

Credential Access with Mimikatz



Lee Allen

PENETRATION TESTER

www.securitysession.com



Mimikatz



Mimikatz

Creator: Benjamin Delpy



Mimikatz is a tool used to extract plain text passwords, hashes, kerberos tickets, and PIN codes from memory. In addition Mimikatz can also be used to pass the hash, pass the ticket or create golden and silver tickets



Mimikatz

Mimikatz is a well-known credential dumping tool with many other capabilities

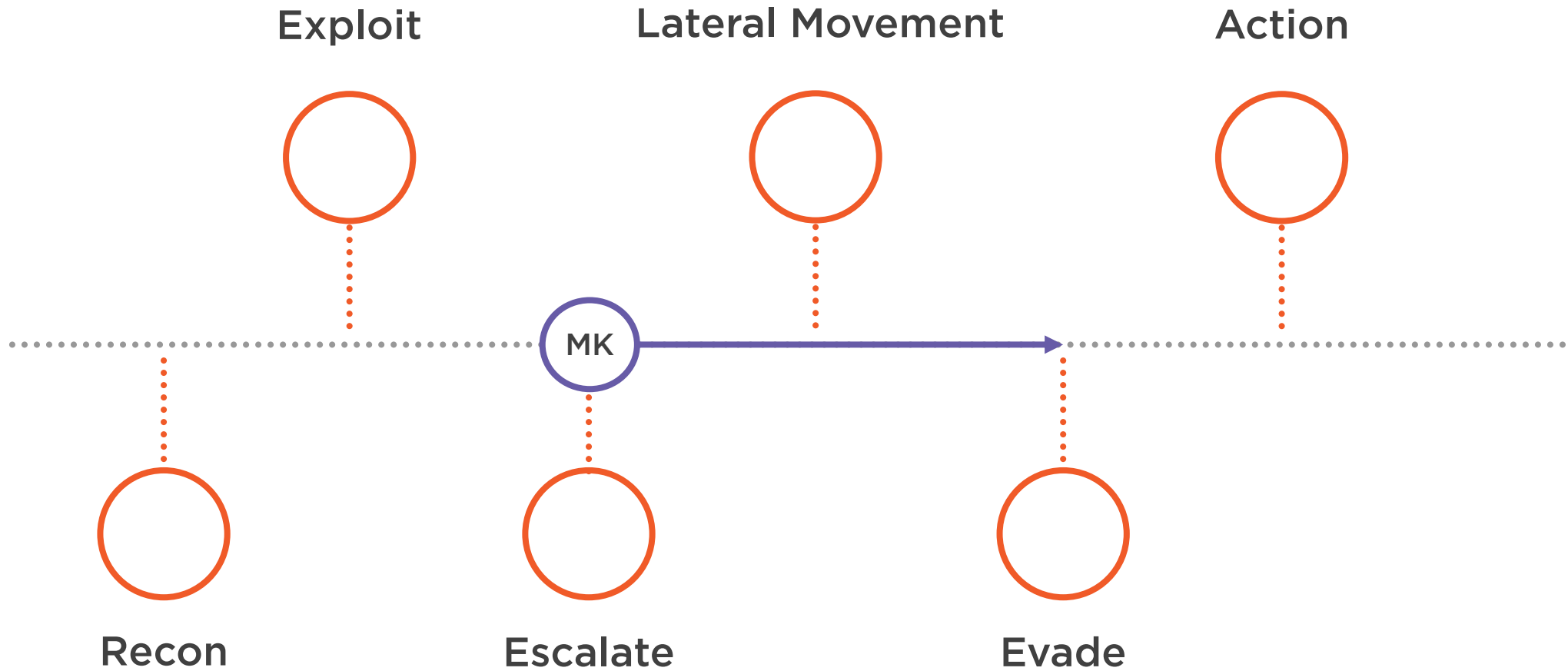
GitHub:

- <https://github.com/gentilkiwi/mimikatz>

Used for both good and evil



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

T1101:

Security Support Provider

T1098:

Account Manipulation

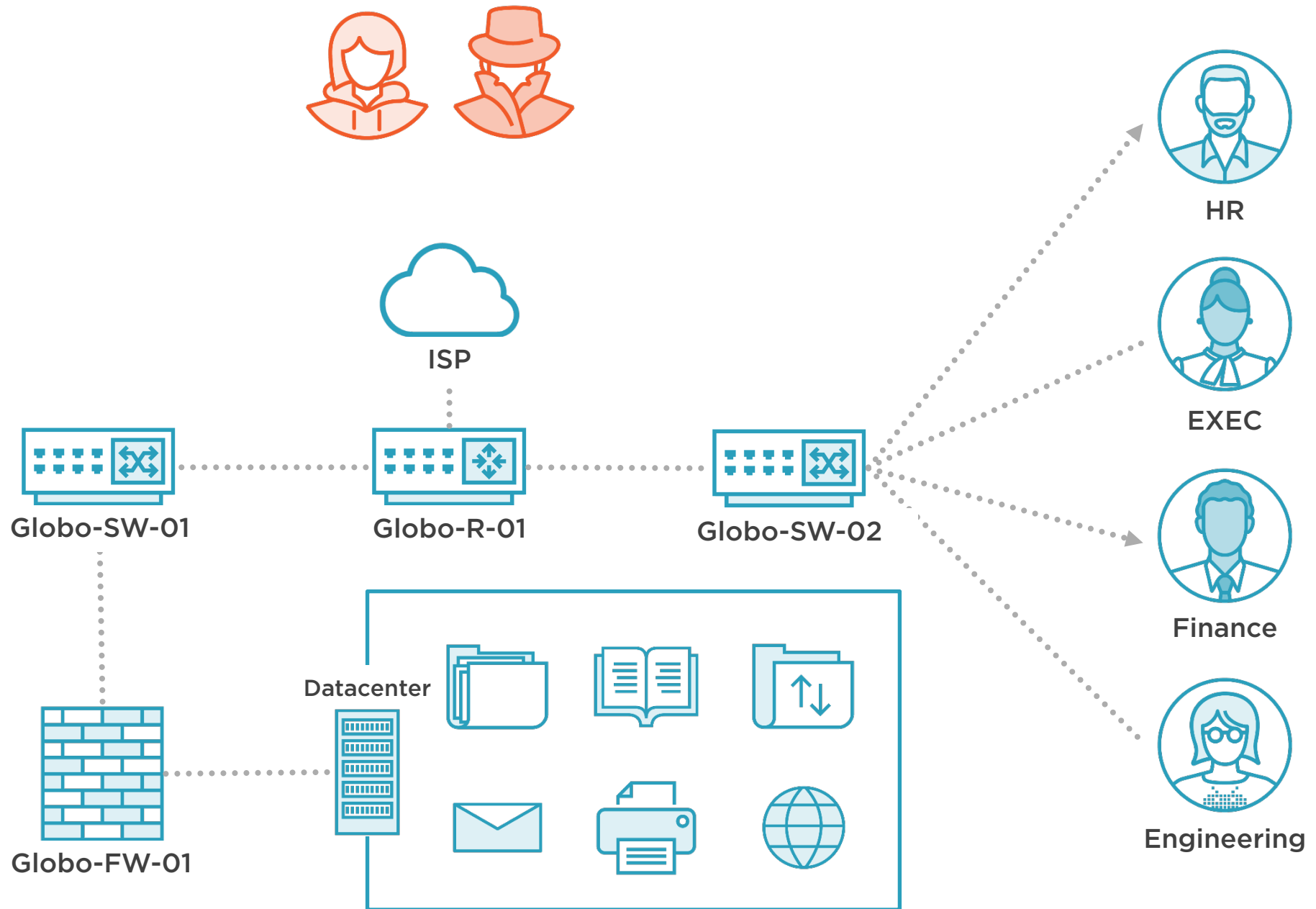
T1003:

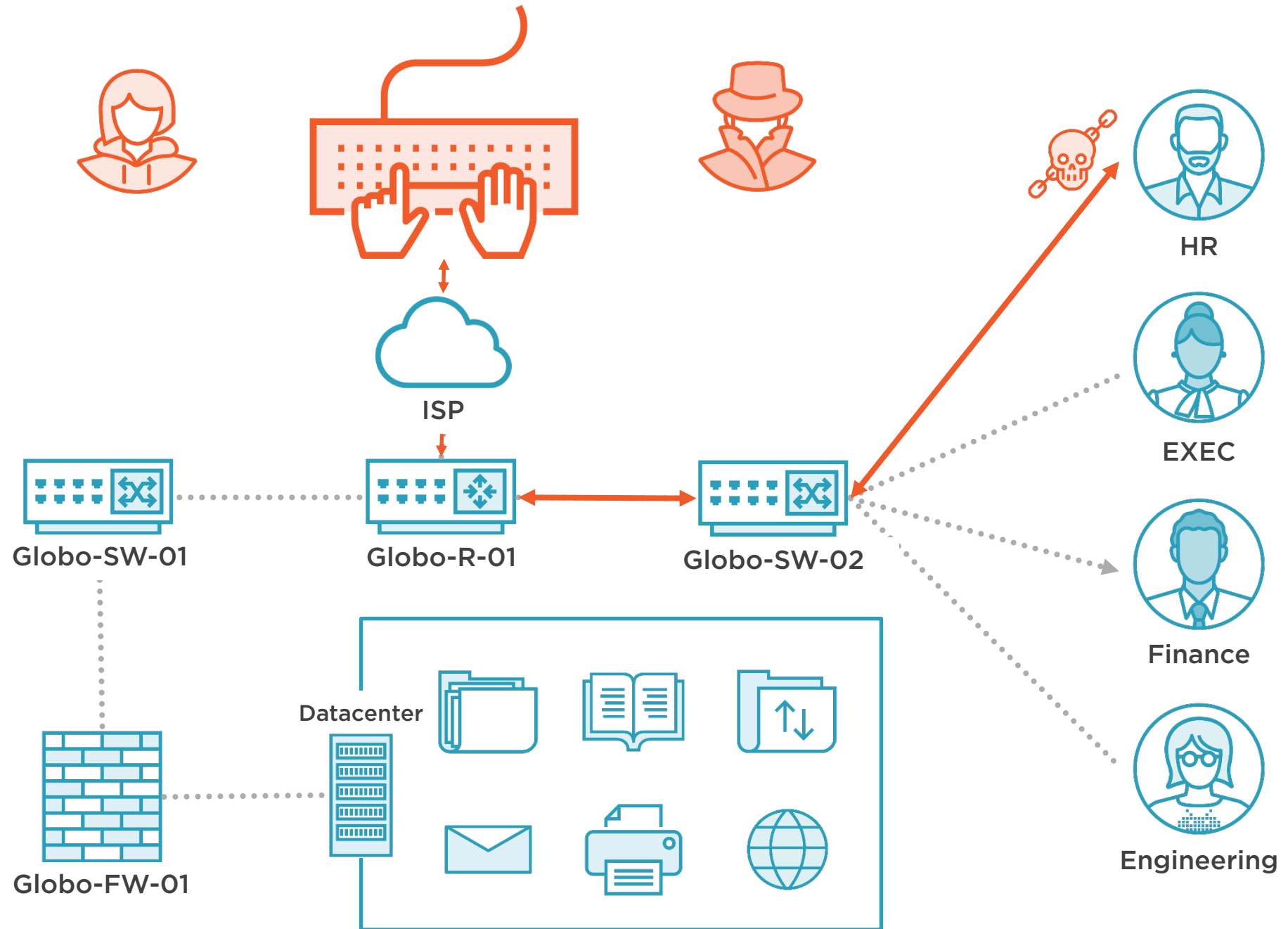
Credential Dumping

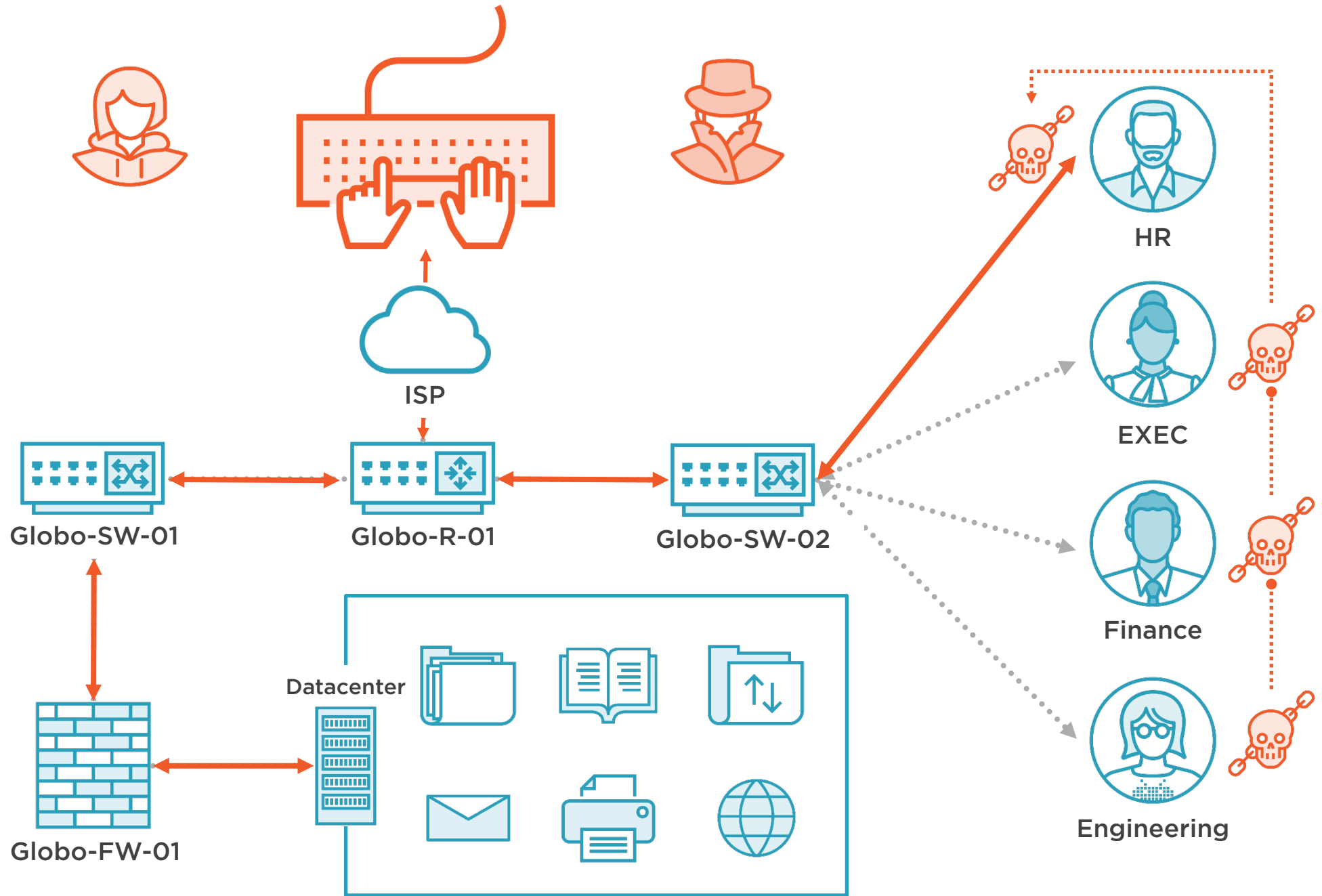
T1081:

Credentials in Files









Demo



Credential dumping with Mimikatz

- Enable clear text passwords in Win10
 - HKLM\System\CurrentControlSet\Control\SecurityProviders\Wdigest
 - UseLogonCredential 1
- Create active login sessions
- Use basic Mimikatz commands to pull clear text passwords
 - privilege::debug
 - log [filename]
 - sekurlsa::logonpasswords



Demo

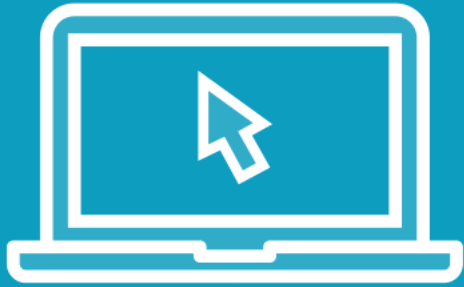


Using Minidump to open a memory dump

- Creating a dump file using task manager
- Opening the dump file in Mimikatz



Demo



Obtain protected credentials in files

Changing an account password

Leveraging MemSSP to store future local accounts in clear text



More Information

Capabilities

Mimikatz Wiki

<https://github.com/gentilkiwi/mimikatz/wiki>

MITRE ATT&CK

<https://attack.mitre.org/software/S0002/>

Active Directory Security - Unofficial Guide to Mimikatz & Command Reference

<https://adsecurity.org/?p=2207>

Additional Resources

Benjamin Delpy on Twitter

<https://twitter.com/gentilkiwi?lang=en>

