Daniel Griggs

Daniel Griggs is the CEO and founding partner at cmdSecurity, an IT firm in the DC area specializing in Apple device security and management at scale. Before starting cmdSecurity Dan worked with various government agencies including working on the STIG, the security guidance for the Department of Defense. Dan created and maintains cmdSecurity's Apple device security and management platform as well as continues to advise on multiple security standards.

Managing Security with the Growing Threat of Malware

Daniel Griggs

Founder & CEO of cmdSecurity

https://cmdsec.com

MACTECH PRO EVENTS

cmdSecurity

dan — Hogwarts

```
Last login: Sat Apr 23 14:18:05 on ttys000

dan@Hogwarts: ~
$whoami
```

- Daniel Griggs, CEO and founding partner cmdSecurity
- Worked for the US DoD and other government agencies including writing the STIG for OS X and iOS
- Specializing in OS X security and management at scale for more than 10 years
- Continue to advise on multiple security standards for the government and private sector

This is going to get scary

MACTECH PRO EVENTS

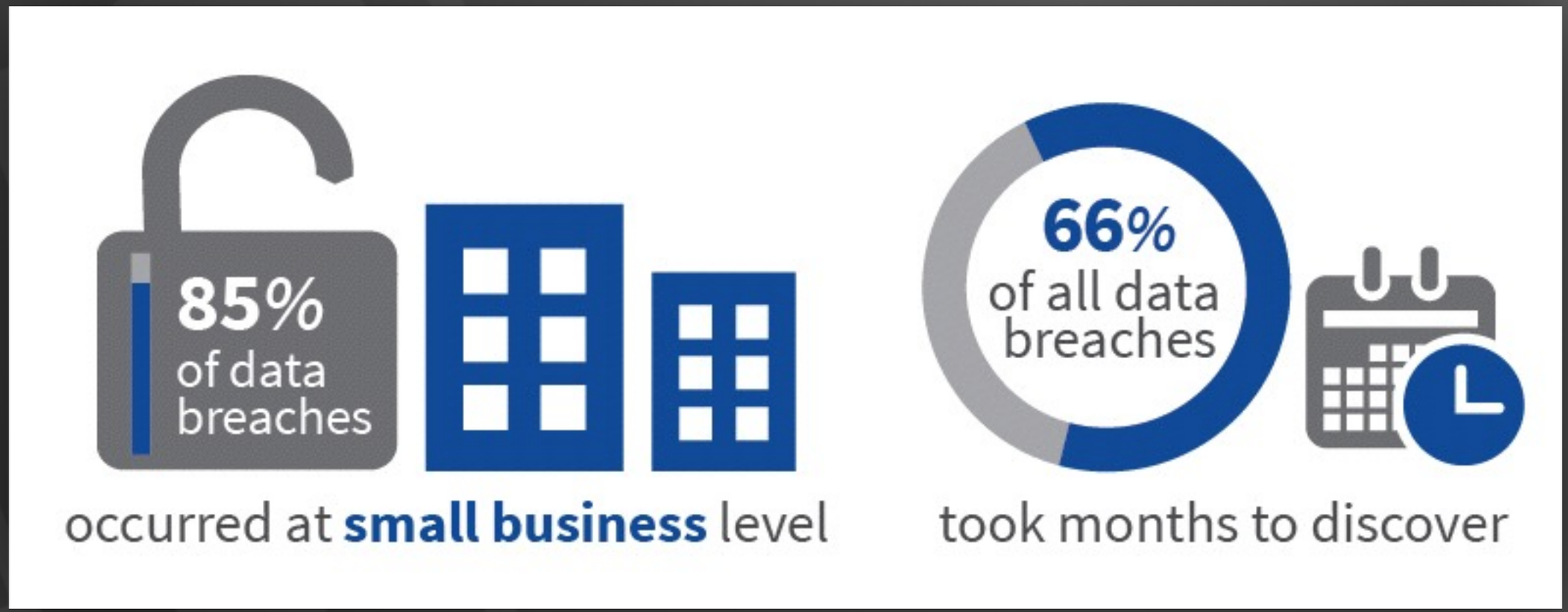
cmdSecurity

Why Security is Important

MACTECH PRO EVENTS

cmdSecurity

small business vulnerabilities



MACTECH PRO EVENTS

cmdSecurity

Definitions

Vulnerability -> Exploit -> Malware/Virus

- **Vulnerability:** A mistake in software that can be directly used by a hacker to gain access to a system or network
- **CVE:** Common Vulnerabilities and Exposures
  - Gives a common serial number to publicly known cybersecurity vulnerabilities
  - https://nvd.nist.gov/

Definitions

Vulnerability -> Exploit -> Malware/Virus

- **Exploit:** A sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software
- **HOW** an attacker uses a vulnerability to gain access to a computer

Definitions

Vulnerability -> Exploit -> Malware/Virus

- **Malware/Virus:** A malicious program that, when installed, performs some form of harmful activity. These activities can be
  - Data corruption or exfiltration
  - Movement to other, more important systems
  - Denial of service(s)
- **WHAT** an attacker is using vulnerabilities and exploits to place on your computer

Definitions

Phishing

- **Phishing:** the activity of defrauding an online account holder of financial information by posing as a legitimate company
- **HOW** an attacker side-steps all of your protections by communicating with the user directly, typically by email

Macs are immune though, right?

CVE(s) in the past 3 Months

- Mac CVE: 95
- Windows CVE: 193
- Linux CVE: 110

https://nvd.nist.gov

What NOT to do

"I am just trying to stay off the front page of the Washington Post"

What NOT to do

Relying on “do everything” security network devices or software

What NOT to do

Blame users for getting phished, exploited, or any other security incident-ed

What NOT to do

Every service and user has full admin rights

YES: Review POSIX permissions (rwxrw---)

