CROWDSTRIKE

CYBERSECURITY LESSONS LEARNED

Understanding the K-12 Threat Landscape

Jeff Worthington

Quick Bio

JEFF WORTHINGTON

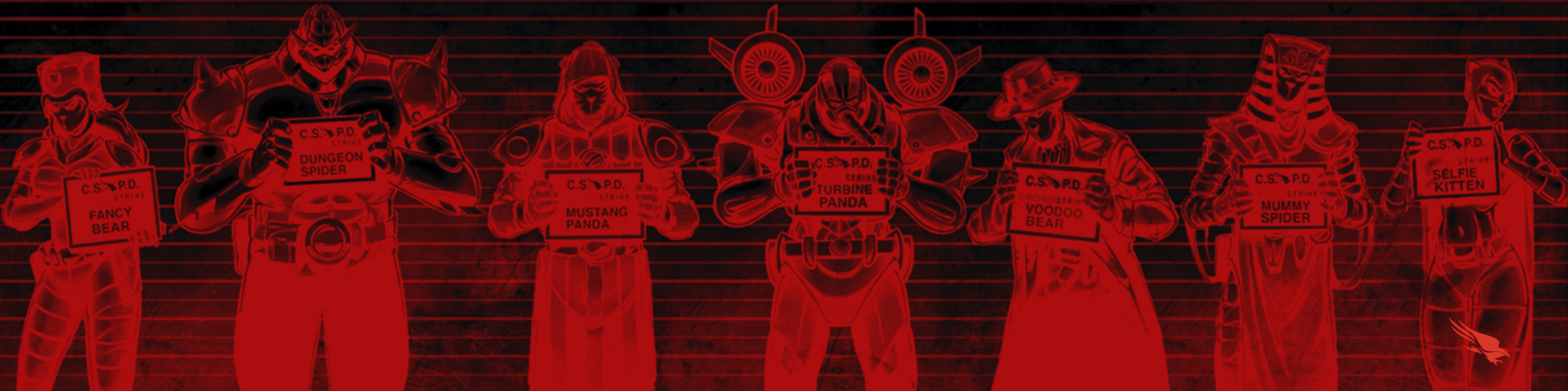
EXECUTIVE STRATEGIST
CROWDSTRIKE INDUSTRY BUSINESS UNIT

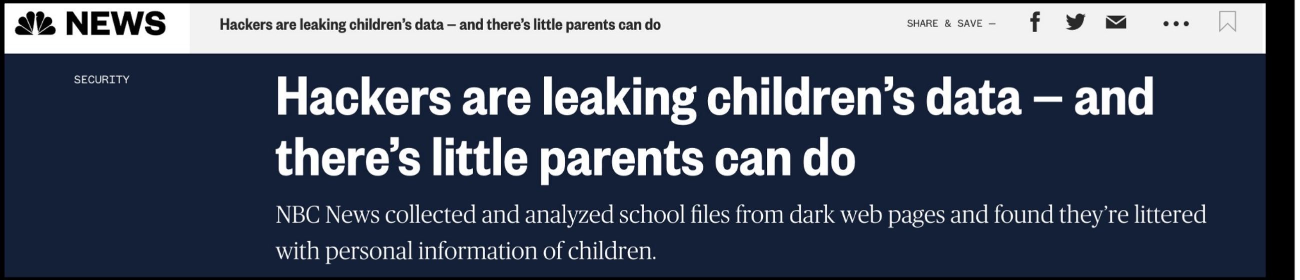
Jeff Worthington is a member of a unit within CrowdStrike that provides strategic advisory services related to enterprise cybersecurity solutions. Jeff has spent 30 years in the Department of Defense running IT programs and leading our Nation's Service Members in Joint and Special Operations Units as well as two White House Administrations.

Just prior to joining CrowdStrike, he most recently served as the CIO for Joint Special Operations Command at Fort Bragg, NC.

AGENDA

- SECURITY THEMES
- THE ADVERSARY OPERATIONS LIFECYCLE
- E-CRIME REVIEW
- THE WAY FORWARD



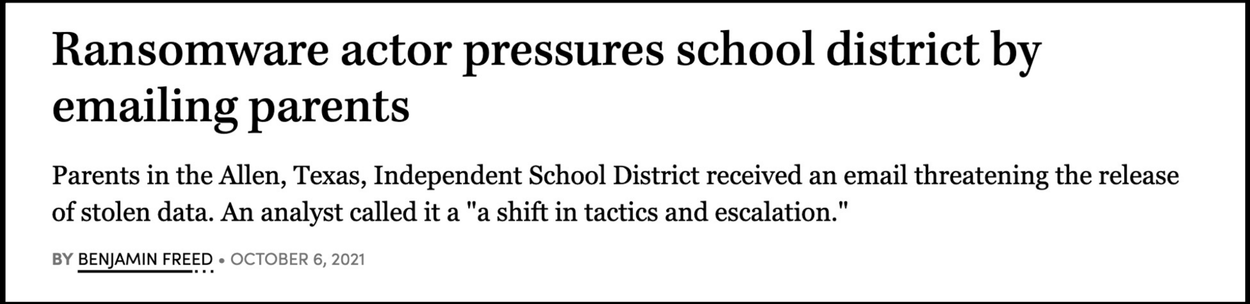


NBC NEWS | Hackers are leaking children's data – and there's little parents can do | SHARE & SAVE –

SECURITY

Hackers are leaking children's data – and there's little parents can do

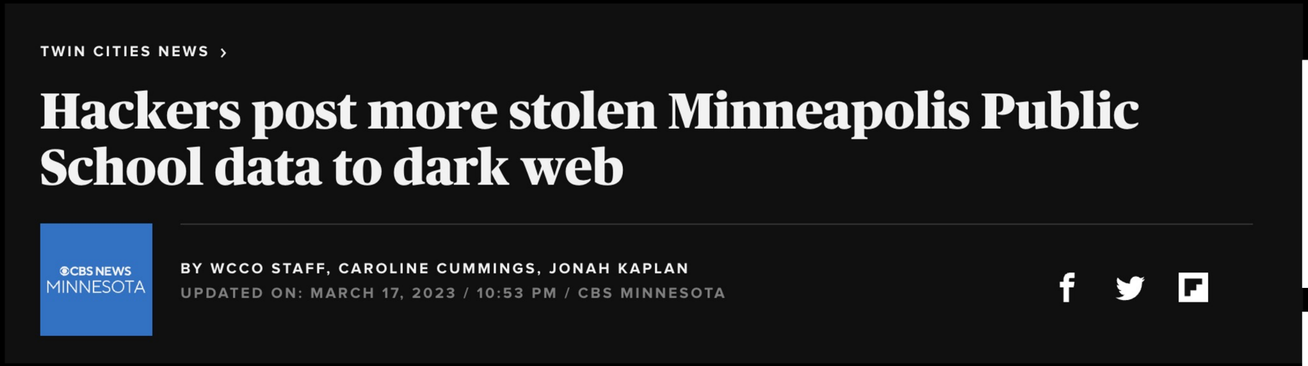
NBC News collected and analyzed school files from dark web pages and found they're littered with personal information of children.



Ransomware actor pressures school district by emailing parents

Parents in the Allen, Texas, Independent School District received an email threatening the release of stolen data. An analyst called it a "a shift in tactics and escalation."

