WANTED

for

Account Takeover

Average Loss:
$4.81 Million
per Attack

Bobby compromises legitimate email accounts to exfiltrate sensitive data, access connected apps, or send additional attacks. His campaigns are among the most damaging—with the average cost of a data breach caused by compromised credentials totaling $4.81 million.

BOBBY BEAUX-GUS

WANTED

for Vendor Email Compromise

Attempted $36 Million Invoice Fraud Attack

Opting to impersonate vendors rather than internal employees, Frauderick convinces his targets to pay fake invoices, send fraudulent wire transfers, or update banking account details. The largest vendor fraud attack stopped by Abnormal to date involved a request for $36 million.

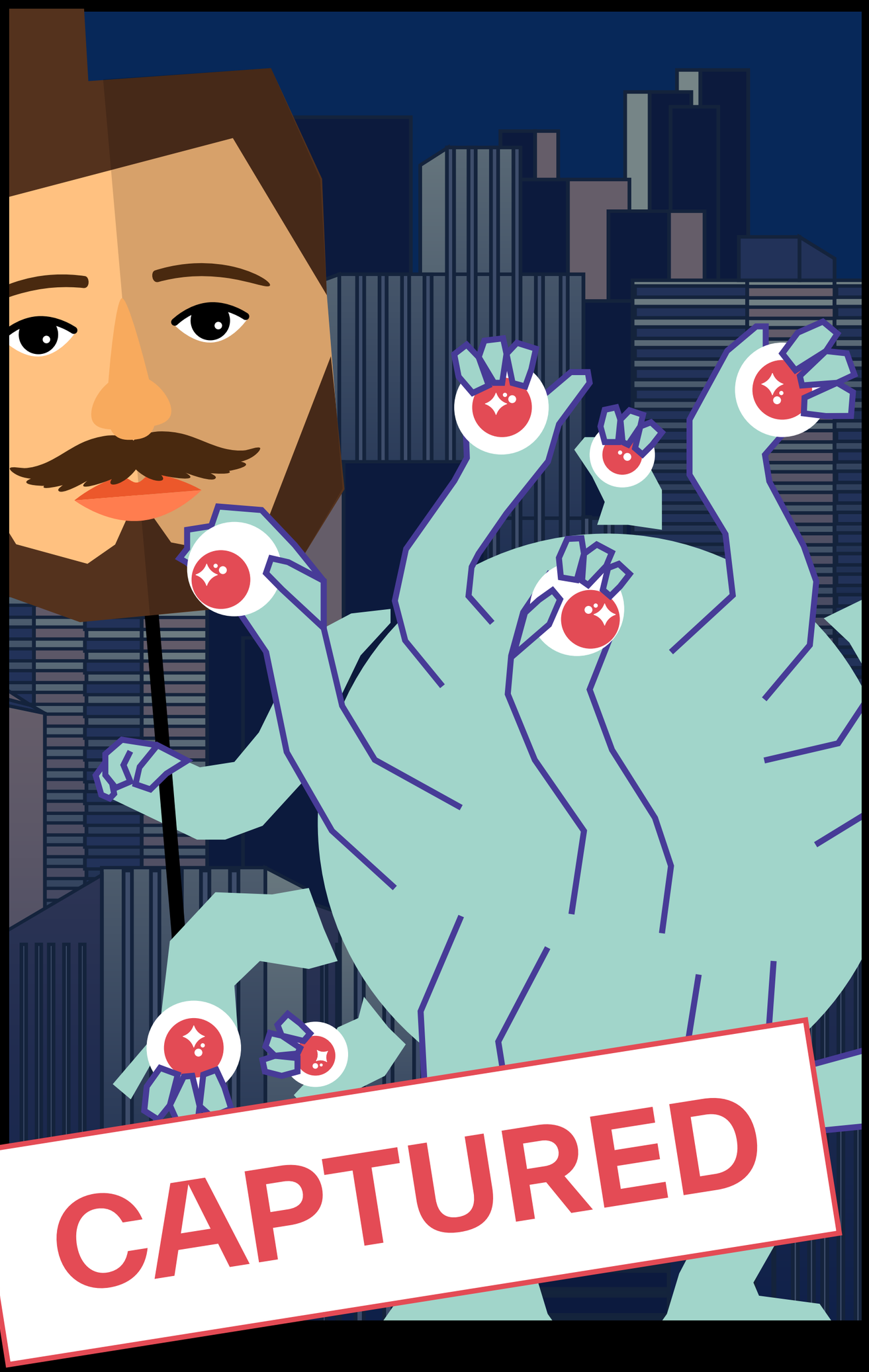
FRAUDERICK

WANTED

for
Business Email Compromise

Caused $2.95 Billion in Losses in 2023

Greta’s modus operandi is impersonating executives and other internal employees. Using social engineering tactics, she encourages recipients to provide valuable data and send her money. Greta’s successful BEC attacks accounted for nearly $3 billion in losses last year alone.



GRIFTY GRETA

WANTED

for

Malware + Ransomware

Increased Attack Losses by 74%

Malcolm's attacks exploit trusted digital entities and use emails that reference relevant topics to urge recipients to click on malicious links or download malicious attachments. A growing threat, the total losses from his attacks increased by 74% from last year.

