#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AFD-R02**

Combatting Cybercrime and Fraud with Threat Intelligence

Mary C. Yang

Chief Marketing Officer
LookingGlass Cyber Solutions
@techgirlmary

Matthew J. Swenson

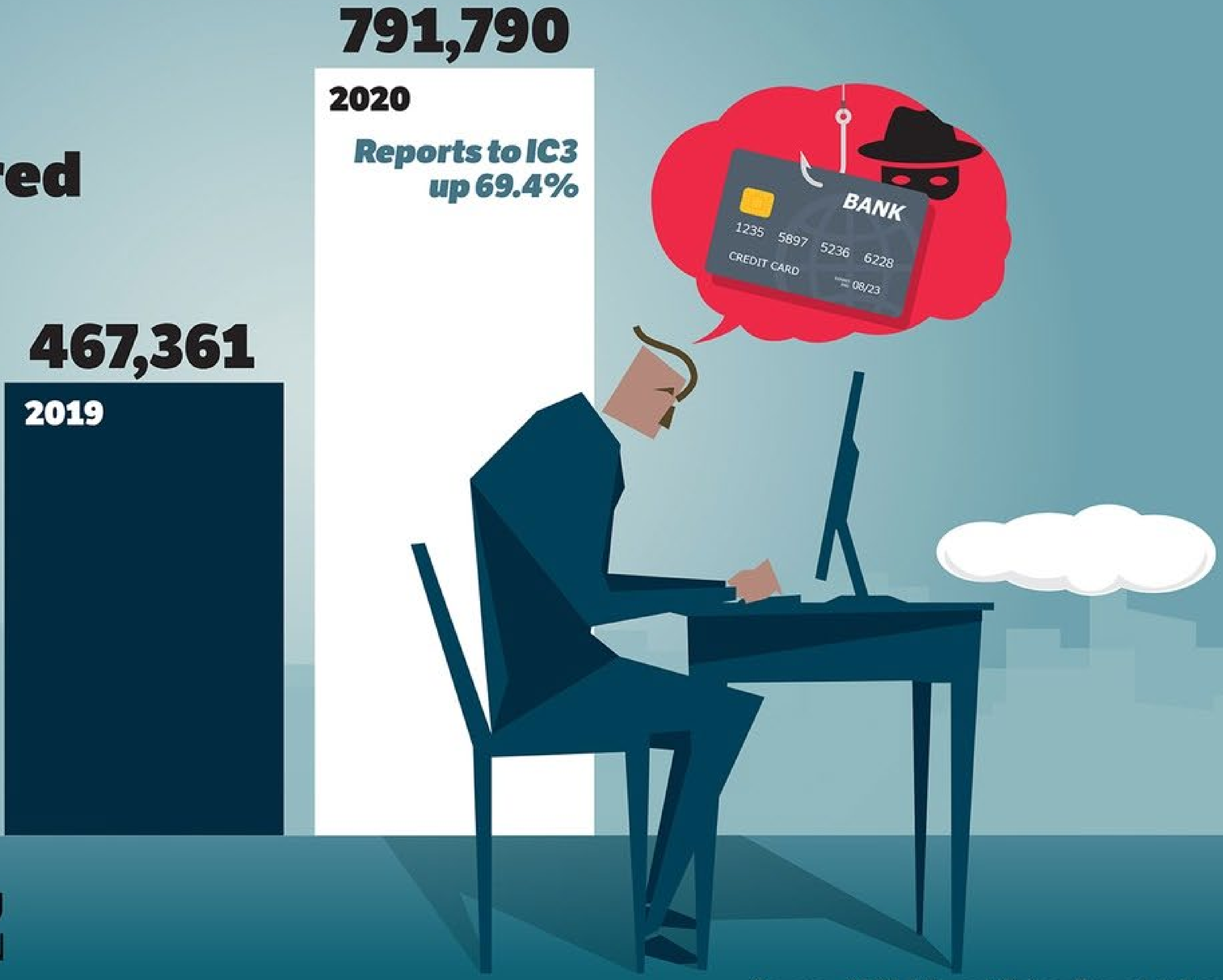
Special Agent & Division Chief
Homeland Security Investigations (HSI),
Cyber Crimes Center (C3)

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

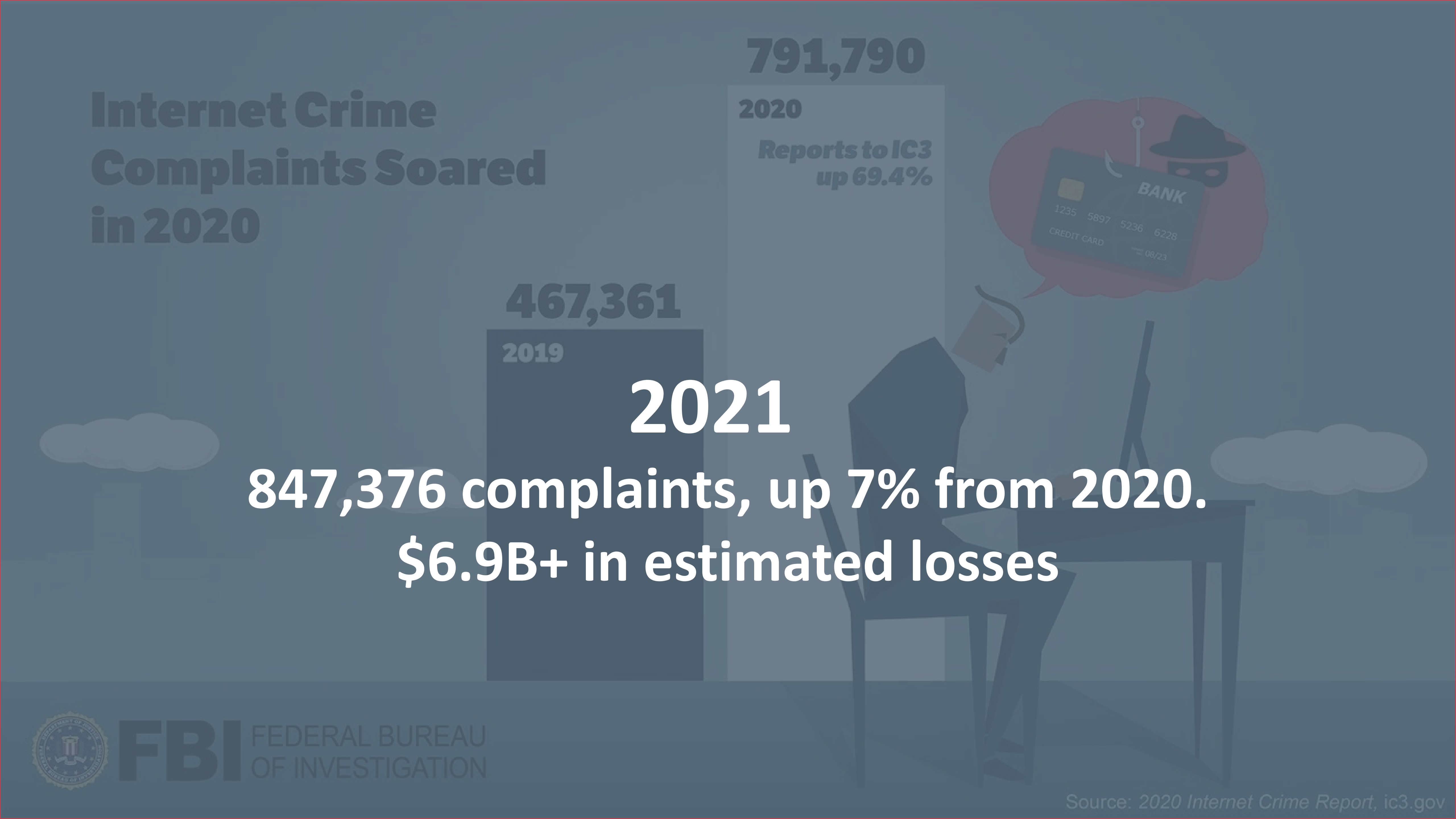
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Internet Crime Complaints Soared in 2020