BY BENJAMIN FREED • OCTOBER 6, 2021



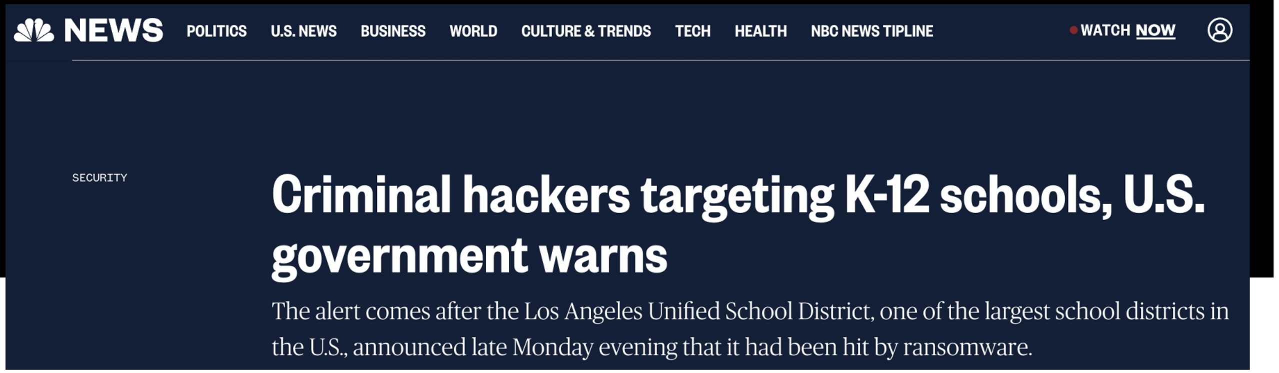
TWIN CITIES NEWS ›

Hackers post more stolen Minneapolis Public School data to dark web

CBS NEWS MINNESOTA

BY WCCO STAFF, CAROLINE CUMMINGS, JONAH KAPLAN

UPDATED ON: MARCH 17, 2023 / 10:53 PM / CBS MINNESOTA

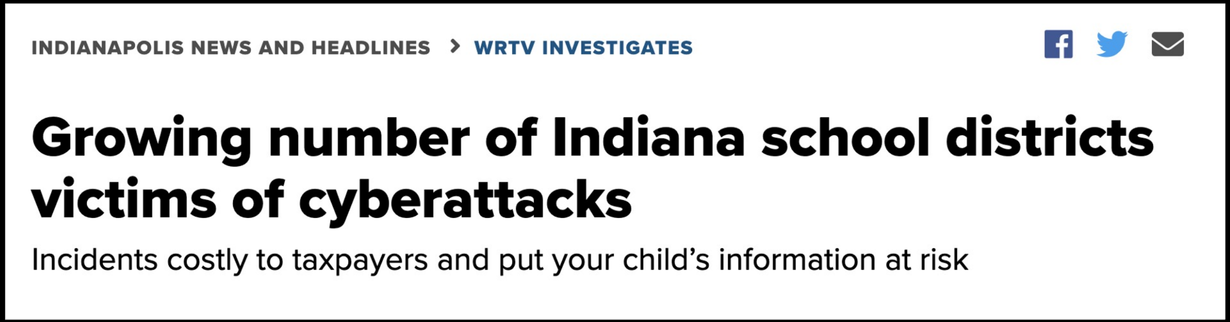


NBC NEWS | POLITICS | U.S. NEWS | BUSINESS | WORLD | CULTURE & TRENDS | TECH | HEALTH | NBC NEWS TIPLINE | WATCH NOW

SECURITY

Criminal hackers targeting K-12 schools, U.S. government warns

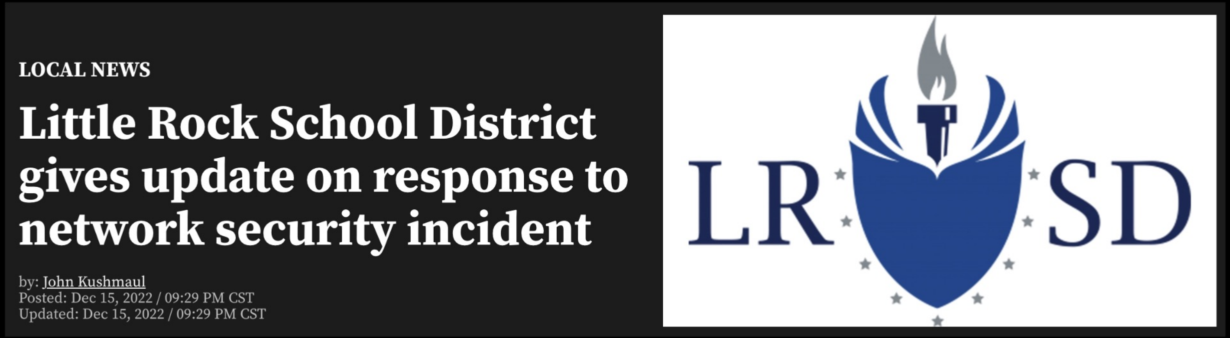
The alert comes after the Los Angeles Unified School District, one of the largest school districts in the U.S., announced late Monday evening that it had been hit by ransomware.



INDIANAPOLIS NEWS AND HEADLINES › WRTV INVESTIGATES

Growing number of Indiana school districts victims of cyberattacks

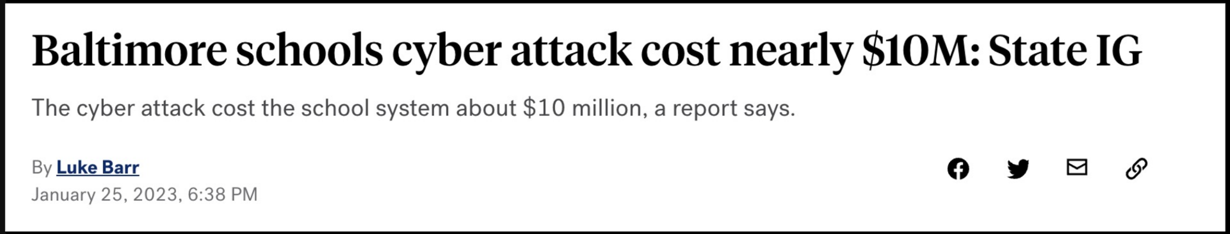
Incidents costly to taxpayers and put your child's information at risk



LOCAL NEWS

Little Rock School District gives update on response to network security incident

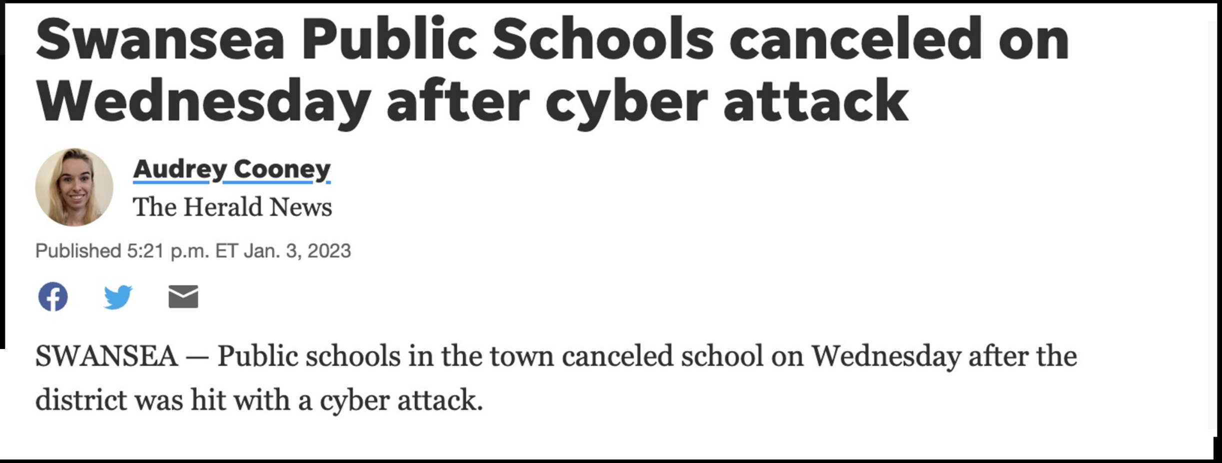
by: John Kushmaul
Posted: Dec 15, 2022 / 09:29 PM CST
Updated: Dec 15, 2022 / 09:29 PM CST



Baltimore schools cyber attack cost nearly $10M: State IG

The cyber attack cost the school system about $10 million, a report says.

