Defense through Collaboration

The Use of Free Software in Preventing Proprietary Software Based Virus Attacks

Free Software > Open Source Software > Proprietary Software

Free Software

- The freedom to run the program as you wish, for any purpose.
- The freedom to redistribute copies so you can help your neighbor.
- The freedom to study how the program works, and change it so it does your computing as you wish.
- The freedom to distribute copies of your modified versions to others.

https://www.gnu.org/philosophy/free-sw.en.html

Open Source Software:

Allows the source code, blueprint or design to be viewed.

Allows the source code to be used, modified and/or shared under <u>defined terms and conditions</u>.

- Proprietary Software:

Publisher carries intellectual property rights, such as copyright and patent rights.

Source code is not available to the public.

AUUG, Inc. (March 2003). "Chapter 1. Definitions"
AUUGN. AUUG, Inc. p. 51. Retrieved 29 June 2017.

```
                    uuu$::$::$::$::$::$uu
                 uu$$$$$$$$$$$$$$$$$$$uu
               u$$$$$$$$$$$$$$$$$$$$$$$$$u
              u$$$$$$$$$$$$$$$$$$$$$$$$$$$u
             u$$$$$$$$$$$$$$$$$$$$$$$$$$$$$u
             u$$$$$$$$$$$$$$$$$$$$$$$$$$$$$u
             u$$$$$$*   *$$$*   *$$$$$$u
             *$$$$*      u$u       $$$$*
              $$$u       u$u       u$$$
              $$$u      u$$$u      u$$$
               *$$$$uu$$$   $$$uu$$$$*
                *$$$$$$$*   *$$$$$$$*
                  u$$$$$$$u$$$$$$$u
                   u$*$*$*$*$*$*$u
        uuu        $$u$ $ $ $ $u$$       uuu
       u$$$$        $$$$$u$u$u$$$       u$$$$
        $$$$$uu      *$$$$$$$$$*     uu$$$$$$
      u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$$
      $$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
       ***      **$$$$$$$$$$$uu **$***
              uuuu **$$$$$$$$$$uuu
     u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
     $$$$$$$$$$****           **$$$$$$$$$$$*
      *$$$$$                     **$$$$**
        $$$*       PRESS ANY KEY!       $$$$*
```

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:
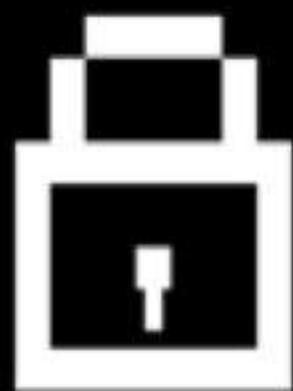
    1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

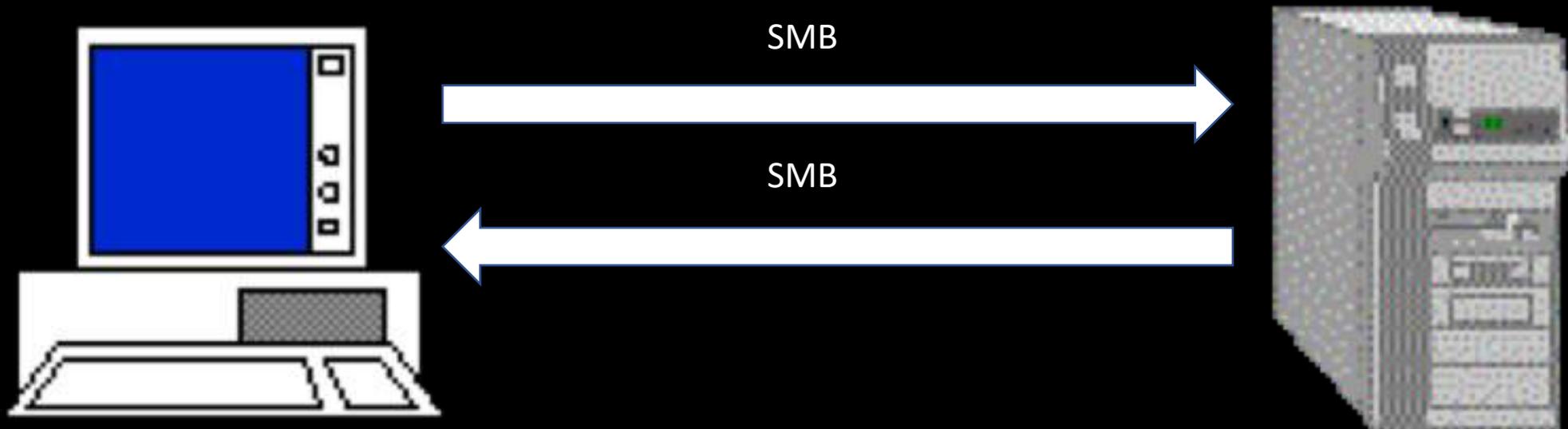   Ap5JVb-qhTAHy-HyeyS2-wqeQEK-YtHQeK-w7NUmZ-11RBUq-fuu4Wa-zpv8dS-zeQNGS

