

Cybercrime Ecosystems

MSCS630: Cybercrime Investigation and Digital Evidence

Dr. Mouatez Karbab



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joaan Bin Jassim Academy for Defence Studies

September 23, 2026



Outline

- 1 Understanding the Adversaries
- 2 The CaaS Ecosystem: Crime as a Product
- 3 Specialized Roles in the Cybercrime Supply Chain
- 4 Underground Marketplaces and Forums
- 5 The Illicit Data Marketplace



Introduction to Cybercrime Ecosystems I

Chapter Objectives

- Modern cybercrime is an organized business, not a hobby.
- The types of attackers at work, and what drives each.
- The Cybercrime-as-a-Service (CaaS) model that arms them.
- The specialized jobs that keep a digital attack running.

Why This Matters

- Understanding the business predicts an attacker's next move.
- It also exposes weaknesses in their operation.
- Each purchased role leaves its own trace to follow.



Outline

- 1 Understanding the Adversaries
- 2 The CaaS Ecosystem: Crime as a Product
- 3 Specialized Roles in the Cybercrime Supply Chain
- 4 Underground Marketplaces and Forums
- 5 The Illicit Data Marketplace



The Two Questions Every Investigation Asks I

- "Who did this?" and "Why did they do it?"
- *Threat actor profiling* is the method used to answer both.
- It studies an attacker's actions, tools and goals.

Why Profiling Matters

- Understanding motive lets investigators predict the next steps.
- That reveals the full size of the security incident.
- A money-driven attacker acts differently from a state's spy.



Skill Level Sets Priorities I

- Knowing the attacker's skill decides which defenses matter most.
- It also decides which investigation steps come first.
- A less skilled attacker may be stopped by basic security.
- A determined, well-funded group needs a much stronger defense [19].



Motivation Categories I

Main Reasons for Cyberattacks

- **Financial Gain:** ransomware, business email compromise, data theft.
- Financial gain drives most cybercrime.
- **Espionage:** secret information, intellectual property, state secrets.
- Espionage seeks strategic, economic or political benefit.
- **Ideology:** attacks supporting a political, social or religious cause.
- **Notoriety:** fame or respect inside hacker communities.
- **State-Directed Objectives:** sabotage, information warfare, weakening another country.
- State-directed acts are done by, or for, a government.



A Wide Range of Capability I

- Attackers vary in technical skill, resources and security practices.
- Knowing the attacker's level is important for a successful investigation.
- Four broad tiers run from amateur to state-backed.



Script Kiddies I

Definition: Script Kiddies

- Amateur attackers at the lowest skill level.
- They use tools, scripts and software made by other people.
- They look for easy targets: unpatched or poorly configured systems.
- Motivated by curiosity, attention from friends, or a wish to damage.
- Rarely a threat to a well-protected organization.
- They can still cause serious problems for unprotected targets.



Hacktivists I

Definition: Hacktivists

- People or groups attacking to support a political or social cause.
- The name combines "hacker" and "activist".
- **DDoS:** *Distributed Denial-of-Service* attacks against a target.
- **Defacement:** replacing a site's content with a political message.
- **Doxing:** leaking private data to embarrass or hurt a target.
- Groups such as Anonymous ran major campaigns against governments and companies [6].
- Their motivation is purely ideological, never financial.



Organized Crime Syndicates I

- The professional businesses of the cybercrime world.
- Focused on money, and very highly organized.
- Responsible for the biggest and most harmful cybercrimes.
- Ransomware, large phishing campaigns, banking trojans.

They Work Like Real Companies

- Managers, specialized jobs, hiring processes.
- Even customer support for their illegal services.
- Organization plus money makes them a very dangerous threat.



Nation-State Actors and APTs I

Definition: Nation-State Actor

- The most skilled attackers, often called *Advanced Persistent Threats (APTs)*.
- Funded by a government, or part of its intelligence agency or military.
- Their goal is not quick money.
- They seek long-term strategic benefit.
- Espionage, sabotage, or influence campaigns.



Speed Versus Persistence I

- Criminal groups optimise for speed.
- Espionage groups optimise for persistence.
- They favour edge devices: VPN appliances and routers.
- Those carry little security monitoring.
- They dwell on a network for months [12].



What APTs Are Known For I

Four Distinguishing Traits

- **Advanced Capabilities:** custom malware they built themselves.
- *Zero-day exploits:* flaws the software maker does not yet know.
- Advanced methods to avoid being detected.
- **Persistence:** stay inside the network for months or years.
- **Large Resources:** backed by a national government's budget.
- **Specific Targeting:** never random.
- Operations are planned against industries the government cares about.

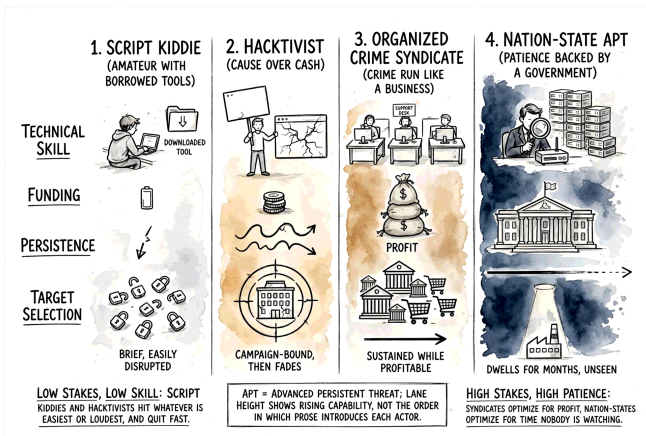


The Adversary Spectrum I

- Capability rises on every axis at once.
- Skill, funding, patience and choice of target climb together.
- From the script kiddie to the nation-state actor.
- So the way an intrusion is conducted tells you who is behind it.
- Reading rule: method and patience narrow the field of suspects.



The Adversary Spectrum I



Hands-On: Profiling from Intrusion Behaviour I

Objective

- Infer actor tier and motive from observed intrusion behaviour.

Prerequisites

- The four tiers: script kiddie, hacktivist, syndicate, nation-state.
- The five motivation categories from this section.
- Public incident write-ups with a timeline of attacker actions.



Hands-On: Profiling from Intrusion Behaviour II

Steps

- ① Pick three public incidents with published attacker timelines.
- ② For each, record dwell time, tooling origin and target selection.
- ③ Note whether tools were bought, borrowed or custom-built.
- ④ Note whether the entry point was an edge device or a user.
- ⑤ Assign a tier and a motive to each incident.
- ⑥ Write one sentence of evidence supporting each assignment.

Expected Outcome

- Long dwell plus edge devices points to espionage [12].
- Fast encryption plus rented tooling points to a criminal syndicate.



Hands-On: Profiling from Intrusion Behaviour III

Common Pitfalls

- Reading advanced tooling as proof of an advanced actor.
- Rented capability now reaches unskilled buyers.
- Confusing a noisy attack with an unskilled one.



Section 1: Assessment (1/3) I

Question 1

Which motivation best characterises a hacktivist campaign?

- A. Financial gain through extortion.
- B. Ideology supporting a political or social cause.
- C. Long-term state-directed espionage.
- D. Reselling network access to other criminals.



Section 1: Assessment (1/3) - Answer I

Question 1

Which motivation best characterises a hacktivist campaign?

- A. Financial gain through extortion.
- B. Ideology supporting a political or social cause. (✓)
- C. Long-term state-directed espionage.
- D. Reselling network access to other criminals.

