

DISA Technical Exchange Meeting

April 9, 2024

Presented by:

Rick Hedeman rick.h@cybersixgill.com

Edan Cohen edan@cybersixgill.com

Agenda

- About Cybersixgill
- Core Capabilities and Use Cases
- Live Demo
- Questions



Who are we?

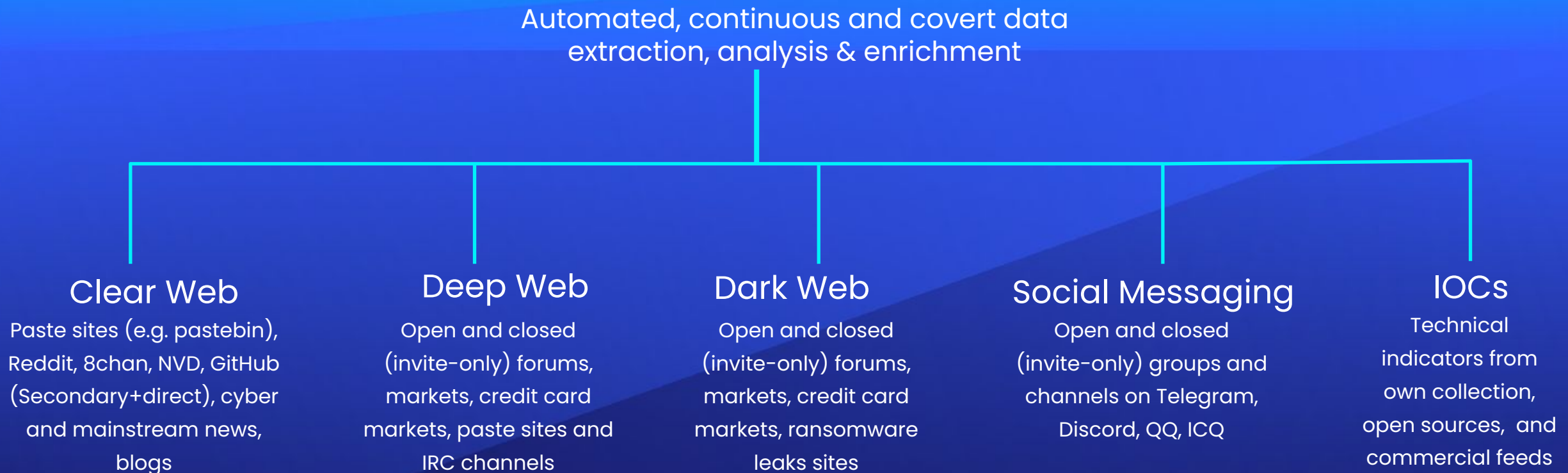
Cybersixgill delivers actionable Cyber Threat Intelligence directly from the underground for Government agencies, Enterprises, Global Systems Integrators, Technology companies, MSSPs, and Law Enforcement.

Leveraging Cybersixgill's strategic, operational and tactical intelligence, organizations can proactively detect, investigate, and respond to imminent threats.



Sources of collection – where we are collecting from

Collecting and enriching data in real time with AI – in any language, in any format and on any platform.

