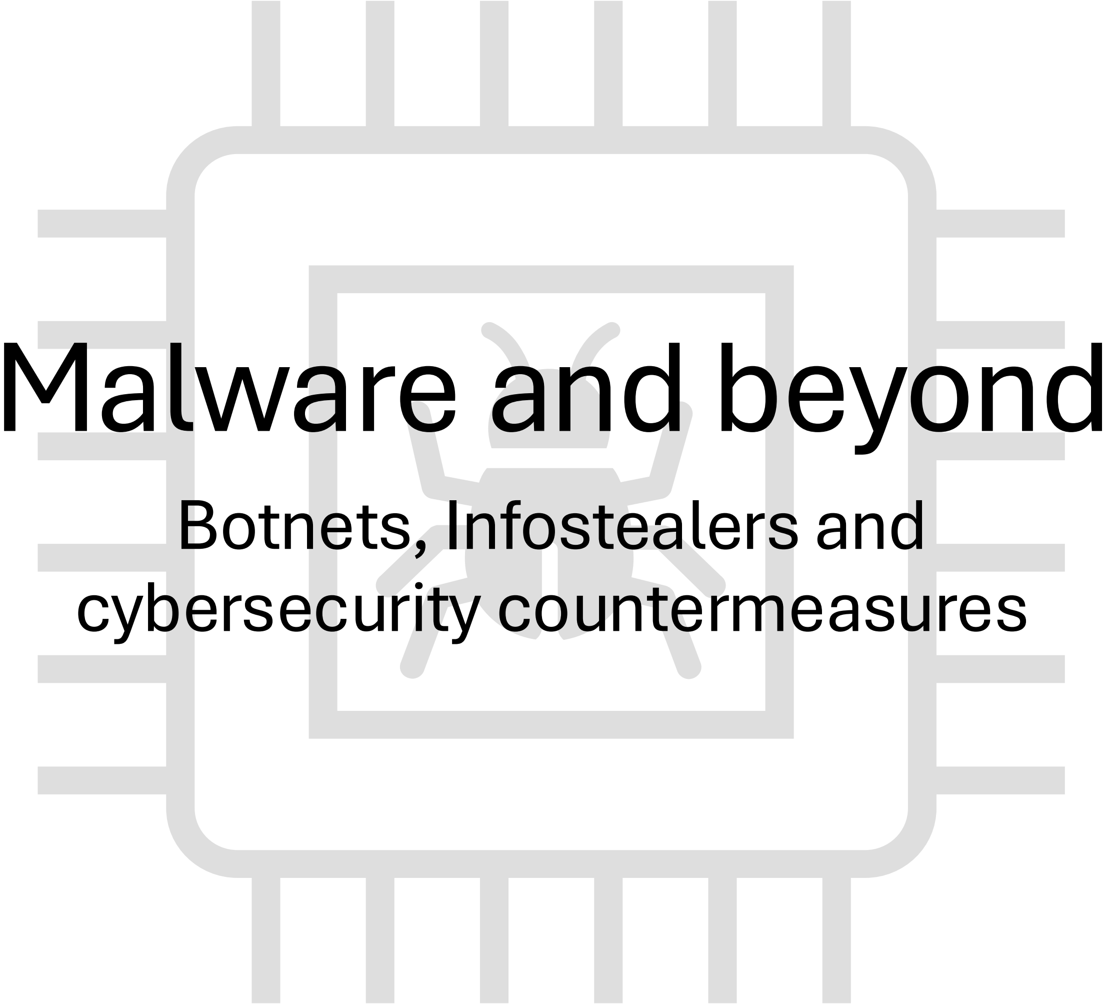


Malware and beyond

Botnets, Infostealers and cybersecurity countermeasures

Background

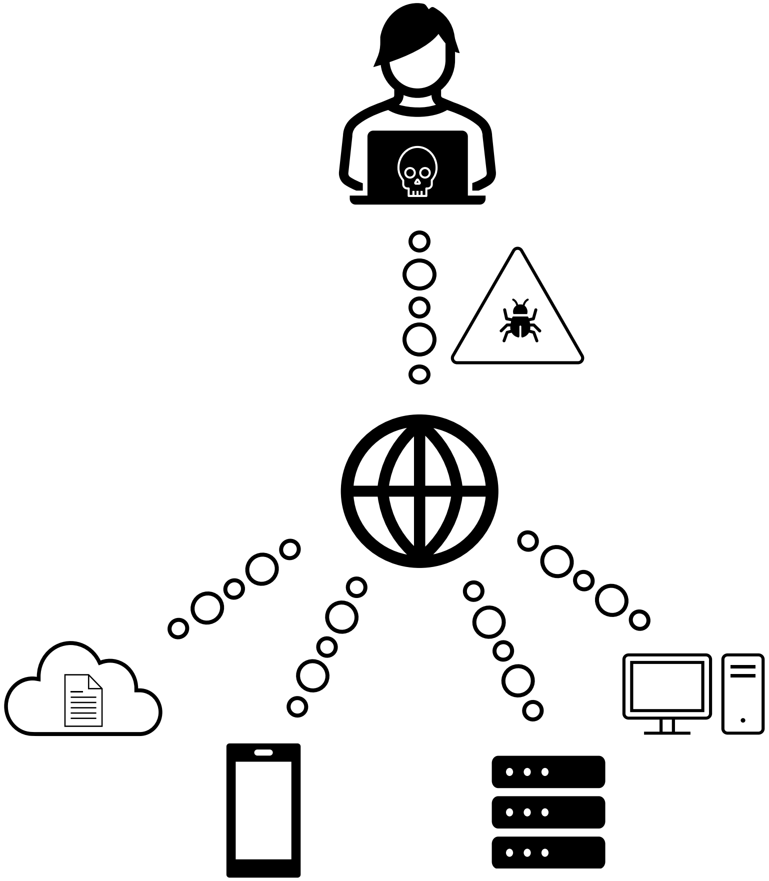
The **Internet and the worldwide Web** have **made great progress in how society communicates and the face of business**.

Malwares are becoming one of the most substantial **threats to information security**.

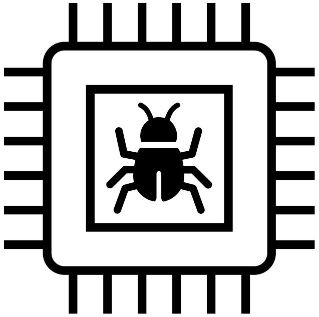
Infostealers are a significant threat to **organizations and individuals**.

The **creation of infostealers has become relatively easy**, with many tools and kits available on the dark web.

Malware-as-a-Service model allow cybercriminals **to access to malicious software and related infrastructure for a fee**.



Malware

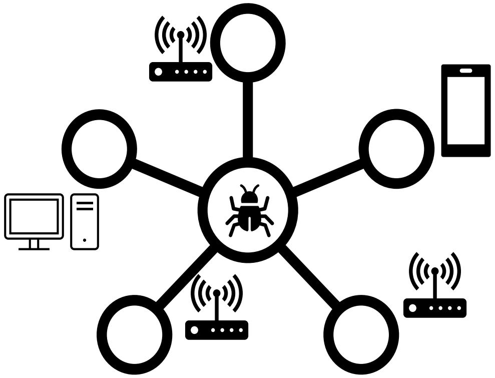


Malicious software intentionally designed to **cause harm to a computer**.

Defined as: ”any code added, changed or removed from a software system in order to intentionally cause harm or subvert the intended function of the system”.

The **history of malware dates back to 1966**, when John von Neumann was developing the concept of ”**Theoretical malware**”, a **program that could reproduce and spread itself throughout a system**.

There are **many types of malware**, some of which are virus, worm, trojan, ransomware, botnet and infostealer.



