#C2MATRIX
A COMPARISON OF C2 FRAMEWORKS

PRESENTED BY
@JORGEORCHILLES
Jorge Orchilles
C2 Matrix Speaker

Leads the offensive security team at a large financial institution.

Published author with industry contributions including:

- Common Vulnerability Scoring System (CVSSv3.1)
- Threat-led penetration testing framework (GFMA)
- SANS Certified Instructor
- Author of SEC564: Red Team Exercises and Adversary Emulation
- ISSA fellow
- Board of the ISSA South Florida since 2010
- Author of Windows 7 Administrators Reference

@JORGEORCHILLES
/IN/JORGEORCHILLES/
➢ Python2 server; *nix and windows agents
➢ Automatically configures lightweight agents with listener
➢ C2 via http or https (proxy aware) as beacons
➢ Cryptographically secure communication (regardless of TLS)
➢ Rapid deployment of post-exploitation modules, with a variety of module types: powersploit, powerbreach, powerup, powerview
➢ Reliable, consistent, not many bugs; operational security!
➢ Thank you! @Harmj0y | @sixdub | @enigma0x3 rvrsh3ll | @killswitch_gui | @xorrior

EMPIRE WAS THE BEST...
"The project's time has passed and newer frameworks with better capabilities have been released. So it is time to say farewell to EMPIRE"
THE MISSION

Choose the best modern, replacement for Empire. One that is reliable, consistent, user-friendly and that meets these requirements.
OUR REQUIREMENTS

- Operationally secure
- Multiple C2 channels
- Multiple agents/payloads
- Custom profiles
- Domain fronting capable
- Proxy aware
- Internal pivoting
- Multi-user
- Community involvement
THERE ARE A LOT OF DIFFERENT FRAMEWORKS

30 TO BE EXACT
FRAMEWORKS

➢ APFELL
➢ C3
➢ CALDERA
➢ COBALT STRIKE
➢ COVENANT
➢ EMPIRE
➢ EVILOSX
➢ FACTION C2
➢ FLYINGAFALSEFLAG
➢ GODOH
➢ IBOMBSHELL
➢ INNUENDO
➢ KOADICC3
➢ MACSHELLSWIFT
➢ MERLIN
➢ NUAGES
➢ POSHC2
➢ POSHC2_PYTHON
➢ POWERHUB
➢ PRISMATICA
➢ PUPY
➢ QUASARRAT
➢ RED TEAM TOOLKIT
➢ REDVIPER
➢ SCYTHE
➢ SILENT TRINITY
➢ SLIVER
➢ THROWBACK
➢ TREVOR C2
➢ VOODOO

A SPECIAL THANK YOU TO ALL CONTRIBUTING DEVELOPERS!!!!

@JORGEORCHILLES
Phase 1
➢ Evaluate and document all C2 frameworks
➢ Focus on communication channel and C2 features

