PRESENTED BY:

- João Luís | 107403
- Luís Leal | 103511
- Ricardo Quintaneiro | 110056
- Vítor Santos | 107186

SHELLSHOCK

CVE-2014-6271

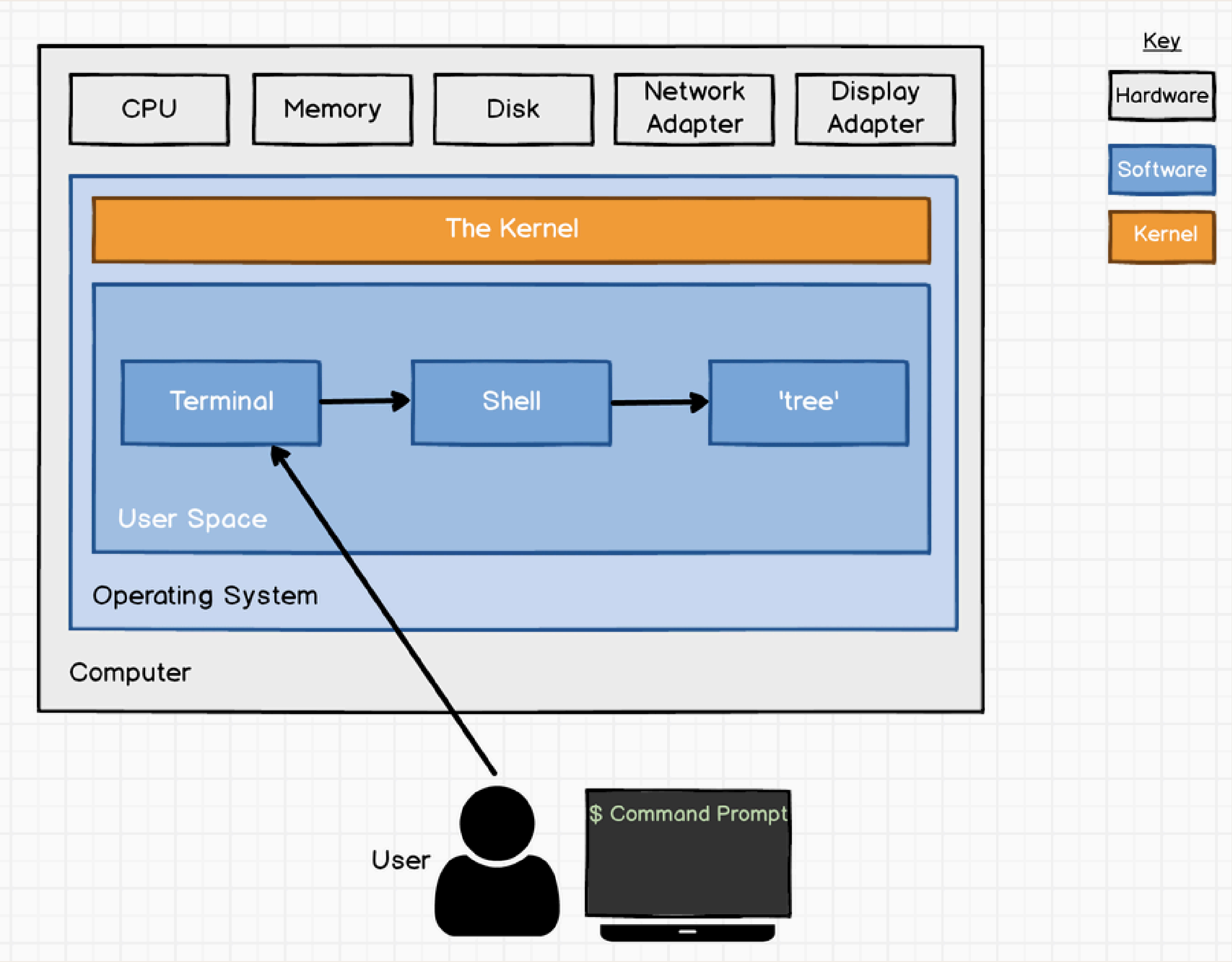
AEV - ANALYSIS AND EXPLORATION OF VULNERABILITIES

1

INTRODUCTION

OPERATING SYSTEM SHELL

- **OS kernels** provide a collection of services (filesystem management, process management, etc...) in the form of an **API**.
- Shells exist as an **interactive wrapper** application for these services, available to users via a CLI or GUI.



