Securing the managed environment

You, me, and everybody

Pepijn Bruienne

@bruienne

R&D Engineer

Duo Security

About Me

- 15+ year as Mac Admin
  - Small, medium, large enterprise
  - Higher Education
- FOSS user, contributor and author
  - AutoNBI
  - BSDPy
- Break Macs for profit
  - Protect customers
  - Contribute to community
- Active contributor
  - Slack (macadmins.org)
  - Twitter
  - Github
  - Macadmins.org podcast

The Problem

The Numbers

Top three failures causing data breaches

95%

Of breaches involved compromised **credentials**

75%

Of breaches involved compromised **endpoints**

26%

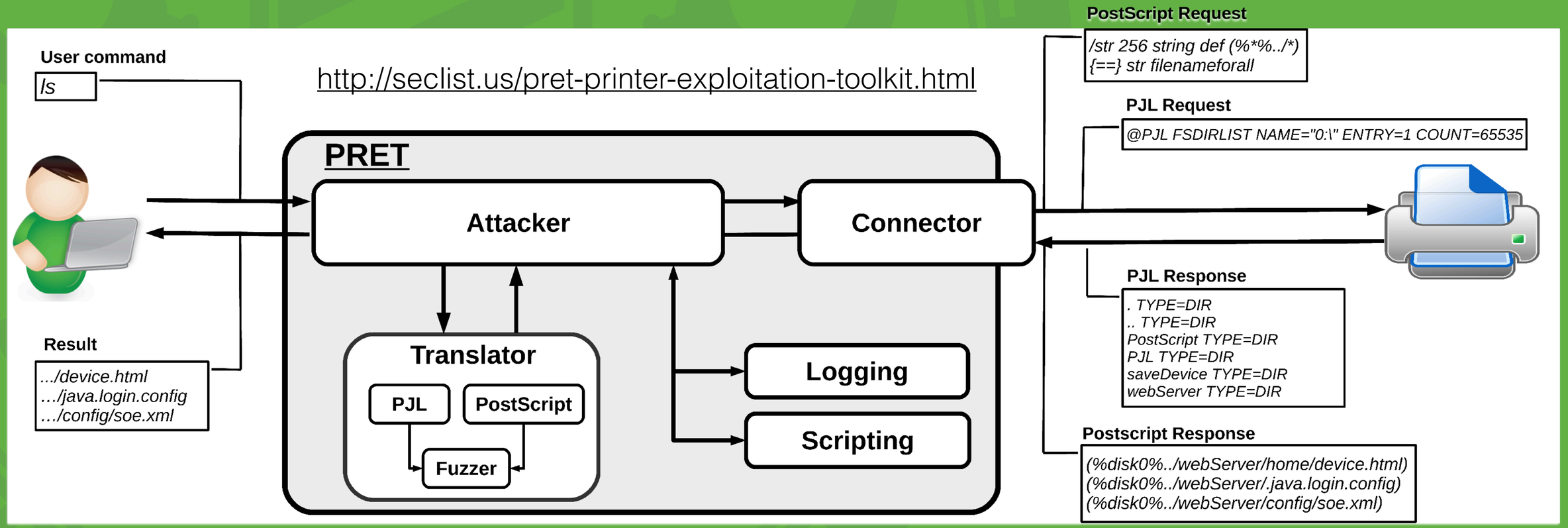
Of breaches involved **printers**

Source: Verizon 2015 Data Breach Investigations Report

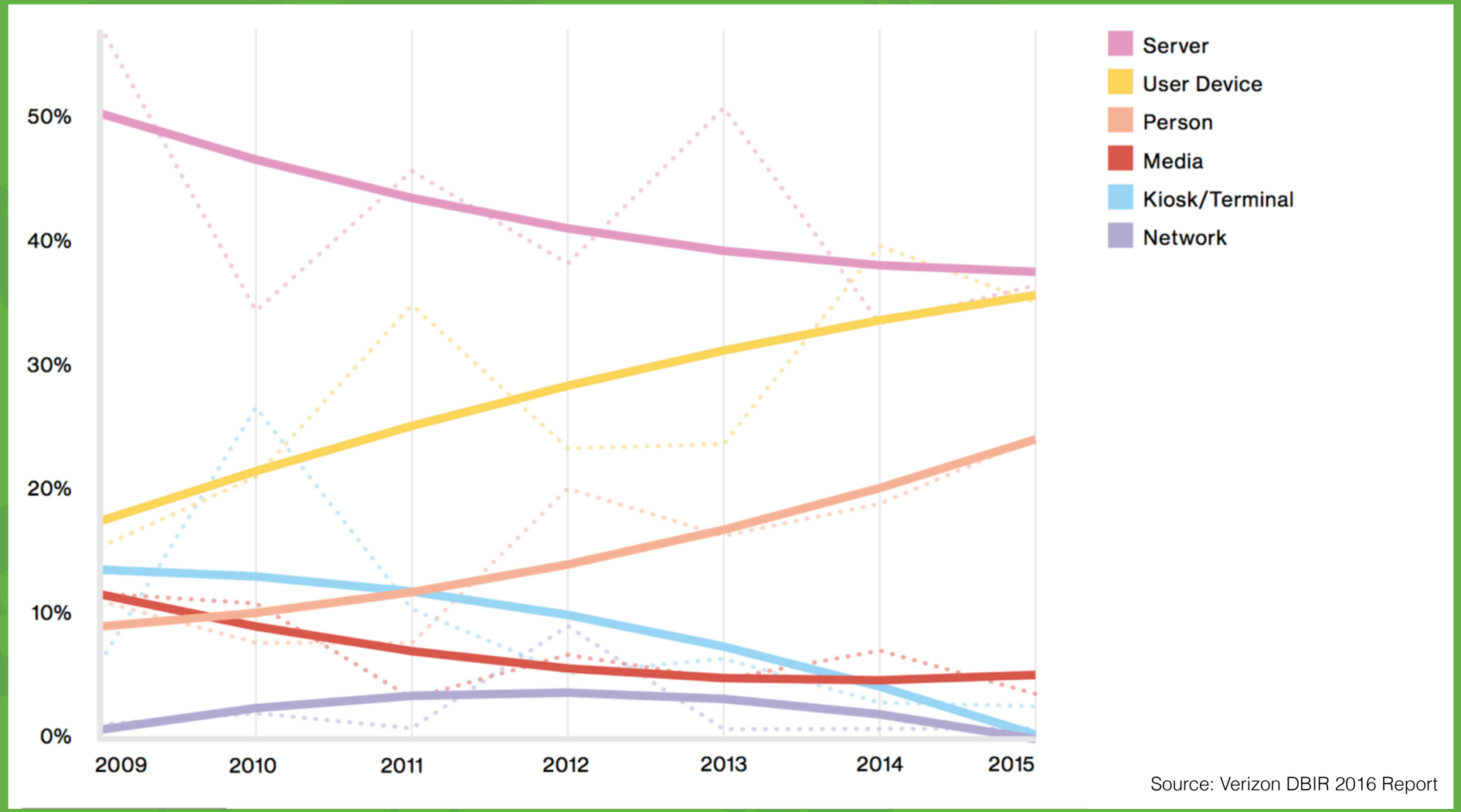
Wait. Printers?

Yes. Printers.