MALICIOUS MALCOLM

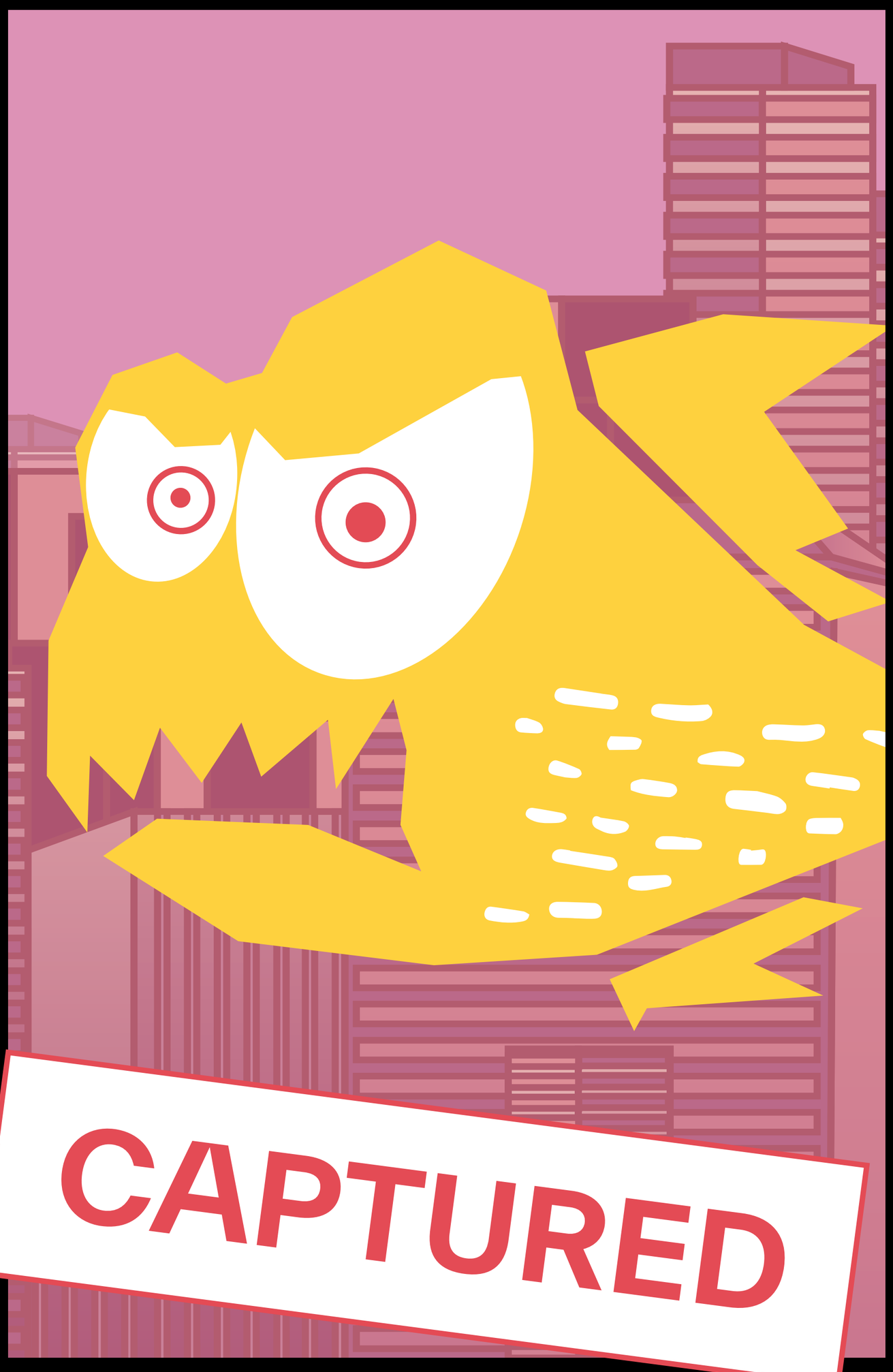
WANTED

for

Credential Phishing

Launched 73% of All Advanced Email Attacks in 2023

Disguising his emails as legitimate communication from a known organization or individual, Reeler sends fraudulent messages to trick employees into revealing their credentials for enterprise applications. He's very popular! Reeler's messages account for 73% of all advanced email attacks.



REELER

WANTED

for
QR Code Attacks

Contributed to 300,000 Phishing Attacks in 2023

Olivia Obscura burst onto the scene in 2020, capitalizing on the sudden ubiquity of QR codes. Masquerading as trusted brands, Olivia compels targets to scan malicious QR codes connected to phishing pages. Her campaigns contributed to the nearly 300,000 phishing incidents reported in 2023.

OLIVIA OBSCURA

WANTED

for

AI-Generated Attacks

Top Concern for 98% of Security Leaders

A relative newcomer to the Anomalies, GenAimee uses data scraped from social media, online activity, and previous correspondence to craft malicious emails tailored to individual recipients with unprecedented precision. Her threats are a significant challenge for security leaders—98% of whom report security risks from generative AI are a major concern.

GEN AIMEE

WANTED

for

Third-Party App Attacks

Average Loss:
$4.46 Million
per Attack

Rather than target the inbox directly, Victor takes advantage of vulnerabilities created by integrations with third-party applications. He exploits third-party apps connected to the email environment to gain access and steal information, costing organizations an average of $4.46 million per incident.

VICTOR VECTOR