Phase 2
➢ Post exploitation features, lateral movement, ATT&CK mapping

Phase 3?
➢ You tell us
<table>
<thead>
<tr>
<th>INITIAL ACCESS</th>
<th>EXECUTION</th>
<th>PERSISTENCE</th>
<th>PRIVILEGE ESCALATION</th>
<th>DEFENSIVE EVASION</th>
<th>CREDENTIAL ACCESS</th>
<th>DISCOVERY</th>
<th>LATERAL MOVEMENT</th>
<th>COLLECTION</th>
<th>COMMAND AND CONTROL</th>
<th>EXFILTRATION</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRIVE-BY COMPROMISE</td>
<td>APPSCRIPT</td>
<td>.BASH_PROFILE AND .BASHRC</td>
<td>ACCESS TOKEN MANIPULATION</td>
<td>ACCESS TOKEN MANIPULATION</td>
<td>ACCOUNT MANIPULATION</td>
<td>ACCOUNT DISCOVERY</td>
<td>APPSCRIPT</td>
<td>AUDIO CAPTURE</td>
<td>COMMONLY USED PORT</td>
<td>AUTOMATED EXFILTRATION</td>
<td>DATA DESTRUCTION</td>
</tr>
<tr>
<td>EXPLOIT PUBLIC-FACING APPLICATION</td>
<td>CMSTP</td>
<td>ACCESSIBILITY FEATURES</td>
<td>ACCESSIBILITY FEATURES</td>
<td>BITS JOBS</td>
<td>BASH HISTORY</td>
<td>APPLICATION WINDOW DISCOVERY</td>
<td>APPLICATION DEPLOYMENT SOFTWARE</td>
<td>AUTOMATED COLLECTION</td>
<td>COMMUNICATION THROUGH REMOVABLE DATA</td>
<td>DATA COMPRESSED</td>
<td>DATA ENCRYPTED FOR IMPACT</td>
</tr>
<tr>
<td>EXTERNAL REMOTE SERVICES</td>
<td>COMMAND-LINE INTERFACE</td>
<td>ACCOUNT MANIPULATION</td>
<td>APPCERT DLLS</td>
<td>DINARY PADDING</td>
<td>BRUTE FORCE</td>
<td>BROWSER BOOKMARK DISCOVERY</td>
<td>DISTRIBUTED COMPONENT OBJECT MODEL</td>
<td>CLIPBOARD DATA</td>
<td>CONNECTION PROXY</td>
<td>DATA ENCRYPTED</td>
<td>DEFACTION</td>
</tr>
<tr>
<td>HARDWARE ADDITIONS</td>
<td>COMPILED HTML FILE</td>
<td>APPCERT DLLS</td>
<td>APPINIT DLLS</td>
<td>ACCOUNT CONTROL BYPASS USER</td>
<td>CREDENTIAL DUMPING</td>
<td>DOMAIN TRUST DISCOVERY</td>
<td>EXPLOITATION OF REMOTE SERVICES</td>
<td>DATA STAGE</td>
<td>CUSTOM COMMAND AND CONTROL PROTOCOL</td>
<td>DATA TRANSFER SIZE LIMIT</td>
<td>DISK CONTENT WIPE</td>
</tr>
<tr>
<td>REPLICATION THROUGH REMOVABLE MEDIA</td>
<td>CONTRLR PANEL ITEMS</td>
<td>APPINIT DLLS</td>
<td>APPLICATION SHIMMIMG</td>
<td>CMSTP</td>
<td>CREDENTIALS IN FILES</td>
<td>FILE AND DIRECTORY DISCOVERY</td>
<td>LOGON SCRIPT</td>
<td>DATA FROM INFORMATION REPOSITORIES</td>
<td>CUSTOM CRYPTOGRAPHIC PROTOCOL</td>
<td>EXFILTRATION OVER ALTERNATIVE PROTOCOL</td>
<td>DISK STRUCTURE WIPE</td>
</tr>
<tr>
<td>SPEARPHISHING ATTACHMENT</td>
<td>DYNAMIC DATA EXCHANGE</td>
<td>APPLICATION SHIMMIMG</td>
<td>BYPASS USER ACCOUNT CONTROL</td>
<td>CLEAR COMMAND HISTORY</td>
<td>CREDENTIALS IN REGISTRY</td>
<td>NETWORK SERVICE SCANNING</td>
<td>PASS THE HASH</td>
<td>DATA FROM LOCAL SYSTEM</td>
<td>DATA ENCODING</td>
<td>EXFILTRATION OVER COMMAND AND CONTROL CHANNEL</td>
<td>ENDPOINT DENIAL OF SERVICE</td>
</tr>
<tr>
<td>SPEARPHISHING LINK</td>
<td>EXECUTION THROUGH API</td>
<td>AUTHENTICATION PACKAGE</td>
<td>DLL SEARCH ORDER HUACKING</td>
<td>CODE SIGNING</td>
