Turning Your TableTop Exercises Into Action!!

ResponderCon

$ WHOAMI

Ali Hadi
@binaryz0ne

Dylan Navarrow
@Chromosom3_

CYBER5W

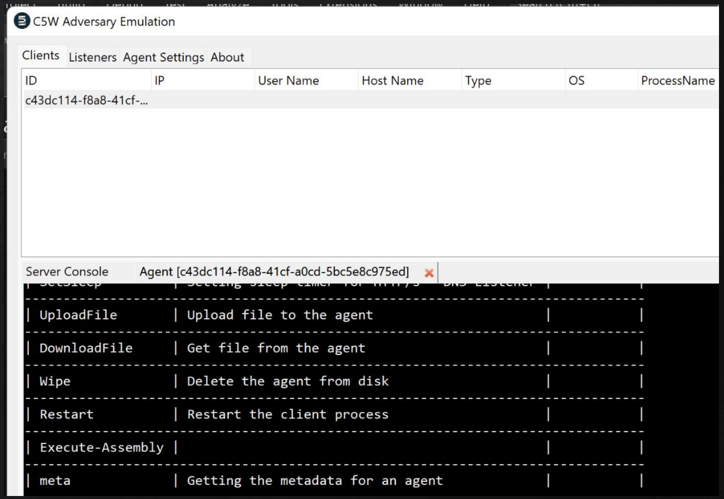
Shady Shaheen
@Th3Hunger_

Samuel Barrows
@inst4ll3rwizard

Champlain College

Workshop is Not!!!

- ✘ About reverse engineering ransomware
- ✘ About decrypting ransomed files
- ✘ How to compromise networks
- ✘ How to catch threat actors



C5W Adversary Emulation

ID	IP	User Name	Host Name	Type	OS	ProcessName
c43dc114-f8a8-41cf-...						

```
| SetSleep        | Setting sleep timer for HTTP/S - DNS Listener |            |
--------------------------------------------------------------------------------
| UploadFile      | Upload file to the agent                      |            |
--------------------------------------------------------------------------------
| DownloadFile    | Get file from the agent                       |            |
--------------------------------------------------------------------------------
| Wipe            | Delete the agent from disk                    |            |
--------------------------------------------------------------------------------
| Restart         | Restart the client process                    |            |
--------------------------------------------------------------------------------
| Execute-Assembly |                                              |            |
--------------------------------------------------------------------------------
| meta            | Getting the metadata for an agent             |            |
```

Workshop Format

- ✘ Isolated Environment
  - ○ Windows Domain with Multiple Client Systems and ELK
  - ○ Human Ransomware Operator → Us 👻😈
  - ○ Ransomware Victim → You 😁

- ✘ Cover multiple ransomware simulations
- ✘ Not much on Theory we already learned a lot from ResponderCon presentations, but more on the hands-on stuff...
- ✘ Learn how to detect Ransomware and respond using free tools!

Assumptions…

- ✘ We already have access to victim network|system through an IAB
- ✘ Agent already delivered to victim's system through DC
    - ○ Run it with administrator 😅😁😋

- ✘ The presentation is used for introducing the simulations covered, but the work is done using the manuals so we can *learn be doing*…

Another Adversary Simulation System?

#1: Plugin-Engine

- ✘ Load and unload at runtime
- ✘ Extend Capabilities with New Tools

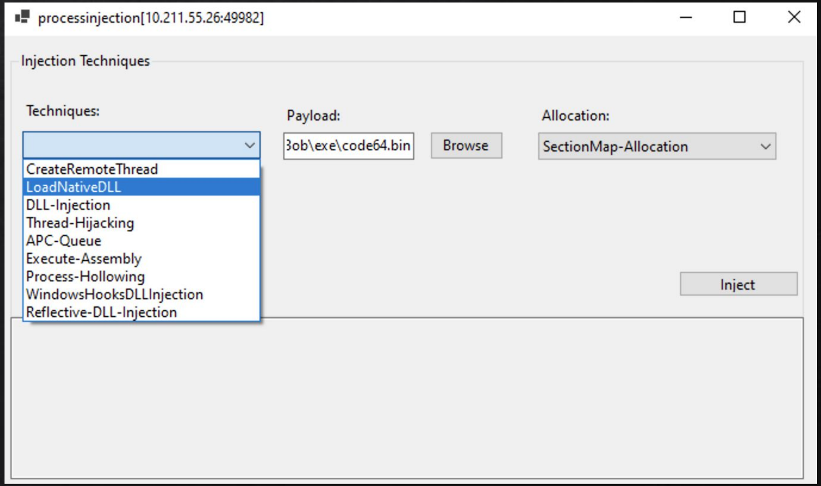
#2: Core System Control

- ✘ Upload/Download files, meta, etc

#3: Multi-Injection Techniques

- ✘ Thread Hijacking, APC Queue, DLL Injection, Process Hollowing, Reflective DLL Injection, Shellcode RDI, others...

