

# Credential Access with LaZagne

---



**Gavin Johnson-Lynn**

Offensive Security Specialist, Software Developer

@Gav\_JL [www.gavinjl.me](http://www.gavinjl.me)



The LaZagne Project

! BANG BANG !





Creator: “Alessandro Zanni”



**The LaZagne project is an open-source application used to retrieve lots of passwords stored on a local computer... developed for the purpose of finding passwords for the most commonly-used software.**



# The LaZagne Project

## ! BANG BANG !

### Post exploitation tool

- Written in Python
- Targets Windows, Linux and Mac

### Github repository

- <https://github.com/AlessandroZ/LaZagne>

### Credentials from various software

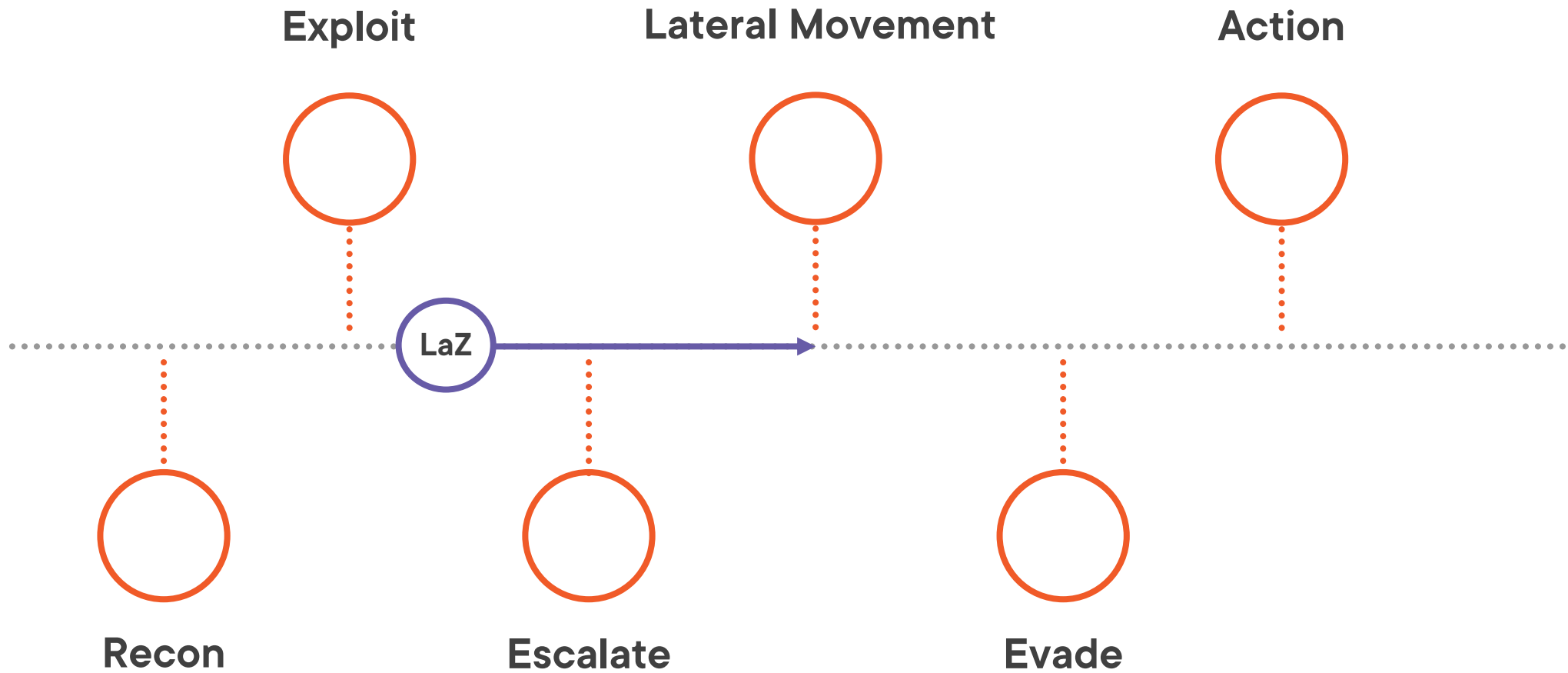
- Browsers
- Admin tools
- Operating systems

### Threat Groups

- APT3, APT33, MuddyWater, LeafMiner



# Kill Chain



# MITRE ATT&CK

## Tactics

**Initial Access**  
**Execution**  
**Persistence**  
**Privilege Escalation**  
**Defense Evasion**  
**Credential Access**  
**Discovery**  
**Lateral Movement**  
**Collection**  
**Command & Control**  
**Exfiltration**  
**Impact**



