Cybercrime as a Service

CMPT 980 - Enterprise Security

Group 6

Sa Wang, Ali Alden, Yangyang Jiang, Robin Li, Sanjit Mann, Ahmed Tawfik

Start

Table Of Contents

Table Of Contents

01

Introduction to Cybercrime

What is Cybercrime?

- Definition: Illegal activities conducted over the internet, targeting individuals, companies, or governments.
- Evolution: Cybercrime has grown from basic hacking attempts to a highly organized industry.

Cybercrime as a Service (CaaS) Model

- Overview: Similar to Software as a Service (SaaS), cybercrime has adopted an "as a service" model.
- Impact of CaaS: Even non-technical criminals can now rent or purchase tools like ransomware, phishing kits, and other hacking services.
- Key Drivers:
  - Technological Advances: Cloud computing, the dark web, and anonymous payments (e.g., cryptocurrency) facilitate CaaS.
  - High Profitability: The lucrative nature of cybercrime attracts organized groups to develop and sell criminal services.

Challenges in Combating CaaS

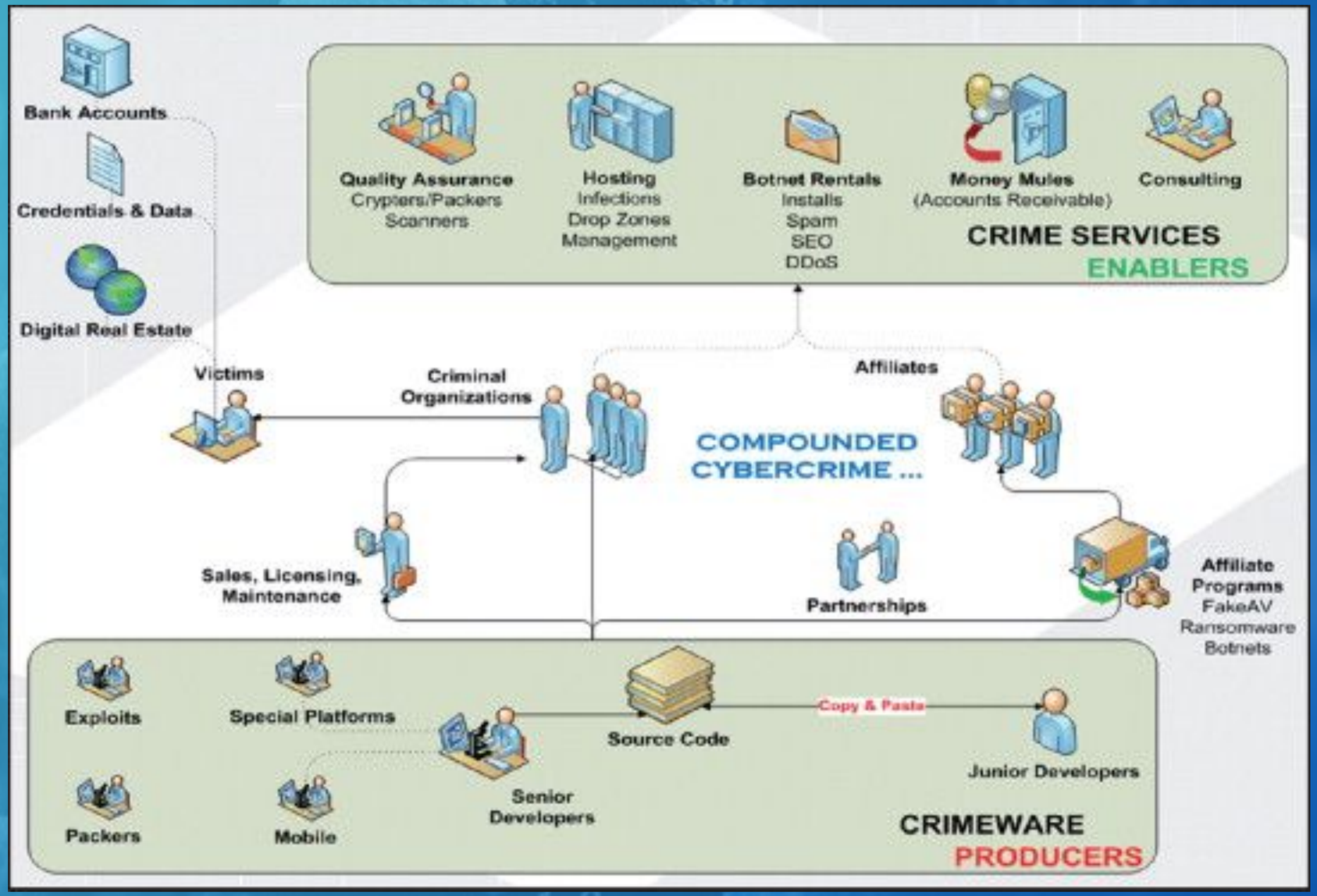
- Legal Issues: Cybercrime often crosses international borders, leading to jurisdictional challenges and difficulty in enforcement.
- Technology Gaps: Rapidly advancing technologies, like encryption and anonymization tools, make tracking and stopping cybercriminals difficult.

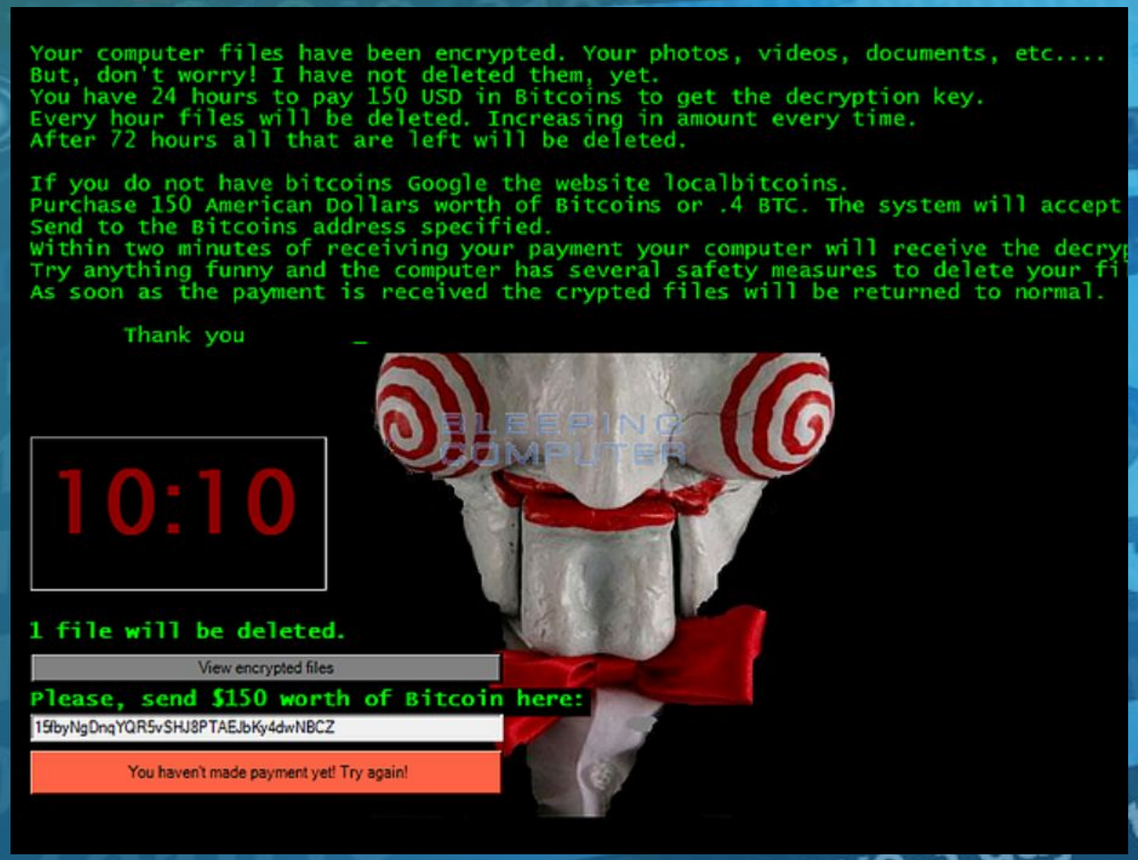
Importance of Cybercrime Awareness and Prevention

Organizations and individuals need to:

- Stay Informed: Keep up with the latest cybercrime tactics.
- Strengthen Security: Implement robust cybersecurity measures and regularly update systems.
- Promote Awareness and Education: Training and awareness are essential for effective prevention.

