Living Off the WAN
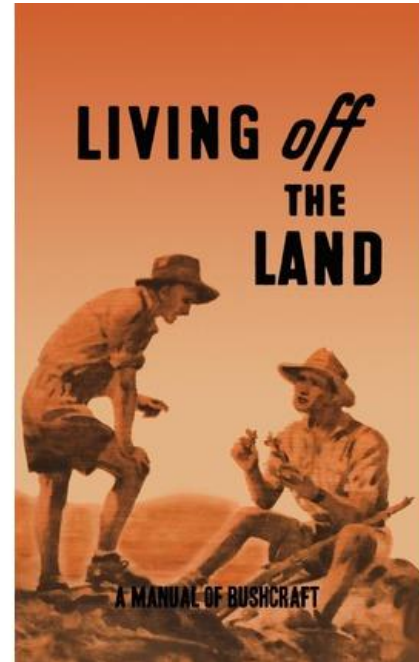
Seattle Bsides, 2019

Agenda

- Living Off the Land
- Objective
- C2 infrastructure
- Slack as a C2
- Pushed to innovate
- Issues Arise
- Solution found?
- Demo

Living Off The Land

What is this talk? Objective

- Introduce people to Command and Control (C2) infrastructure
- Advantages of public web apps
- Spark curiosity

Scenario
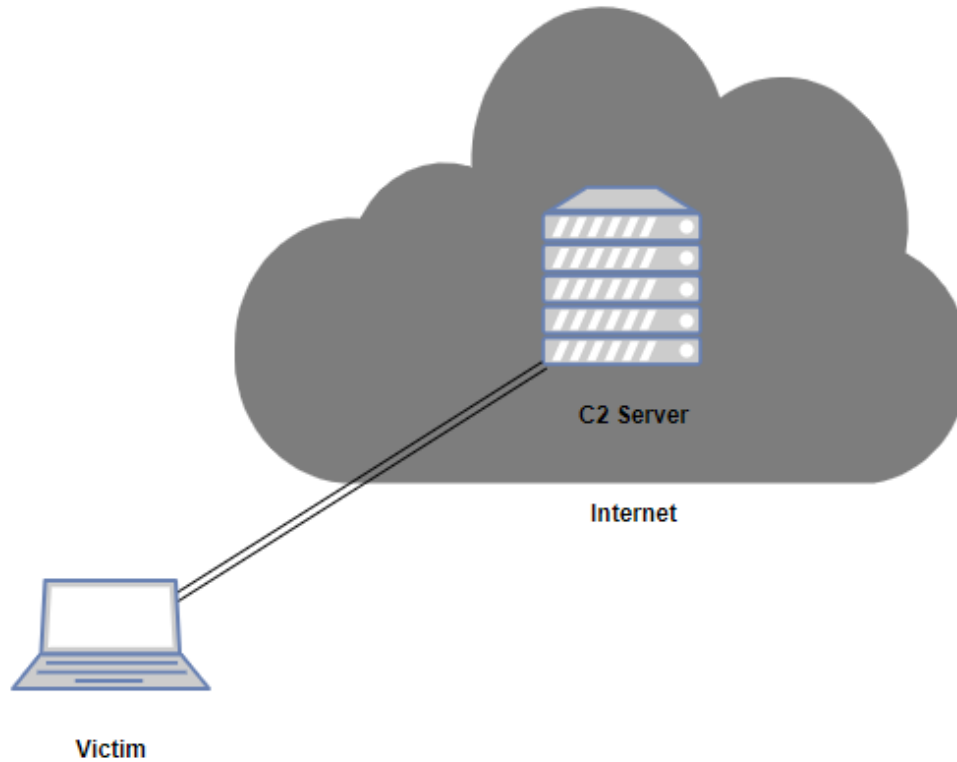
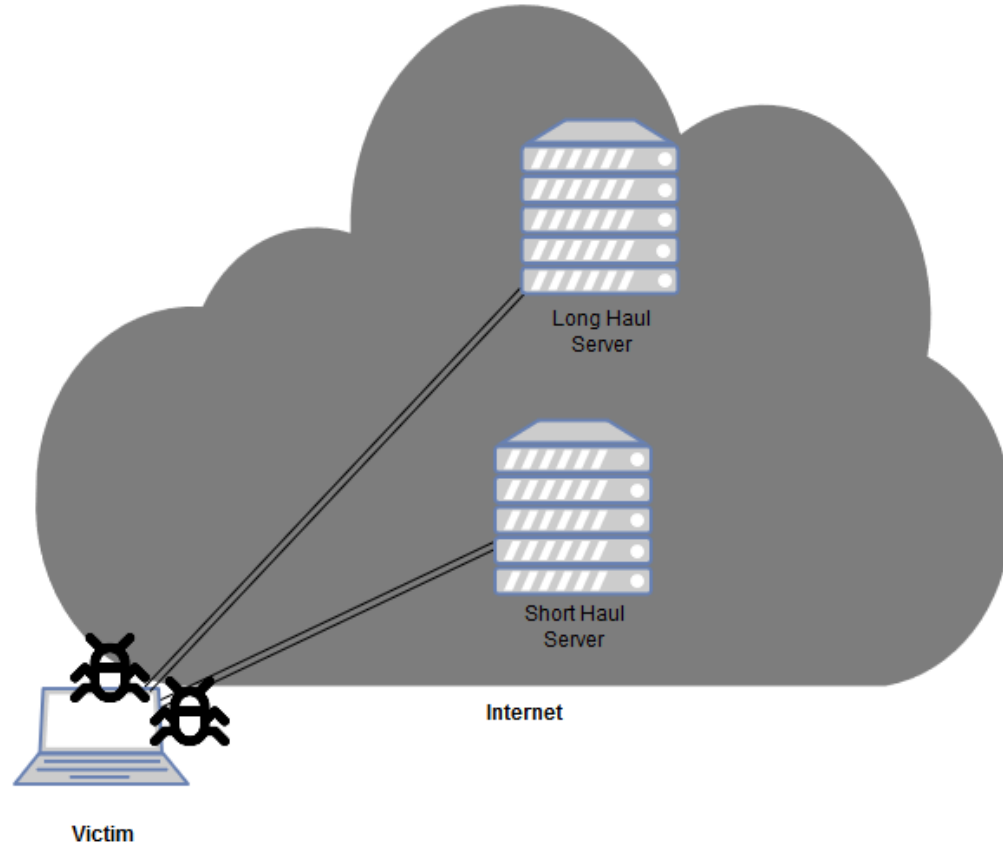Red Teaming Engagement