Explanation:

- Hacktivist motivation is purely ideological, not financial.
- Methods are DDoS, defacement and doxing [6].



Section 1: Assessment (2/3) I

Question 2

Which behaviour most strongly suggests an espionage group rather than a criminal one?

- A. Encrypting every file within hours of entry.
- B. Posting stolen data on a leak site.
- C. Months of quiet dwell on unmonitored edge devices.
- D. Demanding payment in Monero.



Section 1: Assessment (2/3) - Answer I

Question 2

Which behaviour most strongly suggests an espionage group rather than a criminal one?

- A. Encrypting every file within hours of entry.
- B. Posting stolen data on a leak site.
- C. Months of quiet dwell on unmonitored edge devices. (✓)
- D. Demanding payment in Monero.

Explanation:

- Criminal groups optimise for speed, espionage groups for persistence.
- VPN appliances and routers carry little monitoring [12].



Section 1: Assessment (3/3) I

Question 3

What is a *zero-day exploit*?

- A. An attack launched on the day a company is founded.
- B. An exploit for a flaw the software maker does not yet know about.
- C. Malware that deletes itself after zero days.
- D. A tool available free on public forums.



Section 1: Assessment (3/3) - Answer I

Question 3

What is a *zero-day exploit*?

- A. An attack launched on the day a company is founded.
- B. An exploit for a flaw the software maker does not yet know about. (✓)
- C. Malware that deletes itself after zero days.
- D. A tool available free on public forums.

Explanation:

- No patch exists, so ordinary defenses do not apply.
- Listed among the advanced capabilities that mark an APT.



Outline

- 1 Understanding the Adversaries
- 2 The CaaS Ecosystem: Crime as a Product
- 3 Specialized Roles in the Cybercrime Supply Chain
- 4 Underground Marketplaces and Forums
- 5 The Illicit Data Marketplace



Crime Becomes a Product I

Definition: Cybercrime-as-a-Service (CaaS)

- Skilled criminals create hacking tools, systems and services.
 - They sell or rent them to other, often less skilled, criminals.
 - The illegal version of *Software-as-a-Service (SaaS)*.
- This is the most important change in the business of cybercrime.



Why CaaS Grows So Fast I

- The model made cybercrime accessible to many more people.
- It lowers the barrier for people with little technical skill.
- Little programming knowledge is needed to launch a complex attack.
- The tools are simply bought from a secret online market.

Specialization Drives the Economy

- Some criminals build tools.
- Others use the tools to attack systems.
- Others focus on making money from the attacks [14].

Not a Niche Any More

- Europol's 2026 assessment records the same structure at scale.
- The service economy is now the ordinary way cybercrime is conducted [9].



Operators and Affiliates I

Definition: Ransomware-as-a-Service (RaaS)

- The most famous and profitable part of the CaaS market.
- **Operators:** the main developer group.
- They build and manage the ransomware software.
- They also run the payment website.
- And the system for negotiating with victims.
- **Affiliates:** hired by the operators.
- Their job is to break into the victim's network.
- Then install the ransomware there.

The RaaS Affiliate Payout Model I

Algorithmic Breakdown: A Criminal Business Process

- 1 **Lease:** developer rents malware and control platform to an affiliate.
- 2 **Infect:** affiliate infects a victim network by their chosen method.
- 3 Phishing, a software weakness, or access bought from another criminal.
- 4 **Encrypt & Extort:** software encrypts files, then shows a ransom note.
- 5 The note carries a unique cryptocurrency wallet address.
- 6 **Payment:** the victim sends Bitcoin or Monero to that address.
- 7 **Split:** the payment system divides the money automatically.
- 8 Developer takes roughly 20-30%, affiliate takes roughly 70-80%.
- 9 **Launder:** both must hide the money's illegal origin.
- 10 They use cryptocurrency mixers or illegal exchanges.

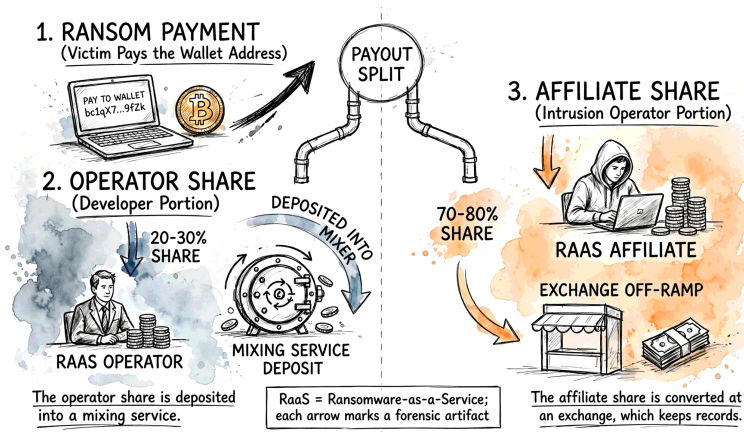


The RaaS Payout Split I

- One ransom payment becomes two money trails.
- The payout system splits the transfer before either party launders it.
- Developer and affiliate then launder separately.
- A single incident produces two divergent sets of financial artifacts.
- Investigative consequence: follow two chains, not one.



The RaaS Payout Split I



Brands Are Not Actors I

The Reading Rule

- Ransomware brands turn over quickly.
 - An investigator should not mistake a brand for an actor.
-
- LockBit became the most deployed ransomware variant in the world.
 - Operation Cronos, led by the UK National Crime Agency, ended that.
 - February 2024: its administration environment and source code were seized.
 - The action identified 194 affiliates [13].



ALPHV, RansomHub and the Same People I

- ALPHV, also called BlackCat, collapsed the following month.
- It took a \$22 million payment and kept the affiliate's share.
- An exit scam against its own workforce.
- Many of those affiliates moved to RansomHub.
- RansomHub recruited them with a 90/10 split in the affiliate's favour [16].
- The people carrying out intrusions largely stayed the same across all three names.
- So attribution to a brand answers a narrower question than it appears to.



Case Study: The Conti Leaks I

Real-World Story: The Conti Leaks

- February 2022: Conti declared support for the Russian invasion of Ukraine.
- Shortly after, a Ukrainian researcher leaked two years of private chats [15].
- What the messages describe is a company.

A Payroll, Not a Gang

- Payroll fluctuated between 65 and more than 100 salaried staff [10].
- Paid in Bitcoin on the first and the fifteenth of each month.
- Most earned between \$1,000 and \$2,000 a month.
- A Human Resources department interviewed new hires continuously [11].



Conti as a Corporate Case Study I

- The group ran performance reviews.
- It named an employee of the month [3].
- Staff complained about working for days without sleep.
- Managers ignored requests for time off.
- Units were held to budgets, and staff complained about those too.

Why It Still Matters

- Closest thing the field has to a ransomware organisational chart.
- Conti remains the standard case study of corporate crime online.



Phishing as a Packaged Product I

- *Phishing* is one of the most common ways attackers first get in.
- *Phishing-as-a-Service (PhaaS)* makes starting a campaign very easy.
- For a small price a criminal buys a complete *phishing kit*.

What a Phishing Kit Contains

- Professionally designed email templates.
 - Copies of real login pages for big companies.
 - Microsoft 365, Bank of America, DHL and similar brands.
 - A control panel to collect the stolen passwords.
-
- Selling kits lets criminals phish on a very large scale.



