

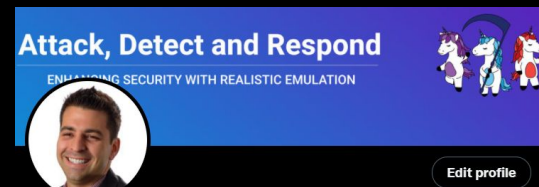
# State of C2 – 2021 Update



@C2\_Matrix

# T1033 - System Owner/User Discovery

- C2 Matrix Co-Creator
- Chief Technology Officer - SCYTHE
- Purple Team Exercise Framework (PTEF)
- 10 years @ Citi leading offensive security team
- Certified SANS Instructor: SEC699, SEC560, SEC504
- Author SEC564: Red Team Exercises and Adversary Emulation
- ISSA & NSI Technologist Fellow
- Contributor
  - MITRE ATT&CK
  - Atomic Red Team
  - CVSSv3.1 Working Group Voting Member
  - GFMA: Threat-Led Pentest Framework



**Jorge Orchilles**   
@jorgeorchilles

CTO @scythe\_io  #C2Matrix | Author of #SEC564 #PenTest #RedTeam  
#PurpleTeam Frameworks | Certified @SANS Instructor | #CVSS #EPSS WG | @ISSA & NSI Fellow



**C2 Matrix | #C2Matrix**  
@c2\_matrix

Matrix of Command and Control (C2) Frameworks #C2Matrix How-To:  
howto.thec2matrix.com @jorgeorchilles @brysonbort @Adam\_Mashinchi

📍 The Matrix 🌐 thec2matrix.com 📅 Joined September 2019



# What is Command and Control (C2)?

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques

<https://attack.mitre.org/tactics/TA0011/>

C2

## Command and Control

The adversary is trying to communicate with compromised systems to control them.

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

ID: TA0011

Created: 17 October 2018

Last Modified: 19 July 2019

[Version](#) [Permalink](#)

No Communication = No Control

# What is a Command and Control (C2) Framework?



```
[Empire] Post-Exploitation Framework
=====
[Version] 3.3.2 BC-Security Fork | [Web] https://github.com/BC-SECURITY/Empire
=====
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
=====
```

**Target**



**C2 Server**


```
302 modules currently loaded
1 listeners currently active
457 agents currently active
```

```
(Empire) > █
```

9:44 PM  
11/15/2020



# C2 Matrix idea

- **July 2019** - SANS SEC564 is almost complete with Empire as the main C2 used during labs because it is **reliable and consistent**
- **July 31, 2019** - this happens 
- **August 2019** - "What C2 are y'all using?"
  - 8 different answers
- **September 2019** - Jorge, Bryson, Adam discuss C2 Matrix idea
- **September - November** - Evaluation of C2s
- **November 2019** - C2 Matrix is launched