Ecosystem


Bank Accounts
Credentials & Data
Digital Real Estate
Quality Assurance
Crypters/Packers
Scanners
Hosting
Infections
Drop Zones
Management
Botnet Rentals
Installs
Spam
SEO
DDoS
Money Mules
(Accounts Receivable)
Consulting
CRIME SERVICES
ENABLERS
Victims
Criminal Organizations
Affiliates
COMPOUNDED CYBERCRIME ...
Sales, Licensing, Maintenance
Partnerships
Affiliate Programs
FakeAV
Ransomware
Botnets
Exploits
Special Platforms
Source Code
Copy & Paste
Junior Developers
Senior Developers
Packers
Mobile
CRIMEWARE
PRODUCERS



02 Ransomware As a Service (RaaS)

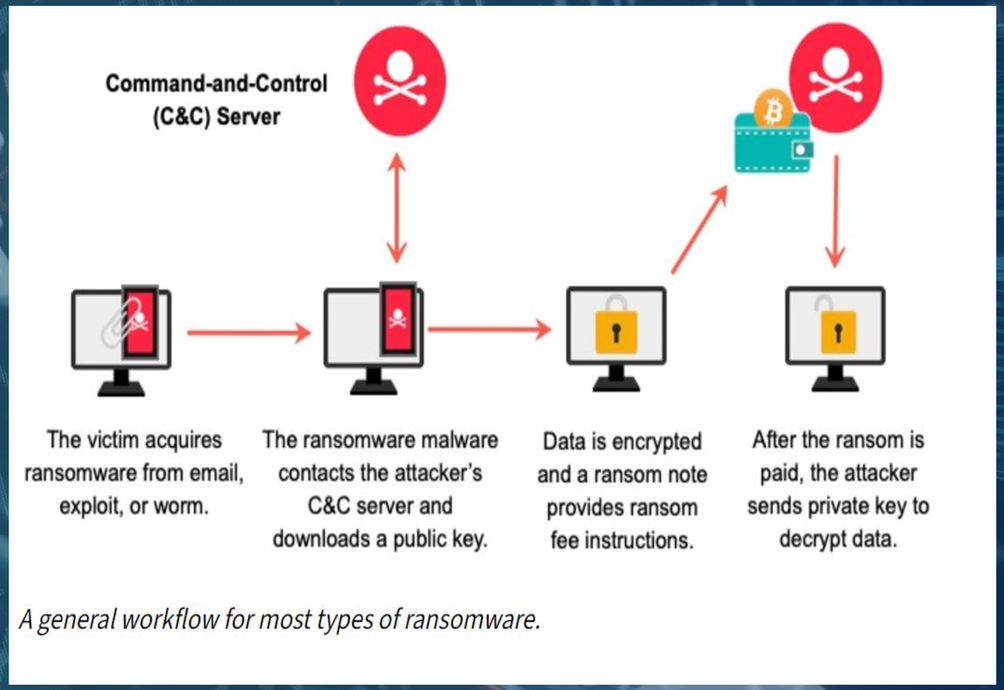
RaaS Introduction

- What is RaaS (Ransomware as a Service?)
  - A new type of organized cybercrime model where the hacker sell ransomware tools and software.
  - as of 2024, 20% of all cybercrime are ransomware attacks on SMB and enterprise data.[1]
  - Less technical threat actors can now carry out complicated attacks on enterprise data through subscription services.

[1] https://www.ibm.com/topics/ransomware-as-a-service

How does RaaS work?

- We'll take a look at the recent July 2024 enterprise hacks with El-Dorado Raas.
  - A malicious software gets sent through a server network usually sent beforehand by a threat actor.
  - The malicious program is usually installed through a backdoor or with admin access from an accomplice.
  - It surveils the infected device for a few days and steal data through covert channels.



A general workflow for most types of ransomware.

[1] https://www.ibm.com/topics/ransomware-as-a-service

How does RaaS work? (cont.)

- Data is then encrypted through RSA-OAEP encryption technology
- Device gets a notification and has a set amount of time to pay until data is destroyed.[1] (supposedly)
- Stolen data is sold on the dark web for more bitcoins.
- If Victim pays the ransom, the data usually is given back as a sign of “trust” for the next attack.
- A percentage or cut is given to the Ransomware subscription provider.

[1] https://www.group-ib.com/resources/knowledge-hub/raas/

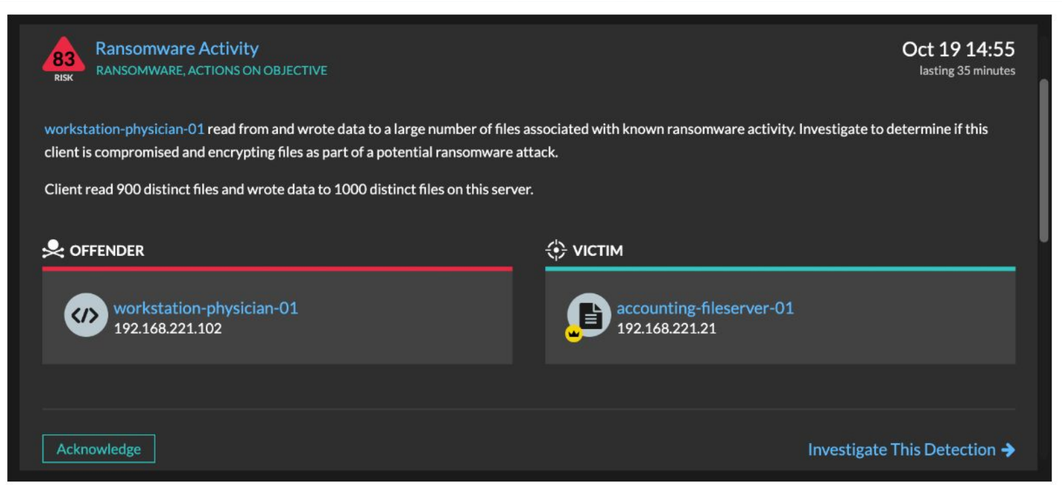
Case Study

- HTE Technology is a $19.7 Million USD manufacturing company based in Missouri.
- Eldorado successfully entered HTE's system, disrupting IT and OT operations and stopping production with the ransomware attack.
- The stolen data was ransomed back to them (unknown amount of bitcoins) but also sold online on the Tor networks.[1]
- As of November 2024, HTE's data leak has caused reputational damage to the company.