OPERATING SYSTEM SHELL

- Often implement a **scripting language** interpreter for written commands.

- **Widely** used by developers and software applications (**33.9%** with **extensive development** in the StackOverflow 2024 survey)

- **Simple task automation scripts** for file & process management and **environment configuration**.

```
:(){ :|:& };:
```

This is a fork bomb! A DoS attack in only 13 characters!

DO NOT EXECUTE

```
rm -rf /*
```

This deletes your entire filesystem!

GNU BASH

- Developed for the **GNU Project** by Bryan Fox and released in **1989** as a **free software** alternative to the Bourne shell
- Operates within a text window and supports the execution of commands from files (**shell scripts**) which facilitates **automation**
- Incorporates features from multiple shells, such as Bourne shell, C shell (csh) and Korn shell (ksh), making it both **POSIX-compliant** and **feature-rich**.

GNU BASH RELEVANCE

- **Most popular shell** among Linux users
- **Linus Torvalds** complemented the **Linux kernel** by porting the Bash shell
- **96.3%** of the **top 1,000,000 web servers run Linux**
- **Docker** and **Kubernetes use bash** for container orchestration and management
- Other relevant bash uses include **system administration**, **automating application deployment** and **IoT**

IBM
intel
cisco
CERN
aws
NYSE
NASA

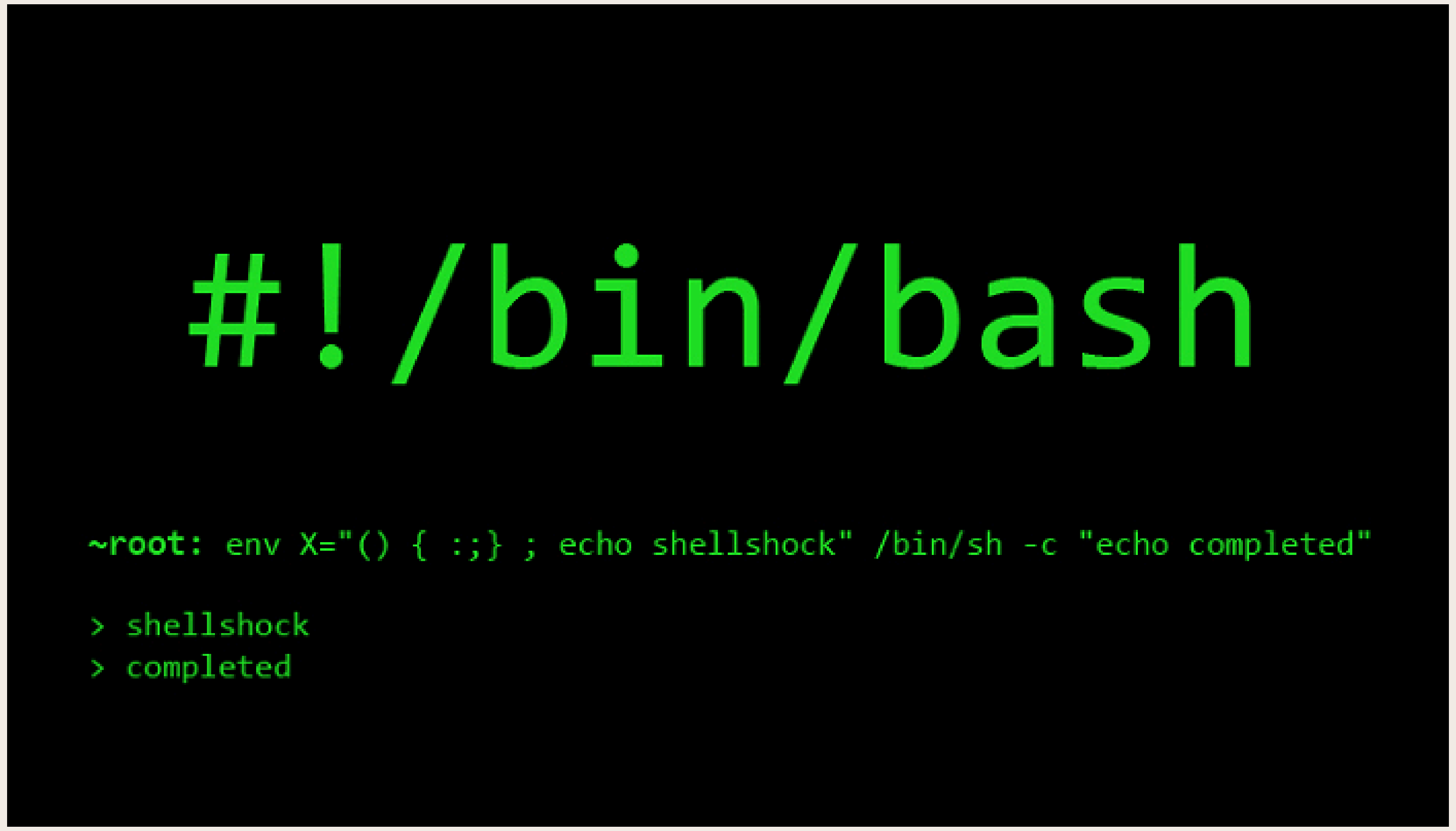
Companies that use Linux as of 2023

