Maintaining Access: Hiding Your Tools

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Shhhh…I'm hiding from stupid people!

A T-Shirt

Rootkits

Root + Kit = Mother-Puss-Bucket

Back in my day…

Why use a rootkit?

Several types of rootkits

Hard to remove

Why Are Rootkits Used?

Remote control

Eavesdropping

Polymorphism

Types of Rootkits

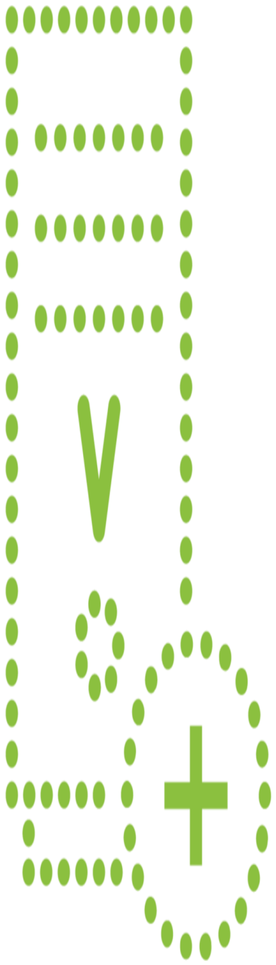
User-mode

Kernel-mode

Hybrid

Firmware

Virtual

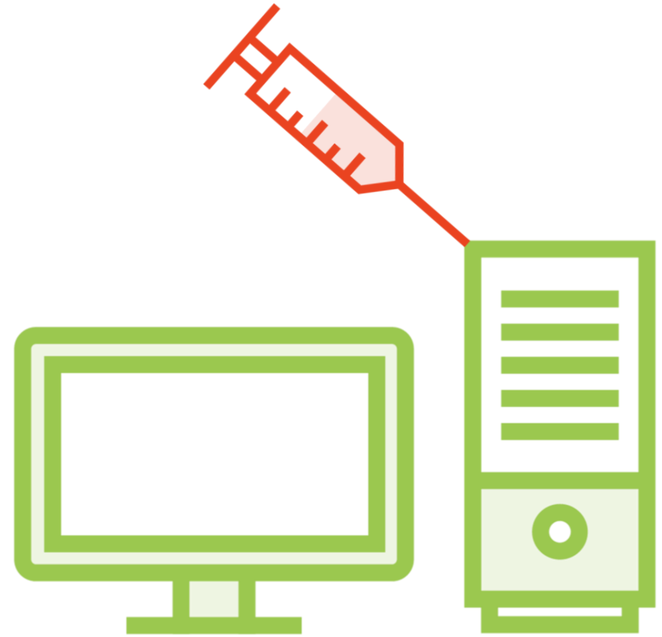


But I've Got Anti-virus

Yeah... I don't care

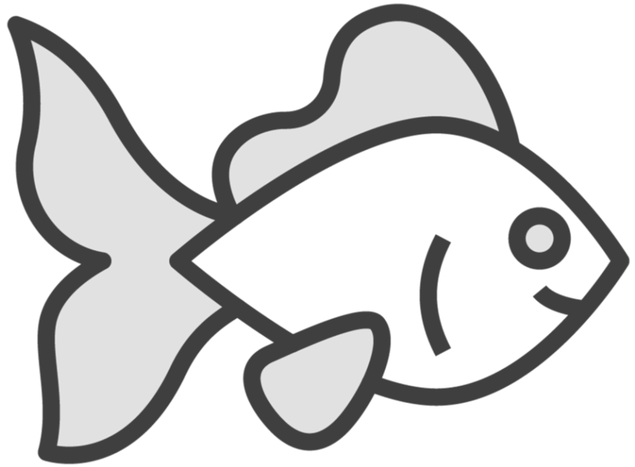
You can try, but...

SuperDale rule #385



Two Interesting Ones

Horse Pill



Gray Fish

Detecting Rootkits

Detecting Rootkits

Integrity-Based

Signature-Based

Runtime Execution Path Profiling

Heuristic/Behavior-Based

Detecting via File System

```
C:> dir /s /b /ah

C:> dir /s /b /a-h


Boot from CD run the same commands


Download WinDiff on both results
```

Alternate Data Streams

DO I HAVE YOUR ATTENTION?!

The Issue

This is NOT a well known feature

Around since NT 3.1 – still used

Data fork + resource fork

Allow you to hide files…very effectively

Demo

Alternate Data Streams

Steganography

Hiding in Plain Sight

Hiding data inside or behind other data

Replaces unused data bits with the hidden file bits

Extremely hard to detect

Two classifications

- Technical
- Linguistic

Steganography Types

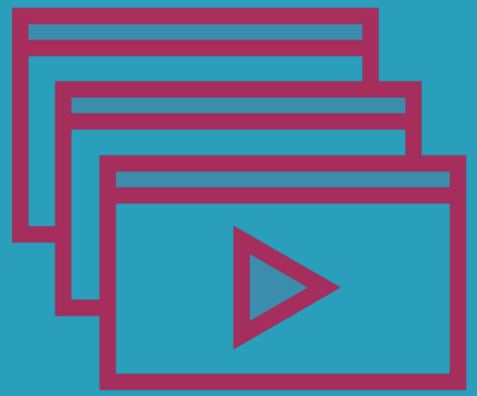
Image based

Document based

Folder based

Audio based

Steganography Types



Video based

Web based

White Space based

Email based

Steganography Types

DVD ROM based

Natural text based

Hidden OS based

Learning Check

Learning Check

- Rootkit
- User-mode
- Firmware
- Grayfish
- Data fork / Resource fork

Learning Check

- Dir /s /b /ah
- WinDiff
- 5MB
- Steganography
- Snow

Key Terms

- **Rootkits and trust**
- **ADS**
- **Steganography**

Next Up:

Phase 5: Clearing Logs – Covering Your Tracks