black hat ASIA 2020
OCTOBER 1-2, 2020
BRIEFINGS

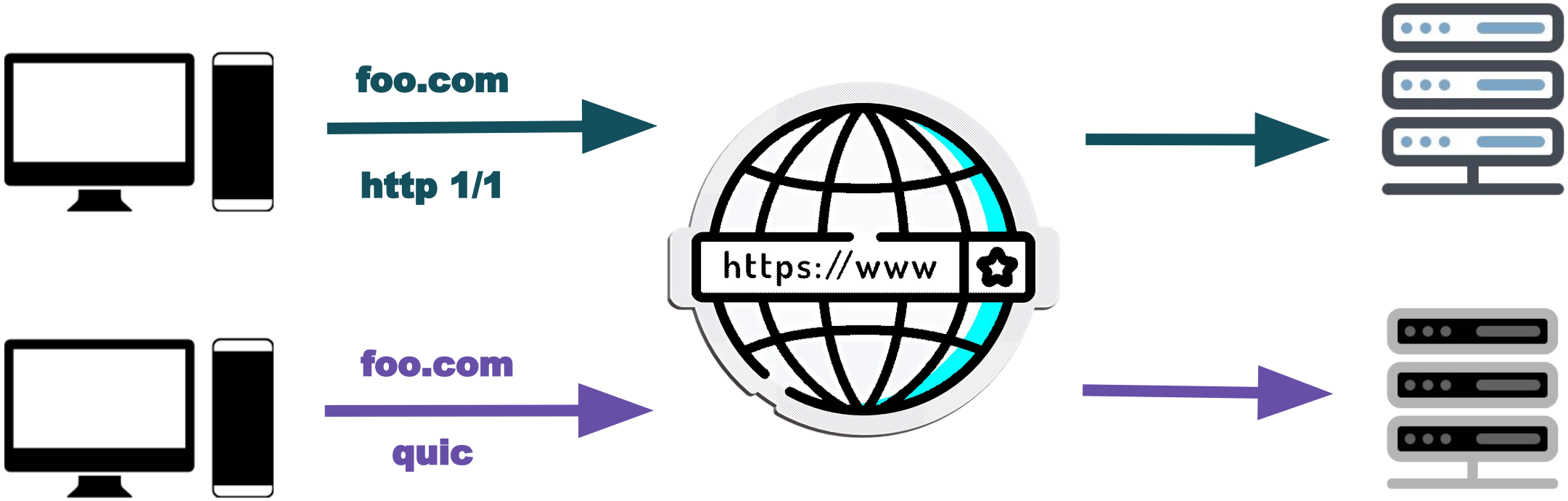
The Evil Alt-Ego: (ab) using HTTP Alternative Services

Trishita Tiwari,
@fork_while_1

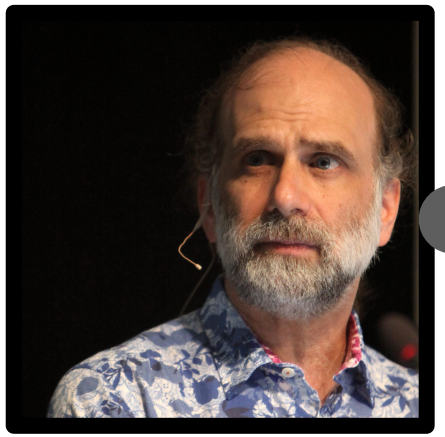
Ari Trachtenberg,
people.bu.edu/trachten/

David Starobinski
people.bu.edu/staro/

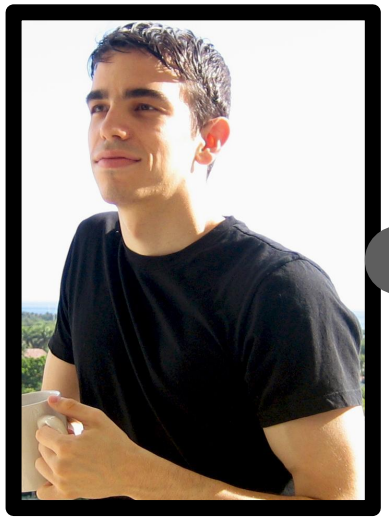
Your Mission

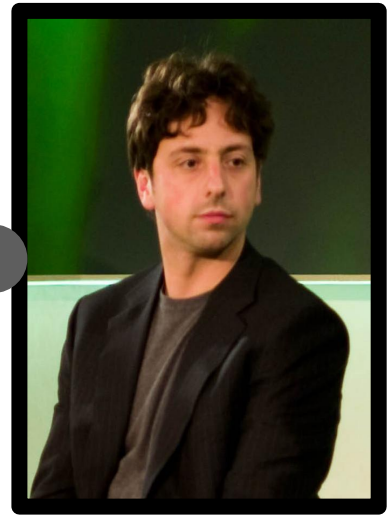


New Design File, Icons8, Kiss Clip Art



Your Team





Can you do it ???

HTTP to the rescue ...

HTTP

- **HTTP/1.0 in 1996**
- **Simple headers:**
  - **Hostname**
  - **Referer**
  - **User-Agent**

[Docs] [txt|pdf] [draft-ietf-http...] [Tracker] [Diff1] [Diff2]

INFORMATIONAL

Network Working Group — T. Berners-Lee
Request for Comments: 1945 — MIT/LCS
Category: Informational — R. Fielding
UC Irvine
H. Frystyk
MIT/LCS
May 1996

Hypertext Transfer Protocol -- HTTP/1.0

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Iconlibrary

HTTP

- **HTTP additions:**
  - **Caching**
  - **Dynamic content**
  - **Request multiplexing**

- **Result:**

More papers for security researchers!!!

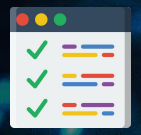
Iconlibrary

HTTP

- **HTTP is 23 yrs old this year (feel old yet?)**

- **Still hard to introduce secure protocol updates.**

Iconlibrary



The Alt-Svc

Welcome to *Alternative* Services (RFC 7838)

- Yet another HTTP header!!
- Allows website to specify equivalent alternate endpoint

Flaticon

The Alt-Svc

https://original.com/

New Design File, Icons8, Flaticon

The Alt-Svc

https://original.com/

New Design File, Icons8, Flaticon

The Alt-Svc

New Design File, Icons8, Flaticon

The Alt-Svc

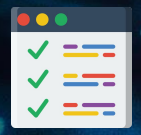
New Design File, Icons8, Flaticon

The Alt-Svc

New Design File, Icons8, Flaticon, Freeiconshop

The Alt-Svc

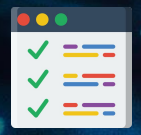
New Design File, Icons8, Flaticon, Freeiconshop



Alt-Svc Format

Alt-Svc: 'h2="www.google.com:123"; ma=123456'

Flaticon



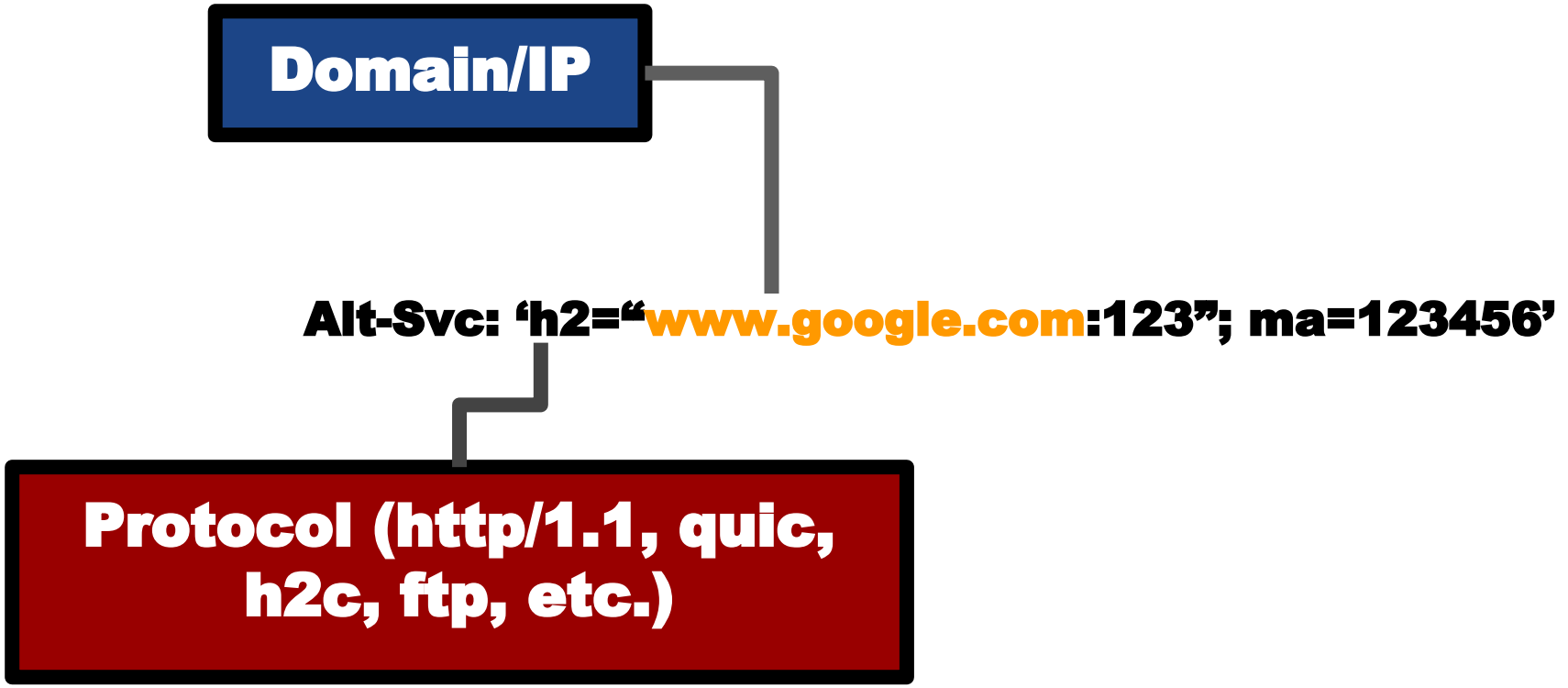
Alt-Svc Format

Alt-Svc: ‘h2=“www.google.com:123”; ma=123456’

Protocol (http/1.1, quic, h2c, ftp, etc.)

