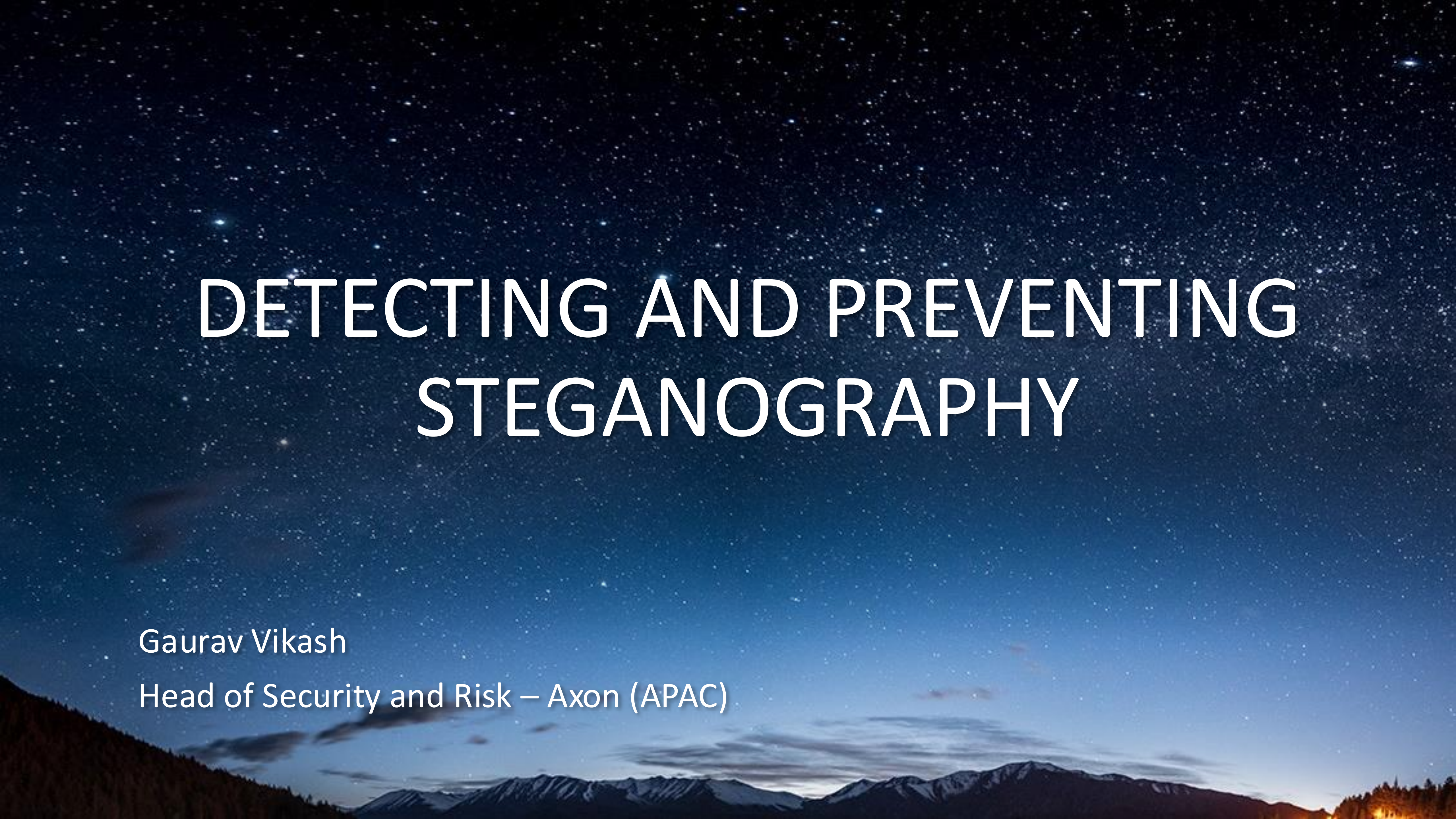


# DETECTING AND PREVENTING STEGANOGRAPHY

Gaurav Vikash

Head of Security and Risk – Axon (APAC)