By Luke Barr
January 25, 2023, 6:38 PM



Swansea Public Schools canceled on Wednesday after cyber attack

Audrey Cooney
The Herald News

Published 5:21 p.m. ET Jan. 3, 2023

SWANSEA — Public schools in the town canceled school on Wednesday after the district was hit with a cyber attack.

Today's Security Themes

Attack Sophistication

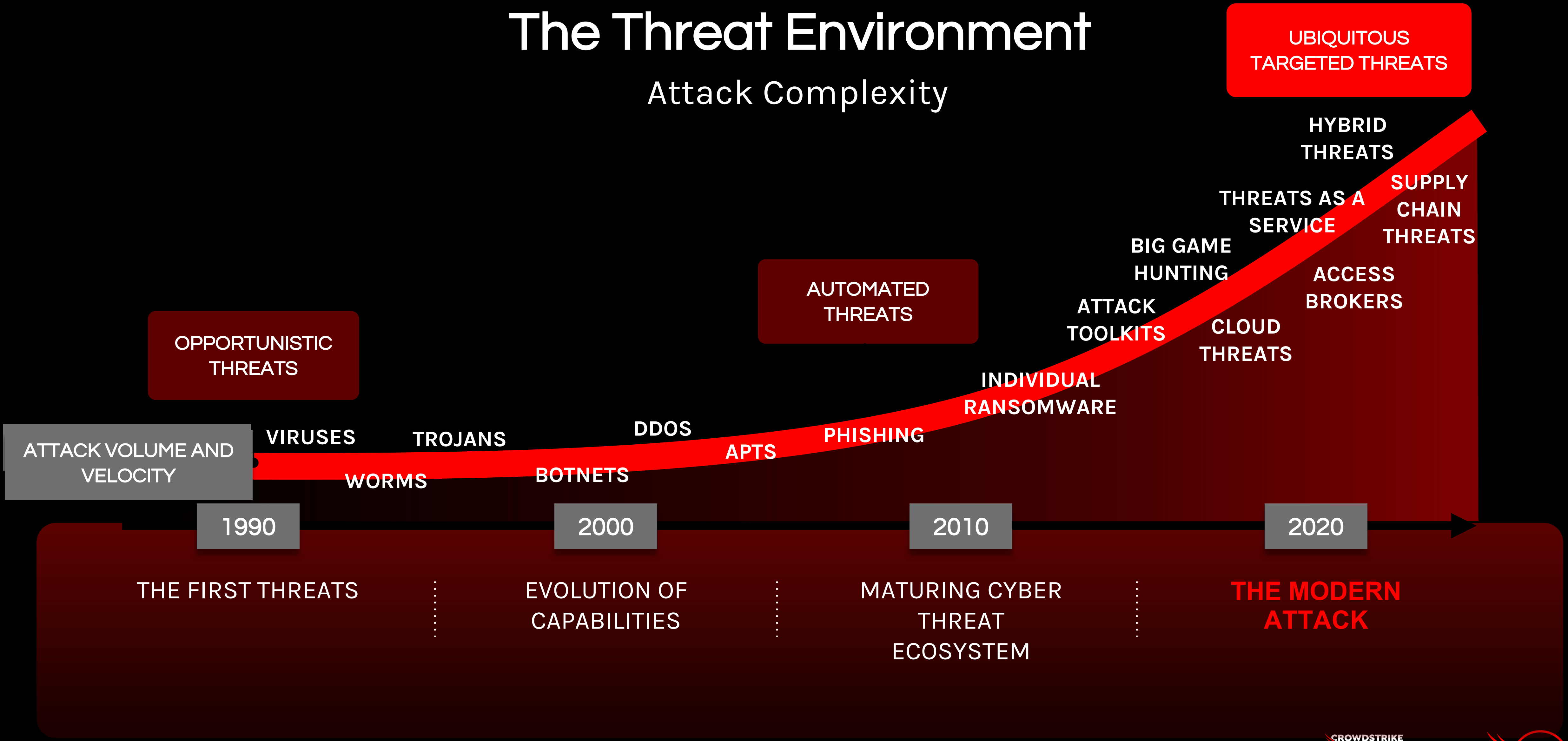
Innovation & Simplification

Skill Shortages

CROWDSTRIKE

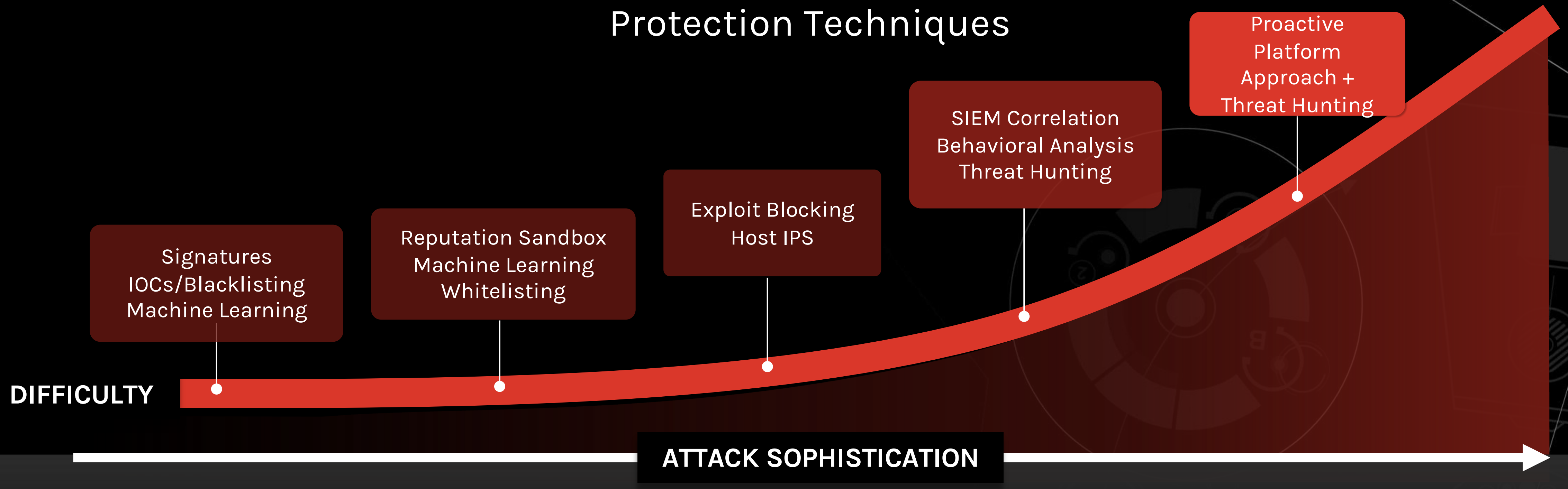
The Threat Environment

Attack Complexity



The Threat Environment

Protection Techniques



Signatures
IOCs/Blacklisting
Machine Learning

Reputation Sandbox
Machine Learning
Whitelisting

Exploit Blocking
Host IPS

SIEM Correlation
Behavioral Analysis
Threat Hunting

Proactive
Platform
Approach +
Threat Hunting

DIFFICULTY

ATTACK SOPHISTICATION

FILE BASED MALWARE

- Malware
- Zero-Day Malware

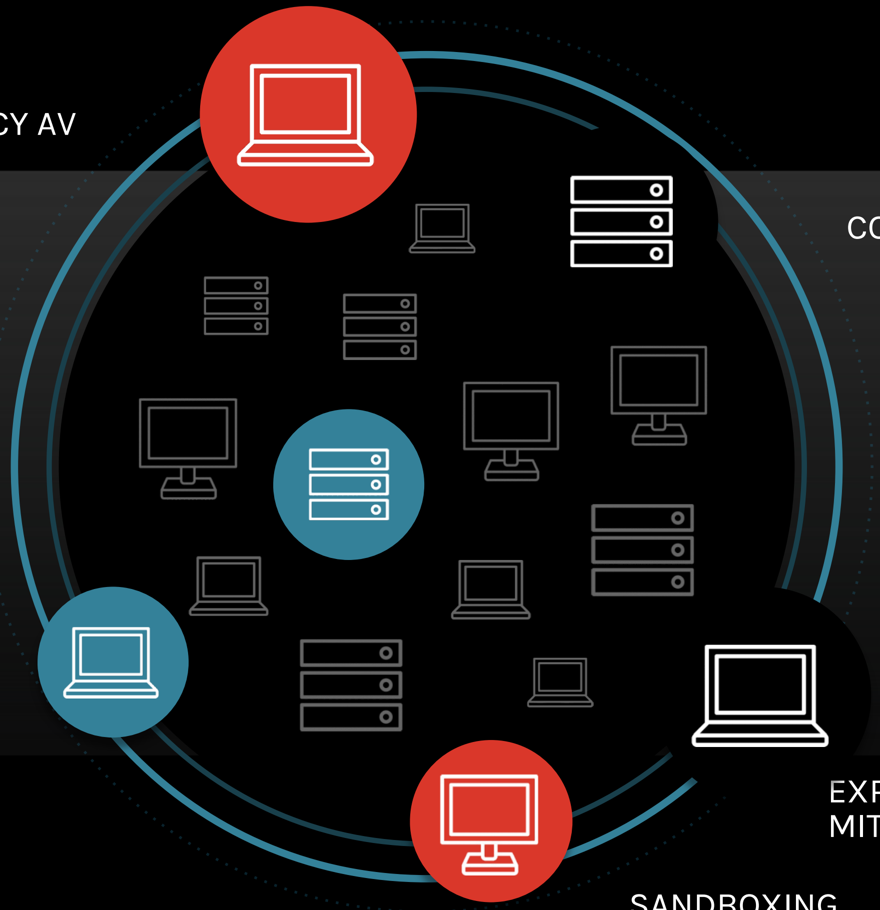
FILELESS AND EXPLOITS