Post exploitation phase

Budget = $0.00

$0.00

C2 Basics

C2 Architecture

C2 Server

Internet

Victim

More Advanced

C2 selection based on environment

Slack as a C2

SlackShell

Slack as a C2 but with powershell

https://github.com/bkup/SlackShell
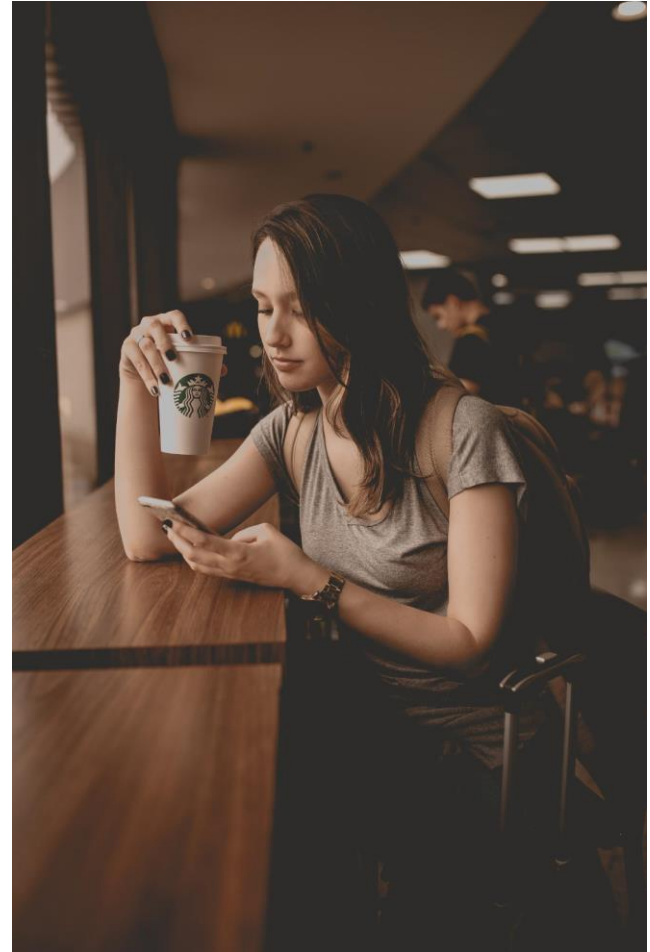
Slack RTM API