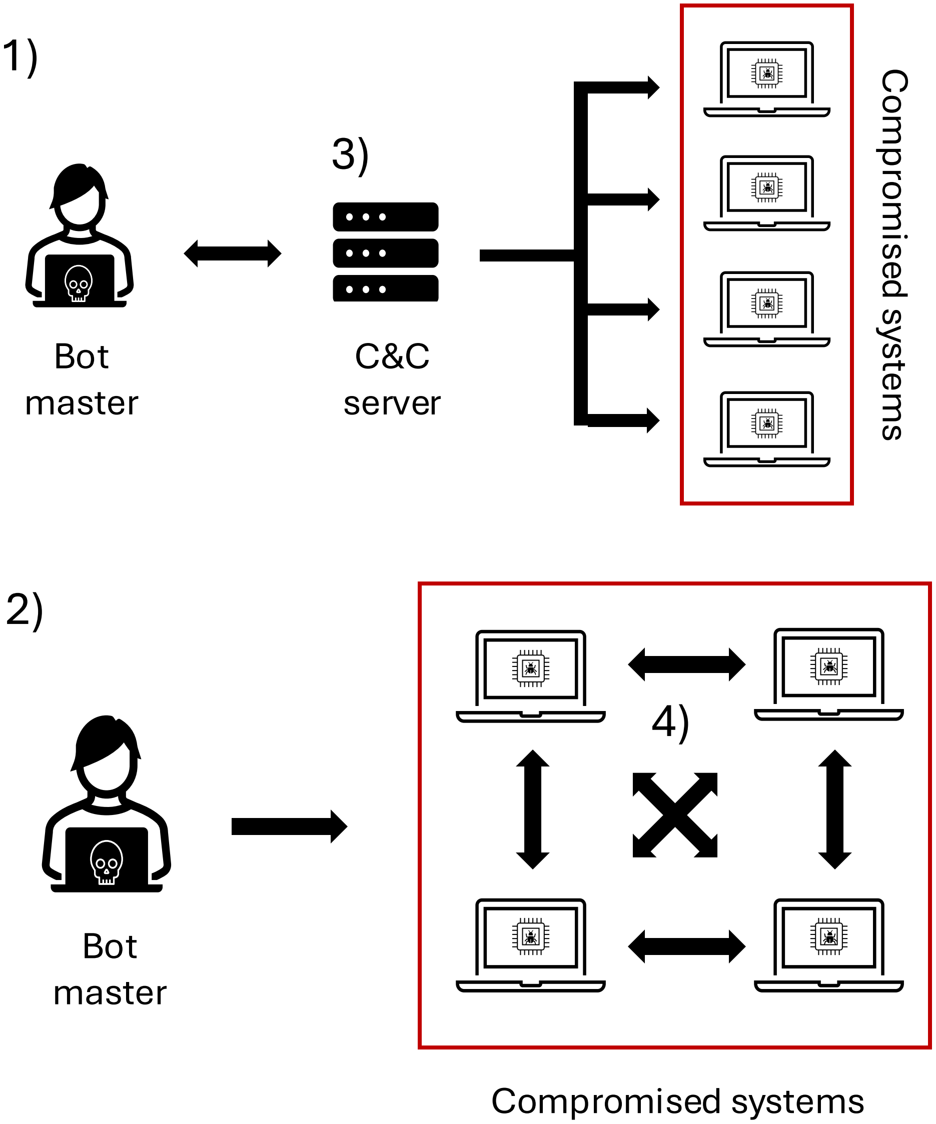
Botnet

A **botnet is a network of malware-infected hosts** typically **controlled by a botmaster**.

Botnet architectures are usually divided into **two main categories**, centralized botnets (1) and Peer-to-Peer (P2P) botnets (2).

In the centralized structure a central **C&C server** (3) is **responsible for sending commands to bots**.

In a **P2P network**, the **botnet commands are propagated throughout** the P2P **overlay network** (4).



