C

Crimeware: Definition, Examples, and Protection

Crimeware is software or tooling designed to facilitate profit-driven cybercrime. Learn how it differs from malware, common examples, the criminal ecosystem, and how to respond.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Crimeware vs malware and cybercrime
02 Common types of crimeware
03 How the crimeware ecosystem works
04 A typical crimeware attack chain
05 Warning signs
06 What to do after a suspected crimeware infection
07 How to protect against crimeware
08 Frequently asked questions
09 References

Crimeware is software or a set of tools designed to facilitate or automate financially motivated cybercrime. It can steal credentials and payment data, take over accounts, extort victims, redirect transactions, operate botnets, or provide other criminals with access to compromised systems.

Crimeware is defined mainly by criminal purpose and business use, not by one technical behavior. It includes malware families as well as phishing kits, credential-testing tools, botnet panels, and services that support fraud.

01 Crimeware vs malware and cybercrime

Term	Definition	Example
Malware	Software created or used to harm, disrupt, spy, or gain unauthorized access	A Trojan, wiper, worm, or ransomware payload
Crimeware	Tools used to automate or enable profit-driven digital crime	An information stealer sold with a control panel
Cybercrime	The broader illegal activity involving computers, accounts, networks, or data	Account takeover, fraud, extortion, or data trafficking
Malware-as-a-Service	A commercial model that rents malware capability or infrastructure	A subscription to a stealer builder or ransomware operation

Many malware families are crimeware, but not all malware is best described that way. Espionage tools and destructive wipers may pursue strategic or political objectives rather than direct profit. Crimeware can also include infrastructure and automation that are not themselves installed on a victim's device.

02 Common types of crimeware

- **Information stealers and keyloggers** collect passwords, cookies, payment details, cryptocurrency wallets, and documents.

- **Banking Trojans** manipulate online banking sessions, forms, or transactions.
- **Ransomware and extortion tools** encrypt data or support threats to publish stolen information.
- **Botnet malware** turns devices into remotely controlled resources for spam, fraud, attacks, or proxying.
- **Phishing kits** reproduce login pages and send captured credentials to an operator.
- **Credential-stuffing and checking tools** test stolen username-password pairs at scale.
- **Point-of-sale and payment skimmers** capture card data from terminals or online checkout pages.
- **Loaders and access brokers' tooling** establish entry that is sold or used for later attacks.

03 How the crimeware ecosystem works

Modern operations divide work among specialized roles. A developer creates a stealer, loader, or phishing kit. Infrastructure providers supply hosting, proxy networks, or bulletproof services. Distributors deliver the payload through spam, malicious advertising, fake software, or compromised sites. Initial-access brokers sell working access. Other actors monetize stolen accounts, data, cryptocurrency, or ransomware victims.

Forums, marketplaces, affiliate programs, and service subscriptions lower the technical barrier for attackers. This business structure is why disrupting one executable or server may not end the campaign.

04 A typical crimeware attack chain

1. **Targeting and delivery:** phishing, malicious ads, fake updates, cracked software, credential reuse, or vulnerability exploitation.
2. **Execution and persistence:** a loader runs, changes startup settings, or abuses legitimate system tools.
3. **Collection:** credentials, cookies, documents, payment data, or system access are gathered.

4. **Control and transfer:** data or commands move through attacker infrastructure.
5. **Monetization:** accounts are abused or sold, payments diverted, data extorted, or access resold.

05 Warning signs

- Unexpected password-reset messages, multifactor prompts, or account logins.
- New mailbox forwarding rules, payment beneficiaries, browser extensions, or remote-access tools.
- Security alerts for stealers, banking Trojans, loaders, bots, keyloggers, or ransomware.
- Transactions, cryptocurrency transfers, advertisements, or messages you did not authorize.
- Security tools disabled, new exclusions, persistent startup items, or unexplained network traffic.

Some crimeware is intentionally quiet. Identity, financial, email, and network monitoring may reveal the attack before the endpoint user notices anything.

06 What to do after a suspected crimeware infection

1. Isolate the affected device if malware execution or remote access is suspected.
2. Preserve alerts, timestamps, messages, transaction details, paths, hashes, and logs.
3. From a clean device, revoke sessions and tokens and change exposed passwords. Replace API keys, certificates, and other stored secrets where necessary.
4. Contact banks, payment providers, cryptocurrency services, or merchants immediately about unauthorized activity. Speed matters for possible holds or recovery.
5. Scan and investigate for persistence, secondary payloads, data access, and lateral movement. Rebuild systems when trust cannot be restored.
6. Report the crime to the appropriate law-enforcement, fraud-reporting, insurer, regulator, or organizational contacts.

Keep receipts and a timeline. Do not pay a supposed recovery agent or criminal without independent validation; fraud victims are commonly targeted again.

07 How to protect against crimeware

- Use unique passwords in a reputable password manager and phishing-resistant multifactor authentication.
- Patch operating systems, browsers, internet-facing services, and business applications promptly.
- Download software only from verified sources and avoid cracks, fake updates, and unexpected attachments.
- Apply least privilege, separate administrative accounts, and restrict execution from user-writable paths.
- Monitor identity, endpoint, email, network, and payment systems together.
- Maintain tested offline or immutable backups and a practiced incident-response plan.
- For organizations, verify payment changes through a separate trusted channel.

08 Frequently asked questions

Is crimeware a virus?

Crimeware is a broader category based on criminal purpose. A virus can be used as crimeware, but stealers, phishing kits, bots, and fraud tools do not all behave like viruses.

What does Crimeware-as-a-Service mean?

It describes criminal capabilities rented or sold with support, updates, infrastructure, or affiliate arrangements, making attacks accessible to customers who did not develop the tools.

Can antivirus stop crimeware?

Endpoint protection is important, but crimeware also abuses passwords, cloud accounts, social engineering, and legitimate tools. Layered identity, email, network, financial, and backup controls are needed.

09 References

- Kaspersky: What is crimeware?
- Canadian Centre for Cyber Security: Introduction to the cyber threat environment

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com