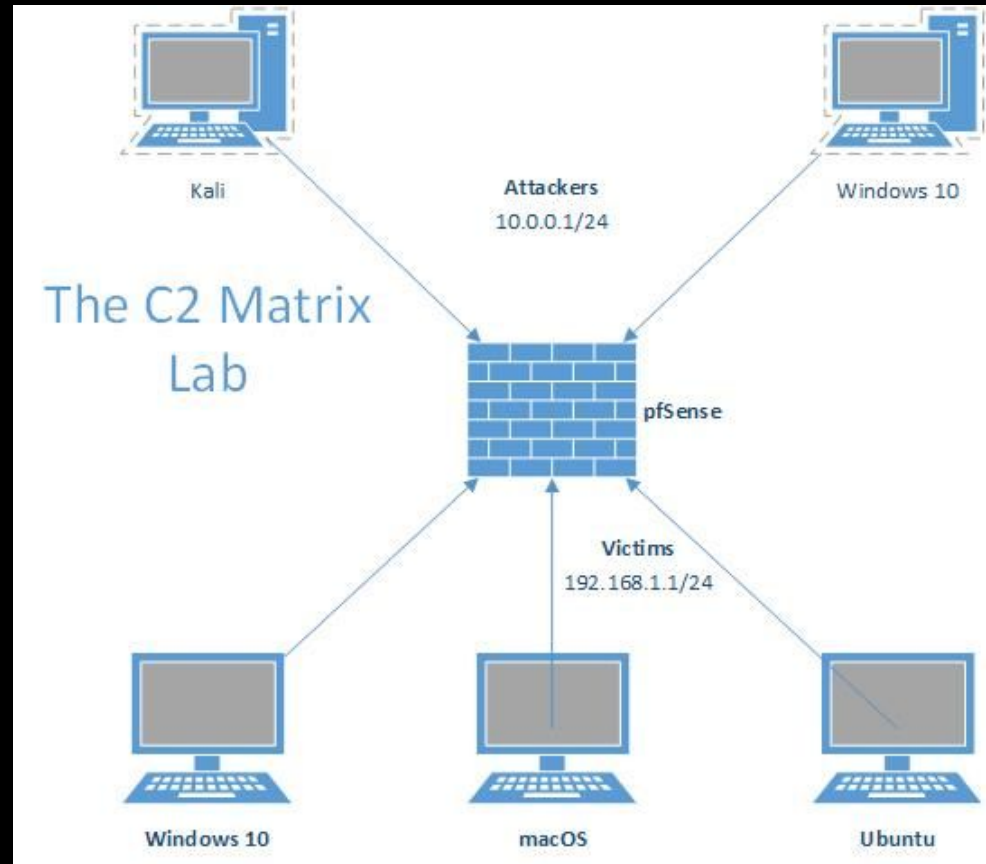
# Original Goals

- Choose the best modern, replacement for Empire
- One that is reliable, consistent, user-friendly and that meets these requirements:
  - Operationally secure
  - Multiple C2 channels
  - Multiple agents/payloads
  - Custom profiles
  - Domain fronting capable
  - Proxy aware
  - Internal pivoting
  - Multi-user
  - Community involvement



# Evaluation Lab

- pfSense with 3 interfaces:
  - WAN - for Internet access
  - Attackers - LAN Segment
  - Victims - LAN Segment
- Windows Victim
  - Wireshark
  - Sysmon
- Linux Victim
  - tcpdump
- macOS
  - Wireshark



<https://howto.thec2matrix.com/lab-infrastructure/c2-matrix-eval-lab>



# What features matter?

- Coding Language
  - Server
  - Implants
- User Interface
  - Multi-User
  - Interface
    - Web
    - GUI
    - CLI
  - Dark Mode
  - API
- Implant
  - Windows
  - Linux
  - macOS
- Communication Channels
  - TCP
  - HTTP
    - Proxy Aware
    - Custom Profile
    - Domain Fronting
  - HTTP2
  - HTTP3
  - DNS
  - DoH
  - ICMP
  - FTP
  - IMAP
- Capabilities
- Support

