

Evading Detection on the Network



William Hardy
Security Engineer





Encoding the payload

SSL certificates

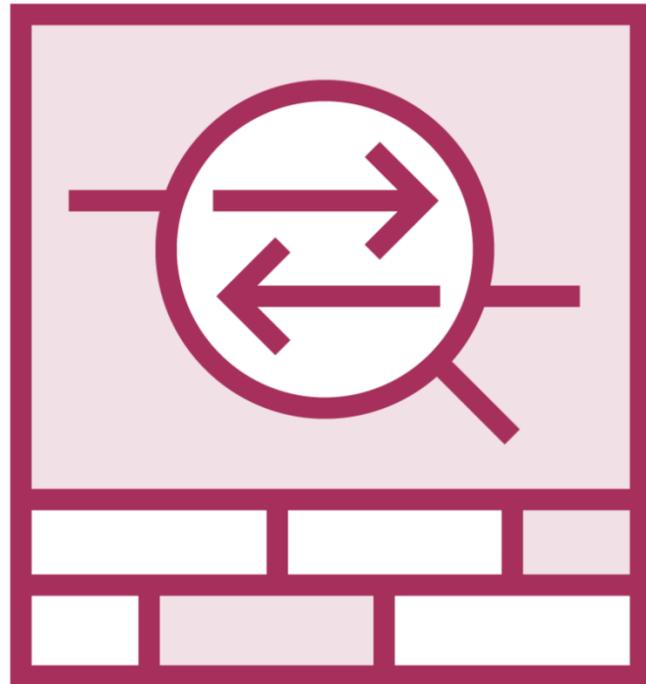
Ja3/Ja3s fingerprints

Tips and tricks

Demo



Encoding the Payload



Signatures are also used on the network and can detect our payload when the handler sends it back to the stager



We can avoid this by encoding the payload before sending it back to the stager



SSL Certificates



When using HTTPS stagers, make sure you don't use the default certificate

Some IDS and antivirus solutions have a signature on the certificate



Ja3/Ja3s Fingerprints

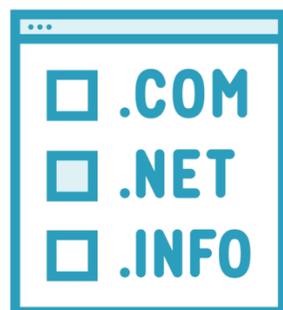


Ja3/Ja3s fingerprints can be used to identify a stager connection to a Metasploit handler

This fingerprint can be altered by using alternate TLS ciphers.



Tips and Tricks



Domain fronting to evade domain categorization filters and SSL interception



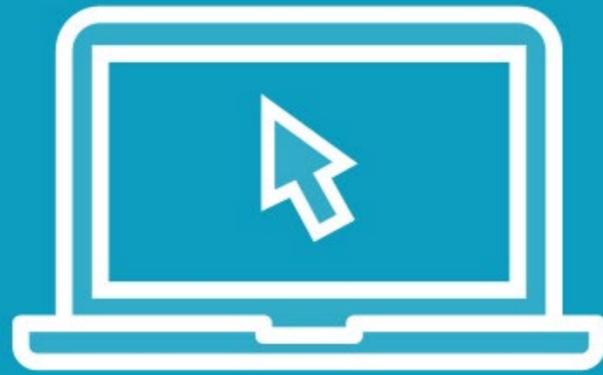
Realistic user-agents, headers and authentication



Stage-less payloads can be used to avoid sending the payload through the network



Demo



Payload Encoding

- Evading Windows Defender
- Evading ClamAV on the Network