WHAT

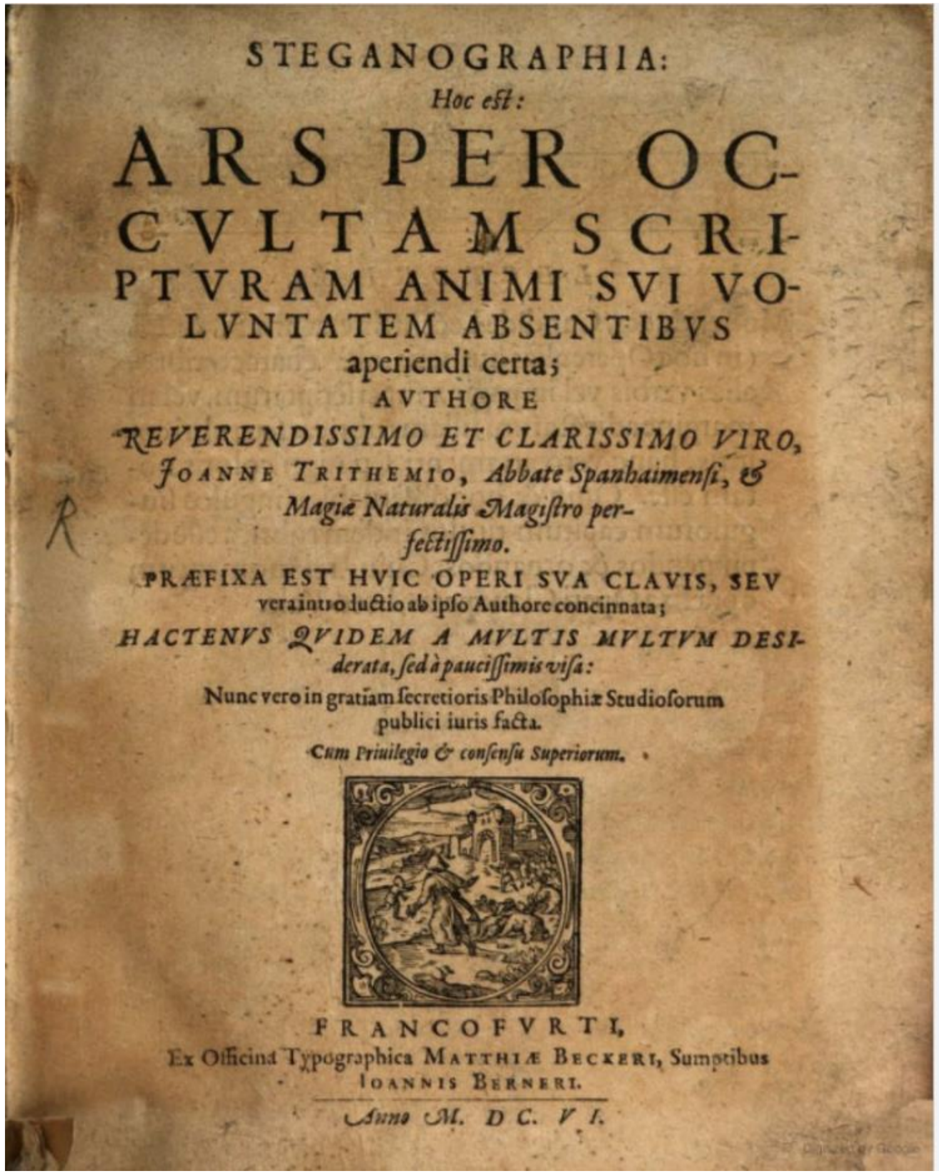
TECHNIQUES

DETECT

PREVENT

TAKEAWAYS

# HISTORY



STEGANOGRAPHIA:
*Hoc eſt:*
ARS PER OCCULTAM SCRIPTURAM ANIMI SUI VOLUNTATEM ABSENTIBUS
aperiendi certa;
AUTHORE
*REVERENDISSIMO ET CLARISSIMO VIRO,*
*IOANNE TRITHEMIO, Abbate Spanhaimenſi, &*
*Magiæ Naturalis Magiſtro perfectiſſimo.*

R

PRÆFIXA EST HUIC OPERI SUA CLAVIS, SEU
veraintroductio ab ipſo Authore concinnata;
*HACTENUS QUIDEM A MULTIS MULTUM DESIderata, ſed à pauciſſimis viſa:*
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
*Cum Priuilegio & conſenſu Superiorum.*

FRANCOFURTI,
Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus
IOANNIS BERNERI.
*Anno M. DC. VI.*