# Google Sheets

	C2 Info					C2 Matrix Info							La
Name	License	Price	GitHub	Site	Twitter	Evaluator	Date	Version	Implementation	How-To	Slingshot	Kali	Server
Ares	NA	NA	<a href="https://github.com/sweetsoftware/Ares">https://github.com/sweetsoftware/Ares</a>			<a href="#">Contribute</a>							Python
AsyncRAT-C#	MIT	NA	<a href="https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp">https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp</a>			<a href="#">Contribute</a>							
BabyShark	NA	NA	<a href="https://github.com/UnkL4b/BabyShark">https://github.com/UnkL4b/BabyShark</a>			<a href="#">Contribute</a>		Beta 1.0	pip3				
C3	BSD3	NA	<a href="https://github.com/https://labs.f-secure.com/tools">https://github.com/https://labs.f-secure.com/tools</a>	@FSecureLabs		<a href="#">Contribute</a>		1.0.0					
CALDERA	Apache 2	NA	<a href="https://github.com/mitre/caldera">https://github.com/mitre/caldera</a>			@jorgeorchilles	10/6/2019	2	pip3	Yes			Python
Callidus	GNU GPL3	NA	<a href="https://github.com/3xpl01tc0d3r/Callidus">https://github.com/3xpl01tc0d3r/Callidus</a>		@chiragsavla94	@chiragsavla94	5/8/2020			Yes			.Net Core
CHAOS	BSD3	NA	<a href="https://github.com/tiagorlampert/CHAOS">https://github.com/tiagorlampert/CHAOS</a>		@tiagorlampert	@leekirkpatrick4	5/14/2020	3	Go		No		Go
Cobalt Strike	Commercial	\$3,500	<a href="https://www.cobaltstrike.com/">https://www.cobaltstrike.com/</a>			@TimMedin	11/20/2019	3.14	binary				Java
Covenant	GNU GPL3	NA	<a href="https://github.com/https://cobbr.io/tags#covenant">https://github.com/https://cobbr.io/tags#covenant</a>	@cobbr_io		@jorgeorchilles	10/6/2019	0.3	Docker	Yes	Yes	Yes	C#
Dali	MIT	NA	<a href="https://github.com/https://h0mbre.github.io/Image">https://github.com/https://h0mbre.github.io/Image</a>	@h0mbre_		@jorgeorchilles	12/24/2019	POC	pip3				Python
DeimosC2	MIT	NA	<a href="https://github.com/DeimosC2/DeimosC2">https://github.com/DeimosC2/DeimosC2</a>		@CharlesDardar	@jasc22	9/17/2020	1.1.0 Beta	Golang				Golang
Eggshell	GNU GPL2	NA	<a href="https://github.com/neoneggplant/EggShell">https://github.com/neoneggplant/EggShell</a>			<a href="#">Contribute</a>							
Empire	BSD3	NA	<a href="https://github.com/BC-SECURITY/Empire">https://github.com/BC-SECURITY/Empire</a>		@BCSecurity1	@jorgeorchilles	1/30/2020	3.0.5	install.sh	Yes	Yes	Yes	Python
EvilOSX	GNU GPL3	NA	<a href="https://github.com/Marten4n6/EvilOSX">https://github.com/Marten4n6/EvilOSX</a>			@cabbagesalad2	11/12/2019	7.2.1	pip3			Yes	Python
Faction C2	BSD3	NA	<a href="https://github.com/https://www.factionc2.com/">https://github.com/https://www.factionc2.com/</a>			@jorgeorchilles	10/30/2019	NA	install.sh	Yes	Yes	Yes	.NET
FlyingAFalseFlag	GNU GPL3	NA	<a href="https://github.com/monoxgas/FlyingAFalseFlag">https://github.com/monoxgas/FlyingAFalseFlag</a>			@jorgeorchilles	11/12/2019	POC	pip3				Python
FudgeC2	GNU GPL3	NA	<a href="https://github.com/Ziconius/FudgeC2">https://github.com/Ziconius/FudgeC2</a>		@Ziconius	@jorgeorchilles	2/11/2020	Beta	pip3			Yes	Python
godoh	GNU GPL3	NA	<a href="https://github.com/sensepost/goDoH">https://github.com/sensepost/goDoH</a>		@leonjza	@cabbagesalad2	10/31/2019	1.6	binary			Yes	Go
GRAT2	NA	NA	<a href="https://github.com/r3nh4t/GRAT2">https://github.com/r3nh4t/GRAT2</a>			<a href="#">Contribute</a>	9/22/2020	Beta	C#				
HARS	MIT	NA	<a href="https://github.com/onSec-fr/Http-Asynchronous-Reverse-Shell">https://github.com/onSec-fr/Http-Asynchronous-Reverse-Shell</a>			@leekirkpatrick4	3/24/2020	POC	python				Python
HTTP-RevShell	GNU GPL3	NA	<a href="https://github.com/3v4Si0N/HTTP-revshell">https://github.com/3v4Si0N/HTTP-revshell</a>		@3v4Si0N	<a href="#">Contribute</a>							

# thec2matrix.com

← → ↻ thec2matrix.com

[ABOUT](#)[ASK](#)[DOCUMENTATION](#)[FEEDBACK](#)[GUI](#)[MATRIX](#)

