ANOMALI®

CYBER Q6

PREVENT FRAUD, DATA BREACHES, AND OTHER ELECTRONIC CRIMES

Actionable and targeted e-crime intelligence collected 24/7 from the dark & deep web, private chat platforms, malware networks, botnets, and other cybercrime infrastructure

ANOMALI AND Q6 CYBER JOINT SOLUTION FEATURES:

- **Comprehensive Coverage of the 'Digital Underground'** — Not only the dark & deep web, but also malware networks, botnets, and private messaging platforms.
- Powerful combination of proprietary technology and human intelligence (HUMINT).
- **Finished Intelligence** — Immediately actionable, tailored and real-time.
- **Outside-in Monitoring** — No access required to your systems or data.
- **High Impact** — Measurable ROI through significant reduction of fraud losses and security breaches; on average, investment recovered in less than 3 months.
- **Fusion** — Shared e-Crime Intelligence for Intelligence, Anti-Fraud, Financial Crimes, and AML teams.

IMMEDIATE TIME-TO-VALUE

- Proactively identify and protect customers at high risk of account takeover.
- Act preemptively by flagging credit, debit, and gift cards that have been compromised, before the fraud occurs.
- Receive alerts of merchant breaches weeks before they are made public and mitigate payment card fraud.
- Flag internal and external mule accounts to prevent illicit fund transfers.
- Detect and quickly remediate network intrusions, system or data breaches, and insider threats.
- Discover data breaches and network compromises of your key vendors and partners.
- Track the latest cybercriminals and schemes targeting your organization and peer companies.

Q6 CYBER E-CRIME INTELLIGENCE

Our 24x7 comprehensive monitoring of the Digital Underground can help you transform your information security and anti-fraud operations from reactive to proactive. We track cybercriminals and fraudsters wherever they operate to proactively identify and eliminate emerging threats and imminent attacks — before they rear their ugly heads.

CRITICAL INTELLIGENCE

E-crime prevention through 24x7 monitoring of the digital underground.

FLEXIBLE DEPLOYMENTS

Fast, scalable implementation on-premises and in the cloud.

IMMEDIATE RESULTS

Highly actionable e-Crime Intelligence with immediate reduction of fraud-related losses and security breaches.

This is the next generation of the next generation of threat intelligence. *CISO, Fortune 100 company*

CASE STUDY: ACCOUNT TAKEOVERS

CHALLENGE:

A large bank lacked visibility into targeted malware campaigns and was suffering increasing losses related to customer account takeovers.

SOLUTION:

Q6 detected a sophisticated malware campaign targeting customers of a large global bank. The cybercriminal ring planned to take over and cash out hundreds of victim accounts. Q6 provided the bank with many of the compromised victim accounts ahead of the cash-out, as well as intelligence regarding the operation and the cybercriminal ring. The bank took immediate steps to protect these customer accounts and track the activities of the threat actors.

CUSTOMER BENEFIT:

The bank implemented enhanced anti-fraud controls to defeat similar schemes going forward. The solution prevented over one million dollars in fraud losses.

CASE STUDY: PAYMENT CARD FRAUD

CHALLENGE:

A regional bank in the USA had been experiencing significant increases in debit card fraud losses and engaged Q6 to help.

SOLUTION:

Q6's E-Crime Intelligence platform discovered large amounts of the bank's compromised payment cards trading on numerous criminal Dark Web marketplaces as well as "best practice" guides for cashing out the bank's cards shared on prominent Dark Web communities.

CUSTOMER BENEFIT:

Q6's ongoing monitoring enabled the bank to proactively identify and flag compromised accounts ahead of fraud and to implement additional anti-fraud controls to block the fraudsters' schemes. This ultimately reduced debit card fraud losses by more than 30%.

CASE STUDY: BREACH ALERTS

CHALLENGE:

A large hospitality company did not have visibility into breaches at their franchised and corporate-owned properties.

SOLUTION:

Q6 detected a network intrusion of a leading hospitality company including a breach of sensitive corporate and client data. Q6 immediately alerted the company, which quickly initiated its incident response protocol. The company quickly contained the incident and limited the damage.

CUSTOMER BENEFIT:

By monitoring a large-scale malware operation run by a sophisticated cybercriminal organization, a major incident was averted.

CASE STUDY: THIRD-PARTY RISK

CHALLENGE:

An E-Commerce company could not monitor in real-time its exposure to third and fourth party vendors.

SOLUTION:

While monitoring foreign language, invitation-only hacking forums on the Dark Web, Q6 detected "chatter" regarding a breach of a company providing services to the E-Commerce industry. Q6 alerted its client, a large E-Commerce company, about its potential exposure resulting from the breach of a key vendor.

CUSTOMER BENEFIT:

The company immediately took steps to mitigate its exposure. A major incident was averted.