- Exploitation of vulnerabilities
- Zero-Day Malware
- Credential Theft

LIVE ATTACKER/INSIDER

- Living off the land
- Hands-on keyboard

Solution Complexity



LEGACY AV

APPLICATION WHITELISTING

FORENSICS

VULNERABILITY ASSESSMENT

MOBILE + TABLETS

CONTAINERS

DEVICE CONTROL

ENDPOINT DETECTION & RESPONSE

SECURITY HYGIENE

EXPLOIT MITIGATION

SANDBOXING

COSTLY TO DEPLOY

DIFFICULT TO MAINTAIN

POOR USER EXPERIENCE

MINIMAL SECURITY EFFECTIVENESS

The Adversary

What’s Changed

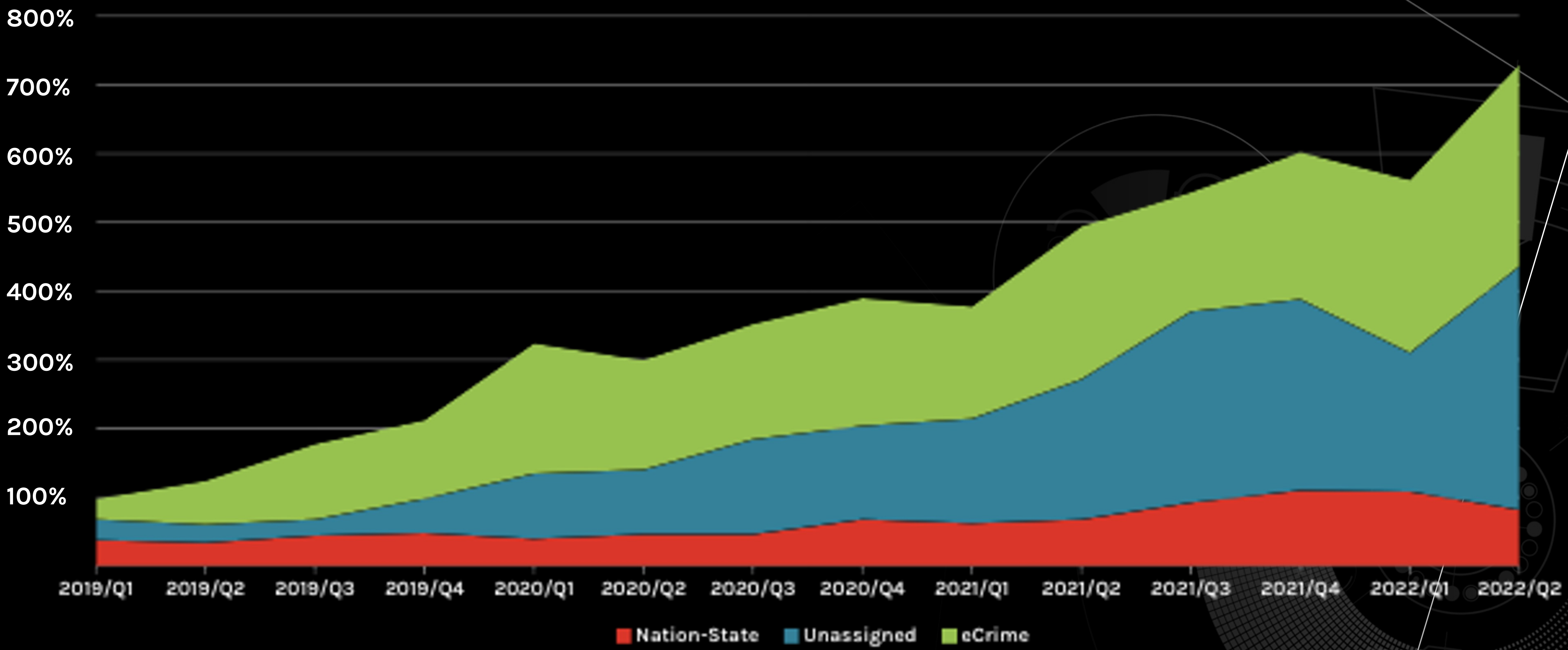
THREE PRIMARY METRICS FOR MEASURING THE ADVERSARY

Volume

Speed

Sophistication

CrowdStrike Distinct & Sophisticated Intrusion Telemetry



CROWDSTRIKE

eCrime Adversary Average Breakout Time

2018

9H 42M

2022

1H 24M

CROWDSTRIKE

[redacted]

2023 Global Threat Report
Top Findings

Top industries targeted by interactive intrusion activity included tech, telecom, healthcare, manufacturing and academia

