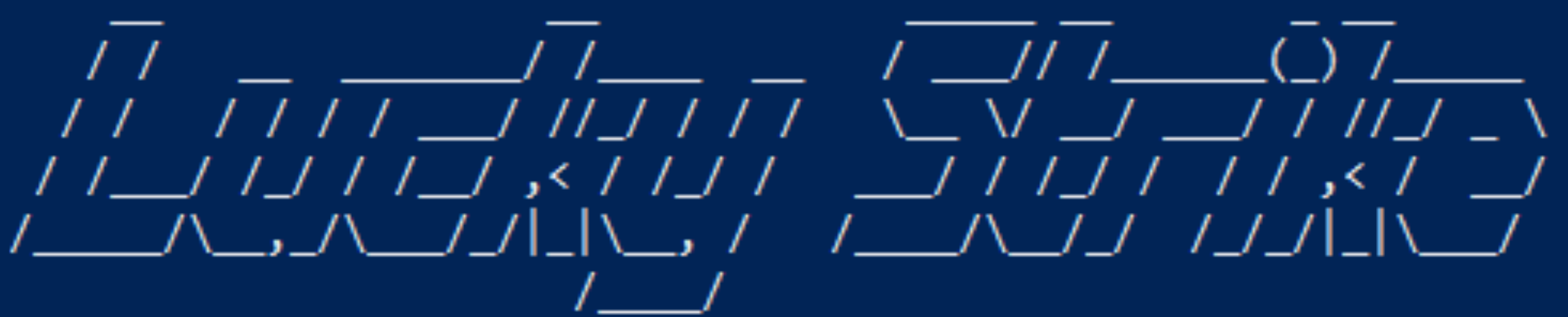
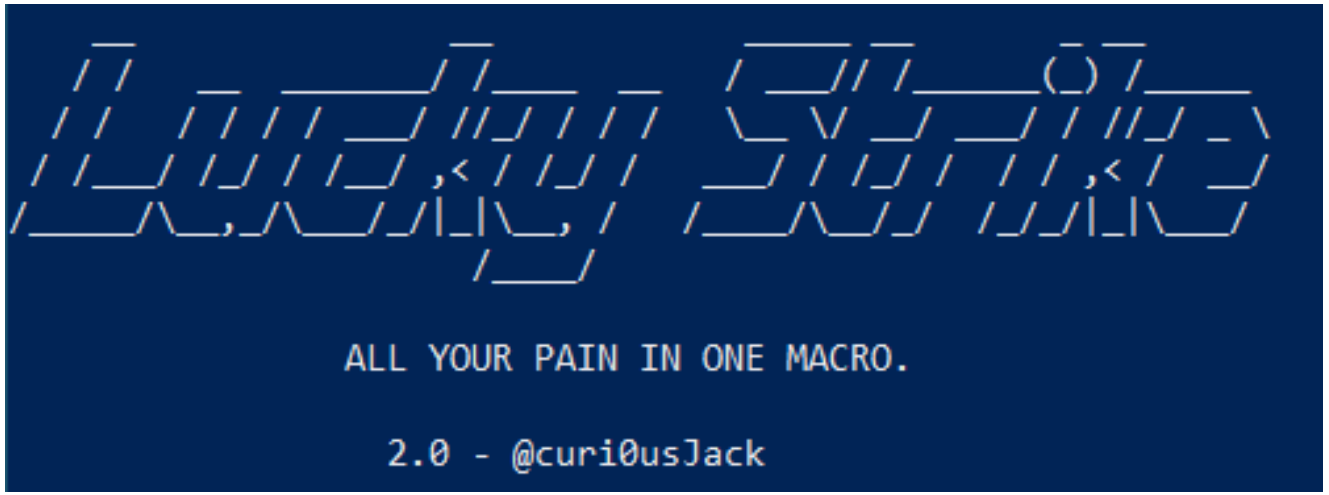
Initial Access with Lucky Strike

Dr. Josh Stroschein
MALWARE ANALYST AND SECURITY RESEARCHER

@jstrosch 0xevilc0de.com



ALL YOUR PAIN IN ONE MACRO.