FBI FEDERAL BUREAU OF INVESTIGATION

Source: *2020 Internet Crime Report*, ic3.gov



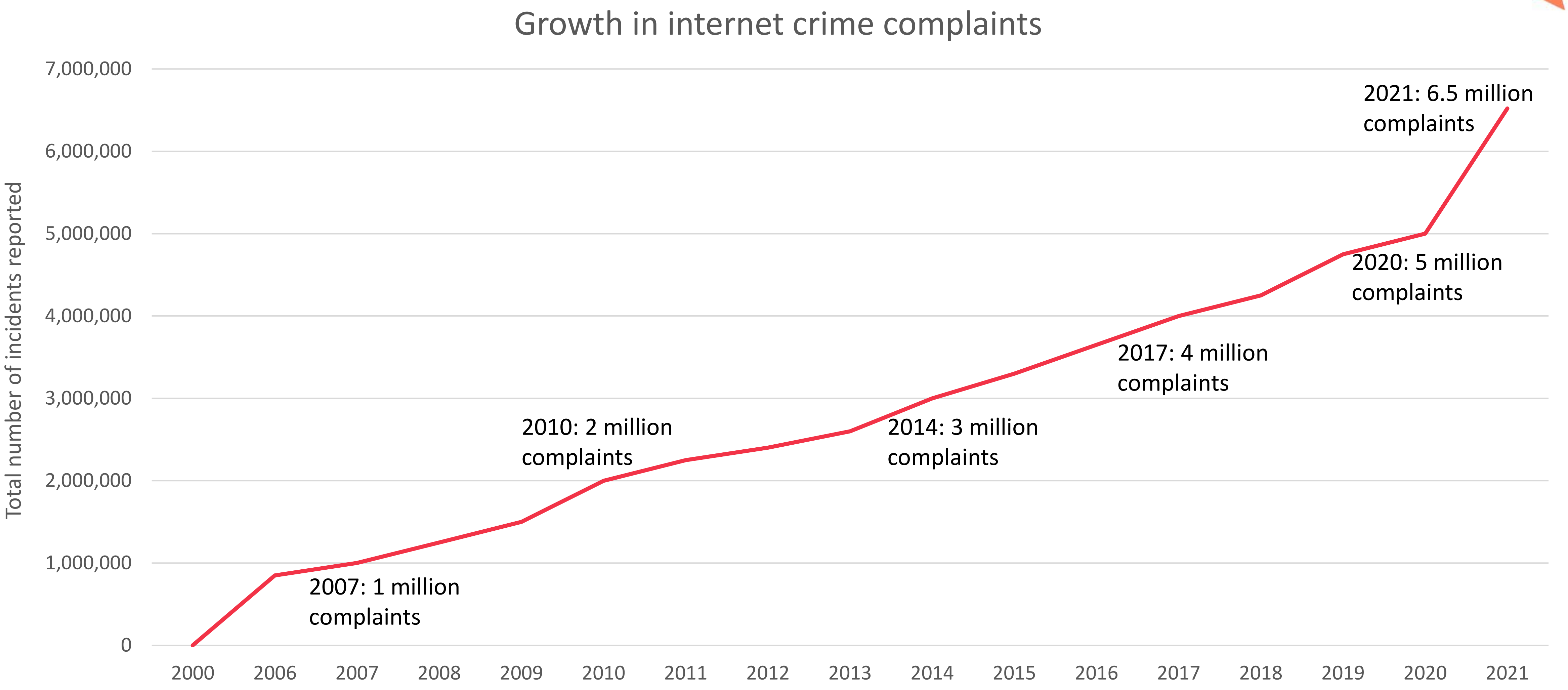
2021

847,376 complaints, up 7% from 2020.

$6.9B+ in estimated losses

Source: *2020 Internet Crime Report*, ic3.gov

2021: Deja Vu



Statistics from the Internet Cyber Crime Center, www.ic3.gov

Cybersecurity Attacks vs Cybercrime vs Fraud

- Cybersecurity attacks often focus on breaching government or corporate networks.
- Cybercrime has typically targeted individuals or people as they navigate online life.
  - Ransomware as a type of cybercrime has grown significantly for businesses over the last few years.
- Fraud is wrongful or criminal deception that results in financial or personal gain for the fraudster.

Leveraging Threat Intelligence & DNS

- Cybersecurity approaches can help combat cybercrime & fraud.
- Enriched Domain Name System (DNS) intelligence:
  - Domain information and reputation
  - Threat intelligence
  - Context and behavior