Started as a hobby to learn offensive coding and create educational scenarios that we can use to help our students practice on true incidents...



processinjection[10.211.55.26:49982]

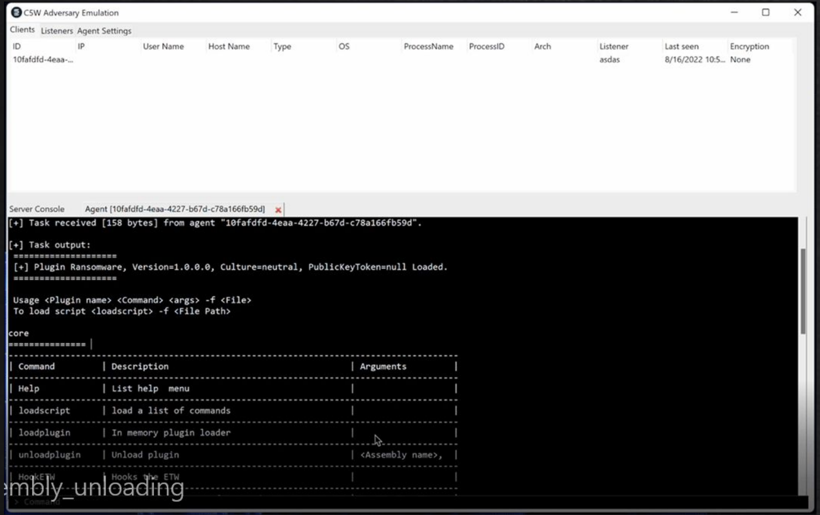
Injection Techniques

Techniques:

Payload: 3ob\exe\code64.bin

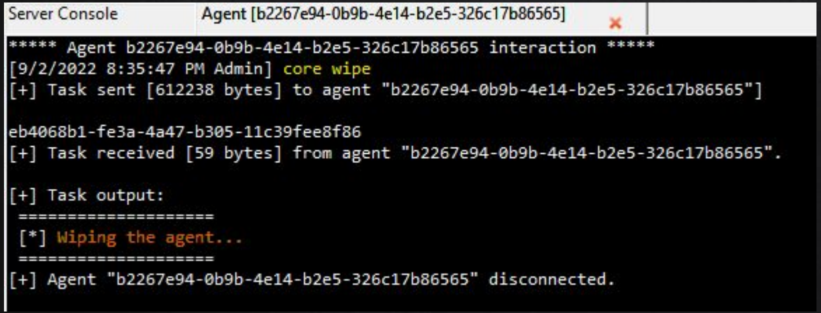
Allocation: SectionMap-Allocation

Another Adversary Simulation System? – Cont.



ID	IP	User Name	Host Name	Type	OS	ProcessName	ProcessID	Arch	Listener	Last seen	Encryption
10fafdfd-4eaa-...									asdas	8/16/2022 10:5...	None

```
[+] Task received [158 bytes] from agent "10fafdfd-4eaa-4227-b67d-c78a166fb59d".

[+] Task output:
 ====================
 [+] Plugin Ransomware, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null Loaded.
 ====================

 Usage <Plugin name> <Command> <args> -f <File>
 To load script <loadscript> -f <File Path>

core
=============== |
------------------------------------------------------------------------------------------
| Command         | Description                                           | Arguments      |
------------------------------------------------------------------------------------------
| Help            | List help  menu                                       |                |
------------------------------------------------------------------------------------------
| loadscript      | load a list of commands                               |                |
------------------------------------------------------------------------------------------
| loadplugin      | In memory plugin loader                               |                |
------------------------------------------------------------------------------------------
| unloadplugin    | Unload plugin                                         | <Assembly name>, |
------------------------------------------------------------------------------------------
| HookETW         | Hooks the ETW                                         |                |
------------------------------------------------------------------------------------------
```



