@fork_while_1

Alternative (ab)uses for HTTP Alternative Services

Trishita Tiwari

Ari Trachtenberg

Boston University

This research was partly supported by National Science Foundation, grant CCF-1563753

Outline

1. Background: HTTP

2. Alt-Svc header

3. Attacks w/ Alt-Svc

4. Mitigations

5. Industry response

6. Conclusion

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
Request for Comments: 1945
Category: Informational

T. Berners-Lee
MIT/LCS
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.

HTTP

- HTTP expanded:
  - Caching
  - Dynamic content
  - Request multiplexing
- Result = more papers for security researchers 😉

HTTP

- HTTP is as old as me (22 yrs)
- Yet hard to introduce secure protocol updates.

Alternative Services (RFC 7838)

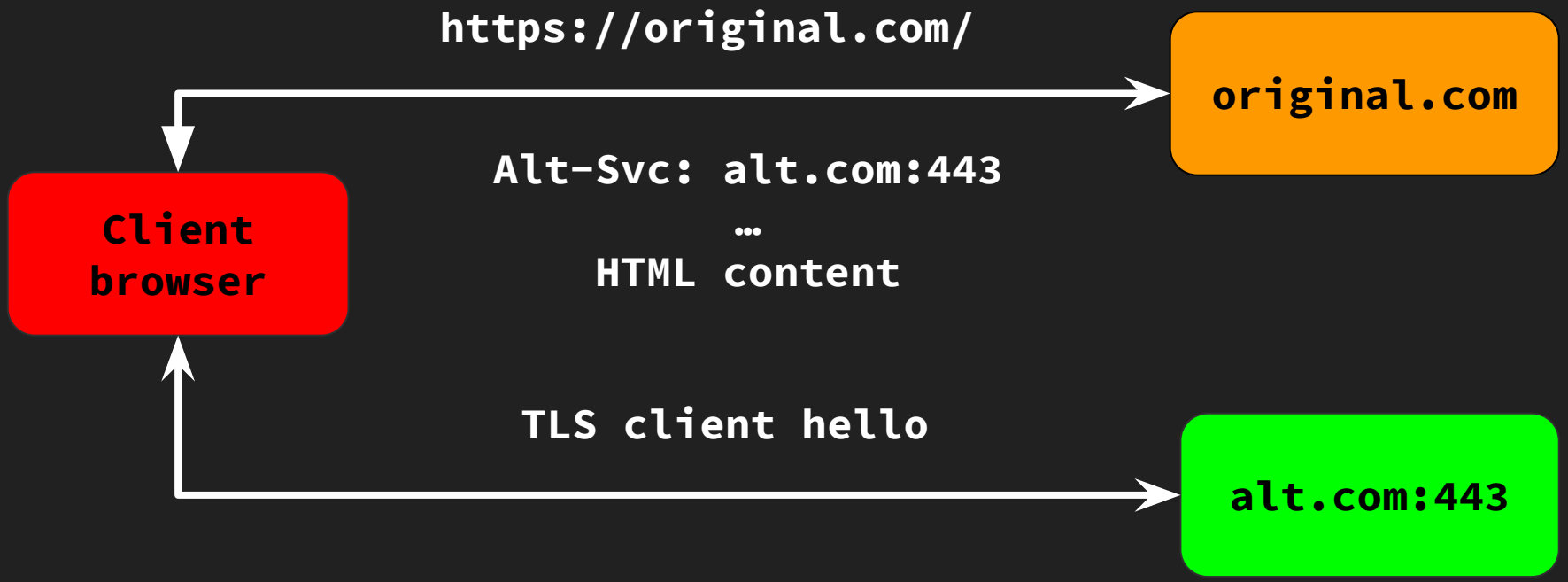
- Yet another HTTP header!!
- Allows website to specify equivalent alternate endpoint

Tired senior who needs to finish thesis

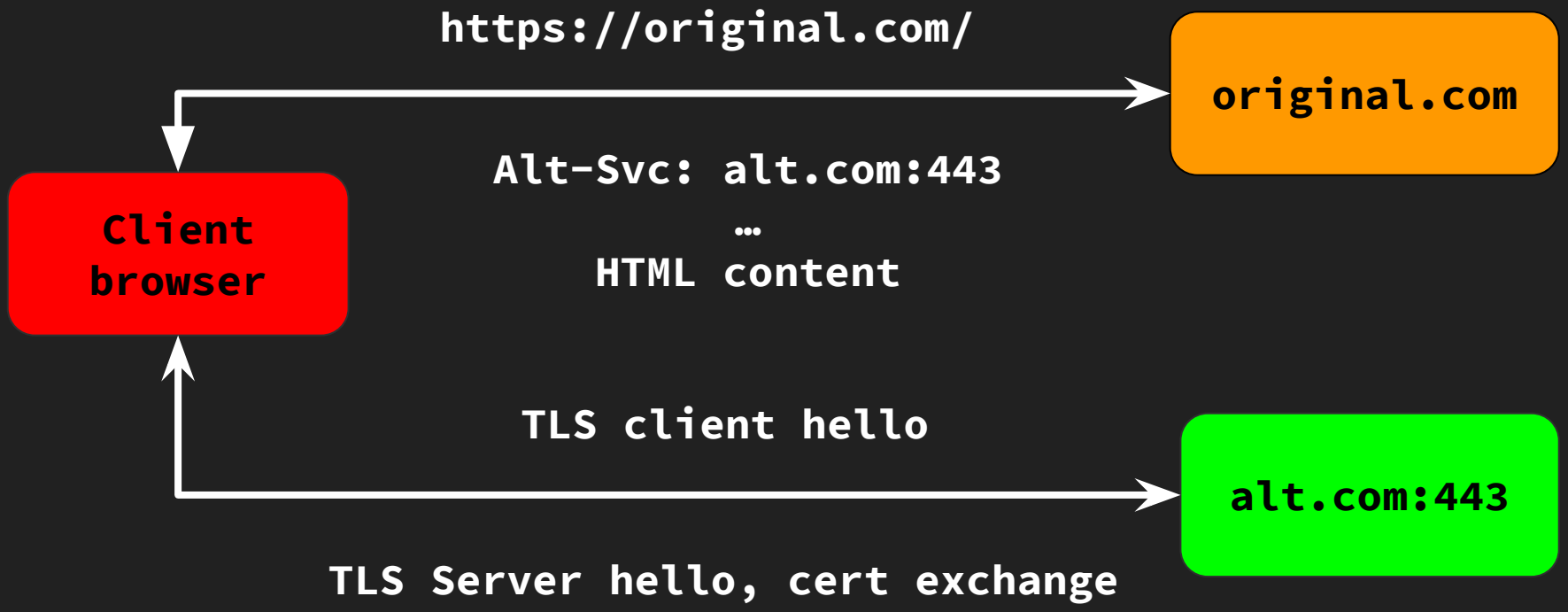
Alternative Services (RFC 7838)

