

The Cyberint logo is located in the top right corner. It features the word "Cyberint" in a white, sans-serif font, with a small red dot above the letter 'i'.

Cyberint

TARGETED THREAT INTELLIGENCE

The background of the slide features a complex, abstract network visualization. It consists of numerous glowing blue and yellow nodes connected by thin, white lines, creating a dense web of connections. The nodes are scattered across the right side of the slide, with some appearing as bright yellow dots and others as smaller blue dots. The lines connecting them are thin and white, creating a sense of movement and connectivity. The overall color scheme is dark blue and black, with the glowing nodes and lines providing a high-contrast visual element.

CyberInt's Targeted Threat Intelligence Based on Argos™ Platform

Every day, companies and organizations face the challenge of ever-evolving cyber criminals and threat actors, who become more sophisticated and more resilient to traditional perimeter-based security technologies. Under current targeted cyberthreats, the most robust traditional security is unable to adequately protect an organization. Redefining your cybersecurity strategy is critical in today's and tomorrow's reality in order to outsmart threat actors.



CyberInt's Argos™ Targeted Threat Intelligence solution offers your organization a threat-centric approach to detect in the darknet, deep and open web the threats targeting your organization in order to protect what matters to you most: your customers, employees, business and brand. The solution is based on the machine learning technology platform that automatically crawls 1000's of data sources in the darknet, deep and open web, contextualizes the events and enriches them leveraging AI algorithms to provide prioritized alerts according to the threat to our customers.

Augmented by our multilingual team of cyber experts and intelligence analysts, the platform is finetuned by their deep dive investigations and high touch relationship with our customers' security teams to verify the threat, understand the potential impact, alert and act with the mitigation and remediation steps accordingly. With their expertise in financial services, retail, and ecommerce industries, they are able to detect vertical specific threats as well as sophisticated cyber TTPs.

Argos™ Targeted Threat Intelligence offers full coverage of industry specific threat intelligence sources, including 4shared, mpgh, wwh-club, QQ and IRC rooms.

KEY BENEFITS:

Discovers vulnerabilities and threats to enable mitigation before they turn into incidents or breaches

Detects phishing attempts and provides take downs per customer engagement

Detects fraud such as refund scams, carding, and others

Tracks 'refund as a service' providers

Why Argos™ Targeted Threat Intelligence?

Gathering targeted and actionable intelligence, Argos™ Targeted Threat Intelligence pools both technological and human resources to:

- Generate real-time alerts of targeted attacks, data leakage and stolen credentials compromising your organization
- Identify threat actors targeting you in real time and provide contextual data about them
- Assess hundreds of sources of collected targeted data (feeds, IRC, Dark Web, blogs, social media, forums, and paste sites)
- Automate a proven intelligence process
- Analyze results and provide practical mitigation support
- Utilize a strong entity database of threat actors and tools for attribution and to maximize context

WHAT CUSTOMERS ARE SAYING

"CyberInt's threat intelligence is unlike any other's. It is not just threat intelligence for retail. It is threat intelligence that is specifically tailored to us"

Large UK-based ecommerce retailer

”

USE CASES

Targeted Threat Intelligence In Action

- **Personally Identifiable Information (PII) and Payment Card Industry (PCI) data leak**
Compromised personal and financial customer data available online
- **Confidential Data Exposure**
Internal financial leaks and confidential corporate exposures
- **Credential Stuffing**
Automated injection of stolen usernames/emails and passwords in order to gain unauthorized access to user accounts
- **Accounts for Sale**
Hacked accounts offered for sale on dark web marketplaces

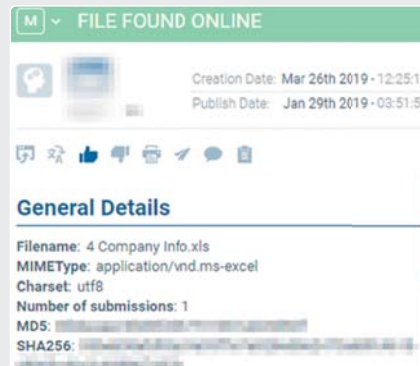
Targeted Threat Intelligence

Indicators on Argos™

Credential stuffing tool
targeting CompanyX



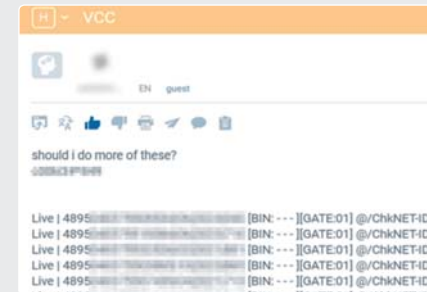
CompanyX's Confidential Data
Available Online



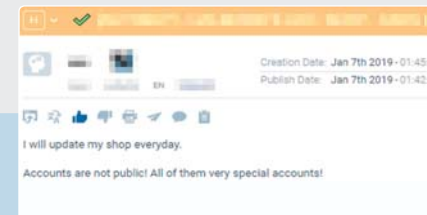
4

Cyberint

Leaked credit cards



CompanyX's customers
accounts offered for sale



Cyberint Copyright © All Rights Reserved 2019

USE CASES

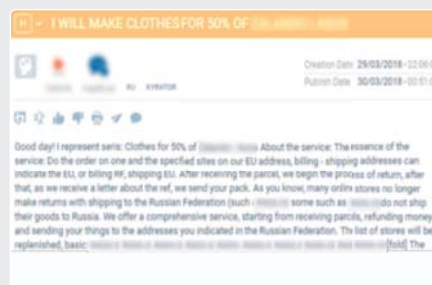
Targeted Threat Intelligence In Action

- **Brand Abuse**
Be it in a mobile app, website or social media asset, threat actors are utilizing well known brands to lure targets
- **Fraudulent Refund Scams**
Cybercriminals exchange knowledge and data that allows them to scam retailers into giving out fraudulent refunds
- **Carding**
Identified as an increasingly popular phenomenon, carding typically involves the holder of the stolen card purchasing retailer-branded gift cards, to be later sold to others, or used to purchase other goods that can be sold for cash
- **Fake Vouchers**
Fake vouchers generated and sold on various markets

Targeted Threat Intelligence

Indicators on Argos™

Fraudulent Refund



Carding



Cyberint

USA

Tel: +1-646-568-7813 | 214 W 29th Street, Suite 06A-104
New York, NY, 10001 | USA

United Kingdom

Tel: + 44203514151525 | Fox Court
14 Grays Inn Rd, Holborn, London WC1X 8HN, Suite 2068

Israel

Tel: +972-3-7286777 | Fax: +972-3-7286777
17 Ha-Mefalsim St | 4951447 | Kiryat Aryeh Petah-Tikva | Israel

Singapore

Tel: +65-3163-5760 | 10 Anson Road
#33-04A International Plaza 079903 | Singapore

sales@cyberint.com

Cyberint.