[1] https://x.com/FalconFeedsio/status/1798698965669675422

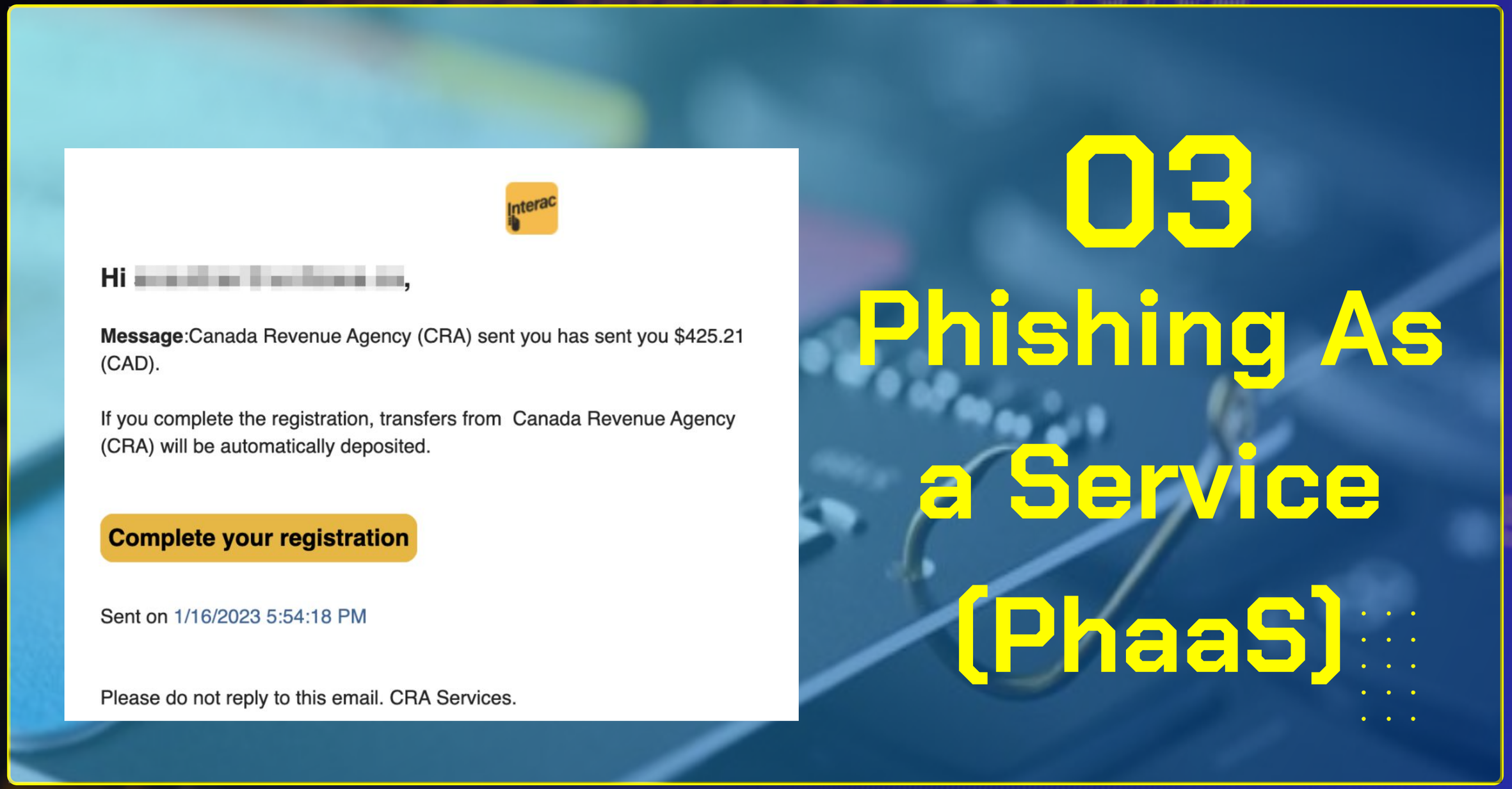
Conclusion and Mitigation

- Mitigation Strategies: companies that are part of the cloud are more resilient to ransomware attacks.
- Quantum Computing Technology: has been proven to unlock encrypted data but still in its early stages.
- SOC tools for cybersecurity specialists to trace evidence of ransomware attack on a device network.



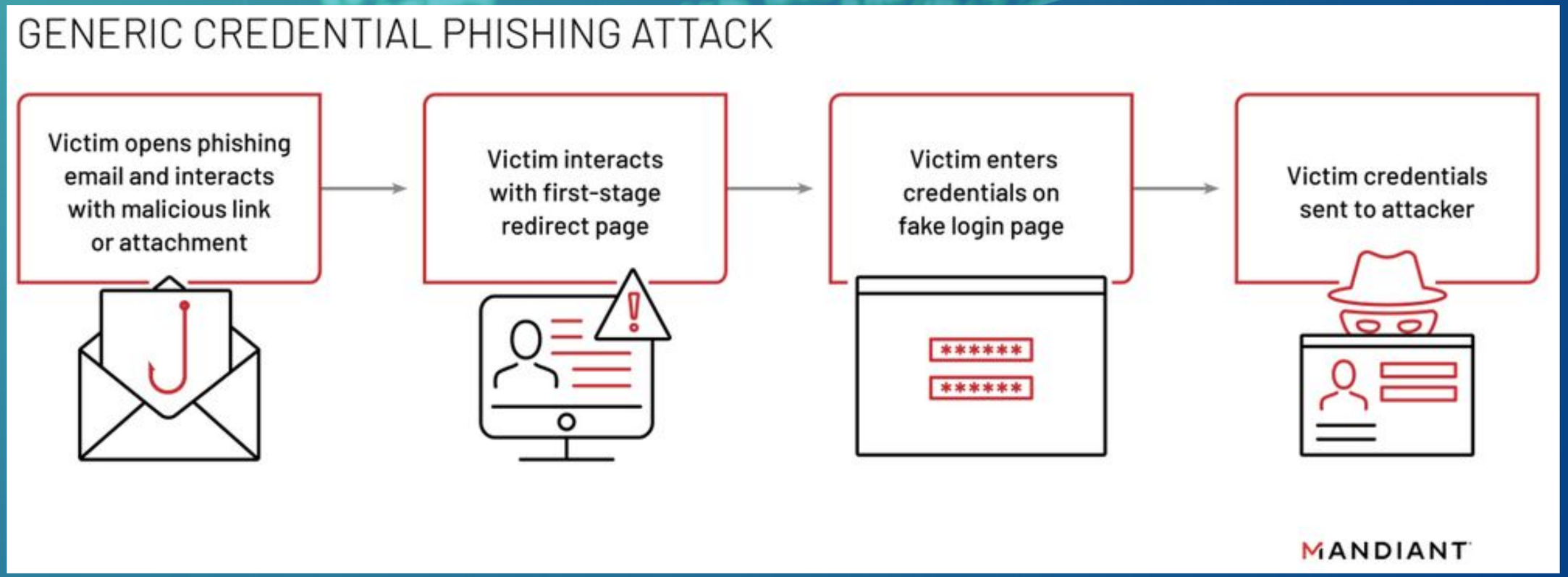
Ransomware malware typically scans files and then encrypts them. This behavior appears as distinct file reads and writes.

[1]https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/


Interac
Hi [redacted],
Message:Canada Revenue Agency (CRA) sent you has sent you $425.21 (CAD).
If you complete the registration, transfers from Canada Revenue Agency (CRA) will be automatically deposited.
Complete your registration
Sent on 1/16/2023 5:54:18 PM
Please do not reply to this email. CRA Services.
03
Phishing As a Service (PhaaS)

What is Phishing As a Service (PhaaS)

- **What is Phishing?**
  - Social engineering to steal sensitive information.
  - Example: Fake websites, malicious links, email impersonation.
- **What is PhaaS?**
  - Subscription-based phishing kits and services.
  - Accessible on the dark web for attackers of all skill levels.
- **Why it matters:** PhaaS increases the scale and ease of cyberattacks.


GENERIC CREDENTIAL PHISHING ATTACK
Victim opens phishing email and interacts with malicious link or attachment
Victim interacts with first-stage redirect page
Victim enters credentials on fake login page
Victim credentials sent to attacker
******
******
MANDIANT

How PhaaS Works

Key Features of PhaaS:

- Pre-built phishing kits (e.g., templates, scripts, hosting).
- Tools like DNStwist for domain generation.
- Intuitive dashboards for creating and managing campaigns.
- Techniques like hiding phishing content behind proxies for evasion.

Steps:

1. Set up fake domains and clone websites.
2. Configure email servers (DKIM, SPF, DMARC) to bypass spam filters.
3. Launch campaigns to collect user credentials.

	Phishing kits	Phishing-as-a-Service (PhaaS)
Payment	One-time	Subscription-based *(Available weekly, bi-weekly, monthly, or annual)*
Email templates	✓	✓ *(Optional)*
Site templates	✓	✓
Email delivery		✓ *(Optional)*
Site hosting		✓
Credential theft		✓
Credential redistribution		✓
"Fully undetected" links/logs		✓