Alternative Services (RFC 7838)

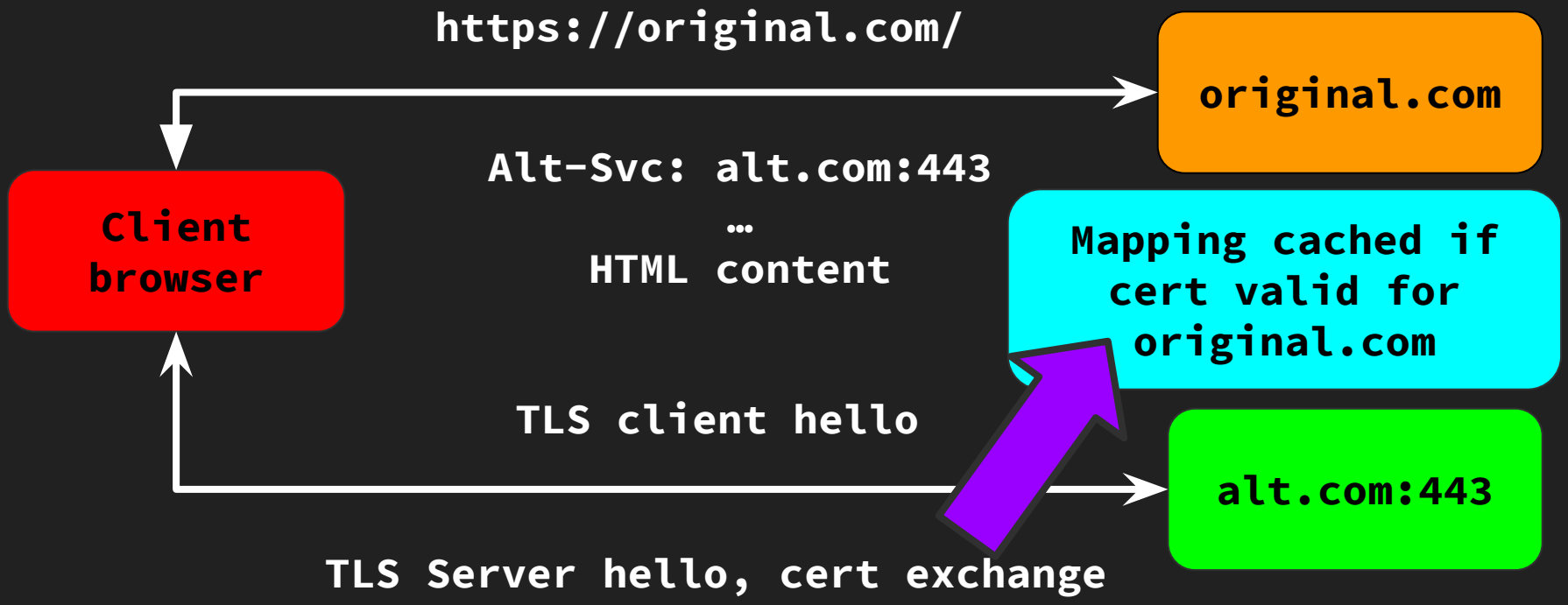
Alternative Services (RFC 7838)



Alternative Services (RFC 7838)



Alternative Services (RFC 7838)