# DEFINITIONS

PAYLOAD

THE INFORMATION TO BE CONCEALED

KEY

ENCRYPT/ENCODE THE PAYLOAD

CARRIER

THE OBJECT IN WHICH THE PAYLOAD IS HIDDEN

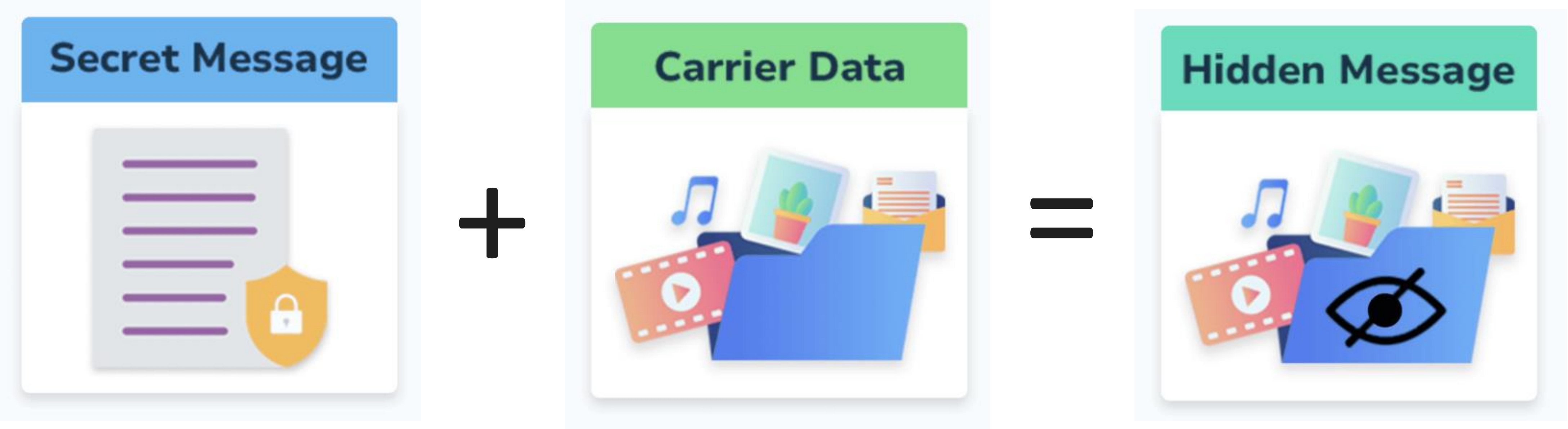
STEGO-SYSTEM

THE TECHNOLOGY OF HIDING A PAYLOAD IN A CARRIER

CHANNEL

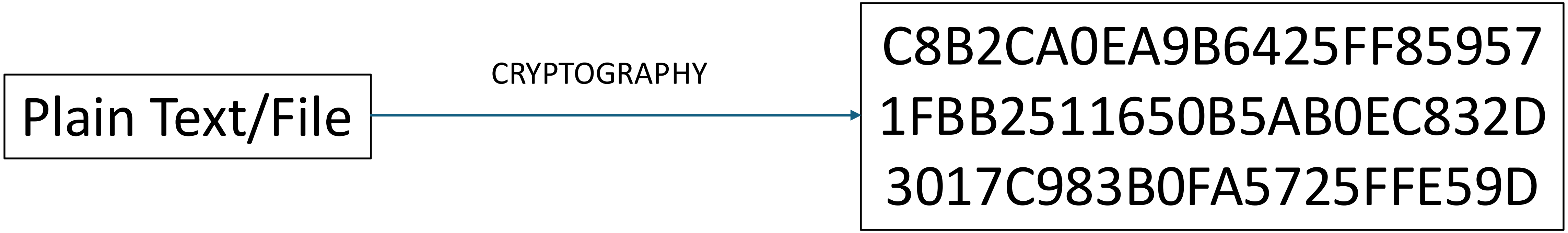
THE CHANNEL OVER WHICH THE CARRIER IS TRANSFERRED

# STEGANOGRAPHY



TEXT | IMAGE | AUDIO | VIDEO | SOCIAL MEDIA | QR CODES | WEB ADS | IT/IoT NETWORK

# CRYPTOGRAPHY



Plain Text/File

CRYPTOGRAPHY

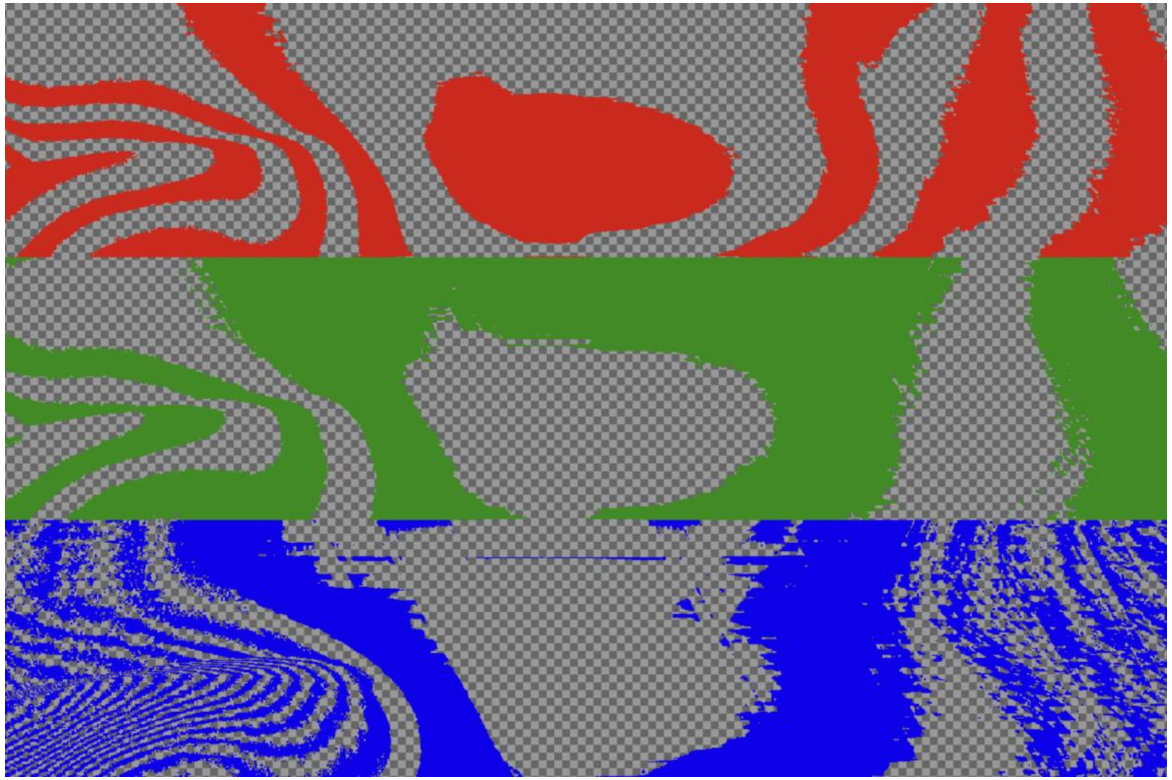
C8B2CA0EA9B6425FF85957
1FBB2511650B5AB0EC832D
3017C983B0FA5725FFE59D