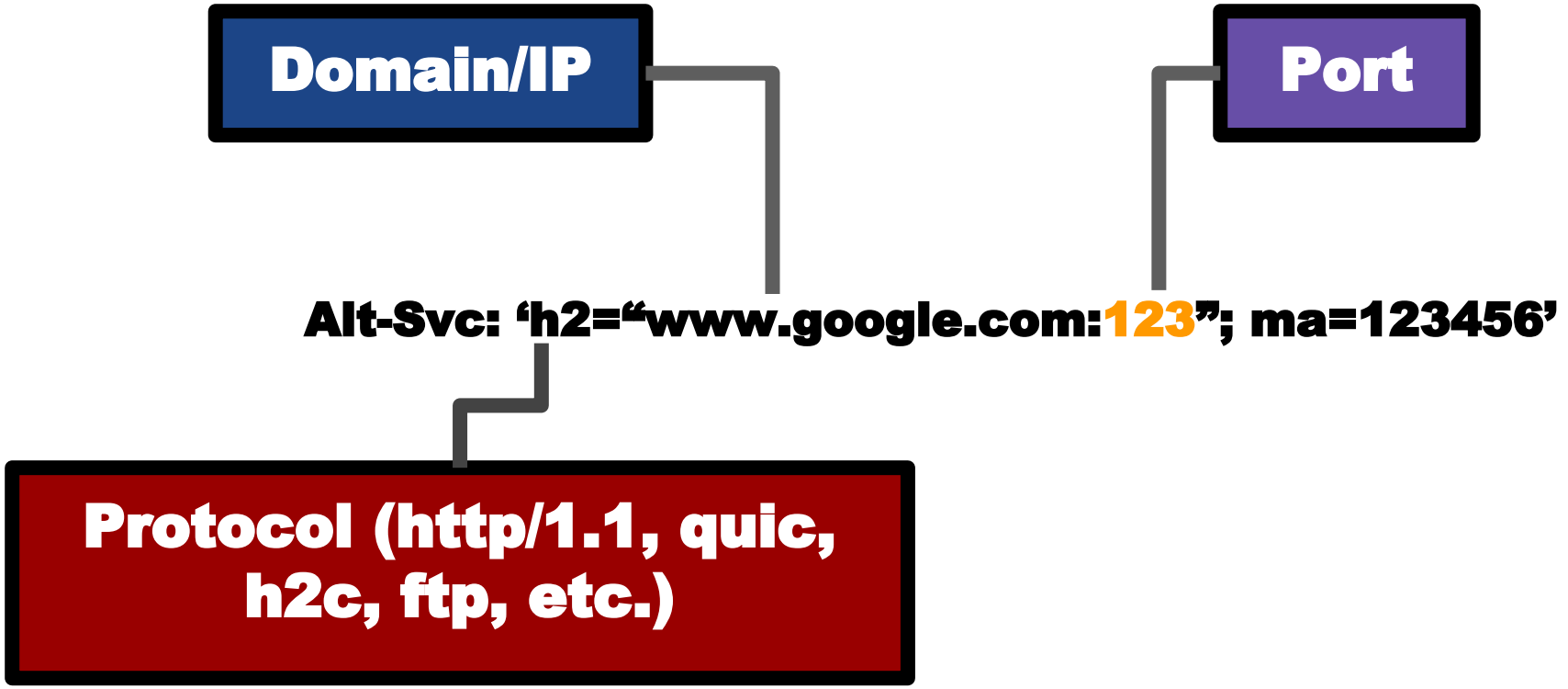
Flaticon

Alt-Svc Format



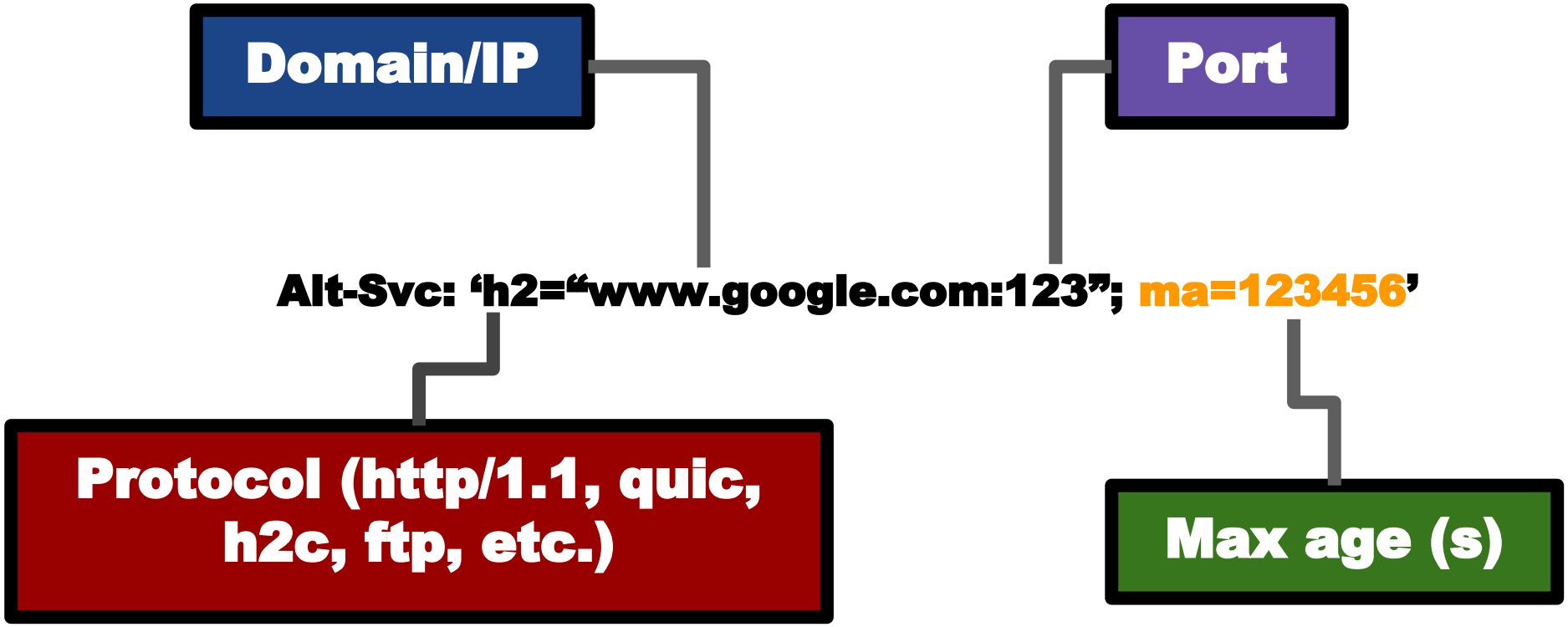
Flaticon

Alt-Svc Format

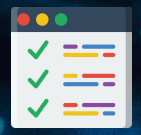


Flaticon

Alt-Svc Format



Flaticon



Alt-Svc Uses

- **Load balancing**
- **Client segmentation**
- **Advertising endpoints with new protocols**

Flaticon

Overview of abuse

Port Scan (CVE 2019-11728)

- **Alt-Svc Abuses**

Flaticon

Overview of abuse

Port Scan (CVE 2019-11728)

DDoS

Alt-Svc Abuses

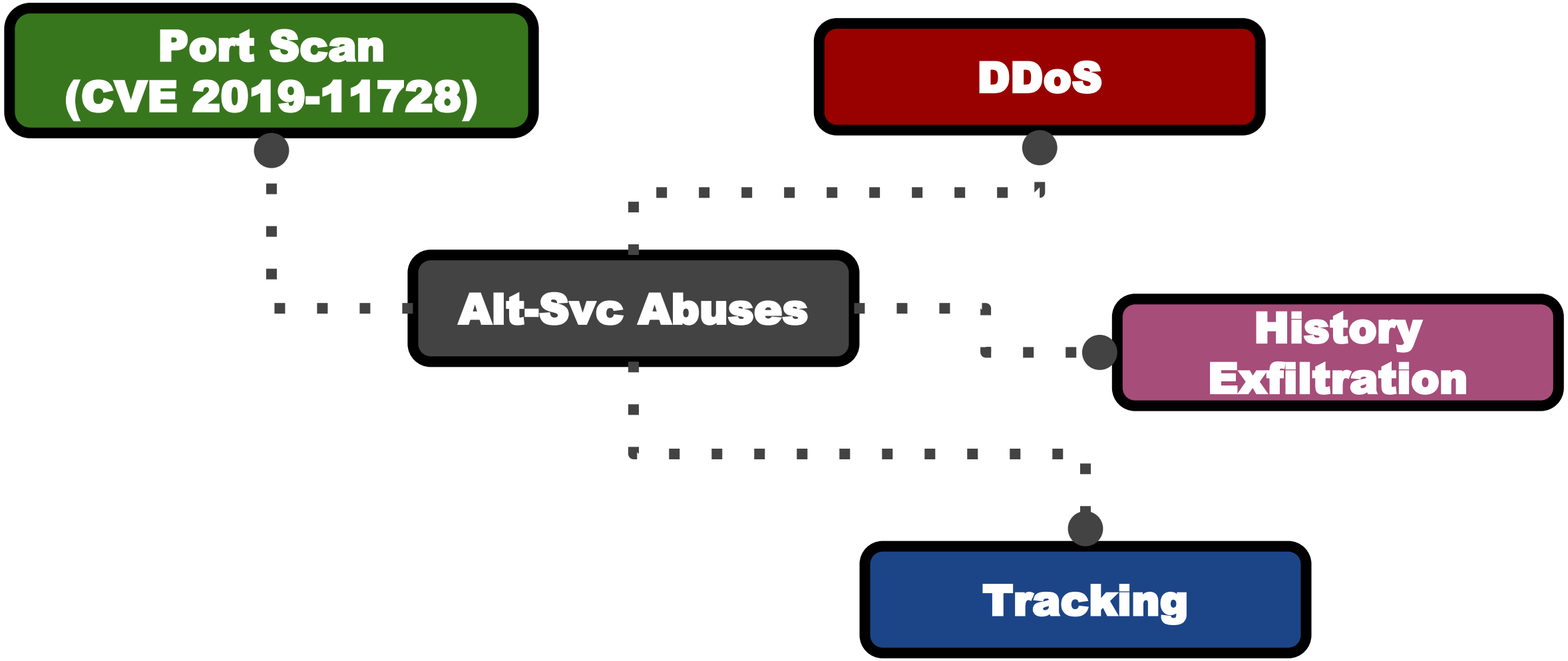
Flaticon

Overview of abuse

- Port Scan (CVE 2019-11728)
- DDoS
- Alt-Svc Abuses
- History Exfiltration

Flaticon

Overview of abuse



Flaticon

Overview of abuse

- Port Scan (CVE 2019-11728)
- DDoS
- Alt-Svc Abuses
- History Exfiltration
- Malware protection bypass
- Tracking

Flaticon

Threat Model

- **Case 1:**
  - **Attacker controls website(s)**
- **Case 2:**
  - **Attacker controls website(s)**
  - **Monitors victim network traffic**
    - ***e.g.* Cafe/Airport WiFi**

Sandstein / CC BY (https://creativecommons.org/licenses/by/3.0)

Flaticon

Threat Model

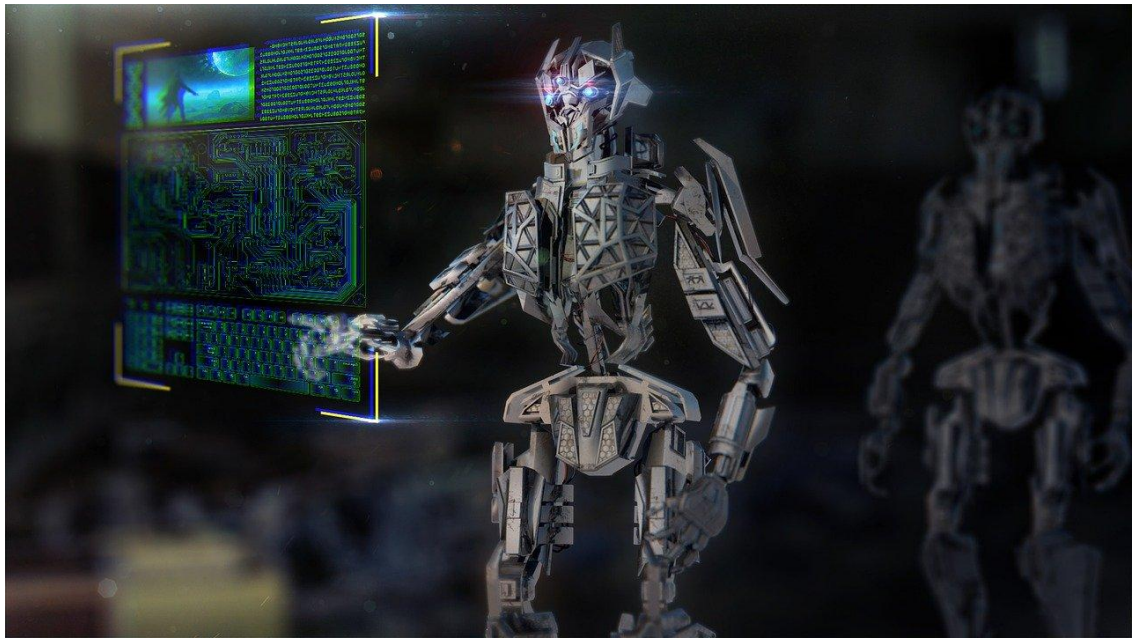
- **Case 1:**
  - Attacker controls website(s)

- **Case 2:**
  - Attacker controls website(s)
  - Monitors victim network traffic
    - *e.g.* Cafe/Airport WiFi

Flaticon

Why is this so bad?