Alt-Svc format

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

Alt-Svc format

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

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

Alt-Svc format

Domain/IP

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

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

Alt-Svc format

Domain/IP

Port

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

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

Alt-Svc format

Domain/IP

Port

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

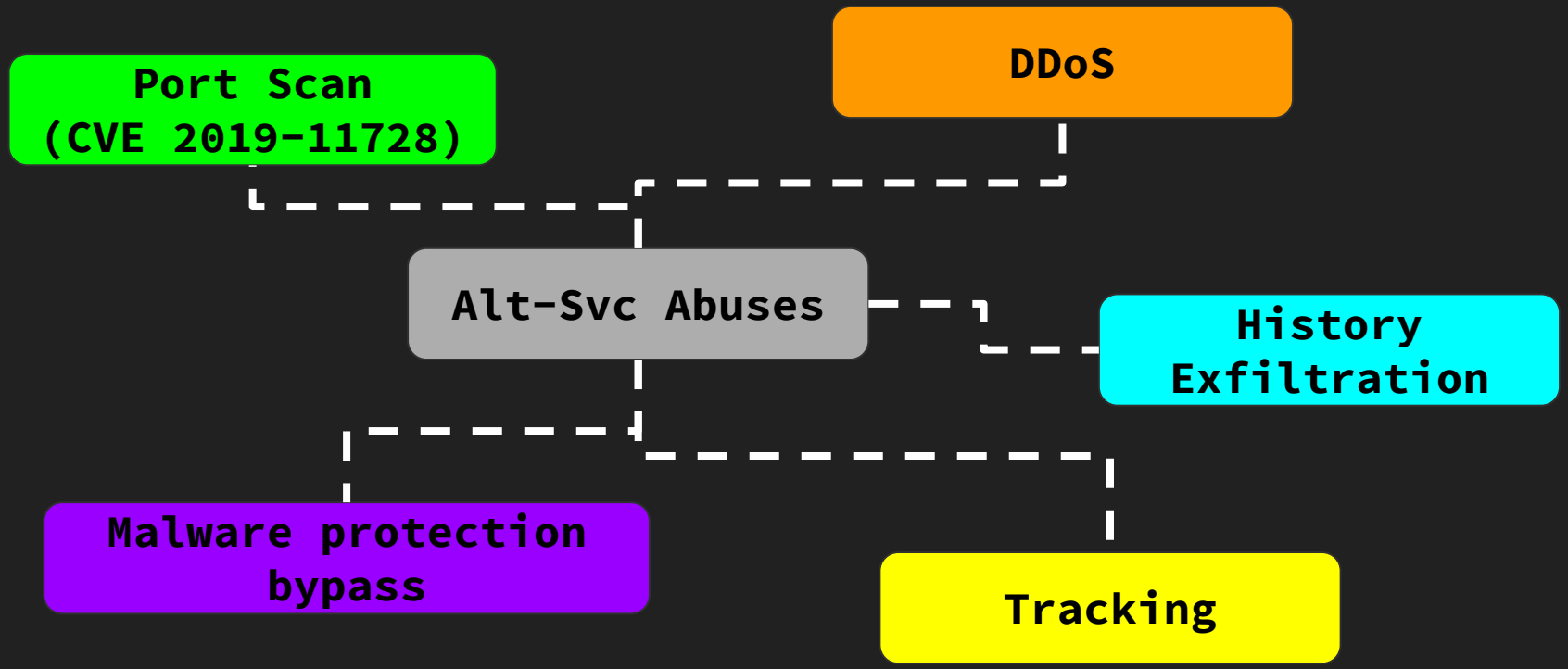
Protocol (http/1.1, quic, h2c, ftp, etc.)

Max age (s)

Alt-Svc Uses

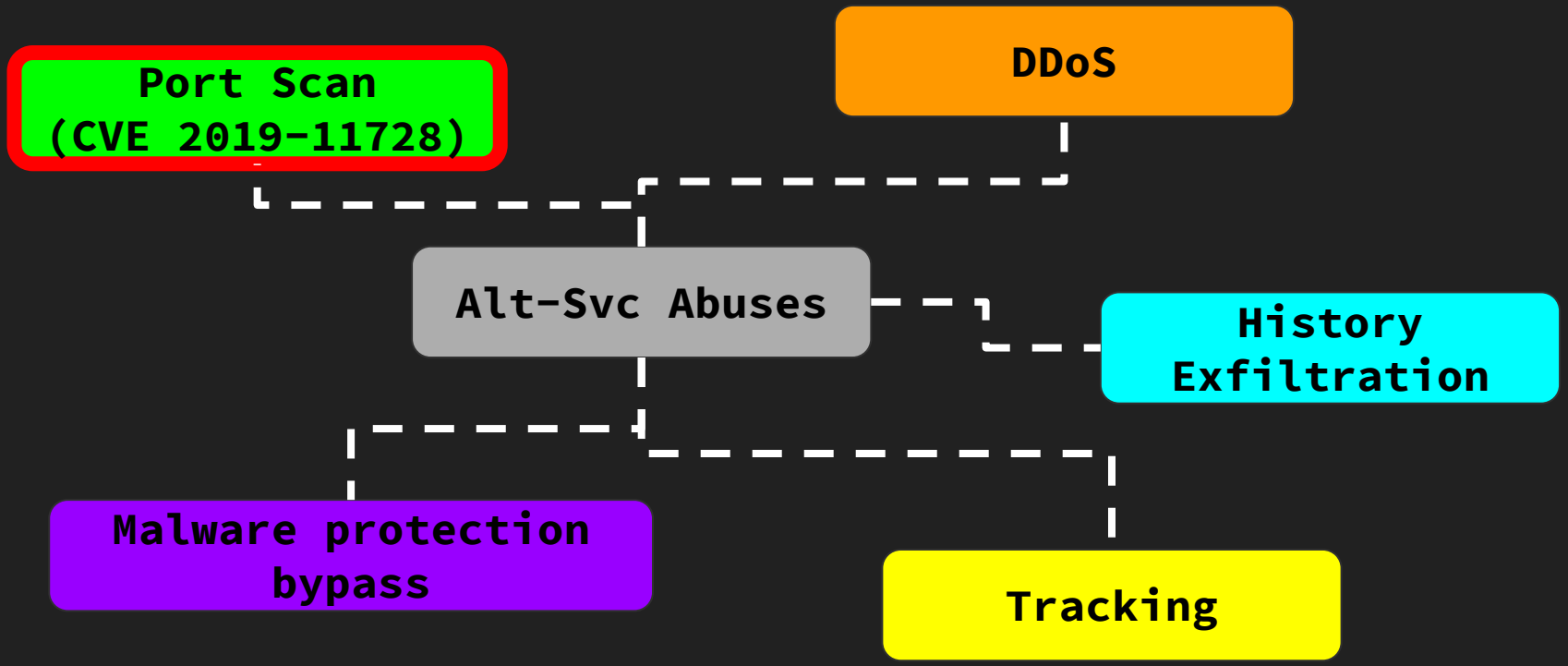
- Load balancing
- Client segmentation
- Advertising endpoints with new protocols

Overview of abuse



Threat model

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


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

Port-Scan (CVE-2019-11728)

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

```
http://evil.com/p1
Alt-Svc: “h2=localhost:25”
```

Port-Scan (CVE-2019-11728)

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

```
http://evil.com/p1
Alt-Svc: “h2=localhost:25”
```

Browser validates Alt-Svc

Port-Scan (CVE-2019-11728)