# STEGANOGRAPHY

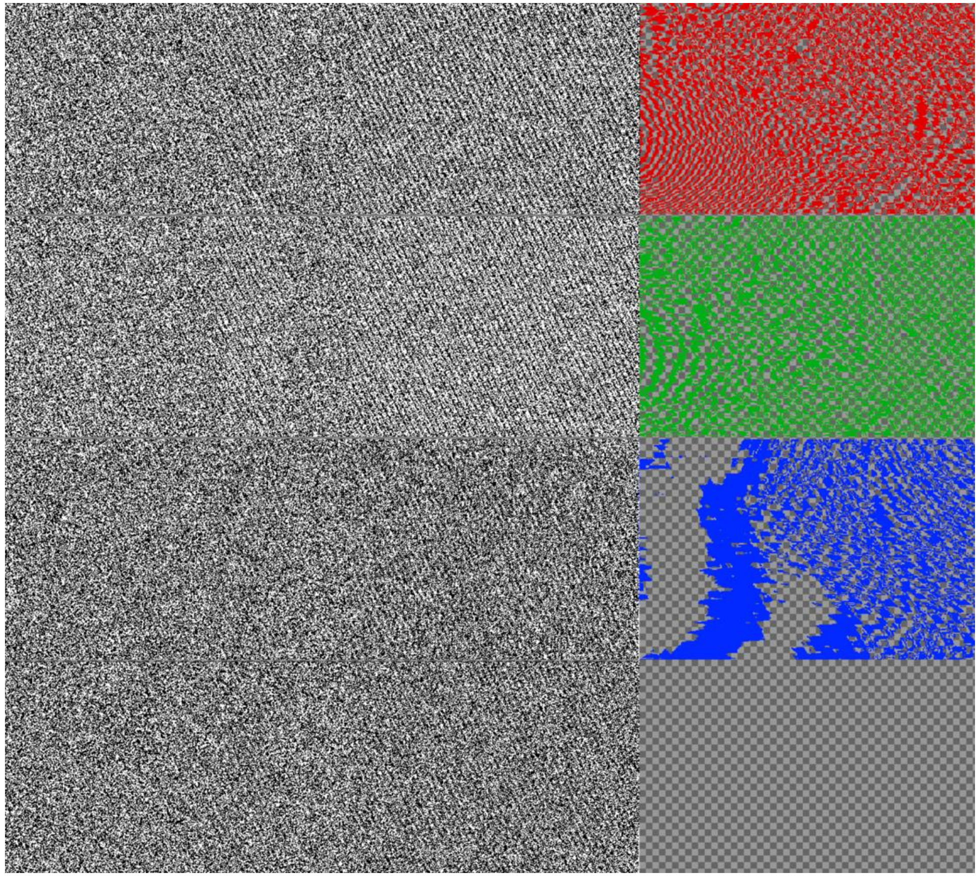
**A PNG image file containing the info-stealer**

*Source: Avast*

# RGB PLANE



RANDOM RGB PLAIN WITHOUT HIDDEN PAYLOAD



LSB PLAIN WITH ENCODED AND ENCRYPTED PAYLOAD

# GOOD & BAD

## GOOD

- Watermarking Digital Media
- Securing Comms in Restricted States
- Metadata for Digital Forensics
- Covert Military or Intelligence Comms
- Data Integrity Verification

## BAD

- Malware Distribution
- Data Leakage
- Fraudulent Financial Transactions
- Stealthy Comms for Cyber Espionage
- Concealing Evidence of Illegal Activities