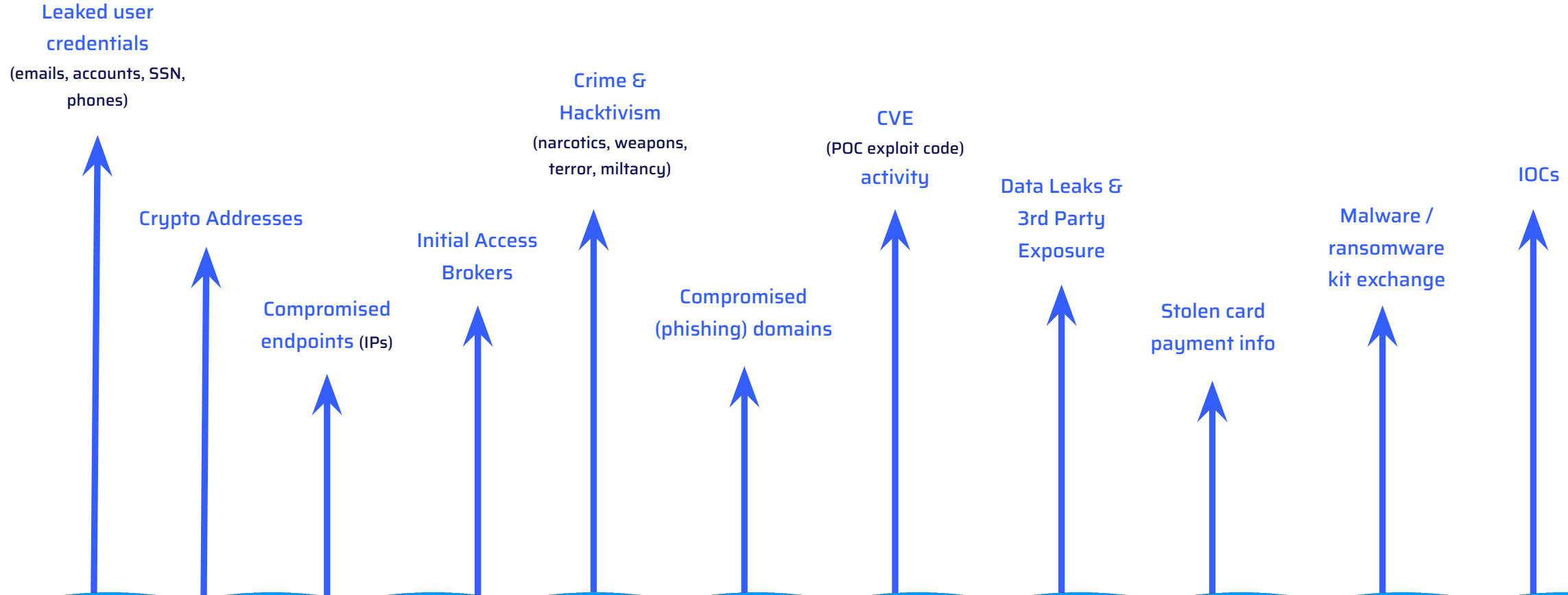


CYBERSIXGILL DATA LAKE



Exposed Threat Intelligence Data Sets Serving Many Use Cases

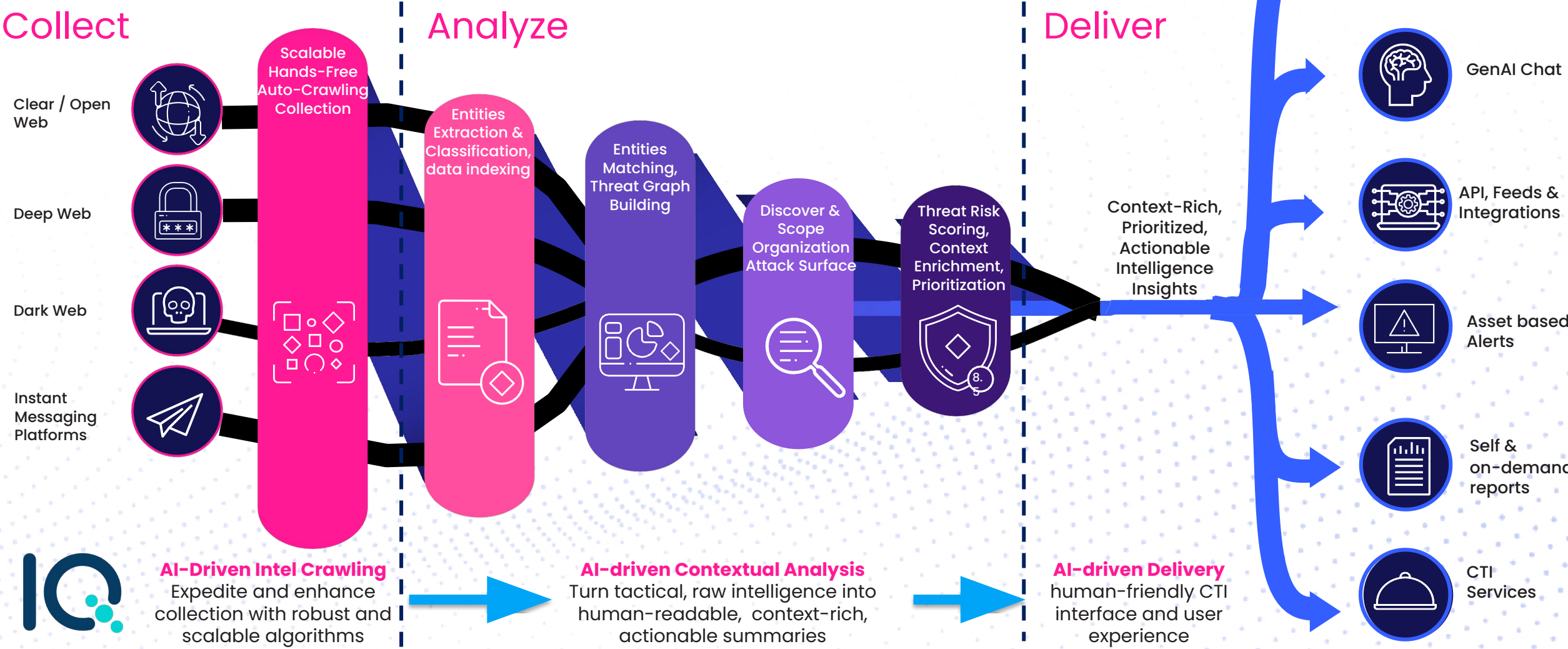
Extracting data in real-time in any language, any format, and on any platform.



