

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

- The types of attacker at work, and what separates them.
- The Cybercrime-as-a-Service model that arms them.
- The specialized jobs that keep a digital attack running.
- Where the marketplaces and the stolen data change hands.

Why This Matters

- Modern cybercrime is an organized business, so treat it as one.
- Knowing the structure predicts the attacker's next move.
- It also exposes the weak points in their operation.
- Every purchased service leaves its own separate trace.

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



Profiling: Who, and Why I

- Every investigation answers two questions: who did this, and why.

Definition: Threat Actor Profiling

- Studying an attacker's actions, tools and goals.
- Motive predicts the next step, and the true size of the incident.
- Skill level decides which defenses and steps matter most.
- Basic security stops an amateur; a funded group needs far more [19].

Five Motivations

- **Financial gain:** ransomware, business email compromise, data theft.
- **Espionage:** secrets and intellectual property for strategic benefit.
- **Ideology:** a political, social or religious cause.
- **Notoriety:** status and respect inside hacker communities.
- **State-directed:** sabotage, information warfare, weakening a country.



The Lower End: Amateurs and Activists I

Script Kiddies

- Amateurs running tools and scripts written by other people.
- They hunt easy targets: unpatched or badly configured systems.
- Motivated by curiosity, attention, or a wish to cause damage.
- Rarely a threat to a defended organization; serious for an undefended one.

Hacktivists

- "Hacker" plus "activist": attacks in support of a cause.
- Methods: DDoS, website defacement, and *doxing* of private data.
- Anonymous ran major campaigns against governments and companies [6].
- Motivation is purely ideological, never financial.



The Upper End: Syndicates and APTs I

Organized Crime Syndicates

- The professional businesses of cybercrime, focused on money.
- Behind the largest ransomware, phishing and banking trojan campaigns.
- They run like companies: managers, hiring, specialised jobs, support.
- Organisation plus capital makes them a very dangerous threat.

Nation-State Actors (APT)

- Funded by a government, or part of its intelligence or military.
- Not quick money: long-term espionage, sabotage, influence.
- Criminals optimise for speed; espionage groups optimise for persistence.
- They favour VPN appliances and routers, which carry little monitoring.
- They dwell on a network for months [12].
- Custom malware, *zero-day exploits*, deliberate evasion.
- Targeting is specific, never random, and set by government goals.

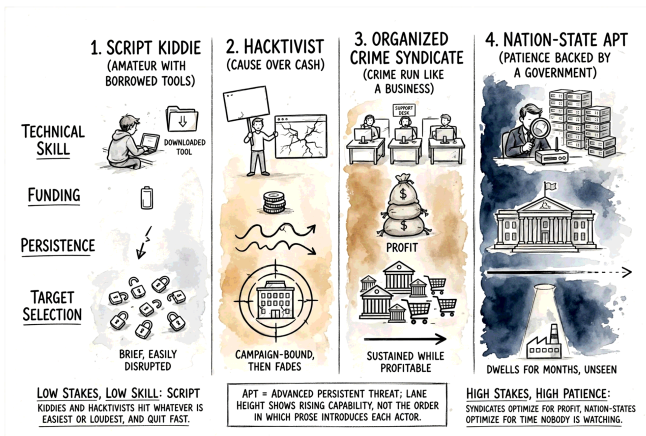


The Adversary Spectrum I

- Capability rises on every axis at once, not one at a time.
- Skill, funding, patience and target choice climb together.
- So how an intrusion is conducted says much about who ran it.



The Adversary Spectrum II



Section 1: Assessment I

Question 1

An intruder sits on a router for eight months and takes nothing. Most likely actor?

- A. Script kiddie running a downloaded scanner.
- B. Hacktivist preparing a defacement.
- C. Nation-state actor optimising for persistence.
- D. Ransomware affiliate staging an encryption run.



Section 1: Assessment - Answer I

Question 1

An intruder sits on a router for eight months and takes nothing. Most likely actor?

- A. Script kiddie running a downloaded scanner.
- B. Hacktivist preparing a defacement.
- C. Nation-state actor optimising for persistence. (✓)
- D. Ransomware affiliate staging an encryption run.

Explanation:

- Criminal crews optimise for speed; espionage groups for persistence.
- Edge devices carry little monitoring, so they are the preferred foothold [12].



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



Ransomware-as-a-Service: The Payout Model I

- The most famous and most profitable part of the CaaS market.
- **Operators:** build the malware, the payment site, the negotiation system.
- **Affiliates:** hired to break in and deploy it.