Infostealer

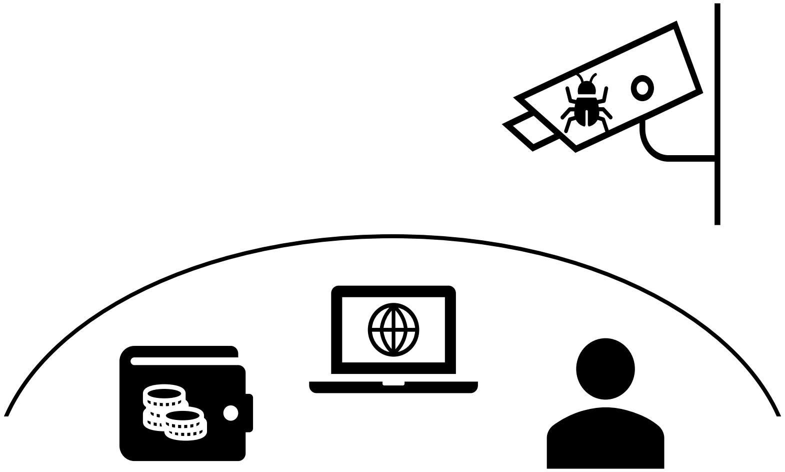
Type of **malicious software designed to extract sensitive information from compromised systems**.

Used by **cybercriminals** to **gather valuable data** that can be **sold on the dark web** or used for further malicious activities.

The **targets** of infostealers can includes:

- **Browser-saved credentials**
- **Financial data**
- **Personal identifiable information**

Employs techniques such as keylogging, form grabbing, and credential dumping to capture sensitive data.



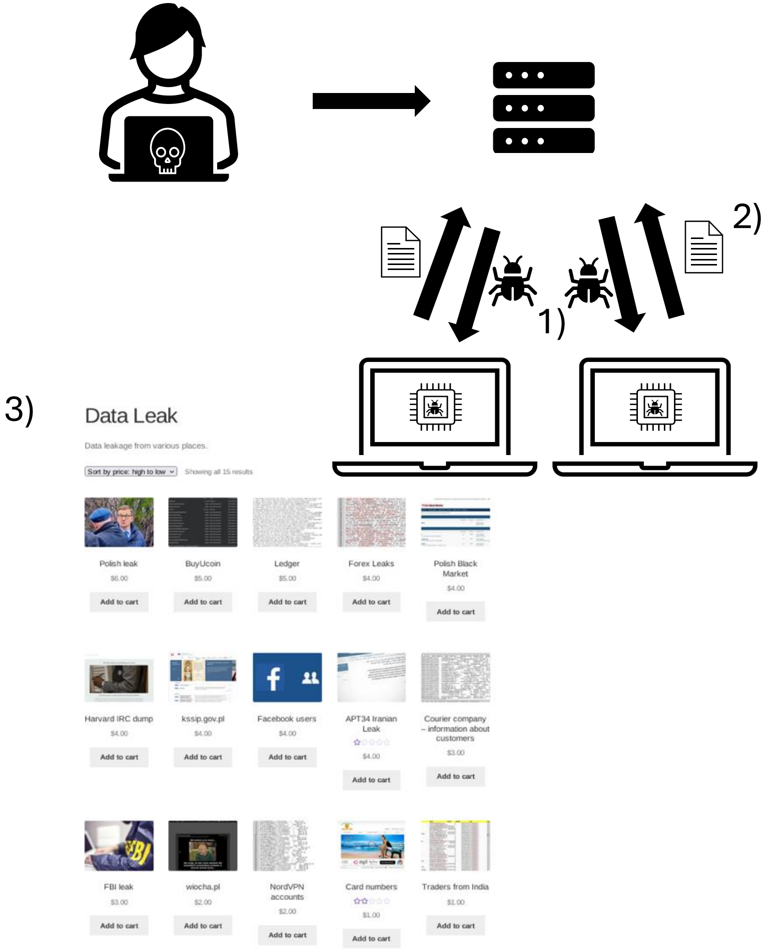
The role of botnets in infostealer operations

Botnets play a crucial role in the operation of infostealers by **providing a network of compromised devices** that can be controlled remotely.