Creator: Jason Lang / curi0usJack

Generating a malicious macro doc is something that every pentester is well acquainted with. Malicious macros are used all the time to gain footholds when other attacks don't work. Lucky Strike attempts to automate as much as possible, allows for payload reuse, and include as many built in AV evasion techniques as possible

PowerShell framework

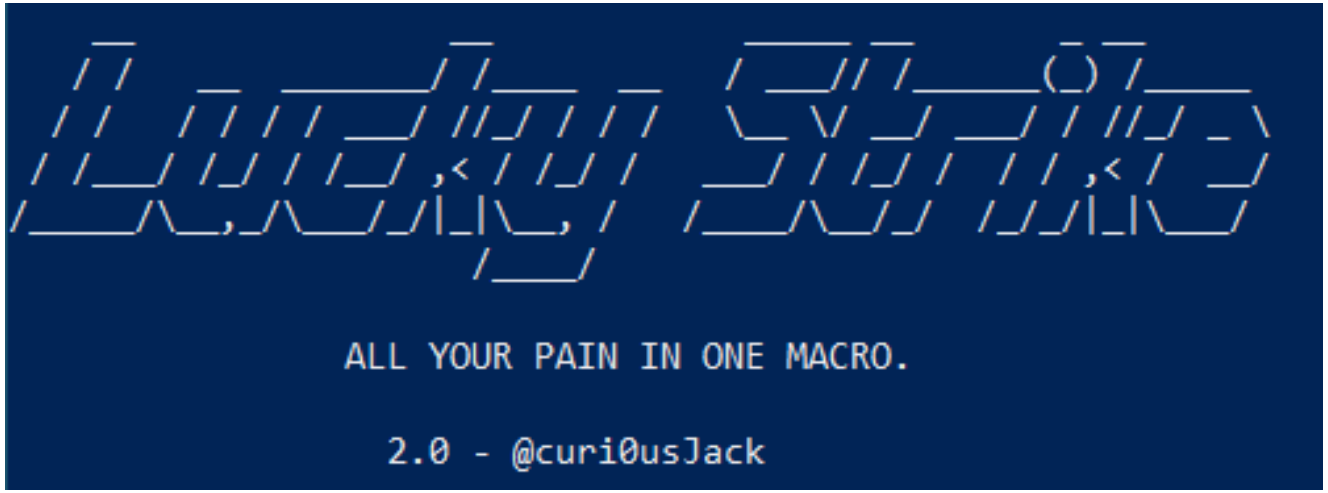
Available on GitHub

Generate documents

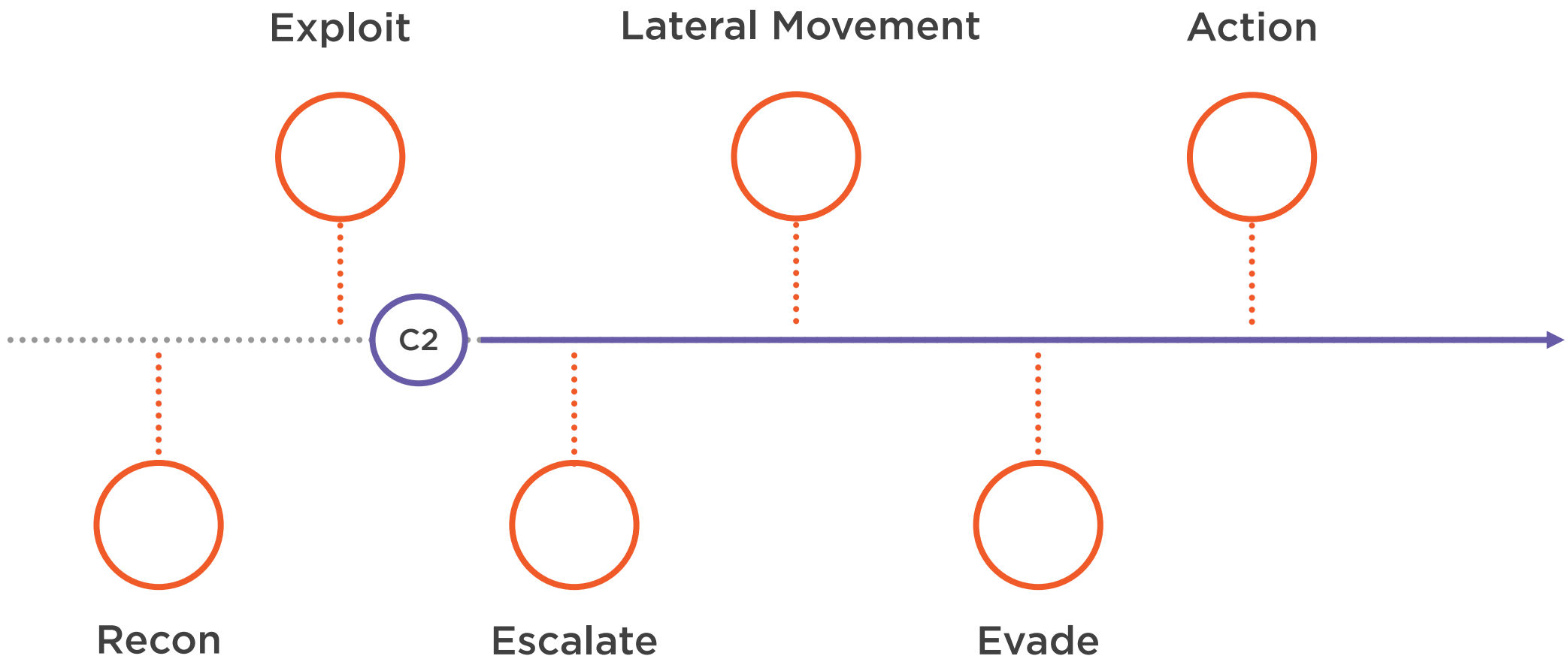
Use templates

Customize payloads

Anti-virus evasion



Kill Chain