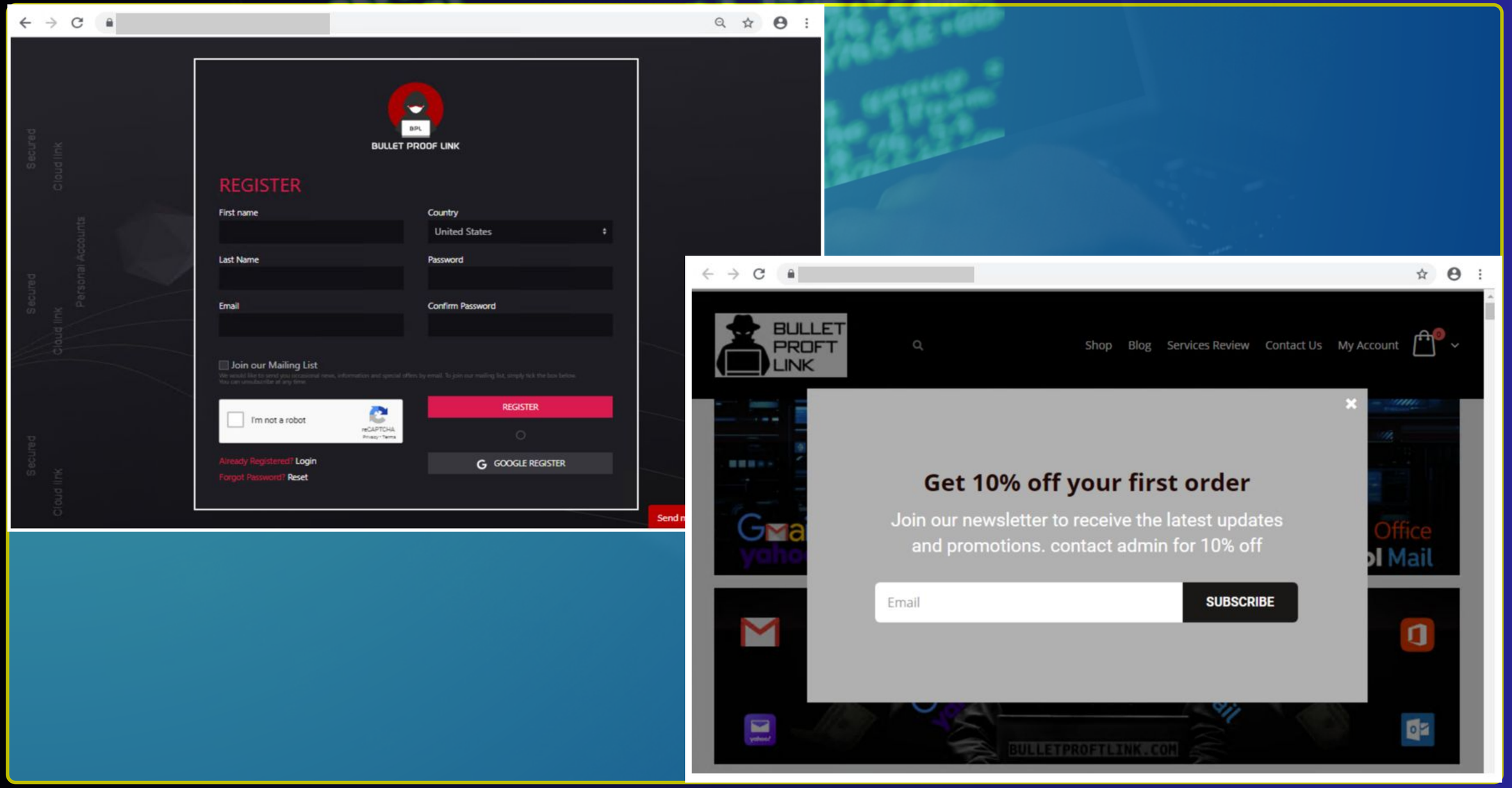
Real World Example:

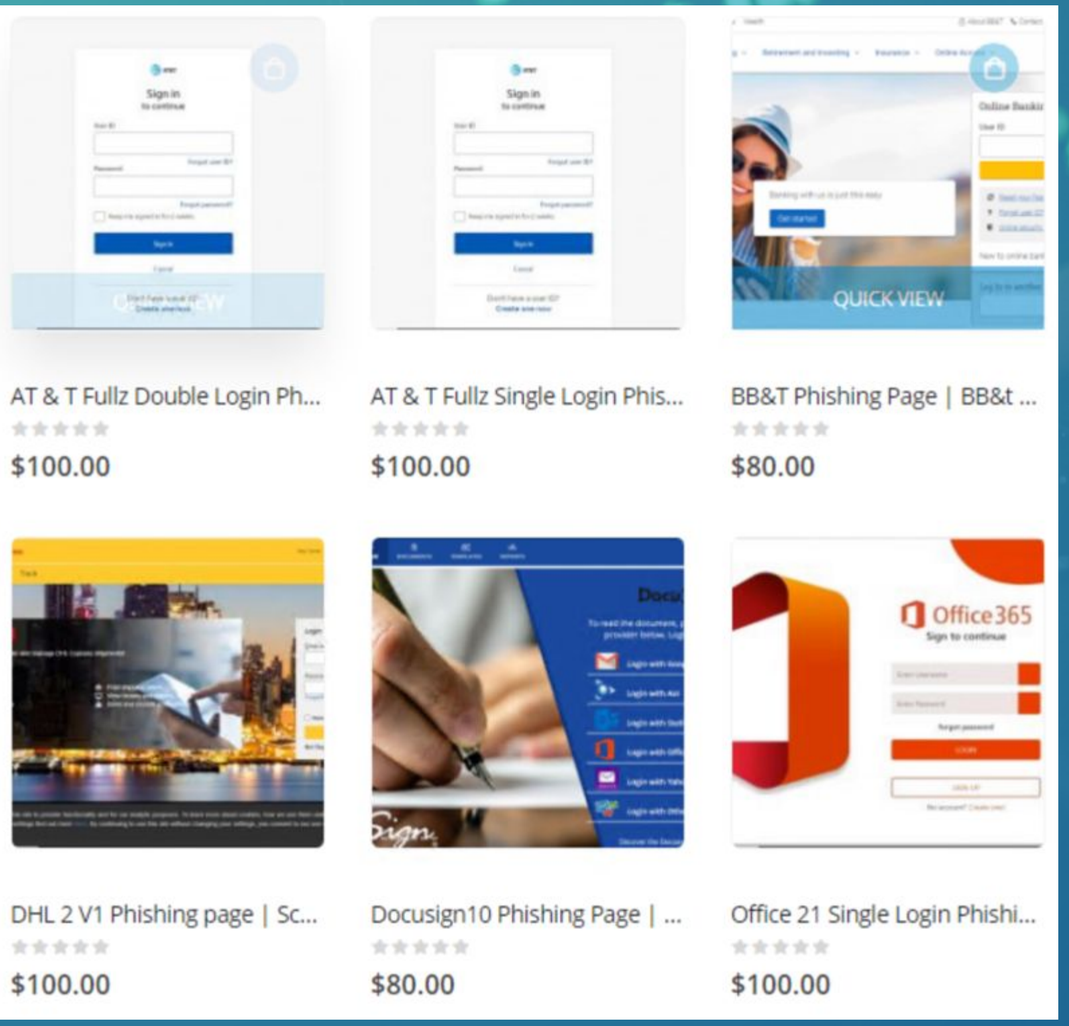
About BulletProofLink:

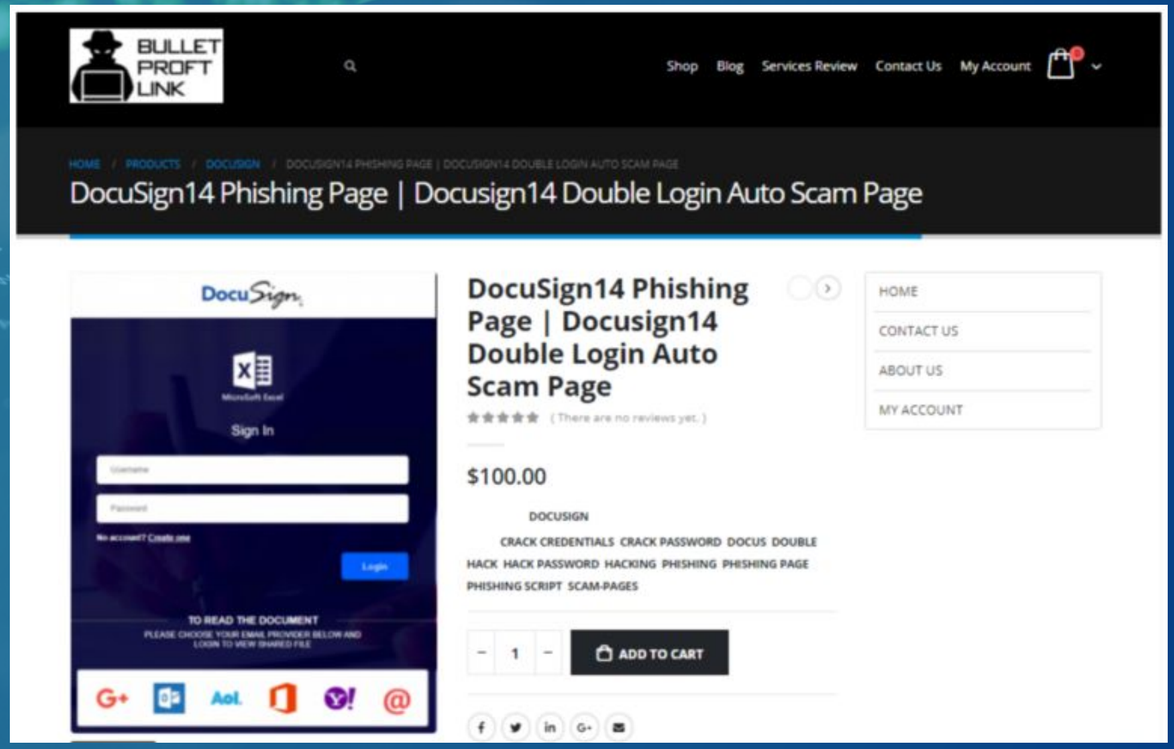
- A Phishing-as-a-Service (PhaaS) platform active since 2018.
- Offers over 100 phishing templates mimicking trusted brands.
- Services include phishing kits, email templates, hosting, and customer support.