CYBERSIXGILL DATA LAKE

Technology Overview

Using AI to Transform Data into Threat Intelligence



Consumption through API and Integrations

TIP/ TI modules

ANOMALI

CYWARE

MISP
Threat Sharing

eclectic iq

THREATQUOTIENT

OPENCTI

ANALYST1

SOAR

Chronicle

CORTEX
XSOAR
BY PALO ALTO NETWORKS

splunk>

SWIMLANE

ThreatConnect.

STRIKE
READY

D3 SECURITY

resilient
an IBM Company

SIEM

IBM
Radar

Microsoft
Azure

splunk>

Elastic Security

sumo logic

CLOUD

snowflake

DATADOG

Intelligence

CROWDSTRIKE

CISCO

MALTEGO



EASM

Randori

CYCOGNITO

censys

CORTEX Xpanse
BY PALO ALTO NETWORKS

IONIX

Security Automation

torq

tines

VM

Qualys
tenable

Ticketing

servicenow

Jira Software

Asset Man.

AXONIOUS

Harnessing the Power of AI with **cybersixgill IQ**

Providing out of the box use case specific customized intelligence to security stakeholders

Strategic Intelligence

- Ad-hoc sectorial & geopolitical threat landscape reports
- Cyber campaign reports
- Executive briefs

Operational Intelligence

- Personalized dashboards
- Threat actors and malware overviews
- Asset-based CTI alert explainability
- security orchestration workflows

Tactical Intelligence

- Efficient Intelligence collection
- Intel item summarizations
- Vulnerability Intelligence insights





Embracing Generative AI across the platform



Intel Analysis

Turning tactical, raw intelligence into human-readable, context, insight-rich and actionable summaries

Intelligence & alerts
Summarization



Intel Generation

Delivering finished intelligence in seconds - customized to industry, geography, persona & use cases

Automatic curated and
customized reports



Intel Experience

Transforming CTI delivery and interface, answering intel questions in a human-friendly way

Chat bot

Live Demo





Highlighted Unique Capabilities

Easing analyst workflows, reducing investigation times, and increasing visibility



Unlimited Investigation
Capabilities



Generative AI Capabilities



Full Data Source
Transparency



Flexible Intelligence Consumption
(UI, API, Integrations)



Access to Raw Data



Vulnerability Intelligence



Images Analysis



Case Management System

Thank you for your time

Questions?

Rick Hedeman, Federal + Sr. GSI Director
rick.h@cybersixgill.com

Edan Cohen, Solution Architect
edan@cybersixgill.com

Visit us at AFCEA Technet Baltimore 2024




Cybersixgill IQ Capability Examples





Advanced search, forensics & investigation capabilities



cybersixgill

Active Filters

Modules

Sites

Site Grade

Source Types

Categories

Tags

Actors

Items

Analytics

Images

Activity by Date

Past Month

59,456 Items

Show 12 duplicates

Order by

Results: 50

	Title And Content	Site	Replies
English	Fullz + method for jd Sign Up (https://cybercarders.com/register/) or Login (https://cybercarders.com/login/) to view this post and enjoy everything our site ha...	forum_cybercard...	-
English	Fullz + method for jd Sign Up (https://cybercarders.com/register/) or Login (https://cybercarders.com/login/) to view this post and enjoy everything our site ha...	forum_cybercard...	-
English	Fullz + method for jd Sign Up (https://cybercarders.com/register/) or Login (https://cybercarders.com/login/) to view this post and enjoy everything our site ha...	forum_cybercard...	-
English	Fullz + method for jd Sign Up (https://cybercarders.com/register/) or Login (https://cybercarders.com/login/) to view this post and enjoy everything our site ha...	forum_cybercard...	-