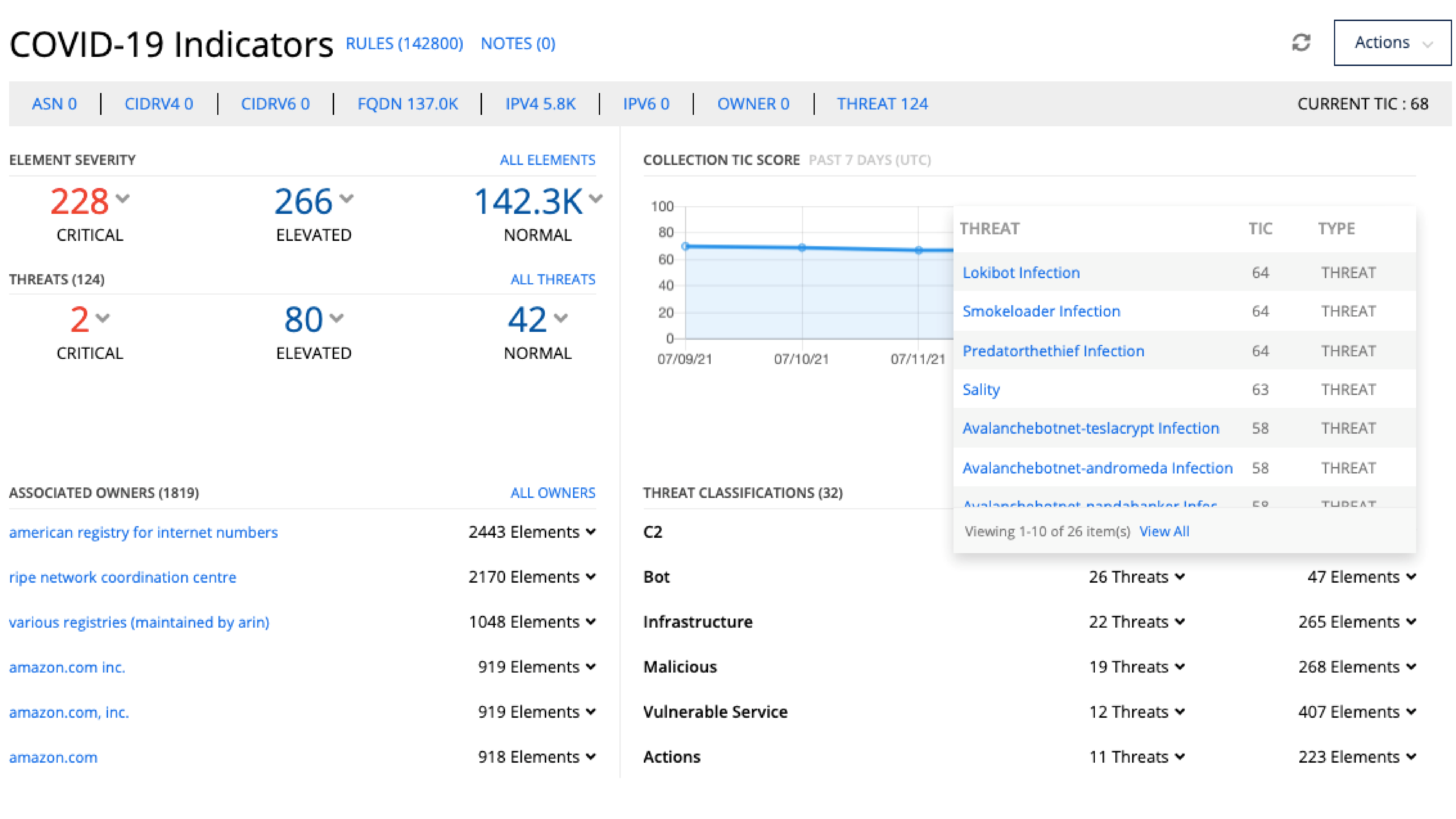
Step 1: Identify Relevant Domains

- February 11: World Health Organization named the global health emergency as "COVID-19"
  - Attackers started to actively deploy opportunistic campaigns
  - The following week, attacks increased eleven-fold*
- Large-scale data collection of newly registered domains
  - Domain name registrations grew by 14.9 million, or 4.2 percent, in 2020 (vs 2019)
- Filter for related terms used in the domains (e.g., COVID-19 terms)

*Government Technology, *Does the Pandemic Explain Recent Spikes in Cyber Crime?*, June 2021

Step 2: Enrich domain information

- Leverage cyber threat data and contextual data to enrich the websites to prioritize which sites need actual investigation.
- Automated enrichment:
  - Identifying the IP hosting the website
  - Network hierarchy and ownership of the IP
  - Whois record and registrant
  - Any associated cyber threat data



COVID-19 Indicators

RULES (142800) NOTES (0)

Actions

ASN 0 | CIDRV4 0 | CIDRV6 0 | FQDN 137.0K | IPV4 5.8K | IPV6 0 | OWNER 0 | THREAT 124

CURRENT TIC : 68

ELEMENT SEVERITY — ALL ELEMENTS

228	266	142.3K
CRITICAL	ELEVATED	NORMAL

THREATS (124) — ALL THREATS

2	80	42
CRITICAL	ELEVATED	NORMAL

COLLECTION TIC SCORE PAST 7 DAYS (UTC)

THREAT	TIC	TYPE
Lokibot Infection	64	THREAT
Smokeloader Infection	64	THREAT
Predatorthethief Infection	64	THREAT
Sality	63	THREAT
Avalanchebotnet-teslacrypt Infection	58	THREAT
Avalanchebotnet-andromeda Infection	58	THREAT
Avalanchebotnet-pandabanker Infec	58	THREAT

Viewing 1-10 of 26 item(s) View All

ASSOCIATED OWNERS (1819) — ALL OWNERS

american registry for internet numbers	2443 Elements
ripe network coordination centre	2170 Elements
various registries (maintained by arin)	1048 Elements
amazon.com inc.	919 Elements
amazon.com, inc.	919 Elements
amazon.com	918 Elements

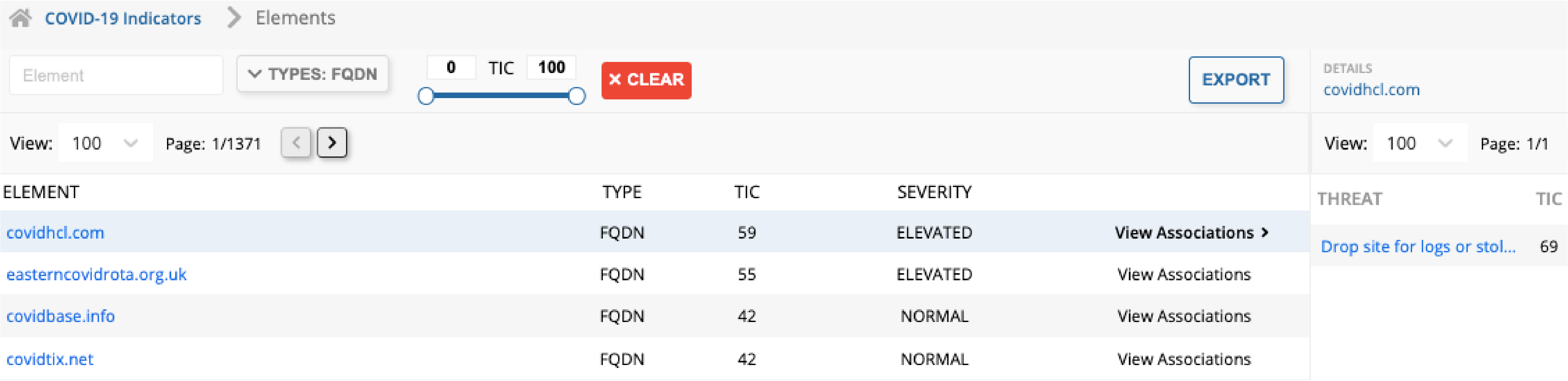
THREAT CLASSIFICATIONS (32)

C2		
Bot	26 Threats	47 Elements
Infrastructure	22 Threats	265 Elements
Malicious	19 Threats	268 Elements
Vulnerable Service	12 Threats	407 Elements
Actions	11 Threats	223 Elements

