NICE · ACTIMIZE

Using Dark Web Intelligence for Proactive Fraud Prevention

eBook

NICE · ACTIMIZE

The Dark Web

A home base, storage platform and open exchange for cybercriminals specializing in targeting financial institutions (FSOs). A lawless marketplace that includes communication and collaboration of stolen information.

With financial losses
from identity fraud reaching

$56 billion in 2020,[1]

FSOs must not only fight back,
but stay vigilant.

The Digital Underground supports a vast array of global financial crime.

Security and anti-fraud and evasion tools and controls are shared.

Financial mules are recruited and shared.

Stolen PII, or synthetic identities, are available.

Massive quantities of compromised payment card data are traded.

Black market e-commerce sites sell stolen financial account data either à la carte or via large troves.

The Growth Trajectory of Fraud Manifesting from Dark Web Obtained Data

FSOs need to understand various types of fraudulent attacks and trends to identify their vulnerabilities, strengthen their fraud prevention programs, and better safeguard their organization and customers.

The COVID-19 pandemic has caused great shifts in consumer buying behavior, such as digital transactions, types and amounts of purchases. Rapid increases of legitimate transactions have stressed and perhaps “broken” older anti-fraud detection models, creating opportunities for cybercriminals.

NICE · ACTIMIZE

18.7 billion identity records were circulating across the Dark Web in 2019, an increase of **25%** from the previous year.[1]

What is Account Takeover (ATO) and Why is It Difficult to Detect?

NICE · ACTIMIZE

Increased Account Takeover (ATO) scams coincided with exponential increases in online transactions during the COVID-19 pandemic.

Cybercriminals can log into a victim's online banking account using the victim's own machine. Once in, this unauthorized log is very difficult to detect and the cybercriminal now has access to any number of financial crimes such as wire fraud, ACH fraud, fraudulent Zelle transfer, stock manipulation, payroll fraud and more.

NICE · ACTIMIZE

Detection challenge: Dark Web marketplaces have account credentials for sale for as low as $2-9 per account.[2] These accounts feed malware harvesting attacks.

SOCIAL MEDIA	E-COMMERCE	FINANCIAL SERVICES		FOOD DELIVERY SERVICES
Avg Price/Account $2	Avg Price/Account $3	Avg Price/Account $4.30	Avg Price/Account $2	Avg Price/Account $2

Image illustrates the availability of accounts for select leading companies across industries.[3]

What is Payment Card Fraud and Why is It Difficult to Detect?

Credit card fraud is popular among cybercriminals. Global card fraud losses reached $28.65 billion in 2019[4] with projections to only increase in scale and sophistication in the coming years.

Payment card fraud has continued to grow during the COVID-19 pandemic. FSOs have reported that the dollar volume of attempted fraudulent transactions rose

35% over the prior year[5] since April 2020, a trend expected to continue.

Detection challenge: Illicit Dark Web e-commerce platforms sell not only card data, but also offer account holder PII (social security number, date of birth, mother's maiden name, email passwords, IP address, last paid amount, ATM or wireless PIN). Victim's PII, along with compromised card data, increases the ability to bypass anti-fraud controls.

Data is not the only product that helps criminals. "Best practice" guides for cashing out the bank's cards are available on prominent Dark Web marketplaces.

NICE ACTIMIZE

Total payment card volume is forecasted to be

$56.182 trillion

by 2025, with gross card fraud globally estimated to be

$35.31 billion.[5]

What are Mule Accounts and Why are They Difficult to Detect?

Mule accounts are essential to illicit financial transactions like fraud and money laundering.

Over 90% of money mule transactions are connected to cybercrimes such as malware attacks, phishing, business email compromise (BEC), CEO fraud, online action fraud, romance scams and others.[6]

Given this percentage, mule accounts detection is a high priority for financial infrastructures. Using peer-to-peer instant payment platforms such as Zelle, mule accounts can execute rapid transactions with stealth.

Detection challenge: Criminal groups use the Dark Web to recruit and manage large networks of mules “as-a-service” ahead of time, making advanced detection difficult.

Using the Dark Web as a Tool Against Fraudsters & Cybercriminals

Incorporating digital underground and Dark Web e-crime intelligence allows FSOs to identify and eliminate fraud and financial crime before an attack can be carried out, and transform anti-fraud and financial strategies from reactive to proactive.

Proactive Fraud Detection with IFM-X Dark Web Intelligence

Using IFM-X Dark Web Intelligence from NICE Actimize, clients can effectively defend their customers. Security experts collect and analyze massive volumes of data to track security events and provide intelligence on bad actors.

IFM-X Dark Web Intelligence

NICE · ACTIMIZE

Three major data feeds are infused into this analysis:

- **Account Takeovers:** Contains compromised details that can be used to identify customers at high risk of takeover before it occurs.
- **Compromised Payment Cards:** Includes debit, prepaid, credit and gift cards that have been compromised and are at high risk of fraud.
- **Mule Accounts:** Contains financial mule accounts associated with fraud, money laundering and other financial crimes across FSOs.

Defend Against Bad Actors with Actionable Dark Web Intelligence

NICE · ACTIMIZE

IFM-X Dark Web Intelligence delivers immediately actionable, tailored and constantly refreshed intelligence and monitoring across post-breach pre-fraud scenarios, resulting in significant reduction of fraud losses and financial crime.

- Deploy holistic coverage across customer account takeovers, compromised payment cards and mules accounts.
- Minimize operational expenses associated with fraud prevention and investigation.
- Facilitate streamlined integration with existing fraud prevention processes and controls, and security systems while mitigating the need for downstream processing or analysis.
- Allows FSOs to build and optimize fraud prevention models based on current and emerging attack vectors.
- Leverage shared intelligence to augment and empower financial crime, AML, information security and anti-fraud teams.

Proactive Fraud Detection with IFM-X Dark Web Intelligence

Real-time intelligence from **IFM-X Dark Web Intelligence** drives immediate fraud prevention. Mitigate customer account takeover attempts, combat payment card fraud without causing undue customer friction, and block mule activity in its tracks.

Schedule a Demo

1 Puranik, T. (2021, March 23). Total Identity Fraud Losses Soar to $56 Billion in 2020. Javelin. https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020

2 (2020). 4iQ Identity Breach Report 2020. 4iQ. https://4iq.com/2020-identity-breach-report/

3 Dark Web Price Index 2021 - Dark Web Prices of Personal Data. Privacy Affairs. (2021, June 1). https://www.privacyaffairs.com/dark-web-price-index-2021/.

4 (2020, December 1). Card Fraud Losses Reach $28.65 Billion. Nilson Report. https://nilsonreport.com/mention/1313/1link/

5 Andriotis, A., & McCaffrey, O. (2020, May 27). Borrower, Beware: Credit-Card Fraud Attempts Rise During the Coronavirus Crisis. The Wall Street Journal. https://www.wsj.com/articles/borrower-beware-credit-card-fraud-attempts-rise-during-the-coronavirus-crisis-11590571800

6 Money Muling: Public Awareness and Prevention Guide. Europol. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling

7 Mayfield, J. (2021, February 4) New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020. Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com