PRET - Printer Exploitation Toolkit
https://github.com/RUB-NDS/PRET



The Target



Source: Verizon DBIR 2016 Report

The Goal

Source: Verizon DBIR 2016 Report

Early Conclusion

The Threats

Malware aka APTs

Credential theft

Server attack

Malware/APT

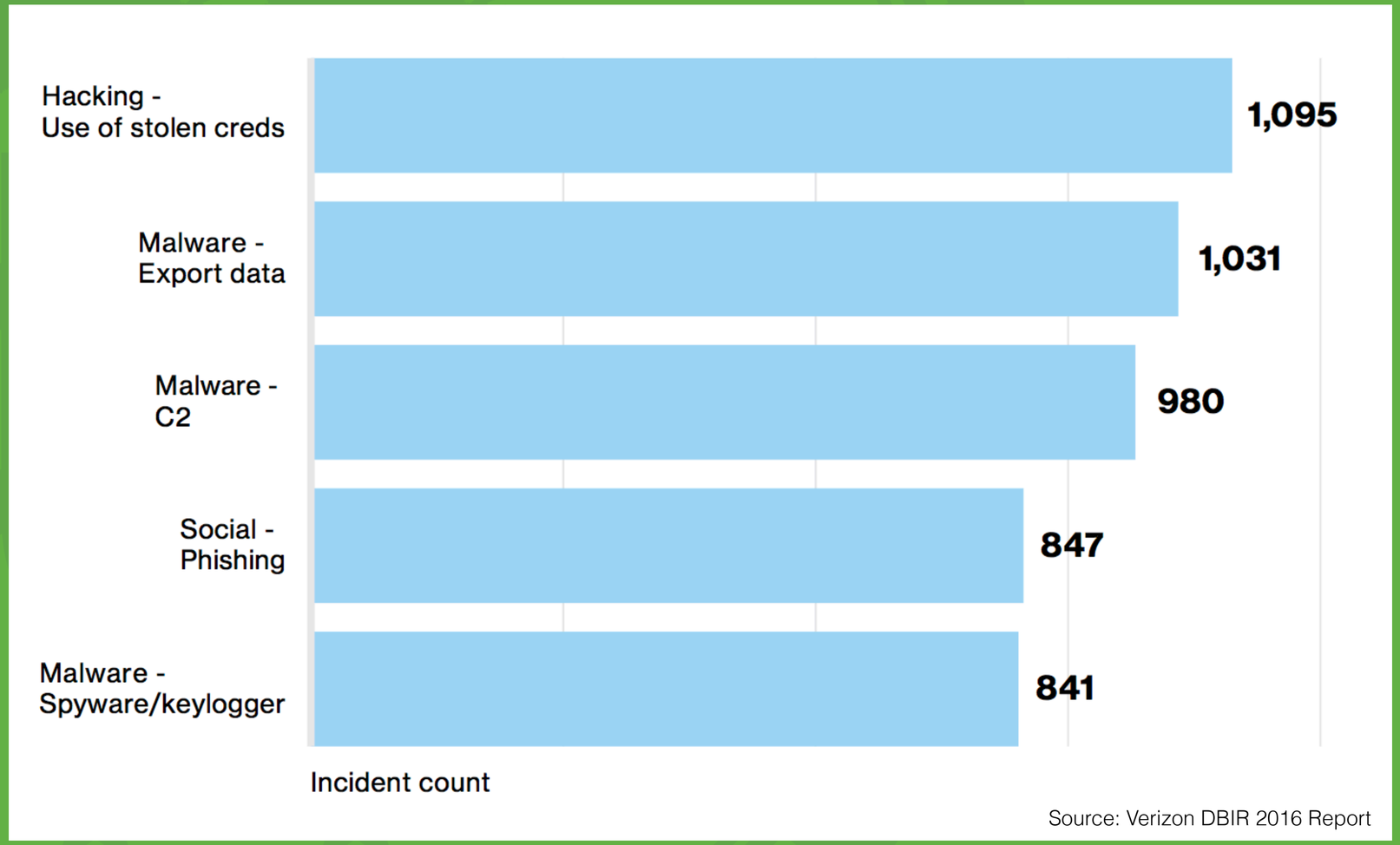
- Adware
  - Mostly just annoying, can deliver malware via Flash, leak data
- Spyware
  - Records A/V, takes screenshots, keylogging, data exfil
- Ransomware
  - Encrypts local/network data and backups
- Virus/APT
  - Everything else bad, deliver any of the above

Breach Lifecycle

Credentials

- **Credential bypass**
  - **Vulnerable systems**
  - **Brute force**
  - **0-day use**
  - **No credentials**
- **Credential exposure**
  - **Phishing**
  - **Insecure storage**
  - **Default settings**