# TECHNIQUES

# TECHNIQUES

## TEXT

- STATISTICAL ANALYSIS
- LINGUISTIC ANALYSIS

## IMAGE

- LEAST SIGNIFICANT BIT
- SPREAD SPECTRUM
- DISCRETE COSINE TRANSFORMATION

## AUDIO

- LEAST SIGNIFICANT BIT
- PHASE CODING
- SPREAD SPECTRUM
- ECHO HIDING

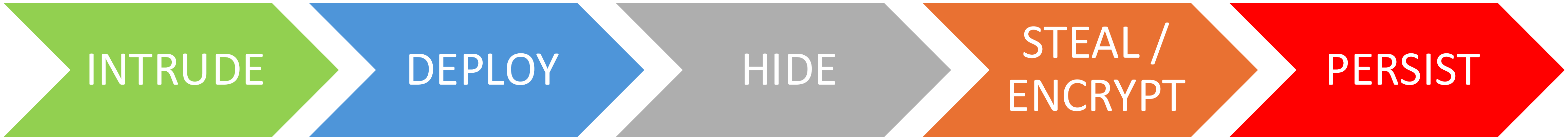
## VIDEO

- FRAME MANIPULATION
- SPATIAL DOMAIN
- TRANSFORM DOMAIN
- TEMPORAL DOMAIN

## NETWORK

- PROTOCOL
- PAYLOAD
- TIMING
- TRAFFIC

# TECHNICAL GOALS



INTRUDE

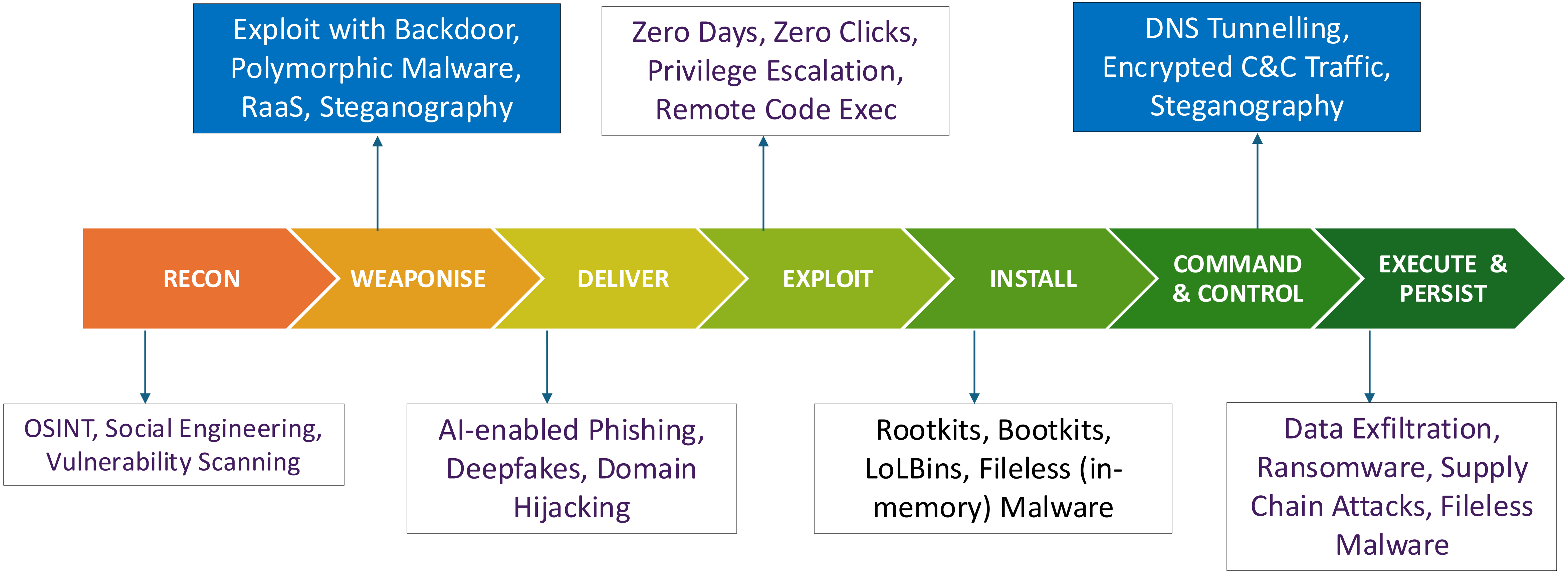
DEPLOY

HIDE

STEAL / ENCRYPT

PERSIST

# CYBER KILL CHAIN – ATTACKERS’ VIEW



RECON

OSINT, Social Engineering, Vulnerability Scanning

WEAPONISE

Exploit with Backdoor, Polymorphic Malware, RaaS, Steganography

DELIVER

AI-enabled Phishing, Deepfakes, Domain Hijacking

