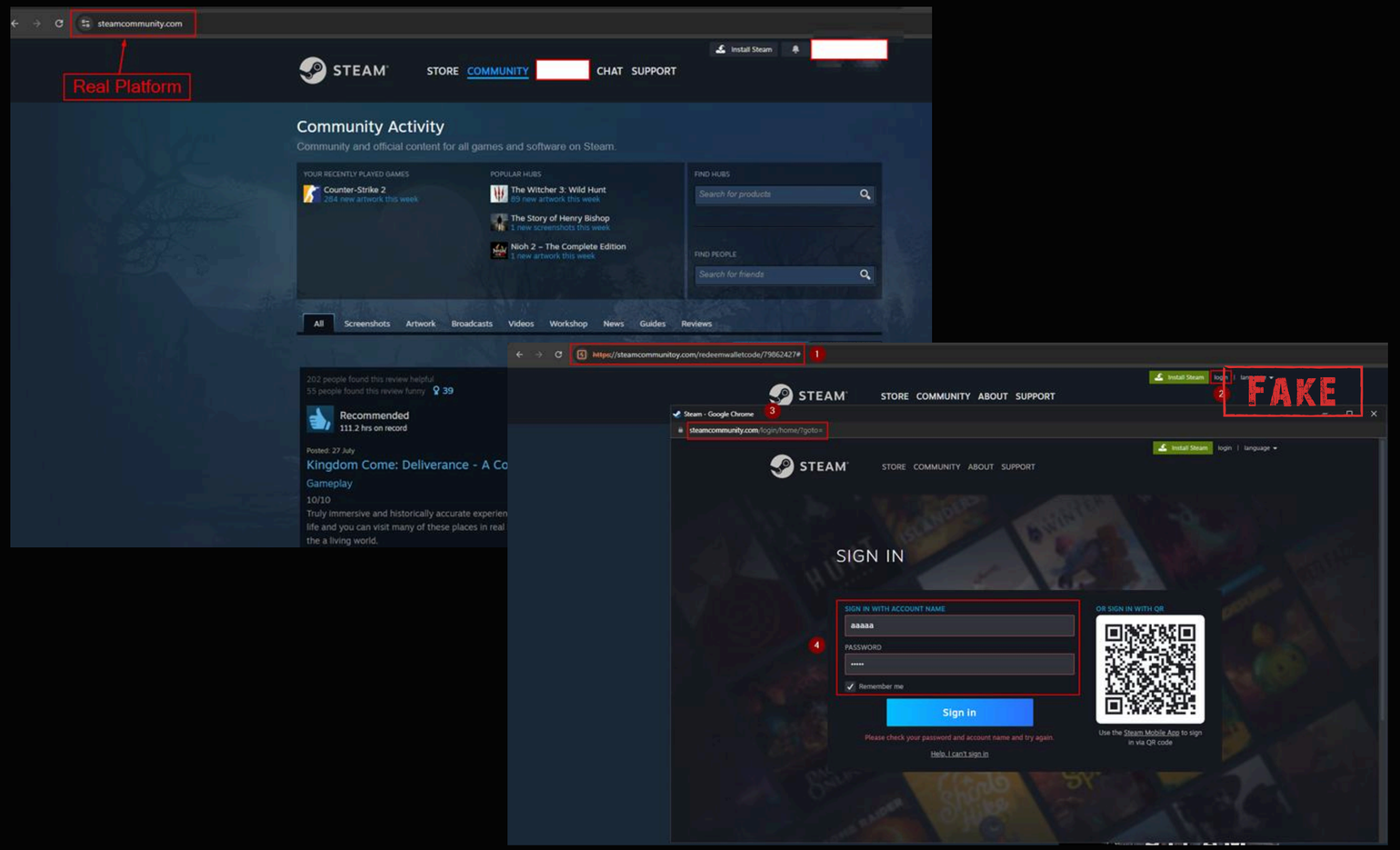
Phishing Campaign Targeting Aditya Birla Capital

ThreatWatch360 detected an ongoing phishing campaign targeting Aditya Birla Capital, a major BFSI player. Threat actors launched lookalike websites and fake job portals to harvest sensitive data, including login credentials and personal financial details.

Leveraging our Anti-Phishing, Early-Warning, and Social Media Intelligence modules, we uncovered numerous impersonation domains, fake profiles, and coordinated campaigns across Telegram, Instagram, WhatsApp, and Facebook groups that were promoting fraudulent investment schemes.

Impact: Timely alerts and threat intelligence enabled swift takedown actions—preventing customer data theft, financial fraud, and reputational loss in the BFSI sector.

Case study 4: Gaming industry (Steam platform)



Malicious Campaign Targeting Gaming Industry – Steam Users

ThreatWatch360 uncovered a malicious campaign targeting the gaming industry, where phishing websites were designed to mimic popular gaming platforms like Steam to steal user credentials for account takeover and in-game assets.

Using our Anti-Phishing and Early-Warning modules, we detected multiple lookalike domains configured with login forms, SSL certificates, and Steam-themed branding to deceive users.

POC: A Deep Dive into Anti-Phishing Detection Targeting Steam Platform Users

One domain closely mimicked the official Steam login page, tricking users into entering their credentials, which were then used for account hijacking and black-market trading.

Impact: Early detection and takedown of phishing sites helped prevent gamer identity theft, financial losses, and platform abuse, reinforcing our role in protecting digital platforms in the gaming sector.

THREATWATCH360
See Risk, Secure Instantly

Yes, we're built to meet RBI, IRDAI, and NDSL / SEBI Regulated Entities compliance.

RBI Compliance (Banks And NBFCs)

- Aligned With The RBI Cybersecurity Framework For Proactive Threat Detection, Breach Alerting, And Incident Response.
- Supports Early Identification Of Phishing Domains, Credential Leaks, And Unauthorized Access Attempts.

NDSL / SEBI Regulated Entities Compliance (Depositories And Participants)

- Real-Time Monitoring Of Credential Exposure And Digital Asset Breaches.
- Supports NSDL IT Security Policy (Point No. 2) By Ensuring Timely Detection Of Threats Impacting Investor Data And Core Business Systems.

IRDAI Compliance (Insurance Sector)

- Enables Rapid Detection And Takedown Of Phishing Campaigns And Brand Impersonation Threats, In Line With IRDAI's 2023 Cybersecurity Guidelines.
- Provides Compliance-Ready Reports For Faster Breach Notification And Regulatory Reporting.

THREATWATCH360
See Risk, Secure Instantly

Express Towers, Nariman Point,
Marine Drive, Mumbai, MH 400021

Want To See Who’s Targeting Your Brand Right Now? Let’s Talk.

contact@threatwatch360.com

https://threatwatch360.com/