YES: Least permission possible

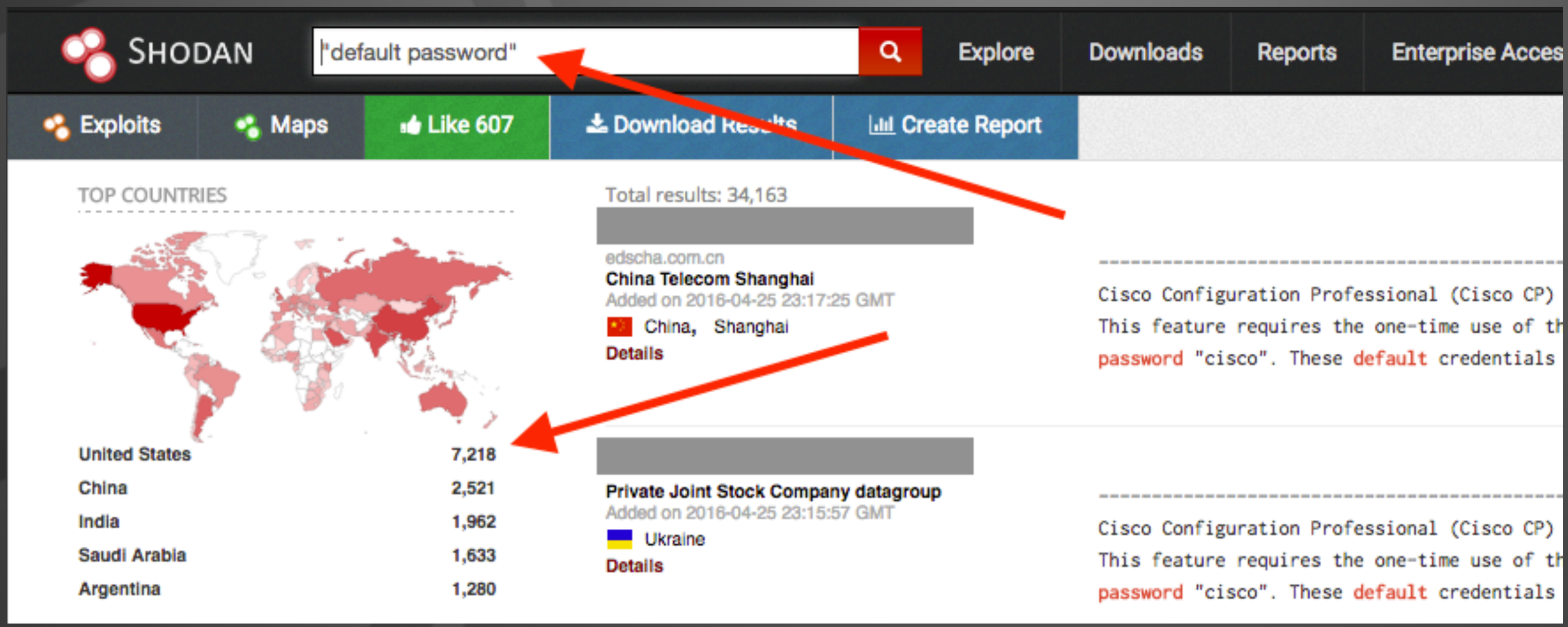
YES: Audit and review service accounts

What NOT to do

Thinking you are too small or obscure to be vulnerable to hackers

What NOT to do

Thinking you are too small or obscure to be vulnerable to hackers



MACTECH PRO EVENTS

cmdSecurity

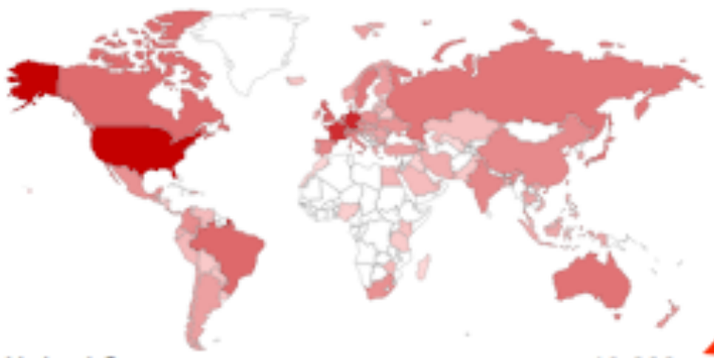
What NOT to do

Thinking you are too small or obscure to be vulnerable to hackers

SHODAN "os x" Explore Downloads Reports Enterprise Ac

Exploits Maps Share Search Download Results Create Report

TOP COUNTRIES



United States	13,609
Germany	6,985
France	6,178
Netherlands	1,955
United Kingdom	1,922

Total results: 50,006

[redacted]

AT&T Internet Services
Added on 2016-04-26 00:33:19 GMT
United States
Details

Firmware: 1
Hostname: [redacted]
Vendor: Mac OS X, Apple Computer, Inc

[redacted]

Added on 2016-04-26 00:32:39 GMT
France
Details

SSL Certificate
Issued By:
|- Common Name: localhost.localdomain
|- Organization: SomeOrganization
Issued To:

MACTECH PRO EVENTS

cmdSecurity

Macs are immune though, right?

CVE(s) in the past 3 Months

- Mac CVE: 95
- Windows CVE: 193
- Linux CVE: 110

https://nvd.nist.gov

The Good News

- It is the best spend of your company's money to train YOU
- A trained security professional will ALWAYS be better than automated security tools or automated attacks
- The goal of very good security is 100% attainable with a little work

“One of the NSA’s worst nightmares is a sysadmin who pays attention.”
-Rob Joyce, NSA TAO

(TAO) is a cyber-warfare intelligence-gathering unit of the National Security Agency (NSA)

This is your new benchmark: If you give someone like the NSA trouble, you defeat 99% of attackers

MDM - Central to Everything

- Audit and enforce every security setting
- Look for things you don’t expect
- An unmanaged computer is an insecure computer
- JAMF’s Casper Suite is current best in class