Real Time Messaging API as the conduit
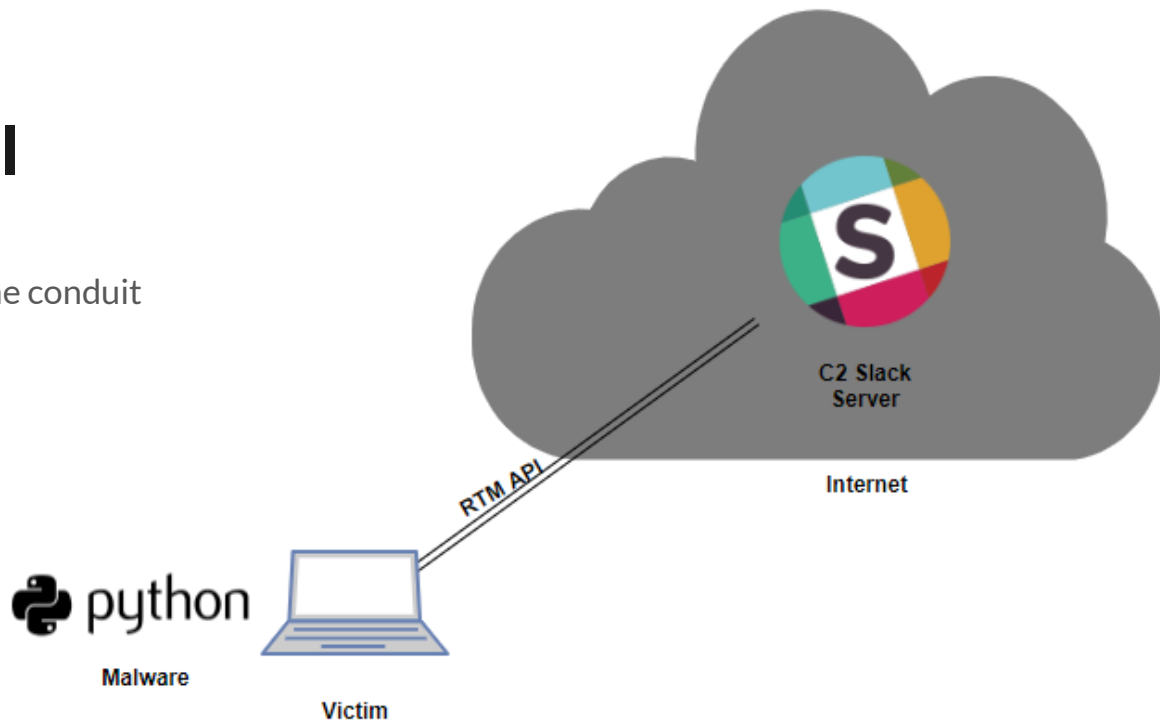
DEMO TIME!

Slack Benefits

- Trustworthy slack servers
- TLS connection
- Benefits of using SaaS
- Cross platform experience… Do you know what that means??

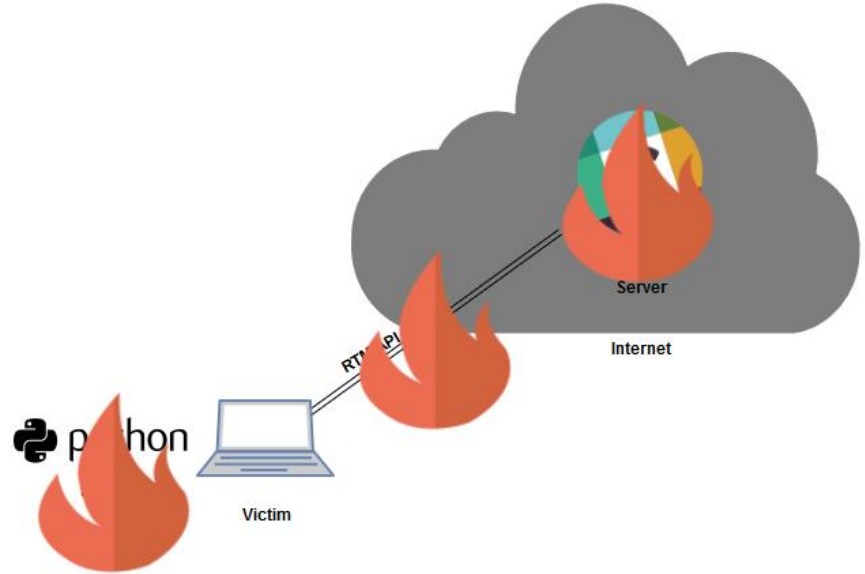# PWN on the go and...