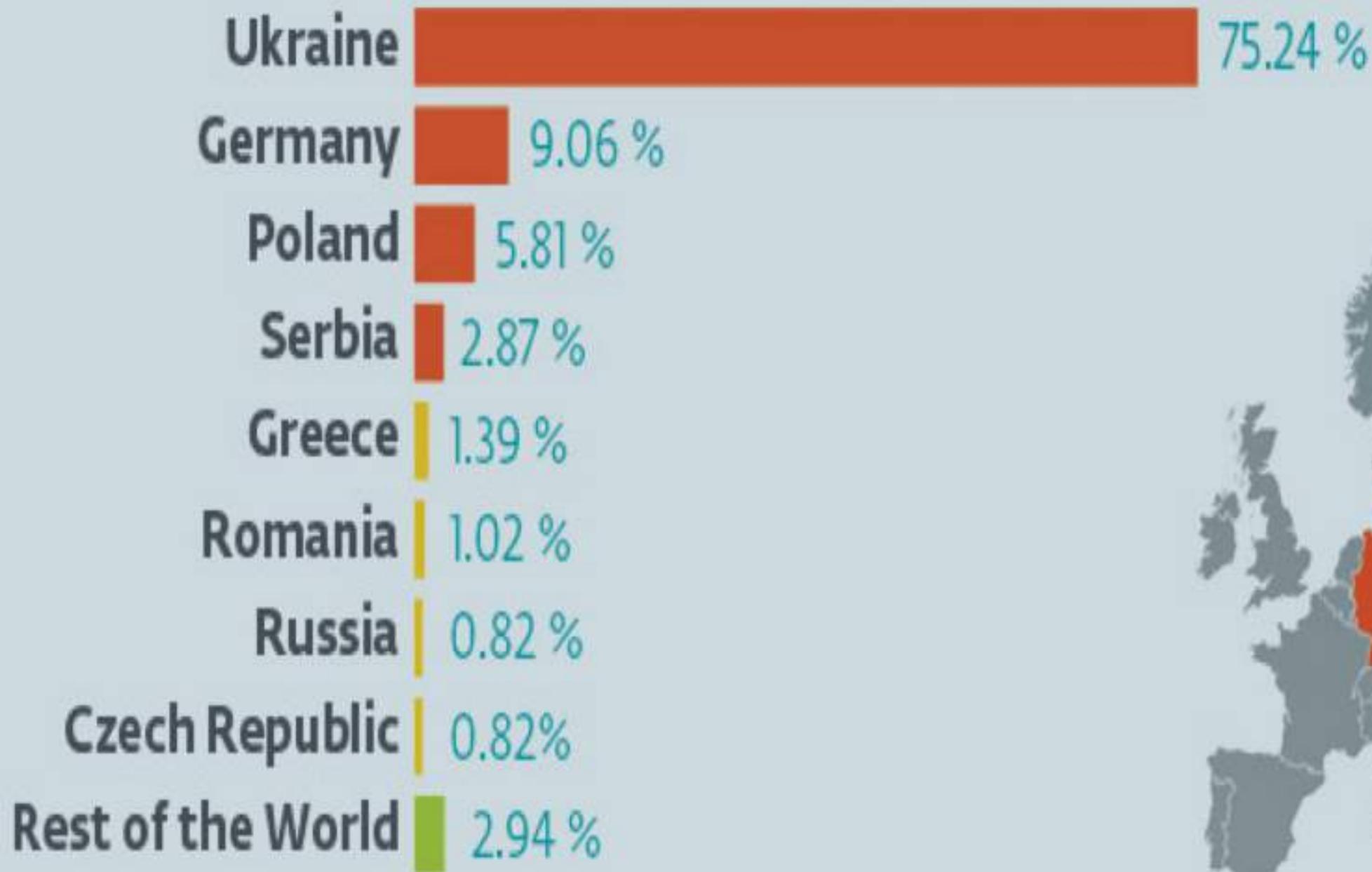If you already purchased your key, please enter it below.
Key:

NOTPETYA

ETERNALBLUE

NotPetya Infections by Country

Country	Percentage
Ukraine	75.24 %
Germany	9.06 %
Poland	5.81 %
Serbia	2.87 %
Greece	1.39 %
Romania	1.02 %
Russia	0.82 %
Czech Republic	0.82%
Rest of the World	2.94 %

Why is this important?

Cyber Warfare is Unlike Any Other Warfare Humanity Has Seen

- A wider cast of players.
- Attackers are not always obvious.
- Attacks aren't always noticeable.
- The attacks are faster.

Cyber Attacks are Crossing Into the Real World

Abfahrt   Linie   Ziel   Gleis

Ziel   Nach   8

Über   Olbernhau   11

Zeit   Über
Flöha - Pockau-Lengefeld   Hbf
22:10   10
RB81   Flöha - Frei   (S) Hbf
22:30   8
RB30   - Fährt heut
        Hohenstein   g-B. Süd
22:31   9
RB30   Flöha - Zsc
22:36   5
RB80
        rt heute von   Hbf
22:36   14
B45   Geithain - B
2:44   Einsiedel - Thalheim (Erzgeb)   Aue (Sachs)
E6   11
2:45   Flöha - Freiberg (Sachs) - Tharandt   Dresden Hbf
89
:30   Flöha - Freiberg (Sachs)
        Fährt heute von Gleis 11 -

BMG | MIS

Ooops, your files have been encrypted!

Was geschieht mit meinem Computer?

Kann ich meine Dateien wiederherstellen?

Wie bezahle ich?

