

# Initial Access with King Phisher

---



**Jeff Stein**

CISSP, GCED, CEH, CHFI, SECURITY+

[www.securityinobscurity.com](http://www.securityinobscurity.com)







Creator: SecureState



Tooling for building complex phishing attack scenarios as well as coordinating and monitoring successful phishing campaigns. Created for the purpose of testing and promoting user awareness by simulating real world phishing attacks.





Open source software for coordinating phishing attacks

Available from the king-phisher github repository: <https://github.com/rsmusllp/king-phisher>

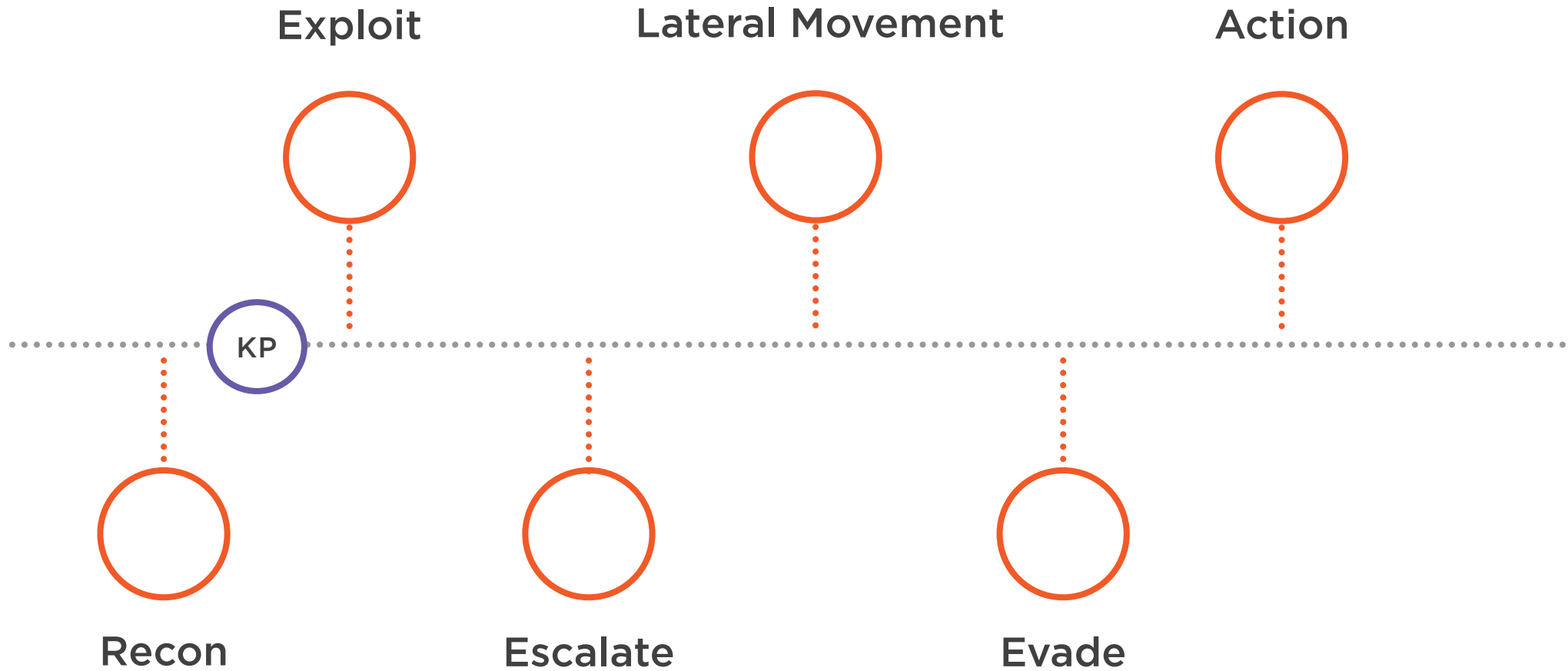
Pre-installed on Kali Linux

Host of prebuild content templates to increase the legitimacy of your phishing messages.

Create landing pages for harvesting credentials from your attacks.