PWN and go...

Challenges to overcome

Scaling

Bot token management

Total of 10 bots per slack workspace

What happens if Slack gets burned?

How would this happen?

Detection via the network

- DNS (microooooosoft.slack.com)
- Windows Server doesn't run slack...

Host based detection

Policy can make detection more difficult

So we want better C2 infrastructure… How?

If slack gets burned we're toast (burned toast)

Diversify so not just slack as the short haul server

Central location for our long haul server to tie in. Either client side program or some central server…
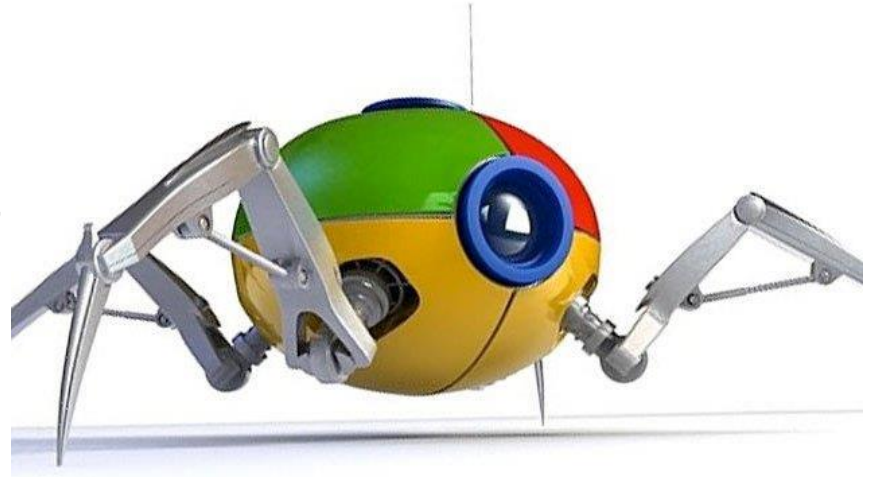
One night in bed...

Google Search

How do we get the data there?

- Google crawls websites
- But how often?
- Can we get it to automatically crawl it?
- Yes?

"Crawling can take anywhere from a few days to a few weeks."

BING to the rescue...

"allows you to submit upto 10,000 URLs per day for immediate crawl"

Hot Damn!

Intelligent approach though

A Novel Search Engine-Based Method for Discovering Command and Control Server

December 16, 2015….

https://link.springer.com/chapter/10.1007/978-3-319-27137-8_24

ONE WEEK LATER...

Reading a bit more: "The Submit URLs
feature in Webmaster Tools is currently
restricted to **root domains** only and will not
accept the submission of subdomains."

AHHHHH!!!!!

SNOWPOCALYPSE
2017 9

GitHub Pages + free domains

bsidesseattle **.tk**	• FREE	USD 0.00	Get it now!
bsidesseattle **.ml**	• FREE	USD 0.00	Get it now!
bsidesseattle **.ga**	• FREE	USD 0.00	Get it now!
bsidesseattle **.cf**	• FREE	USD 0.00	Get it now!
bsidesseattle **.gq**	• FREE	USD 0.00	Get it now!

SEO for my C2

Got Bing to allow me to enter the domain in for automatic indexing.

But……

"The URLs are immediately evaluated for search indexation and **when quality criteria are met**, they will begin to surface in Bing search."

Other ways of getting information in Search

NVM Google come back I love you

What does google crawl the most?