# MITRE ATT&CK

## Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

**Credential Access**

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

**T1552:**

Unsecured Credentials

**T1552.001**

Credentials in Files

**T1555:**

Credentials from Password Stores

**T1555.003**

Credentials from Web Browsers



# Staying Legal

**Accessing and using someone else's computer is against the law**

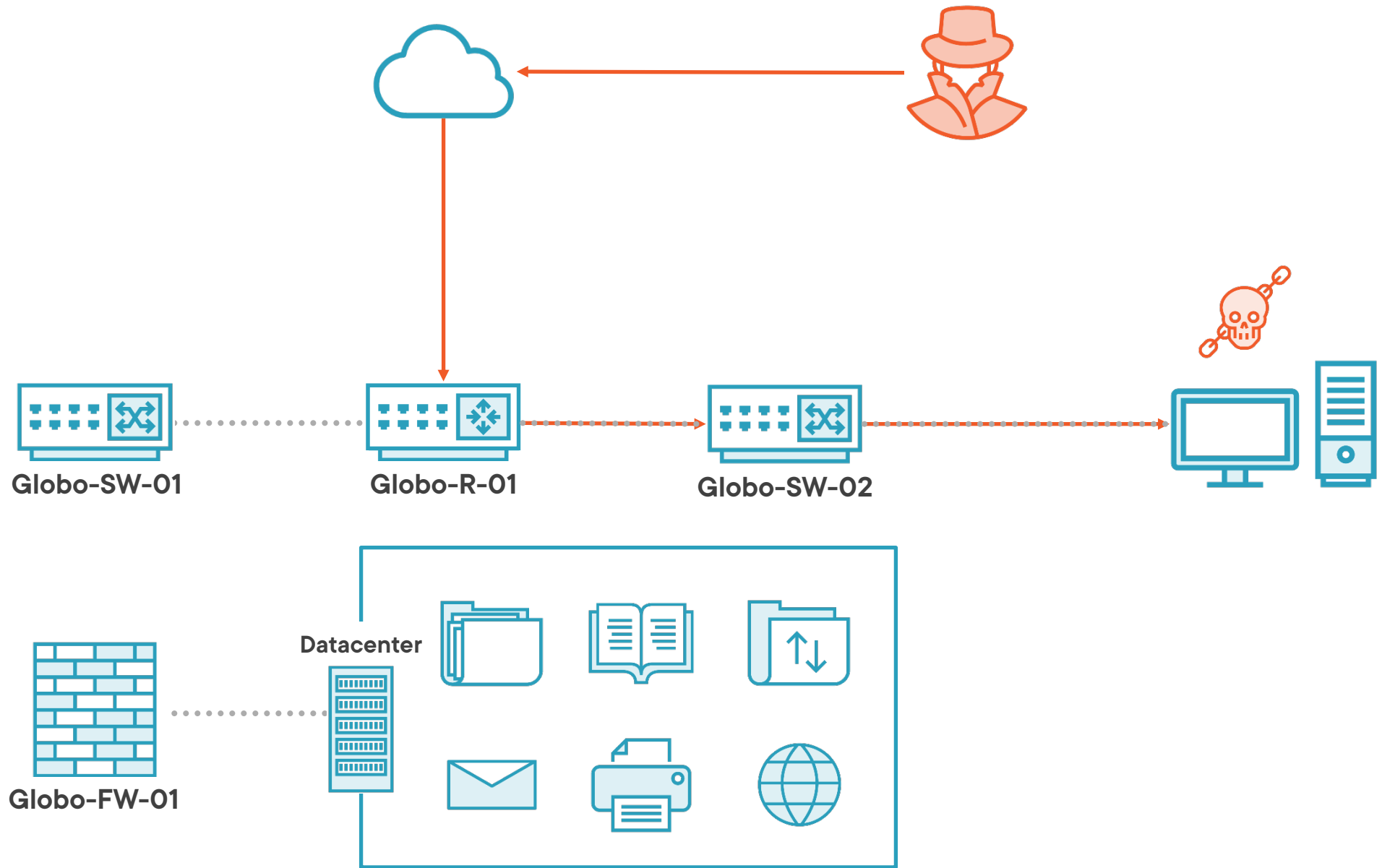


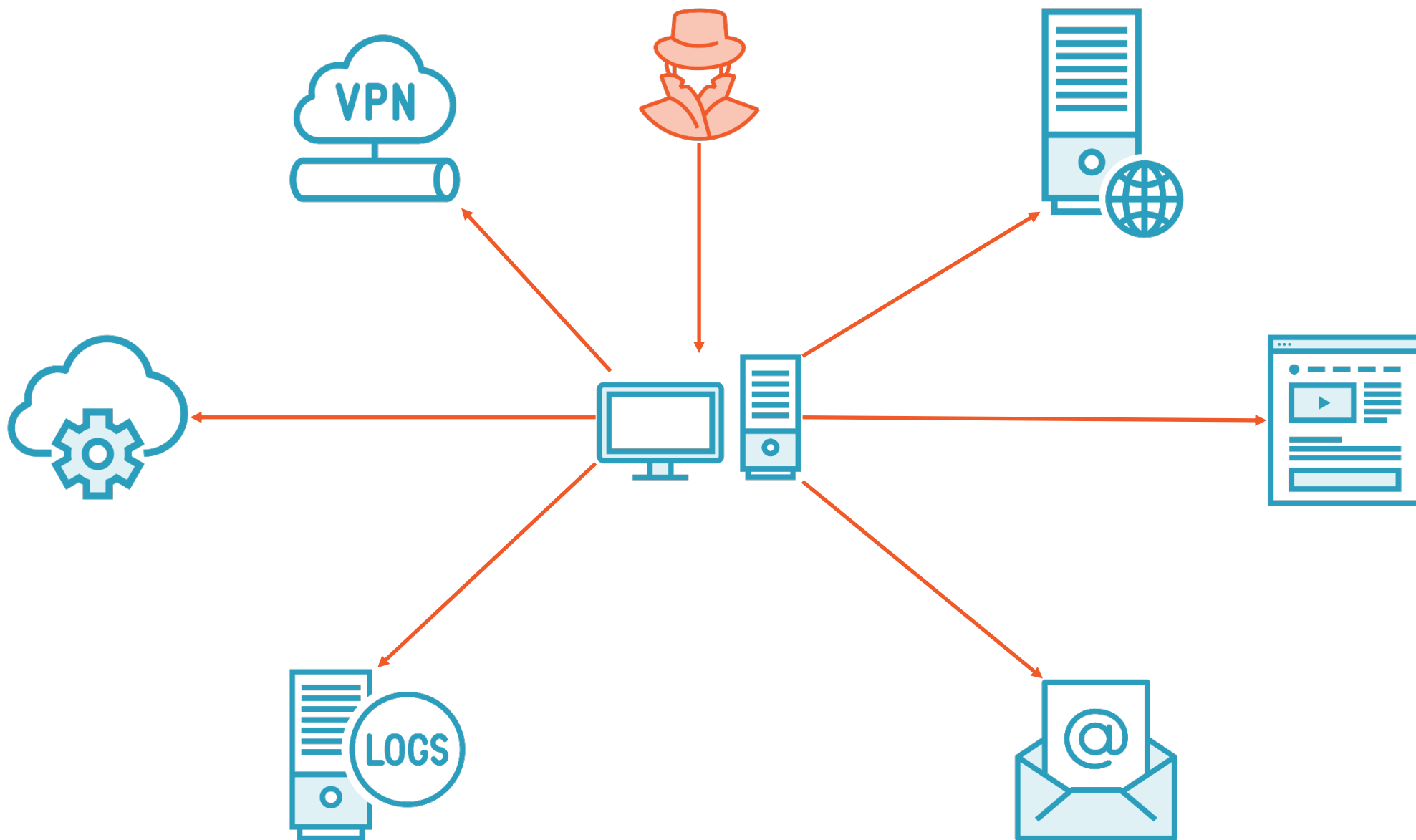
**Seek permission**

**Be familiar with the laws**









# Popular Targets

## **Windows/Linux/Mac**

Chrome and Firefox

## **Linux**

SSH, FileZilla, AWS,  
KeePass 1 & 2, Thunderbird

## **Windows**

Outlook, VNC,  
RDPManager, OpenSSH,  
OpenVPN, Wireless  
network, Password hashes



# Demo Environment



**Windows 10**

**Python 3.9.1**

**Windows Defender**

- LaZagne allowed

# Demo



## Installation tips

- Python and its dependencies
  - <https://github.com/AlessandroZ/LaZagne>

## Compiling the executable

- Better for a Windows target
- <https://github.com/AlessandroZ/LaZagne/releases/>
- Build it ourselves
- <https://github.com/AlessandroZ/LaZagne/wiki/How-to-compile>



# Demo



## Credentials from web browsers (T1555.003)

### Storing credentials in browsers

- Great for usability
- Bad for security



# Demo



## Unsecured Credentials: Credentials In Files (T1552.001)

- SysAdmin programs



# Demo



## **Find all the passwords**

- Lots of modules, especially for Windows
- Noisy
- Time saving

## **Output formats**