# 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

T1078:

Valid Accounts

T1566:

Phishing

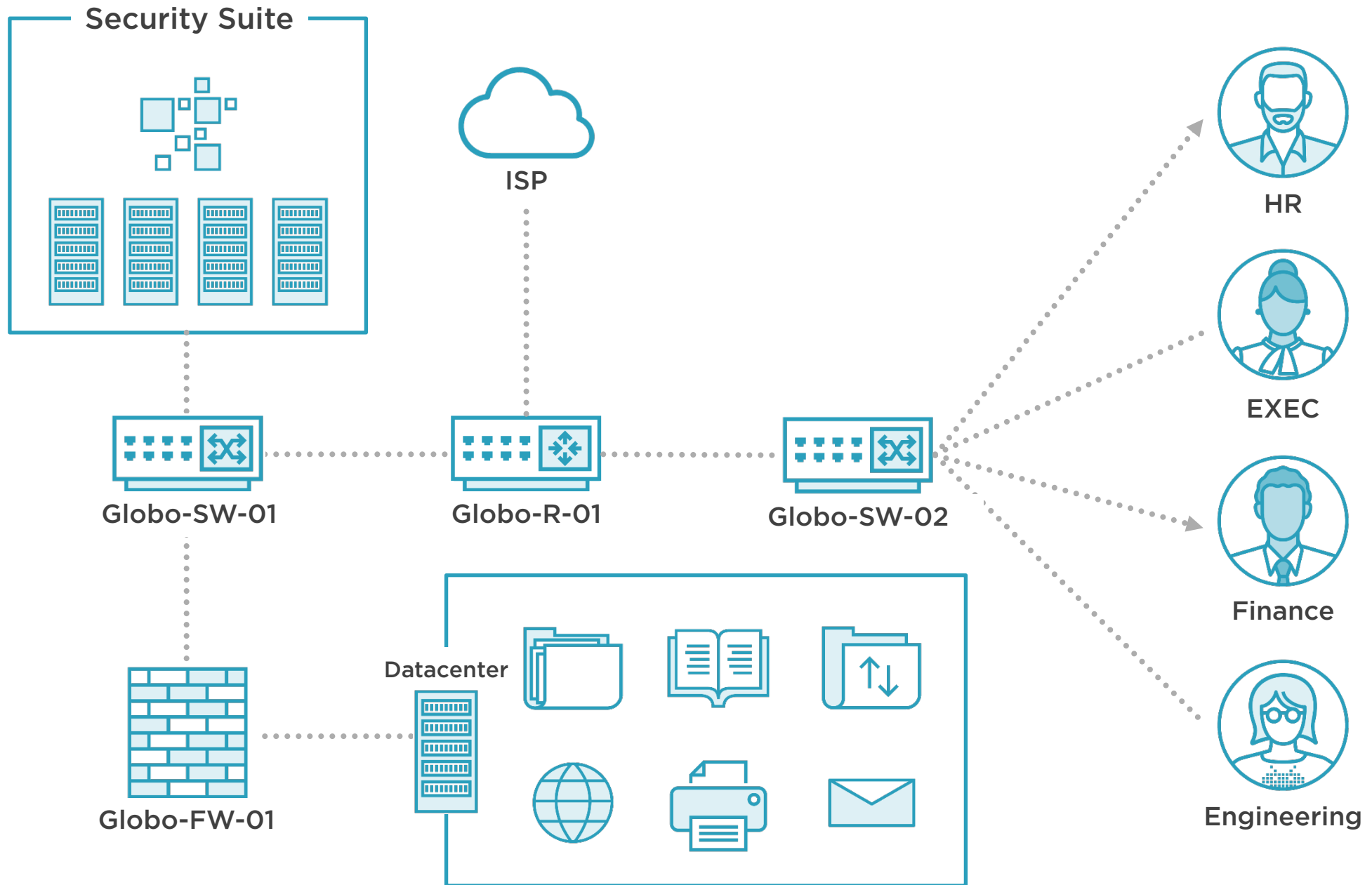
T1566.002

Spearphishing Link

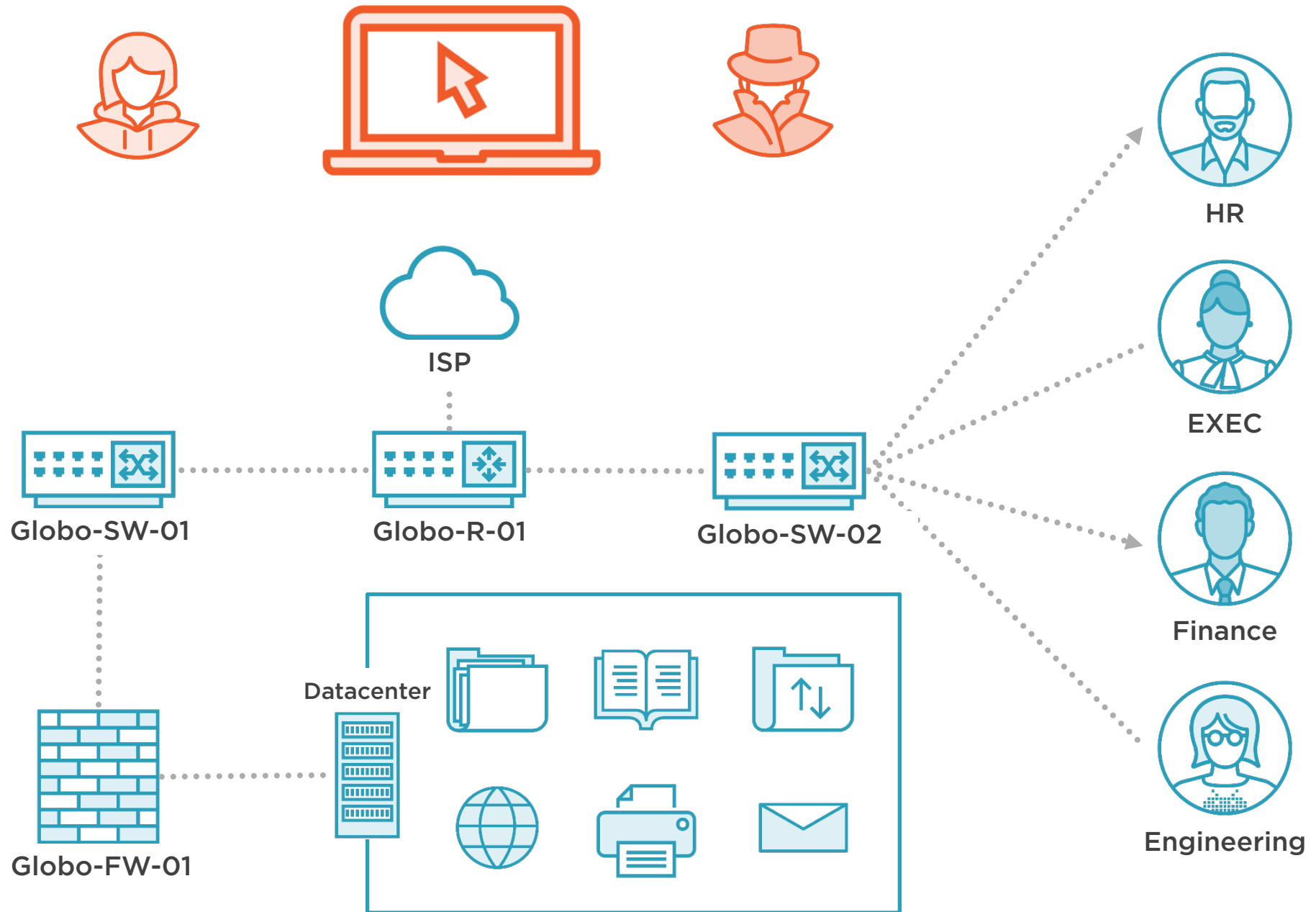
T1566.003