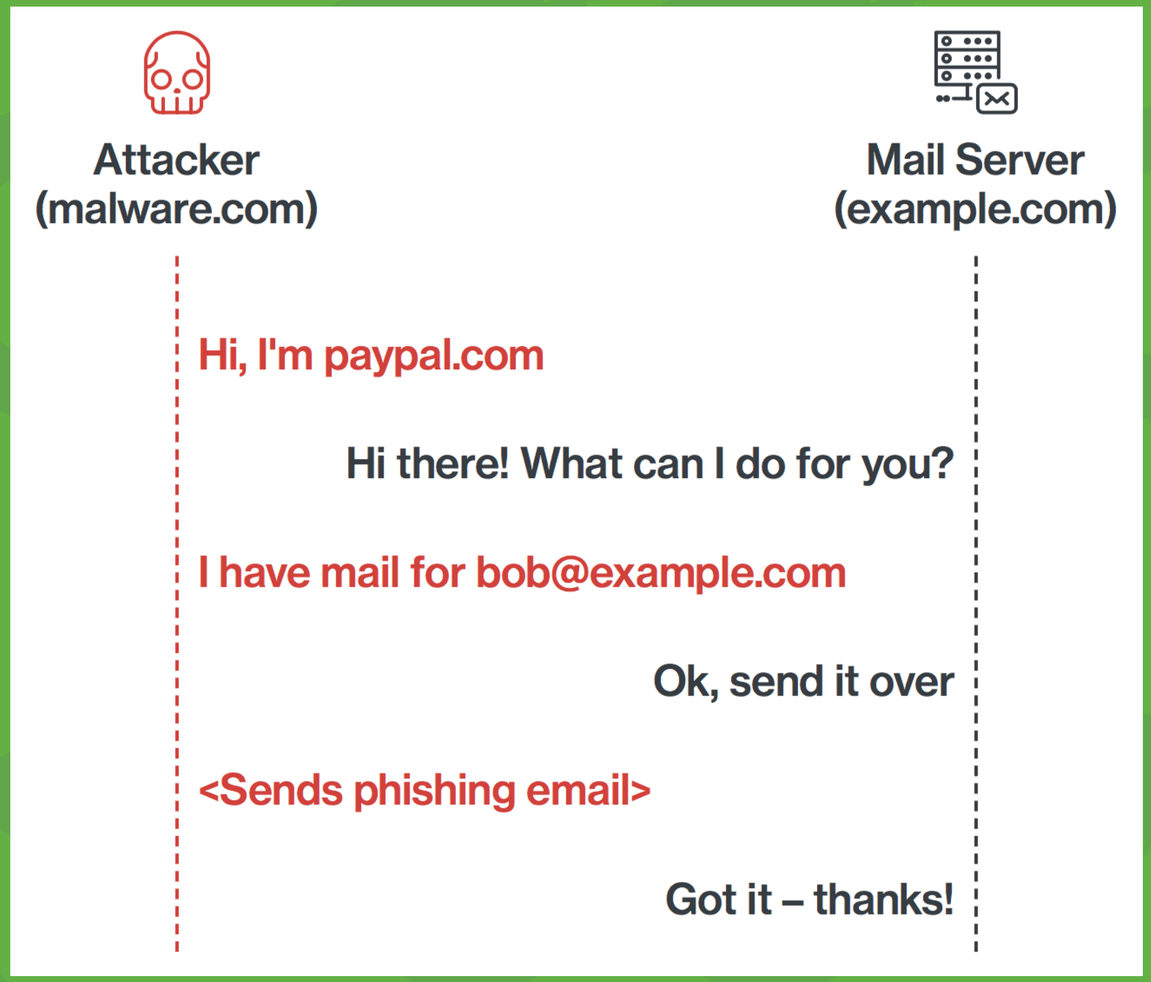
Credential Compromise



Source: Verizon DBIR 2016 Report

Phishing?

