LOADER CYBER KILL CHAIN

Bui Viet Dung

June 26, 2025

1 Loader overview

1.1 Definition of Loader

Loader malware is type of malicious software with main function is to set up an initial place on the target system And then download as well as execute 1 secondary Payload, Often have greater destruction and Loader K itself directly harms the system.

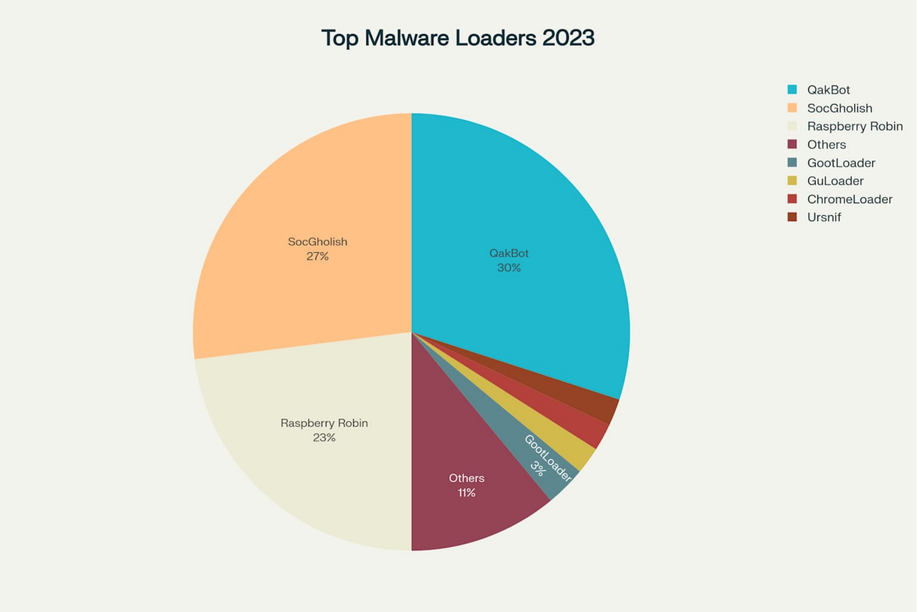


Figure 1: Top loader 2023

1.2 The relationship between Loader, IAB, Raas

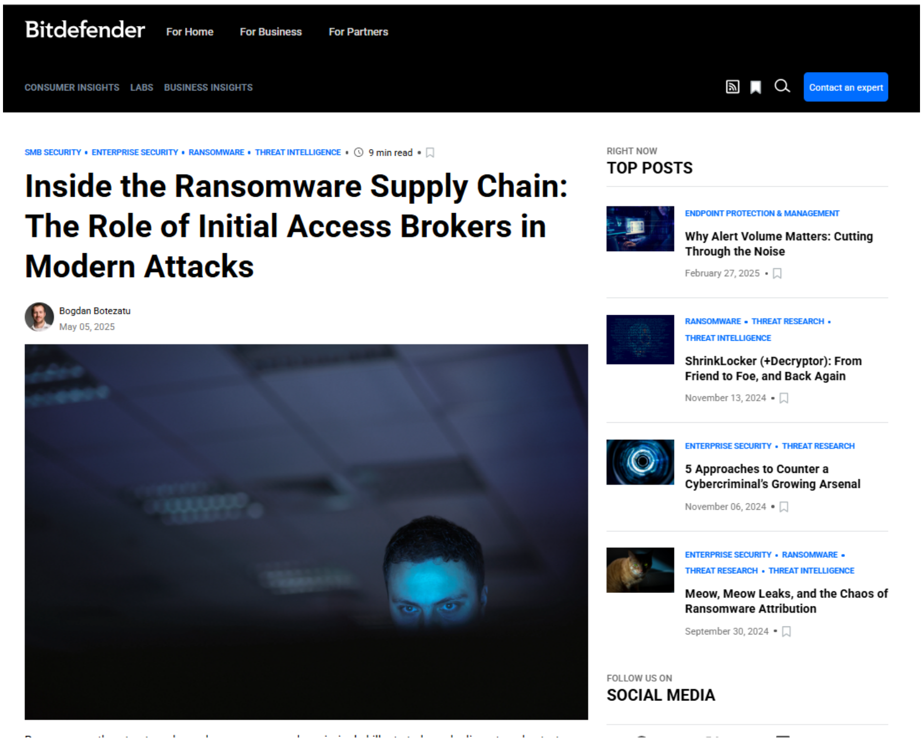
The current cyber criminal context is characterized by specialization, acting as a business model. Crime as a Service model in this form of service includes a few separate factors for different actors .