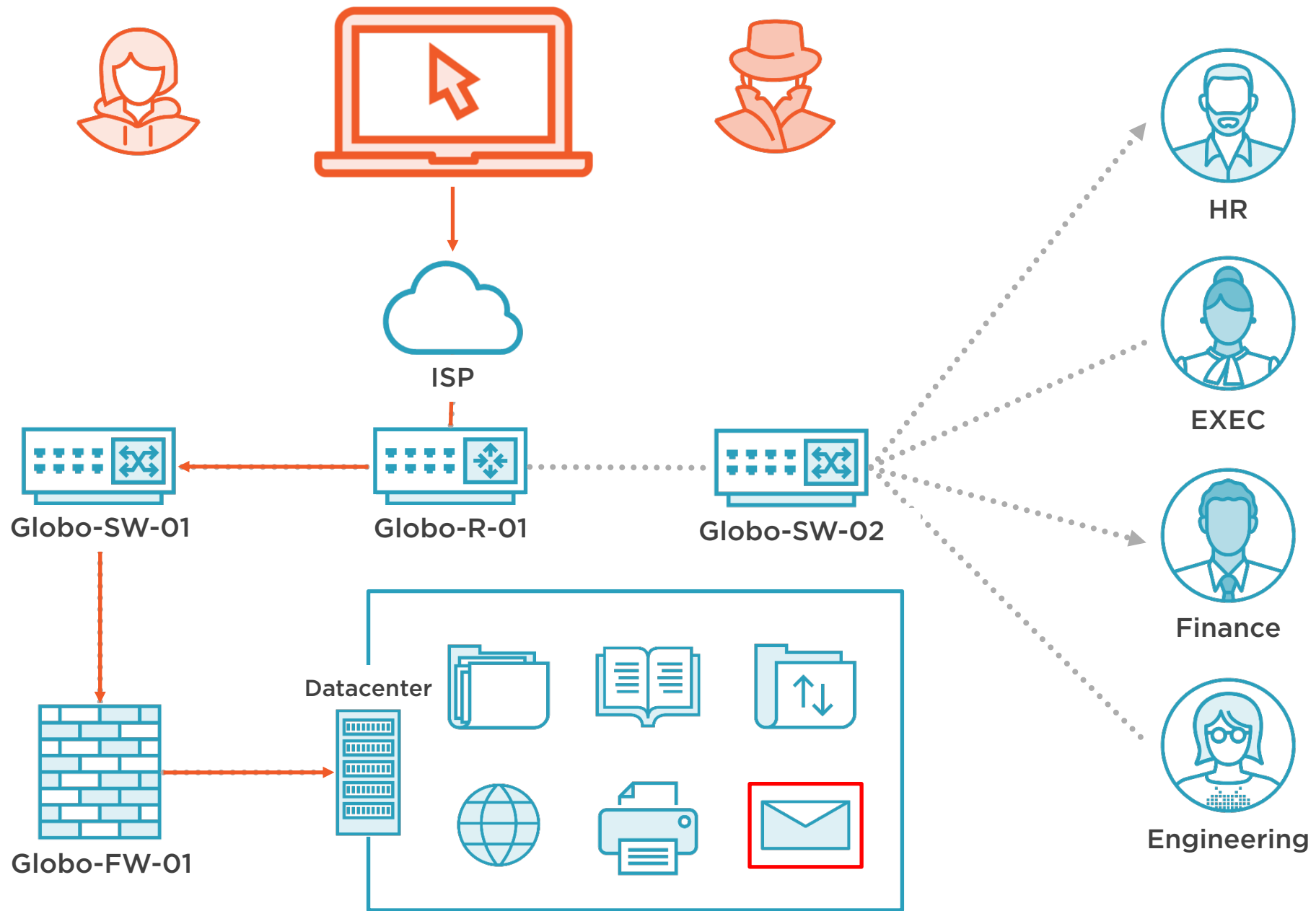
Spearphishing via Service

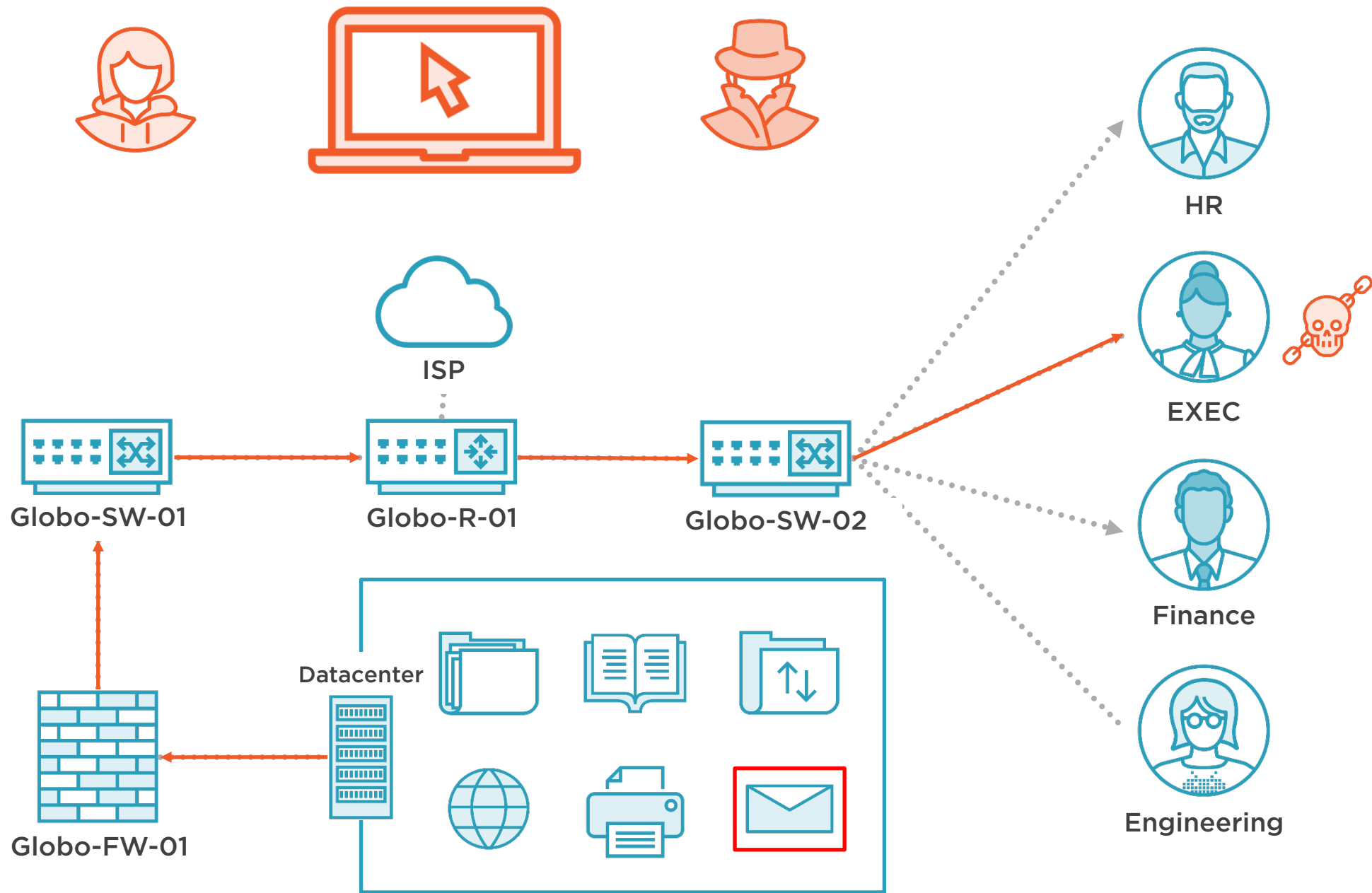


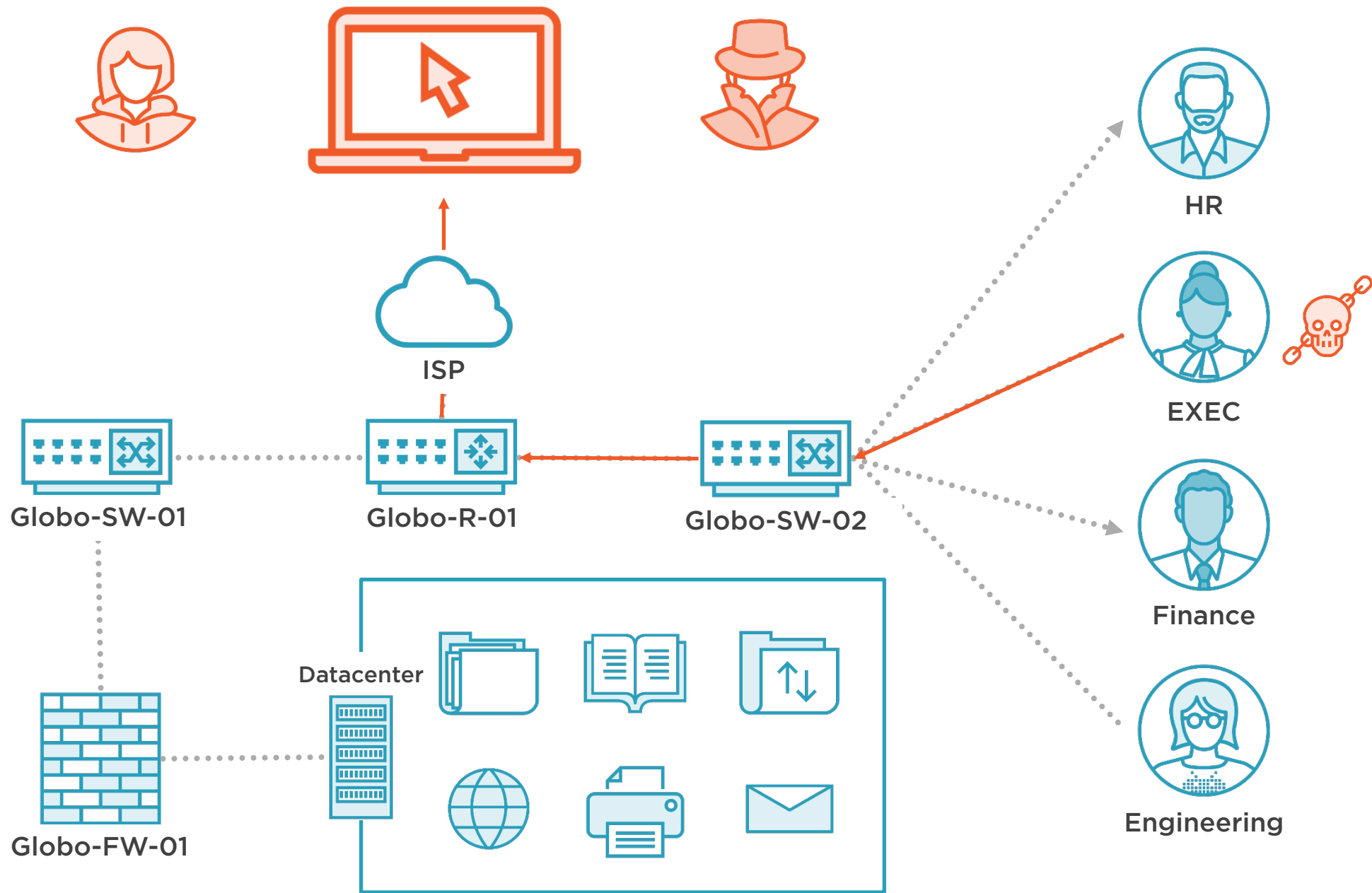




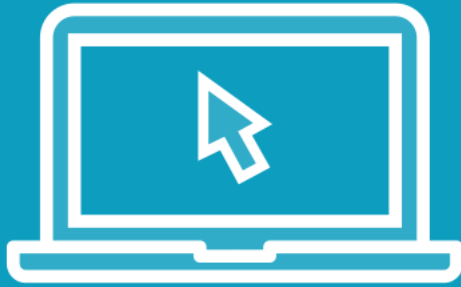