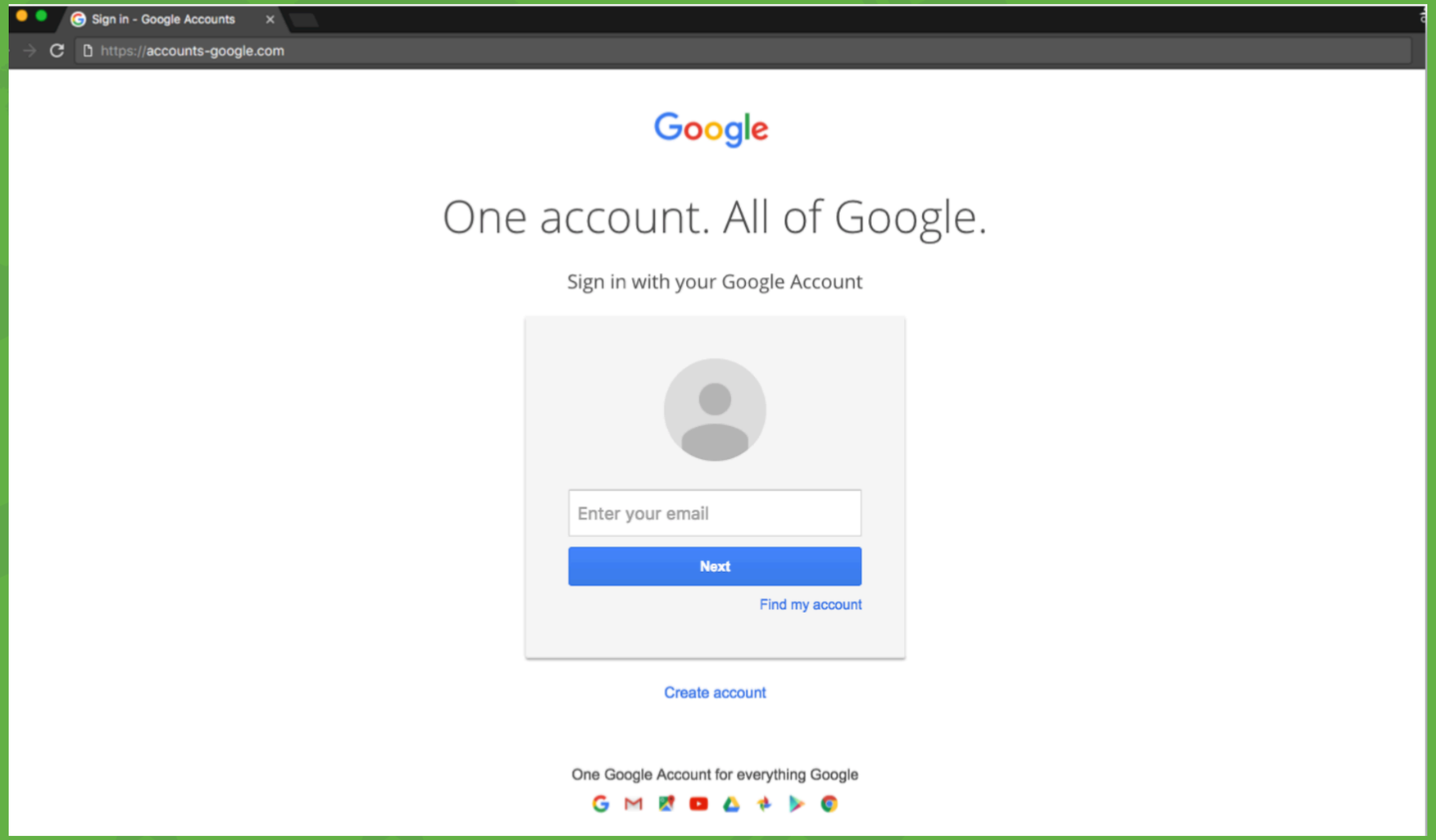
Phishing Basics



It's important to note that email addresses aren't always spoofed. They don't have to be. Attackers can be tricky and do things like:

- **Register a similar domain name (example: account-google.com as