Closed Port	Open Port

Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	

Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT

Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
	PKT

Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
	PKT
	PKT

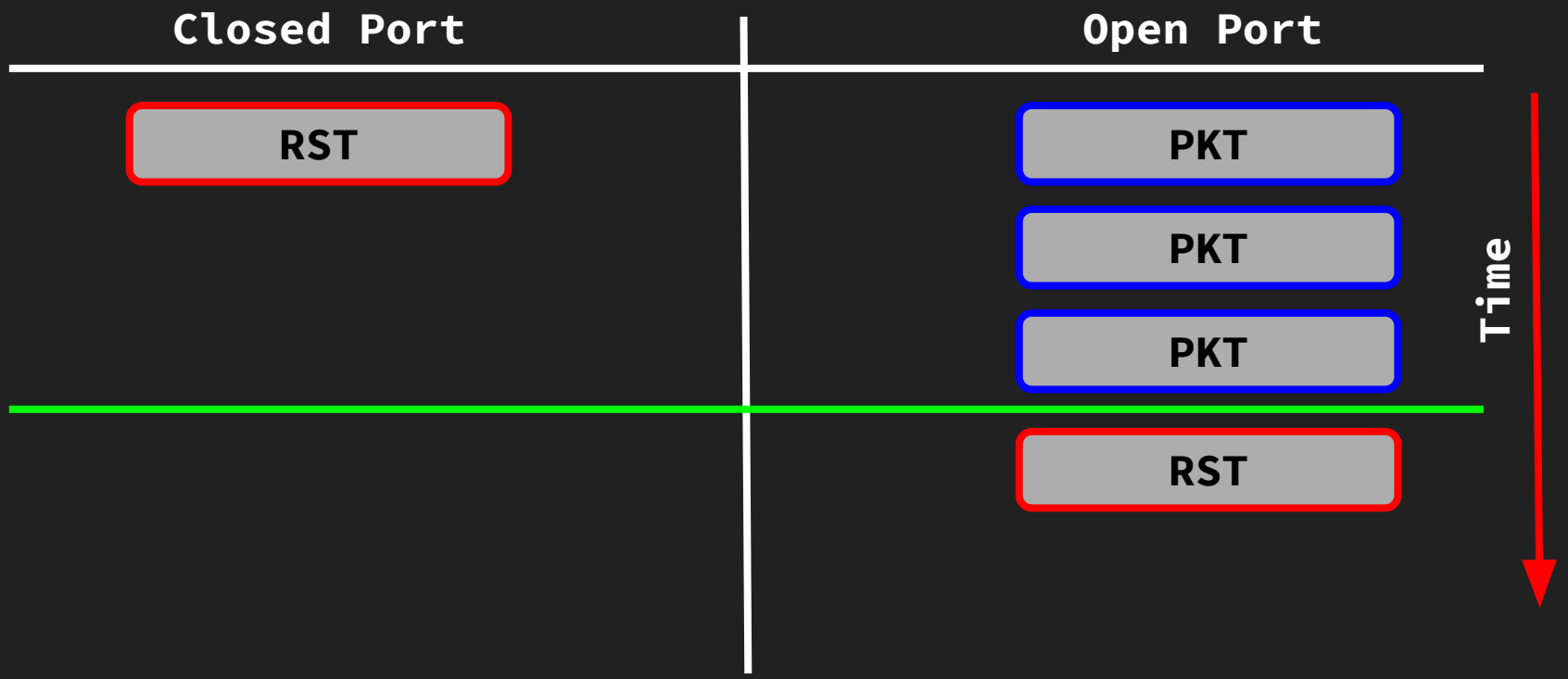
Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
	PKT
	PKT
	RST

Time

Port-Scan (CVE-2019-11728)



Port-Scan (CVE-2019-11728)

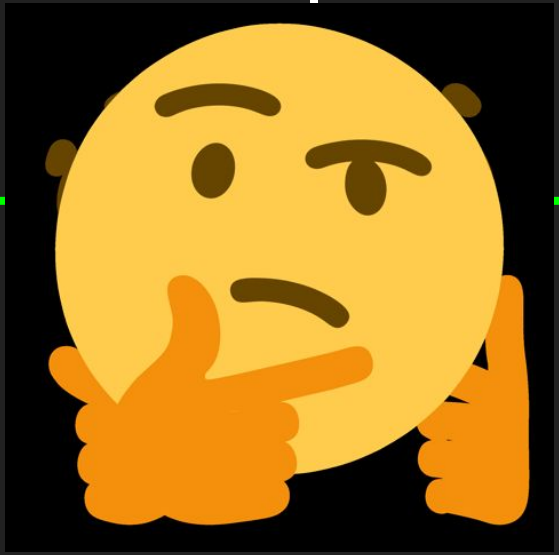
Closed Port	Open Port
RST	PKT PKT PKT
⊘	?

Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
	PKT
	PKT

Time



Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
Redirect: http://evil.com/p2 Alt-Svc: “h2=evil2.com:443”	PKT
	PKT

Time

Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
Redirect: http://evil.com/p2 Alt-Svc: “h2=evil2.com:443”	PKT
	PKT
Browser connects to new Alt-Svc	