Payment will be raised on
Time Left

Your files will be lost on
Time Left

Send $300 worth of bitcoin to this address

Check Payment   Decrypt

ancock
Regional Hospital

MAIN ENTRANCE
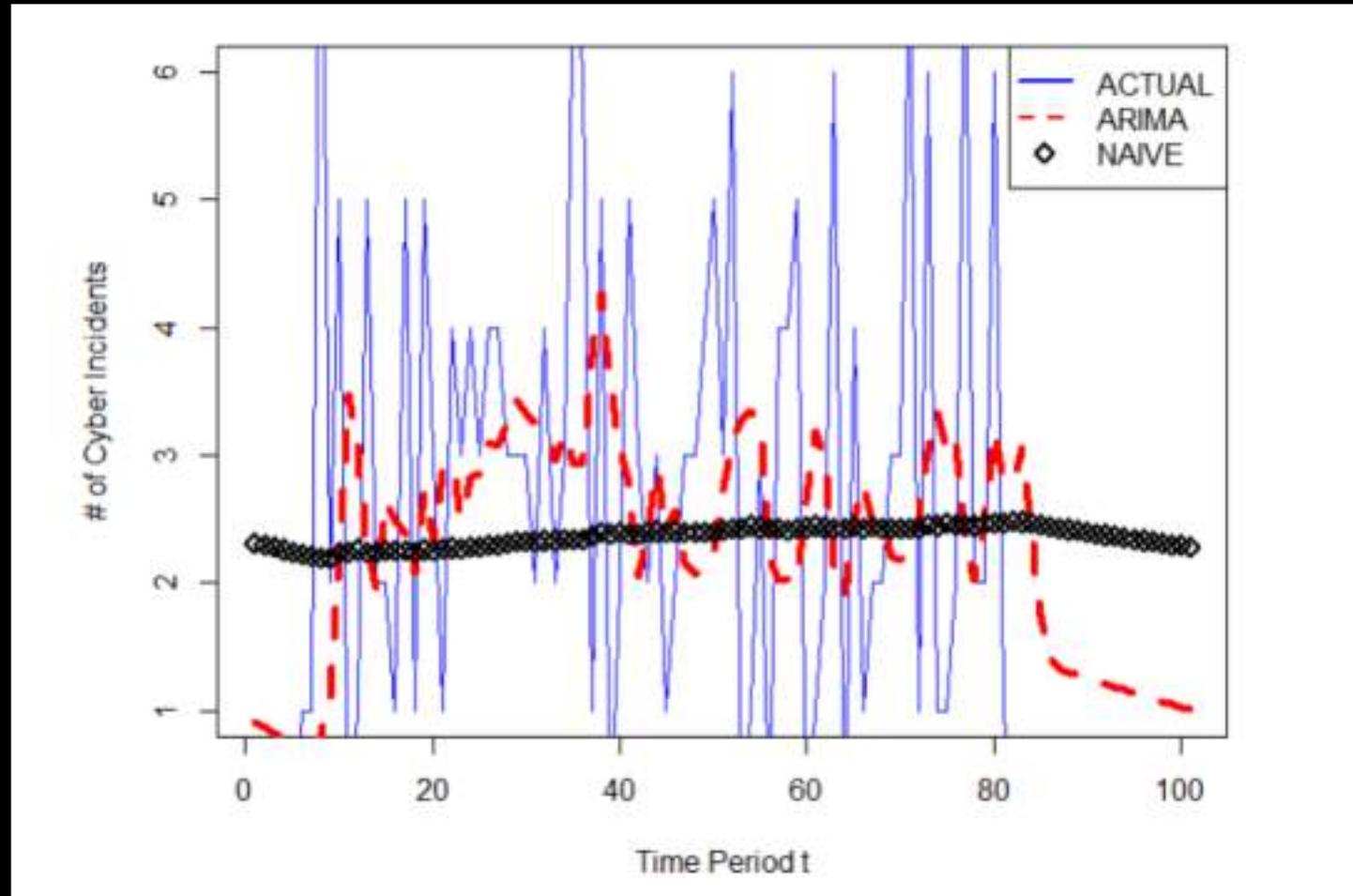Patient Registration
Visitor Entrance

8 MALWARE ATTACK SHUTS DOWN COMPUTER
NETWORK AT HANCOCK REGIONAL HOSPITAL

The Frequency of Cyber Attacks Are Increasing

What do we do?

- It is important to build infrastructure that is resilient to cyberwarfare.
- As developers, we must build our systems with free software.
- For everyone else, we must use free software.

Free Software > Open Source Software > Proprietary Software

Closed Source Vs Open Source

Free Software ≠ Open Source Software

- The freedom to run the program as you wish, for any purpose
- The freedom to redistribute copies so you can help your neighbor.
- The freedom to study how the program works, and change it so it does your computing as you wish.
- The freedom to distribute copies of your modified versions to others.