2

SHELLSHOCK

DESCRIPTION

- Discovered by Stéphane Chazelas;
- Bash allowed command execution when commands were concatenated to the end of function definitions stored in the environment variables;
- It could allow ACE (Arbitrary Code Execution) and gain unauthorised access;
- Related CWE: 78- Improper Neutralization of Special Elements used in an OS Command;



```
#!/bin/bash

~root: env X="() { :;} ; echo shellshock" /bin/sh -c "echo completed"

> shellshock
> completed
```

EVOLUTION OF THE SOFTWARE BUG

1 September 1989

Bug released in Bash v1.03

12 September 2014

Stéphane Chazelas informed Bash's maintainer of his discover of the original bug

24 September 2014

First patch
CVE-2014-6271 (CVSS: 9.8)

Second patch
CVE-2014-7169 (CVSS: 9.8)

25 September 2014

Third Patch

27 September 2014

CVE-2014-6277 (CVSS: 10)

28 September 2014

CVE-2014-7186 (CVSS: 10)
CVE-2014-7187 (CVSS: 10)

30 September 2014

CVE-2014-6278 (CVSS: 10)

EXPLOITATION VECTORS

- **CGI (Common Gateway Interface)**- Used by Apache. Exploit can be done intercepting the web page request, and changing User-Agent header to the malicous payload (in Bash);

- **OpenSSH server**- Exploiting variable “SSH_ORIGINAL_COMMAND”. However, interactive shell needs to be turned off;

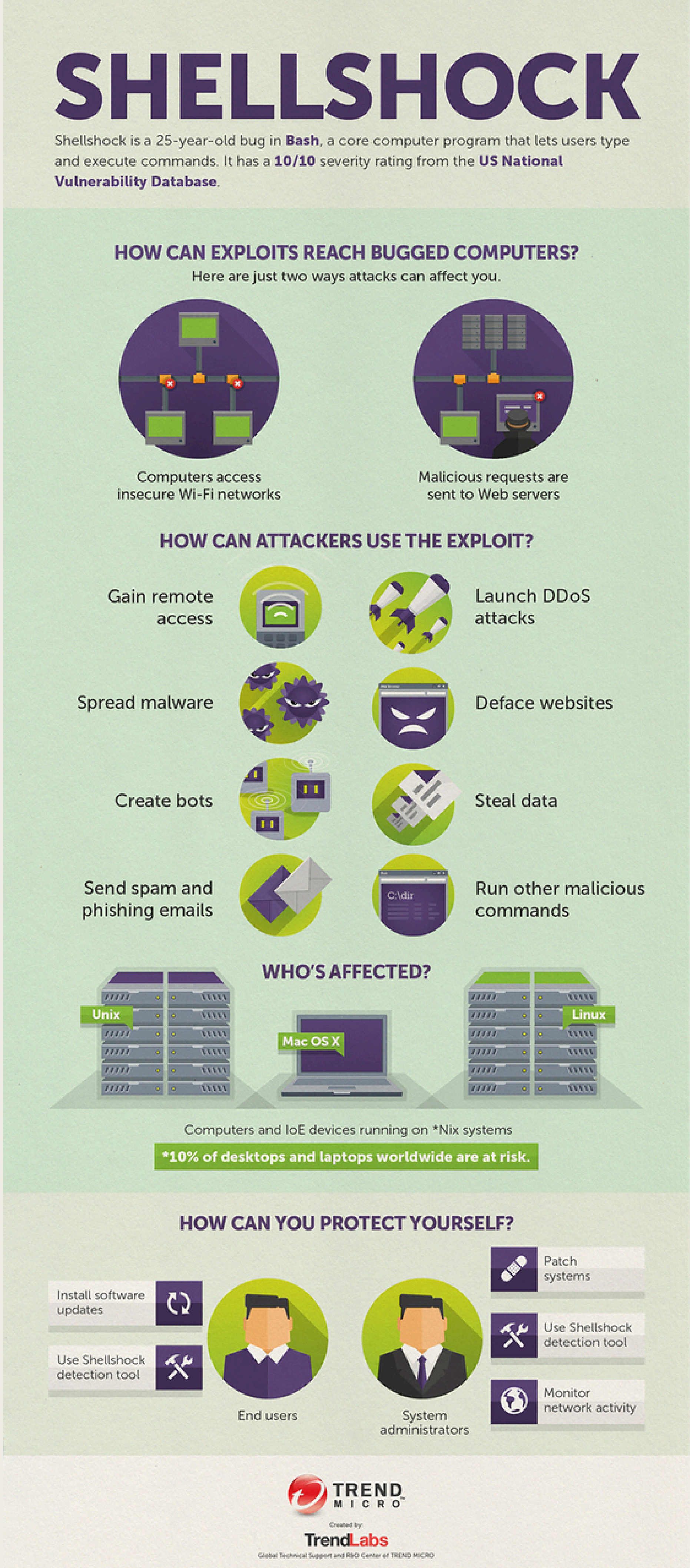
- **DHCP clients**- A malicious DHCP server can do a “DHCP Offer” that contains a malicious payload in environment variables;

