

Don't RAT Me OUT!



Lilly Chalupowski
October 29, 2018

whois lilly.chalupowski

Table: *who.is results*

Name	Lilly Chalupowski
Status	Employed
Creation Date	1986/11/29
Expiry	A Long Time from Now
Registrant Name	GoSecure
Administrative contact	Travis Barlow
Job	Security Application Developer - Threat Intelligence

Agenda

What will we cover?

- Disclaimer
- What is a RAT?
- Brief History of the RAT
- Why build a RAT?
- The Laboratory RAT
 - CnC Server
 - Victim Sessions
 - Command Queue
 - NCurses
- Evasion
 - NIDS/NIPS
 - Debugging
 - Virtual Machines
- POC / Demo / Questions

Disclaimer

Don't be a Criminal

disclaimer.log

The tools and techniques covered in this presentation can be dangerous and are being shown for educational purposes.

It is a violation of Federal laws to attempt gaining unauthorized access to information, assets or systems belonging to others, or to exceed authorization on systems for which you have not been granted.

Only use these tools with/on systems you own or have written permission from the owner. I (the speaker) do not assume any responsibility and shall not be held liable for any illegal use of these tools.

What is a RAT?



What is a RAT?

The Animal



Figure: Army RAT!

What is a RAT

The Tool

The screenshot shows the Swamp RAT interface. At the top, it displays 'victims: 1' and the victim's details: 'ae6027fb-343d-4c4f-a41e-05d20f5e90a6 c3rb3ru5@lillypad'. Below this, it shows the system configuration: 'arch:x86_64 release:4.14.65-gentoo hostname:d3d53c load:5 ping:47'. The middle section is a large red box labeled 'Swamp' containing the victim's desktop screen. At the bottom, it shows 'commands: 0' and a command history from 'lillypad':

```
[c3rb3ru5@d3d53c ~]$ cd Tools/swamp-rat/
[c3rb3ru5@d3d53c swamp-rat]$ cd bin/
[c3rb3ru5@d3d53c bin]$ ./stub
[+] connected to 127.0.0.1:4444
[+] 127.0.0.1:4444 OK
```

To the right of the command history, a quote by Elizabeth Bowen is displayed: "Fate creeps like a rat." - Elizabeth Bowen.

On the far right, there is a small window titled 'scrot' showing a screenshot of the victim's desktop.

Figure: Swamp RAT



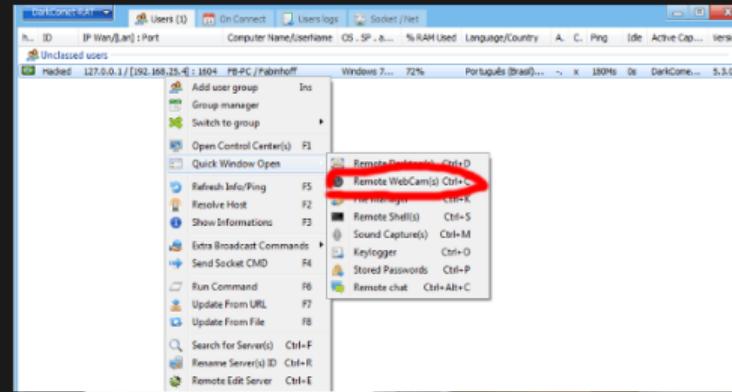
History of the RAT

System Administrators

- Central management
- Supporting larger user base
- Fixing issues remotely
- Solved user issues

History of the RAT

Well that Escalated Quickly



Why Build a RAT?



Figure: Hackers IRL

Why Build a RAT?

Because Linux

- Linux
- C Programming Language
- Learning Experience
- Find Detection Limitations
- Research the Linux Malware Ecosystem
- It's Cool
- Because I Can

The Laboratory RAT



CnC Server

In the C Programming Language

- Sockets
 - Create
 - Bind
 - Listen
 - Accept
 - Receive
 - Process
 - Send
- PThreads

CnC Server

It can be painful when written in C

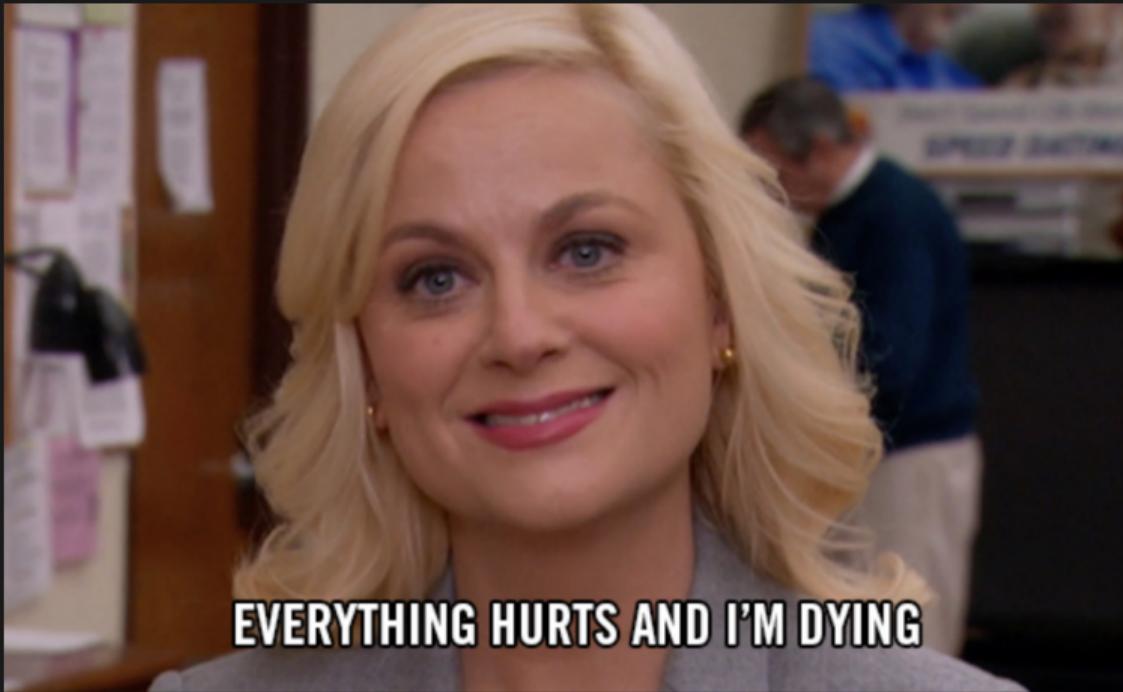


Figure: Leslie Knope