Inital Access Brokes - IAB

These actors specialize in gaining illegal access to networks and then selling that access to other crimes.Loader is the main tool used by the IAB to effectively penetrate the victim on a large scale.

Ransomware-as-a-Service - RaaS

Ransomware groups buy access from IAB to streamline their activity, allowing them to focus on extracting and encrypting data instead of the initial penetration.



SMB SECURITY • ENTERPRISE SECURITY • RANSOMWARE • THREAT INTELLIGENCE • 9 min read •

Inside the Ransomware Supply Chain: The Role of Initial Access Brokers in Modern Attacks

Bogdan Botezatu
May 05, 2025

RIGHT NOW
TOP POSTS

ENDPOINT PROTECTION & MANAGEMENT
Why Alert Volume Matters: Cutting Through the Noise
February 27, 2025 •

RANSOMWARE • THREAT RESEARCH • THREAT INTELLIGENCE
ShrinkLocker (+Decryptor): From Friend to Foe, and Back Again
November 13, 2024 •

ENTERPRISE SECURITY • THREAT RESEARCH
5 Approaches to Counter a Cybercriminal's Growing Arsenal
November 06, 2024 •

ENTERPRISE SECURITY • RANSOMWARE • THREAT RESEARCH • THREAT INTELLIGENCE
Meow, Meow Leaks, and the Chaos of Ransomware Attribution
September 30, 2024 •

FOLLOW US ON
SOCIAL MEDIA

Figure 2: https://www.bitdefender.com/en-us/blog/businessinsights/ransomware-supply-chain-initial-access-broker-role

A criminal group can specialize in developing and distributing the initial access code (Loader), while another group specializes in the final Payload.This assignment has created a market for "access", allowing excellent agents to gain access to initially making money from this skill by selling it to others, marking the birth of IAB.The existence of a powerful IAB market, motivated by effective loaders, has allowed RAAS models to thrive.

2 Cyber kill chain overview

The Cyber Kill Chain is a strategic model that outlines the stages of a cyberattack, from initial reconnaissance to achieving the final objective. This framework is often mirrored in penetration testing (pentest), a legal and authorized simulated attack on a computer system performed to evaluate its security. By understanding the steps in the Cyber Kill Chain, penetration testers can mimic the strategies of malicious attackers, exploring vulnerabilities at each stage of the chain. This approach allows organizations to evaluate their defensive measures across the full spectrum of an attack, identifying weaknesses and enhancing their security protocols accordingly. In essence, the Cyber Kill Chain provides a roadmap for pen-testers to systematically evaluate an organization's cyber defences.

Cyber Kill Chain.

1. Reconnaissance

The attacker gathers information about the target to identify exploitable weaknesses. This may include scanning public data sources, probing open ports, or harvesting data from social media.
Techniques used:

- Open-source intelligence (OSINT)
- Port and service scanning
- Network topology analysis

2. Weaponization

After gathering sufficient intelligence, the attacker creates or customizes malicious code to exploit discovered vulnerabilities.
Techniques used:

- Crafting custom malware
- Embedding malware into legitimate files
- Leveraging exploit toolkits

3. Delivery

The attacker transmits the malware to the target via email, malicious websites, or infected USB drives.
Techniques used:

- Phishing emails
- Drive-by downloads
- USB-delivered malware

4. Exploitation

Upon activation, the malware exploits system vulnerabilities to execute and gain control.
Techniques used:

- Software vulnerability exploitation
- Malicious document macros
- Browser-based attacks

5. Installation

The malware installs itself to maintain persistence.
Techniques used:

- Dropping backdoors or trojans
- Creating persistent services or scheduled tasks
- Using rootkits for stealth

6. Command and Control (C2)

The compromised host establishes contact with an external C2 server for instruction and data transfer.
Techniques used:

- HTTP/HTTPS communications
- DNS tunneling
- Cloud or social media-based C2

7. Actions on Objectives

The attacker executes their final objectives such as stealing data, deploying ransomware, or disrupting systems.