Linus' Law

"Given enough eyeballs, all bugs are shallow"

Types of Attacks That Don't Need Source Code
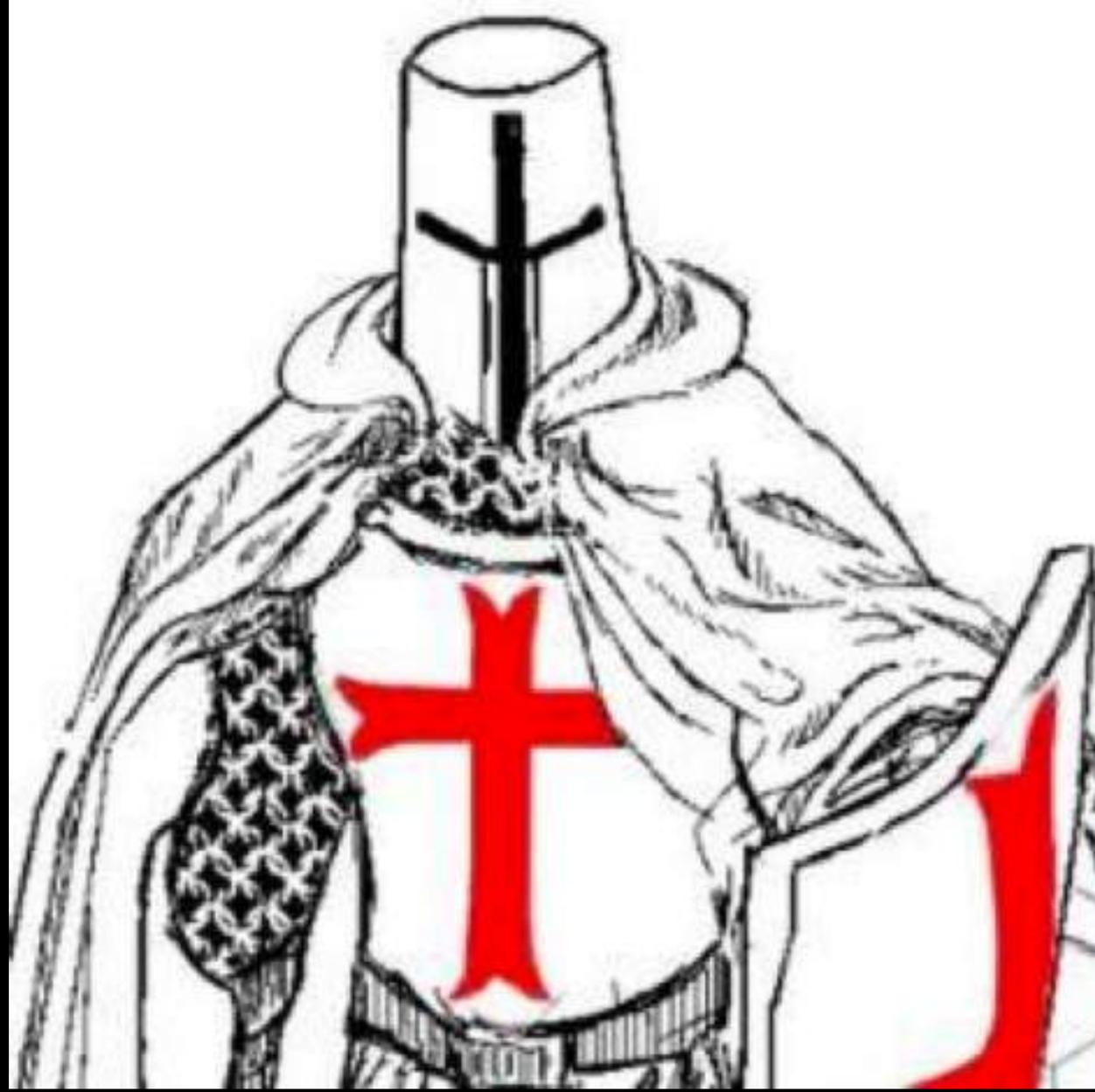
- Binary Analysis.
- Dynamic Attacks.
- Code Injection.

Open Source Hardening Project

MalwareMustDie

Monoculture Effect

THE IRISH FAMINE—SCENE AT THE GATE OF THE WORK-HOUSE.