Time

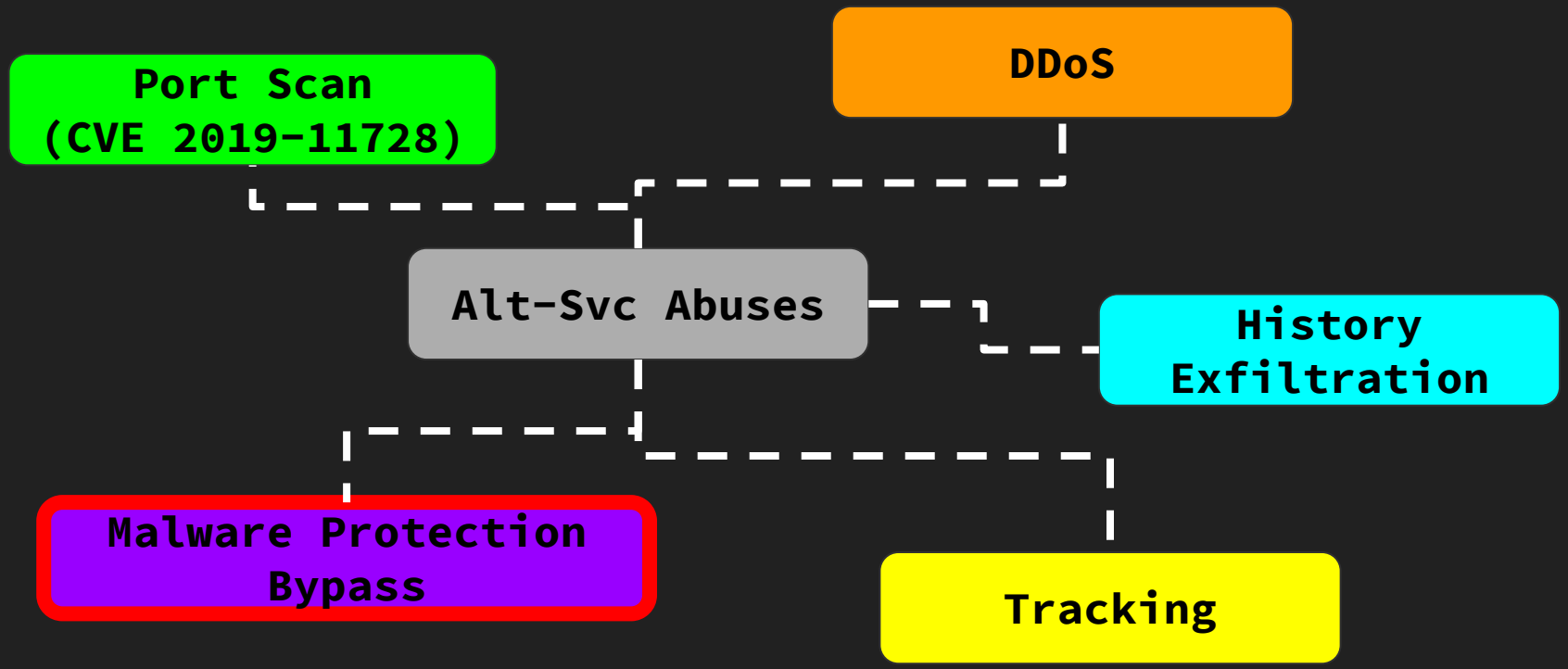
Port-Scan (CVE-2019-11728)

Closed Port	Open Port
RST	PKT
Redirect: http://evil.com/p2 Alt-Svc: “h2=evil2.com:443”	PKT
	PKT
Browser connects to new Alt-Svc	Browser DOES NOT connect to new Alt-Svc

Time

Port-Scan consequences

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

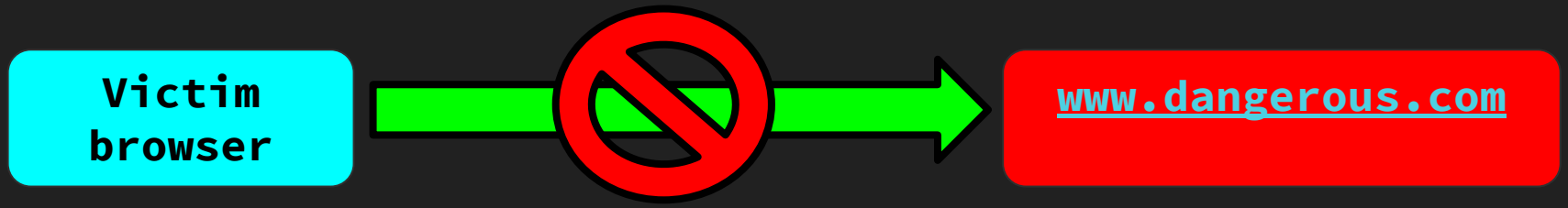

Port Scan
(CVE 2019-11728)
DDoS
Alt-Svc Abuses
History
Exfiltration
Malware Protection
Bypass
Tracking