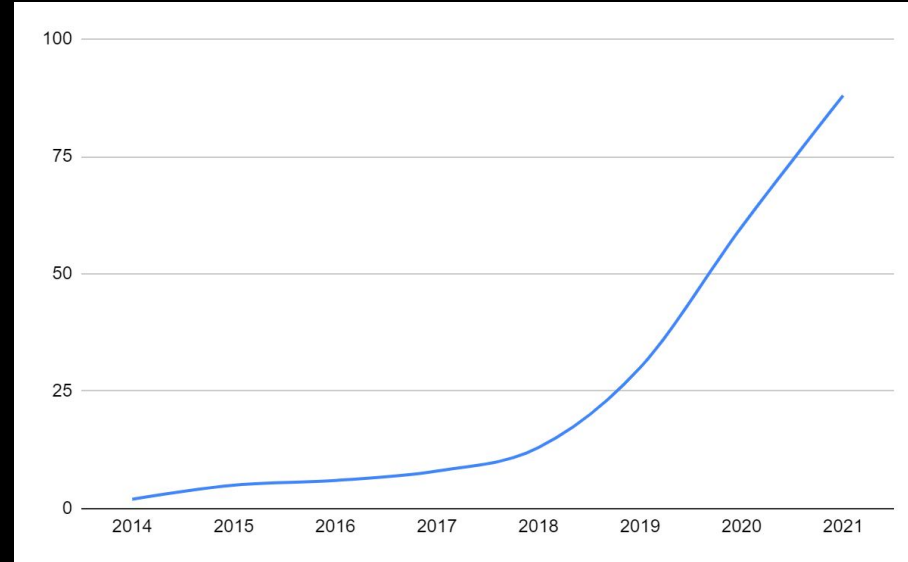
Find out which C2 fits your needs

ASK THE MATRIX



# So what has changed?

- More C2s
  - November 2019 → 30
  - November 2020 → 60
  - November 2021 → 88
- Those are not *all* the C2s
- C2 != C2 Framework
- Writing a C2 != Maintaining a C2
- OST Debate - still going





# Sponsorware



**Marcello**

@byt3bl33d3r

📢 Ok peeps, have an announcement: all future tools and updates I release will be Sponsorware. Only people who have sponsored me on Github at a specific tier will get access to them initially. Finally, they will be made publicly available only after I reach a target n of sponsors

10:06 PM · Jun 23, 2020 · Twitter for iPhone

51 Retweets 15 Quote Tweets 248 Likes

You Retweeted



**BC Security**

@BCSecurity1

We reached our first sponsorship goal and, as such, have added popout windows to Starkiller. It's available right now in the 1.5.0-RC1 build!

#redteam #infosec #cybersecurity



**Release v1.5.0-RC1 - BC-SECURITY/Starkiller**

Added popout windows for agents. Now you can work on and get live updates from multiple agents at one time.

[github.com](#)

3:14 PM · Nov 10, 2020 · Twitter Web App

# Commercial C2s (12.5% of C2s)

- Brute Ratel - Dark Vortex (single dev)
- Cobalt Strike - bought by HelpSystems
- Haven - Pivot Labs (consulting company)
- Innuendo - Immunity bought by AppGate
- Nighthawk - MDSec (consulting company)
- OST Stage 1 - Outflank (consultant company)
- Oyabun - Red Code Labs
- Prelude - ex-Caldera devs
- Red Team Toolkit - bought by NetSPI (consulting company)
- SCYTHE - spun out from GRIMM (consulting company)
- Voodoo - S2 Security (consulting company)



@ElementalX2



# Specialization

- InfoSec
  - Security Architecture, AppSec, NetSec. SOC, DFIR, CTI, Threat Hunting, Offense
- Offense
  - Vulnerability Assessment, Penetration Testing, Bug Bounty, Vuln Research, Red Teaming
- Red Teaming
  - Developer, operator, attack infrastructure maintainers, tradecraft research
  - Operator != Developer