1 hr and 24 minutes, average eCrime adversary breakout time

200+ adversaries tracked, **33 new**

112% increase in access broker activity

50% increase in interactive intrusion, **hands on keyboard** activity

71% of attacks were **malware-free**

Global Threat Landscape

CRIMINAL

- Alchemist Spider
- Aviator Spider
- Bitwise Spider
- Carbon Spider
- Chariot Spider
- Clockwork Spider
- Cyborg Spider
- Doppel Spider
- Feral Spider
- Graceful Spider
- Hidden Spider
- Hive Spider
- Indrik Spider
- Knockout Spider
- Lunar Spider
- Mallard Spider
- Mummy Spider
- Narwhal Spider
- Night Spider
- Outbreak Spider
- Outlaw Spider
- Percussion Spider
- Pinchy Spider
- Prophet Spider
- Salty Spider
- Samba Spider
- Scully Spider
- Slippy Spider

CHINA

- Aquatic Panda
- Circuit Panda
- Emissary Panda
- Karma Panda
- Kryptonite Panda
- Mustang Panda
- Octane Panda
- Pirate Panda
- Puzzle Panda
- Shattered Panda
- Sunrise Panda
- Vixen Panda
- Wicked Panda

NORTH KOREA

- Labyrinth Chollima
- Ricochet Chollima
- Silent Chollima
- Stardust Chollima
- Velvet Chollima

IRAN

- Charming Kitten
- Chrono Kitten
- Haywire Kitten
- Imperial Kitten
- Nemesis Kitten
- Pioneer Kitten
- Refined Kitten
- Spectral Kitten
- Static Kitten
- Tracer Kitten

INDIA

- Hazy Tiger
- Quilted Tiger
- Razor Tiger
- Viceroy Tiger

RUSSIA

- Berserk Bear
- Cozy Bear
- Ember Bear
- Fancy Bear
- Primitive Bear
- Venomous Bear
- Voodoo Bear

PAKISTAN

- **Mythic Leopard**
- **Fringe Leopard**

VIETNAM

- Ocean Buffalo

SOUTH KOREA

- Shadow Crane

SYRIA

- Deadeye Hawk

COLOMBIA

- Galactic Ocelot

TURKEY

- Cosmic Wolf

ACTIVIST

- Curious Jackal
- Frontline Jackal
- Intrepid Jackal
- Partisan Jackal
- Regal Jackal
- Renegade Jackal

CROWDSTRIKE ADVERSARY UNIVERSE WORLD TOUR 22

Education Sector - Adversary Motivations

Nation State

7

eCrime

13

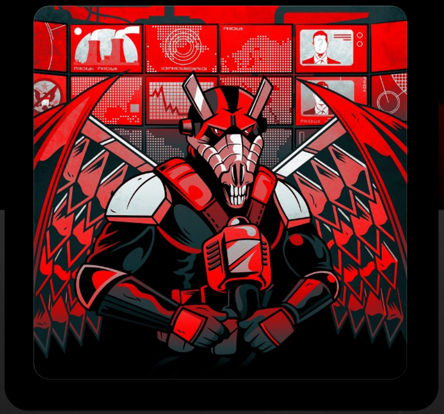
Hacktivist

2

EDUCATION SECTOR -- NATION STATE TRENDS

CHINA

1



DPRK (North Korea)

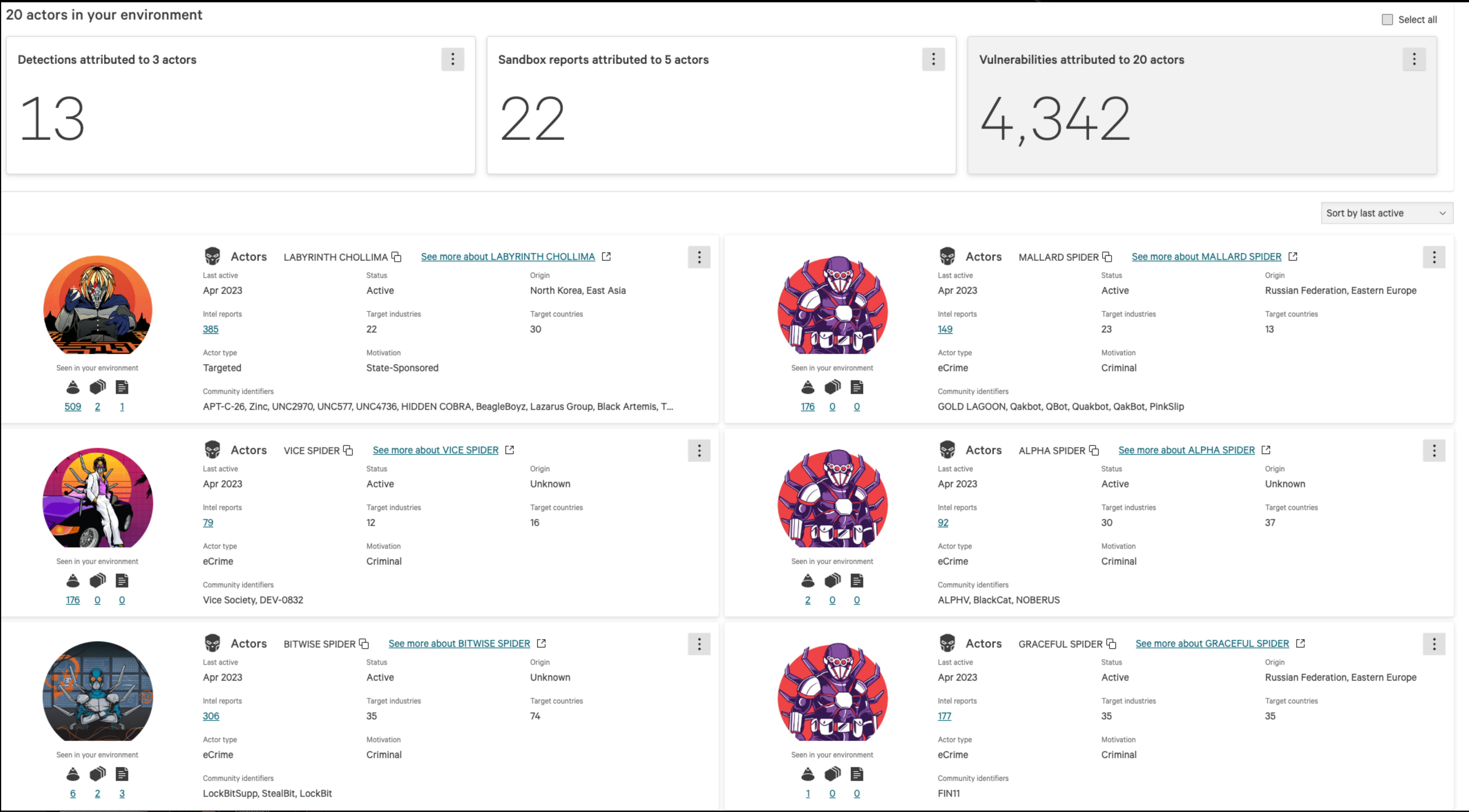
4

RUSSIA

2

IRAN

0



20 actors in your environment

□ Select all

Detections attributed to 3 actors

13

Sandbox reports attributed to 5 actors

22

Vulnerabilities attributed to 20 actors

4,342

Sort by last active

Actors LABYRINTH CHOLLIMA See more about LABYRINTH CHOLLIMA

Last active: Apr 2023
Status: Active
Origin: North Korea, East Asia
Intel reports: 385
Target industries: 22
Target countries: 30
Actor type: Targeted
Motivation: State-Sponsored
Community identifiers: APT-C-26, Zinc, UNC2970, UNC577, UNC4736, HIDDEN COBRA, BeagleBoyz, Lazarus Group, Black Artemis, T...