Malware protection bypass

Victim browser

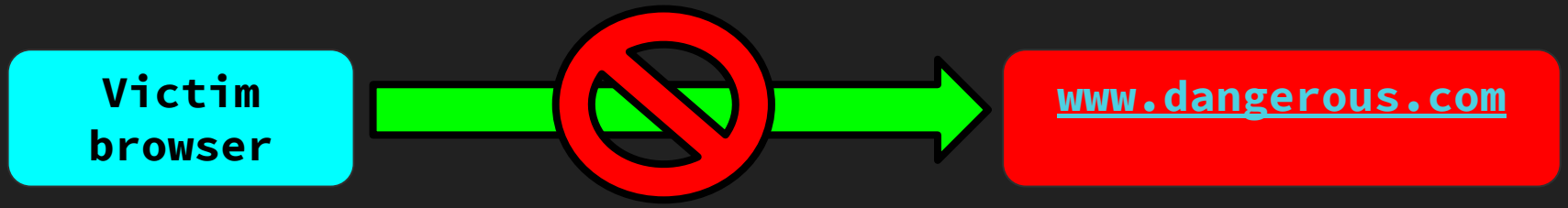
www.dangerous.com

Malware protection bypass



Safe browsing

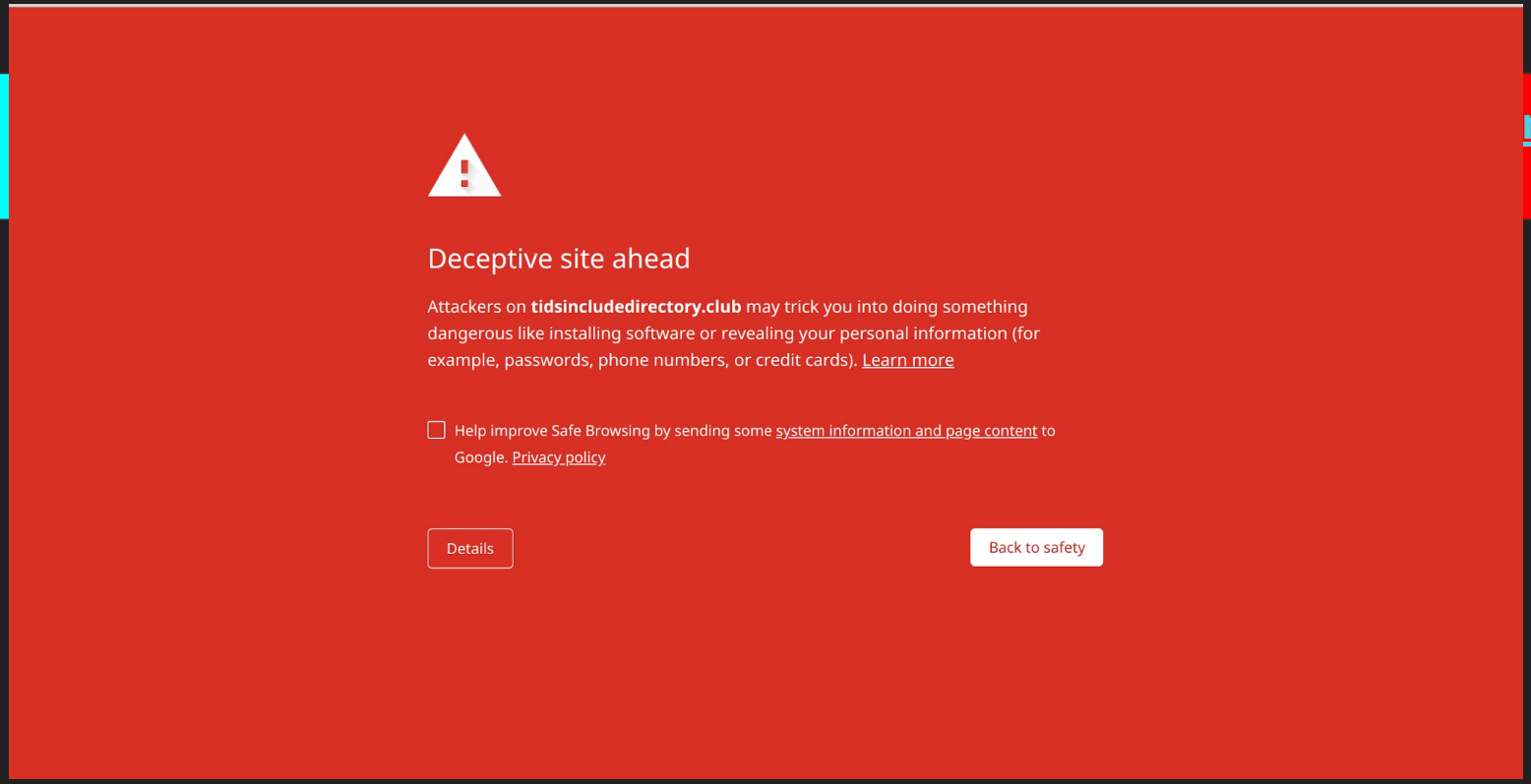
Malware protection bypass



Safe browsing

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

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!

Malware protection bypass

- www.exam com as it's Alt-Svc.
- Browser dangerous.com!

Malware protection bypass

- www.example.com specifies any dangerous.com as it's Alt-Svc.
- Browser [illegible] dangerous.com!