Phytophthora infestans
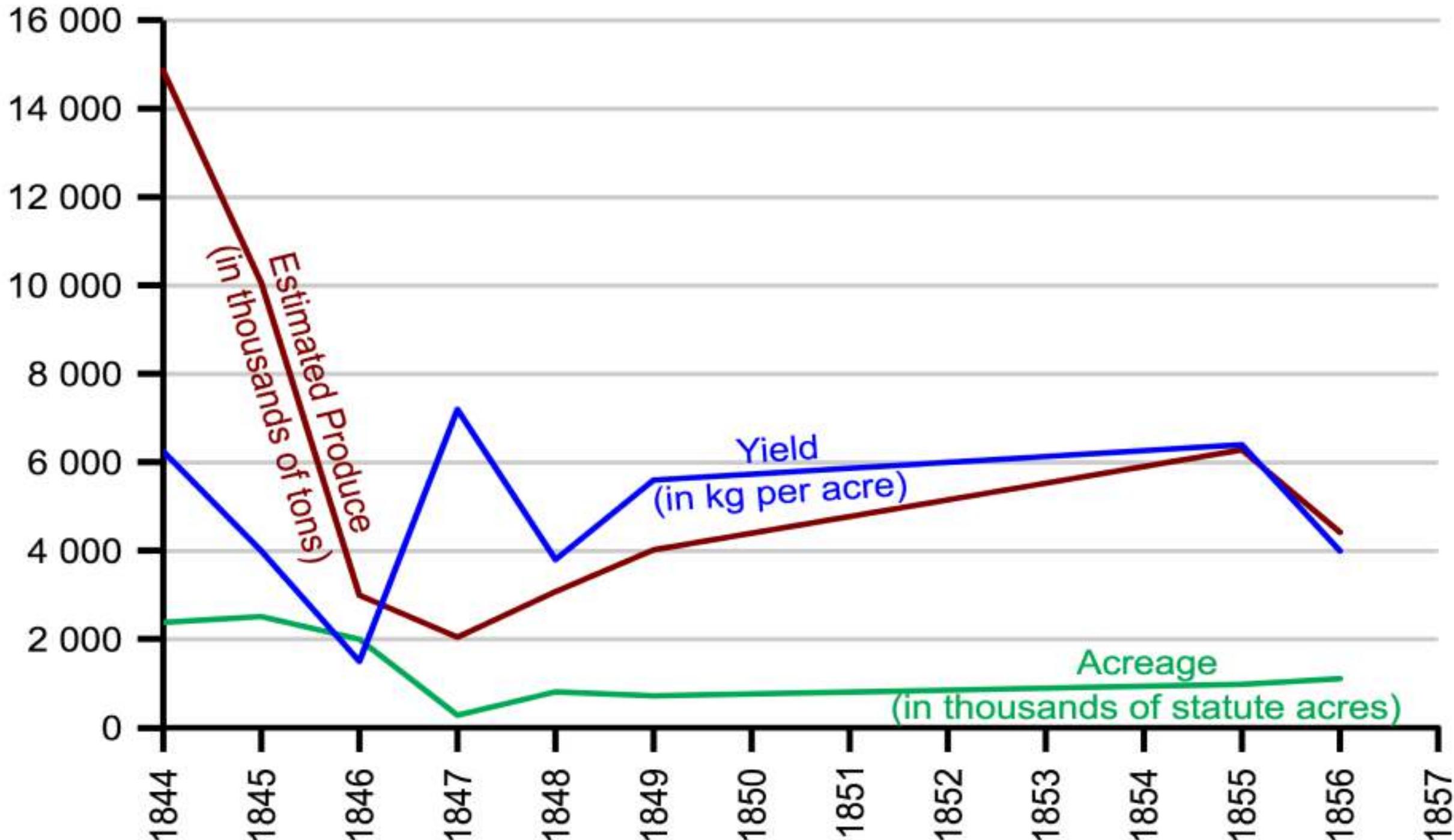
ETERNALBLUE
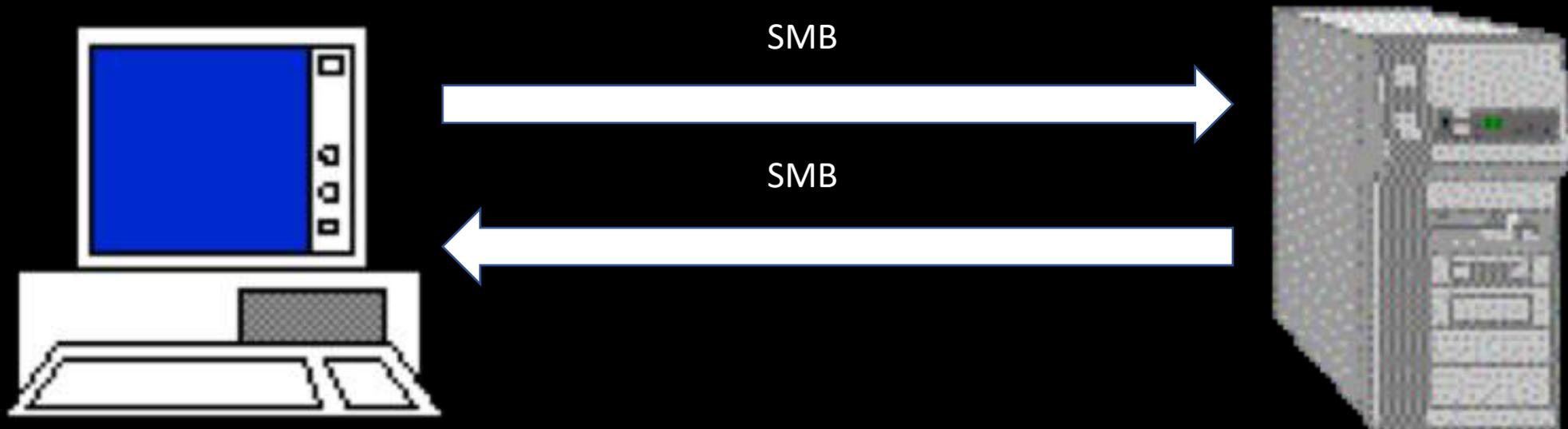
Operating Systems by Usage

Windows Mac OSX Linux Other

https://www.statista.com/statistics/218089/global-market-share-of-windows-7/#0

redhat MEPIS turbolinux LUNAR EvilEntity debian Vine Linux cAos/CentOS MiniKazit UTUTO

archlinux monowall jamd Knoppix STD gentoo linux DeLi Linux Hiweed amlug slackware yellow dog linux

Fedora LPG PLD SLAX COREL LINUX Progeny GeeXBox BIGLINUX FREEDUC Lycoris

EnGarde Mandrakelinux BeatrIX Linspire suse 中文延伸套件 YOPER BearOps ASPLINUX kalango

Slackintosh Frugalware Foresight Mint PCLinuxOS ubuntu JULEX blag

Which Linux based OS should I go for?

