SilkETW & SilkService

blackhat

Because free telemetry is free!

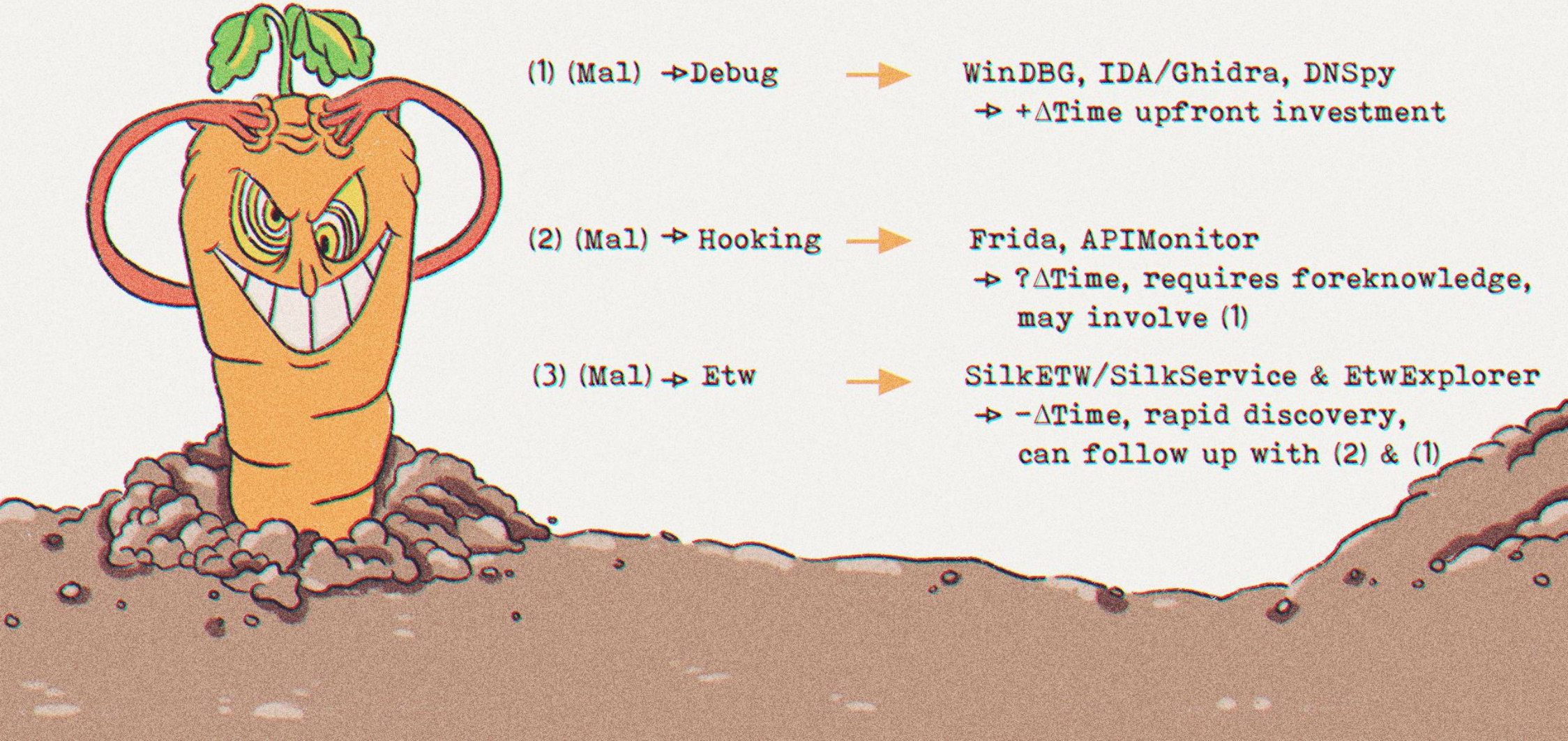
Ruben Boonen (@FuzzySec)
FireEye Advanced Practises

What is it? Where can I get it?