Loaders and Droppers for Rent I

Definition: Malware-as-a-Service (MaaS)

- Selling or renting specific types of *malware*.

Definition: Loader or Dropper

- The first piece of malware to infect a computer.
- Its only job is to get inside the victim's machine.
- Once active it downloads and runs more harmful software.
- Ransomware, spyware, or banking information stealers.



The Service Outlives the Family I

- QakBot, IcedID and Emotet long operated on this model.
- They acted as delivery systems for different organized crime groups.
- All three have since been disrupted.
- Emotet was taken down in January 2021.
- QakBot fell to Operation Duck Hunt in August 2023.
- That action reached more than 700,000 infected computers [18].
- IcedID was one of six droppers dismantled by Operation Endgame, May 2024.
- Endgame took down over 100 servers and more than 2,000 domains [8].

Investigative Consequence

- Successors appeared in each case; Latrodectus followed IcedID most directly.
- Treat a loader name as a current campaign, not a fixed adversary.



Booters and Stressers as a Product I

- *DDoS-as-a-Service (DaaS)* packages booter and stresser services.
- Chapter 1 introduced those booter and stresser services.
- A customer can often buy an attack for only a few dollars.
- Payment is made in cryptocurrency.
- Anyone can shut down a business website or silence someone online.



The Same Idea, Applied More Broadly I

- Every service so far replaces a skill a criminal would otherwise need.
- Generative and agentic AI is that idea applied more broadly.
- It has moved from criminal forum discussion to working tooling.



Bought, Not Built I

Unit 42 Investigation, September 2026

- Documents what agentic attack tooling looks like when bought [4].
- An attacker paired frontier AI models with agentic attack frameworks.
- A fortnight of operator work compressed into one overnight run.

What the Agents Did

- Carried out reconnaissance.
- Harvested credentials.
- Escalated privileges.
- Took over pipeline infrastructure.
- Applied more than fifty distinct MITRE ATT&CK techniques.

Why the Speed Was Possible I

- Not any single clever exploit.
- The agents read the output of each tool.
- They worked out what it meant.
- They chose the next step without waiting for a human.
- The pauses that normally separate intrusion stages disappeared.

What It Does to an Investigation

- A timeline too short to review.
- A decision record held off the victim's network.
- Chapter 1's machine-speed section sets this out in full.
- The capability arrives the way every other service does.
- Rented, priced, and available to a buyer who could not build it.
- The investigative method belongs to the agentic AI systems chapter.
- That covers agent execution traces and human versus machine decisions.

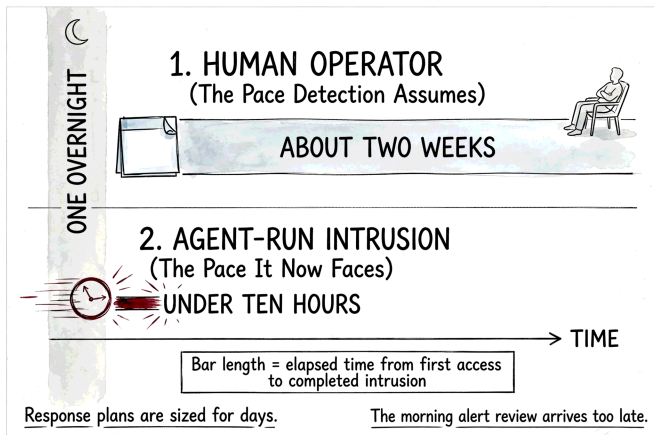


Agentic Tooling in the Chain I

- Agentic tooling enters the chain as one more rented service.
- The Unit 42 operator bought orchestration rather than skill.
- The agents supplied reconnaissance, credential access and privilege escalation.
- Separate specialists would otherwise have been hired for each [4].



Agentic Tooling in the Chain I



Hands-On: Costing a Ransom Payment I

Objective

- Trace one ransom payment through the RaaS split into two trails.

Prerequisites

- The six-step payout model from this section.
- A spreadsheet or a sheet of paper.
- The published affiliate splits for LockBit and RansomHub.



Hands-On: Costing a Ransom Payment II

Steps

- 1 Assume a \$1 million ransom paid in Bitcoin.
- 2 Split it at 20/80, then again at the RansomHub 90/10 rate [16].
- 3 List the artifacts each split produces: addresses, timestamps, amounts.
- 4 Add the laundering fee each party then pays a specialist.
- 5 Mark which artifacts a subpoena could reach.
- 6 Repeat assuming the same intrusion under a different brand name.

Expected Outcome

- Two distinct financial trails from one incident, not one.
- Changing the brand changes almost none of the artifacts.



Hands-On: Costing a Ransom Payment III

Common Pitfalls

- Treating the ransom address as the end of the money trail.
- Assuming the brand name identifies the people involved.



Section 2: Assessment (1/3) I

Question 1

In the RaaS model, what is the affiliate's job?

- A. Writing and maintaining the encryption software.
- B. Breaking into the victim network and deploying the ransomware.
- C. Running the payment and negotiation portals.
- D. Laundering the operator's share of the ransom.



Section 2: Assessment (1/3) - Answer I

Question 1

In the RaaS model, what is the affiliate's job?

- A. Writing and maintaining the encryption software.
- B. Breaking into the victim network and deploying the ransomware. (✓)
- C. Running the payment and negotiation portals.
- D. Laundering the operator's share of the ransom.

Explanation:

- Operators build the software and run the payment platform.
- Affiliates supply the intrusion and take the larger share.



Section 2: Assessment (2/3) I

Question 2

Why should an investigator avoid equating a ransomware brand with an actor?

- A. Brands are legally protected trademarks.
- B. Every brand uses identical malware.
- C. Affiliates migrate between brands while the people stay the same.
- D. Brands never appear in ransom notes.



Section 2: Assessment (2/3) - Answer I

Question 2

Why should an investigator avoid equating a ransomware brand with an actor?

- A. Brands are legally protected trademarks.
- B. Every brand uses identical malware.
- C. Affiliates migrate between brands while the people stay the same. (✓)
- D. Brands never appear in ransom notes.

Explanation:

- Operation Cronos seized LockBit and identified 194 affiliates [13].
- Those affiliates largely moved to RansomHub [16].



Section 2: Assessment (3/3) I

Question 3

What made the Unit 42 agentic intrusion so fast?

- A. A previously unknown zero-day exploit.
- B. Agents interpreted tool output and chose the next step unaided.
- C. The victim had no security software installed.
- D. The attacker had physical access to the servers.



Section 2: Assessment (3/3) - Answer I

Question 3

What made the Unit 42 agentic intrusion so fast?

- A. A previously unknown zero-day exploit.
- B. Agents interpreted tool output and chose the next step unaided. (✓)
- C. The victim had no security software installed.
- D. The attacker had physical access to the servers.

Explanation:

- The human pauses between intrusion stages disappeared.
- A fortnight of operator work ran overnight [4].

Outline

- 1 Understanding the Adversaries
- 2 The CaaS Ecosystem: Crime as a Product
- 3 Specialized Roles in the Cybercrime Supply Chain**
- 4 Underground Marketplaces and Forums
- 5 The Illicit Data Marketplace



A Supply Chain of Specialists I

- Like a legal industry, the CaaS system has a supply chain.
- It is staffed by specialists offering very specific services.
- Access, infrastructure, evasion and cash-out are separate trades.