Networks allow attackers to **distribute infostealers** more effectively and **manage the collection of stolen data**.

The process of infostealer so include **three main stages**:

- **Data collection**, infostealer is deployed on the compromised devices and it starts collecting sensitive information. (1)
- **Data distribution**, data are transmitted to C2C servers. (2)
- **Data monetization**, data are sold on underground markets. (3)



Data Leak

Data leakage from various places.

Sort by price: high to low ⌄ Showing all 15 results

Polish leak
$6.00
Add to cart

BuyUcoin
$5.00
Add to cart

Ledger
$5.00
Add to cart

Forex Leaks
$4.00
Add to cart

Polish Black Market
$4.00
Add to cart

Harvard IRC dump
$4.00
Add to cart

kssip.gov.pl
$4.00
Add to cart

Facebook users
$4.00
Add to cart

APT34 Iranian Leak
★☆☆☆☆
$4.00
Add to cart

Courier company – information about customers
$3.00
Add to cart

FBI leak
$3.00
Add to cart

wiocha.pl
$2.00
Add to cart

NordVPN accounts
$2.00
Add to cart

Card numbers
★★☆☆☆
$1.00
Add to cart

Traders from India
$1.00
Add to cart

Mitre ATT&CK framework

Is a **comprehensive, globally accessible knowledge base that outlines the tactics, techniques, and procedures** (TTPs).

Provides a **structured approach to understanding and countering cyber threats**, helping organizations enhance their cybersecurity posture.

Infostealers typically **operate within several key tactics** (check the table).

Infosteares employ techniques like:

- Credetial dumping (T1003).
- Input capture (T1056).
- Data from local system (T1005).
- Exfiltration Over Alternative Protocol (T1048).

Tactic codes	Short description
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0006	Credential Access
TA0009	Collection
TA0010	Exfiltration

Mitigation strategies

Mitigating infostealer threat is an hard challenge, that requires a multi-layered approach.

Strategies includes both **technical solutions** and **organizational practices**.

Technical solutions focus on enhancing the **security posture of systems and networks** through advanced detection, prevention, and response mechanisms.

Organizational practices focus on enhancing the **human and procedural aspects of security**, ensuring that employees are well-informed and prepared to respond to potential threats.

Technical solutions	**Organizational practice**
Endpoint Detection and Response	Employee Awareness Training
Multi-Factor Authentication	Password Management
Anti-Malware Software	Software Updates
Network Segmentation	Incident Response Plan
Dark Web Monitoring	Managed Extended Detection and Response

Reference

- Idika, N., Mathur, A.: A survey of malware detection techniques. Purdue University (2007)
- Von Neumann, J., Burks, A.W., et al.: Theory of Self-reproducing Automata. University of Illinois press Urbana (1966)
- Namanya, A.P., Cullen, A., Awan, I., Pagna Diss, J.: The World of Malware: An Overview, (2018). https://doi.org/10.1109/FiCloud.2018.00067
- Elisan, C.C.: Malware, Rootkits & Botnets A Beginner’s Guide. McGraw Hill Professional(2012)
- Le Bourhis, P., Tibirna, L., Bourgue, Q.: Infostealers: Investigate the cybercrime threat in its ecosystem. In: Presented At: 4 - 6 October, 2023 (2023)
- Netscout: What is MITRE ATT&CK? https://www.netscout.com/ what-is-mitre-attack. Accessed: 2025-01-23
- IBM: MITRE ATT&CK. https://www.ibm.com/think/topics/mitre-attack. Accessed: 2025-01-23