Key Features:

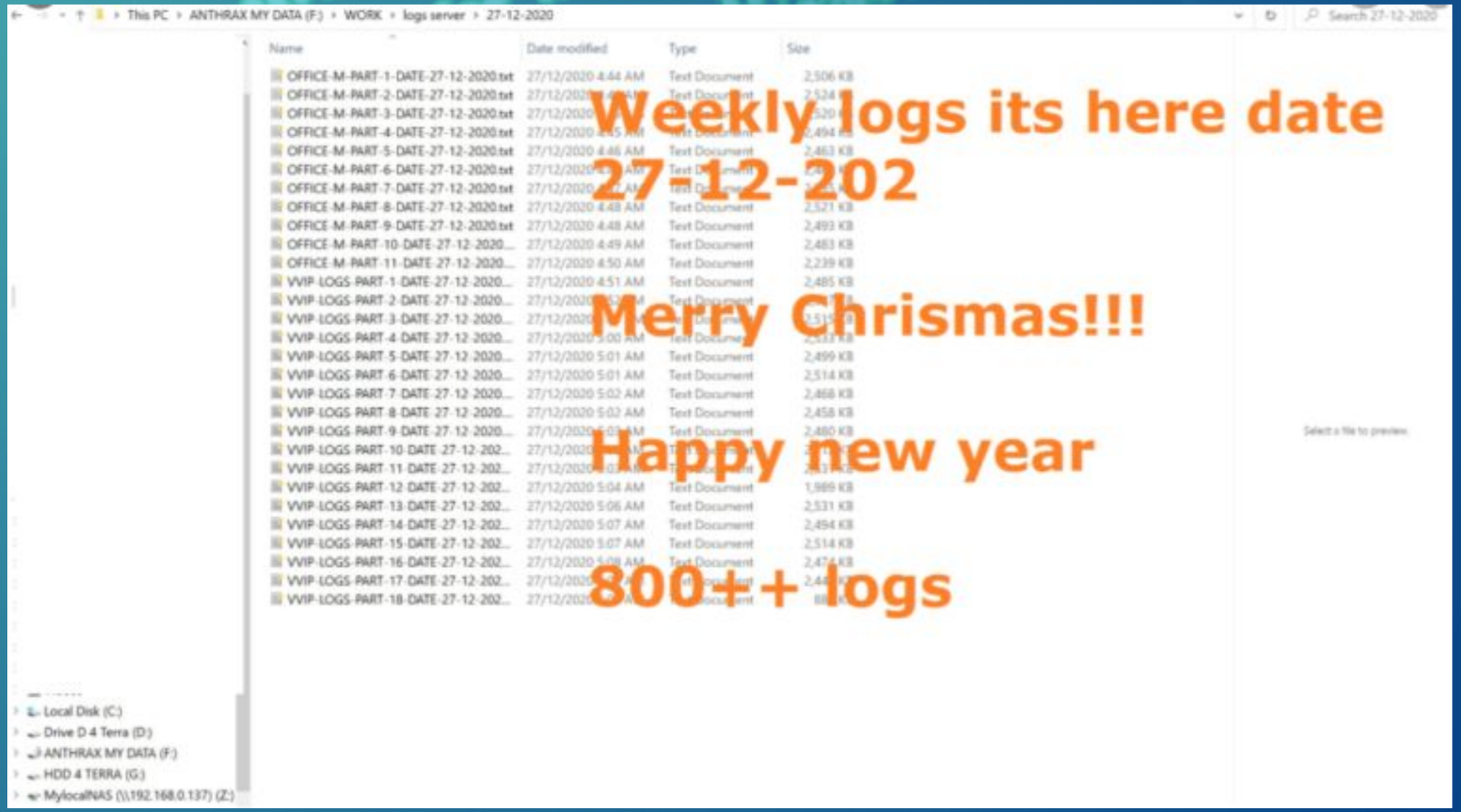
- Subscription-based model with prices up to $800/month.
- “Double Theft” technique: Credentials stolen for both operators and customers.
- Infinite subdomain abuse: Over 300,000 unique subdomains used in a single campaign.


BULLET PROOF LINK
REGISTER
First name
Country
United States
Last Name
Password
Email
Confirm Password
Join our Mailing List
I'm not a robot
reCAPTCHA
REGISTER
GOOGLE REGISTER
Already Registered? Login
Forgot Password? Reset
BULLET PROFT LINK
Shop
Blog
Services Review
Contact Us
My Account
Get 10% off your first order
Join our newsletter to receive the latest updates and promotions. contact admin for 10% off
Email
SUBSCRIBE
BULLETPROFTLINK.COM


AT & T Fullz Double Login Ph...
$100.00
AT & T Fullz Single Login Phis...
$100.00
BB&T Phishing Page | BB&t ...
$80.00
QUICK VIEW
DHL 2 V1 Phishing page | Sc...
$100.00
Docusign10 Phishing Page | ...
$80.00
Office 21 Single Login Phishi...
$100.00


BULLET PROFT LINK
Shop
Blog
Services Review
Contact Us
My Account
DocuSign14 Phishing Page | Docusign14 Double Login Auto Scam Page
DocuSign14 Phishing Page | Docusign14 Double Login Auto Scam Page
$100.00
DOCUSIGN
CRACK CREDENTIALS CRACK PASSWORD DOCUS DOUBLE HACK HACK PASSWORD HACKING PHISHING PHISHING PAGE PHISHING SCRIPT SCAM-PAGES
ADD TO CART
HOME
CONTACT US
ABOUT US
MY ACCOUNT

Logs for Hire works:



Defending Against PhaaS Driven Attacks

Microsoft Defender for Office 365 Protections:

- **Real-Time Analysis:**
  - Uses machine learning, heuristics, and advanced detonation to detect phishing emails, URLs, and landing pages.
- **Campaign Detection:**
  - Identifies phishing kits like BulletProofLink and detects associated phishing emails and websites.
- **Blocking Threats:**
  - Prevents access to phishing websites and malicious URLs through SmartScreen.
  - Detects suspicious and malicious behavior on endpoints.