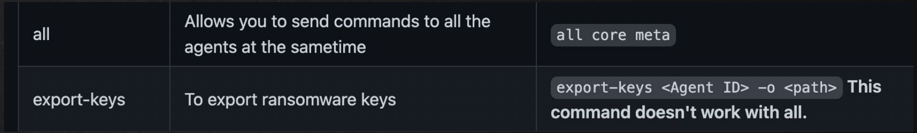
```
***** Agent b2267e94-0b9b-4e14-b2e5-326c17b86565 interaction *****
[9/2/2022 8:35:47 PM Admin] core wipe
[+] Task sent [612238 bytes] to agent "b2267e94-0b9b-4e14-b2e5-326c17b86565"]

eb4068b1-fe3a-4a47-b305-11c39fee8f86
[+] Task received [59 bytes] from agent "b2267e94-0b9b-4e14-b2e5-326c17b86565".

[+] Task output:
 ====================
 [*] Wiping the agent...
 ====================
[+] Agent "b2267e94-0b9b-4e14-b2e5-326c17b86565" disconnected.
```

#4: Multi-Communication Channels

- ✗ TCP, HTTP, and DNS

#5: Multi-Crypto Methods

- ✗ AES (128, 192, and 256),
- ✗ Hybrid RSA + AES → (Very soon)



all	Allows you to send commands to all the agents at the sametime	`all core meta`
export-keys	To export ransomware keys	`export-keys <Agent ID> -o <path>` **This command doesn't work with all.**

#6: Anti-Forensics

- ✗ Unload Plugin from Memory
- ✗ Hooking ETW
- ✗ Wipe Agent
- ✗ More coming…

Malleable C5 Profiles!!!

#1: Sleep Time

- DNS and HTTP

#2: Custom HTTP Headers

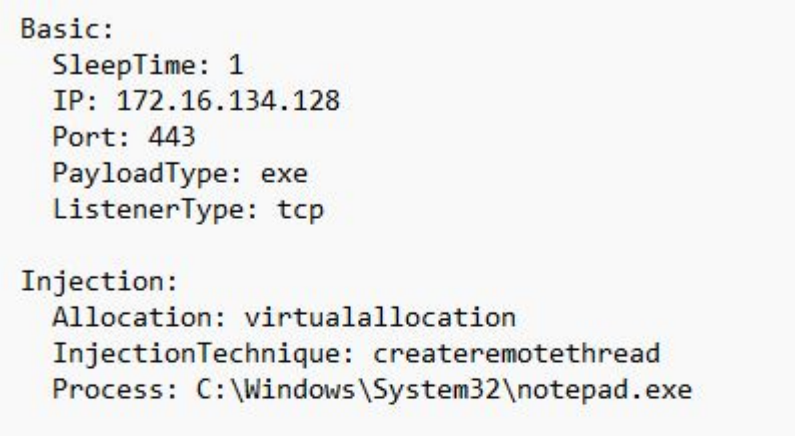
- for both server and client

#3: Network Settings

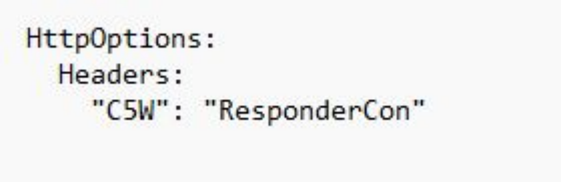
- IP address
- Port #
- Type of Listener

#4: Misc

- Payload Type
- Custom Mutex



```
Basic:
  SleepTime: 1
  IP: 172.16.134.128
  Port: 443
  PayloadType: exe
  ListenerType: tcp

Injection:
  Allocation: virtualallocation
  InjectionTechnique: createremotethread
  Process: C:\Windows\System32\notepad.exe
```



```
HttpOptions:
  Headers:
    "C5W": "ResponderCon"
```

Why RansomCare ?...

- ✘ Is a ransomware simulation plugin for our Adversary Simulation system...