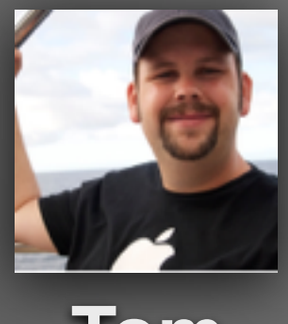
How to start on the road to securing your devices

- Understand some basic security architecture
- Leverage well-documented industry best practice (CIS, STIGs, USGCB, etc)
- It is your **PRIMARY** job to make security easy for your users
- Commit to continuous learning

Security is built on trust

Neil

Trusts



Tom

Vouched for:

Dan

Neil can trust
Dan's services

Security is built on trust

User Laptop

Public Key Cryptography

Trusts

VERISIGN

Cert. Authority

Vouched for:

Dan the Server

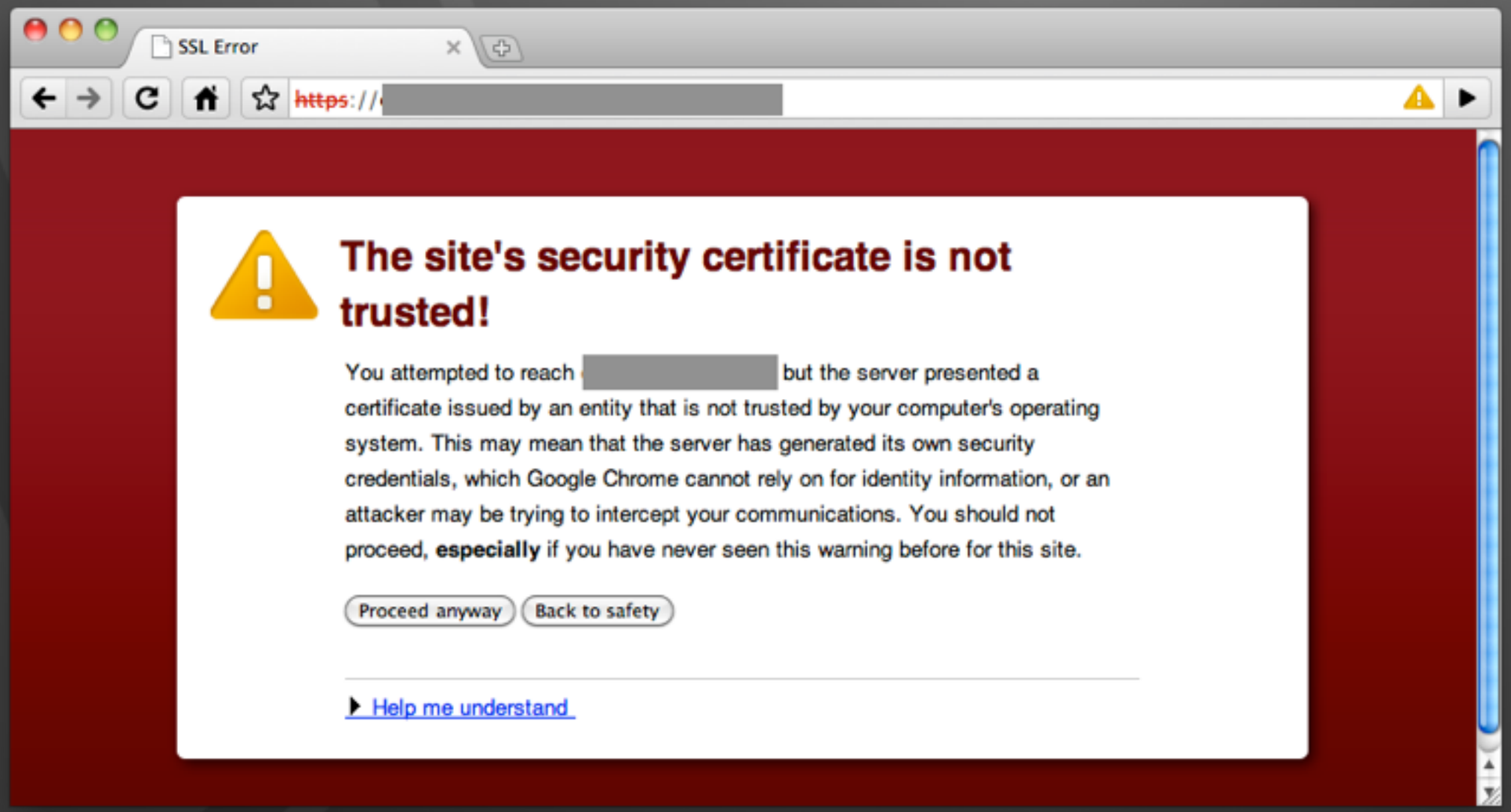
Laptop can trust
Dan the Server's services