opposed to google.com or rnicrosoft.com or payppal.com)**
- **Use a domain that simply doesn't exist. (Yep! These are almost always delivered just fine.)**

Credential Phishing



Drive-by Phishing

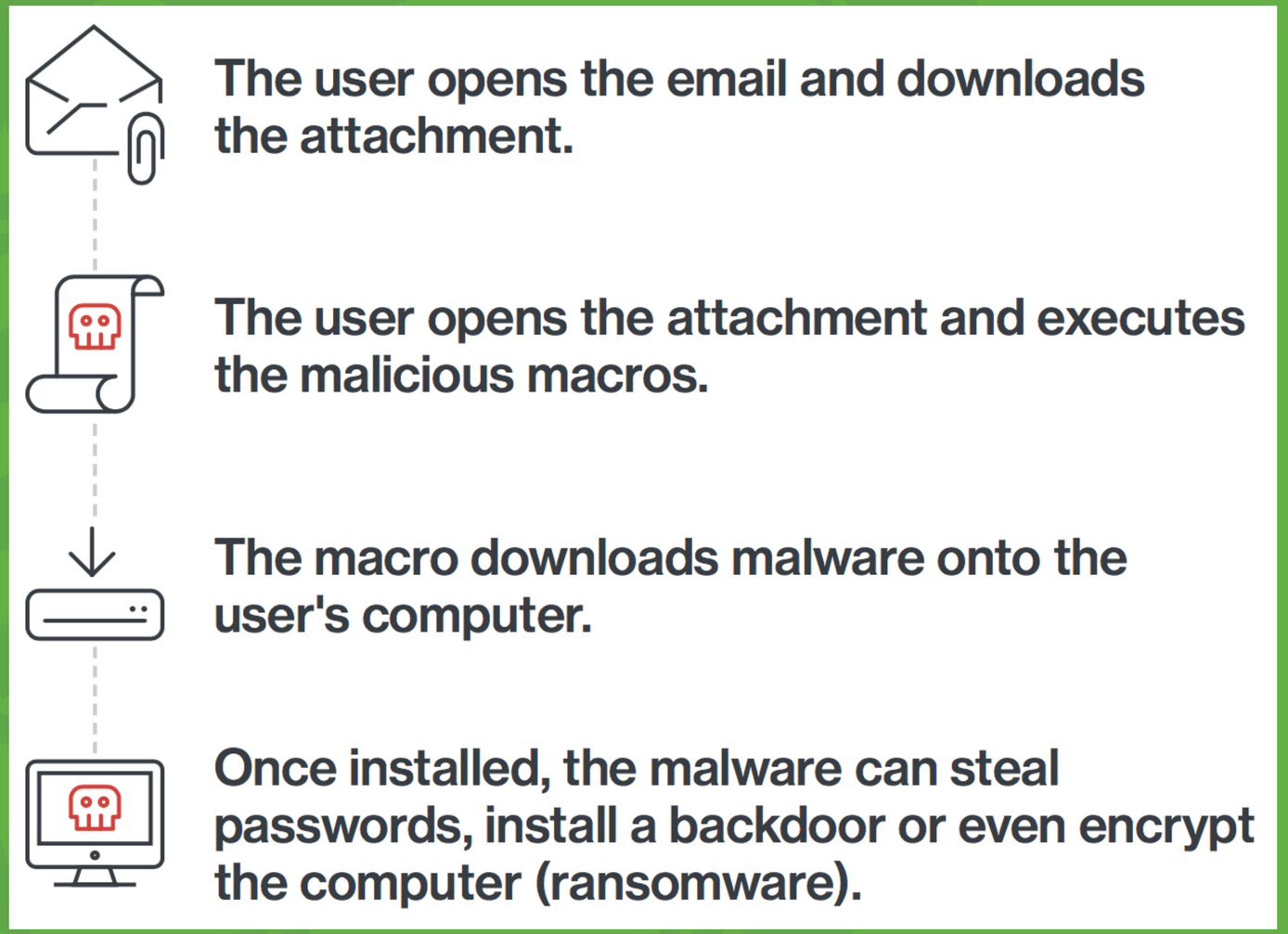
The user opens the email.