Step 3: Layer in Context and Behavior

- Threat actors positioned websites to drive traffic
- Automated context
  - Domain squatting
  - Soliciting donations (i.e., fake charities)
- Manual context
  - Offering news and/or opinions about COVID-19
  - Selling products and/or services related to COVID-19 (i.e., fake PPE)
  - Promoting products and/or services related to COVID-19
  - Copycat sites of legitimate orgs, including government sites, with the use of official logos and branding

Risk Scoring for Prioritization



DETAILS
covidhcl.com

View: 100 Page: 1/1371

ELEMENT	TYPE	TIC	SEVERITY	
covidhcl.com	FQDN	59	ELEVATED	View Associations ›
easterncovidrota.org.uk	FQDN	55	ELEVATED	View Associations
covidbase.info	FQDN	42	NORMAL	View Associations
covidtix.net	FQDN	42	NORMAL	View Associations

View: 100 Page: 1/1

THREAT	TIC
Drop site for logs or stol...	69

Example: “covidhcl[.]com” has a risk score of 59, an elevated severity, and is actively associated w/ stealing credentials.

Results

- Of 125,000 malicious COVID-19 sites reviewed, top five associated threat behaviors:
  - 64% were acting as malware C2s
  - 52% as spyware
  - 20% as sites to “steal” credentials and/or PII
  - 20% as marketplaces selling fake antivirus products
  - 17% observed delivering malware

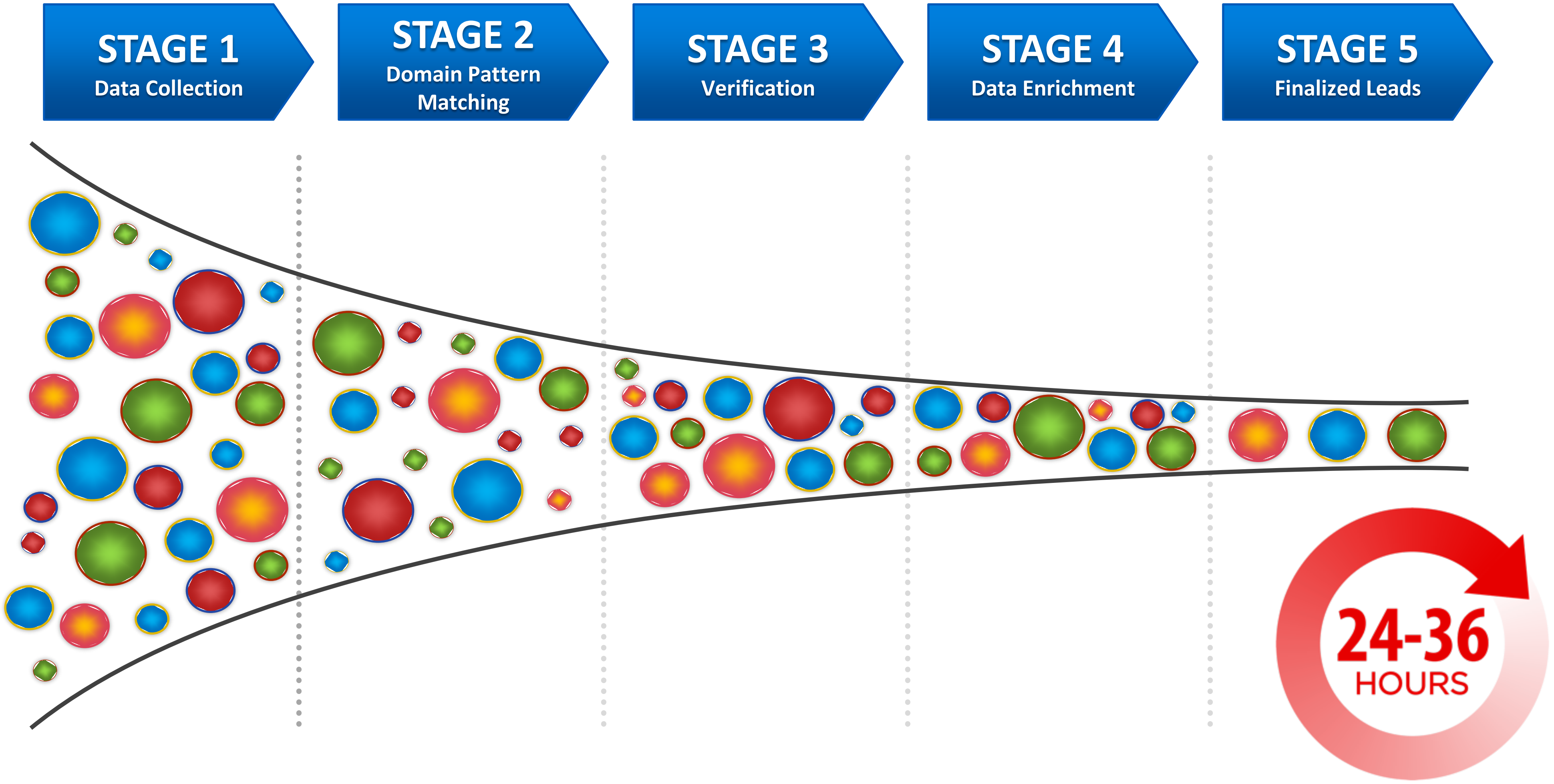
Domain Targeting

Identifying those taking advantage of the COVID-19 pandemic with illicit, financial fraud schemes

Concept & Inception

- Beginning in March 2020, HSI Cyber Crimes Center (C3) was receiving a daily feed of new domains using COVID-19 terms. Develop a workflow using custom script to parse out suspect domains from legitimate domains. Used tools to automate process:
  - Antivirus tools
  - URL scan
  - Cyber threat tools
  - API keys
  - Open-source intelligence

