RE://TERNAL C2

MITRE ATT&CK BASED COMMAND AND CONTROL

Joey Dreijer
joey.dreijer@ing.com

09-05-2019

THE FIRM
TECHNOLOGIES

WHOAMI

Joey Dreijer
Threat Hunter
Security Defense Center - ING Bank

Focus

1. Python
2. Python
3. …
4. Python
5. “Intensive API abuser” ~ Anonymous @ ING

RE://TERNAL

INTRODUCTION

Command and Control Framework

Scenario/Recipe based Command and Control

API and backend built in Python + Web UI built with VueJS

Agent built in GoLang
- Cross compiles to Darwin, Linux, Windows, Android, ARM/Raspberry Pi etc

Traditional command/control with **additional** mapping to ATT&CK Framework
- Based on **Uber's METTA** configuration

RE://TERNAL

WHY

Had to find a hobby project (Game of Thrones season ended);

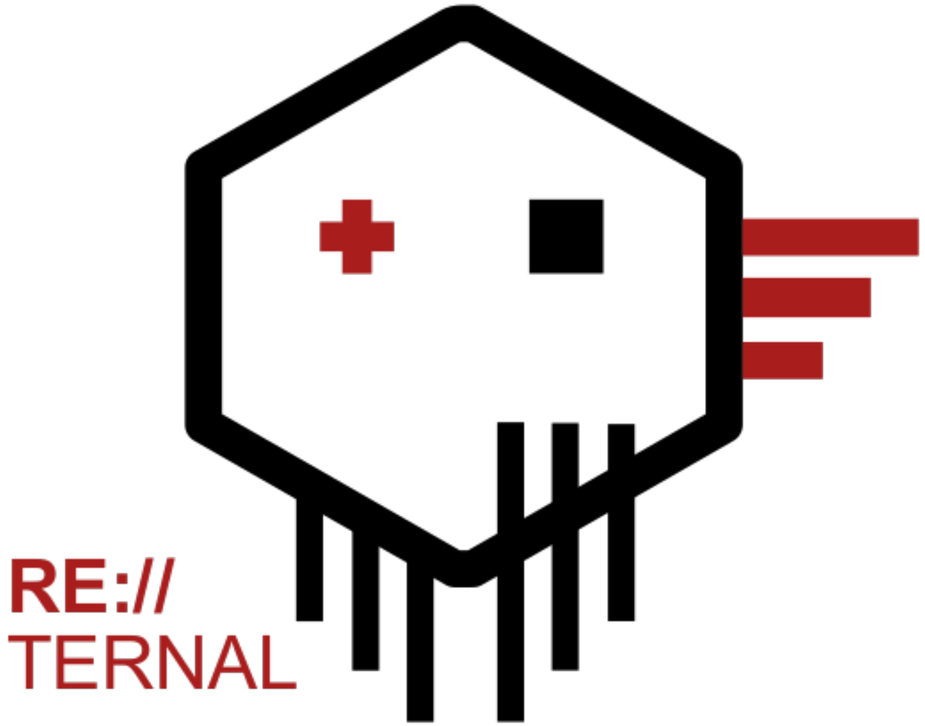
Not bound to ATT&CK:
- Still able to use as a traditional CnC;

More control over what, when and where scenarios or tasks are executed;

Campaign building made easy via clicky/drag UI;

Flexibility in native code and OS API’s for tasks instead of commandline input;

DEMO



ROADMAP

CURRENTLY IN DEVELOPMENT

Finalize core project

- Traffic encryption via key exchange, code cleanup, bug fixes, ansible playbooks

Automated pivot discovery

- Using mDNS/Bonjour to automatically find and relay via other OSX agents

Conditional execution

- Execute tasks on agent ‘X’ when agent ‘Y’ returns ‘Z’

Timeline for tasks execution

Task scoring status

- Ability to rate successful execution of tasks vs. failed in mapping

CONFIG SAMPLE

WITHOUT USING SHELL

```
name: Download latest Game of Thrones Episode
author: JD
description: Download the latest GoT episode from series-online via built-
in Agent HTTP downloader
mitre_technique:
  id: T1337
  platform: Windows
commands:
- type: read_file
  input: https://super-illegal-series-online.tk/
 Game_of_Thrones_EP8.05-1080P[EN].mp4
  sleep: 1
```

CONFIG SAMPLE

WITHOUT USING SHELL

```
name: Steal password written on Windows Vista desktop post-it
author: JD
description: Silly user printed a password on his desktop postit. Create a
screenshot and steal the credz
mitre_technique:
  id: T1113
  platform: Windows
commands:
- type: make_screenshot
  sleep: 1
```

www-data
195.169.160.152
Offline
2019-04-17 02:05:25

History Tasks

www-data
195.169.160.149
Offline
2019-04-17 02:10:34

History Tasks

www-data
195.169.160.146
Offline
2019-04-17 02:19:15

History Tasks

www-data
195.169.160.152
Offline
2019-04-17 02:05:25

History Tasks

www-data
195.169.160.141
Offline
2019-04-17 02:50:39

History Tasks

www-data
195.169.160.132
Offline
2019-04-17 03:20:13

History Tasks

www-data
195.169.160.130
Offline
2019-04-17 03:26:46

History Tasks

www-data
195.169.160.141
Offline
2019-04-17 02:50:39

History Tasks

www-data
195.169.160.244
Offline
2019-04-17 03:49:11

History Tasks

www-data
195.169.160.243
Offline
2019-04-17 04:00:38

History Tasks

www-data
195.169.160.234
Offline
2019-04-17 04:32:06

History Tasks

www-data
195.169.160.244
Offline
2019-04-17 03:49:11

History Tasks

www-data
195.169.160.233
Offline
2019-04-17 04:35:50

History Tasks

www-data
195.169.160.232
Offline
2019-04-17 04:43:19

History Tasks

www-data
195.169.160.226
Offline
2019-04-17 04:49:36

History Tasks

www-data
195.169.160.233
Offline
2019-04-17 04:35:50

History Tasks

www-data
195.169.160.224
Offline
2019-04-17 04:54:41

History Tasks

www-data
195.169.160.220
Offline
2019-04-17 05:00:29

History Tasks

www-data
195.169.160.217
Offline
2019-04-17 05:09:38

History Tasks

www-data
195.169.160.224
Offline
2019-04-17 04:54:41

History Tasks

www-data
195.169.160.215
Offline
2019-04-17 05:13:56

History Tasks

www-data
195.169.160.214
Offline
2019-04-17 05:17:14

History Tasks

www-data
195.169.160.205
Offline
2019-04-17 05:27:39

History Tasks

www-data
195.169.160.215
Offline
2019-04-17 05:13:56

History Tasks

THANK YOU

Git: https://github.com/d3vzer0/
Twitter: @joeydreijer