<td>EXPLOITATION FOR CREDENTIAL ACCESS</td>
<td>NETWORK SHARE DISCOVERY</td>
<td>PASS THE TICKET</td>
<td>DATA FROM NETWORK SHARE DRIVE</td>
<td>DATA OBFUSCATION</td>
<td>EXFILTRATION OVER OTHER NETWORK MEDIUM</td>
<td>Firmware CORRUPTION</td>
</tr>
</tbody>
</table>
- TCP (DIRECT)
- HTTP
  - PROXY AWARE
  - DOMAIN FRONTING
  - CUSTOM PROFILE
- HTTP2
- HTTP3
- DNS
- DOH
- ICMP
- FTP
- IMAP
➢ Consistent connections are poor opsec
   - Meterpreter
   - Koadic (http long poll)
➢ Beacons are better
   - Jitter makes pattern matching a little harder
➢ Working hours
➢ Kill date
<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SlackToken</td>
<td>False</td>
<td>default</td>
</tr>
<tr>
<td>ProxyCreds</td>
<td>False</td>
<td>default</td>
</tr>
<tr>
<td>KillDate</td>
<td>False</td>
<td>12/12/2019</td>
</tr>
<tr>
<td>Name</td>
<td>True</td>
<td>http</td>
</tr>
<tr>
<td>Launcher</td>
<td>True</td>
<td>powershell -noP -sta -w 1 -enc 5</td>
</tr>
<tr>
<td>DefaultDelay</td>
<td>True</td>
<td>0</td>
</tr>
<tr>
<td>DefaultLostLimit</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>WorkingHours</td>
<td>False</td>
<td>#general</td>
</tr>
<tr>
<td>SlackChannel</td>
<td>False</td>
<td>/admin/get.php,/news.php,/login/ process.php</td>
</tr>
<tr>
<td>DefaultProfile</td>
<td>True</td>
<td>/opt/empire/data/</td>
</tr>
<tr>
<td>Host</td>
<td>True</td>
<td><a href="https://10.0.0.11:443">https://10.0.0.11:443</a></td>
</tr>
<tr>
<td>CertPath</td>
<td>False</td>
<td>/opt/empire/data/</td>
</tr>
<tr>
<td>Default3litter</td>
<td>True</td>
<td>0.5</td>
</tr>
<tr>
<td>Proxy</td>
<td>False</td>
<td>default</td>
</tr>
<tr>
<td>UserAgent</td>
<td>False</td>
<td>default</td>
</tr>
<tr>
<td>StagingKey</td>
<td>True</td>
<td>bbff1e3b338c39a6782e0d19283ff247</td>
</tr>
<tr>
<td>BindIP</td>
<td>True</td>
<td>10.0.0.11</td>
</tr>
<tr>
<td>Port</td>
<td>True</td>
<td>443</td>
</tr>
<tr>
<td>ServerVersion</td>
<td>True</td>
<td>Microsoft-IIS/7.5</td>
</tr>
<tr>
<td>StagerURI</td>
<td>False</td>
<td>/download/</td>
</tr>
</tbody>
</table>
**USER INTERFACE**
- Command Line Interface
- Graphical User Interface
- Web
- API
- Multi-Player: the “Team” part of “Red Team”
OPERATIONAL SECURITY

➢ Key exchange regardless of TLS
  – Encrypted Key Exchange
  – aPAKE OPAQUE
  – ECDHE
  – mTLS
  – AES
➢ Warning for bad OPSEC
➢ Know your IOCs!
  – Sysmon
  – Wireshark/tcpdump

```
sliver (REGULAR_TORSO) > shell
? This action is bad OPSEC, are you an adult? No
```
DEMO TIME

www.thec2matrix.com
➢ James Tubberville post on threatexpress.com:


➢ Alex Rodriguez from Secure Ideas:


➢ The Golden Age of C2 by Matthew Toussain on YouTube:

https://www.youtube.com/watch?v=DjChyUrbZd8
THANK YOU

@brysonbort
@Adam_Mashinchi
@cabbagesalad2
@seanqsun
@P1nkFlam1ngo17

@0sm0s1z
@Ne0nd0g
@its_a_feature_
@byt3bl33d3r
@daveaitel
Q & A

#c2matrix

www.thec2matrix.com