Domain Targeting Workflow



STAGE 1 Data Collection

STAGE 2 Domain Pattern Matching

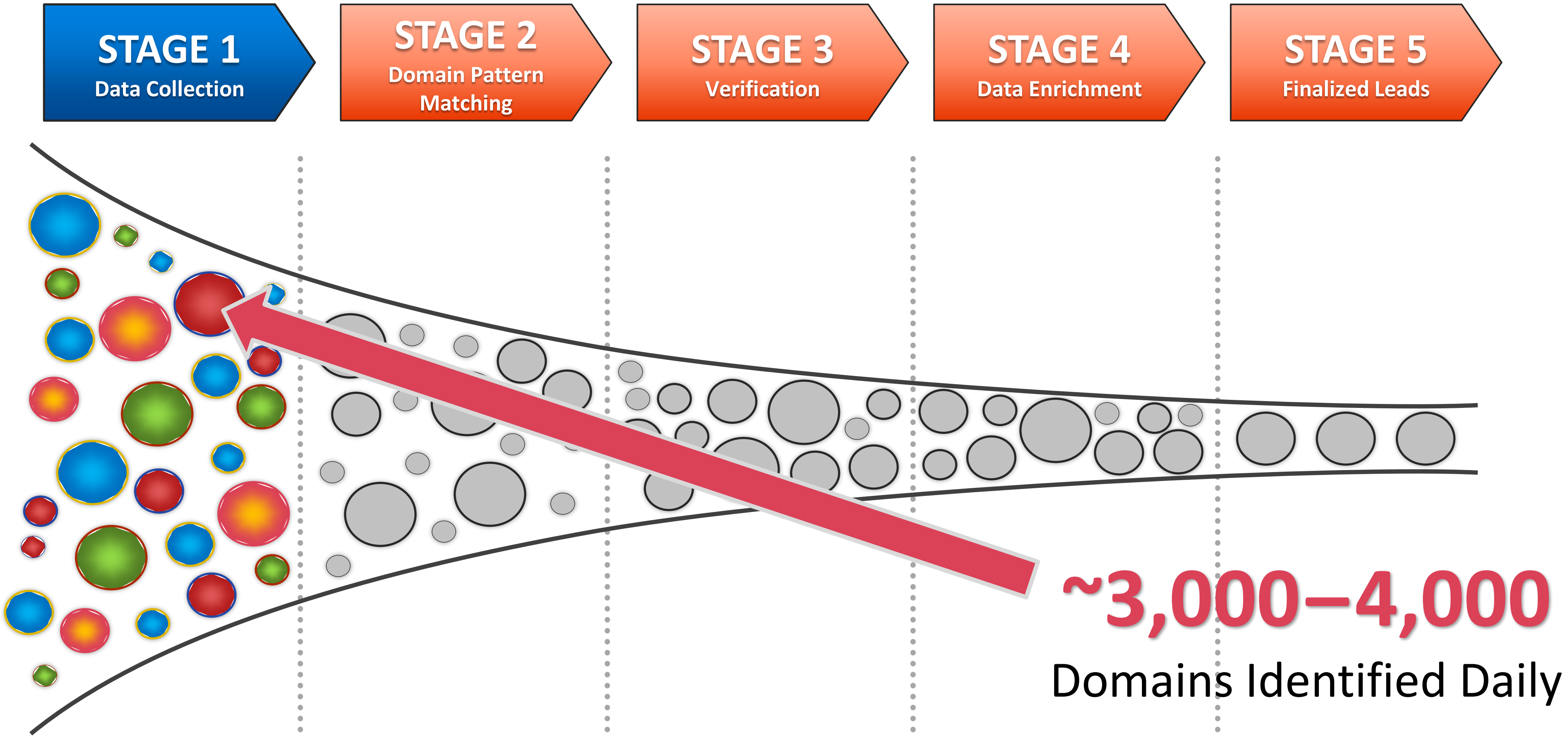
STAGE 3 Verification

STAGE 4 Data Enrichment

STAGE 5 Finalized Leads

Domain Targeting Workflow

Stage 1 – Data Collection



~3,000–4,000

Domains Identified Daily

Pandemic
Pfizer
cure
Moderna
SEARCHING.....

Domain Targeting Workflow
Stage 1 – Data Collection

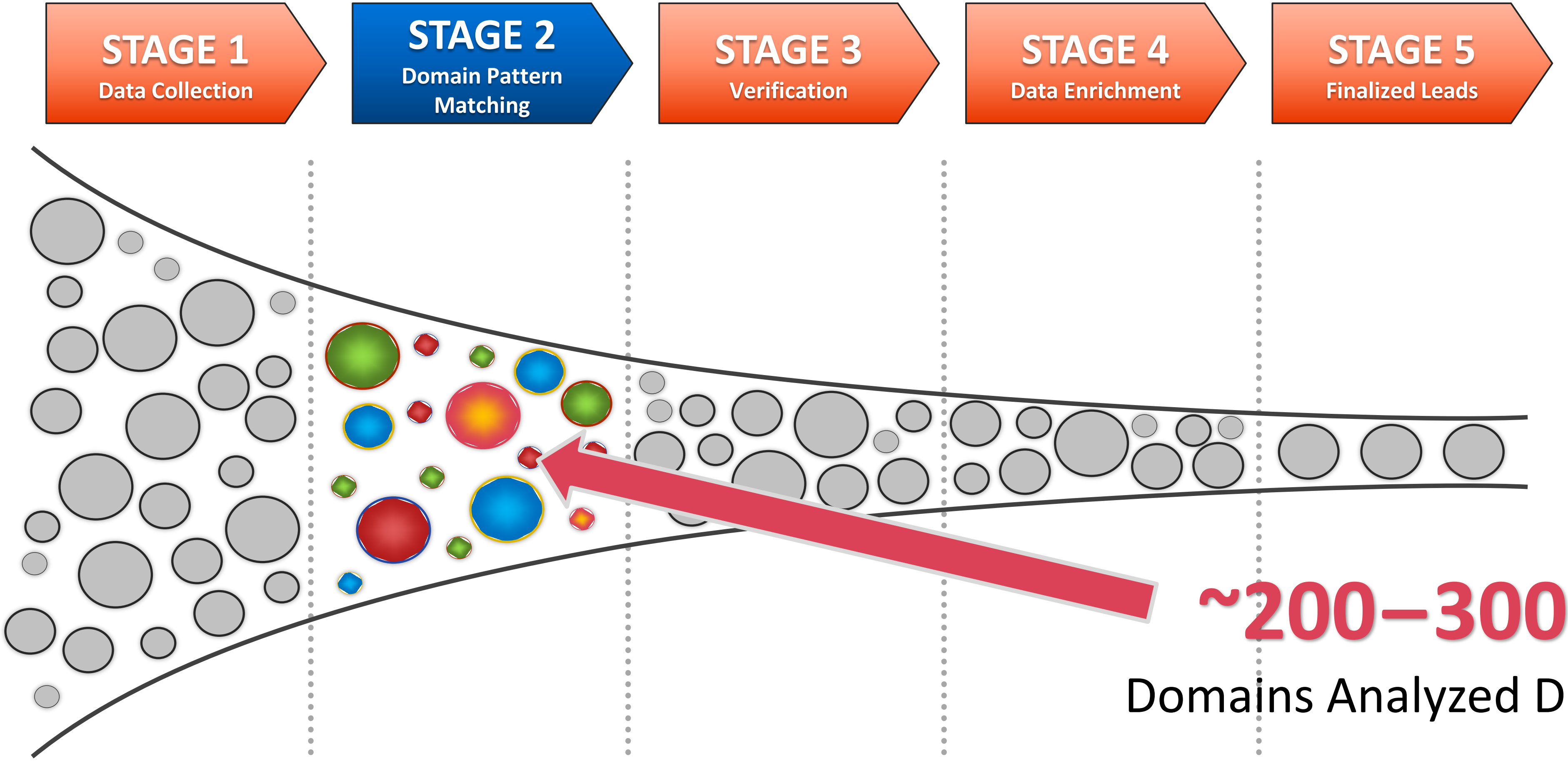
- C3's obtains lists of generated d d its subscription platforms:
  - Examine domain cert in r ime.
    Domain certificates obtain (often self-generated) and can be populat udulent information.
  - Publish "unvetted" do ains.
    It is extremely easy to purchase domains in bulk and have a site up and running within hours.
- HSI monitors these feeds and reports.