The Six Steps

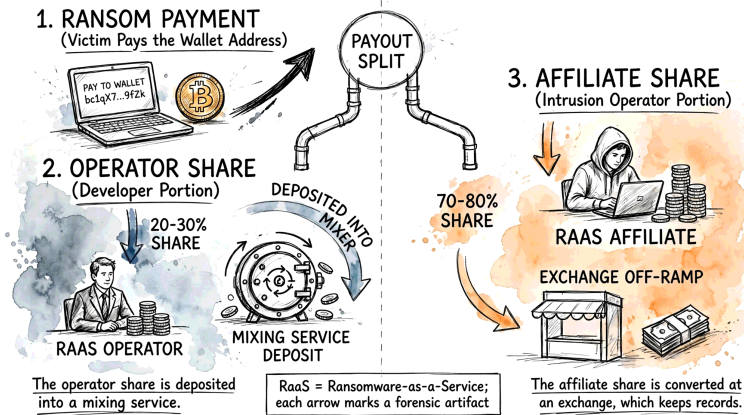
- 1 **Lease:** developer rents malware and control platform to an affiliate.
- 2 **Infect:** phishing, a software weakness, or purchased access.
- 3 **Encrypt & extort:** files encrypted, note names a unique wallet.
- 4 **Payment:** victim sends Bitcoin or Monero to that address.
- 5 **Split:** platform divides it automatically, developer 20-30%, affiliate 70-80%.
- 6 **Launder:** both sides hide the origin via mixers or illegal exchanges.

The RaaS Payout I

- One ransom payment becomes two money trails.
- The split happens before either side launders anything.
- So a single incident yields two divergent sets of financial artifacts.



The RaaS Payout II



Brands Turn Over; the People Do Not I

- **Decision rule:** never mistake a ransomware brand for an actor.

Three Names, Largely One Workforce

- LockBit was the most deployed variant in the world.
- Operation Cronos, led by the UK's National Crime Agency, ended that.
- February 2024: admin environment and source code seized, 194 affiliates identified [13].
- ALPHV (BlackCat) collapsed the next month after a \$22 million payment.
- It kept the affiliate's share: an exit scam against its own workforce.
- Affiliates moved to RansomHub, recruited on a 90/10 split [16].

Investigative Consequence

- The intruders stayed largely the same across all three names.
- Attribution to a brand answers a narrower question than it looks.



Real-World Story: The Conti Leaks I

February 2022

- Conti declared support for the Russian invasion of Ukraine.
- A Ukrainian researcher leaked roughly two years of private chats [15].
- What the messages describe is a company.

The Payroll of a Ransomware Business

- 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].
- Performance reviews, and an employee of the month [3].
- Staff complained about sleepless weeks, refused leave and unit budgets.

- The closest thing the field has to an org chart of a ransomware business.



Phishing, Malware and DDoS as Products I

PhaaS: Phishing-as-a-Service

- A cheap *phishing kit* contains the whole campaign.
- Email templates, cloned login pages, a panel to collect passwords.
- Selling kits puts phishing on an industrial scale.

MaaS: Malware-as-a-Service

- Most often a *loader* or *dropper*: first stage only.
- Its job is to get in, then pull down ransomware, spyware or a banker.
- QakBot, IcedID and Emotet all ran on this model.
- Emotet fell in January 2021.
- Operation Duck Hunt reached QakBot and 700,000 infected machines [18].
- Operation Endgame took IcedID with 100+ servers and 2,000+ domains [8].



Phishing, Malware and DDoS as Products II

The Service Outlives the Family

- Successors appeared in every case; Latrodectus followed IcedID.
- Treat a loader name as a current campaign, not a fixed adversary.
- **DaaS**: booter and stresser services packaged as a product.
- A few dollars in cryptocurrency buys an attack on any website.



Agentic AI Joins the Supply Chain I

- Every service so far replaces a skill the criminal would need.
- Agentic AI is that same idea, applied much more broadly.
- It has moved from forum talk to working, rentable tooling.

Unit 42, September 2026

- Frontier models paired with attack-specific agentic frameworks [4].
- A fortnight of operator work compressed into one overnight run.
- Reconnaissance, credential harvesting, privilege escalation, pipeline takeover.
- More than fifty distinct MITRE ATT&CK techniques applied.



Agentic AI Joins the Supply Chain II

Why It Was Fast

- No single clever exploit was responsible.
- Agents read each tool's output and chose the next step alone.
- The human pauses between intrusion stages simply disappeared.
- Chapter 1 covers what that does to a timeline and a decision record.
- The investigative method belongs to the chapter on agentic attacks.