EXPLOIT

Zero Days, Zero Clicks, Privilege Escalation, Remote Code Exec

INSTALL

Rootkits, Bootkits, LoLBins, Fileless (in-memory) Malware

COMMAND & CONTROL

DNS Tunnelling, Encrypted C&C Traffic, Steganography

EXECUTE & PERSIST

Data Exfiltration, Ransomware, Supply Chain Attacks, Fileless Malware

Credit: Lockheed Martin

# FINAL GOALS

ID, INFO, $, TECH

DEFENCE SECRETS

DISRUPT A NATION

ALL OUT WAR

# INCIDENTS

## STUXNET (2010)

- DUQU, IMAGE
- SPY ON IRAN'S NUCLEAR PROGRAM

## KASPERSKY (2015)

- DUQU 2.0, IMAGE
- STEAL FUTURE TECH INCLUDING ANTI-APT

## 13 GOV ORGS (2018)

- TURLA, AUDIO (.WAV)
- SPY ON 10X GOV AFFAIRS & UNI RESEARCH

## GOV & PRIV (2022)

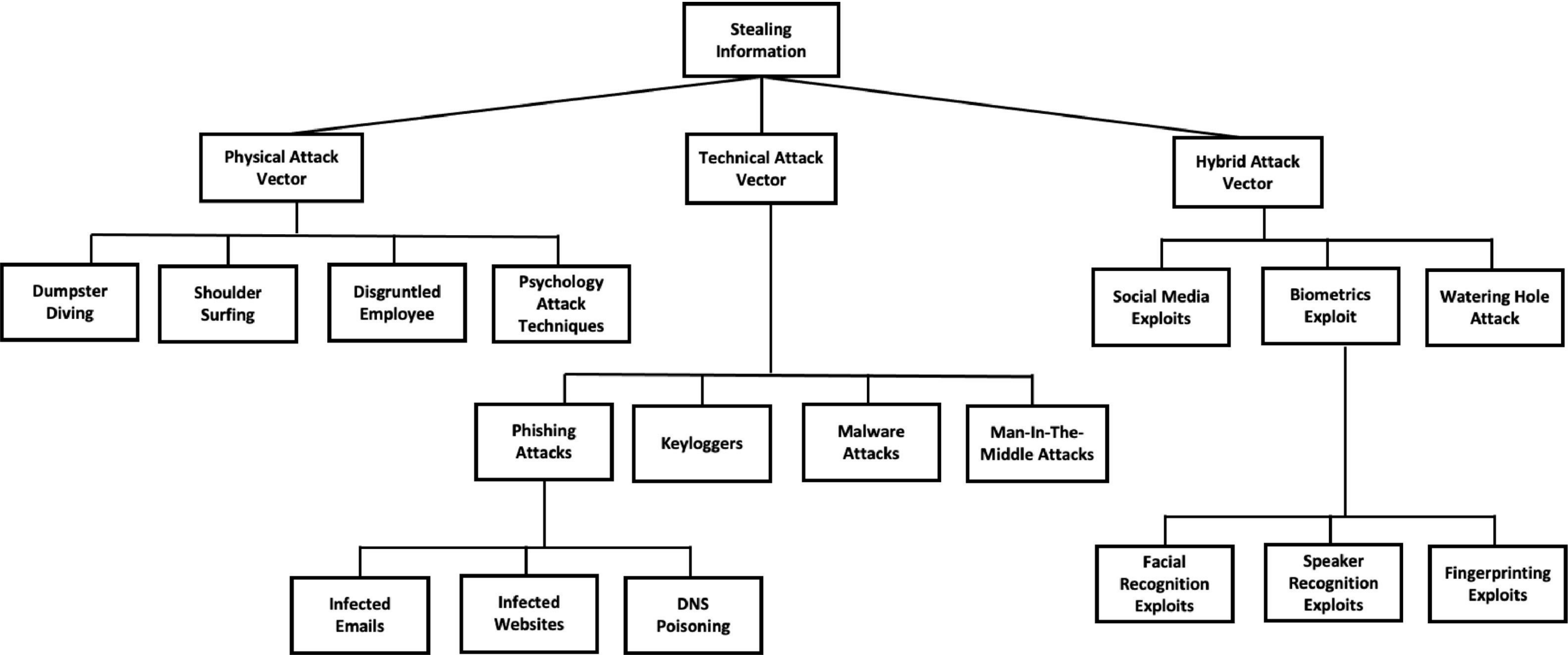
- WOROK, IMAGE
- DISRUPT CRITICAL INFRA
- DROPBOX