CERTSTREAM

ALIEN VAULT
An AT&T Company

Domain Targeting Workflow

Stage 2 – Domain Name Matching



~200–300

Domains Analyzed Daily

LOOKINGGLASS

Domain Targetin w
Stage 2 – Doma ching

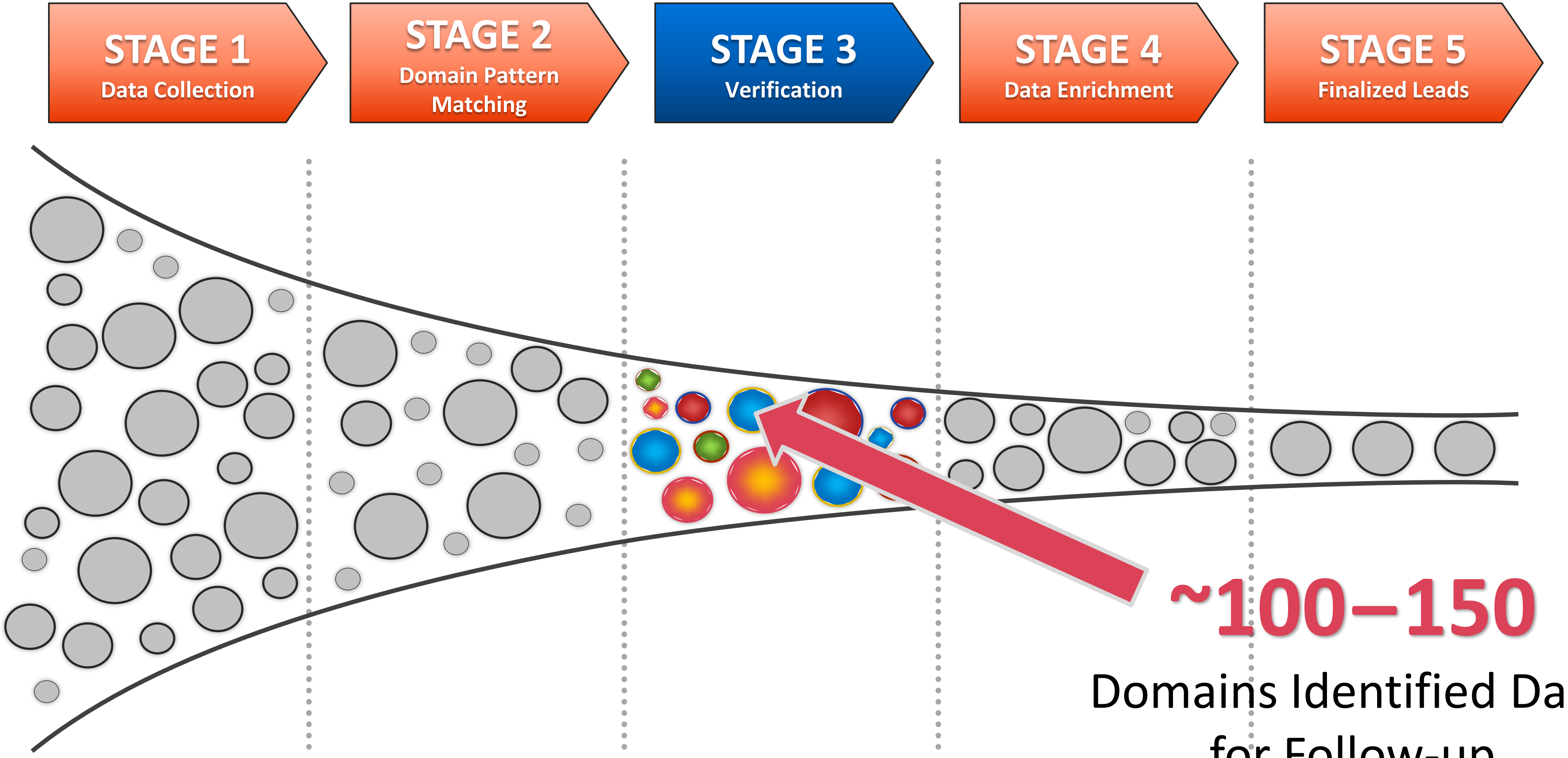
cure vaccine
kit shop test
Chloroquine

- Based on Stage 1 hen:
  - Automated searches for keywords to identify pote ed to COVID-19 fraud activities.
  - Performs manual verification of identified domains.

- In addition, HSI examines secondary marketplaces for additional sellers.

Domain Targeting Workflow

Stage 3 – Verification



~100–150

Domains Identified Daily
for Follow-up

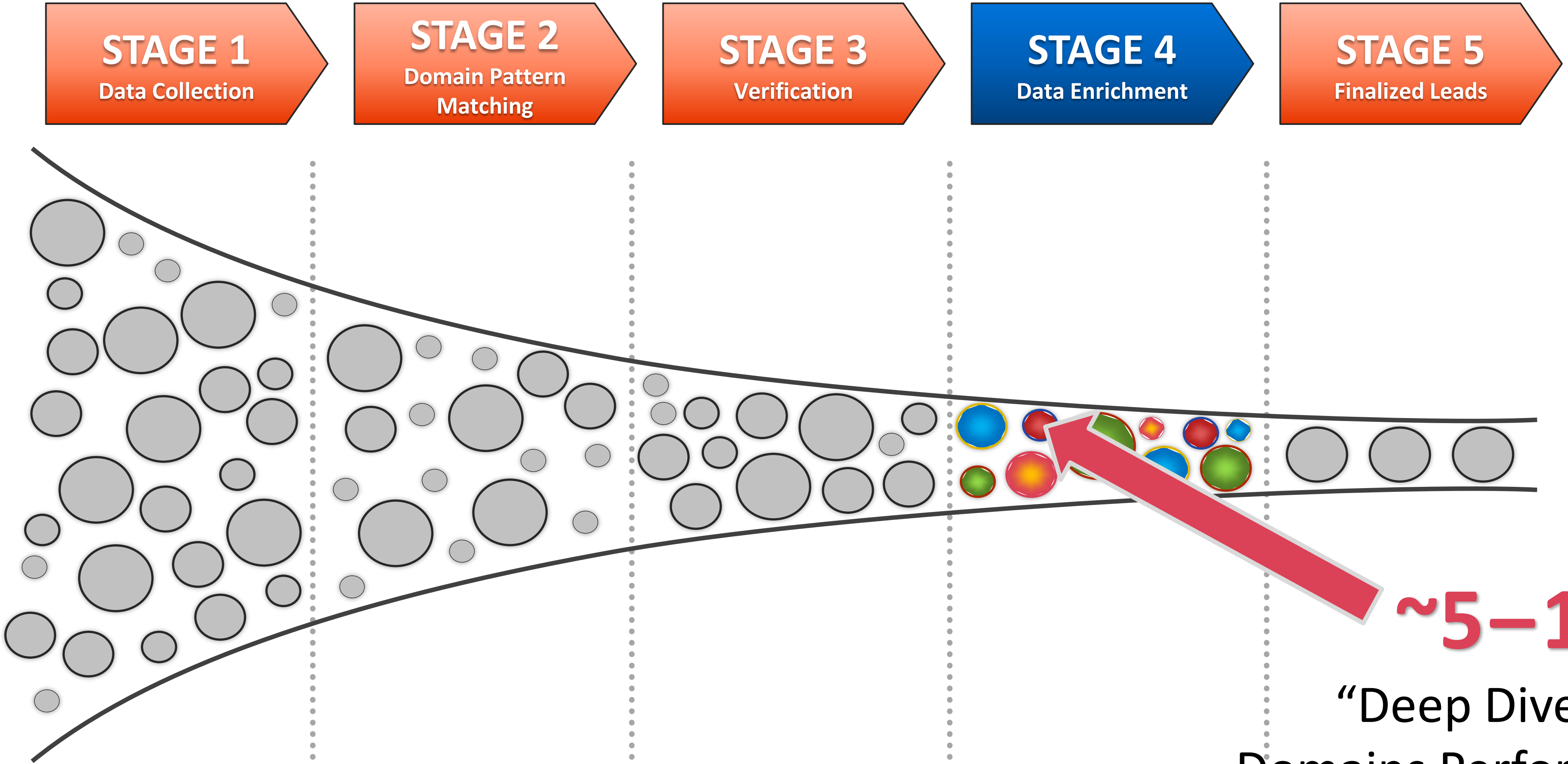
Domain Targeting Workflow
Stage 3 – Verification