Blog post https://www.fireeye.com/blog/threat-research/2019/03/silketw-because-free-telemetry-is-free.html

GitHub https://github.com/fireeye/SilkETW

Why SilkETW? → Premier research tool



(1) (Mal) →Debug → WinDBG, IDA/Ghidra, DNSpy
→ +ΔTime upfront investment

(2) (Mal) → Hooking → Frida, APIMonitor
→ ?ΔTime, requires foreknowledge, may involve (1)

(3) (Mal) → Etw → SilkETW/SilkService & EtwExplorer
→ -ΔTime, rapid discovery, can follow up with (2) & (1)

Research Example: WNF

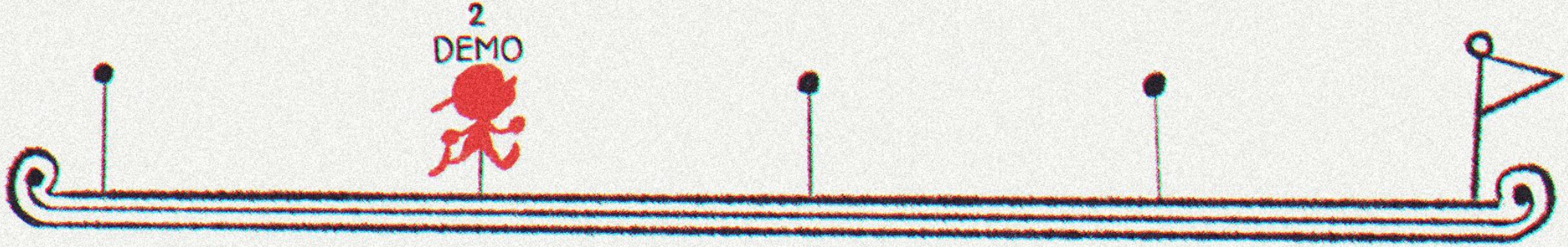
Windows Notification Facility (WNF), is a Kernel level Pub/Sub facility.

- Can be used for stealth IPC and Process injection
- Is a binary using WNF? What is it using WNF for?
- ETW Provider
  - Windows Notification Facility Provider
  - 42695762-ea50-497a-9068-5cbbb35e0b95

Correlating JSON data

We can capture data in bulk and ask it questions

- Simple example
  - DLL load correlation
  - Mimikatz through CobaltStrike
- PowerShell / ELK



Augmenting ETW With Yara

Are you capturing a large volume of data to find specific things?

Can you string match or regex what you are looking for?

Yara has you covered!

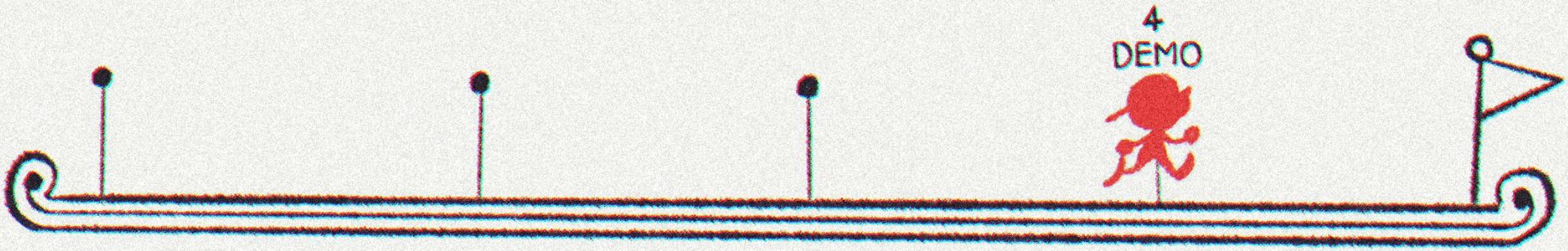
Taming the .NET Dragon

.NET is scary, yes! Current visibility is bad, yes!