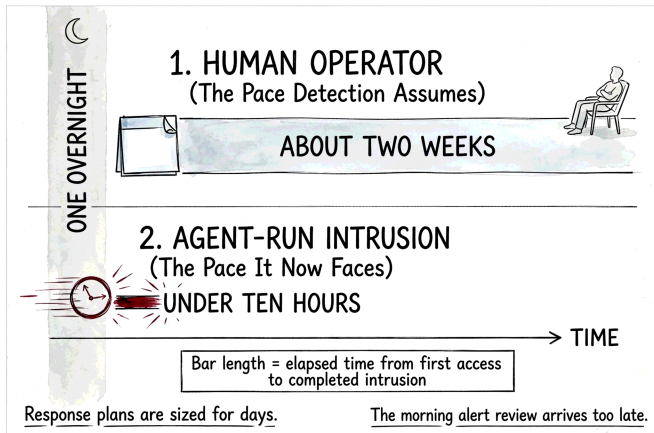


Machine Speed as a Rented Service I

- Agentic tooling enters the chain as one more rented service.
- The operator bought orchestration rather than skill.
- The agents did the work separate specialists would have been hired for.



Machine Speed as a Rented Service II



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



Initial Access Brokers I

Definition: Initial Access Broker (IAB)

- Specialists in one task: unauthorized access to company networks.
- They rarely run the final attack; they resell the access.
- Buyers are RaaS affiliates and others, on closed forums.
- Price depends on the victim and the level of control obtained.
- **What is sold:** RDP credentials; active VPN sessions.
- *Web shells* planted on a public-facing server.
- Valid user accounts, and most valuable, domain administrator accounts.

The Handoff Is Now Instant

- Mandiant measured a median of eight hours to handoff in 2022.
- In 2025 the same median was 22 seconds [12].
- Brokers pre-stage the buyer's preferred tooling during the first infection.
- Treating access and deployment as separable phases no longer holds.



Real-World Story: Colonial Pipeline I

2021: One Credential, One National Emergency

- Ransomware stopped fuel supply on the U.S. East Coast.
- The attackers worked with the DarkSide RaaS group.
- Entry was a stolen username and password for a VPN account [5].
- The account was dormant but still active, with no multi-factor authentication.

What the Investigation Found

- Mandiant found the password in leaked credentials on the dark web.
- That suggests reuse on another service breached earlier.
- How the attackers obtained it was never established [17].
- One dormant account plus one reused password reached national scale.



Infrastructure and Evasion for Hire I

Bulletproof Hosting

- Providers who knowingly host malicious sites and files.
- Usually based where cybercrime law is weak.
- They serve C2 infrastructure, phishing pages and malware.
- Designed from the start to ignore police takedown requests.

Command & Control Rental

- Rent an existing C2 network instead of building one.
- Some services run C2 over Discord, Telegram or Slack.
- Attacker traffic then looks like ordinary business activity.



Infrastructure and Evasion for Hire II

Crypters and Packers

- *Obfuscation* to defeat antivirus and EDR detection.
- *Polymorphism* constantly rewrites the malware's code.
- That changes its signature; the goal is "Fully UnDetectable".
- Sold per file, or on a monthly subscription.



Cashing Out: Mules and Laundering I

Money Mules

- People who move illegal money using their own bank accounts.
- Often recruited by fake job offers or romance scams.
- They receive stolen funds, then forward them, often as cryptocurrency.
- Each mule adds a hop between the money and the principals.

Laundering Is Bought, Not Learned

- Police now track public *blockchains* well, so specialists are hired.
- An affiliate rarely moves their own money.
- The specialist takes a percentage for *mixers*, swaps, complicit exchanges.
- It is one more purchased role, so 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 [2].
- Timing, amounts and address reuse routinely recover the link.

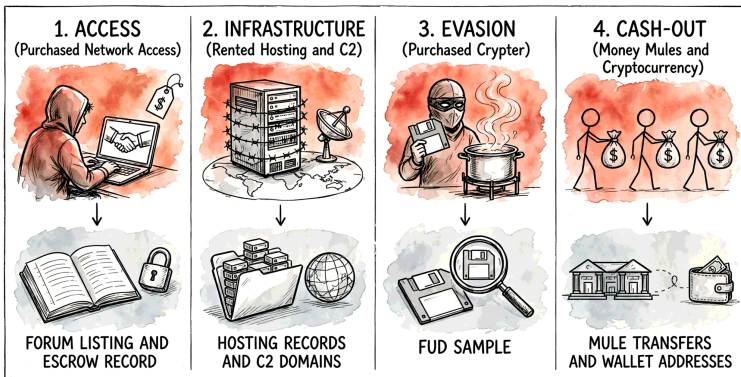


The CaaS Supply Chain I

- Every link in the chain is bought, and every purchase leaves a record.
- Access, infrastructure, evasion and cash-out: four vendors, four transactions.
- Each one deposits an artifact to subpoena, sample or trace.