## The Future of Adversaries is Software Development



Tim MalcomVetter Jul 6, 2019 · 7 min read



# Training: Developing C2 and Implants



## Malware development for advanced adversary emulation

Dates: November, 8-12, 2021

Hours: 1400-1900 UTC | 1500-2000 CET

Duration: 5h x 5 days

Price: 4599 PLN + VAT (for non-company purchases)

Audience Level: All

[https://ekoparty.org/en\\_US/eko17/trainings/ekomalware-crash-course](https://ekoparty.org/en_US/eko17/trainings/ekomalware-crash-course)

<https://twitter.com/pucara/status/1454145971395379204>

<https://www.x33fcon.com/#!/t/malware-nov.md>

# Training: Developing C2 and Implants



<https://wildwesthackinfest.com/antisyphon/enterprise-attacker-emulation-and-c2-implant-development-w-joff-thyer/>

# Training: Developing C2 and Implants



## C2 Development in C#

This training course is aimed at offensive practitioners interested in developing and maintaining their own command and control framework.

Students will begin by creating a RESTful API-driven Team Server, written in ASP.NET Core. They will then write an implant which targets the .NET Framework and implement a variety of post-exploitation capabilities including basic filesystem enumeration, shell and run commands, in-memory .NET execution, token manipulation, and more. Finally, students will write unit and API tests to automate testing and prevent regression bugs.

Students are provided access to approximately 6 hours of pre-recorded step-by-step video tutorials, as well as a full copy of the final Visual Studio solution.