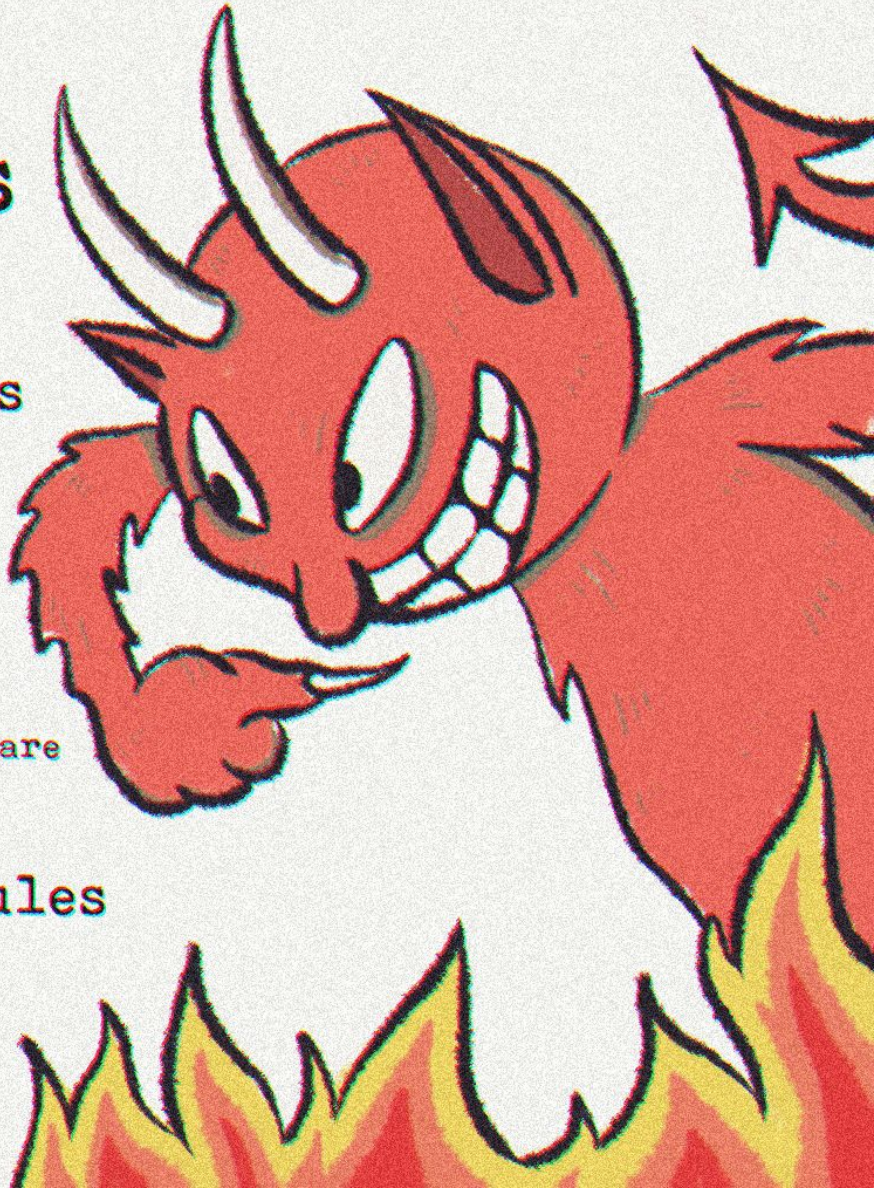
Is the battle lost?

- No!
- With data in hand we can step on attackers!

Seatbelt through CobaltStrike case-study



.NET Detection Considerations



Take care, attackers can rename/obfuscate class and method names

- Most will not do this however = easy win

Try to write regex signatures for things that can not easily be changed

- The .NET IL is a good target for this but it needs a bit of care

Make sure to field-test your yara rules

- Remember the golden yara maxim, always write redundant rules to cover your bases!
  - If you lose a detection you don't lose visibility

SilkETW is a
research / triage
/ detection-engineering tool

- It can't run headless, it can't initiate multiple ETW collectors

What if you want to
automate collection at scale?

- SilkService has you covered!
- Read XML config, has all the capabilities of SilkETW