Alexa 100 will probably give us a good hint
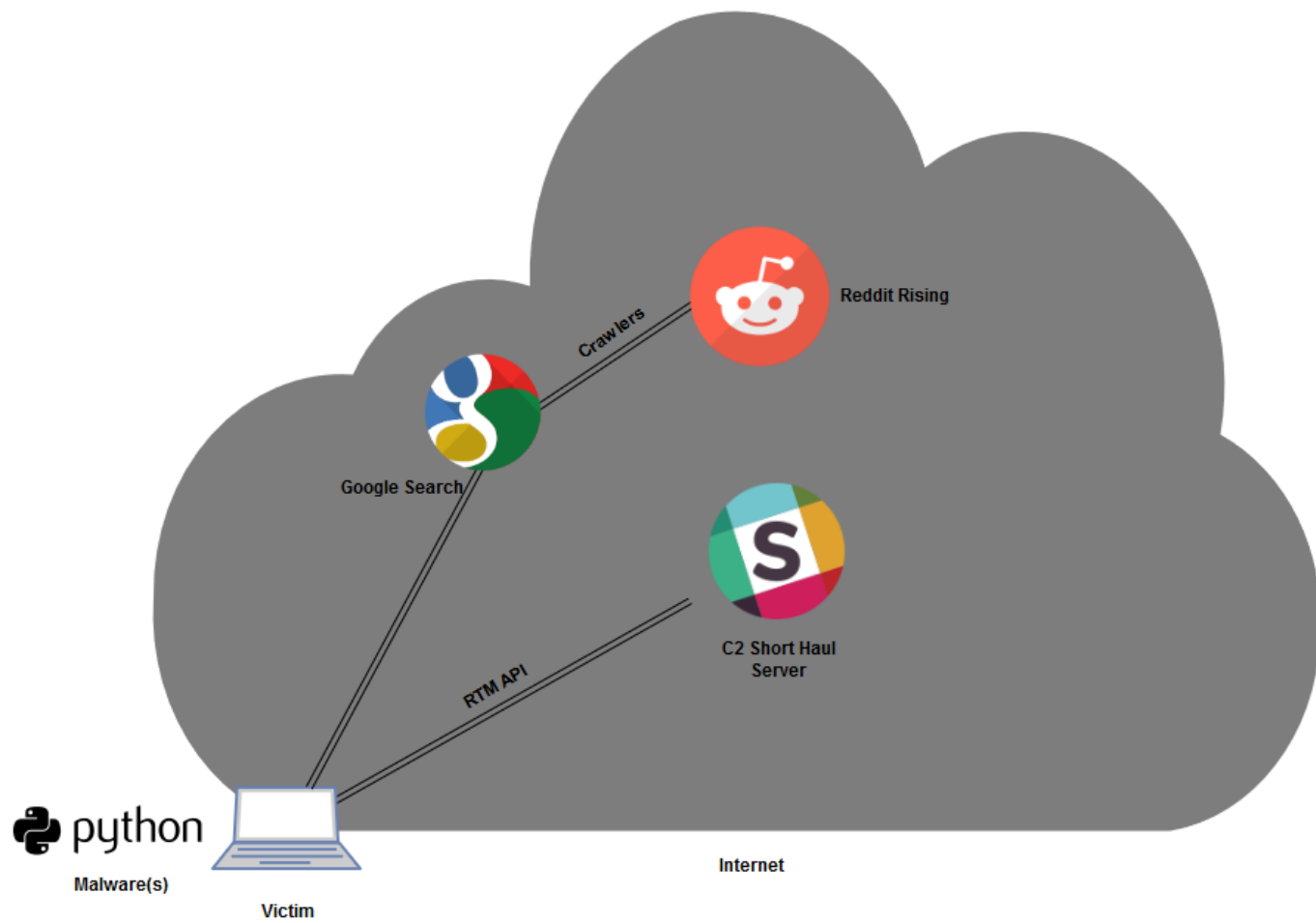
1   Google.com
Enables users to search the world's information, including
webpages, images, and videos. Offers...More