<https://www.zeropointsecurity.co.uk/c2-dev-csharp/overview>

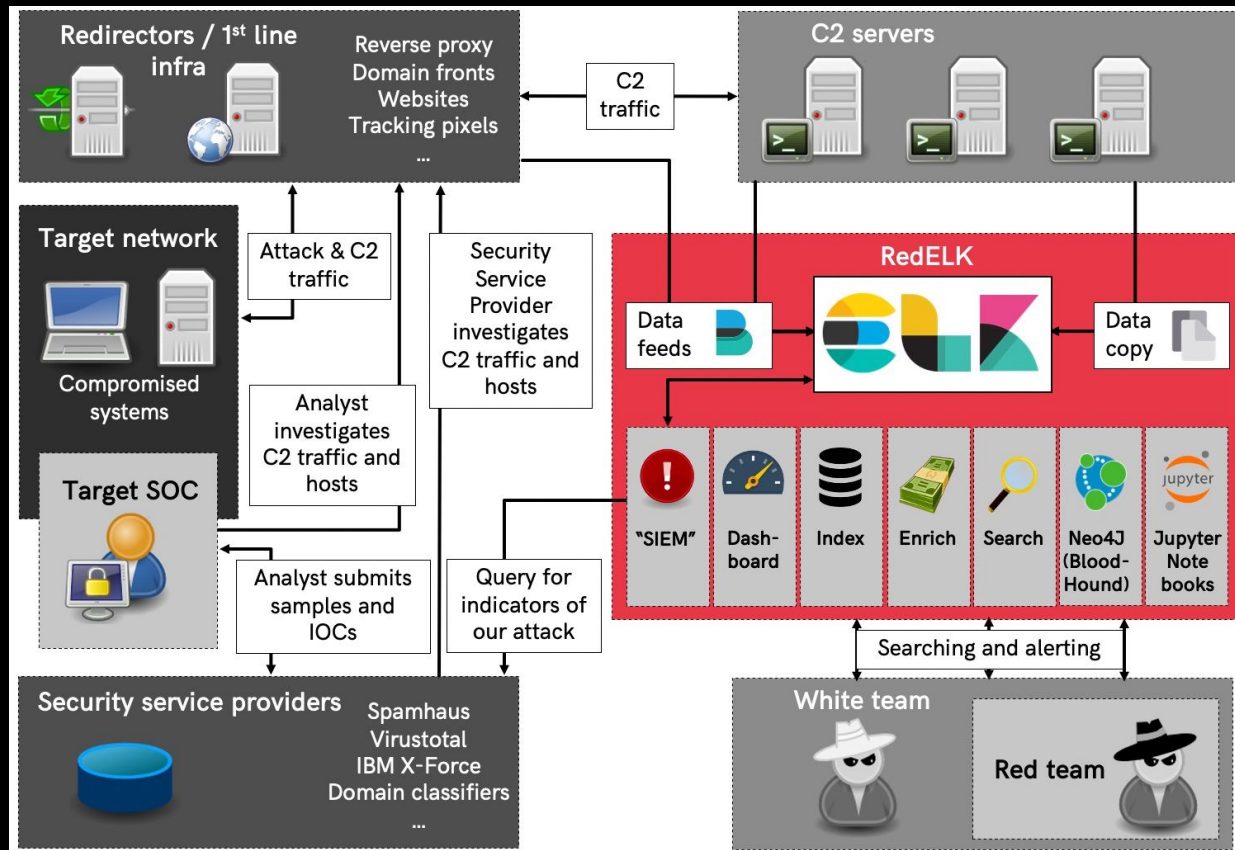
# Attack Infra

- Amazing graph for this talk ->>
- Thanks Marc/Outflank:

- @MarcOverIP
- @OutflankNL



<https://github.com/outflanknl/RedELK/>

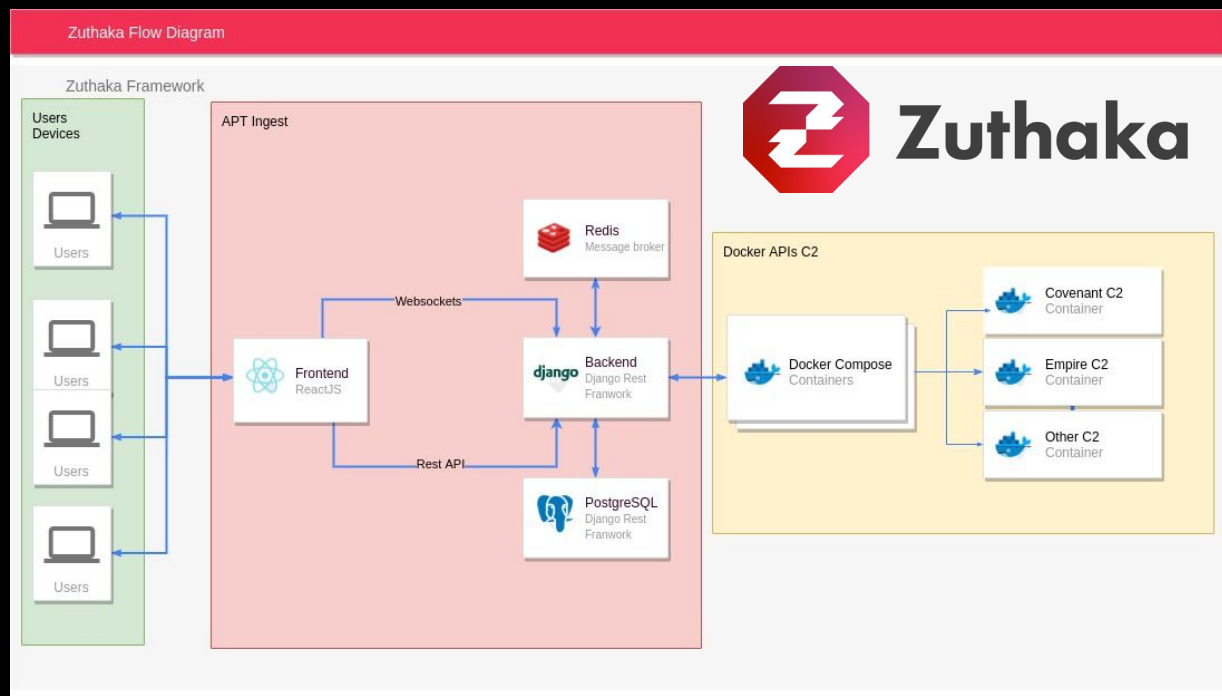


# Attack Infra - Best Practices

- C2 not exposed (use redirectors)
  - "It's 2021, don't expose C2 server ports directly to the internet" - @HackingLZ
- Domain Fronting is Dead... Long live domain fronting
  - Providers don't like it and may ban your account
- Serverless Functions
  - Azure
  - AWS Lambda
  - CloudFlare Workers
- <https://howto.thec2matrix.com/attack-infrastructure/redirectors>