The CaaS Supply Chain II



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.



34 / 68

Section 3: Assessment - Answer I

Question 1

Why does the 22-second broker handoff median change how an incident is scoped?

- A. It proves the broker and the affiliate are the same person.
- B. Initial access and deployment can no longer be treated as separate phases. (✓)
- C. It means VPN logs are no longer worth collecting.
- D. It shows ransomware is now deployed without any human involvement.

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].
- Two actors remain, but no useful time separates their work.



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 Hubs, and What Their Seizure Yields I

- The CaaS economy runs on hidden marketplaces and forums.
- Usually hosted on the *Tor network*, as Chapter 1 demonstrated.
- Criminals advertise services, sell stolen data, trade tools, find partners.
- They are structured like Amazon or eBay: forums plus storefronts.

Two Seizures

- Hydra Market was the highest-turnover illegal marketplace in the world.
- Germany's BKA and the Frankfurt prosecutors shut it down in April 2022 [1].
- Genesis Market sold browser fingerprints, cookies and saved logins.
- Harvested from roughly 460,000 infected devices.
- Operation Cookie Monster: thirteen countries, 100+ arrests [7].



The Hubs, and What Their Seizure Yields II

Why a Seizure Matters Beyond Disruption

- A marketplace keeps records the way any shop does.
- Seizure converts listings, escrow ledgers and buyer accounts into evidence.
- The arrests that follow are usually of customers, not operators.



Trust, and What the Forums Give an Investigator I

Building Trust Among Criminals

- **Vendor reviews:** buyer ratings build a public reputation score.
- **Vendor levels:** a long clean history earns higher status.
- **Escrow:** a neutral third party holds payment until delivery.
- Escrow protects both sides, and leaves the marketplace a ledger.

Investigative Value

- Early warning of new threats, gathered from covert accounts.
- New *TTPs*: the tactics, techniques and procedures in use.
- *IoCs*: malicious IP addresses, domains and other clues.
- The online names and activity of significant criminals.
- The tradecraft of monitoring them belongs to the OSINT chapter.

Practical Demo: Finding Spills with Google Dorks I

- Criminal chatter and stolen data often leak to the clear web.
- Paste sites such as Pastebin are the common landing place.
- *Google dorks* are search operators that find that public data.

```
site:pastebin.com "BEGIN PGP PRIVATE KEY"  
intext:"[Database_Dump]" filetype:sql
```

- The first may surface cryptographic keys published by accident.
- The second may surface leaked SQL database dumps.
- Either can tie a forum handle to real infrastructure or real data.

Section 4: Assessment I

Question 1

Beyond disruption, what does seizing an underground marketplace give investigators?

- A. The private keys of every vendor's cryptocurrency wallet.
- B. Vendor listings, escrow ledgers and buyer accounts as an evidence set.
- C. Automatic jurisdiction over every country the buyers live in.
- D. The identity of the marketplace's operators, by design.

Section 4: Assessment - Answer I

Question 1

Beyond disruption, what does seizing an underground marketplace give investigators?

- A. The private keys of every vendor's cryptocurrency wallet.
- B. Vendor listings, escrow ledgers and buyer accounts as an evidence set. (✓)
- C. Automatic jurisdiction over every country the buyers live in.
- D. The identity of the marketplace's operators, by design.

Explanation:

- A marketplace keeps commercial records like any shop.
- Genesis Market's takedown produced more than 100 arrests [7].
- Those arrests are usually of customers rather than operators.



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



Data Is the Product, Not the By-Product I

- Stolen data is a main reason the criminal economy exists.
- Many attacks are run to obtain it, not producing it incidentally.
- It is the raw ingredient for fraud through to corporate espionage.
- Price depends on the type, the freshness and the completeness.

Personally Identifiable Information (PII)

- Sold in packages called *fullz*.
- Full name, address, national ID or SSN, date of birth.
- Used for identity theft, fake tax refunds, fraudulent credit.

Financial Data

- *Credit card dumps* lifted from in-store payment terminals.
- Also called "CVV" or "CC" data, plus online banking logins.
- Sold cheap in bulk; the profit comes from volume.



Credentials and Corporate Secrets I

Account Credentials

- A very large market: streaming, social media, corporate mail, VPNs.
- Harvested by *infostealer* malware.
- Resold in bulk collections known as *logs*.