- Operates below the browser level
  - not visible to victim
  - not visible to JavaScript detection
- + No user interaction needed
- + Mountable via third-party web



Flaticon

Overview of abuse

- Port Scan (CVE 2019-11728)
- DDoS
- Alt-Svc Abuses
- History Exfiltration
- Malware protection bypass
- Tracking

Flaticon

Port Scan (CVE-2019-11728)

- (Distributed) port scanning (from browser context).

Flaticon

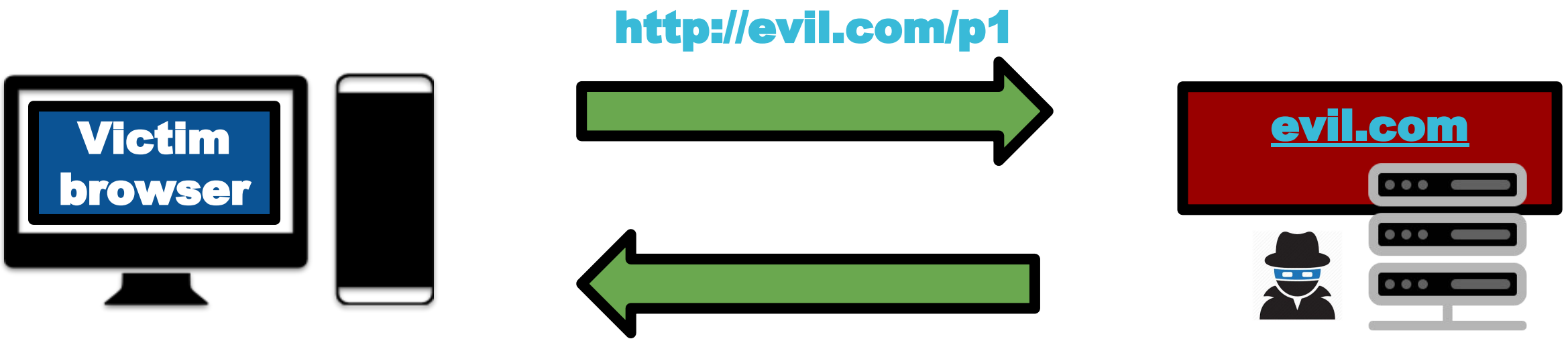
Port Scan (CVE-2019-11728)

- (Distributed) port scanning (from browser context).

New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)

- (Distributed) port scanning (from browser context).



New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)

Alt-Svc: localhost:25

New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)

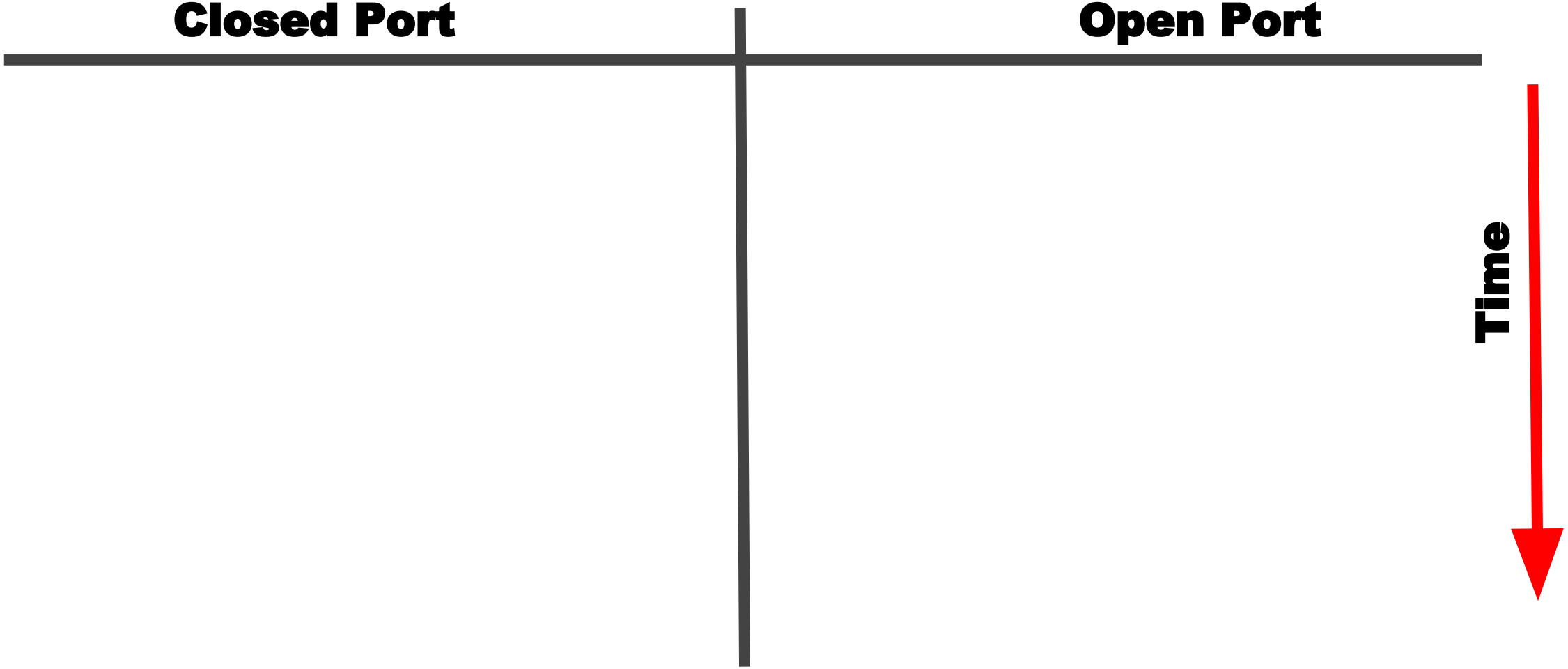
Alt-Svc: localhost:25

Open?

Closed?

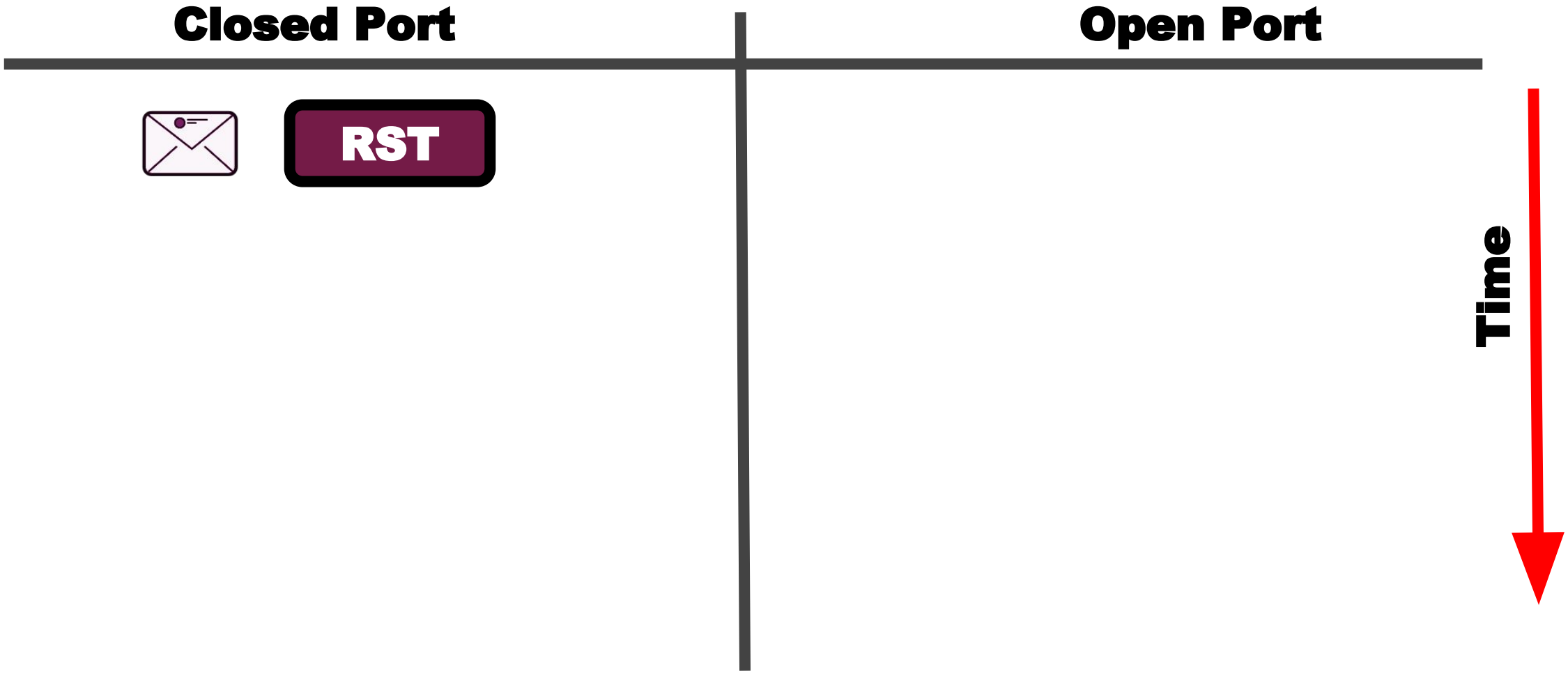
New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)