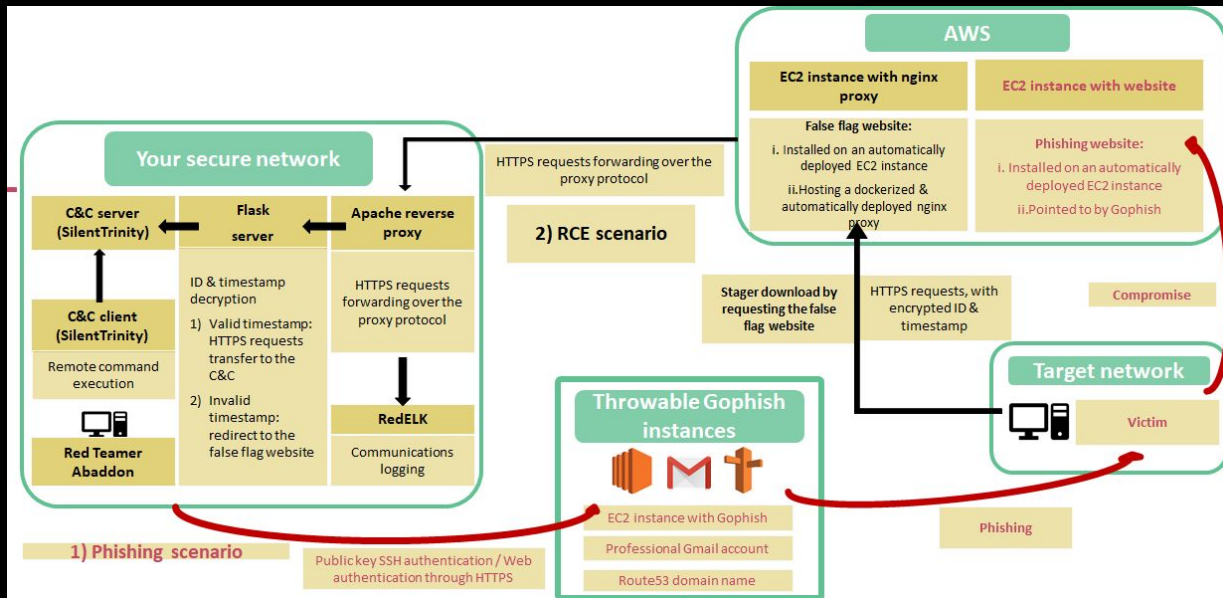


# Attack Infra - Framework for C2s




<https://github.com/pucarasec/zuthaka>

# Attack Infra - Automation



<https://github.com/wavestone-cdt/abaddon>

# Attack Infra - Automation



Features Docs Gear Community

## Attack Infrastructure

that's cloud-native and open source

[Get Started](#)

↓

### Installation | Usage

```
## Requirements:
# An AWS account with full admin privileges
# and terraform v0.13 or greater

git clone https://github.com/havocsh/havoc-deploy.git
cd havoc-deploy
touch terraform.tfvars
echo 'aws_region = "<your-preferred-region>"' >> terraform.tfvars
echo 'aws_profile = "<your-aws-profile>"' >> terraform.tfvars
echo 'campaign_name = "my-campaign"' >> terraform.tfvars
echo 'enable_domain_name = false' >> terraform.tfvars
echo 'campaign_admin_email = "<your-email>"' >> terraform.tfvars
terraform init
terraform plan
terraform apply
```

<https://havoc.sh/>

# Roadmap

- Continue to evaluate all the C2s
- MITRE ATT&CK Mapping
- Lowering the curve for new professionals
- If malicious actors can access these tools, you should be testing them too
  - Attack. Detect. Respond.