Seen in your environment: 509 2 1

Actors MALLARD SPIDER See more about MALLARD SPIDER

Last active: Apr 2023
Status: Active
Origin: Russian Federation, Eastern Europe
Intel reports: 149
Target industries: 23
Target countries: 13
Actor type: eCrime
Motivation: Criminal
Community identifiers: GOLD LAGOON, Qakbot, QBot, Quakbot, QakBot, PinkSlip

Seen in your environment: 176 0 0

Actors VICE SPIDER See more about VICE SPIDER

Last active: Apr 2023
Status: Active
Origin: Unknown
Intel reports: 79
Target industries: 12
Target countries: 16
Actor type: eCrime
Motivation: Criminal
Community identifiers: Vice Society, DEV-0832

Seen in your environment: 176 0 0

Actors ALPHA SPIDER See more about ALPHA SPIDER

Last active: Apr 2023
Status: Active
Origin: Unknown
Intel reports: 92
Target industries: 30
Target countries: 37
Actor type: eCrime
Motivation: Criminal
Community identifiers: ALPHV, BlackCat, NOBERUS

Seen in your environment: 2 0 0

Actors BITWISE SPIDER See more about BITWISE SPIDER

Last active: Apr 2023
Status: Active
Origin: Unknown
Intel reports: 306
Target industries: 35
Target countries: 74
Actor type: eCrime
Motivation: Criminal
Community identifiers: LockBitSupp, StealBit, LockBit

Seen in your environment: 6 2 3

Actors GRACEFUL SPIDER See more about GRACEFUL SPIDER

Last active: Apr 2023
Status: Active
Origin: Russian Federation, Eastern Europe
Intel reports: 177
Target industries: 35
Target countries: 35
Actor type: eCrime
Motivation: Criminal
Community identifiers: FIN11

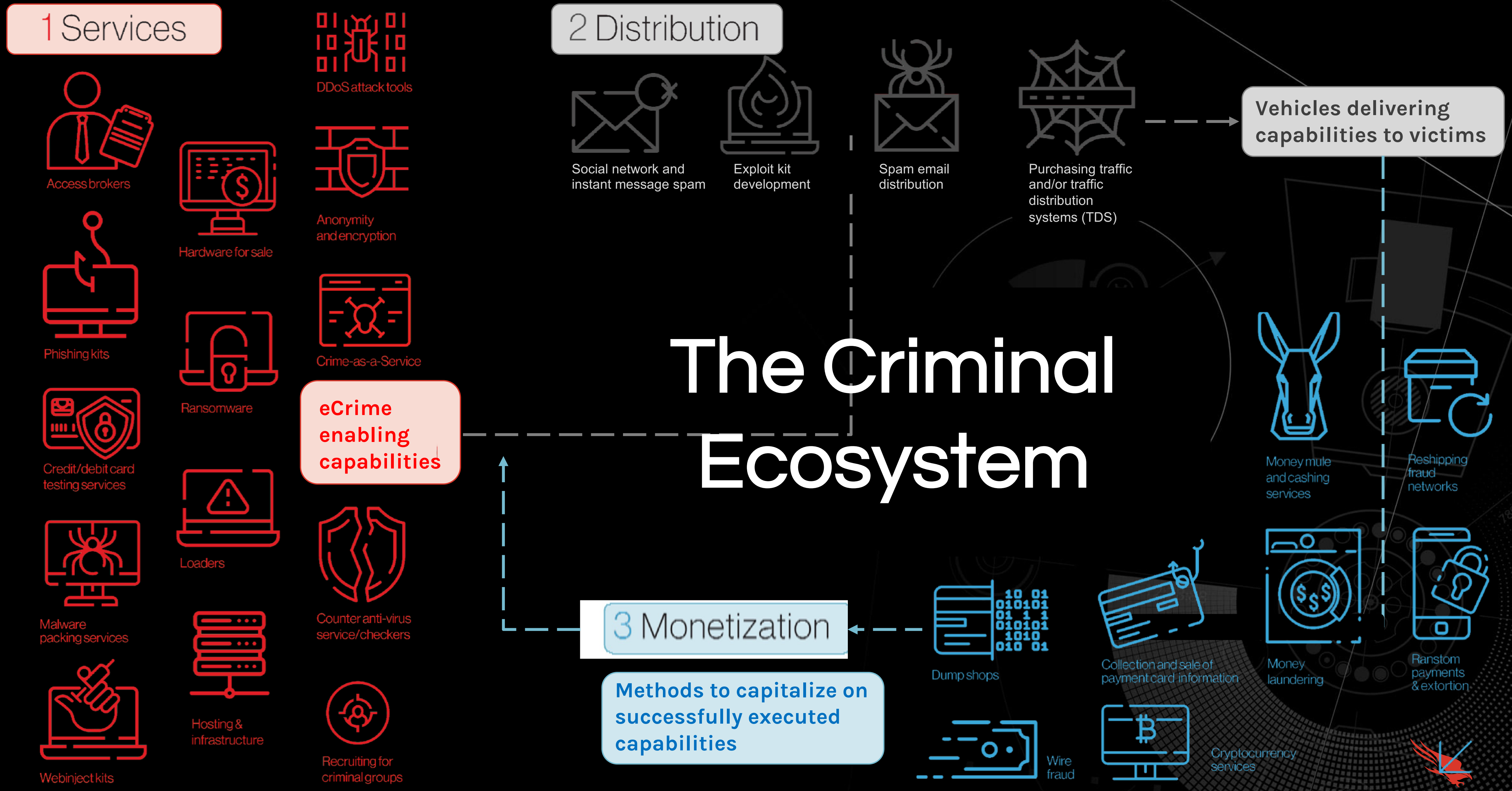
Seen in your environment: 1 0 0

The Adversary Operations Lifecycle

How Advanced Adversaries Engage in Operations

TLP AMBER

The Criminal Ecosystem



1 Services

Access brokers

Hardware for sale

DDoS attack tools

Anonymity and encryption

Phishing kits

Ransomware

Crime-as-a-Service

Credit/debit card testing services

Loaders

Malware packing services

Counter anti-virus service/checkers

Webinject kits

Hosting & infrastructure

Recruiting for criminal groups

eCrime enabling capabilities

2 Distribution

Social network and instant message spam

Exploit kit development

Spam email distribution

Purchasing traffic and/or traffic distribution systems (TDS)

Vehicles delivering capabilities to victims

3 Monetization

Methods to capitalize on successfully executed capabilities

Money mule and cashing services

Reshipping fraud networks

Dump shops

Collection and sale of payment card information

Money laundering

Ranstom payments & extortion

Wire fraud

Cryptocurrency services

The Adversary Operations Lifecycle

Access Operations

How Adversaries gain access

- VALID CREDENTIALS
- SUPPLY CHAIN COMPROMISE
- 0-DAY EXPLOITATION
- MFA BYPASS

Post Exploitation

How Adversaries remain stealthy

- LIVING OFF THE LAND
- RECONNAISSANCE
- PRIVILEGE ESCALATION

Target Environments

What Adversaries are attacking

- DOMAIN CONTROLLERS
- CLOUD WORKLOADS
- EMAIL & DATA SERVERS
- DOWNSTREAM ACCESS

Impact

- RANSOMWARE
- DATA LEAK
- DATA EXTORTION
- DATA EXFILTRATION

K-12 Specific Threats

Ransomware

Third Party Tools

Denial of Service

Access Operations

How Adversaries Gain Access

The Problem

"YOU DON'T HAVE A MALWARE PROBLEM. YOU HAVE AN ADVERSARY PROBLEM"

"Attackers don't break in, they log in."