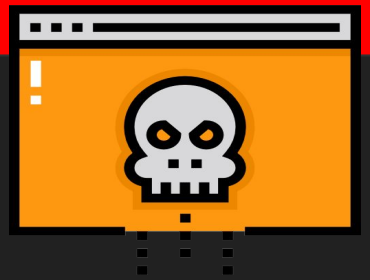
Two-faced content

Original

www.example.com

Alt-Svc

www.dangerous.com



Two-faced content

Original
www.example.com

Automated scanners check

Alt-Svc
www.dangerous.com

User browser loads

Two-faced content

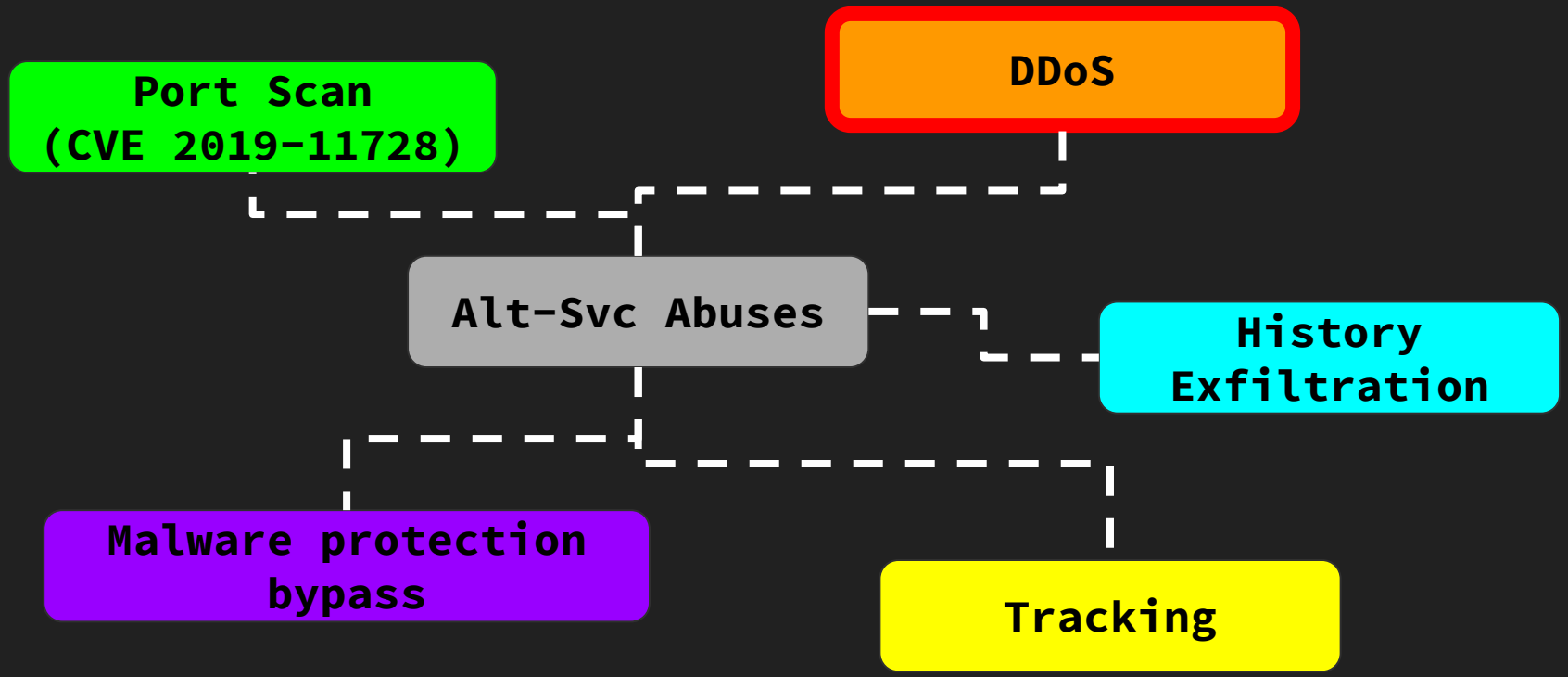
Original
www.example.com

Automated scanners check

Alt-Svc
www.dangerous.com

User browser loads

Vulnerable: URLVoid, VirusTotal, Sucuri, IPVoid

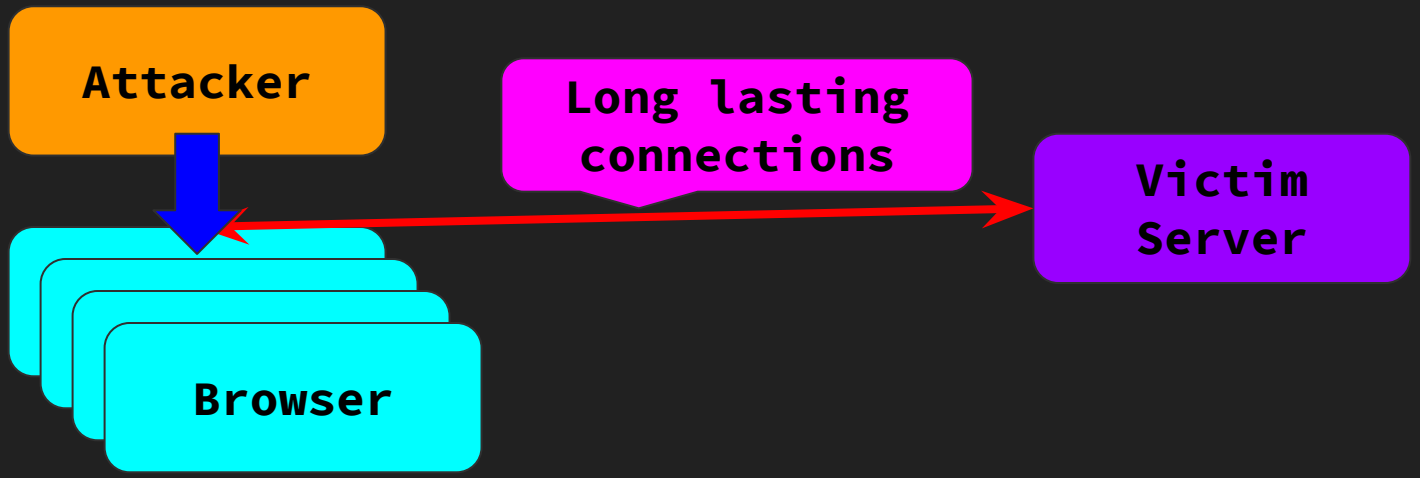

Port Scan
(CVE 2019-11728)
DDoS
Alt-Svc Abuses
History
Exfiltration
Malware protection
bypass
Tracking

DDoS

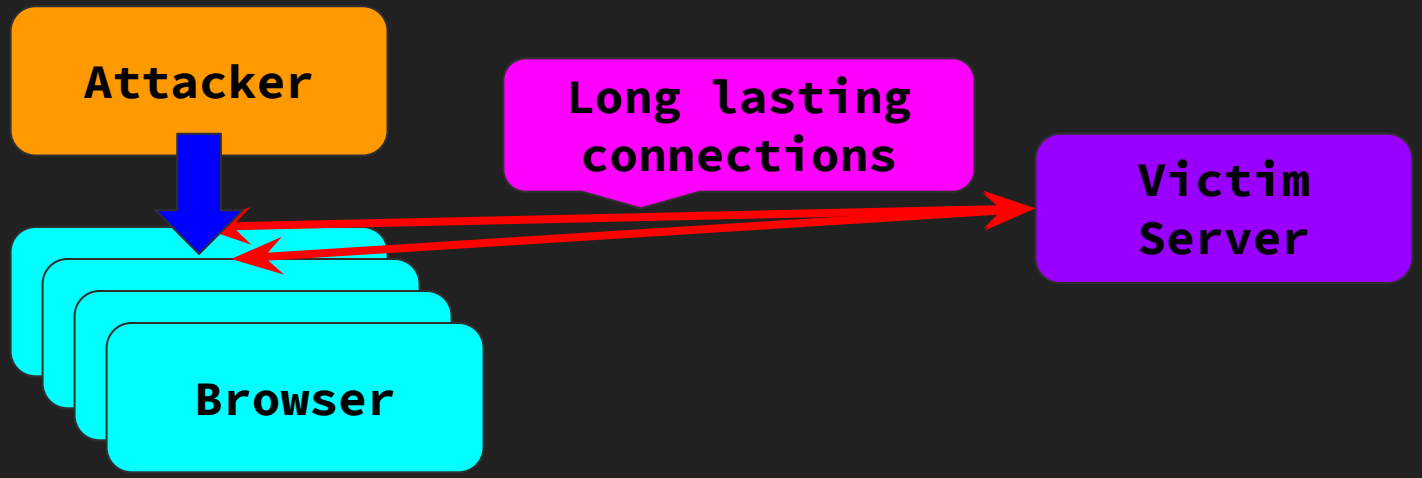
- Many clients connect to victim Alt-Svc endpoint: DDoS!
  - Long timeouts
  - Bandwidth Exhaustion