2   Youtube.com
YouTube is a way to get your videos to the people who matter to
you. Upload, tag and share your...More

3   Facebook.com
A social utility that connects people, to keep up with friends, upload
photos, share links and ...More

4   Amazon.com
Amazon.com seeks to be Earth's most customer-centric company,
where customers can find and disc...More

5   Wikipedia.org
A free encyclopedia built collaboratively using wiki software.
(Creative Commons Attribution-Sh...More

6   Reddit.com
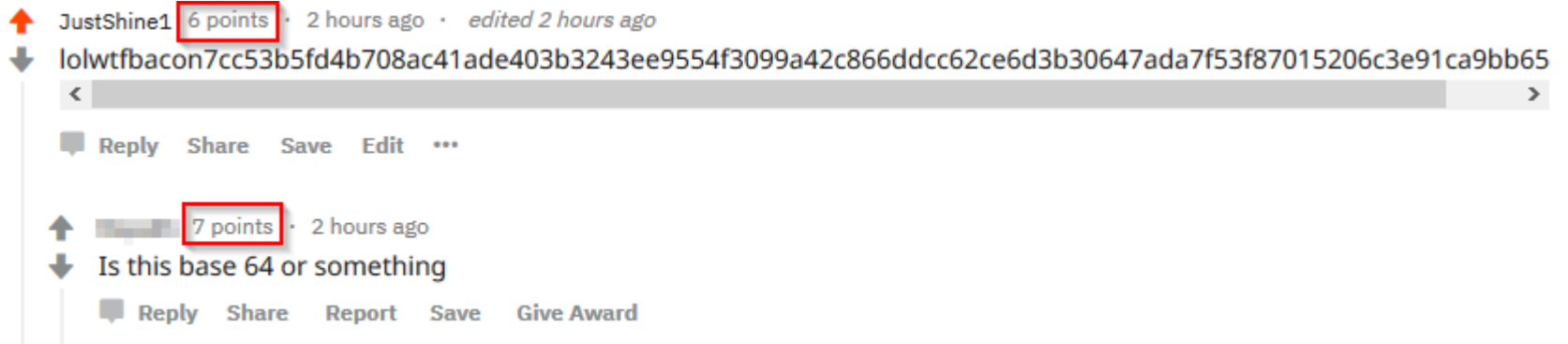User-generated news links. Votes promote stories to the front page.

33

Reddit Rising

What areas does google crawl the most?

Least noticeable by users?

Reddit Rising

Crawlers

Google Search

C2 Short Haul
Server

RTM API

Malware(s)

Victim

Internet
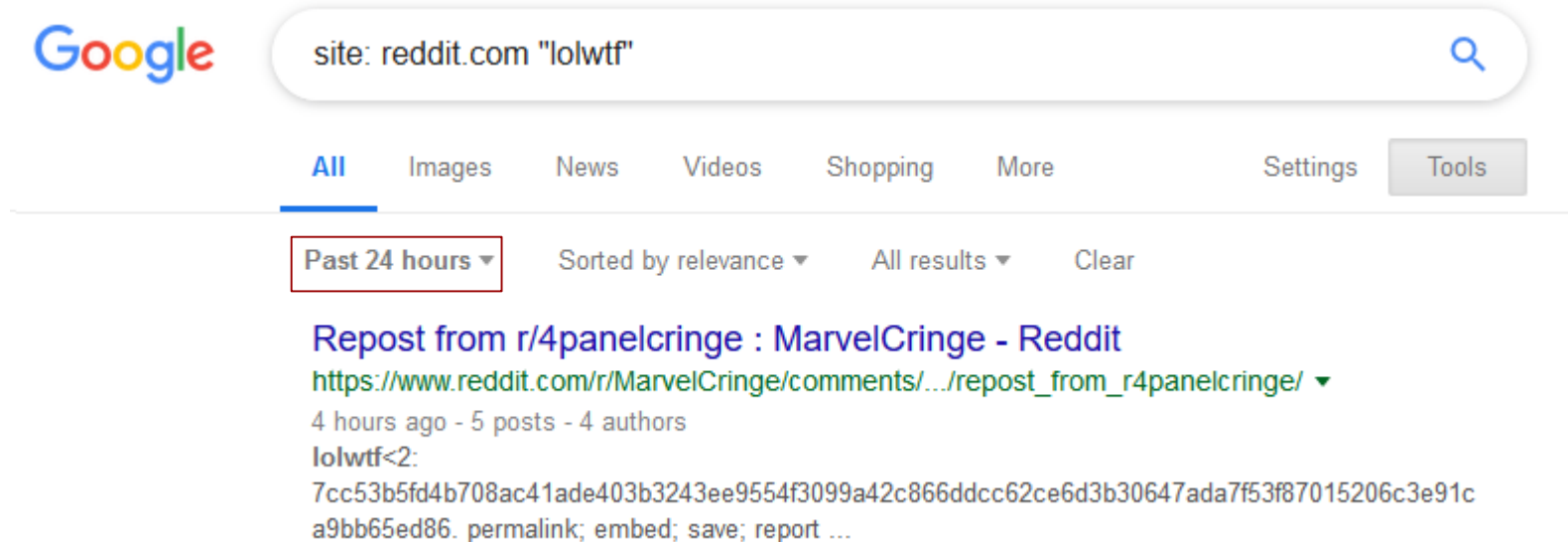
35

Sometimes they're nice

JustShine1 `6 points` · 2 hours ago · *edited 2 hours ago*

lolwtfbacon7cc53b5fd4b708ac41ade403b3243ee9554f3099a42c866ddcc62ce6d3b30647ada7f53f87015206c3e91ca9bb65

Reply Share Save Edit •••

`7 points` · 2 hours ago

Is this base 64 or something

Reply Share Report Save Give Award

Sometimes people just don't get it

JustShine1 · -5 points · 12 hours ago

hahalol<3:7cc53b5fd4b708ac41ade403b3243ee9554f3099a42c866ddcc62ce6d3b30647ada7f53f87015206c3e91ca9bb65e

Reply   Share   Save   Edit   ...