Impacts of PhaaS

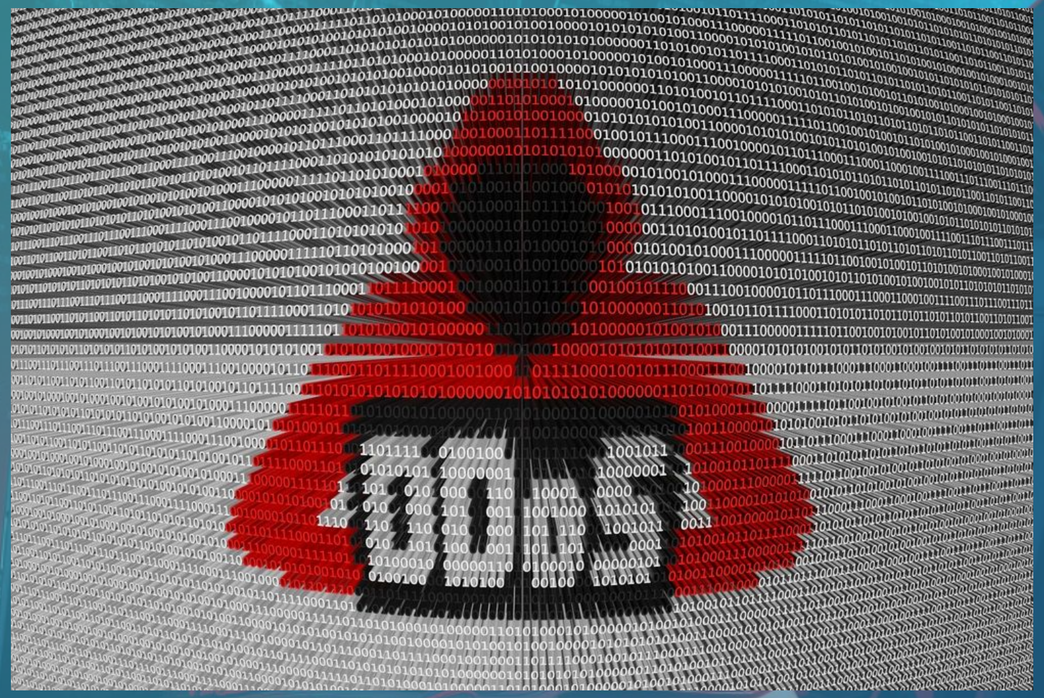
- **Individuals:**
  - Loss of sensitive information (login credentials, financial data).
- **Organizations:**
  - Financial losses, reputational damage, regulatory fines.
- **Broader Trends:**
  - Increase in ransomware and cybercrime.
  - PhaaS platforms lower the barrier to entry for cybercriminals.

Key Takeaways From PhaaS

- Phishing-as-a-Service (PhaaS) democratizes cybercrime, enabling even non-technical actors to launch sophisticated attacks.
- Real-world cases like BulletProofLink demonstrate the scale, accessibility, and evolving tactics of PhaaS.

Why It Matters:

- PhaaS fuels a growing cybercrime economy, targeting individuals and enterprises globally.
- Its subscription-based model ensures a steady revenue stream for operators while increasing the frequency of attacks.



04

DDoS-for-Hire

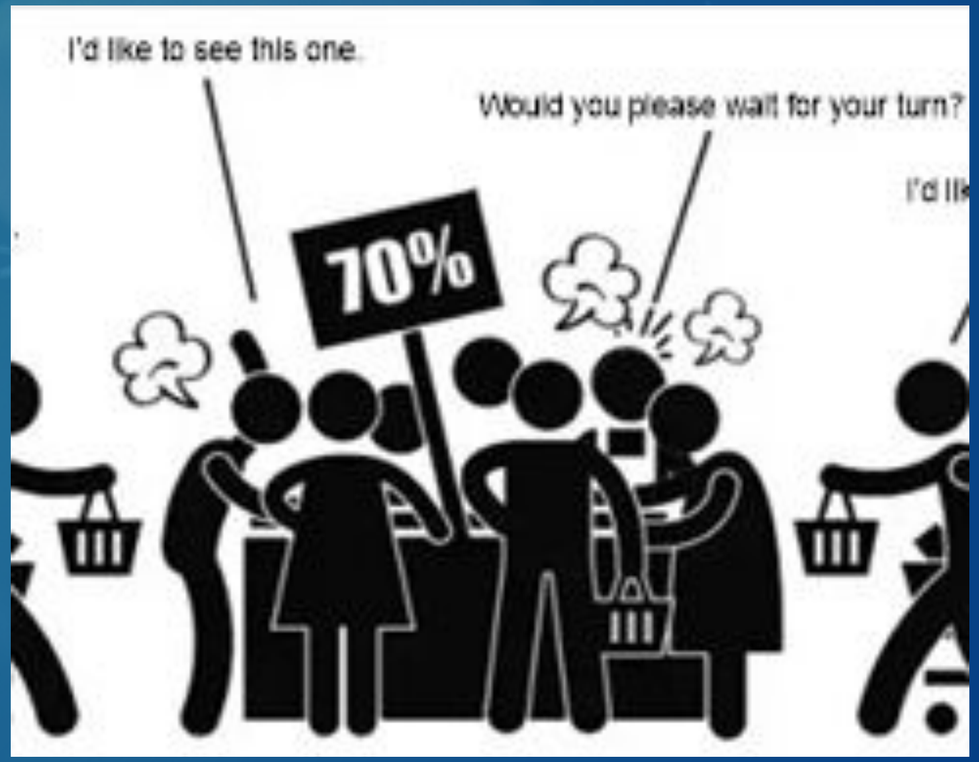
Overview of DDoS-for-Hire

What is DDoS ?

- Distributed Denial of Service (DDoS) is a type of cyberattack that floods a website with fake requests
- DDoS attacks overwhelm the target's server or network, causing it to slow down or crash.

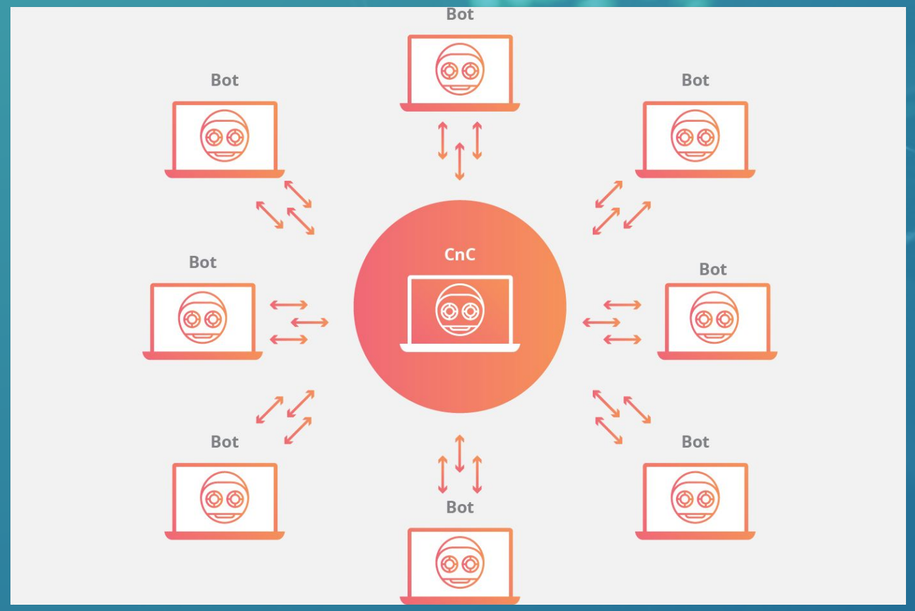
How DDoS-for-Hire works

- Cybercriminals offer DDoS attacks as a service to anyone willing to pay.
- Services are marketed on dark web forums, marketplaces, and some underground platforms.



Tools and Techniques

Botnet and Amplification Attacks



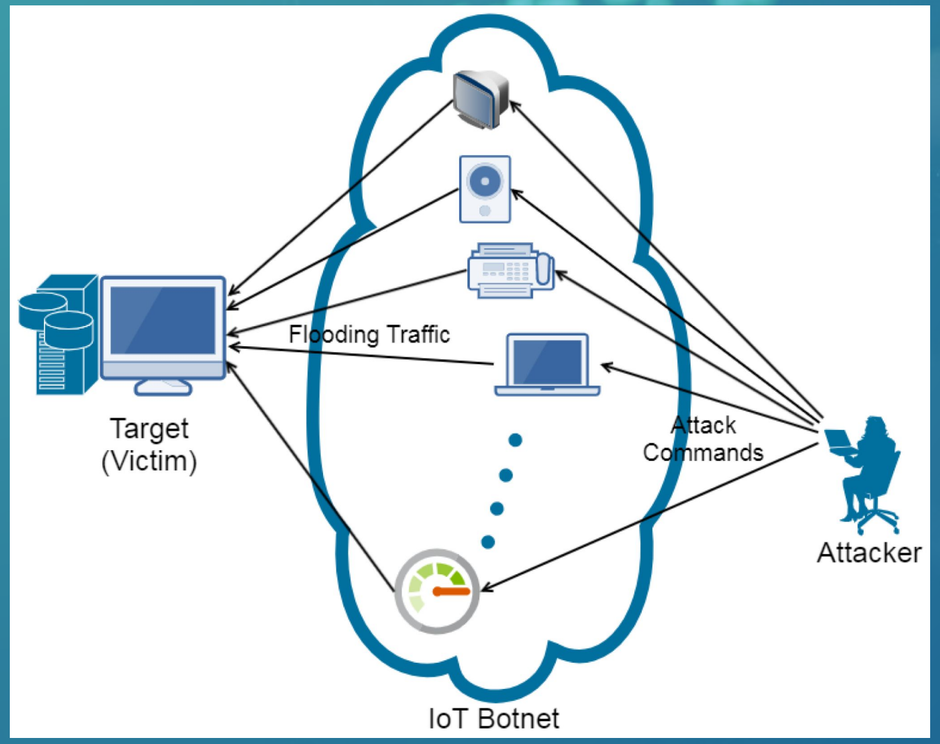
Botnet

- A botnet is a group of devices infected with malware and controlled by attackers.
- Botnets are used for harmful activities (sending spam, etc)
- Attackers create botnets by using malware, weak passwords, or system vulnerabilities.