- **Qmail server** - Specially crafted “MAIL FROM” header due to Qmail not sanitize properly input before setting environmental variables;

- **IBM HMC restricted shell**- Stills allow execution of entirely untrusted software and, therefore, escpe to a normal shell;

KNOWN IMPACTS AND COVERAGE

- Reported compromised machines on the day that the vulnerability was made public;
- Botnets attacks aiming DDoS appeared in the following days;
- By 30 September, CloudFlare said it was tracking approximately 1.5 million attacks per day.



SHELLSHOCK

Shellshock is a 25-year-old bug in **Bash**, a core computer program that lets users type and execute commands. It has a **10/10** severity rating from the **US National Vulnerability Database**.

HOW CAN EXPLOITS REACH BUGGED COMPUTERS?

Here are just two ways attacks can affect you.

Computers access insecure Wi-Fi networks
Malicious requests are sent to Web servers

HOW CAN ATTACKERS USE THE EXPLOIT?

Gain remote access
Launch DDoS attacks
Spread malware
Deface websites
Create bots
Steal data
Send spam and phishing emails
Run other malicious commands
C:\dir

WHO'S AFFECTED?

Computers and IoE devices running on *Nix systems

*10% of desktops and laptops worldwide are at risk.

HOW CAN YOU PROTECT YOURSELF?

3

DEMO

REFERENCES

Operating System Shells:

1. https://www.ibm.com/docs/en/aix/7.2?topic=administration-operating-system-shells
2. https://survey.stackoverflow.co/2024/technology
3. https://nvd.nist.gov/vuln/detail/CVE-2014-6271
4. https://nvd.nist.gov/vuln/detail/CVE-2014-6277
5. https://nvd.nist.gov/vuln/detail/CVE-2014-6278
6. https://nvd.nist.gov/vuln/detail/CVE-2014-7169
7. https://nvd.nist.gov/vuln/detail/CVE-2014-7186
8. https://nvd.nist.gov/vuln/detail/CVE-2014-7187
9. https://www.exploit-db.com/docs/english/48112-the-shellshock-attack-%5Bpaper%5D.pdf?ref=benheater.com
10. https://www.baeldung.com/linux/ssh-shellshock-exploit
11. https://github.com/jeholliday/shellshock/blob/master/README.md
12. https://www.wakko.one/en/ibm-hmc-shellshock-hacked-en.html
13. https://truelist.co/blog/linux-statistics/

Images:

1. https://upload.wikimedia.org/wikipedia/commons/8/84/Bash_demo.png
2. https://effective-shell.com/assets/images/diagram3-terminal-and-shell-31620f593a4c3838051a5a6dcea17577.png
3. https://blogs.quickheal.com/shellshock-bug-care/
4. https://www.trendmicro.com/vinfo/pl/security/news/vulnerabilities-and-exploits/the-shellshock-vulnerability-bash-bug
5. https://www.putorius.net/basics-of-using-bash-history.html