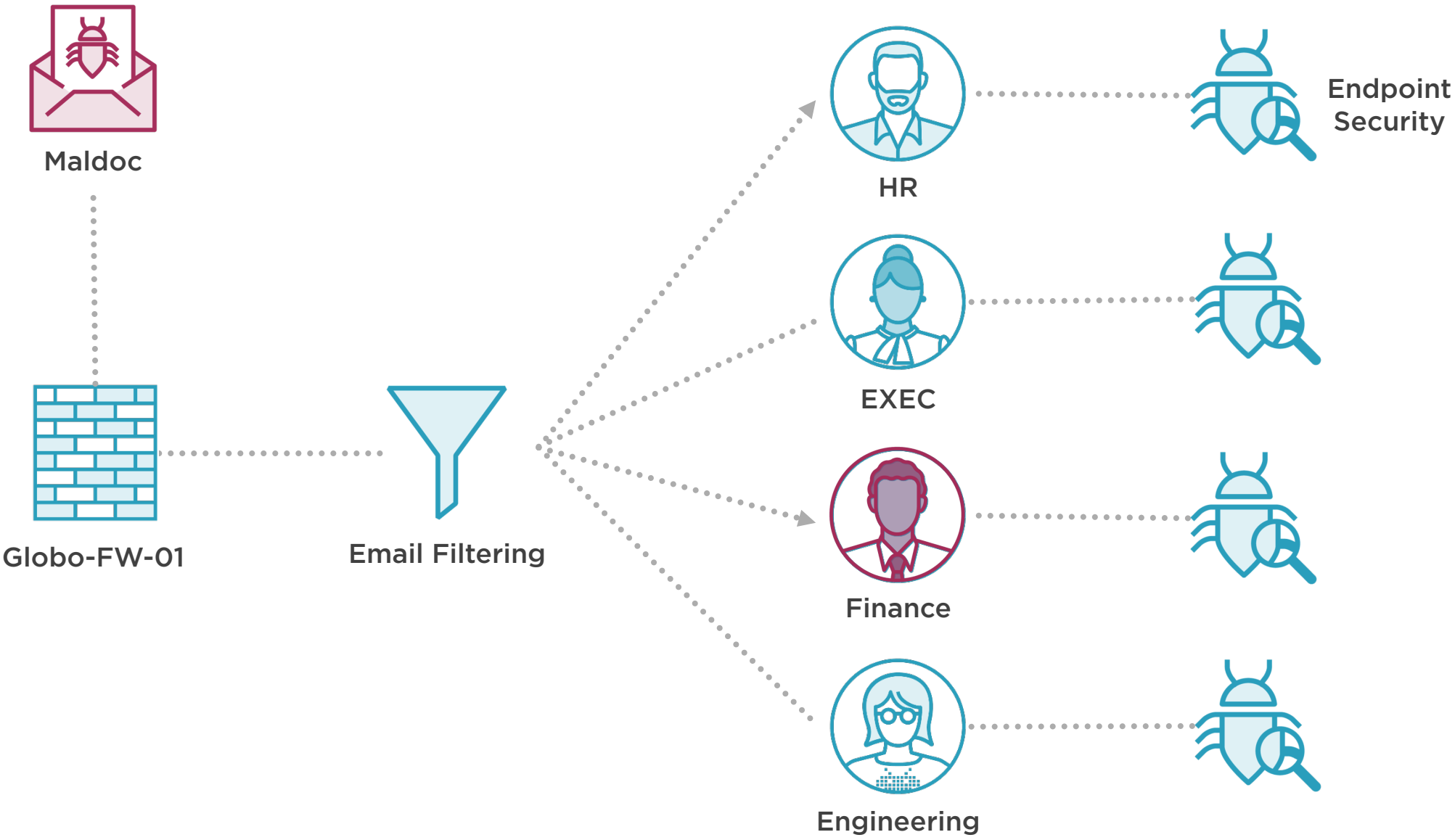
MITRE ATT&CK

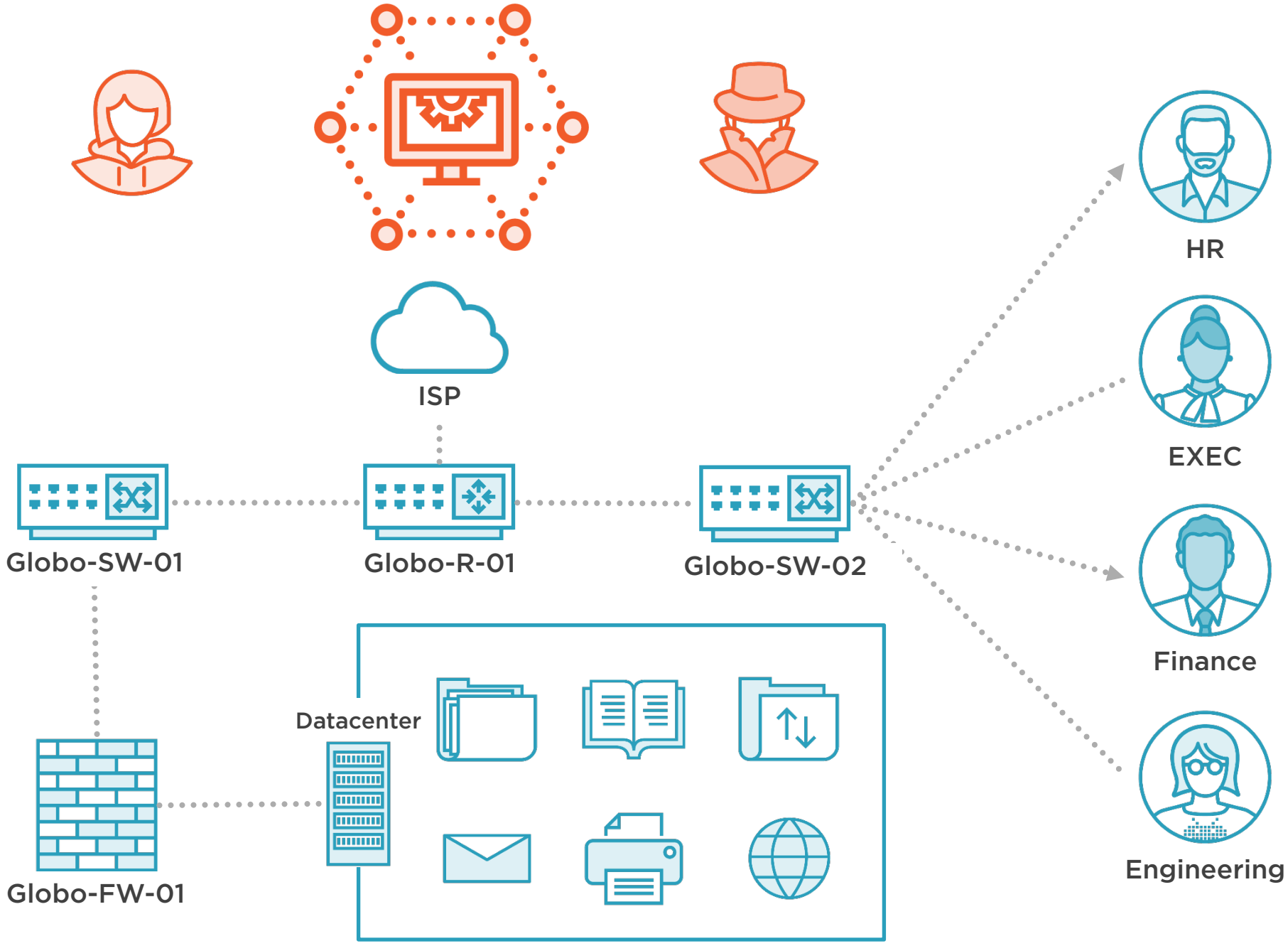
Tactics	Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Command & Control Exfiltration Impact