Who are you?

Business Person | **Hobbyist** | **Normal User** | **Graphic Designer** | **Developer/Programmer**

Business Person
1. OpenSUSE
2. Fedora
3. Debian

Hobbyist

Geek?

Yes → Ever tried Arch?

- **No**
  1. Gentoo
  2. Centos
  3. Debian
  4. Slackware

- **Yes** → Which of the following distro have you used before?

  - **Ubuntu** → Linux Mint
    1. Linux Mint
    2. Ubuntu Mate
    3. Kubuntu
    4. Elementary OS

  - **Linux Mint**
    1. Ubuntu
    2. Kubuntu
    3. Fedora
    3. Manjaro

  - **Fedora** → Manjaro
    1. Apricity OS
    2. Ubuntu
    3. Antergos
    4. Fedora

No → Ever used Linux based OS before?

Normal User

Ever used Linux based OS before?

- **Yes**
  1. Kubuntu
  2. Linux Mint
  3. Apricity OS

- **No** → Where have you come from?

  - **Windows**
    1. Ubuntu
    2. Elementary OS

  - **Mac**
    1. Ubuntu
    2. Ubuntu Gnome
    3. Kubuntu
    4. Linux Mint

Graphic Designer

I want to get things done and get going.
1. Ubuntu
2. Linux Mint
3. Ubuntu Mate
4. OpenSUSE

Developer/Programmer

I like to tweak and configure my OS.
1. Arch Linux
2. Manjaro
3. Antergos
4. Apricity OS

I want to perform penetration testing.
1. KALI Linux
2. Arch Linux

This infographic relies on current trends and personal experience of the author. | Created by Ahmed Noor at Anixel Studio, 2016

Vulnerability Patching

⊙ Watch ▾ | 2,616 | ★ Star | 38,945 | ⑂ Fork | 15,762

⟨⟩ Code   ⊙ Issues 352   ⑄ Pull requests 713   ▥ Projects 0   ┟ Insights

👋 Want to submit an issue to rails/rails?   **Dismiss**

If you have a bug or an idea, read the contributing guidelines before opening an issue.

Filters ▾   🔍 is:issue is:open   Labels   Milestones   **New Issue**

ⓘ **352 Open**   ✓ **10,835 Closed**   Author ▾   Labels ▾   Projects ▾   Milestones ▾   Assignee ▾   Sort ▾

ⓘ   **Cannot copy/paste master.key from password manager**
     #32245 opened 4 hours ago by NetBzz

ⓘ   **Activestorage: S3 presigned url get expired before access.**   💬 1
     #32236 opened 16 hours ago by vsingh-cts

ⓘ   **Rails.logger.reopen does not work because the @logdev does not know it's @filename**   💬 5
     #32211 opened 5 days ago by grosser