# Demo



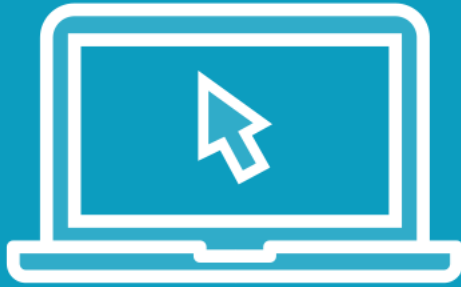
Explore technics to unlock the potential of gaining initial access through phishing

## Enumerate our victim company

- Identify potential targets
- Assess limitations for phishing our targeted domain



# Demo



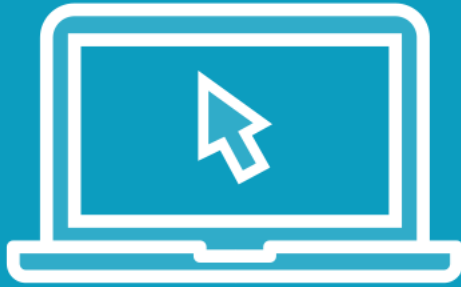
Prepare King Phisher to gain initial access against a victim

Configure campaign and sending settings

Configure message templates to add authenticity to your attack



# Demo



**Craft landing pages to leverage in our attack**

- Add legitimacy to attack
- Extend your attack capabilities

**Send attack campaign to targeted victim**

**Gather credentials to gain initial access**