VIRUSTOTAL

urlscan.io

- Identified domains from S[illegible]ged by HSI for follow-up, and a manual assessment is performed. C3:
  - Examines domains to see if they are serving malware and viruses to visitors.
  - Identifies the hosting platform and country of suspicious domains. Domains must be U.S.-based and consist of an active e-commerce website to be escalated to Stage 4.

Domain Targeting Workflow
Stage 4 – Data Enrichment



~5–10

"Deep Dives" on Domains Performed Daily

LOOKINGGLASS

Domain Targeting Workflow
Stage 4 – Data Enrichment

- C3's subscription platforms scrub sites of investigative value.
- C3 contacts its IC lert them of sites to suspend.

LOOKINGGLASS

SHADOWDRAGON

CROSSLINK™

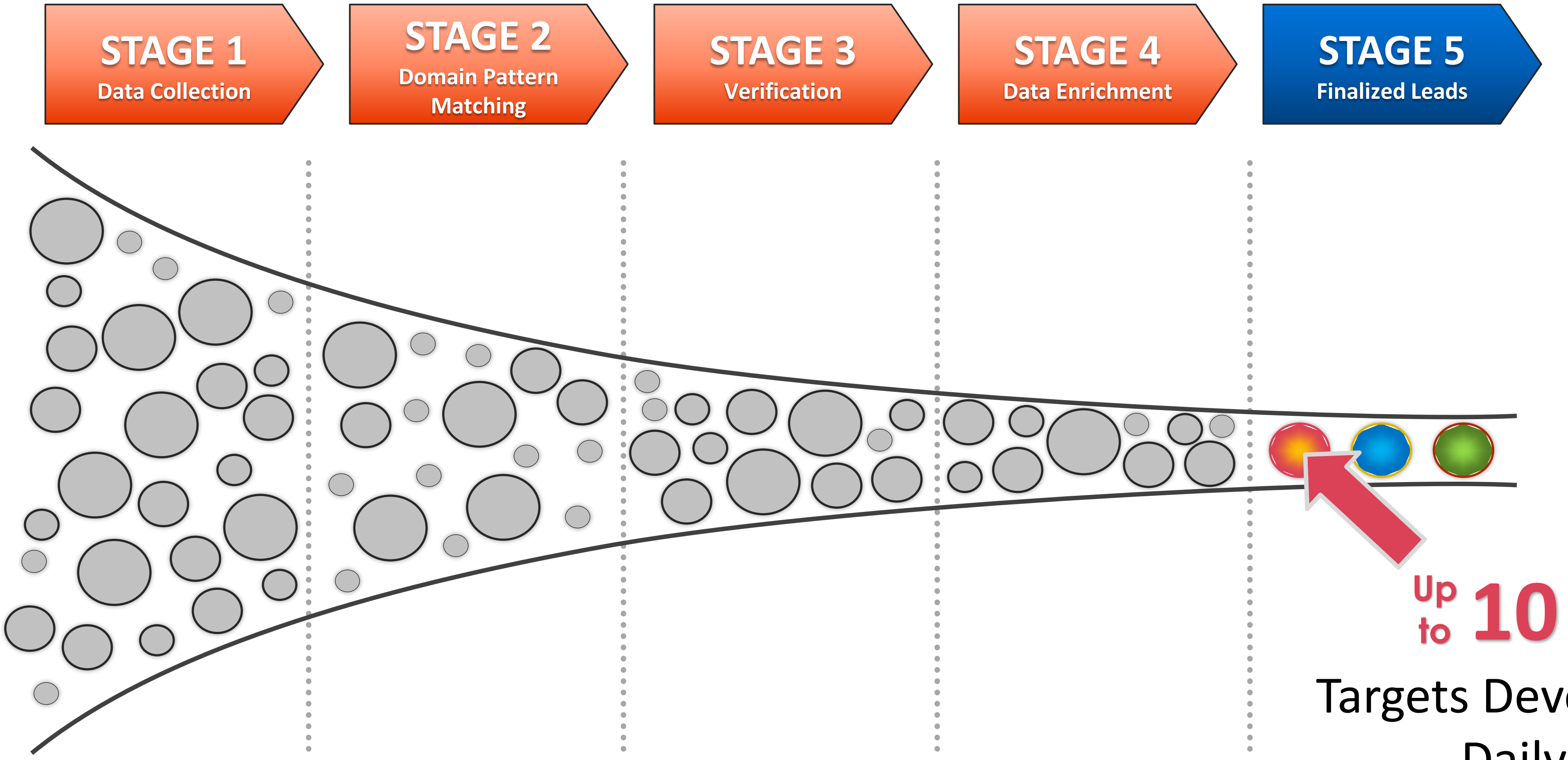
RISKIQ

urlscan.io

SHODAN

Recorded Future

Domain Targeting Workflow
Stage 5 – Finalize Leads



Up to 10

Targets Developed Daily

Domain Targeting Workflow
Stage 5 – Finalize Leads

- HSI sends C3 leads identified for dissemination.
  - C3 passes leads to HSI field offices based on their AOR.
  - Leads include identified person(s) and/or business(es).
- HSI examines ATS cargo import data along with 3rd party information database checks (e.g., CLEAR, Dept. of Licensing) for information related to shipments with suspicious origins or labels.
- The National Cyber-Forensics & Training Alliance (NCFTA) deconflicts with other agencies.