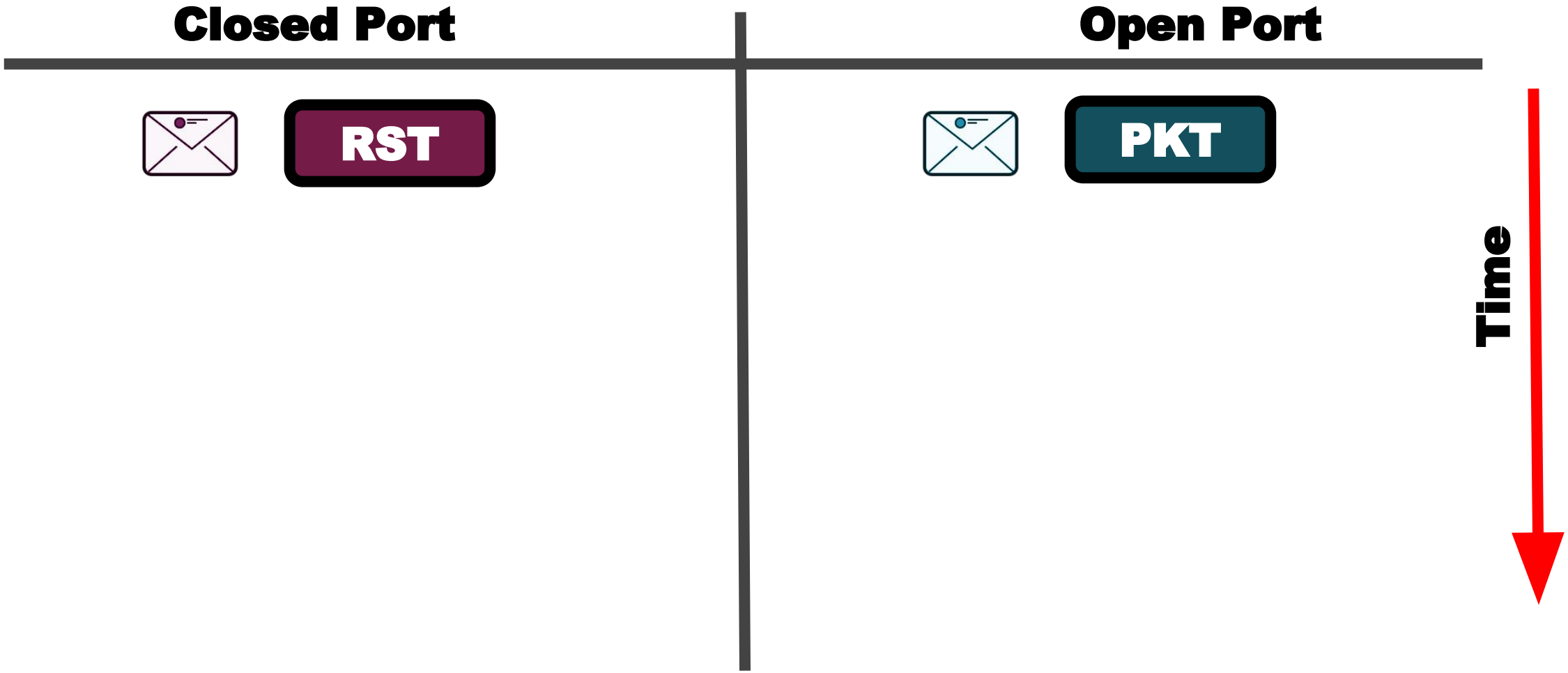
Flaticon

Port Scan (CVE-2019-11728)



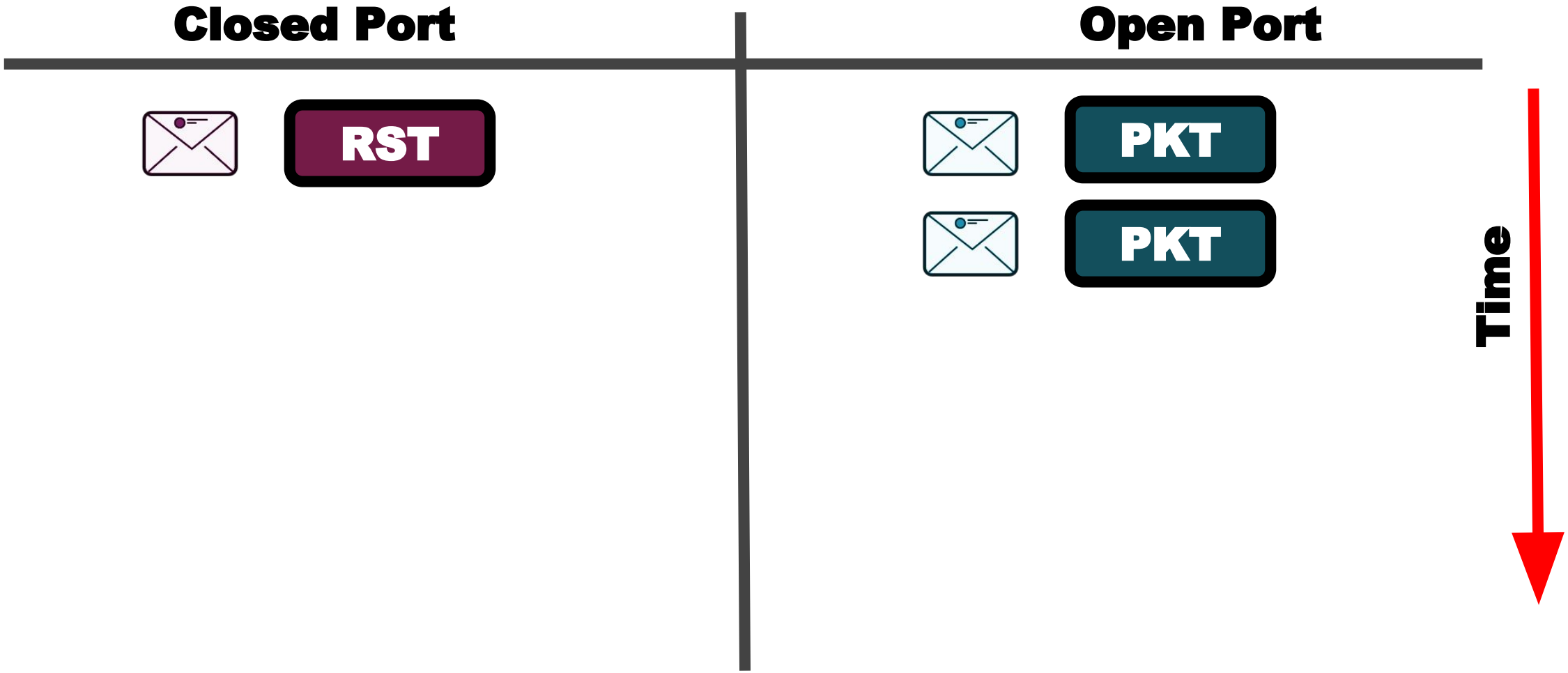
Icons8, Flaticon

Port Scan (CVE-2019-11728)



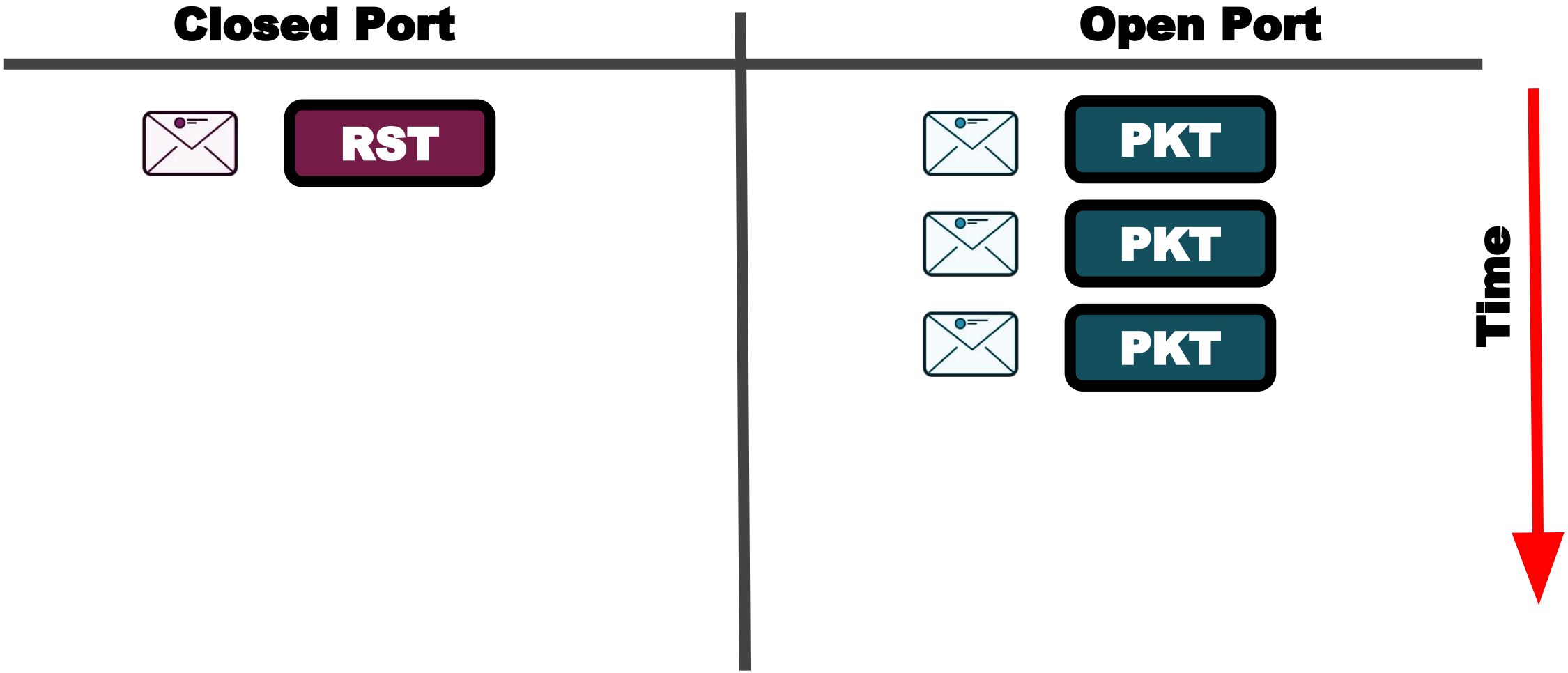
Icons8, Flaticon

Port Scan (CVE-2019-11728)



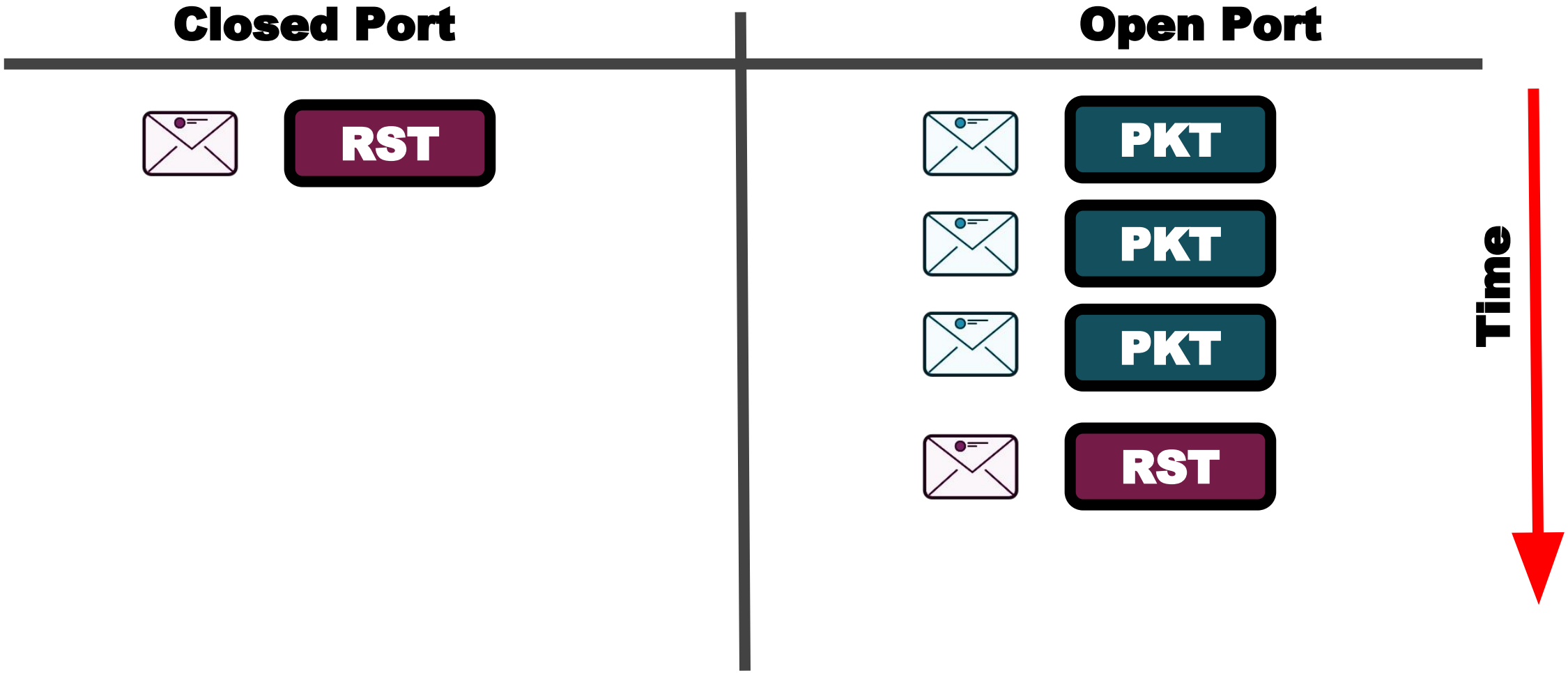
Icons8, Flaticon

Port Scan (CVE-2019-11728)