The user clicks the link in the email, unknowingly visiting a malicious page with an exploit kit.

The exploit kit compromises the user's out-of-date browser and downloads malware.

Once installed, the malware can steal passwords, install a backdoor or even encrypt the computer (ransomware).

Macro Phishing



https://duo.com/assets/ebooks/The%20Trouble%20With%20Phishing.pdf

Server Attack

- Public-facing service
  - Web
  - DB/NoSQL
  - File share 😱
  - DNS 😱 😱
- Network gateway/firewall
- Any other edge device

Server Attack Types

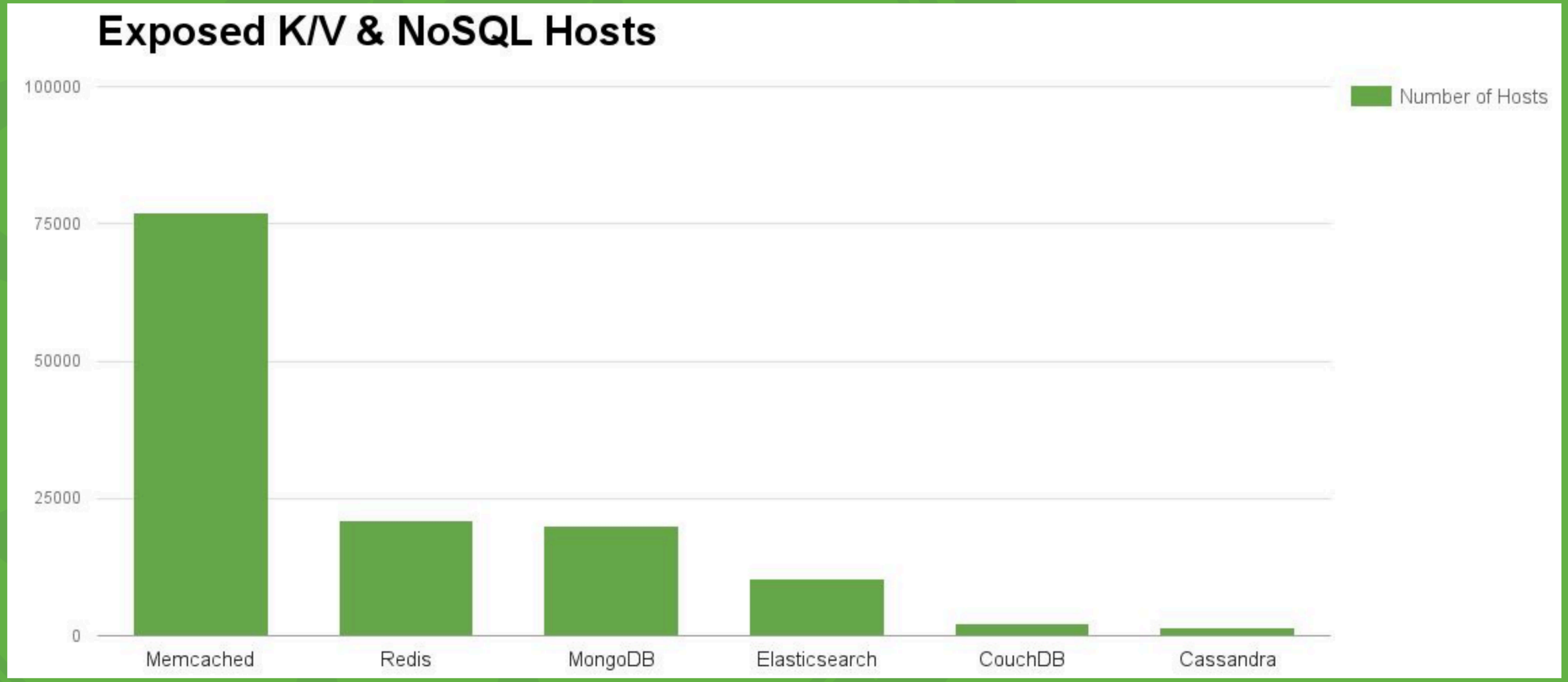
- **Accidental Discovery**: An ordinary user stumbles across a functional mistake in your application, just using a web browser, and gains access to privileged information or functionality.
- **Automated Malware**: Programs or scripts, which are searching for known vulnerabilities, and then report them back to a central collection site.
- **The Curious Attacker**: A security researcher or ordinary user, who notices something wrong with the application, and decides to pursue further.