MACTECH PRO EVENTS

cmdSecurity

What NOT to do

Train your users to click past certificate warnings



User Training

- Focus on the non-technical strange behavior they might see
  - Broken certificates on websites
  - Strange prompts for their password
- They don’t need to know how something is happening, only know when something is out of the ordinary

Antivirus: Pros and Cons

Pros:

- Good corporate citizen for windows clients on same network
- Catch known malware trying to infect your systems
- Easily clean known malware off of infected systems

Antivirus: Pros and Cons

Cons:

- Only catches previously seen viruses, uses rudimentary detection methods on OS X
- Often resource intensive, slows down a user's system
- Completely reliant on the vendor's ability to update the list of known viruses
- Trivial to bypass for malware developers

Users == Admins?

- What do your users need to do day to day?
- How tech savvy are they?
- If you remove admin rights you need to do everything admin for them, are you ready for that?
- Do you have the time to package and patch every app that needs to be patched?

Software Patching

- Absolutely critical to securing your devices
- Special attention to:
  - Oracle Java
  - Adobe Flash
  - OS X Security Updates

Free Tool: RansomWhere?

https://objective-see.com

- Detects when an non-apple process starts encrypting lots of files
- Has its limitations, but overall very good tool

Free Tool: Lockdown

https://objective-see.com

https://github.com/SummitRoute/osxlockdown

- Will run the CIS benchmark scripts on a computer to lock it down
- This WILL affect functionality of the device. Users WILL find features that have been disabled by this tool