Icons8, Flaticon

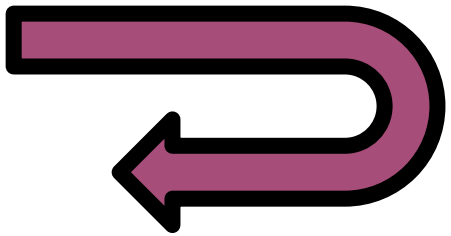
Port Scan (CVE-2019-11728)



Icons8, Flaticon

Port Scan (CVE-2019-11728)

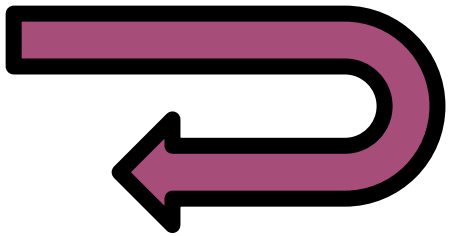
Victim's browser knows status of localhost:25



New Design File, Icons8, Pngio, Flaticon

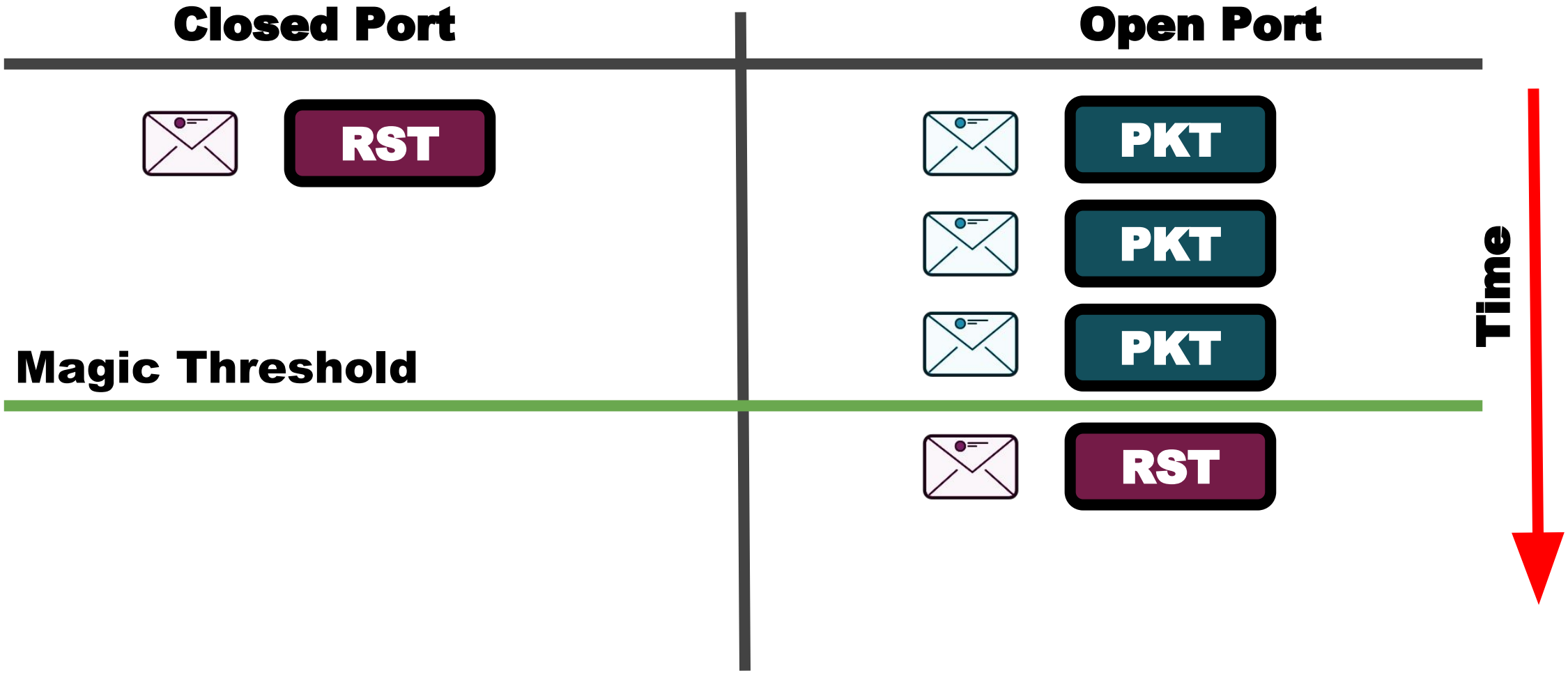
Port Scan (CVE-2019-11728)

Victim's browser knows status of localhost:25



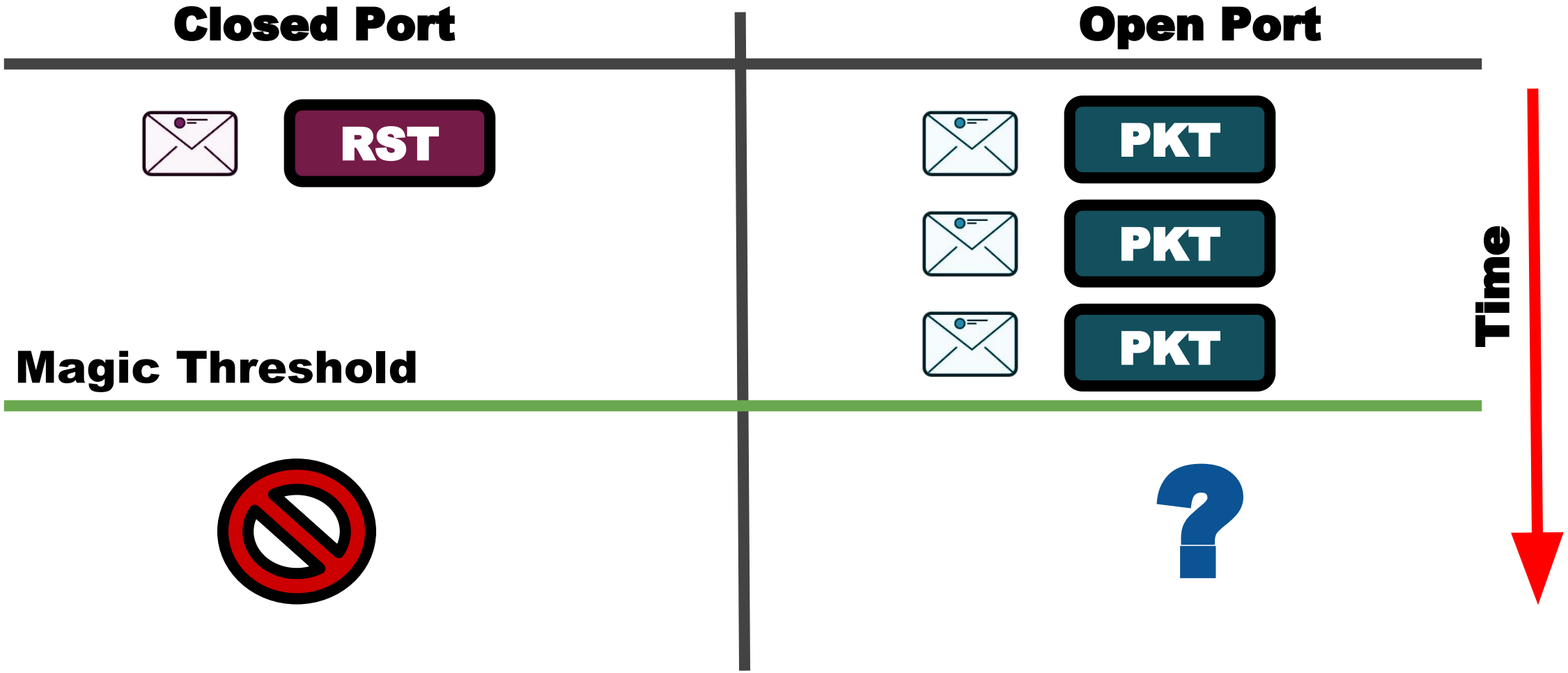
New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)