Disruption & Leads

Once a suspect domain is identified, C3 puts that domain down one or two paths for disruption and lead distribution.

- Referred to domain registrar for disruption
- Develop and distribute a lead package for a field office
- Both can run concurrent due to public safety and to prevent further victimization
- 108 leads sent to the field

- 123 cyber investigations
- 378 domains disrupted
- 6 criminal website seizures
- Numerous arrests

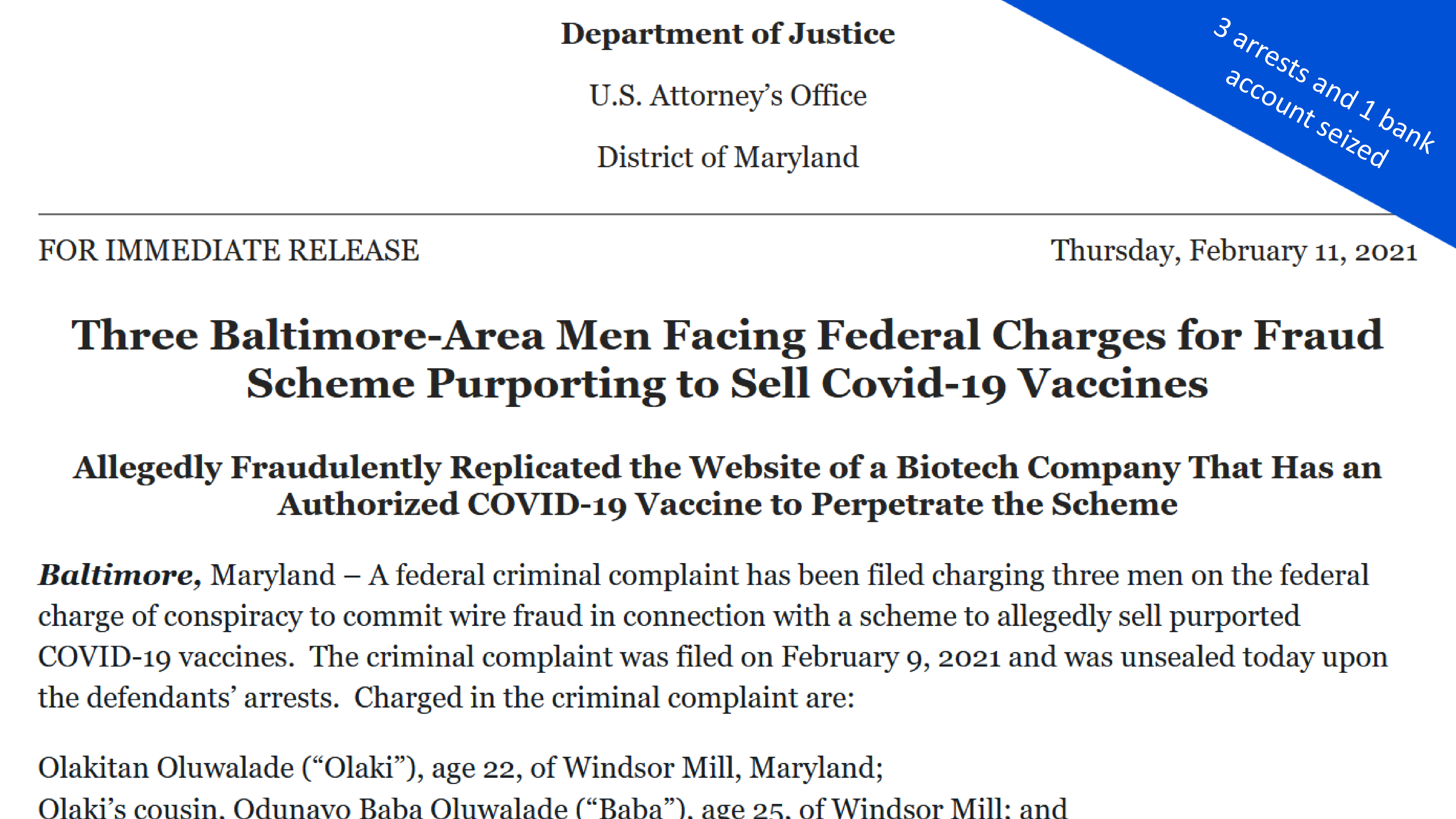
Operation Stolen Promise Cyber Operation

Began in April 2020, daily proactive operation targeting cyber criminals who use publicly reachable websites to exploit the pandemic.

- Cyber-Enabled
  - Financial fraud, supply fraud, miracle cures/vaccines, counterfeit COVID-19 supplies
- Cyber-Dependent
  - Malicious websites
  - Phishing/spoof websites

- Cyber Threat Actors
  - Darknet markets
  - Stolen PII, Cybercrime kits
- 220,000+ Domains identified
- 76,000+ Domains analyzed

LOOKINGGLASS



Department of Justice

U.S. Attorney's Office

District of Maryland

FOR IMMEDIATE RELEASE Thursday, February 11, 2021

Three Baltimore-Area Men Facing Federal Charges for Fraud Scheme Purporting to Sell Covid-19 Vaccines

Allegedly Fraudulently Replicated the Website of a Biotech Company That Has an Authorized COVID-19 Vaccine to Perpetrate the Scheme

Baltimore, Maryland – A federal criminal complaint has been filed charging three men on the federal charge of conspiracy to commit wire fraud in connection with a scheme to allegedly sell purported COVID-19 vaccines. The criminal complaint was filed on February 9, 2021 and was unsealed today upon the defendants' arrests. Charged in the criminal complaint are:

Olakitan Oluwalade ("Olaki"), age 22, of Windsor Mill, Maryland;
Olaki's cousin, Odunayo Baba Oluwalade ("Baba"), age 25, of Windsor Mill; and

3 arrests and 1 bank account seized

Apply What You Have Learned Today (1 of 2)

- Next week you should:
  - Identify local resources (i.e., FBI field office, DHS CISA regional office) and find out the process for obtaining technical and investigative support
  - Understand current cybersecurity capabilities in your toolbox:
    - Sink-holing
    - Newly registered domain feed
  - Engage cyber/fraud counterparts within your organization to understand internal resources and capabilities

Apply What You Have Learned Today (2 of 2)

- In the first three months following this presentation you should:
  - Identify words/phrases associated with your organization or current events that could be used for cybercrime and fraud
  - Define automated process for filtering newly registered domains based on keywords/phrases
  - Explore automated enrichment options to filter list of domains to investigate
- Within six months you should:
  - Track initial investigations of enriched domains to calculate impact
  - Stand up a small working group to review incidents and gather information that can support improved cyber and fraud defenses
- Leverage operations for future events (i.e., Russian/Ukraine conflict)