It actually worked!

Google

site: reddit.com "lolwtf"

All   Images   News   Videos   Shopping   More   Settings   Tools

Past 24 hours ▾   Sorted by relevance ▾   All results ▾   Clear

Repost from r/4panelcringe : MarvelCringe - Reddit
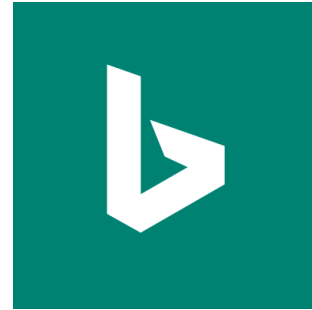https://www.reddit.com/r/MarvelCringe/comments/.../repost_from_r4panelcringe/ ▾
4 hours ago - 5 posts - 4 authors
lolwtf<2:
7cc53b5fd4b708ac41ade403b3243ee9554f3099a42c866ddcc62ce6d3b30647ada7f53f87015206c3e91c
a9bb65ed86. permalink; embed; save; report ...

Let's take a moment... and see why this is possible...
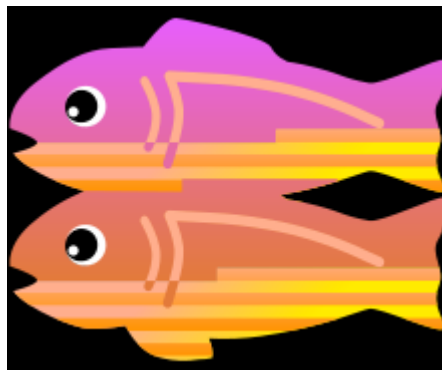
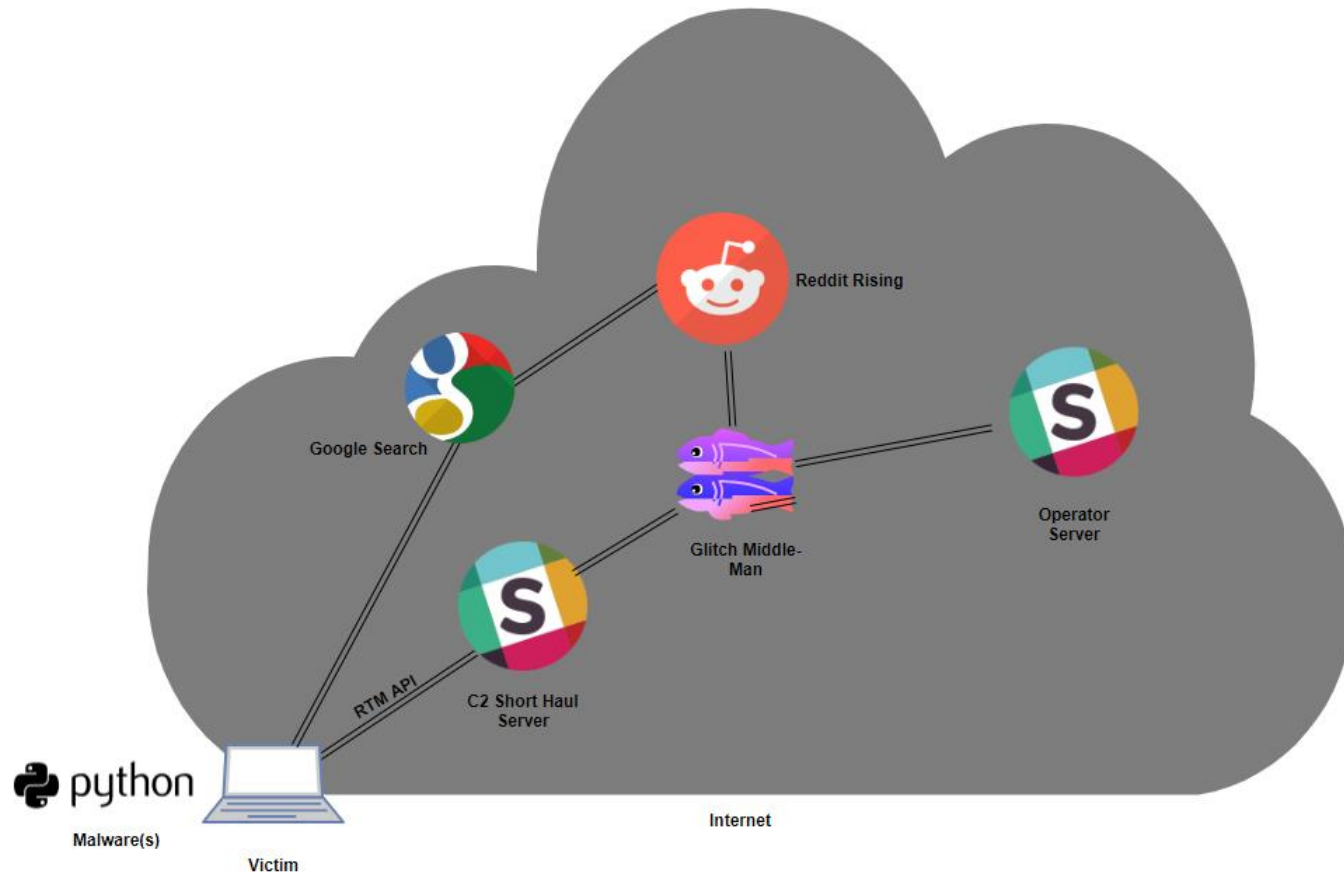# When you're living off the WAN sometimes...