Features

#1: Encryption / Decryption

- $ File and Directories
- $ Targeted Extensions
- $ Custom Extensions

#2: Inhibit System Recovery

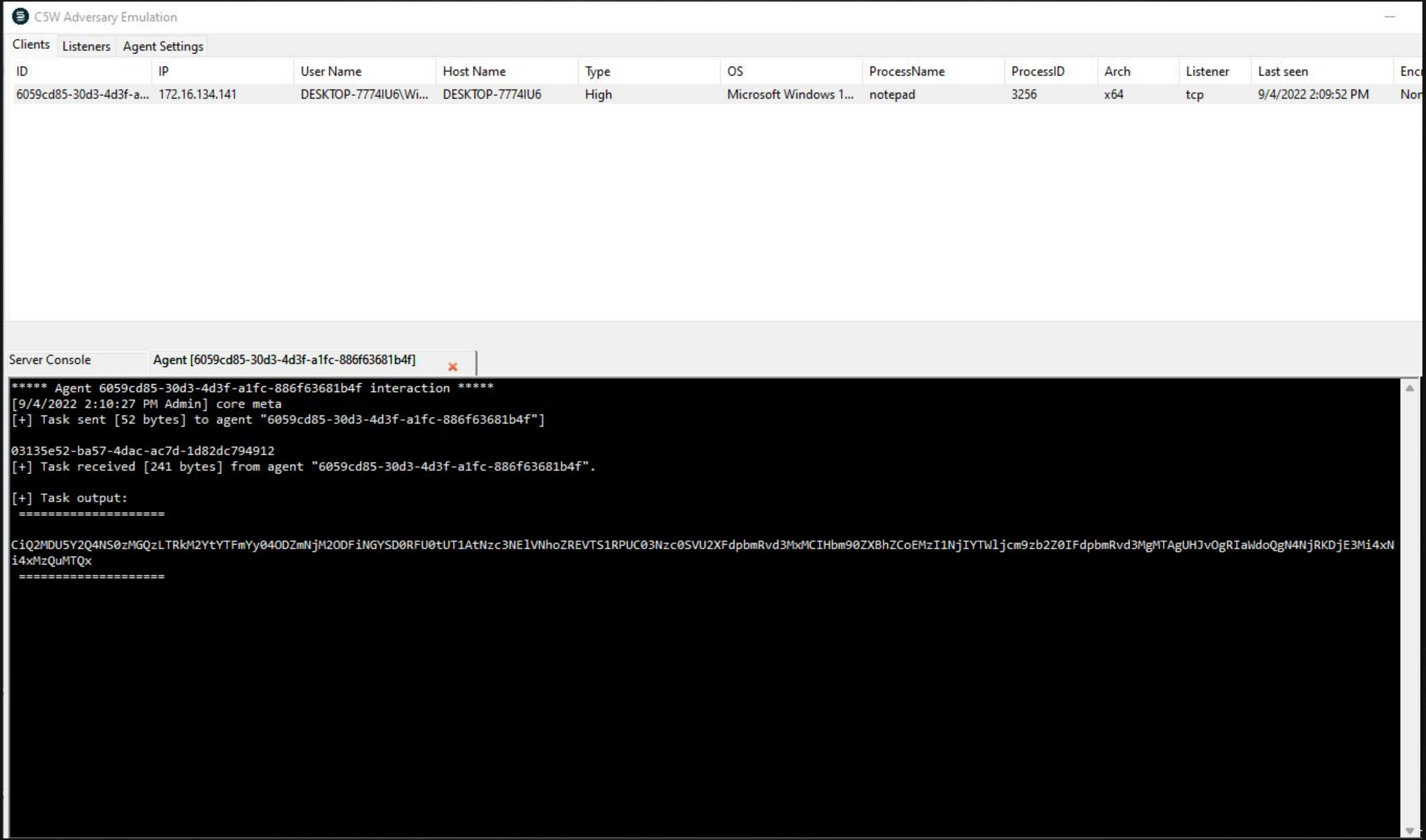
- $ Delete Volume Shadow Copies (VSC)
- $ Delete File and Directories

#3: Miscellaneous

- $ Custom Ransom Notes
- $ Custom Ransom Wallpaper
- $ Memory Based (*process injection*)