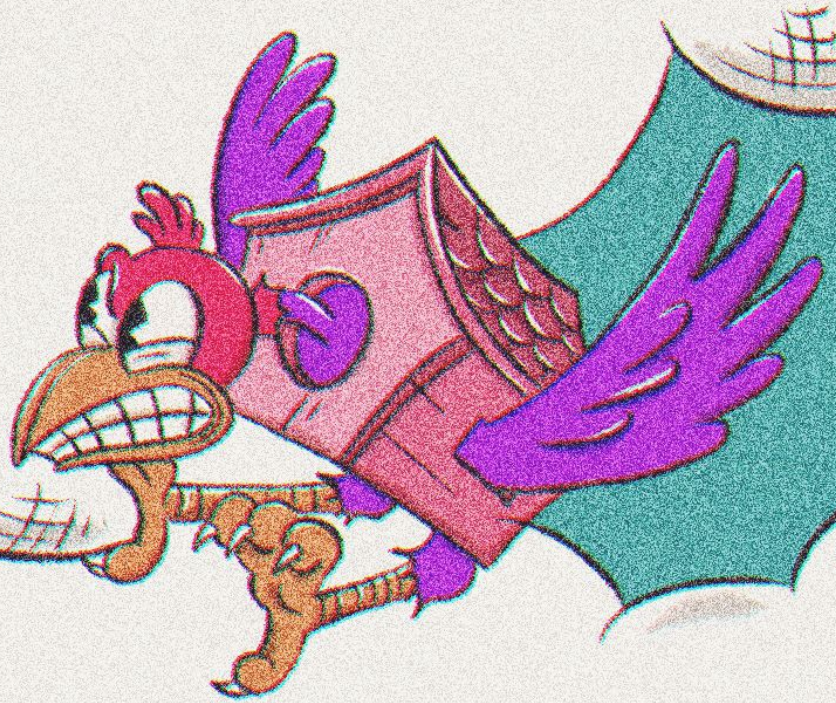
Deploying ETW collection at Scale

Do your testing and research with SilkETW

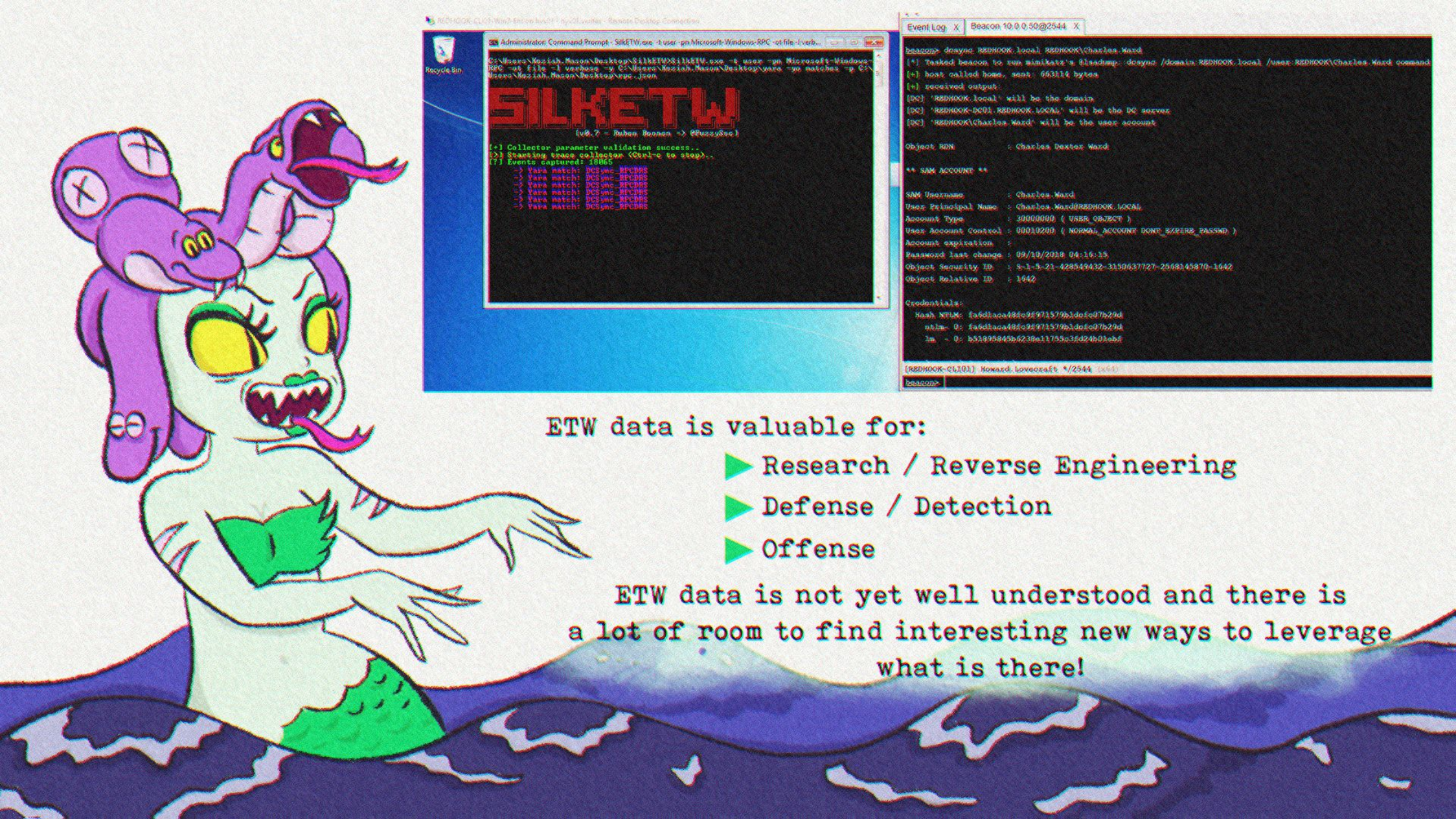
- Promote your research to SilkService

If you want to deploy SilkService broadly remember:

- Do performance testing, CPU utilization scales on collector count
- Remember, this was written by a one-man engineering army :D!