Amplification

- Botnets use techniques to amplify attacks
- Amplification allows attackers to launch powerful attacks with little effort.

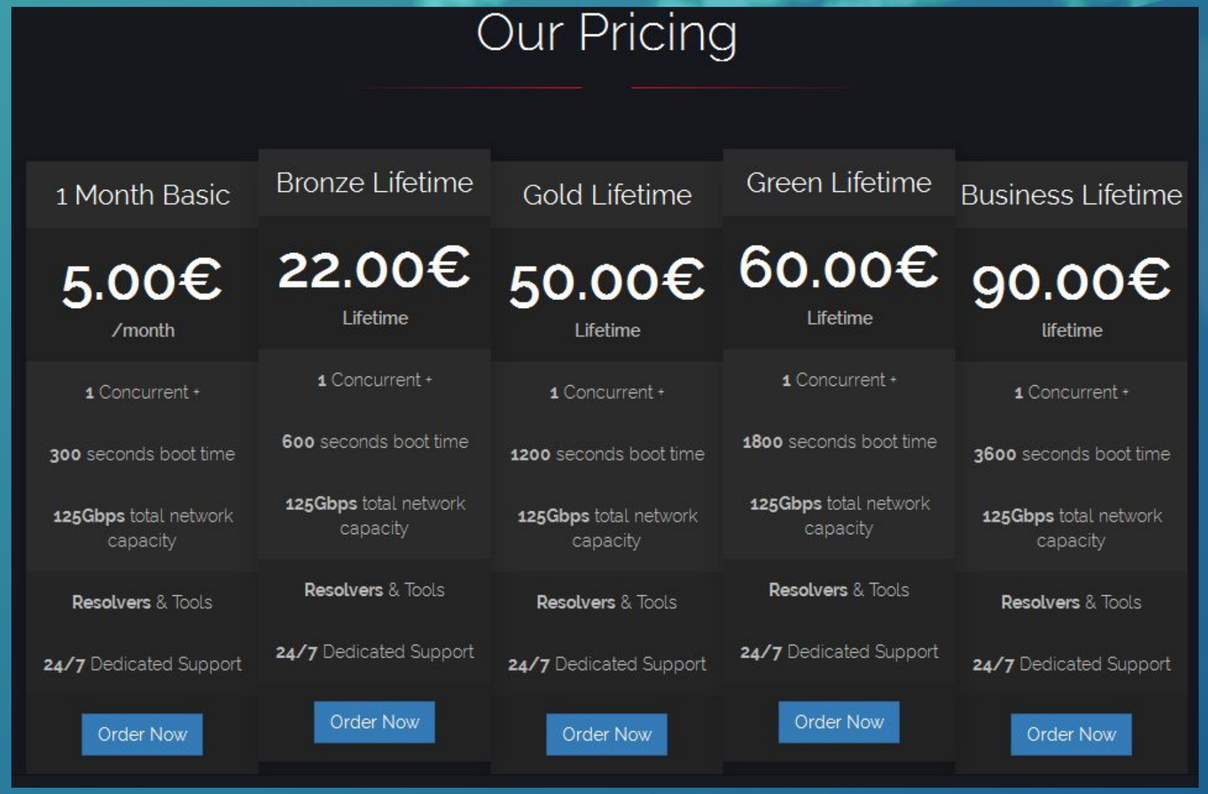
Exploitation of IoT Devices



- Many IoT devices, such as smart speakers, have weak security, using default passwords or outdated software.
- Easier for attackers to break into these devices and turn them into botnet.
- IoT devices have become a popular tool for launching DDoS attacks.

DDoS-for-Hire works:

Marketplace Dynamics



DDoS-for-Hire services typically charge based on the duration and intensity of the attack.

- Hourly Rates - Charges range from a few dollars to hundreds
- Subscription Plans - Monthly or weekly packages offering varying levels of attack capabilities.

Past Mirai Botnet Attacks

Mirai attack on **Dyn on** October 21, 2016

- The Mirai botnet launched a massive DDoS attack on DNS provider **Dyn**
- Big websites like Twitter, Netflix, and Amazon were down for most of the day.
- The attack used around 100,000 infected devices and reached a speed of 1.2 Tbps

Mitigation Strategies

1. Reduce the Attack Surface

- Restrict traffic to specific locations.
- Block outdated ports and protocols.

2. Distribute Traffic

- Use load balancers to prevent single points of failure.

3. Real-Time Threat Monitoring

- Detect anomalies quickly and respond to attacks swiftly.

4. Optimize Server Load

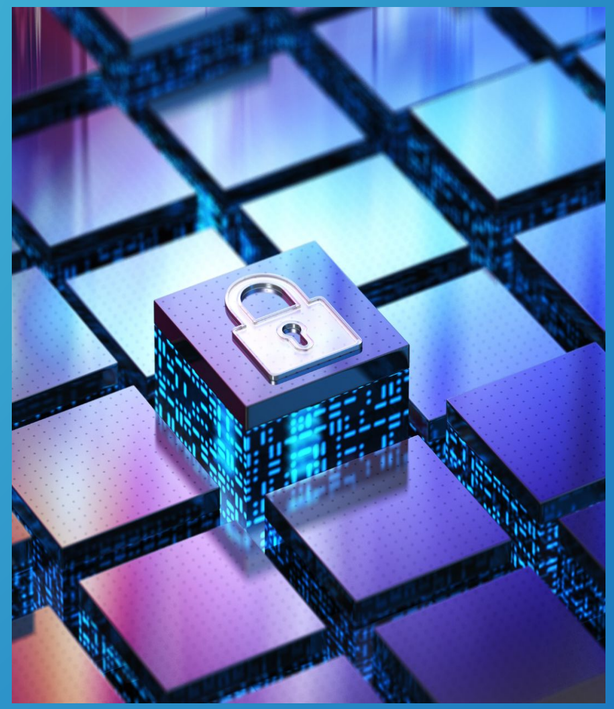
- Use caching and CDNs to reduce server strain by caching frequent content and localizing traffic.

05 Access as a Service (AaaS)

AaaS Overview

Introduction

Key Features

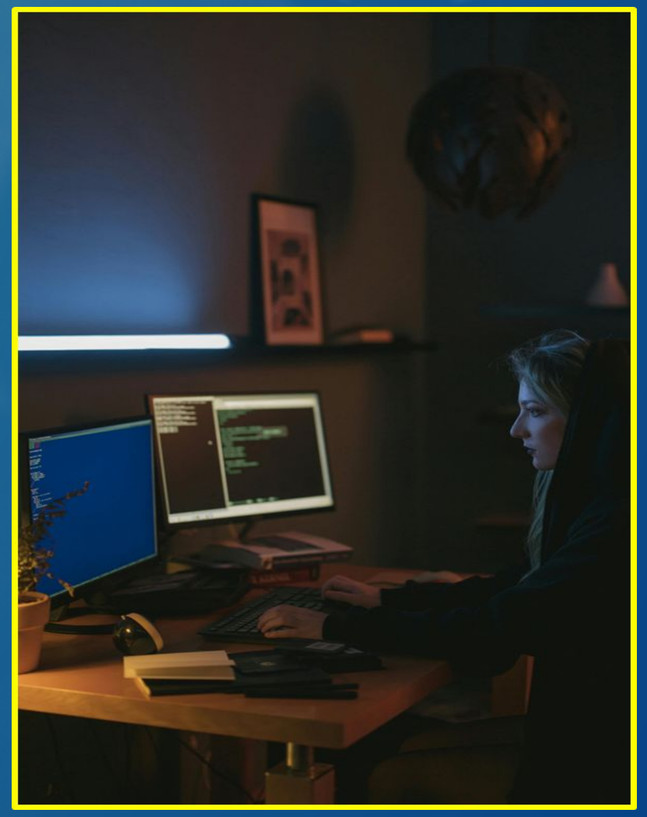


Risks & Challenges

Mitigation Strategies

AaaS Introduction

- What is AaaS (Access as a Service?)
  - Access as a Service (AaaS) is a cybercrime service model in which cybercriminals sell or rent access to compromised systems, networks, or devices. Through AaaS, even individuals or groups without advanced hacking skills can purchase ready-made access channels to carry out further malicious activities, such as data theft, extortion, or destruction.