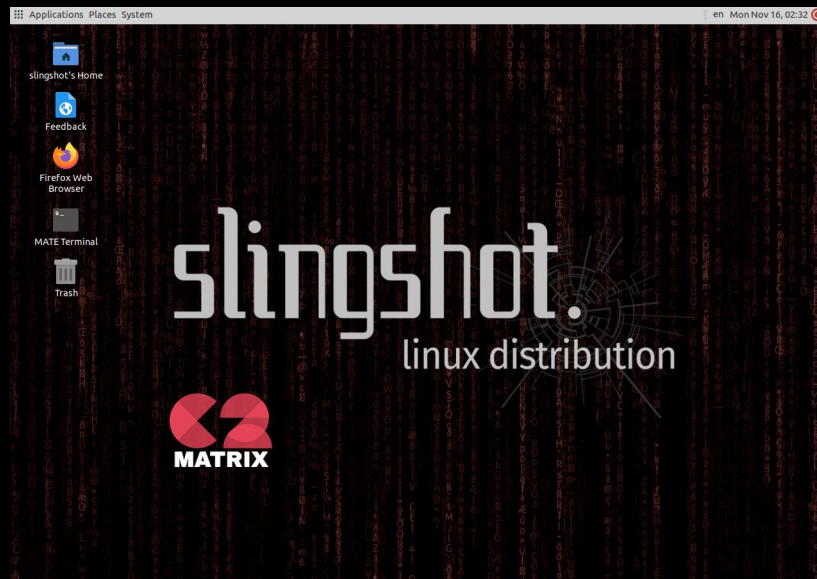
# SANS Slingshot C2 Matrix Edition

## NEW RELEASE

<https://howto.thec2matrix.com/slingshot-c2-matrix-edition>

# SANS Slingshot C2 Matrix Edition

- Goal is to lower the learning curve of installing each C2 framework
- Gets you straight to testing C2s
- Covenant, Empire, Koadic, Merlin, Metasploit, Mythic, Posh, Shad0w, Silent Trinity, and Sliver
- <https://howto.thec2matrix.com/slinsshot-c2-matrix-edition>

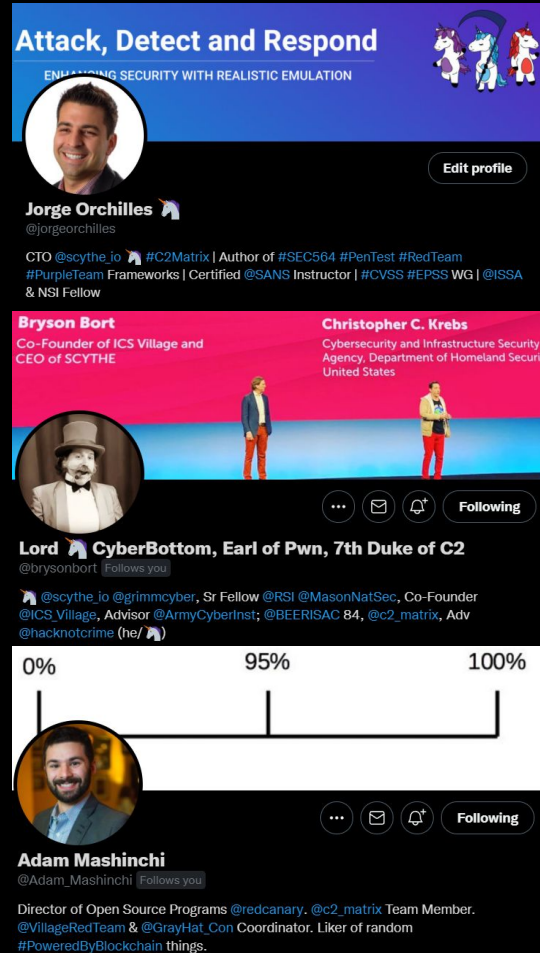


@NonVictus



# Get involved! (Contribute)

- Just ping us:
  - @C2\_Matrix @JorgeOrchilles @BrysonBort @Adam\_Mashinchi
  - <https://www.thec2matrix.com/feedback>
- When a new C2 is released or updated
- Share a blog
- Update request for any field on #C2Matrix
- An evaluation of a new or updated C2
- Feedback on SANS Slingshot C2 Matrix Edition



THANK YOU