Selling the Way In I

Definition: Initial Access Broker (IAB)

- A criminal specializing in one task only.
- Getting unauthorized access to company networks.
- They usually do not perform the final attack themselves.
- They sell the access to other criminals, such as RaaS affiliates.
- Sales happen on secret online forums.
- Price depends on the company breached and the level of control.



What an IAB Sells I

Common Access Types

- Remote Desktop Protocol (RDP) credentials.
- Active Virtual Private Network (VPN) sessions.
- *Web shells* planted on a public-facing server.
- A web shell is a malicious script controlling a web server remotely.
- Valid user accounts.
- Domain administrator accounts, the most valuable of all.



The Handoff Is Now Instant I

- Mandiant measured the gap from access event to handoff.
- 2022: a median of more than eight hours.
- 2025: 22 seconds.
- Brokers now pre-stage the buyer's preferred tooling during first infection [12].

Investigative Consequence

- Access and ransomware deployment are no longer separable phases.
- An investigation assuming time between them uses an outdated model.



Case Study: The Colonial Pipeline Attack I

Real-World Story: Colonial Pipeline, 2021

- A very destructive ransomware attack.
- It stopped fuel supplies on the U.S. East Coast.
- The attack started with one single weakness.
- The attackers worked with the DarkSide RaaS group.
- They entered using a stolen VPN username and password [5].

Why the Account Was Reachable

- The account was no longer in use but was still active.
- It was not protected by multi-factor authentication.



Colonial Pipeline: The Password Trail I

- Mandiant investigated the intrusion.
- It found the password in leaked credentials on the dark web.
- That suggests an employee reused it on another breached service.
- How the attackers themselves obtained it was never established [17].

The Lesson

- One dormant account plus one reused password.
- That grew into a national security emergency.



Bulletproof Hosting I

Definition: Bulletproof Hosting

- Companies that knowingly host malicious websites and files.
- Often located where laws against cybercrime are weak.
- They provide servers for *Command & Control (C2)* infrastructure.
- They also host phishing websites and malware.
- They are designed to ignore police takedown requests.



C2 Infrastructure Rental I

- Criminals need not build their own C2 servers.
- They rent access to existing C2 networks instead.
- Some services run C2 over legal platforms.
- Discord, Telegram and Slack are used this way.
- The attacker's traffic then looks like normal activity.
- That makes detection and identification much harder.



Crypters and Packers I

- Malware must be hidden from antivirus (AV) and EDR software.
- EDR is Endpoint Detection and Response.
- Hiding or disguising code is called *obfuscation*.

Definition: Crypter Service

- A criminal sends their malware to the service.
 - The service changes the malware's digital signature.
 - *Polymorphism* constantly changes the malware's code.
 - Goal: make the malware "Fully UnDetectable" (FUD).
 - Most security software then cannot find it.
-
- Sold per file, or through a monthly subscription.



Money Mules I

Definition: Money Mule

- A person who moves illegal money for a criminal.
- Very important for turning stolen digital money into cash.
- They are often tricked through fake job offers.
- Or through online dating scams.
- They receive stolen money in their own bank accounts.
- They then send it on, often converted into cryptocurrency.
- Each mule makes following the money back harder.



Cryptocurrency Specialists I

- Police have become better at tracking public *blockchains*.
- Bitcoin is the obvious example.
- So criminals now hire cryptocurrency laundering specialists.

Laundering Is Bought, Not Learned

- A newly paid affiliate rarely moves the money themselves.
- They hire a specialist, as they bought their access at the start.
- The specialist takes a percentage for passing the funds through.
- *Mixers* or *tumblers*, cross-chain swaps, complicit exchanges.



One More Purchased Role, One More Trail I

- Laundering is one more purchased role in the chain.
- It leaves one more trail: a fee paid, a service used, an address handed over.
- Mixing degrades a money trail but does not end it.
- Analysts routinely recover the connection anyway.
- From transaction timing, amounts and address reuse [2].
- The methods belong to the dark web and cryptocurrency chapter.

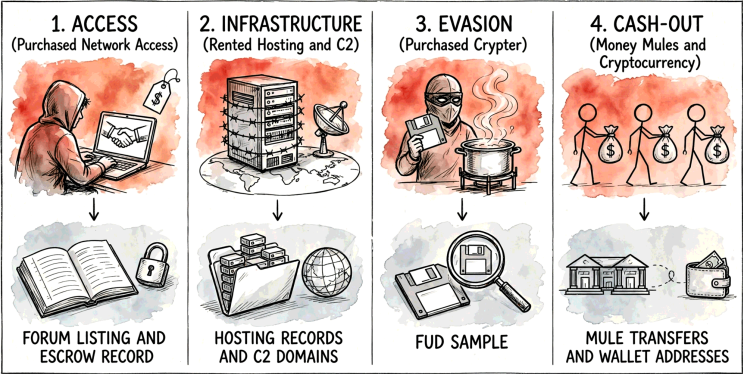


The CaaS Supply Chain I

- Every link in the chain is bought.
- Every purchase leaves a record.
- Access, infrastructure, evasion and cash-out are four transactions.
- Four separate transactions with four separate vendors.
- Each deposits an artifact an investigator can subpoena, sample or trace.



The CaaS Supply Chain I



Each role in the chain is bought from a separate vendor.

LEGEND: C2 = Command and Control; FUD = Fully Undetectable

Each purchase leaves a record an investigator can obtain.

Hands-On: Mapping Vendors to Artifacts I

Objective

- Turn each purchased role into a named, collectable artifact.

Prerequisites

- The four supply-chain stages from this section.
- The Colonial Pipeline write-up [5].
- A blank four-column table.



Hands-On: Mapping Vendors to Artifacts II

Steps

- 1 Label the columns access, infrastructure, evasion, cash-out.
- 2 Place each specialist role from this section in its column.
- 3 For each role, list the artifact its purchase leaves behind.
- 4 Mark whether it sits on the victim network or with a third party.
- 5 Name the legal instrument needed to obtain each one.
- 6 Replay the Colonial Pipeline intrusion across the same table.

Expected Outcome

- Most artifacts sit outside the victim's own network.
- Bulletproof hosting is the column with the fewest reachable artifacts.

Hands-On: Mapping Vendors to Artifacts III

Common Pitfalls

- Assuming an obfuscated sample yields nothing.
- Treating a mixer as the point where a trail ends [2].



Section 3: Assessment (1/3) I

Question 1

Which access type does an IAB price highest?

- A. A single RDP credential for a workstation.
- B. A web shell on a public-facing server.
- C. A domain administrator account.
- D. An expired VPN session.



Section 3: Assessment (1/3) - Answer I

Question 1

Which access type does an IAB price highest?

- A. A single RDP credential for a workstation.
- B. A web shell on a public-facing server.
- C. A domain administrator account. (✓)
- D. An expired VPN session.

Explanation:

- Price tracks the company breached and the level of control.
- Domain administrator rights give control of the whole network.



Section 3: Assessment (2/3) I

Question 2

What is the investigative significance of the 22-second broker handoff?

- A. Ransomware now encrypts faster than before.
- B. Access and deployment can no longer be treated as separate phases.
- C. Brokers have stopped using forums.
- D. VPN logs are no longer useful evidence.



Section 3: Assessment (2/3) - Answer I

Question 2

What is the investigative significance of the 22-second broker handoff?

- A. Ransomware now encrypts faster than before.
- B. Access and deployment can no longer be treated as separate phases. (✓)
- C. Brokers have stopped using forums.
- D. VPN logs are no longer useful evidence.