Identity Threat Detection and Response is Crucial

80%

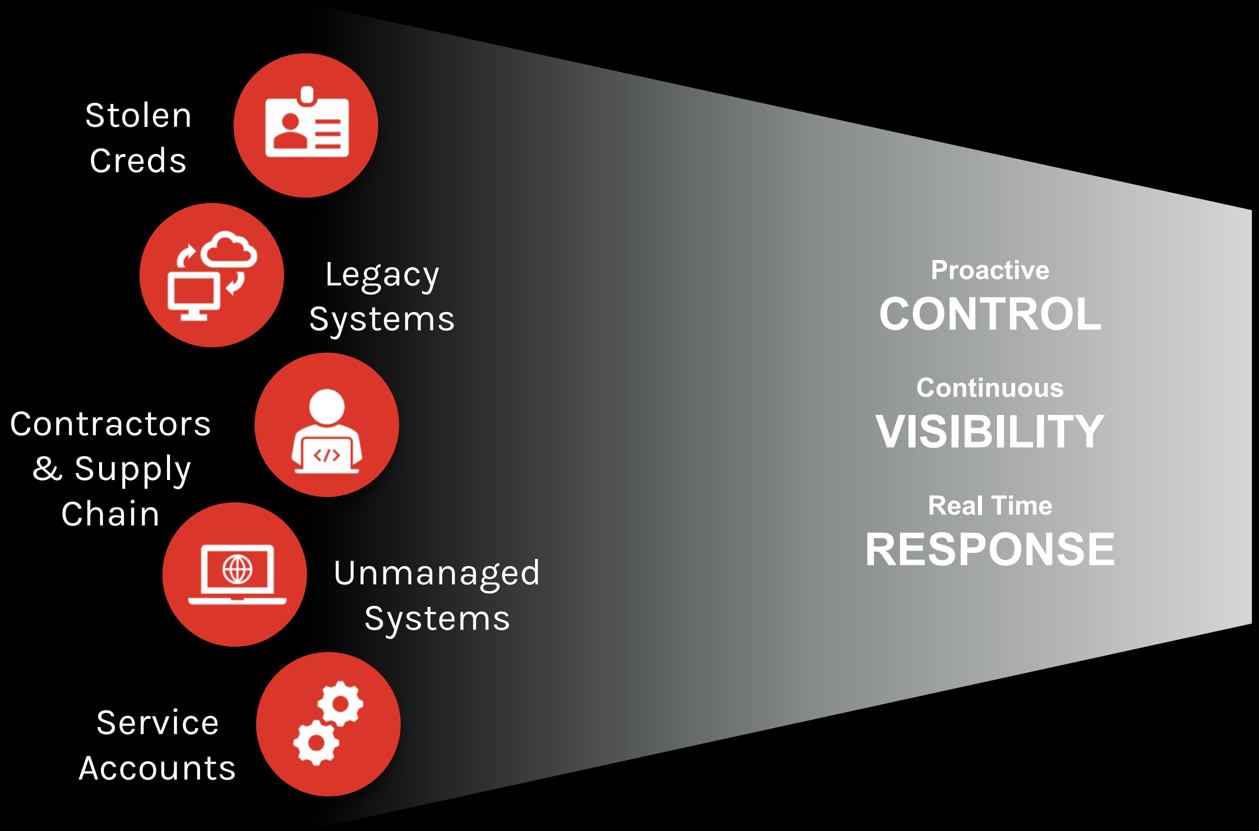
of data breaches have a connection to compromised privileged credentials

- Forrester Research

Breaches from stolen/compromised credentials took the longest to detect:

243 days

- IBM Cost of a Breach Report, 2022



Stolen Creds

Legacy Systems

Contractors & Supply Chain

Unmanaged Systems

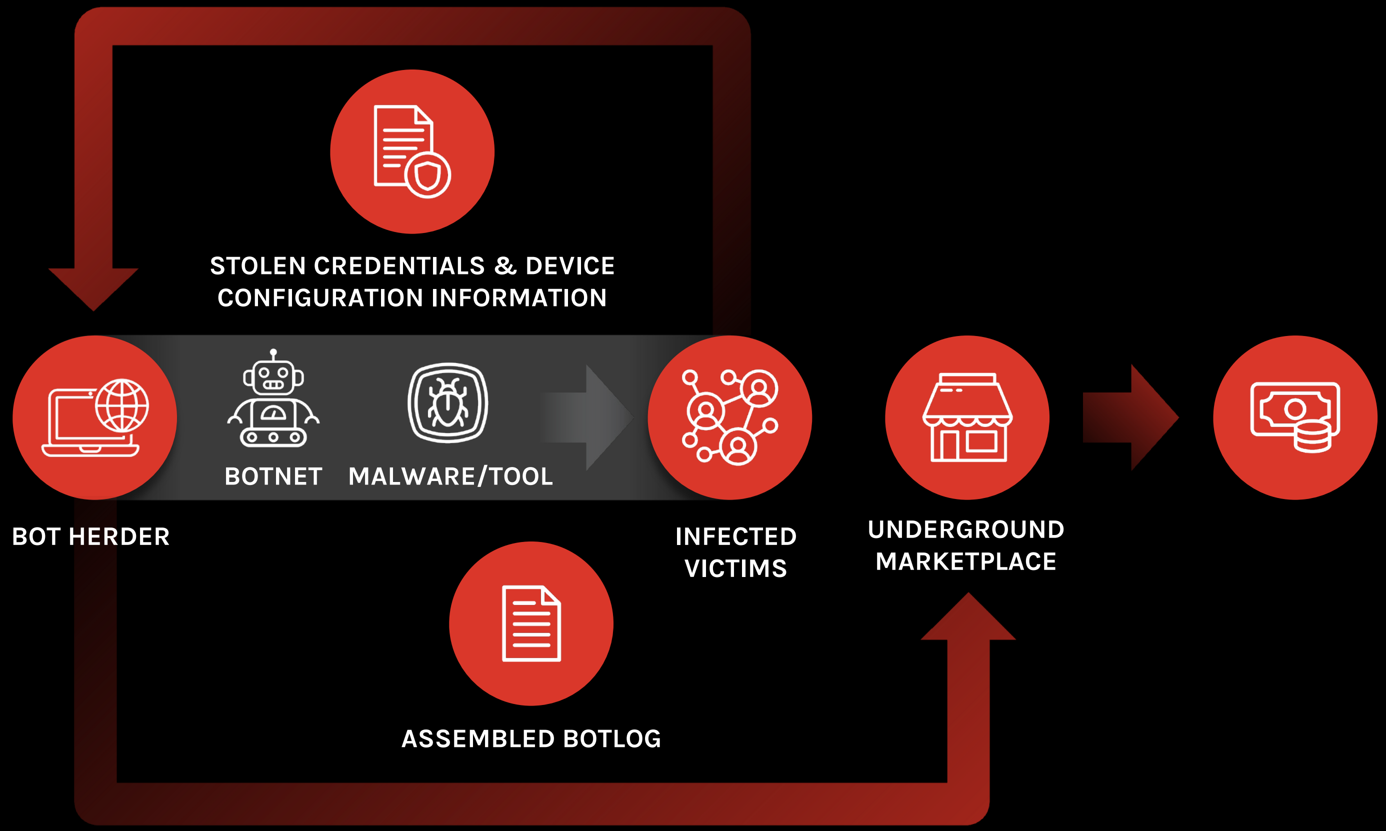
Service Accounts

Proactive **CONTROL**

Continuous **VISIBILITY**

Real Time **RESPONSE**

Access brokers: vital role in the e-crime ecosystem



ACCESS BROKERS ARE THREAT ACTORS WITH A SIGNIFICANT HISTORY OF PROVIDING INITIAL ACCESS TO MULTIPLE ENTITIES

ACCESS BROKERS OFTEN PERFORM ADDITIONAL ROLES IN THE ECRIME ECOSYSTEM

LOGIN CREDENTIALS

DEVICE CONFIGURATION DATA

Post Exploitation

How Adversaries Remain Stealthy

POTENTIAL DISRUPTIVE IMPACTS TO K-12

TECHNOLOGY AND TEACHING TOOLS

LUNCH SYSTEMS AND POS TO PURCHASE LUNCH

SAFETY SECURITY SYSTEM, INCLUDING VIDEO AND DOOR ACCESS

STOLEN TEACHER AND STUDENT DATA AND PII

STOLEN/ADJUSTED SCHOOL RECORDS AND GRADES

The Way Forward

Innovative Protection Capabilities & Recommendations

Protecting Our Future: Partnering to Safeguard K-12 Organizations From Cybersecurity Threats

Recommendations to address insufficient IT resources:

- Consider applying for cybersecurity grants,
- Utilize free or low-cost services,
- Expect third-party technology services to include strong security controls, and
- Take steps to minimize the burden of security.