Corporate and Intellectual Property

- The most expensive part of the data market.
- Source code, drug research, customer lists, merger documents.
- Rarely sold on public markets at all.
- Private auctions, high prices, one seller and a few vetted buyers.
- So the absence of a public listing is not evidence of no sale.



Section 5: Assessment I

Question 1

Stolen source code and merger documents rarely appear on public criminal markets. Why?

- A. Such data has little resale value.
- B. It is traded in private auctions between vetted buyers at high prices.
- C. Marketplaces forbid listing corporate data.
- D. Infostealer malware cannot collect files of that size.



Section 5: Assessment - Answer I

Question 1

Stolen source code and merger documents rarely appear on public criminal markets. Why?

- A. Such data has little resale value.
- B. It is traded in private auctions between vetted buyers at high prices. (✓)
- C. Marketplaces forbid listing corporate data.
- D. Infostealer malware cannot collect files of that size.

Explanation:

- Corporate IP is the most expensive category in the data market.
- Bulk PII and card data sell publicly; secrets sell privately.
- No public listing therefore does not mean no sale occurred.



Phases 1 to 3: Access, Escalation, Exfiltration I

Phase 1: Initial Access & Foothold

- An affiliate of the fictional "AcmeCrypt" RaaS group browses a dark web forum.
- A trusted IAB lists "Domain User VPN Credentials" for a U.S. logistics firm.
- The affiliate pays \$1,500 in Bitcoin through the forum's escrow.
- **Investigate:** VPN logs for unusual source addresses and locations.
- Can the activity be tied to infrastructure known to be the IAB's?

Phase 2: Discovery & Privilege Escalation

- A purchased *reconnaissance tool* maps the internal network.
- Mimikatz pulls a Domain Administrator *hashed password* from memory.
- Cracked within hours, giving full control of the network.
- **Investigate:** memory and disk images for credential and recon tooling.
- Active Directory logs for a normal user suddenly made Domain Admin.



Phases 1 to 3: Access, Escalation, Exfiltration II

Phase 3: Data Exfiltration (Double Extortion)

- Roughly 50 GB of shipping and customer financial data copied out.
- Sent to cloud storage on a **bulletproof provider** that ignores police.
- **Investigate:** NetFlow or sFlow at the internet edge.
- Look for large or long transfers to unapproved cloud services; DLP may alert.

Exfiltration Is Increasingly the Whole Attack

- If the victim pays to keep data private, encryption adds risk without pressure.
- Some crews now extort without ever deploying ransomware.
- No encrypted files is not evidence that nothing happened.
- Network traffic data becomes the primary evidence, not a supporting detail.



Phases 4 and 5: Deployment and Cash-Out I

Phase 4: Ransomware Deployment

- The affiliate uses AcmeCrypt's binary and deployment scripts.
- Domain Admin rights push it via a *Group Policy Object* to every host.
- Files encrypt at a set time; notes point to a Tor negotiation site.
- The note also threatens to publish the stolen data.
- **Investigate:** the binary is key evidence. Reverse engineering yields C2, crypto, IoCs.
- Active Directory GPO change logs show how it was distributed.

Phase 5: Making Money & Laundering

- After a week of talks, the victim pays a \$1 million ransom in Monero.
- The RaaS split runs automatically, as earlier in the chapter.
- The affiliate then hires a **cryptocurrency specialist**.
- Monero denies the investigator the public ledger Bitcoin would have offered.
- *Cross-chain swaps* into Bitcoin, then mixers, then complicit brokers.



Phases 4 and 5: Deployment and Cash-Out II

Where the Trail Restarts

- Pick it up where the specialist converts, not where the victim paid.
- Engage a blockchain analysis firm; even Monero is sometimes traceable.
- Study network data, and the points where funds touch a regulated exchange.
- First step: identify the wallet that received the original payment.



The Two-Track Intrusion Timeline I

- Two clocks run along one timeline.
- Each phase generates its own evidence at the moment it happens.
- Reconstruction means reading actions and artifacts against one shared axis.



The Two-Track Intrusion Timeline II



Conclusion: Key Takeaways I

- **It is a business:** CaaS plus a supply chain of narrow specialists.
- **Each specialist touches one piece:** nobody runs the whole attack.
- **Every piece leaves a trace:** an IAB listing, a mixer ledger, a GPO push.
- **Sophistication is one axis:** skill, funding and patience move together.
- **Brands are not actors:** LockBit, ALPHV and RansomHub shared people.
- **Speed collapsed:** handoff in seconds, and agents that need no operator.

Next Step

- Which traces may be lawfully collected, and on whose authority.
- Move to the legal and regulatory frameworks.

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.



- 56 / 68

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.



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!