Explanation:

- The median fell from over eight hours in 2022 to 22 seconds in 2025.
- Brokers pre-stage the buyer's tooling during the first infection [12].



Section 3: Assessment (3/3) I

Question 3

What does a crypter service sell?

- A. Encrypted storage for stolen data.
- B. Cryptocurrency laundering through mixers.
- C. Obfuscation that makes malware undetectable to AV and EDR.
- D. Encrypted messaging for criminal forums.



Section 3: Assessment (3/3) - Answer I

Question 3

What does a crypter service sell?

- A. Encrypted storage for stolen data.
- B. Cryptocurrency laundering through mixers.
- C. Obfuscation that makes malware undetectable to AV and EDR. (✓)
- D. Encrypted messaging for criminal forums.

Explanation:

- Polymorphism changes the sample's digital signature.
- The goal is a "Fully UnDetectable" (FUD) file.



Outline

- 1 Understanding the Adversaries
- 2 The CaaS Ecosystem: Crime as a Product
- 3 Specialized Roles in the Cybercrime Supply Chain
- 4 Underground Marketplaces and Forums
- 5 The Illicit Data Marketplace



Where the CaaS Economy Trades I

- The whole CaaS economy rests on secret marketplaces and forums.
- They are usually hosted on the *Tor network*.
- Chapter 1's anonymity demonstration covers how that works.

What Happens There

- Criminals advertise their services.
- They sell stolen data.
- They exchange hacking tools.
- They find partners for operations.
- They imitate normal e-commerce sites such as Amazon or eBay.
- Forums for discussion, online stores for buying and selling.



Seizures: Hydra and Genesis I

- These hubs are seized regularly.
- Hydra Market was the highest-turnover illegal marketplace in the world.
- Germany's Federal Criminal Police Office shut it down in April 2022.
- The Frankfurt cybercrime prosecutors acted alongside them [1].
- Genesis Market sold packaged browser fingerprints, cookies and saved logins.
- Harvested from around 460,000 infected devices.
- Operation Cookie Monster took it down a year later.
- Thirteen countries acted, producing more than 100 arrests [7].



Why a Seizure Matters Beyond Disruption I

A Marketplace Keeps Records

- It keeps records the way any shop does.
 - A seizure converts vendor listings into an evidence set.
 - So do escrow ledgers and buyer accounts.
-
- The arrests that follow are usually of customers, not operators.



Reputation in a Market of Thieves I

- In a secret environment, anyone could be a thief.
- Reputation is therefore extremely important.

Trust Mechanisms

- **Vendor Reviews and Ratings:** buyers rate sellers.
- That creates a reputation score other customers rely on.
- **Vendor Levels:** a long, good history earns higher status.
- Higher status brings more attention and apparent trustworthiness.



Escrow Services I

Definition: Escrow Service

- A neutral third party that holds the payment.
- Offered by the marketplace for large sales.
- The buyer sends money to the escrow service.
- The service holds it until the buyer confirms delivery.
- This protects both buyer and seller from being cheated.
- For an investigator, the escrow ledger is a transaction record.



Forums as an Intelligence Source I

- For police and analysts these forums are very valuable.
- Investigators watch the communities, often using secret accounts.

What Monitoring Yields

- Early warnings about new threats.
- New *Tactics, Techniques, and Procedures (TTPs)*.
- TTPs are the methods attackers use.
- *Indicators of Compromise (IoCs)*: clues a system was attacked.
- Malicious IP addresses and domain names, for example.
- The online names and actions of important criminals.



Scope: What Belongs Where I

- This chapter covers what the forums are and why they exist.
- The tradecraft of monitoring them belongs elsewhere.
- So does the operational security it demands of the investigator.
- Both belong to the OSINT and threat intelligence chapter.



Practical Demo: Finding Spills with Google Dorks I

From Dark Web to Clear Web

- Criminal conversations and stolen data sometimes move to the public internet.
- This often happens on text-sharing sites such as Pastebin.
- Investigators use special search commands, called *Google Dorks*.

Two Example Queries

- `site:pastebin.com "BEGIN PGP PRIVATE KEY"`
 - Might find cryptographic keys accidentally made public.
 - `intext:"[Database_Dump]" filetype:sql`
 - Could find leaked SQL database files.
-
- Simple searches can connect a forum handle to real systems.
 - Or to sensitive information carelessly left public.

Hands-On: Google Dorks for Public Spills I

Objective

- Use search operators to locate data spilled onto the clear web.

Prerequisites

- A browser and a general web search engine.
- The two dork patterns from the chapter's demo.
- Written authorisation before touching any live investigation.



Hands-On: Google Dorks for Public Spills II

Steps

- 1 Run `site:pastebin.com "BEGIN PGP PRIVATE KEY"`.
- 2 Record how many results are recent versus stale.
- 3 Run `intext:"[Database_Dump]" filetype:sql`.
- 4 Vary the `site:` operator across other paste services.
- 5 For one result, list the identifiers it exposes.
- 6 Note which identifiers could link a handle to a real system.

Expected Outcome

- A short list of publicly indexed spills and their identifiers.
- A written link between at least one handle and one artifact.



Hands-On: Google Dorks for Public Spills III

Common Pitfalls

- Downloading or reusing exposed credentials, which is itself an offence.
- Searching from an attributable account during a live case.
- Treating an indexed paste as authenticated evidence without preservation.



Section 4: Assessment (1/3) I

Question 1

Beyond disruption, why does a marketplace seizure matter to an investigator?

- A. It permanently removes the vendors from the economy.
- B. It converts listings, escrow ledgers and accounts into evidence.
- C. It decrypts every Tor connection ever made.
- D. It stops all cryptocurrency payments.



Section 4: Assessment (1/3) - Answer I

Question 1

Beyond disruption, why does a marketplace seizure matter to an investigator?

- A. It permanently removes the vendors from the economy.
- B. It converts listings, escrow ledgers and accounts into evidence. (✓)
- C. It decrypts every Tor connection ever made.
- D. It stops all cryptocurrency payments.

Explanation:

- A marketplace keeps records the way any shop does.
- Operation Cookie Monster produced over 100 arrests, mostly of buyers [7].



Section 4: Assessment (2/3) I

Question 2

What did Genesis Market sell?

- A. Ransomware builders and control panels.
- B. Bulletproof hosting for C2 servers.
- C. Browser fingerprints, cookies and saved logins from infected devices.
- D. DDoS attacks priced by the minute.



Section 4: Assessment (2/3) - Answer I

Question 2

What did Genesis Market sell?

- A. Ransomware builders and control panels.
- B. Bulletproof hosting for C2 servers.
- C. Browser fingerprints, cookies and saved logins from infected devices. (✓)
- D. DDoS attacks priced by the minute.

Explanation:

- The packages were harvested from around 460,000 infected devices.
- Hydra Market, by contrast, was the highest-turnover market [1].



Section 4: Assessment (3/3) I

Question 3

What problem does a marketplace escrow service solve?

- A. It anonymises the buyer's IP address.
- B. It holds payment until the buyer confirms delivery.
- C. It launders the seller's proceeds automatically.
- D. It hosts the seller's malware.



Section 4: Assessment (3/3) - Answer I

Question 3

What problem does a marketplace escrow service solve?

- A. It anonymises the buyer's IP address.
- B. It holds payment until the buyer confirms delivery. (✓)
- C. It launders the seller's proceeds automatically.
- D. It hosts the seller's malware.