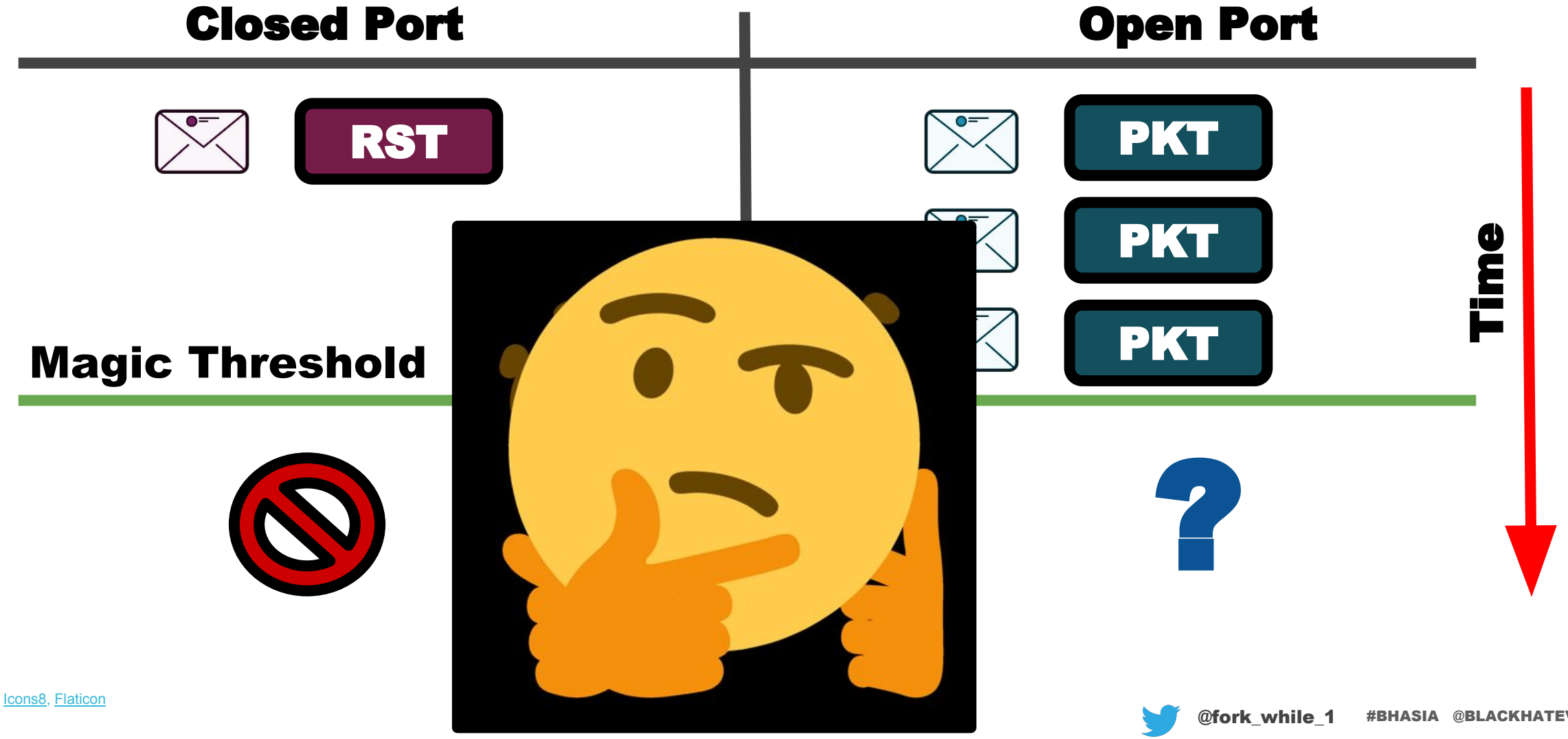
Icons8, Flaticon

Port Scan (CVE-2019-11728)



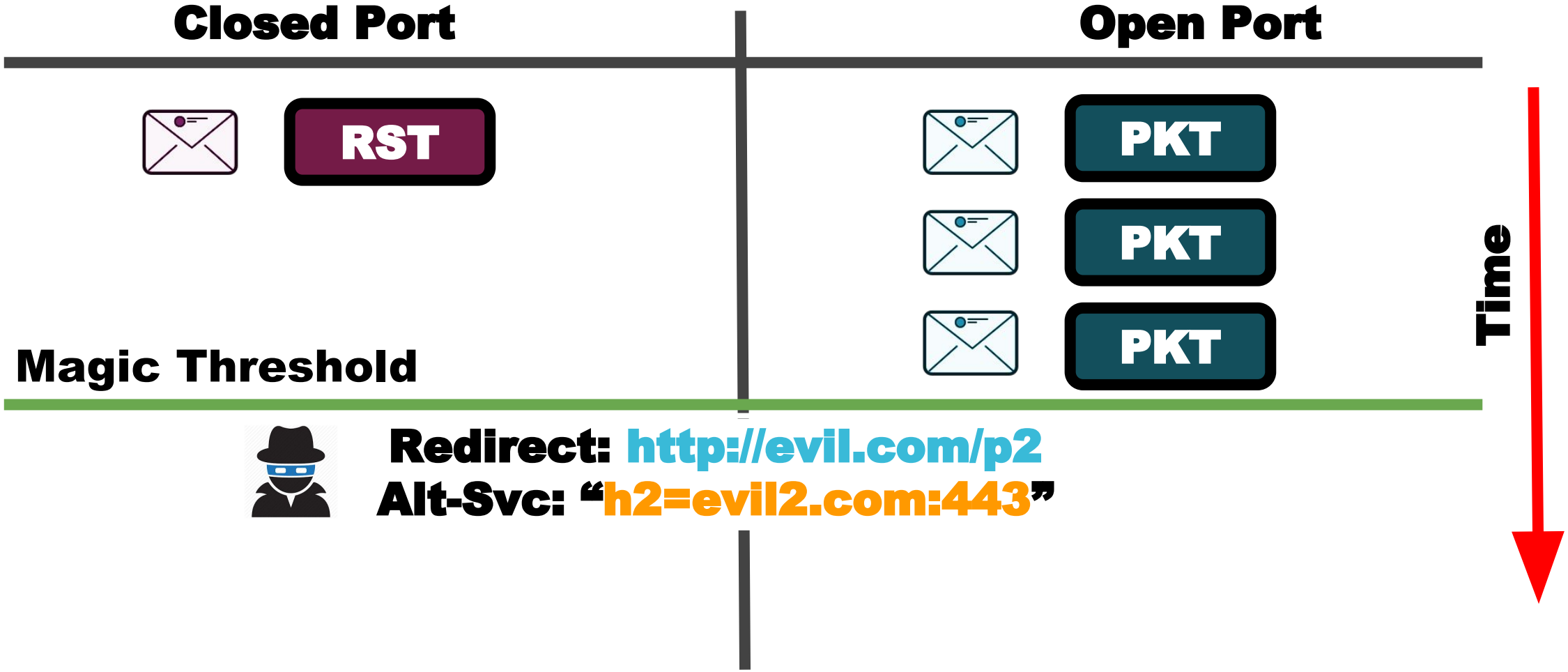
Icons8, Flaticon

Port Scan (CVE-2019-11728)



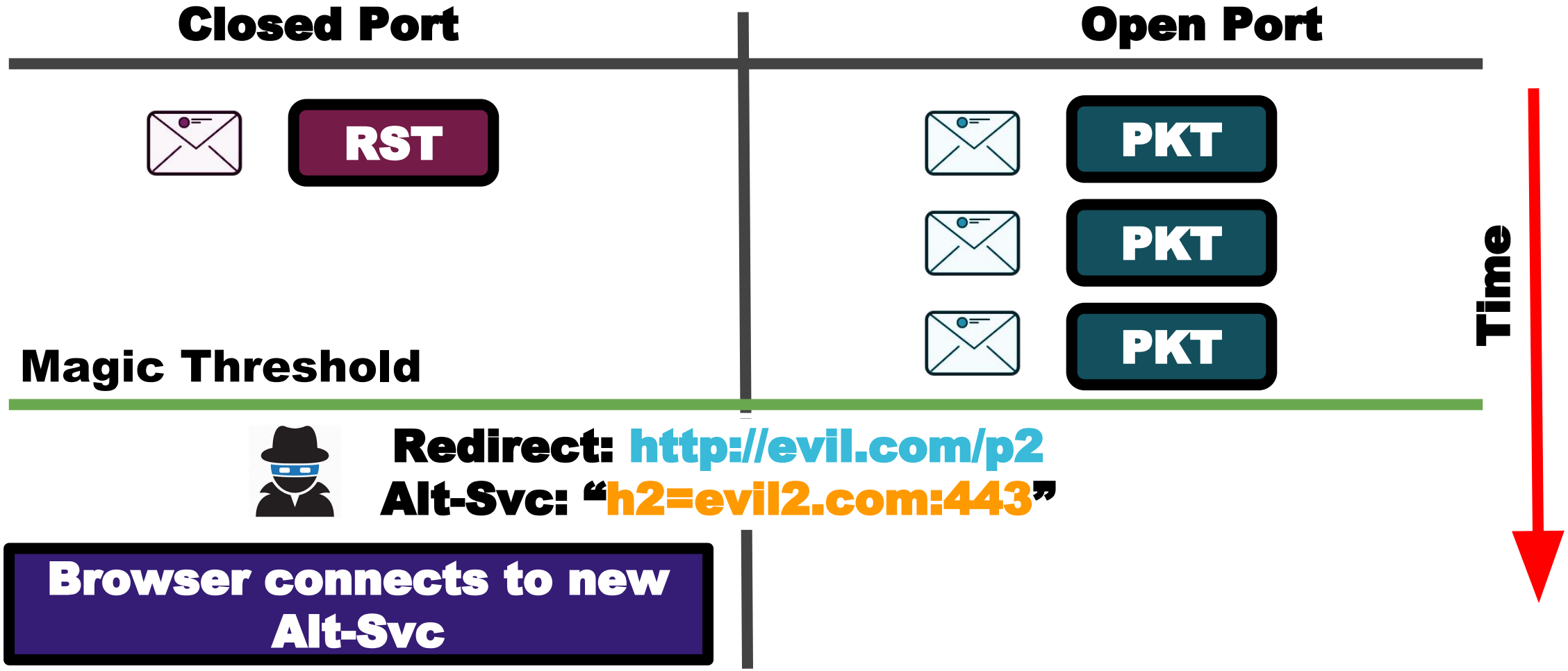
Icons8, Flaticon

Port Scan (CVE-2019-11728)



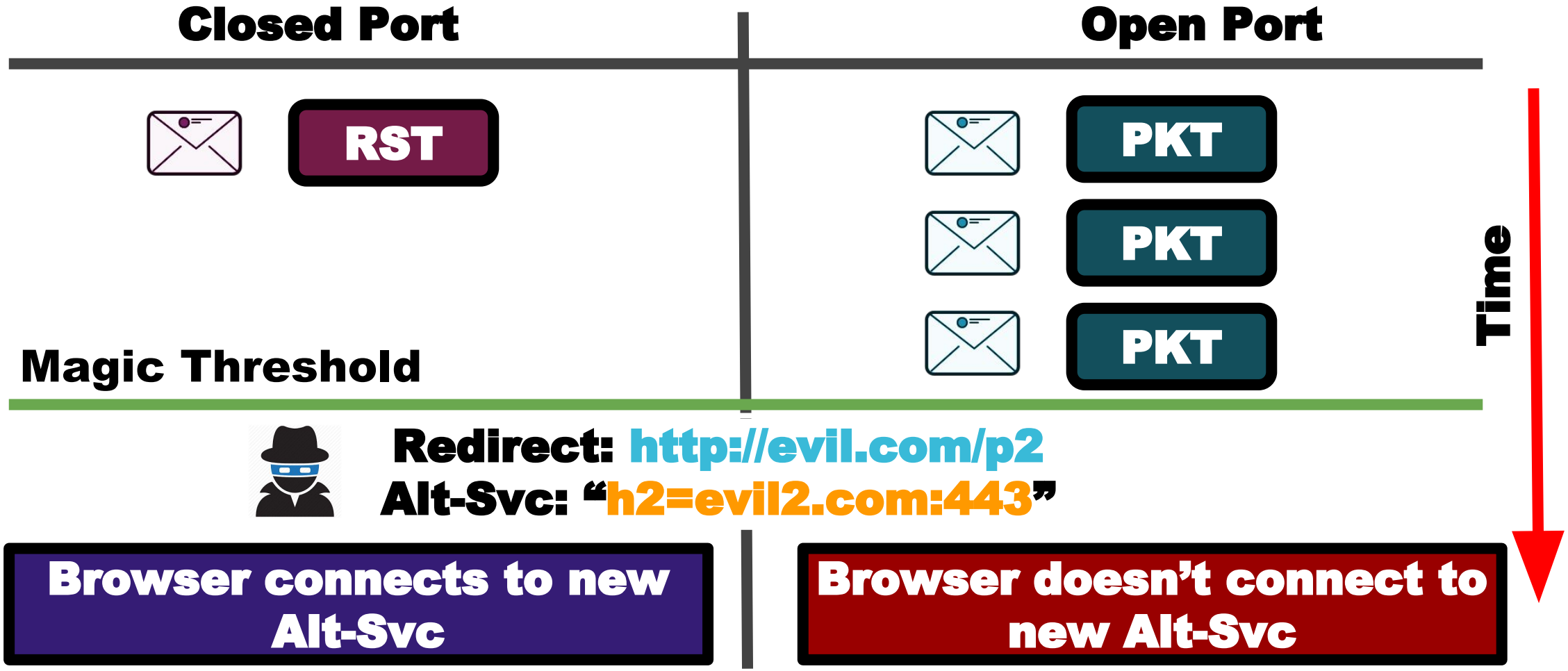
Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)



Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)

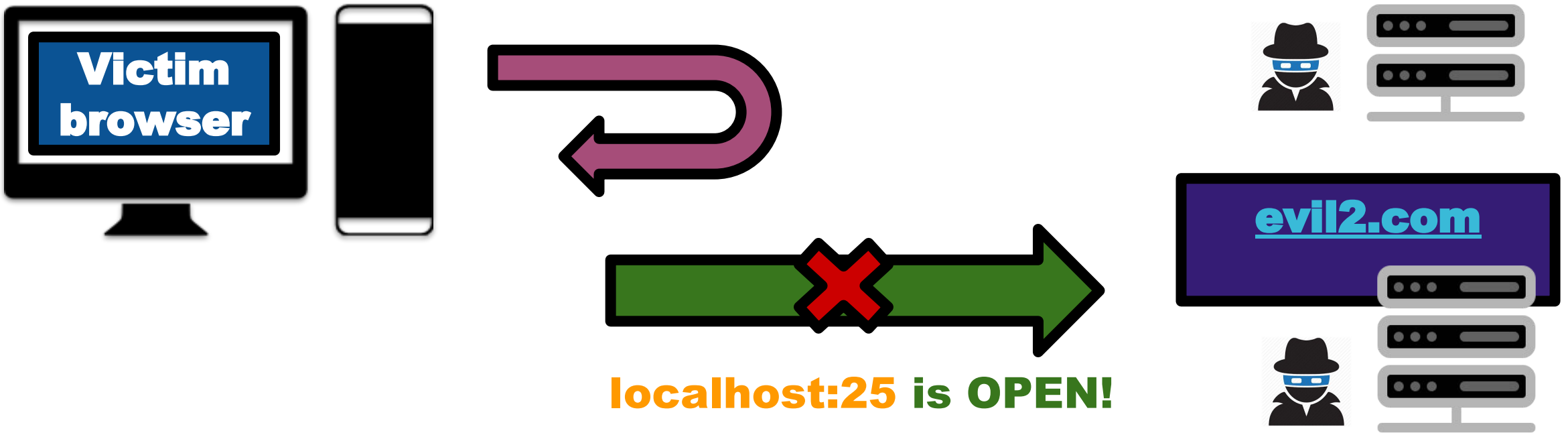


Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)

New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)



New Design File, Icons8, Pngio, Flaticon

Port Scan (CVE-2019-11728)

- Distributed port scanning
- Localhost, private networks (behind firewall/NAT)
- TCP ports, some UDP ports
- Attacker identity is not revealed!

Flaticon

DEMO

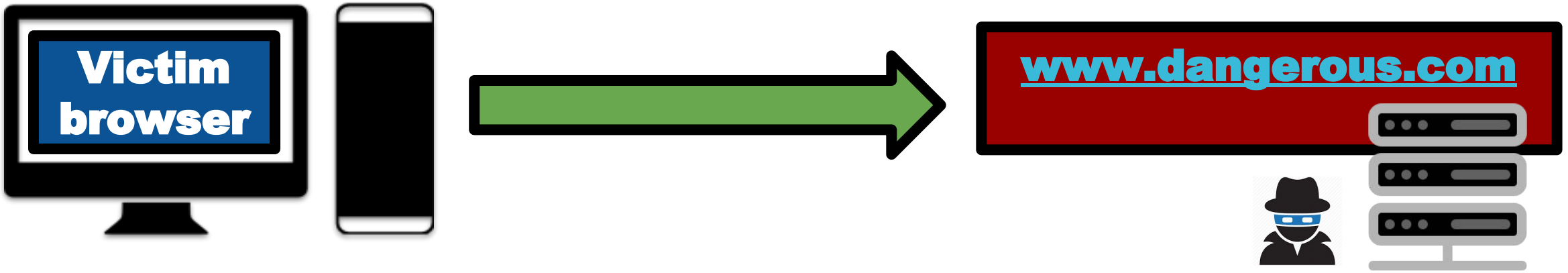
https://youtu.be/CIS_M0C8co0

Overview of abuse

- Port Scan (CVE 2019-11728)
- DDoS
- Alt-Svc Abuses
- History Exfiltration
- Malware protection bypass
- Tracking

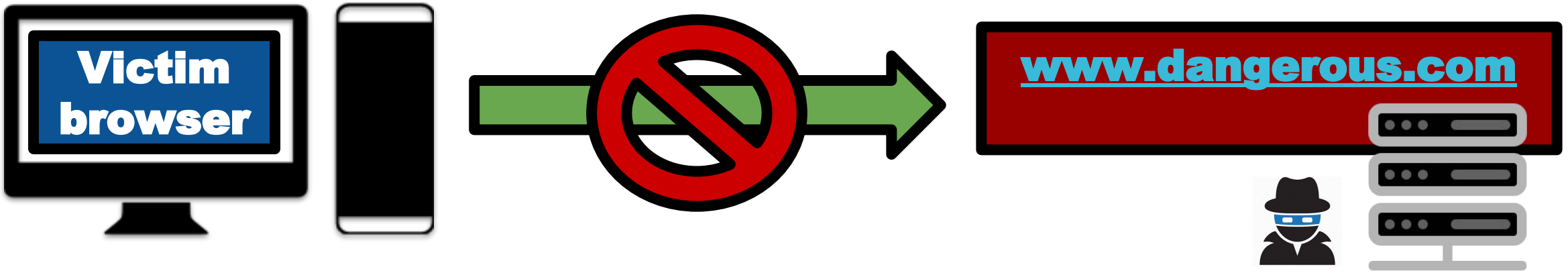
Flaticon

Malware protection bypass



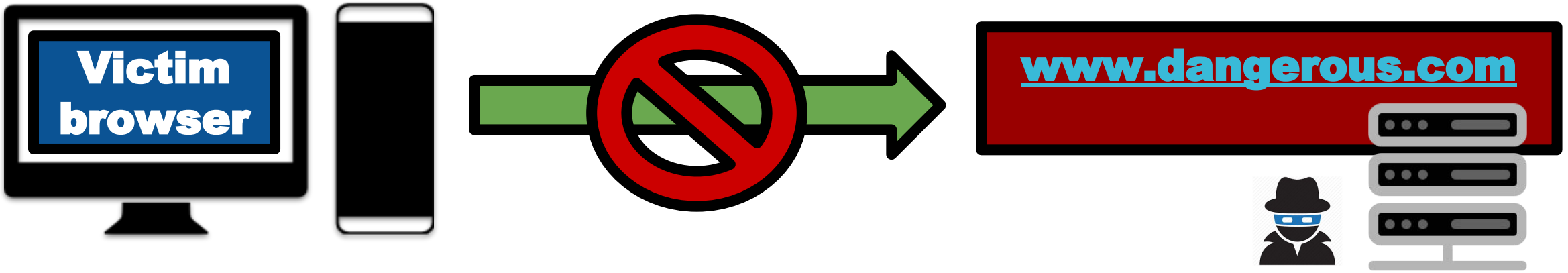
New Design File, Icons8, Pngio, Flaticon

Malware protection bypass



New Design File, Icons8, Pngio, Flaticon

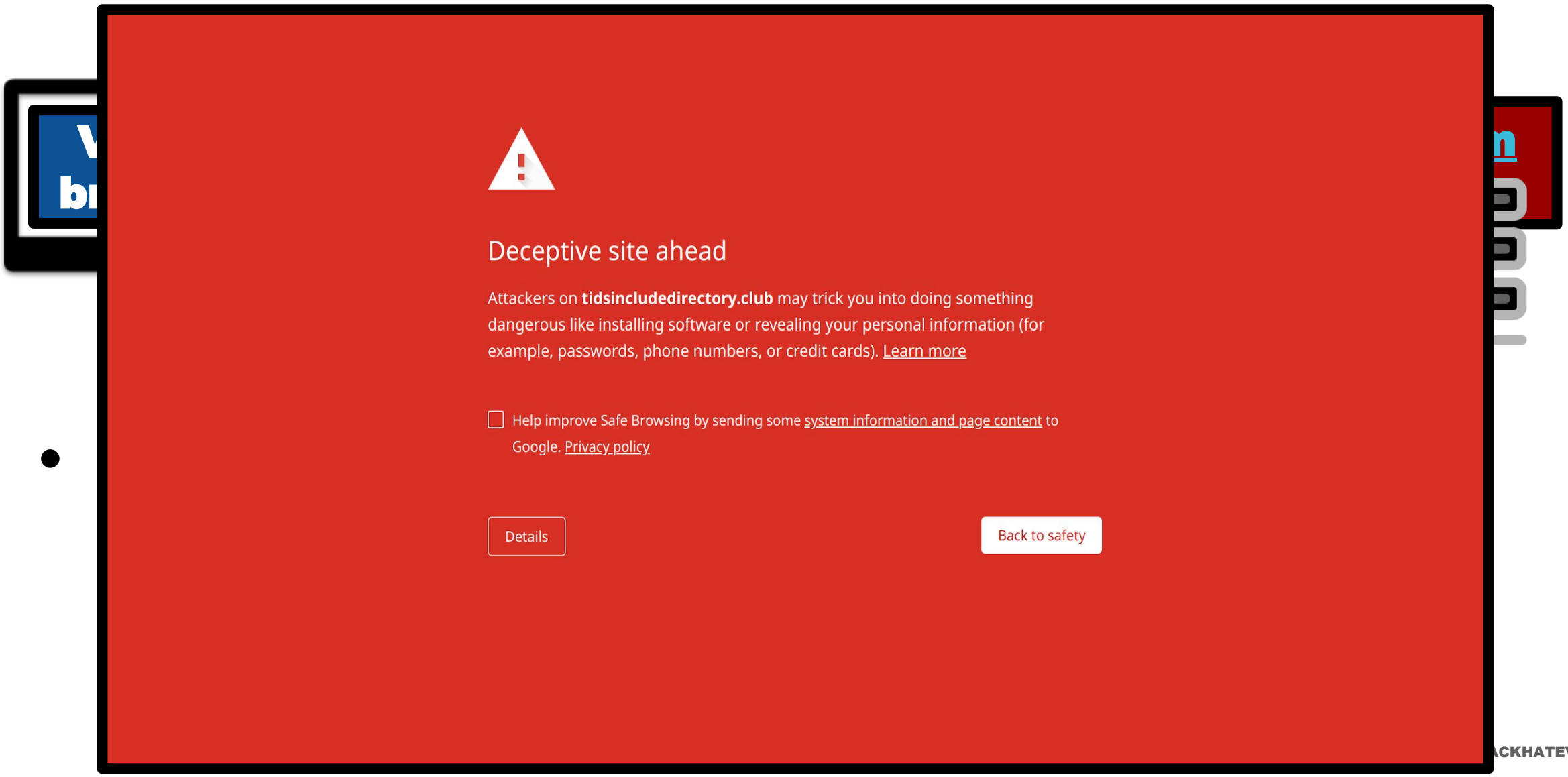
Malware protection bypass



- **Blocks first and third party:**
  - **www.dangerous.com in URL bar**
  - **<img src=www.dangerous.com> in www.example.com**

New Design File, Icons8, Pngio, Flaticon

Malware protection bypass



Malware protection bypass

- www.example.com specifies www.dangerous.com as it's Alt-Svc.
- Browser allows content loading from www.dangerous.com!