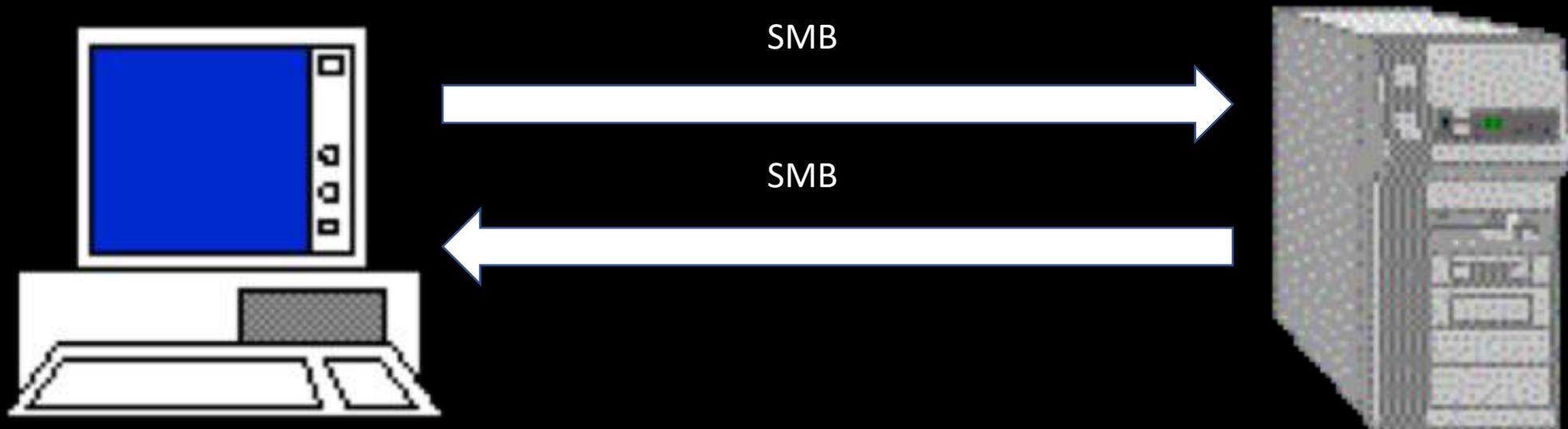
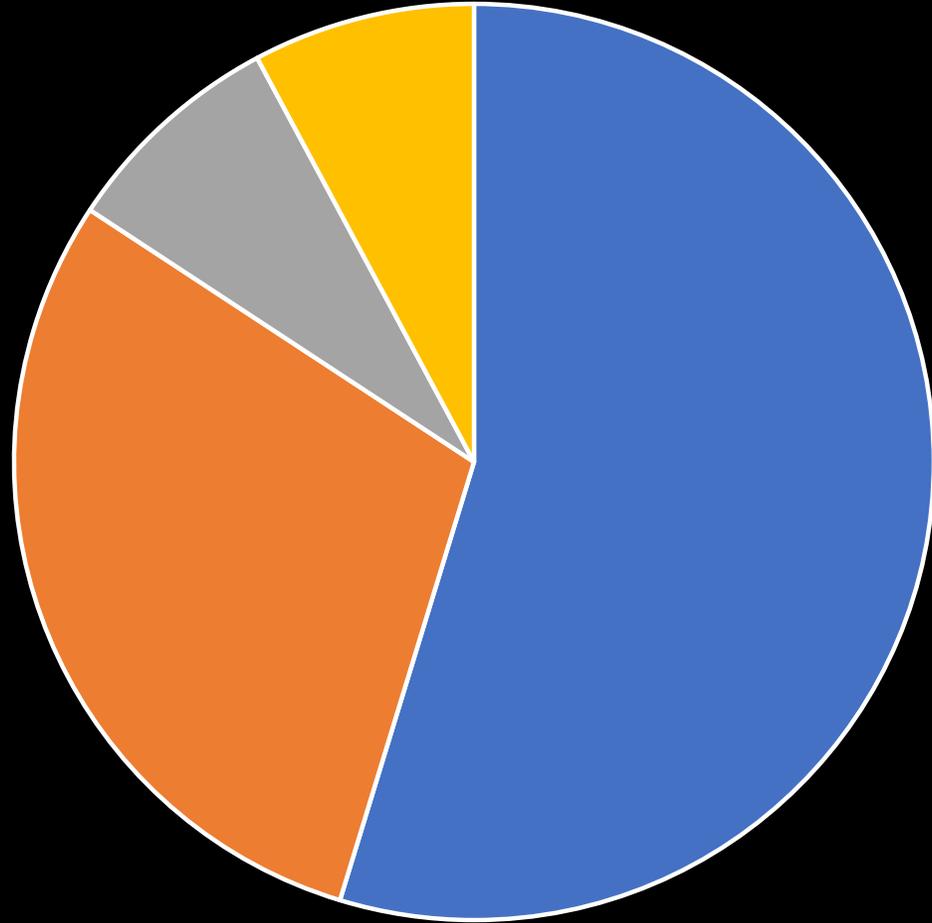ⓘ   **Make ActiveStorage work for API only apps** `activestorage`
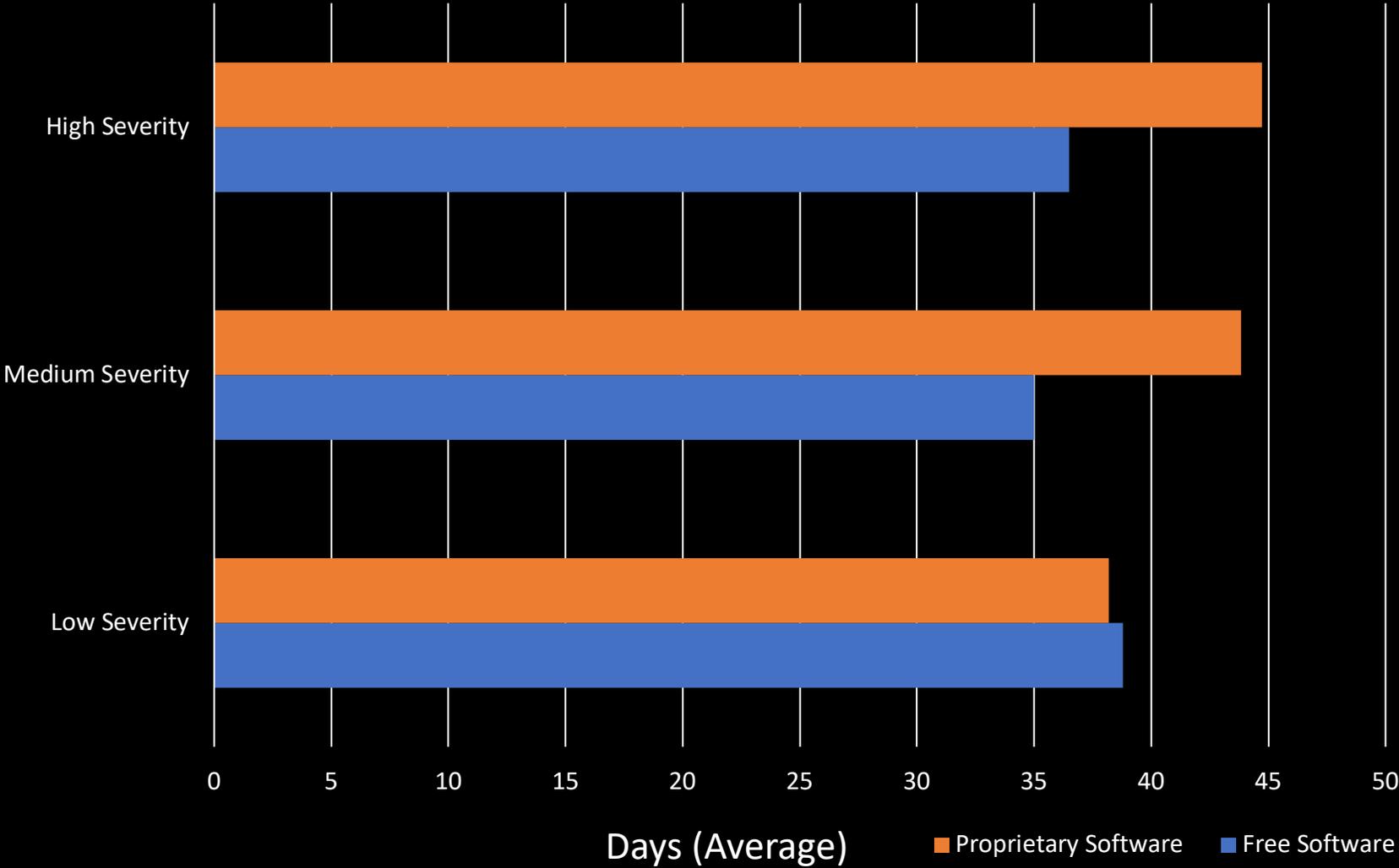   #32208 opened 5 days ago by hector