Explanation:

- A neutral third party protects both sides from being cheated.
- Its ledger becomes evidence when the market is seized.



Outline

- 1 Understanding the Adversaries
- 2 The CaaS Ecosystem: Crime as a Product
- 3 Specialized Roles in the Cybercrime Supply Chain
- 4 Underground Marketplaces and Forums
- 5 The Illicit Data Marketplace



Why the Data Market Exists I

- Stolen data is a main reason the criminal economy exists.
- Many attacks are run in order to obtain it.
- It is not merely a by-product of other attacks.
- Data is the ingredient for many illegal activities.
- From simple fraud to complex corporate spying.

What Sets the Price

- The kind of data it is.
- How new the data is.
- Whether the information is complete.



Personally Identifiable Information I

Definition: Fullz

- PII sold in packages called *fullz*.
 - Full name and address.
 - Social Security Number (SSN) or other national ID.
 - Date of birth (DOB).
-
- Used to steal someone's identity.
 - Used to file fake tax documents for refunds.
 - Used to open credit cards or loans in another person's name.



Financial Data I

- *Credit card dumps*: data stolen from in-store payment machines.
- Also called "CVV" or "CC" data.
- Stolen login details for online bank accounts.
- Sold in large quantities at a low price per card or account.
- Criminals profit through high volume rather than high margin.



Account Credentials I

- A very large market for stolen account logins.
- Streaming services such as Netflix.
- Social media accounts.
- Company email accounts and VPNs.

Definition: Infostealer

- Malware that collects credentials from an infected machine.
- The output is sold in large collections called *logs*.



Corporate and Intellectual Property I

- The most expensive part of the data market.
- Stealing and selling a company's most important secrets.
- Private computer code.
- Drug research.
- Customer lists.
- Secret documents about company mergers.

Where These Sales Happen

- Not usually on public markets.
- Private auctions at high prices instead.
- One seller and a few approved buyers.



Hands-On: Pricing a Stolen Data Set I

Objective

- Rank stolen data types by market value and explain the ranking.

Prerequisites

- The four data categories from this section.
- The three price factors: type, freshness, completeness.
- A published breach notification of your choice.



Hands-On: Pricing a Stolen Data Set II

Steps

- ① List every field the chosen breach exposed.
- ② Sort the fields into the four categories.
- ③ Score each category on type, freshness and completeness.
- ④ Decide whether the set would sell publicly or by private auction.
- ⑤ Name the fraud each category enables.
- ⑥ State which category a victim notification should prioritise.

Expected Outcome

- Fullz and intellectual property rank far above card dumps.
- Card data profits by volume, not by price per record.



Hands-On: Pricing a Stolen Data Set III

Common Pitfalls

- Judging harm by price alone.
- Ignoring freshness, which decays value quickly.
- Seeking out an actual market listing rather than reasoning from the breach notice.

Section 5: Assessment (1/3) I

Question 1

What does a *fullz* package contain?

- A. A full disk image of a victim machine.
- B. Name, address, national ID number and date of birth.
- C. A complete ransomware builder with source code.
- D. Every credential harvested from one company.



Section 5: Assessment (1/3) - Answer I

Question 1

What does a *fullz* package contain?

- A. A full disk image of a victim machine.
- B. Name, address, national ID number and date of birth. (✓)
- C. A complete ransomware builder with source code.
- D. Every credential harvested from one company.

Explanation:

- Fullz is the PII bundle used for identity theft.
- It supports fake tax filings and credit opened in another name.



Section 5: Assessment (2/3) I

Question 2

Where is stolen intellectual property usually sold?

- A. On public marketplaces at a low per-record price.
- B. Through private auctions to a few approved buyers.
- C. On Pastebin, free of charge.
- D. Bundled into infostealer logs.



Section 5: Assessment (2/3) - Answer 1

Question 2

Where is stolen intellectual property usually sold?

- A. On public marketplaces at a low per-record price.
- B. Through private auctions to a few approved buyers. (✓)
- C. On Pastebin, free of charge.
- D. Bundled into infostealer logs.

Explanation:

- Corporate secrets are the most expensive part of the market.
- High prices and few buyers keep these sales off public listings.



Section 5: Assessment (3/3) I

Question 3

Which malware type produces the collections known as *logs*?

- A. A loader or dropper.
- B. A banking trojan.
- C. An infostealer.
- D. A crypter.



Section 5: Assessment (3/3) - Answer I

Question 3

Which malware type produces the collections known as *logs*?

- A. A loader or dropper.
- B. A banking trojan.
- C. An infostealer. (✓)
- D. A crypter.

Explanation:

- Infostealers collect account credentials from infected machines.
- The harvested credentials are sold on in bulk as logs.



A Fictional but Realistic Intrusion I

- A fictional but realistic ransomware attack.
- It ties the chapter's ideas together, phase by phase.
- Each phase is set against the CaaS roles behind it.
- Five phases, each with an action and an investigation angle.



Phase 1: Initial Access & Foothold I

Action

- A mid-level affiliate of the fictional "AcmeCrypt" RaaS group.
- They browse a popular Russian-language dark web forum.
- They find a listing from a trusted **Initial Access Broker (IAB)**.
- It sells access to a mid-sized U.S. logistics company.
- The access is listed as "Domain User VPN Credentials".
- The affiliate buys it for \$1,500 in Bitcoin.
- Payment goes through the forum's escrow service.



Phase 1: Investigation Angle I

What the Investigator Asks

- Find the exact way the attacker first got in.
- Can the company's VPN logs be examined?
- Look for connections from unusual IP addresses or locations.
- Can the activity be tied to systems known to the IAB?
- Or to other criminal groups already on record?

Phase 2: Discovery & Privilege Escalation I

Action

- The affiliate uses the purchased VPN credentials to enter.
- They run a standard *reconnaissance tool* bought on the same forum.
- A reconnaissance tool explores a network and finds information.
- They use Mimikatz to steal passwords from system memory.
- After a few hours they hold a Domain Administrator *hashed password*.
- A hashed password has been scrambled for security.
- They run a program to recover the original password.
- They now have full control over the entire network.



Phase 2: Investigation Angle I

What the Investigator Does

- Analyze memory and hard drive copies.
- Look for signs of password-stealing tools.
- Look for reconnaissance scripts.
- Review Active Directory and system login records.
- Find unusual patterns of a user gaining power.
- A normal account suddenly made Domain Administrator, for example.



Phase 3: Data Exfiltration I

Action: Double Extortion

- Before deploying ransomware, the attacker uses double extortion.
- They find a file server with sensitive shipping documents.
- It also holds customer financial information.
- They copy and steal about 50 GB of data.
- It goes to cloud storage run by a **bulletproof provider**.
- That provider is known to ignore police requests.



Phase 3: Investigation Angle I

What the Investigator Does

- Check network traffic data at the internet boundary.
- NetFlow or sFlow records are the usual sources.
- Look for very large or long-lasting transfers.
- Especially to unknown or unapproved cloud storage services.
- *Data Loss Prevention (DLP)* systems may also alert.
- DLP systems are designed to stop data theft.



When Exfiltration Is the Whole Attack I

A Growing Pattern

- This phase has become the whole attack for some groups.
 - If the victim pays to keep data private, encryption adds risk without pressure.
 - So some crews exfiltrate and extort without deploying ransomware.
-
- Absence of encrypted files is not evidence that nothing happened.
 - In these cases the exfiltration is the incident.
 - Network traffic data becomes the primary evidence.
 - It is no longer merely a supporting detail.