Flaticon

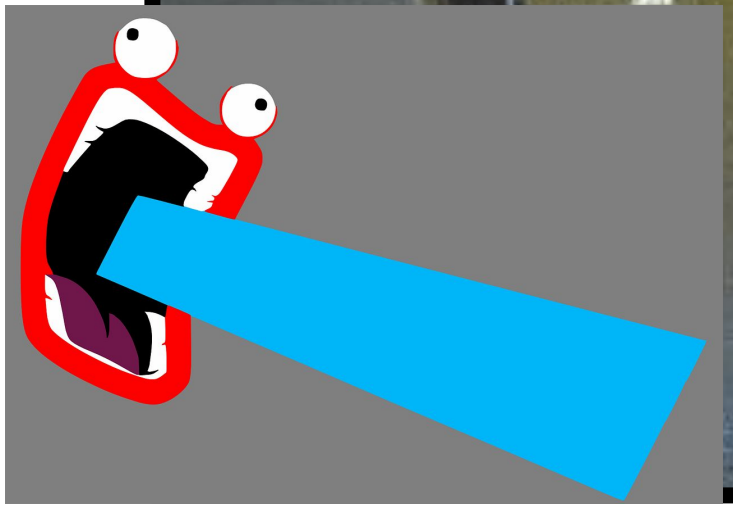
Malware protection bypass

- www.ex[illegible]s.com as it's Alt-Svc.
- Browser[illegible]angerous.com!

Flaticon

Malware protection bypass

- www.ex[illegible]s.com as it's Alt-Svc.
- Browser[illegible]angerous.com!



Flaticon

Malware protection bypass

But why is this actually dangerous?

Flaticon

How most scanners work

Original

www.example.com

Alt-Svc

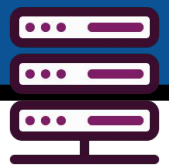
www.example2.com

Flaticon, Iconsforfree

How most scanners work

Original
www.example.com

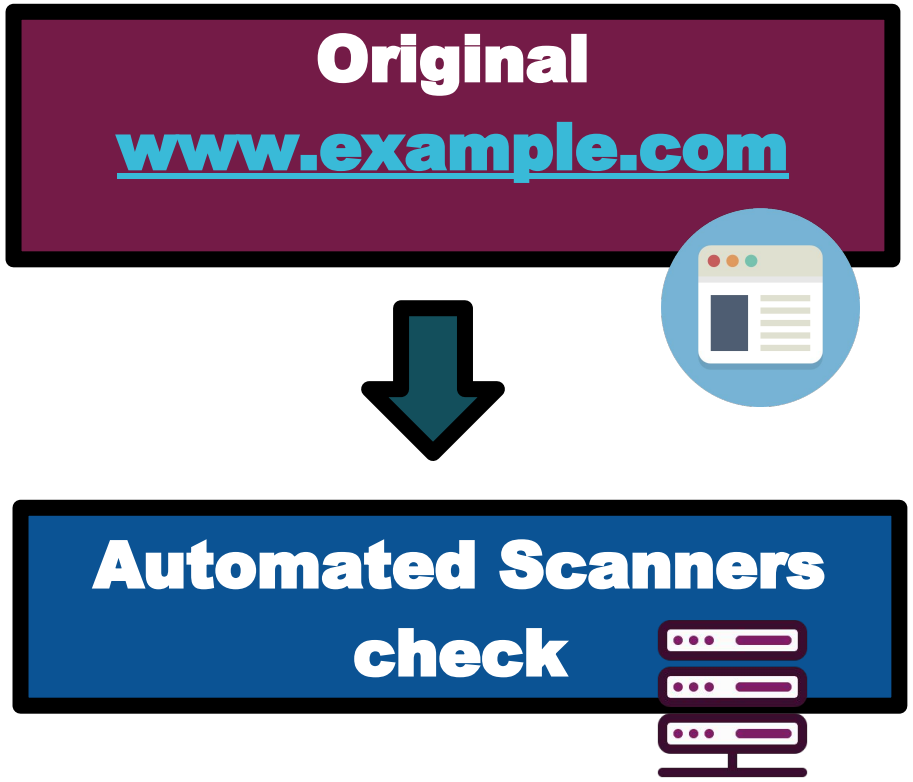
Automated Scanners check



Alt-Svc
www.example2.com

Flaticon, Iconsforfree, Icons8

How most scanners work



Flaticon, Iconsforfree, Icons8

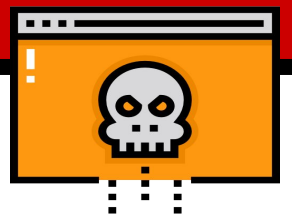
Not Useful

Original

www.example.com

Alt-Svc

www.dangerous.com

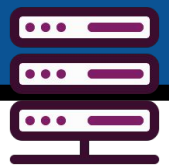


Flaticon

Not Useful

Original
www.example.com

Automated Scanners check



Alt-Svc
www.dangerous.com

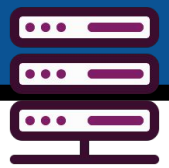
Flaticon, Icons8

Not Useful

Original
www.example.com

Alt-Svc
www.dangerous.com

Automated Scanners check



See malware, blacklist website, GAME OVER!!

Flaticon, Icons8

Malware protection bypass

Now for something more insidious …

Flaticon

Two Faced Content

Original

www.example.com

Alt-Svc

www.dangerous.com

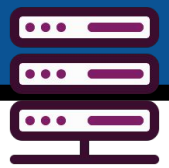
Flaticon

Two Faced Content

Original

www.example.com

Automated Scanners check



Alt-Svc

www.dangerous.com

Icons8, Flaticon

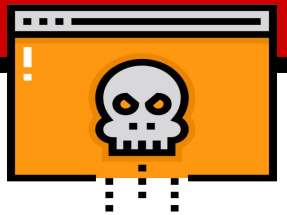
Two Faced Content

Original
www.example.com

Automated Scanners check

See only benign content, website PASSES check!

Alt-Svc
www.dangerous.com

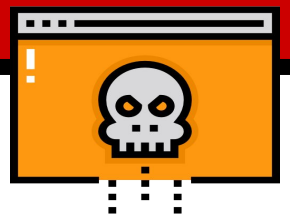


Icons8, Flaticon

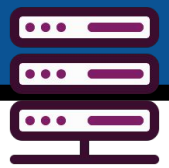
Two Faced Content

Original
www.example.com

Alt-Svc
www.dangerous.com



Automated Scanners check



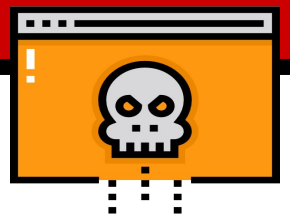
Browser loads

New Design File, Icons8, Flaticon

Two Faced Content

Original
www.example.com

Alt-Svc
www.dangerous.com



Automated Scanners check

Browser loads

Also vulnerable: URLVoid, VirusTotal, Sucuri, IPVoid

New Design File, Icons8, Flaticon

DEMO

https://youtu.be/ZkgJJYU8oJo

Mitigations

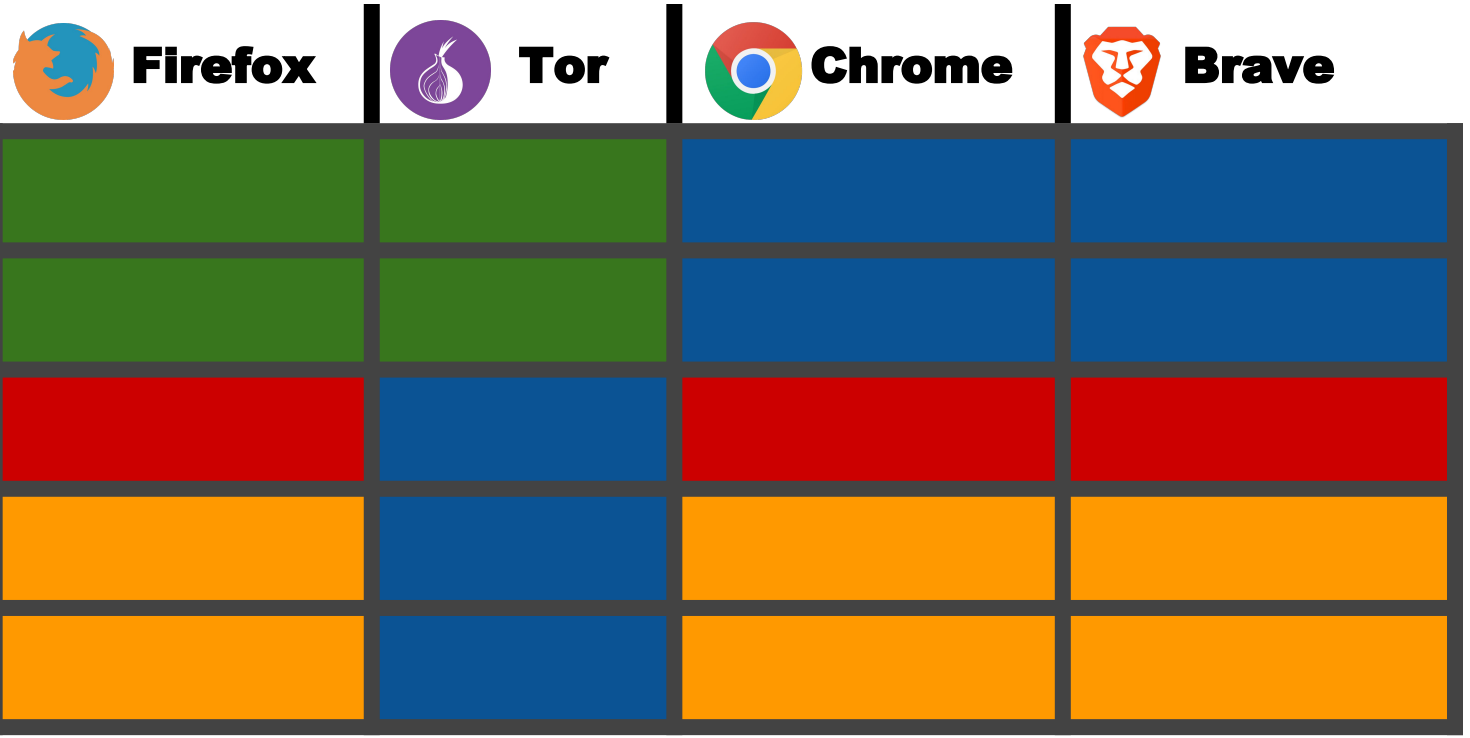
- **Port-Scan, DDoS:**
  Block sensitive ports

- **Safe Browsing:**
  Alt-Svc domain check

- **Tracking, History Exfiltration:**
  Isolate Alt-Svc cache

Flaticon

Industry Response



Fixed	In process	Unpatched	Unaffected

Flaticon, Iconfinder, Iconfinder, Iconfinder

Conclusion

- New but widely adopted Alt-Svc is vulnerable
- 5 attacks(!), despite:
  - Maturity of HTTP
  - Highly competent browser developers
- Securing is not easy!

Flaticon

Questions?

Flaticon

References

- pixabay.com
- Bruce Shneier, Blake Ross, Brendan Eich pictures, Wikipedia
- Video by willbot-studios from pixabay.com.

Flaticon