Glitch.com

- Free serverless platform without login
- Lock functionality (Makes it private)
- Gives you a subdomain at **weird-name.glitch.me**
- CLI access to your own container (Not as root)

Now we have a docker container

- Don't have to use nodejs
- Engage in programmatic behaviour

Google Search

Reddit Rising

Glitch Middle-Man

Operator Server

RTM API

C2 Short Haul Server

python

Malware(s)

Victim

Internet

43

Sooo... That actually didn't work

Slack Events API and Web Hooks

Web hooks receive the data to slack channel

Events API send data

We can now create a bi-directional channel

Summary

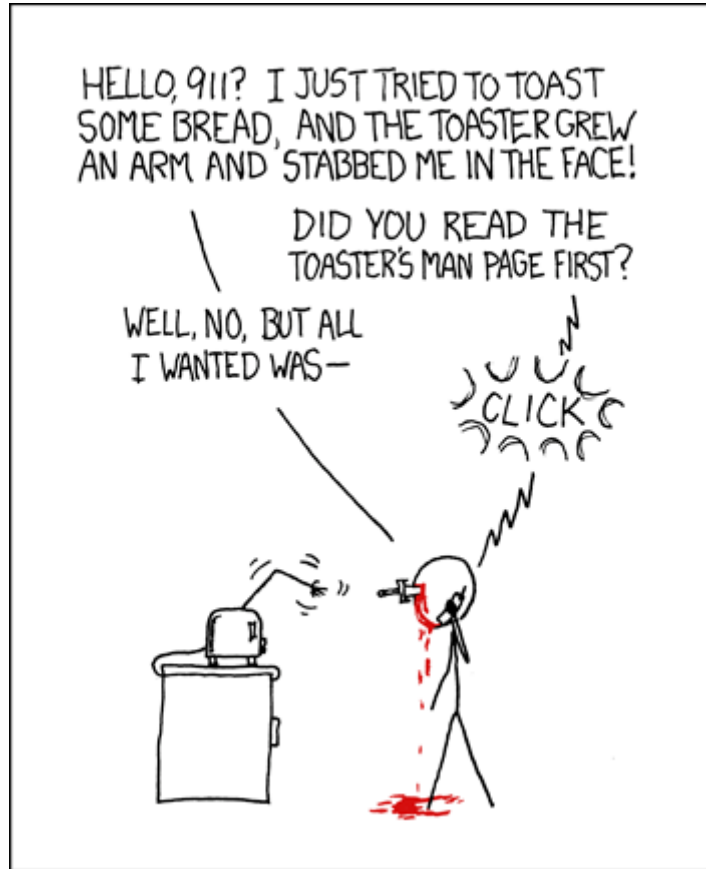We can create advanced C2 infrastructure for free

We can masquerade as legitimate sites to evade detection

Curious what other more advanced C2 infrastructure can be emulated?

What did I learn

TBH… RTFM, all of it! Closely!

Services shift

Additional resources

https://bluescreenofjeff.com/

https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki

Questions?