LOWC2

Living Of the Web Command & Control

Mathieu Saulnier

Sr Manager at Sophos
Co-Organizer of SkiCon
Montreal on-site lead DEATHcon
20+ years in security

Sad Start

Even Before


EXIT
Living Off the Land: A Minimalist's Guide to Windows Post-Exploitation
Command & Control: Example
Easy, inexpensive and strong!
Features:
Value:
Design:
Quality:
Ease of use:
Living Off the Land: A Minimalist's Guide
to Windows Post-Exploitation
Christopher Campbell, Matthew Graeber
ALL IN THE FAMILY
DERBYCON
LOUISVILLE, KENTUCKY ★ 2013

Inoffensive site

GitHub

Some Nerdy (Bad) Influence

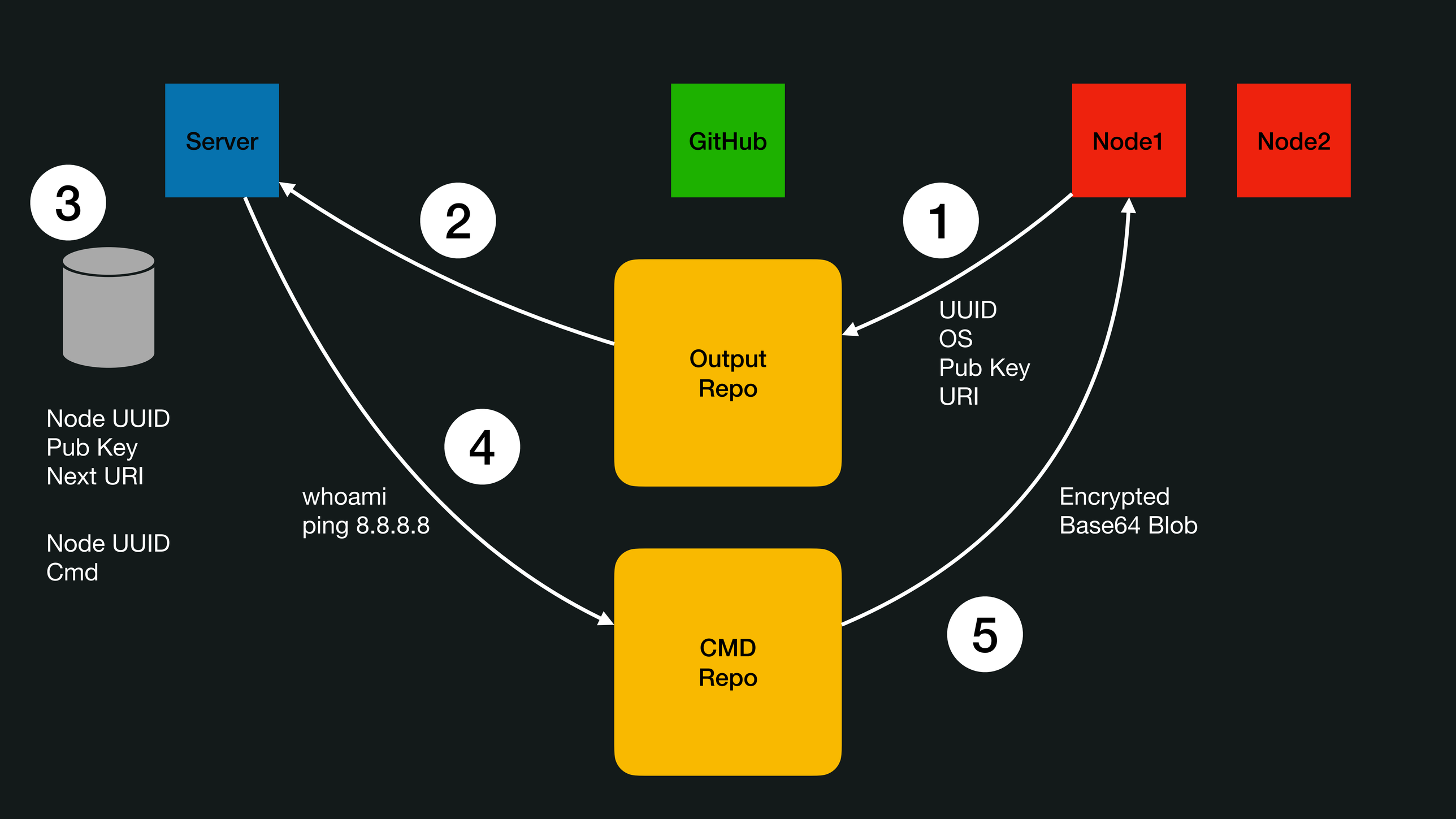
BHIS WebCast

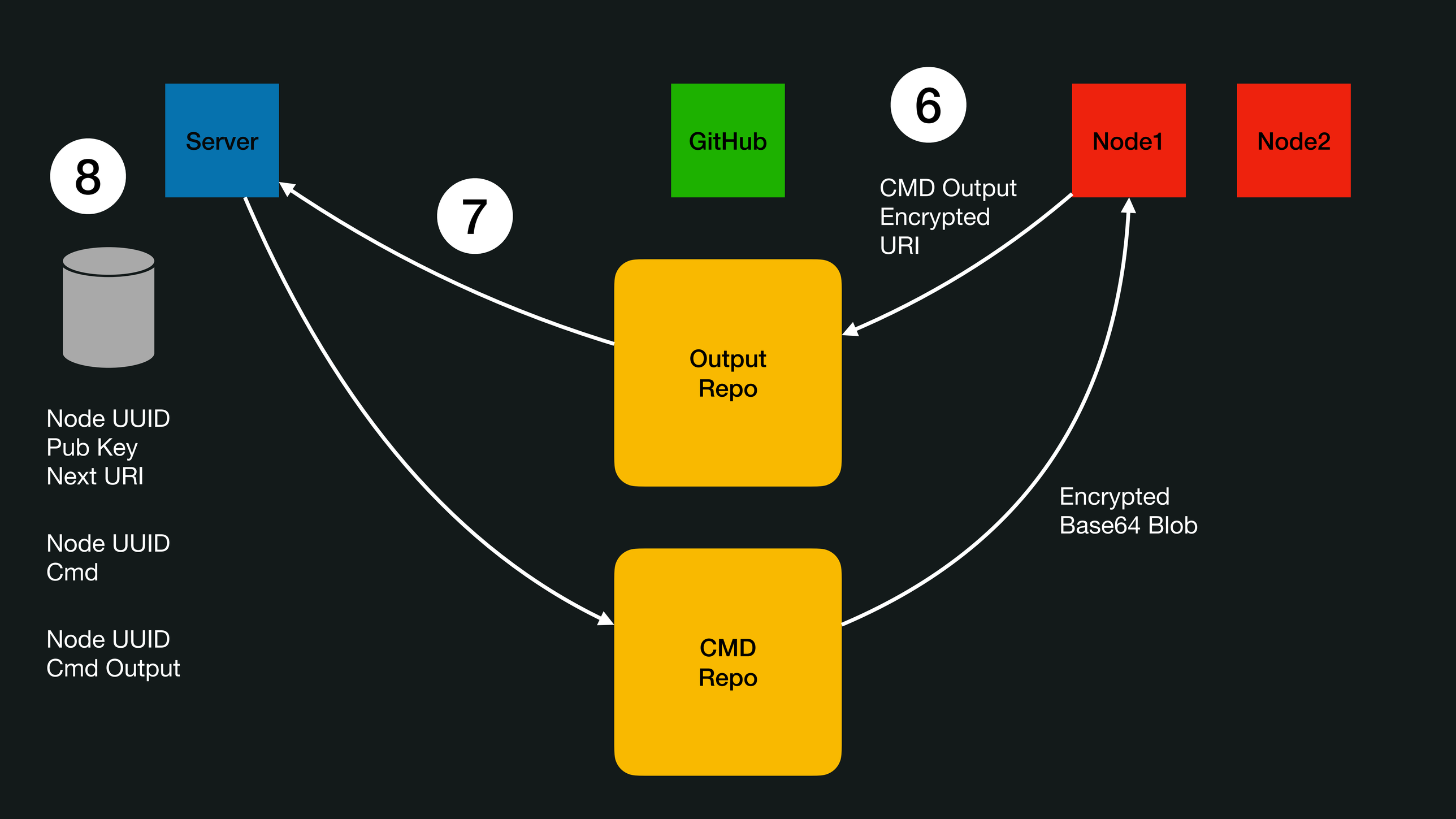
Learning Rust

Ressources

Rasta Mouse’s
LinkedIn Learning

Guiding Principles Architecture


Server
GitHub
Node1
Node2
3
2
1
Output
Repo
UUID
OS
Pub Key
URI
Node UUID
Pub Key
Next URI
Node UUID
Cmd
4
whoami
ping 8.8.8.8
Encrypted
Base64 Blob
CMD
Repo
5


Server
GitHub
Node1
Node2
6
CMD Output
Encrypted
URI
7
8
Output
Repo
CMD
Repo
Encrypted
Base64 Blob
Node UUID
Pub Key
Next URI
Node UUID
Cmd
Node UUID
Cmd Output

Started Coding

Manipulating Repo in Rust

You would think

There’s a comprehensive library

Running cmd on Nodes

Probably the easiest part

Encrypting Exchanges

Choosing Cypher

Public Keys

Able to store in a file

Storing Encrypted Files

Surviving Server Crash

- Storing
  - Node UUID
  - Keys
  - Next cmd Filename

Loading Array

OpSec Considerations

GitHub

Access Tokens

Private Repos

Anti IR Strategies

Use random filename for cmd

Use Branches for Output

Cross Compilation

Rust Takes Care of it

Created gist for the gotchas

Preventing Nodes to Crash

Sounds Easy

Rust prefers to crash than overflow

Tips For Defenders

Simili Beacon

GitHub.com/scoubi/SimiliBeacon

lots-project.com

Living Off Trusted Sites

GitHub -> Phishing & D/L

John Hammond

Hackers Use GitHub For Malware

youtu.be/0wduZ3nO848&t=873

@SoubiMtl

linkedin.com/in/mathieusaulnier