#4: Anti-X Techniques

- $ Hook the Event Tracing for Windows
- $ Wipe Ransomware



ID	IP	User Name	Host Name	Type	OS	ProcessName	ProcessID	Arch	Listener	Last seen	Enc
6059cd85-30d3-4d3f-a...	172.16.134.141	DESKTOP-7774IU6\Wi...	DESKTOP-7774IU6	High	Microsoft Windows 1...	notepad	3256	x64	tcp	9/4/2022 2:09:52 PM	Nor

```
***** Agent 6059cd85-30d3-4d3f-a1fc-886f63681b4f interaction *****
[9/4/2022 2:10:27 PM Admin] core meta
[+] Task sent [52 bytes] to agent "6059cd85-30d3-4d3f-a1fc-886f63681b4f"]

03135e52-ba57-4dac-ac7d-1d82dc794912
[+] Task received [241 bytes] from agent "6059cd85-30d3-4d3f-a1fc-886f63681b4f".

[+] Task output:
 ====================

CiQ2MDU5Y2Q4NS0zMGQzLTRkM2YtYTFmYy04ODZmNjM2ODFiNGYSD0RFU0tUT1AtNzc3NElVNhoZREVTS1RPUC03Nzc0SVU2XFdpbmRvd3MxMCIHbm90ZXBhZCoEMzI1NjIYTWljcm9zb2Z0IFdpbmRvd3MgMTAgUHJvOgRIaWdoQgN4NjRKDjE3Mi4xN
i4xMzQuMTQx
 ====================
```

Simulations

-Encrypt and Delete Volume Shadow Copies-

Access Environment...

✘ For your VM, goto → http://10.0.3.3

Username = UserX

Password = Password123!@#

✘ For your ELK Access, goto → http://10.0.2.14:5601

Username = prd-win10-X (x is your hostname)

Password = l0ng-r4nd0m-p@ssw0rd

WHAT IS COVERED?

T1082 + T1055 + T1486 + T1053.005 + T1547.001 + T1490

Technique: System Information Discovery

- ✘ https://attack.mitre.org/techniques/T1082/

Technique: Process Injection

- ✘ https://attack.mitre.org/techniques/T1055/

Technique: Data Encrypted for Impact

- ✘ https://attack.mitre.org/techniques/T1486/

Technique: Scheduled Task/Job

- ✘ https://attack.mitre.org/techniques/T1053/005

Technique: Logon Autostart Execution – Registry Run Keys / Startup Folder

- ✘ https://attack.mitre.org/techniques/T1547/001/

Technique: Inhibit System Recovery

- ✘ https://attack.mitre.org/techniques/T1490/

Simulation #3

-Wipe Implant and RansomCare-

WHAT IS COVERED?

T1486 + T1070.004

Technique #1: Data Encrypted for Impact

- ✘ https://attack.mitre.org/techniques/T1486/

Technique #2: Indicator Removal on Host: File Deletion

- ✘ https://attack.mitre.org/techniques/T1070/004/

Detection

-ideas to detect suspicious activity-

Detection Ideas ?

#1: Encryption / Decryption

- $ File type changes
- $ Extension changes
- $ Trap Files

#2: Inhibit System Recovery

- $ Access to VSC
- $ Keep Your Backups Safe

#3: Miscellaneous

- $ Honeypots and Traps
- $ Monitor Processes
- $ Monitor Crypto APIs Calls
- $ Monitor High Resource Usage

#4: Anti-X Techniques

- $ EDR
- $ AppLocker

MITRE Techniques (Workshop) ?

#: System Information Discovery

https://attack.mitre.org/techniques/T1082/

#: Process Injection

https://attack.mitre.org/techniques/T1055/

#: Data Encrypted for Impact

https://attack.mitre.org/techniques/T1486/

#: Inhibit System Recovery

https://attack.mitre.org/techniques/T1490/

#: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

https://attack.mitre.org/techniques/T1547/001/

#: Scheduled Task/Job: Scheduled Task

https://attack.mitre.org/techniques/T1053/005/

#: Defense Evasion – T1562 Impair Defenses

https://attack.mitre.org/techniques/T1562/

#: OS Credential Dumping: Security Account Manager

https://attack.mitre.org/techniques/T1003/

#: Lateral Tool Transfer (aka Lateral Movement)

https://attack.mitre.org/techniques/T1570/

The End…

–That's All Folks! –

😃

Thank You For Attending!

Any questions?

send them our way
Info [at] advemu [dot] com

Credits & References...

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Adam, Ideas and Blue Team Fingers, @Hexacorn
- Florian Roth, Sigma Rules and others, @cyb3rops
- Velociraptor, hayabusa, chainsaw, NirSoft, etc
- MITRE Framework, https://attack.mitre.org/techniques/
- Sorry if we missed someone!