TOP RECOMMENDATIONS

CULTURE OF CYBERSECURITY

Community awareness and practice are key to healthy cybersecurity; Engage your execs & board in a risk-based cyber program

ROLL IT OUT, TURN IT ON

Select tech partners who are strategic. Secure all of your tech infrastructure; Enable prevention capabilities, properly integrate. Remove legacy tech

BE VIGILANT & READY TO ACT

Beyond technology, practice incident response. Match defenders and adversaries 24x7x365, leveraging 1-10-60 rule

PROTECT YOUR IDENTITY

Use multi-factor for all accounts, protect service and admin accounts, adopt zero trust approach

CONTROL REMOTE ACCESS

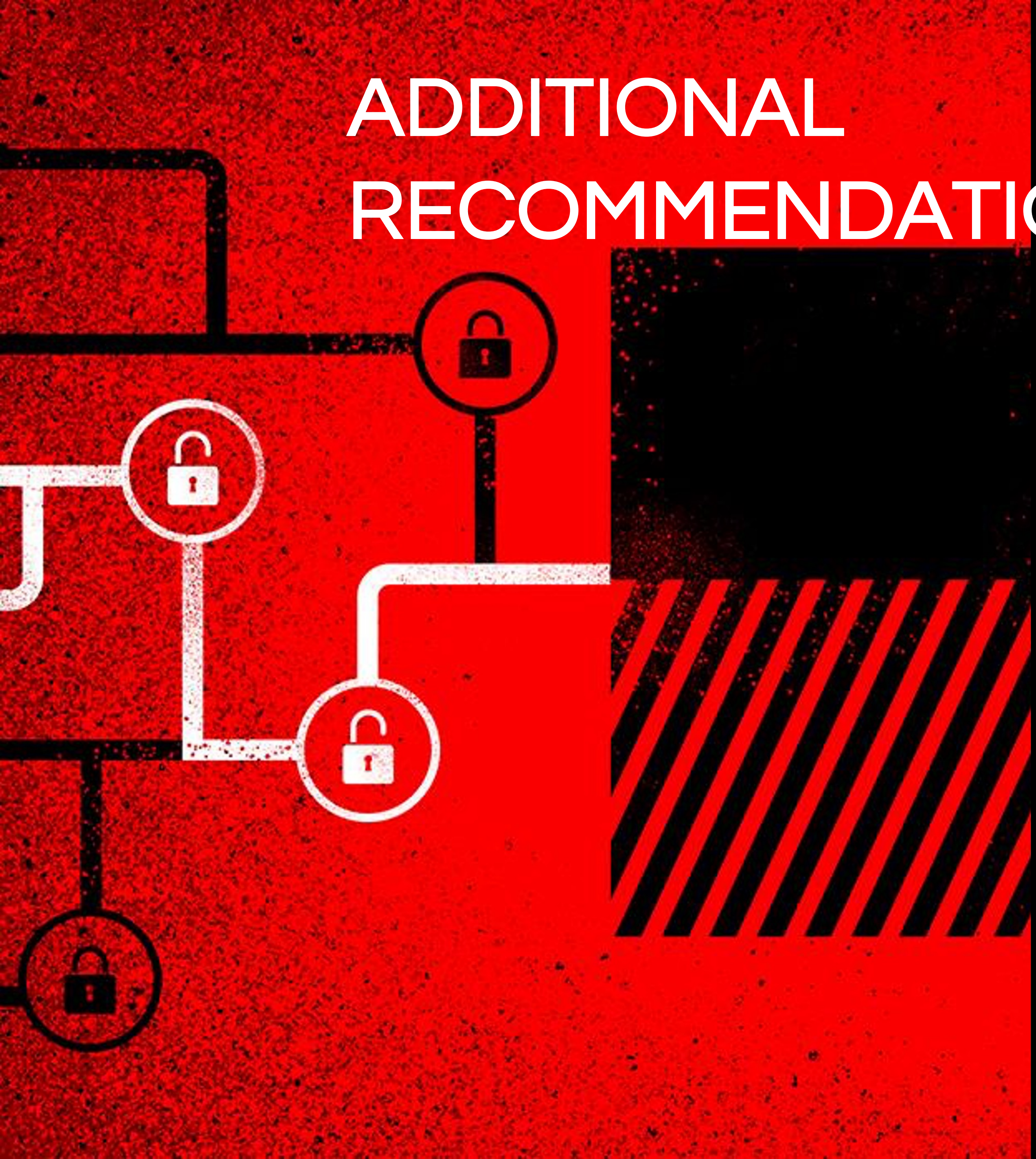
Refrain from exposing SMB and RDP ports to the internet, restrict remote access tools

PRACTICE GOOD HYGIENE

Control software, eliminating unneeded software, keep up-to-date with latest patches

TLP AMBER

ADDITIONAL RECOMMENDATIONS



- Double down on environment hardening and monitoring.
- Audit AD privileges and access, focusing on least privilege and Need to Know enforcement.
- Align detections and countermeasures with applicable TTPs.

Security Operations Enablement

- Review IRP, BCP, and DRP.
- Update detections for relevant TTPs.
- Close logging/visibility gaps.

Cloud, Infrastructure, and Network Security

- Identify and review 3rd party applications and provider rights/scope.
- Patch and harden internet facing systems/crown jewels.

Situational Awareness

- Continuous threat hunting
- Ongoing Exploit/TTP monitoring and validation

Top Ten Things To Do Now That Won’t Break the Bank

1. Leverage a framework to prioritize risk reducing efforts (NIST, etc.)
2. Train for phish and login protection
3. Join some great security organizations (MS-ISAC, etc.)
4. Leverage free assessments to better secure your technology network
5. Leverage free & open source resources
6. Continuously train yourself and your organization
7. Implement a basic incident response plan
8. Create a business continuity plan
9. Practice with tabletop exercises
10.Develop a schedule for executive reporting

CROWDSTRIKE

CISO Business Case
Partnering with CrowdStrike for Proactive Security

IDENTITY IS THE NEW PERIMETER

- We receive executive-level key metrics on identity risks
- We gain awareness of AD incidents, credential scanning and password attacks
- We can stop malicious authentications
- We can alert system admins to critical issues of anomalous behavior
- We can track down behavior and hygiene issues (The Ghost Employee RDP)
- We inspire account and password cleanup
- We get powerful policies and analytics
- We can verify if lockouts are actually malicious
- We can eliminate attack paths to critical accounts

https://www.crowdstrike.com/blog/9-ways-a-public-sector-ciso-uses-crowdstrike-identity-threat-protection/

YOUR ABILITY TO DEFEAT ADVANCED CYBER THREATS RESTS ALMOST ENTIRELY ON YOUR UNDERSTANDING OF THE PROBLEM