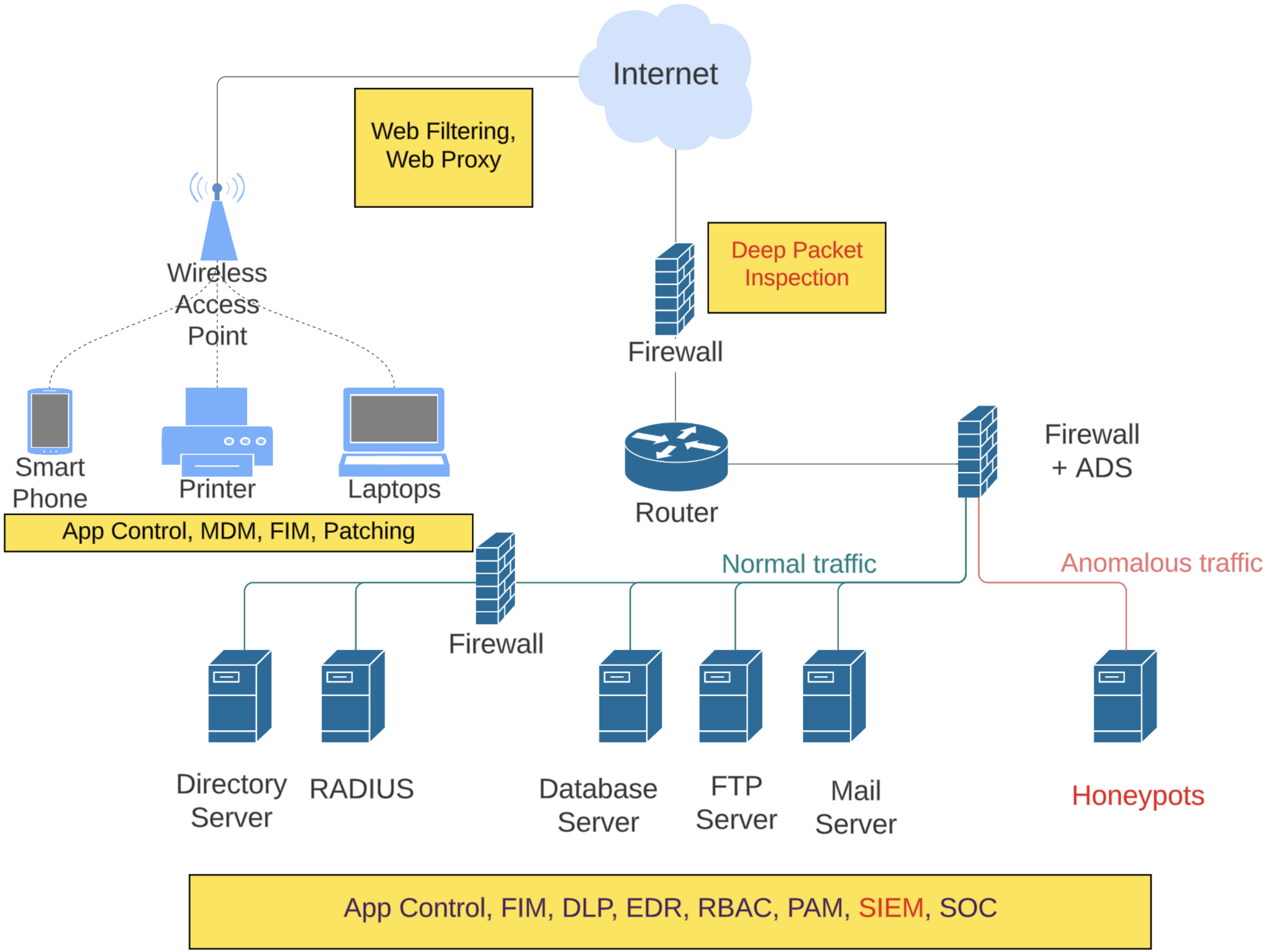
## GLOBAL (2024)