Server Attack Types

- **Script Kiddies:** Common renegades, seeking to compromise or deface applications for collateral gain, notoriety, or a political agenda.
- **The Motivated Attacker:** Potentially, a disgruntled staff member with inside knowledge or a paid professional attacker.
- **Organized Crime:** Criminals seeking high stake payouts, such as cracking e-commerce or corporate banking applications, for financial gain.

🔗https://www.owasp.org/index.php/Threat_Risk_Modeling

NoSQL



Source: Jordan Wright - Scanning IPv4 for free data and free shells

NoSQL

Redis RCE + fake ransomware

- Targets auth-less Redis instance
- Wipes existing on-disk datastore (`flushall`)
- Creates new key with attacker's pub SSH key
- Changes datastore path to `/root/.ssh`
- Renames datastore to `authorized_keys`

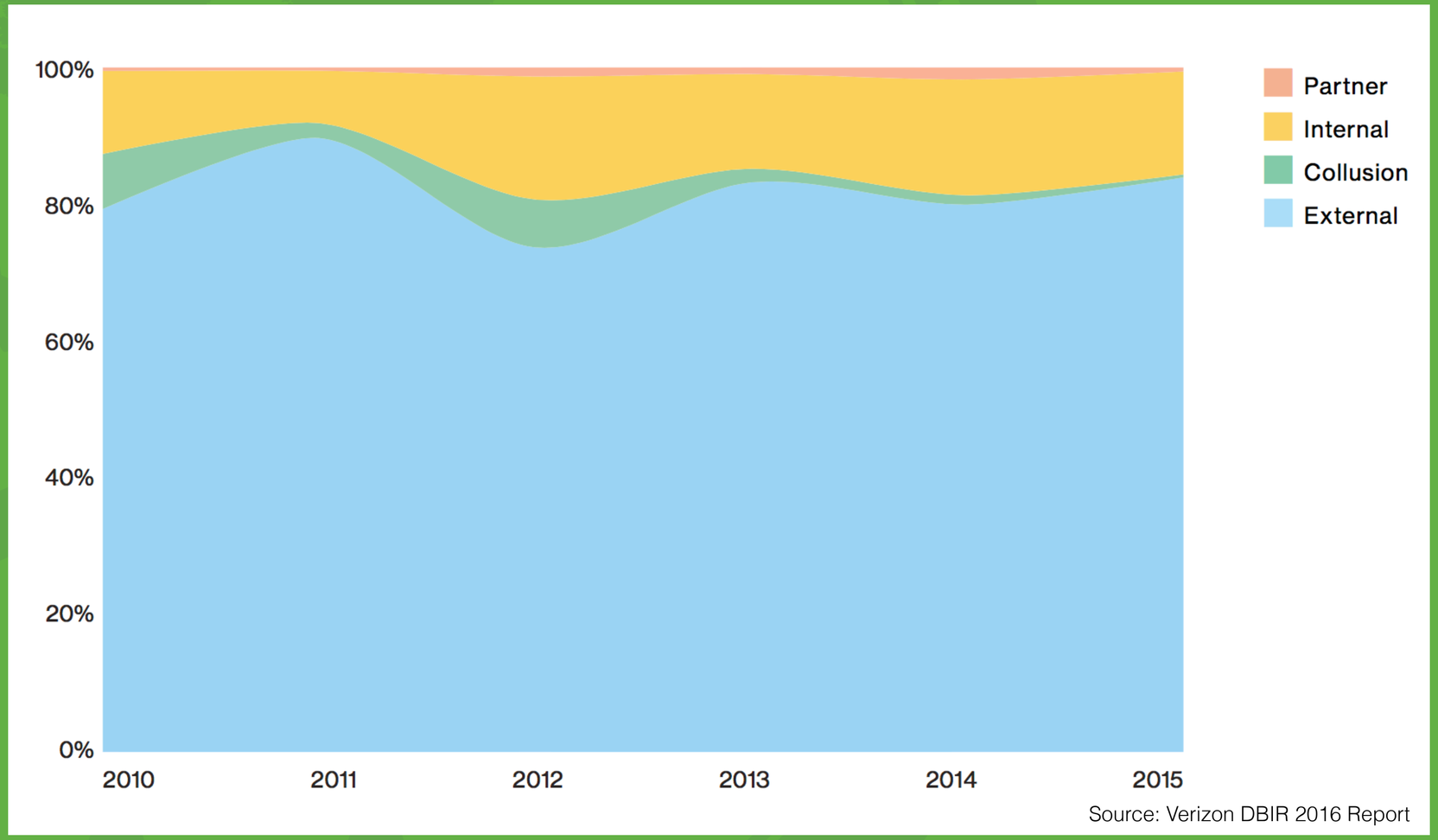
🔗 https://duo.com/blog/why-the-mongodb-ransomware-shouldnt-surprise-anyone

Which of these should Mac Admins worry about?