Techniques used:

- Data exfiltration
- File encryption with ransom demand
- Destructive attacks or wiping

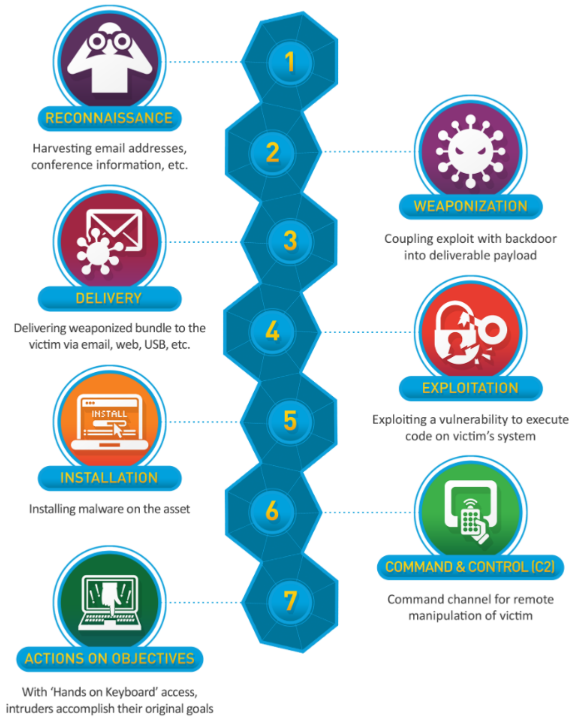

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 3: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

3 Loader in Cyber Kill Chain.

Loader malware, also known as Downloader or Dropper, is a malware designed specifically to penetrate the system and then download as well as execute malicious payloads.The main difference between Loader and other malware lies in their main function: while most malware is developed to directly perform malicious activities such as data stealing or encrypting files, loaders created with the sole purpose of creating conditions for deploying other toxic tools.

The technical distinction between Downloader and Dropper is also important in understanding the operating mechanism of Loader.Downloader requires network connection to download malware from the Internet, while dropper can embed execution files and just "drop" them into the operating system without network connection.However, in reality, this boundary is increasingly faint because many modern loaders maybe combine both functions to increase flexibility and efficiency in the future .

Because of these characteristics , Loader is highest involve in Installation and Command & Control in Cyber Kill Chain.

Mapping loader in cyber kill chain.

1. Reconnaissance:
Loaders are not involved in this stage. The attacker focuses on gathering in-

formation about the target (e.g., system architecture, OS version, open ports), which typically precedes the deployment of any loader.

2. Weaponization :

The loader it self may be a part of the weaponization phase. However, It is not primary actor here.This phase focuses on creating attack payload like ransomeware , info stealer , backdooor , C2 server .....

3. Delivery :

The attacker delivers the loader via phishing, malicious websites, or drive-by download. In many cases, the loader is embedded in a dropper or script that executes upon user interaction.

4. Exploitation :

The loader is executed as a result of user action. When the victim opens a document or visits a compromised page, a macro or exploit triggers the execution of the loader. The loader does not perform the exploitation itself but depends on this phase to gain execution.

5. Installation :

Loader performs its main role here. It installs itself onto the system (e.g., copying into %AppData%, %Temp%), creates persistence via registry keys or scheduled tasks, and prepares for communication with the attacker.

6. Command Control :

Loader contacts its server to download secondary payloads. It may also send system information or check-in status. This is often the point where real-time control or malware delivery begins (e.g., Cobalt Strike, ransomware, infostealers).

7. Action on Obj :

Loader steps aside. The final payload (ransomware, spyware, etc.) takes over to achieve the attacker's objectives. The loader may terminate itself, sleep, or await further instructions.