Phase 4: Ransomware Deployment I

Action

- With the data stolen, the affiliate begins the final step.
- They use the program and scripts supplied by AcmeCrypt.
- Domain Admin powers let them use a *Group Policy Object (GPO)*.
- A GPO applies Windows settings to many computers at once.
- It pushes the ransomware to every server and workstation.
- All files are encrypted at a chosen time.
- A ransom note appears on every screen.
- It directs the victim to a Tor negotiation website.
- It threatens to release the stolen data if no ransom is paid.



Phase 4: Investigation Angle I

What the Investigator Does

- The ransomware file itself is very important evidence.
- *Reverse engineering* takes it apart to see how it works.
- It can reveal the attacker's C2 servers.
- It can reveal how the files were encrypted.
- It yields further IoCs.
- Analyzing GPO changes in Active Directory shows the deployment path.



Phase 5: Making Money & Laundering I

Action

- After a week of talks the victim agrees to pay \$1 million.
- Payment is made in Monero (XMR), a privacy-focused cryptocurrency.
- It is sent to an address the attacker provided.
- The RaaS split described earlier runs automatically.
- The affiliate then hires a **cryptocurrency specialist**.

Why Monero Changes the Problem

- Monero denies the investigator the public ledger Bitcoin would offer.
- The trail must be picked up where the specialist converts.
- *Cross-chain swaps* into Bitcoin, then mixers.
- Finally, exchange into normal money through complicit brokers.



Phase 5: Investigation Angle I

What the Investigator Does

- Hire a company specializing in blockchain analysis.
- Even privacy coins can sometimes be followed.
- Study network data for leaks.
- Find points where money crosses a regulated exchange.
- First step: identify the wallet that received the ransom.



Two Tracks Along One Timeline I

- Two clocks run along one timeline.
- Each phase generates its own evidence as it happens.
- Reconstructing the case means reading both tracks together.
- The attacker's actions on one axis.
- The artifacts they left behind on the same shared axis.



Two Tracks Along One Timeline I



Conclusion: Key Takeaways I

- **It is a business:** cybercrime runs like one because it is one.
- **CaaS:** the model that arms buyers who could not build anything.
- **Supply chain:** specialists each touch only one piece of an attack.
- **Brands are not actors:** the people outlive the name.
- **Every purchase leaves a trace:** an IAB listing, a mixer's ledger, a GPO push.
- **Marketplaces keep records:** a seizure turns a shop into an evidence set.
- **Data is the product:** price tracks type, freshness and completeness.

Next Step

- Turn to the legal and regulatory frameworks.
- They decide which traces may lawfully be collected.
- And on whose authority.

References I

- [1] Bundeskriminalamt.
Illegaler Darknet-marktplatz “Hydra Market” abgeschaltet.
Bundeskriminalamt press release, 4 2022.
Published 5 April 2022; accessed 2026-09-10.
- [2] Chainalysis Inc.
Crypto crime reaches record high in 2025 as nation-state sanctions evasion moves on-chain at scale.
The 2026 Crypto Crime Report, 1 2026.
Accessed: 2026-09-05.
- [3] CNBC.
Leaked documents show notorious ransomware group has an HR department, performance reviews and an “employee of the month”.
CNBC, 4 2022.
Published 14 April 2022; no byline recorded on the article. Accessed 2026-09-10.
- [4] Renzon Cruz, Nicolas Bareil, Eric Semaan, and Omar Jbari.
An AI-assisted cyber attack: Inside a Unit 42 investigation.
Palo Alto Networks Unit 42, 9 2026.
Accessed: 2026-09-05.



References II

- [5] Cybersecurity and Infrastructure Security Agency.
Alert (aa21-131a): Darkside ransomware: Best practices for preventing business disruption from ransomware attacks.
Technical report, CISA, 5 2021.
Accessed August 2, 2025.
- [6] Dorothy E. Denning.
The rise of hacktivism.
Georgetown Journal of International Affairs, 9 2015.
Published online 8 September 2015. The volume, issue and page range previously carried here could not be verified against the print issue and have been removed pending a library check.
- [7] Eurojust.
Online market selling stolen account credentials to criminals worldwide taken down in multi-country effort dubbed Operation Cookie Monster.
Eurojust, 4 2023.
Published 5 April 2023; accessed 2026-09-10.



References III

[8] Europol.
Largest ever operation against botnets hits dropper malware ecosystem.
Europol, 5 2024.
Operation Endgame, 27–29 May 2024; accessed 2026-09-10.

[9] Europol.
The evolving threat landscape: How encryption, proxies and artificial intelligence are expanding cybercrime.
Internet organised crime threat assessment (iocta), European Union Agency for Law Enforcement
Cooperation (Europol), 4 2026.
11th edition, published 28 April 2026; accessed 2026-09-06.

[10] Brian Krebs.
Conti ransomware group diaries, part i: Evasion.
Krebs on Security, 3 2022.
Accessed August 2, 2025.

[11] Brian Krebs.
Conti ransomware group diaries, part II: The office.
Krebs on Security, 3 2022.
Published 2 March 2022; accessed 2026-09-10.

References IV

- [12] Mandiant.
M-trends 2026: Data, insights, and strategies from the frontlines.
Technical report, Mandiant, Google Cloud, 3 2026.
Published 24 March 2026; based on over 500,000 hours of incident response in 2025. Accessed 2026-09-10.
- [13] National Crime Agency.
The NCA announces the disruption of LockBit with Operation Cronos.
United Kingdom National Crime Agency, 2 2024.
Announced 20 February 2024; accessed 2026-09-10.
- [14] David Sancho and Mayra Rosario Fuentes.
Inside the halls of a cybercrime business.
Technical report, Trend Micro Research, 4 2023.
Accessed: 2026-08-16.
- [15] Dina Temple-Raston.
Inside Conti leaks: The Panama Papers of ransomware.
The Record, Recorded Future News, 3 2022.
Published 8 March 2022; accessed 2026-09-10.

References V

- [16] Trend Micro Research.
Ransomware spotlight: RansomHub.
Trend Micro, 12 2024.
Published 20 December 2024, updated 8 August 2025; accessed 2026-09-10.
- [17] William Turton and Kartikay Mehrotra.
Hackers breached colonial pipeline using compromised password.
Bloomberg, 6 2021.
Published 4 June 2021; accessed 2026-09-10.
- [18] United States Department of Justice.
Qakbot malware disrupted in international cyber takedown.
Office of Public Affairs press release, 8 2023.
Published 29 August 2023; accessed 2026-09-10.
- [19] Verizon.
2026 data breach investigations report.
Technical report, Verizon Business, 5 2026.
Covers incidents from 1 November 2024 to 31 October 2025; accessed 2026-09-10.



Acronyms and Terminology I

APT (Advanced Persistent Threat) A common term for highly skilled, government-funded attacker groups (Nation-State Actors) known for their advanced tools and long-term, stealthy presence in a target's network.

Affiliates In the context of CaaS, these are the criminals who rent malware (like ransomware) and infrastructure from developers to carry out attacks, typically sharing a percentage of the profits.

AV (Antivirus) Software designed to detect, prevent, and remove malicious software (malware) from computer systems.

BEC (Business Email Compromise) A type of scam where an attacker tricks company employees into transferring money by impersonating a trusted executive or partner via email.

Blockchain A distributed digital ledger that publicly records all transactions for a cryptocurrency, like Bitcoin.