ALL OF THEM

The Managed Environment

The Source



Source: Verizon DBIR 2016 Report

The Managed Environment

Vulnerability vectors

The Managed Environment

Vulnerability vectors

The Cloud

Shadow IT

BYOD

Management tools

The Managed Environment

The Cloud

- Credential compromise
- Code vulnerabilities
- Off-site data
- Patched too slow

The Managed Environment

Shadow IT

- Vulnerabilities
- Malware/APT
- Data exfiltration
- Bypass managed resources

The Managed Environment

BYOD

- Malware/APT transmission
- Unprotected data
- Stored credentials

The Managed Environment

Management Tools

- Licensed software theft
- No payload verification
- Apple management tools
- DEP -> MDM exposure

Management Tools

Insecure Default Configuration

- JAMF SSL configuration defaulted to no verification
- Allows an attacker to MITM connection
  - SSL MITM allows viewing traffic in the clear
  - See plaintext XML, settings, passwords

🔗 https://www.okta.com/blog/2016/09/deploying-jamf-server-software/

Management Tools

- Software deployment compromised
- No payload integrity checking performed
  - TUF - The Update Framework
  - Use multiple keys to validate payloads
- Insert replacement payload for existing item
  - Now deploys item + APT (as root!)

Management Tools

DEP to MDM brute-force

- DEP API *only* requires a valid serial number
- Example: run `/usr/libexec/mdmclient dep nag`
- DEP API returns MDM config if serial number found
- Apple serial numbers can be easily guessed/generated
- Guess serial -> send DEP request -> get MDM config
- MDM enrollment -> get 🥓

The Admin

What is their attack surface?

The Admin

- Access to credentials for many systems
- More access than needed (just sudo/yolo it)
- Lack full picture of sensitive systems
- Imperfect security hygiene
  - Also vulnerable to phishing!
- Password reuse / weak passwords

The Admin

- Store shared secrets in a common system
  - Credentials compromised
  - Admin access on other systems
- Example: Palantír
  - Red team gained access to wiki
  - Contained JAMF admin credentials
  - Rogue payload added

The Admin

https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

What is U2F?

https://www.yubico.com/about/background/fido/

The User

What is their attack surface?

The User

- Top phishing target
- Shadow IT to use tools they want
- BYOD to use devices they want
- Security hygiene
  - Misconceptions
  - Lack thereof

The User

- Phishing gains access to user
- Attacker gains further access by pivoting
  - Access internal-only systems/networks
  - Use contacts to phish other higher-privileged users, gain access
  - Host CNC server for further attacks

The User

https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

What's the Solution?

Not The Solution

- Cycling passwords every month/week/day
  - Cycle SSL certs instead
- MOAR Antivirus!
  - Checkbox security is not security
- MDM!
  - Fancy management tools won't fix bad practices

The Solution - Managed Environment

- Don't expose services that don't need it
- Leave no default configuration unchecked
- Use 2FA where possible - **U2F = best**
- Use PKI for SSH access to servers
- Have a testing environment
- Demand better from your vendor

The Solution - Users

- Educate users on good security hygiene
  - Apply updates quickly
  - Phishing awareness
  - Strong, unique passwords
  - Password manager
  - 2FA (Push, U2F)
- Use 2FA? Stop using SMS!

The Solution - Admins

- Take your own advice!
  - Offer software updates quickly
  - Phishing affects you too, more damaging
  - Strong, unique passwords
  - Password manager
  - 2FA (Push, U2F)
- Use 2FA? Seriously, stop using SMS!

Conclusion

- All members of the managed environment are important
- Overall security is only as strong as your weakest part
  - Perfect users + lax admins = ☠️
  - Lax users + perfect admins = ☠️
  - Perfect systems + lax humans = ☠️

Conclusion

- Point is to make it a lot harder to be breached using simple to follow practices
- Rise of phishing = lazy works
- Unless you are Google/Facebook/Twitter/GH no one is going to burn a 0-day on you
- Implement the top 5 and be 99% more secure than you are now

Thank you!

https://seclist.us/pret-printer-exploitation-toolkit.html

https://github.com/RUB-NDS/PRET

https://duo.com/assets/ebooks/The%20Trouble%20With%20Phishing.pdf

https://www.owasp.org/index.php/Threat_Risk_Modeling

https://duo.com/blog/why-the-mongodb-ransomware-shouldnt-surprise-anyone

https://www.okta.com/blog/2016/09/deploying-jamf-server-software/

https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

https://www.yubico.com/about/background/fido/

https://duo.com/assets/pdf/Scanning%20IPv4%20for%20Free%20Data%20and%20Free%20Shells.pdf

Questions?