JAYMART.CO.TH

Type: Post | 07/26/2023, 4:29:11 PM |

Translate ON

IP (104) IP_global (104) +4

Cybersixgill IQ

Victim:
- Company: JAYMART.CO.TH

Geography:
- Headquarters: Ramkamheang Road Rat Phatthana Saphan Sung, Bangkok, 10240, Thailand

Summary:
This post is about a ransomware attack on JAYMART.CO.TH, a consumer electronics and computers retail company based in Bangkok, Thailand. The attack was carried out by the CL0P ransomware group. The company's employee databases, including personal information such as names, addresses, dates of birth, phone numbers, and emails, were compromised. Additionally, databases of sales of mobile phones, wallet balances, transaction files associated with Stellar, and password-protected archives and databases were also affected. The attackers have published a list of folders and files, along with download links for encrypted files. The post also warns that the company has neglected customer security.

Sector:
- Industry: Consumer Electronics & Computers Retail, Retail

Did you find this helpful?

Headquarters:


Ramkamheang Road Rat Phatthana Saphan Sung, Bangkok, 10240, Thailand

Phone:

+6623088196

Website:

POWERED BY



Cybersecurity entity - deep analysis

The screenshot displays the 'Entity Navigator' interface for 'cybersixgill'. The left sidebar contains navigation icons, including a search icon and a list of entity types. The main panel shows a search bar and filters for 'All Entities', 'Malware', 'APTs', 'Actors', 'Domains', 'IPs', 'Hashes', and 'Filters'. The search results list 600 results, with 'APT32' selected. The details for 'APT32' are shown, including its description, aliases, and sources. A 'Histogram' chart is also visible.

Entity Navigator

Search

All Entities Malware **APTs** Actors Domains IPs Hashes Filters: Related mal... Country Mitre Att&ck Clear all

600 results

Name	Type
APT21	apt
APT23	apt
APT24	apt
APT26	apt
APT29	apt
APT32	apt
APT33	apt
APT37	apt
APT40	apt
APT41	apt
APT42	apt
APT43	apt
APT5	apt
APT6	apt
AVIATOR SPIDER	apt

APT32

Insights IOCs Intel Items

Description

IQ • Malpedia • MITRE

Cybersixgill IQ

APT32 is a cyber espionage group that is believed to be operating out of Vietnam. The group is also known as OceanLotus and has been active since at least 2014. APT32 is known for targeting organizations in Southeast Asia, particularly those in Vietnam, as well as other countries such as the Philippines, Laos, and Cambodia. The group has been linked to a number of high-profile attacks, including the 2016 cyber attack on the Vietnamese airline, Vietnam Airlines, and the 2017 cyber attack on the Philippine government. APT32 is also believed to have been involved in the 2019 cyber attack on Toyota Vietnam. APT32 is known for using a range of sophisticated techniques to carry out its attacks, including spear-phishing, malware, and social engineering. The group has also been known to use zero-day vulnerabilities to gain access to target systems. APT32 is believed to be a state-sponsored group, with some experts suggesting that it may be linked to the Vietnamese government. However, the group's exact motivations and affiliations remain unclear.

Details

Entity type: apt
Mitre ID: G0050
Aliases:
APT32
Planet and Diacauso
Ocean Lotus
OceanLotus Group
OceanLotus
APT-32
DANDY LOACH

Sources

social... 55%
im 14%

Histogram

20
16
12
8
4
0

8/8 8/29 9/19 10/10 10/31 11/21 12/12 1/2 1/2

Did you find this helpful?

Malpedia



AI based (Cybersixgill IQ) Strategic analysis

B report for my CISO about the MGM attacks

IQ Title: Report on MGM Resorts Cyberattacks

Date: 2023-11-15

Prepared by: [Your Name]

Position: [Your Position]

Organization: [Your Organization]

Executive Summary:

This report provides an overview of the cyberattacks on MGM Resorts, including the impact, perpetrators, and response. The attacks targeted MGM Resorts' systems and resulted in the compromise of employee data and potential financial losses. The report aims to provide insights into the incident for the Chief Information Security Officer (CISO) and recommend measures to prevent similar attacks in the future.

1. Background:

On September 14, 2023, MGM Resorts International was targeted by the cybercrime group Scattered Spider, the same group that had previously breached Caesars Entertainment Inc. The attackers demanded a ransom from MGM Resorts, although the exact amount remains undisclosed. The attacks exploited vulnerabilities in the identity management vendor Okta, which both MGM and Caesars used.

2. Impact:

- Employee Data Compromise: MGM Resorts employees' personal and banking information was reportedly

POWERED BY