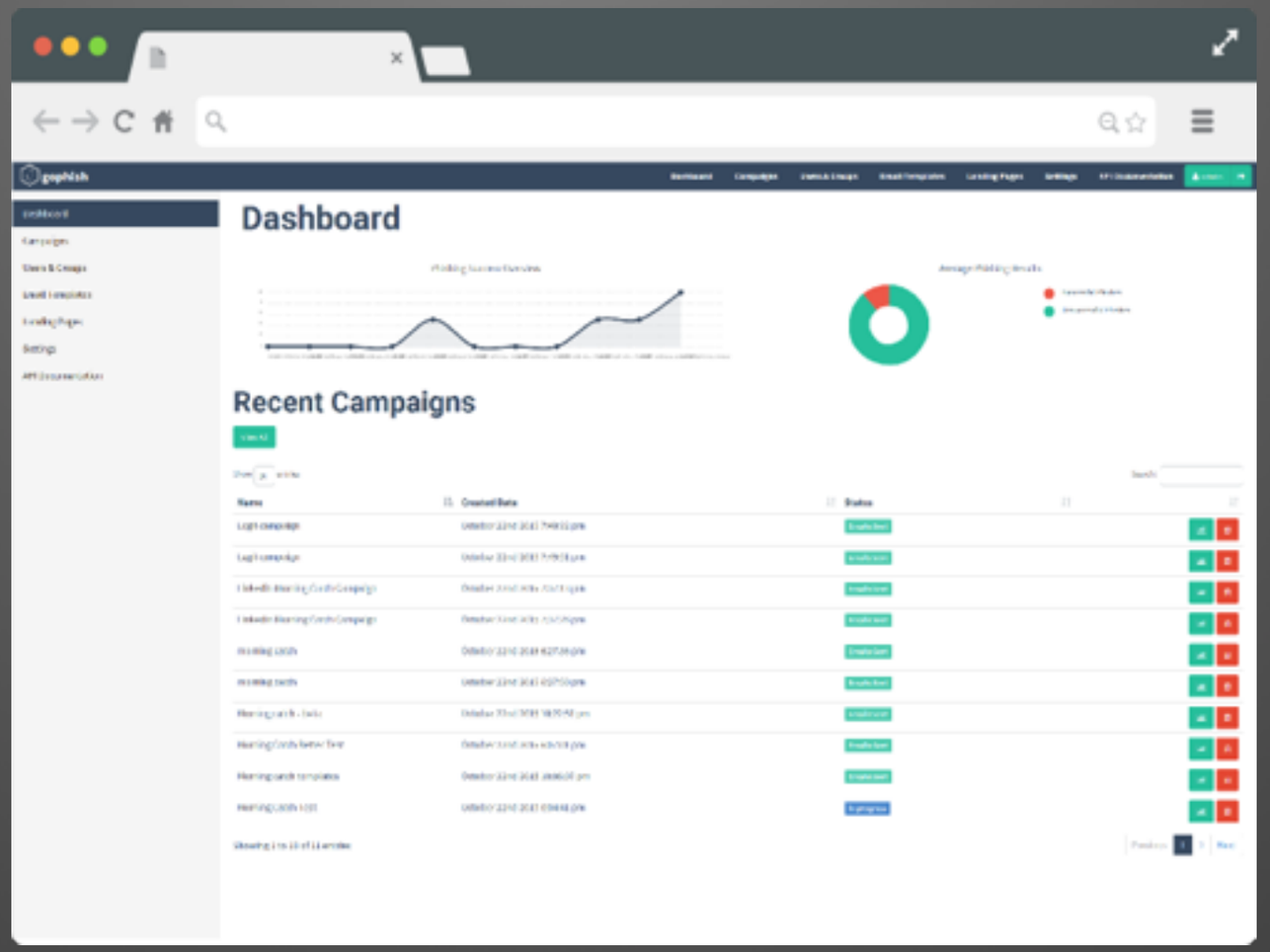
Free Tool: Ostiarius

https://objective-see.com

- Apple's gatekeeper on steroids
- User cannot bypass running unsigned apps from the internet
- Limited use case, all apps would pretty much need to come from app store

Free Tool: Simple Phishing Toolkit

https://github.com/gophish/gophish



MACTECH PRO EVENTS

cmdSecurity

Free Tool: osQuery

```
osquery> SELECT uid, name FROM listening_ports l, processes p WHERE
                                                    l.pid=p.pid;
```

osquery gives you the ability to query and log things like running processes, logged in users, password changes, usb devices, firewall exceptions, listening ports, and more.

You can perform ad-hoc queries or schedule them. More details can be found here

Enterprise Ready

CentOS, Ubuntu LTS and OSX are supported with no dependencies. osquery powers some of the most demanding companies, including Facebook.

Differential Changes

Know when critical objects are added, modified or deleted from a system.

Feature Velocity

You control the roadmap. Developed in the open, by the community, for the community.

Training Available

- www.sans.org
  - Courses: SEC301, SEC401, SEC506, SEC511
- CISSP - Non technical, read some of the many books
- Security + (CISSP Lite)
- CompTIA Linux Certification courses
- RedHat Linux Courses

MACTECH PRO EVENTS

cmdSecurity

Security Resources

- https://www.cisecurity.org/
- http://iase.disa.mil/stigs
- http://csrc.nist.gov/publications/PubsSPs.html
- https://usgcb.nist.gov/ (no OS X yet)

Questions?

MACTECH PRO EVENTS

cmdSecurity