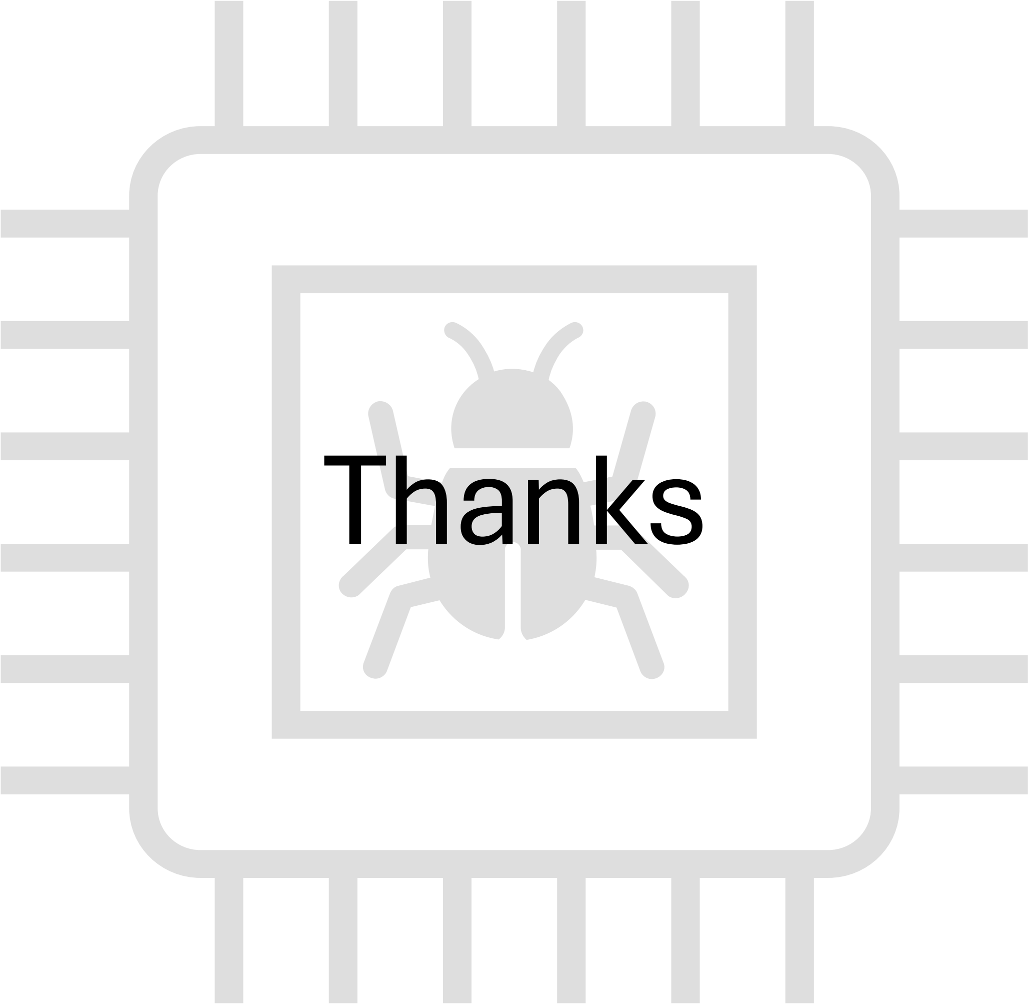
Reference

- Corvus Insurance: Mitigating Infostealer Malware: Best Practices and Strategies. https://www.corvusinsurance.com/blog/mitigating-infostealer-malware. Accessed: 2025-01-22

- Proton: Infostealers: What They Are and How to Protect Yourself. https://proton.me/blog/infostealers. Accessed: 2025-01-22

- ACS: Infostealer: Cosa Sono e Come Proteggersi. https://www.acs.it/it/blog/

- Infosecurity Europe: Guide to Infostealer Malware. https://www. infosecurityeurope.com/en-gb/blog/threat-vectors/guide-infostealer-malware.html. Accessed: 2025-01-23



Thanks