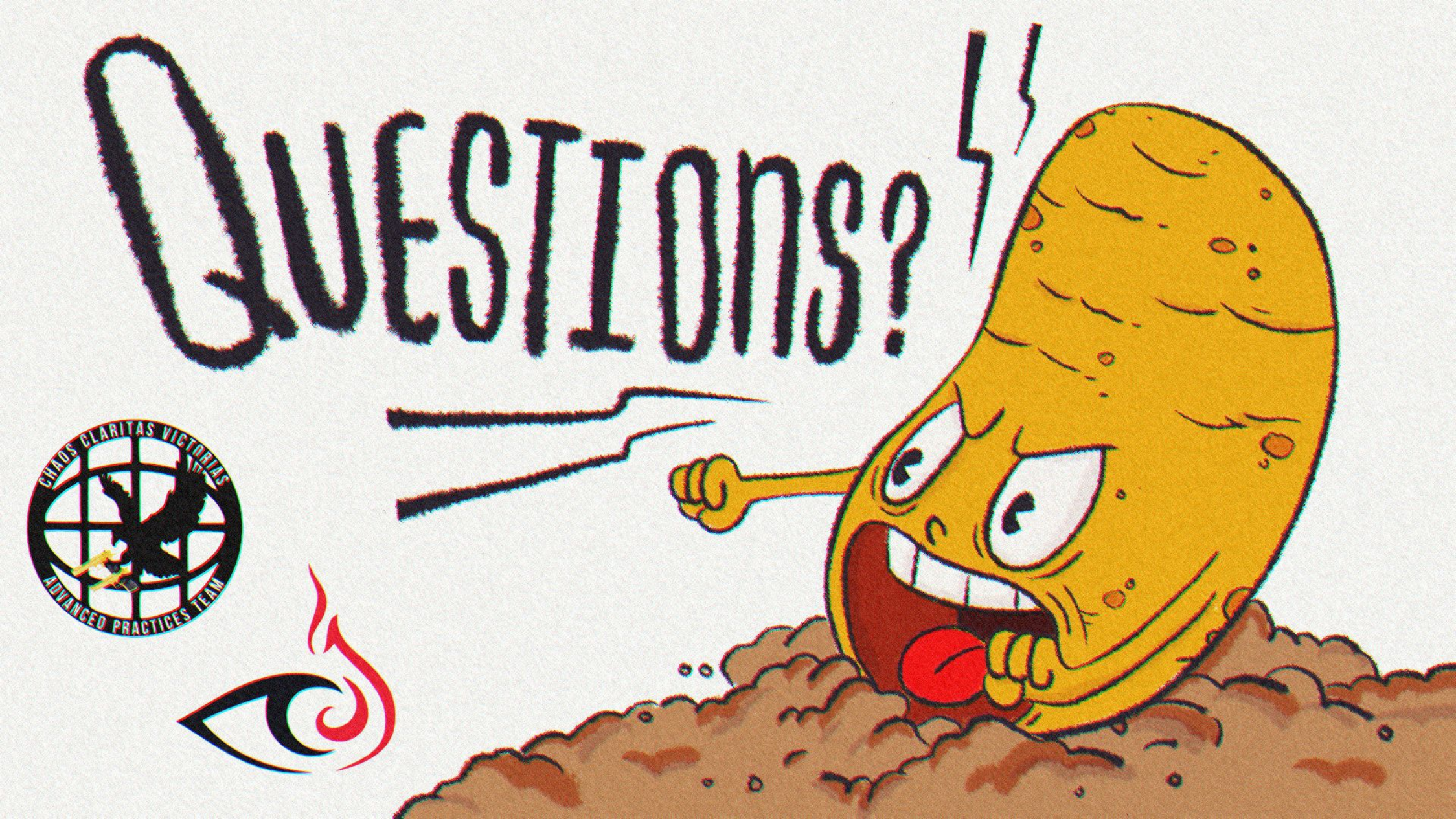
SilkService SOP & Caveat



ETW data is valuable for:

- Research / Reverse Engineering
- Defense / Detection
- Offense

ETW data is not yet well understood and there is a lot of room to find interesting new ways to leverage what is there!


QUESTIONS?
CHAOS CLARITAS VICTORIAS
ADVANCED PRACTICES TEAM