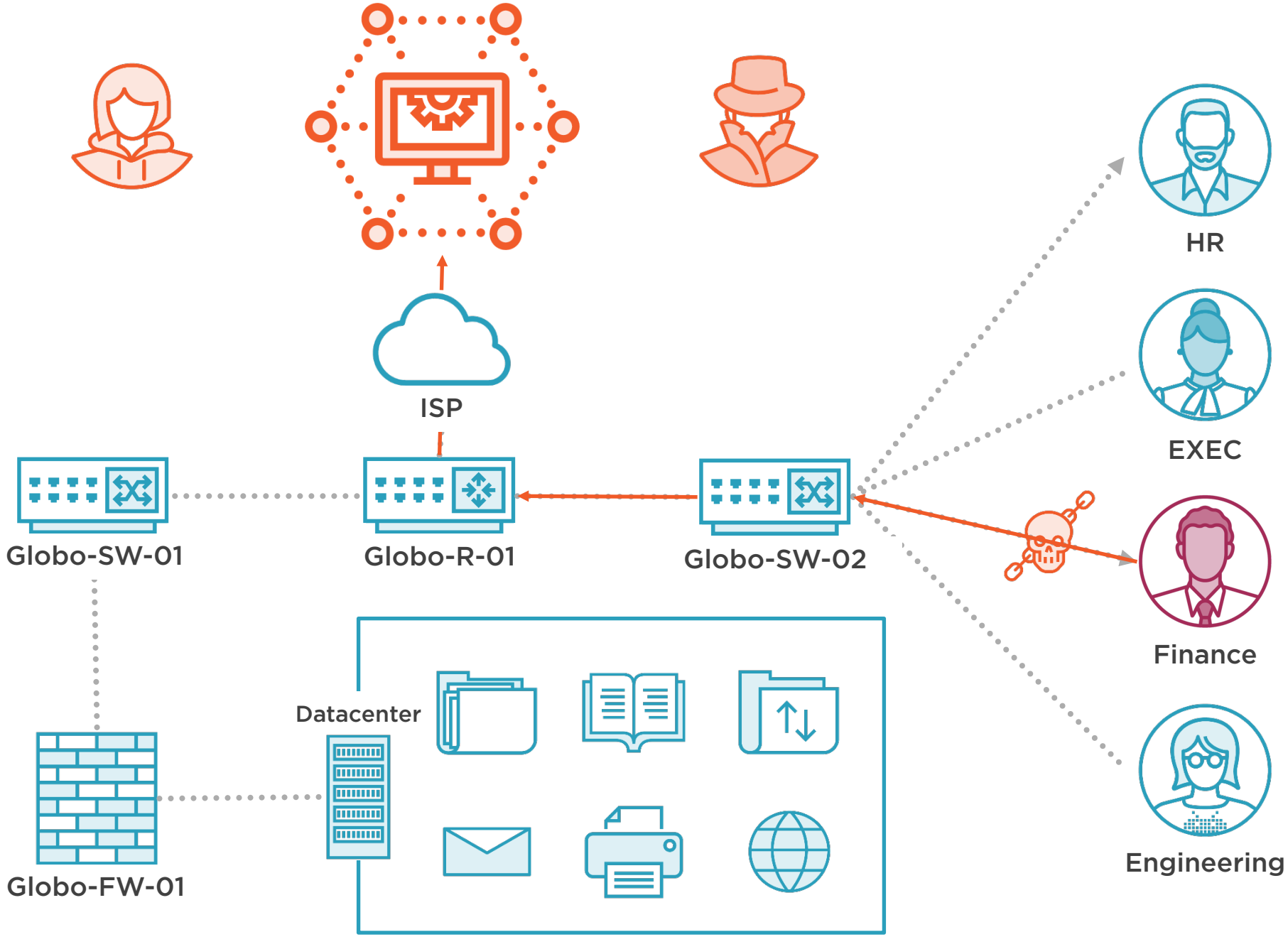
MITRE ATT&CK

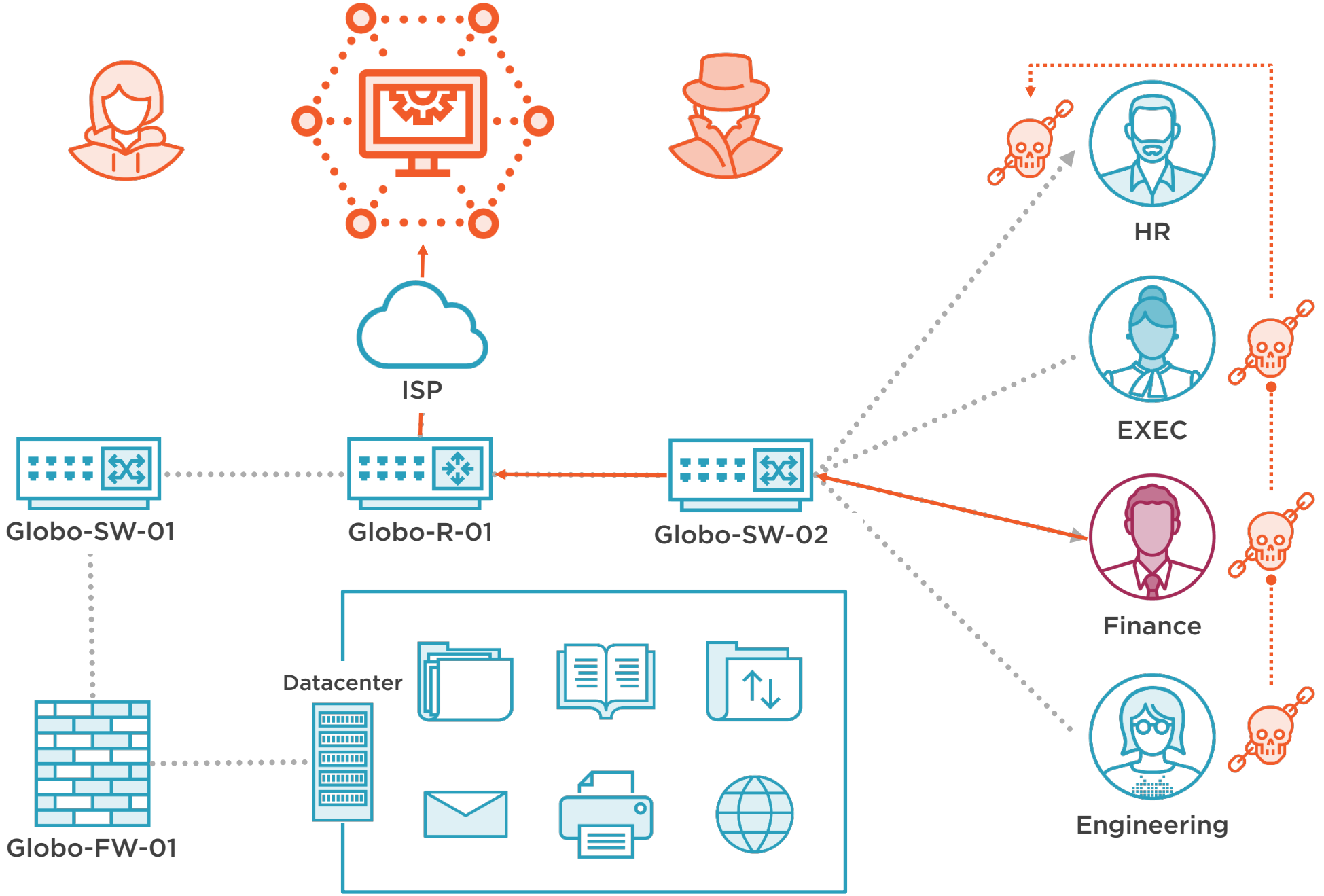
Tactics

- **Initial Access** — T1193: Spearphishing Attachments
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact


Maldoc
Globo-FW-01
Email Filtering
HR
EXEC
Finance
Engineering
Endpoint
Security


ISP
Globo-SW-01
Globo-R-01
Globo-SW-02
HR
EXEC
Finance
Engineering
Datacenter
Globo-FW-01


ISP
Globo-SW-01
Globo-R-01
Globo-SW-02
HR
EXEC
Finance
Engineering
Datacenter
Globo-FW-01


ISP
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter
HR
EXEC
Finance
Engineering

Demo

Prepare our host for installation

Install Lucky Strike

Install Invoke-Obfuscation

Ensure Lucky Strike is operational

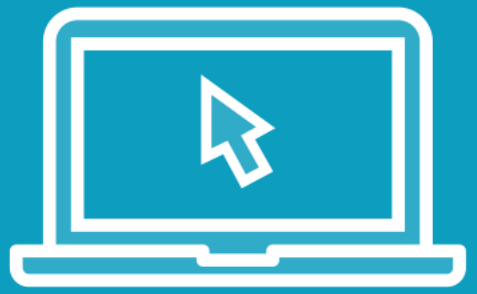
Demo

Discuss payloads and catalogs

Create a maldoc using shell command

Create a maldoc using PowerShell

Demo



Discuss templates

Add and utilize a custom template

Analyze generated macro code

Demo

Discuss how to add an executable payload

Discuss how to use PowerShell generated from the Unicorn framework

Decode PowerShell for use in Lucky Strike

More Information

Capabilities

Framework and resources:

https://github.com/curi0usJack/luckystrike

https://github.com/danielbohannon/Invoke-Obfuscation

Macro generators:

https://github.com/trustedsec/unicorn

https://github.com/rapid7/Metasploit-framework/wiki

Related Information

Info about specific tactic category.

https://attack.mitre.org/tactics/TA0001/

List of subjects in the area

- Custom payloads
- Establishing persistence
- Lateral movement