ETERNALBLUE

Percentage of Usage

Windows 7   Windows 10   Windows XP   Windows 8.1

Source: NetMarketShare

Vulnerability Patching Time by Severity

Source: Vulnerabilities and Patches of Open Source Software: An Empirical Study
Kemal Altinkemer, Jackie Rees, and Sanjay Sridhar
Purdue University

- By opening up the source code, vulnerabilities are easier to find. And overall, this makes the code more secure.
- The monocultural effect of proprietary software provides less defense against widespread virus attacks.
- And free software vendors, on average, outperform patching time than proprietary software. Additionally, they have only technical merits dictating whether a vulnerability gets patched.
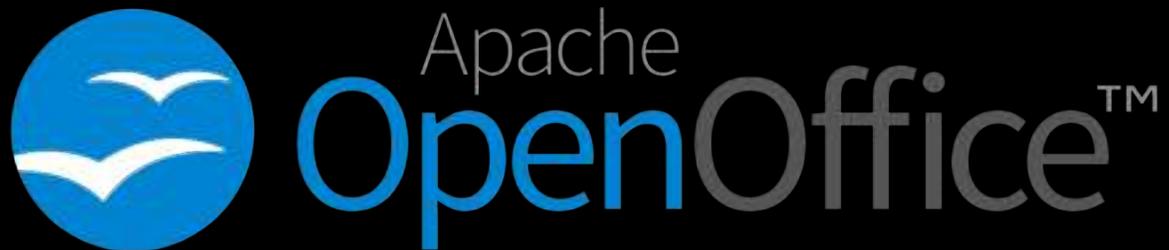
Low Vulnerability		Medium Vulnerability		High Vulnerability		Sum	
OpenOffice	MS Office	OpenOffice	MS Office	OpenOffice	MS Office	OpenOffice	MS Office
2	3	6	50	8	55	16	108

Source: Open Source VS Closed Source Software: Towards Measuring Security
Guido Schryen, Rouven Kadura
International Computer Science Institute, Berkeley, CA
RWTH Aachen University, Aachen, Germany

	Debian	OpenBSD	Solaris
Security Features Score	6.42	7.09	5.92
Vulnerabilities Score	7.72	4.19	7.74
Final Score	-1.0	10.2	-3.5

Source: On The Security of Open Source Software
Christian Payne
Murdoch University
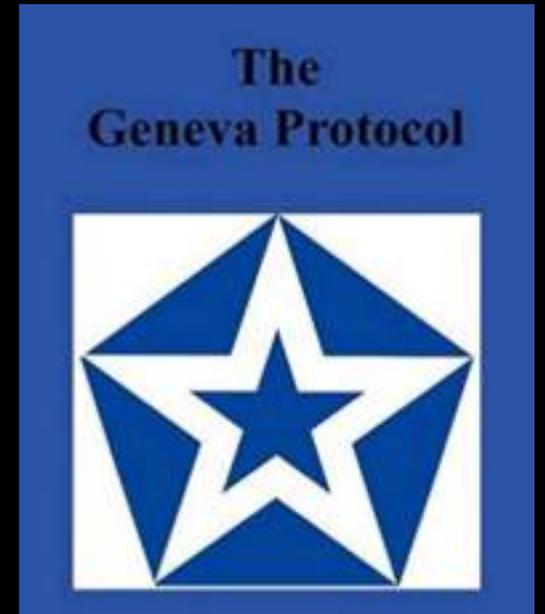
Free Software Is Not the End All Be All!

- High development standards must be used.

- Vulnerabilities will be found in free and proprietary software.

- Source code of critical systems must be audited by individuals with the necessary credentials.

Building Resiliency

A World Without Cyberwarfare

Going forward

- We must advocate for free software in our workplaces and institutions.
- Developers must hold ourselves to high standards of code quality and security.
- Developers should use free software when building applications.
- We must advocate for comprehensive treaties on Cyberwarfare.

Questions?