- TA558, IMAGE, TEXT
- STEAL $, 320X
- 2017 MS, SMTP

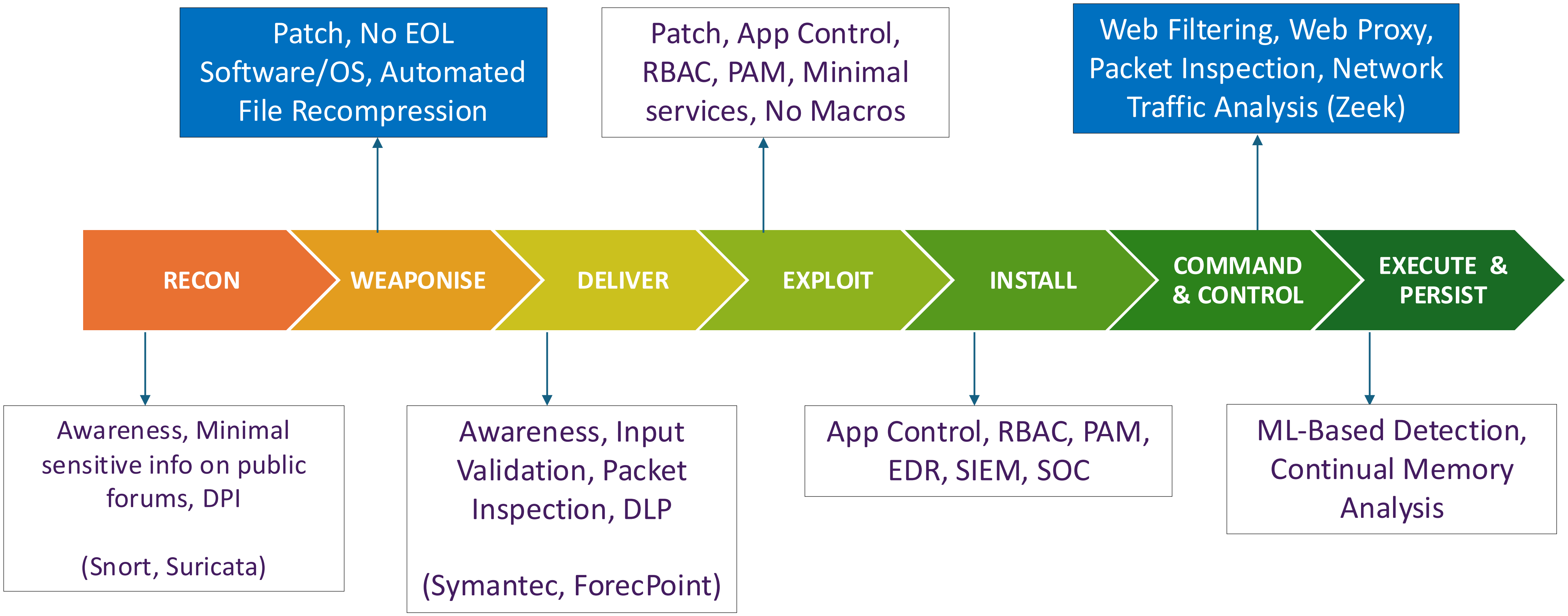
# DETECT & PREVENT

# ATTACK TREE


Stealing Information
Physical Attack Vector
Technical Attack Vector
Hybrid Attack Vector
Dumpster Diving
Shoulder Surfing
Disgruntled Employee
Psychology Attack Techniques
Social Media Exploits
Biometrics Exploit
Watering Hole Attack
Phishing Attacks
Keyloggers
Malware Attacks
Man-In-The-Middle Attacks
Infected Emails
Infected Websites
DNS Poisoning
Facial Recognition Exploits
Speaker Recognition Exploits
Fingerprinting Exploits


Internet
Web Filtering, Web Proxy
Wireless Access Point
Deep Packet Inspection
Firewall
Smart Phone
Printer
Laptops
Router
Firewall + ADS
App Control, MDM, FIM, Patching
Firewall
Normal traffic
Anomalous traffic
Directory Server
RADIUS
Database Server
FTP Server
Mail Server
Honeypots
App Control, FIM, DLP, EDR, RBAC, PAM, SIEM, SOC

# CYBER KILL CHAIN – DEFENDERS' VIEW



Patch, No EOL Software/OS, Automated File Recompression

Patch, App Control, RBAC, PAM, Minimal services, No Macros

Web Filtering, Web Proxy, Packet Inspection, Network Traffic Analysis (Zeek)

RECON

WEAPONISE

DELIVER

EXPLOIT

INSTALL

COMMAND & CONTROL

EXECUTE & PERSIST

Awareness, Minimal sensitive info on public forums, DPI

(Snort, Suricata)

Awareness, Input Validation, Packet Inspection, DLP

(Symantec, ForecPoint)

App Control, RBAC, PAM, EDR, SIEM, SOC

ML-Based Detection, Continual Memory Analysis

# TAKEAWAYS

# KEY TAKEAWAYS

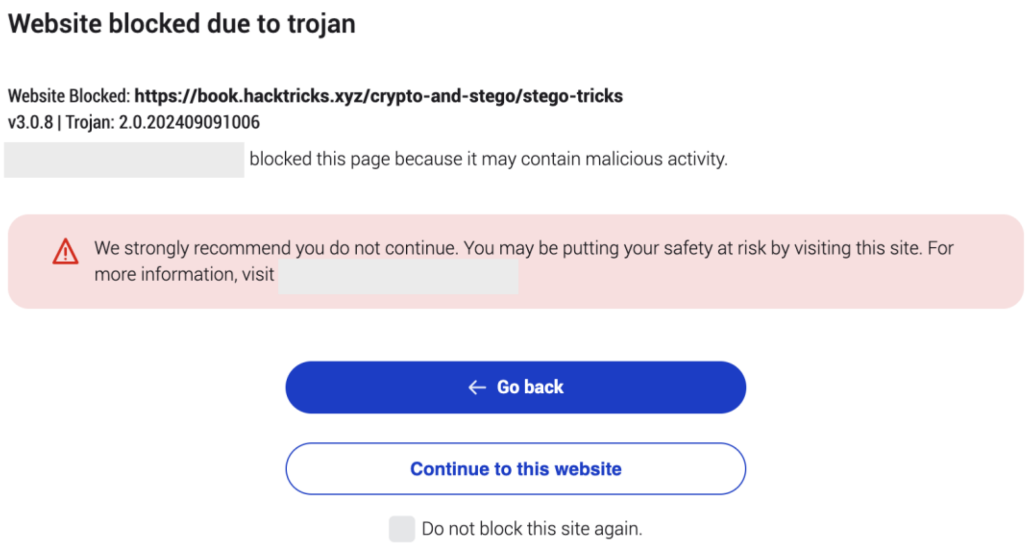
Know Your Blind Spots

Automated & Scalable Solutions

PEOPLE: Hiring Practices, Culture, Awareness

PROCESS: BCP, DRP, IRP

TECH: App Control, Patching, MFA, PAM, MDM, Browser Security, Backup (Essential 8)



**Website blocked due to trojan**

Website Blocked: **https://book.hacktricks.xyz/crypto-and-stego/stego-tricks**
v3.0.8 | Trojan: 2.0.202409091006

[redacted] blocked this page because it may contain malicious activity.

⚠ We strongly recommend you do not continue. You may be putting your safety at risk by visiting this site. For more information, visit [redacted]

□ Do not block this site again.

# THANK YOU

Gaurav Vikash