Key Features of AaaS

- **Source of Access**
  - **Initial Attackers**: Compromising the target system or network using various attack techniques. Sell it to other criminals for profit.
  - **Exposed Credentials**: Gained through leaked usernames and password combinations. From illegal channels and resell them.

- **Types of Services**
  - **Network Access:** Provides full access to an organization's network. Criminals can infiltrate internal resources, steal sensitive data, or implant malware.
  - **Device Access:** Offer remote access to individual computers, servers, or IoT devices, allowing other criminals to control the devices for malicious purposes.
  - **VPN/RDP (Remote Desktop Protocol) Access**: Allow attackers to bypass many external defenses and gain direct access to a target's network.

- **Customer Base**
  - **Ransomware Groups**: Quick path to infiltration. Deploy ransomware to lock down data or systems for ransom.
  - **Espionage**: Including state-sponsored hackers, may purchase access to gather sensitive political, economic, or military intelligence.
  - **Data Thieves**: Steal customer information, credit card numbers, intellectual property, or business plans.

Key Features of AaaS

- **Transactions in the Dark Web**
  - List access to compromised targets in underground forums or encrypted marketplaces.
  - Provide detailed descriptions of the target, such as the size of the organization, industry type, and network structure.
  - Payments are made in cryptocurrency to keep everything anonymous.

- **Pricing Models**
  - **Target-based Pricing:** The value of the target (e.g., network size, data sensitivity) influences the price of the access.
  - **One-time Payment or Subscription:** Allowing buyers to receive updated access over time.

Risks and Challenges of AaaS

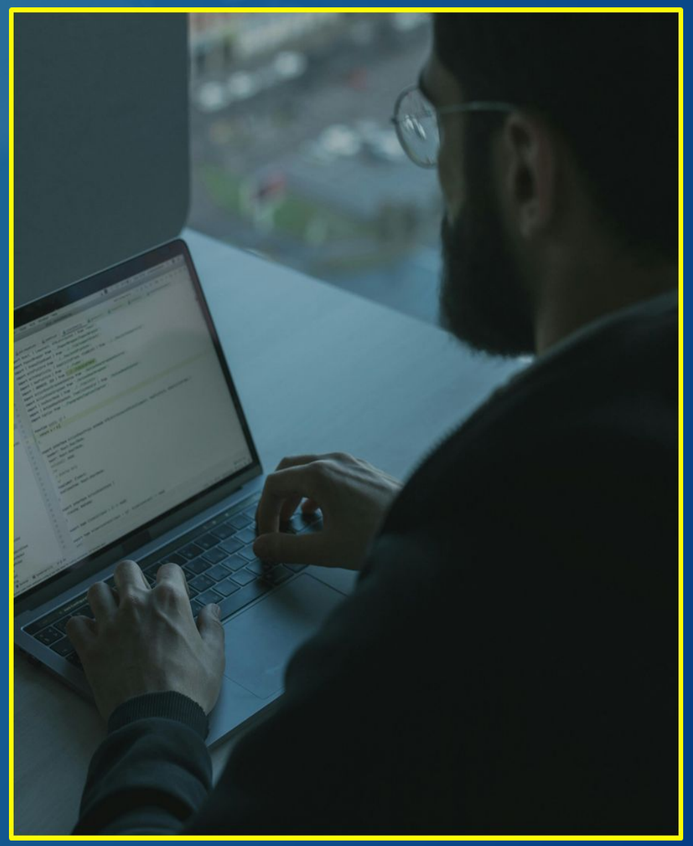
- **Scale and Industrialization of Cyberattacks**
  - Lower the barrier to launching attacks on large organizations and critical infrastructure.
  - Even lacking technical expertise can launch sophisticated attacks by purchasing access.

- **Diverse Attack Vectors**
  - Data Theft: Stealing corporate data, intellectual property, etc., to sell on the black market or demand ransom.
  - Insider Attacks: Impersonating legitimate users to carry out financial fraud, illegal transfers, and more.
  - Persistent Attacks: Maintain long-term access, repeatedly infiltrating a network by selling access over time.

- **Increased Difficulty for Law Enforcement**
  - High anonymity and global nature of AaaS.
  - Different countries and jurisdictions, making cross-border cooperation difficult.
  - Hidden nature of cybercrime complicates tracking and evidence collection.

How to Defend Against AaaS Threats

- **Multi-Factor Authentication (MFA)**
  - Organizations should enforce multi-factor authentication to protect systems and sensitive resources from password-based attacks.
- **Continuous Monitoring and Threat Detection**
  - Implement strong network monitoring and intrusion detection systems to identify and respond to suspicious activities in real time.
- **Cybersecurity Awareness Training**
  - Regularly train employees to recognize phishing emails and social engineering attacks, reducing the likelihood of successful initial intrusions.
- **Regular Credential Updates and Access Control**
  - Conduct regular audits of systems, update or remove unnecessary access rights, and enforce regular password changes for outdated credentials.



06 Countermeasures and Defense Strategies

Countermeasures Overview

- AI & Automation
- Legal Frameworks
- International Coop

- Targeted Education
- Technical Defenses
- Ecosystem Disruption

AI and Automation in Combating CaaS

- **Monitor Criminal Forums**
  - Scrape and analyze dark web discussions using NLP to identify threats in multiple languages.
- **Identify Patterns**
  - Detect behavioral patterns in payment methods, tool usage and IP activity to flag suspicious activity.
- **Automated Takedowns**
  - Automatically bring down malicious domains, dark web marketplaces, and infrastructure in collaboration with ISPs.

Legal Countermeasures

- **Criminalize Tools and Services**
  - Ban the creation, distribution and purchase of exploit kits and other CaaS tools with **clear legal penalties**.
- **Regulate Cryptocurrency**
  - Enforce stricter AML and KYC protocols at exchanges
  - Empower authorities to freeze wallets associated with illicit activities via court orders.
- **Streamlined Prosecution**
  - Create cybercrime-specific courts for faster processing of cases.
  - Align international legal guidelines and extradition processes for faster prosecution of cyber criminals.

Global Collaboration against CaaS

- **Task Forces**
  - Establish regional task forces with technical experts.
  - Coordinate with private companies for technical expertise.
- **Joint Operations**
  - Execute coordinated operations to dismantle marketplaces, seize servers, and apprehend operators.
- **Intelligence Sharing**
  - Share intel on known operators, tools and vulnerabilities using **real-time communication platforms**.

Educating Stakeholders

- **Businesses**
  - Conduct workshops, threat simulations and share industry-specific intelligence.
- **Law Enforcement**
  - Train teams in dark web investigations, blockchain analysis and malware reverse engineering.
- **Public Campaigns**
  - Launch awareness campaigns on CaaS risks, legal consequences, and victim stories.

Technical Defenses

- **Traffic Monitoring**
  - Monitor network traffic for suspicious patterns and C2 communications using IDS.
- **Harden Systems**
  - Patch systems, enforce strict access controls and deploy EDR solutions to mitigate attacks.
- **Deploy Honeypots**
  - Use honeypots to attract and study CaaS operators, sharing intelligence with the cybersecurity community.

Pulling the Plug: Ecosystem Disruption

- **Target Payments**
  - Leverage blockchain analytics to trace and block payments linked to flagged wallets.
- **Takedown Operations**
  - Take down servers, DNS records and other infrastructure hosting CaaS platforms.
- **Infiltration**
  - Infiltrate dark web marketplaces with fake profiles and data to undermine trust among operators.

Conclusion: A Coordinated Defense

- Combating CaaS requires targeted technical, legal and cooperative strategies.
- Proactive efforts can dismantle the ecosystems enabling CaaS.
- Innovation and vigilance are key to staying ahead of this evolving threat.

Thank You