Botnet A network of computers infected with malware and controlled as a group by an attacker, often used to launch DDoS attacks.

Bulletproof Hosting A web hosting service that knowingly hosts malicious content (like phishing sites or C2 servers) and intentionally ignores takedown requests from law enforcement.



Acronyms and Terminology II

C2 / C&C (Command & Control) The server infrastructure an attacker uses to send commands to and receive data from infected computers (bots).

CaaS (Cybercrime-as-a-Service) An illegal business model where criminals sell or rent hacking tools, infrastructure, and services to other, often less-skilled, attackers.

Credit Card Dump A collection of raw data stolen from the magnetic stripes of credit or debit cards, typically captured from point-of-sale (POS) terminals.

Cross-chain Swap A money laundering technique where one type of cryptocurrency is exchanged for another to obscure the money trail.

Crypter A software tool or service used to encrypt or disguise malware, making it "Fully UnDetectable" (FUD) to antivirus and other security programs.

DaaS (DDoS-as-a-Service) An illegal service, also known as a "booter" or "stresser," that allows customers to pay to launch a Distributed Denial-of-Service attack against a target.

DDoS (Distributed Denial-of-Service) An attack that makes a website or online service unavailable by overwhelming it with traffic from multiple sources, often from a botnet.

DLP (Data Loss Prevention) A set of security tools and processes designed to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.



Acronyms and Terminology III

- DOB (Date of Birth)** A key piece of Personally Identifiable Information (PII) often sold in data packages called "fullz."
- Double Extortion** A ransomware tactic where attackers not only encrypt the victim's files but also steal sensitive data and threaten to leak it publicly if the ransom is not paid.
- Doxing** The act of researching and publicly broadcasting an individual's private information (like their home address or phone number) without their consent.
- EDR (Endpoint Detection and Response)** An advanced security solution that continuously monitors end-user devices (endpoints) to detect and respond to complex cyber threats in real-time.
- Escrow Service** A trusted third-party service used in underground marketplaces that holds a buyer's payment until the promised goods or services are delivered, protecting both parties from scams.
- FUD (Fully UnDetectable)** A term used by malware authors and crypter services to advertise that their malicious software can bypass all or most security products.
- Fullz** A package of stolen Personally Identifiable Information (PII) that includes enough detail (e.g., full name, address, SSN, DOB) to facilitate identity theft.
- Google Dorks** Advanced search queries using special operators to find specific information or vulnerabilities on the public internet that are not easily found with normal searches.



Acronyms and Terminology IV

GPO (Group Policy Object) A feature in Microsoft Windows Active Directory that allows an administrator to apply specific configurations to a group of users or computers. Attackers often abuse GPOs to deploy malware across an entire network at once.

Hacktivist A person or group who uses hacking techniques to promote a political agenda or social cause.

Hashed Password A password that has been transformed into a fixed-length string of characters through a one-way cryptographic function, used to securely store passwords rather than saving them in plain text.

HR (Human Resources) In the context of cybercrime, this refers to the organized "departments" within large criminal syndicates that manage recruitment, payroll, and performance of their criminal employees.

IAB (Initial Access Broker) A specialized cybercriminal who gains unauthorized access to computer networks and then sells that access to other criminals, such as ransomware affiliates.

Infostealer A type of malware specifically designed to steal sensitive information from an infected computer, such as usernames, passwords, and credit card numbers.

IoCs (Indicators of Compromise) Digital evidence or forensic data, such as an IP address, file hash, or domain name, that indicates a security breach has occurred on a system or network.



Acronyms and Terminology V

- Launder (Money Laundering)** The process of concealing the origins of illegally obtained money, typically by passing it through a complex sequence of transfers or commercial transactions.
- Loader / Dropper** A type of malware whose primary function is to gain a foothold on a victim's system and then download and execute additional, more damaging malware.
- Logs** In the context of cybercrime marketplaces, this refers to collections of stolen data, particularly user credentials, gathered from infostealer malware.
- MaaS (Malware-as-a-Service)** A business model where criminals sell or rent access to malware, such as loaders or infostealers, often via a subscription.
- Malware** Short for "malicious software," this is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- Mixer / Tumbler** A cryptocurrency laundering service that mixes potentially identifiable crypto funds with a large pool of other funds to obscure the trail back to the original source.
- Money Mule** A person who, knowingly or unknowingly, transfers or moves illegally acquired money on behalf of someone else, helping criminals convert digital currency into cash.
- Nation-State Actor** An attacker group operating on behalf of, or with direct support from, a national government to conduct espionage, sabotage, or influence operations. Also known as an APT.



Acronyms and Terminology VI

Obfuscation The technique of making malware code difficult for humans and security software to understand in order to evade detection.

PhaaS (Phishing-as-a-Service) An illegal service that provides aspiring criminals with the tools and infrastructure needed to launch phishing campaigns, including email templates and fake login pages.

Phishing A type of social engineering attack where an attacker sends fraudulent communications (e.g., emails) that appear to come from a reputable source to trick individuals into revealing sensitive information.

Phishing Kit A package sold on the dark web that includes all the components needed for a phishing attack, such as email templates, fake website code, and a control panel for collecting credentials.

PII (Personally Identifiable Information) Any data that could be used to identify a particular person, such as a name, address, or Social Security Number.

Polymorphism An advanced obfuscation technique used by malware to constantly change its own code, creating unique variants that are difficult for signature-based antivirus software to detect.

RaaS (Ransomware-as-a-Service) A CaaS model where ransomware developers lease their malware to affiliates, who then carry out the attacks. The profits from the ransom payment are split between the developers and the affiliates.



Acronyms and Terminology VII

RDP (Remote Desktop Protocol) A Microsoft protocol that allows a user to connect to and control another computer over a network connection. Stolen RDP credentials are a common way for attackers to gain initial access.

Reverse Engineering The process of deconstructing a piece of software or hardware (like malware) to understand its design, functionality, and inner workings.

SaaS (Software-as-a-Service) The legitimate business model of licensing software on a subscription basis, which the CaaS model illegally imitates.

Script Kiddie An amateur attacker with limited technical skill who uses pre-written scripts or tools created by others to launch attacks against easy targets.

SSN (Social Security Number) A unique identification number assigned to U.S. citizens, which is highly valuable data for identity theft.

Threat Actor Profiling The practice of analyzing an attacker's motivations, skills, tools, and objectives to predict their behavior and attribute attacks.

Tor Network A volunteer-operated network that enables anonymous communication by directing internet traffic through a series of relays, hiding a user's location and identity. It is often used to host underground marketplaces.



Acronyms and Terminology VIII

TTPs (Tactics, Techniques, and Procedures) A framework used to describe and analyze the behavior of a cyber attacker. TTPs detail how an adversary conducts their operations from start to finish.

VPN (Virtual Private Network) A technology that creates a secure and encrypted connection over a less secure network, such as the public internet. Stolen VPN credentials are a valuable commodity for IABs.

Website Defacement An attack on a website that changes its visual appearance, where the attacker replaces the original content with their own message.

Web Shell A malicious script uploaded to a web server that allows an attacker to execute commands and maintain remote control over the server.

XMR (Monero) A type of cryptocurrency known for its strong privacy features, which makes it a popular choice for ransom payments as it is more difficult to trace than Bitcoin.

Zero-day Exploit A cyberattack that targets a previously unknown vulnerability in a piece of software or hardware, for which no patch or fix yet exists.



Thank You!