DDoS: Long timeouts

DDoS: Long timeouts



DDoS: Long timeouts



DDoS: Long timeouts

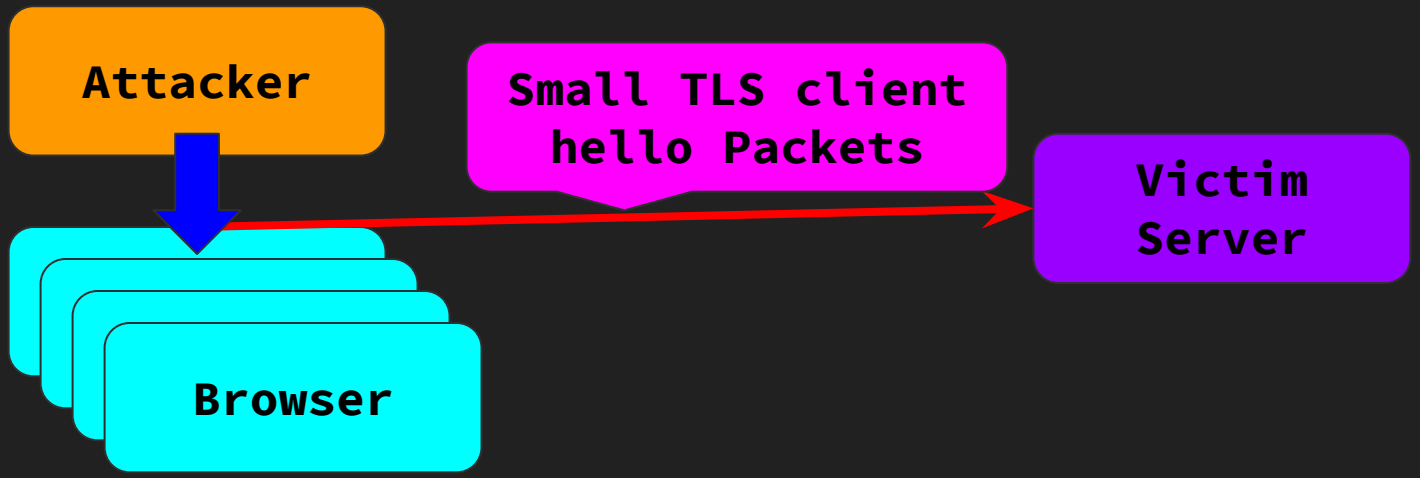
DDoS: Long timeouts

DDoS: Long timeouts

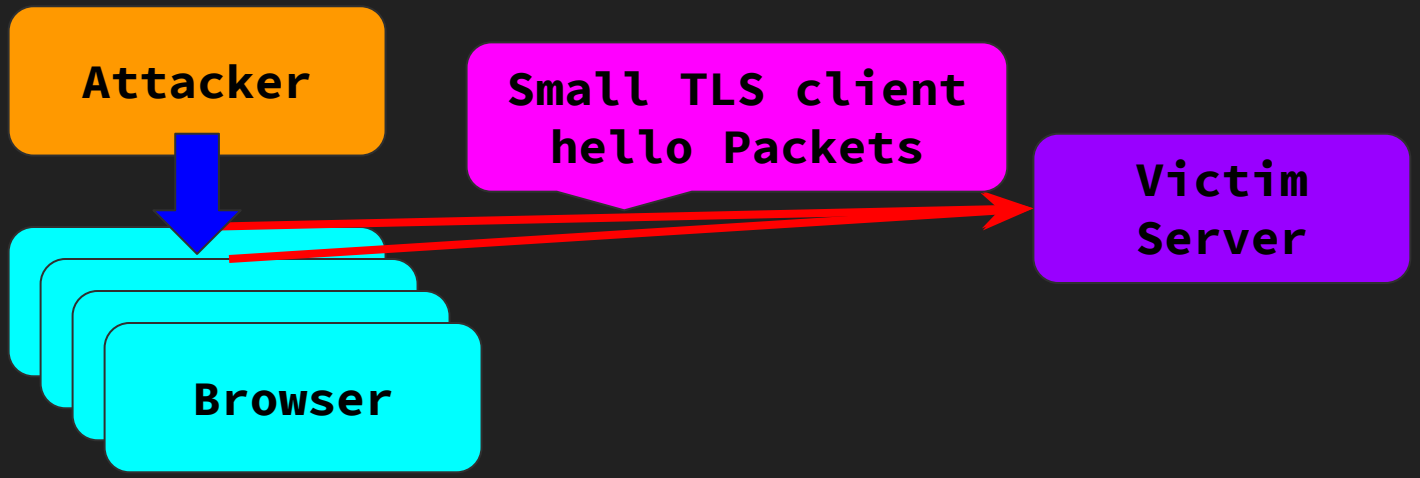
- FTP, SMTP, etc. servers

DDoS: Bandwidth exhaustion

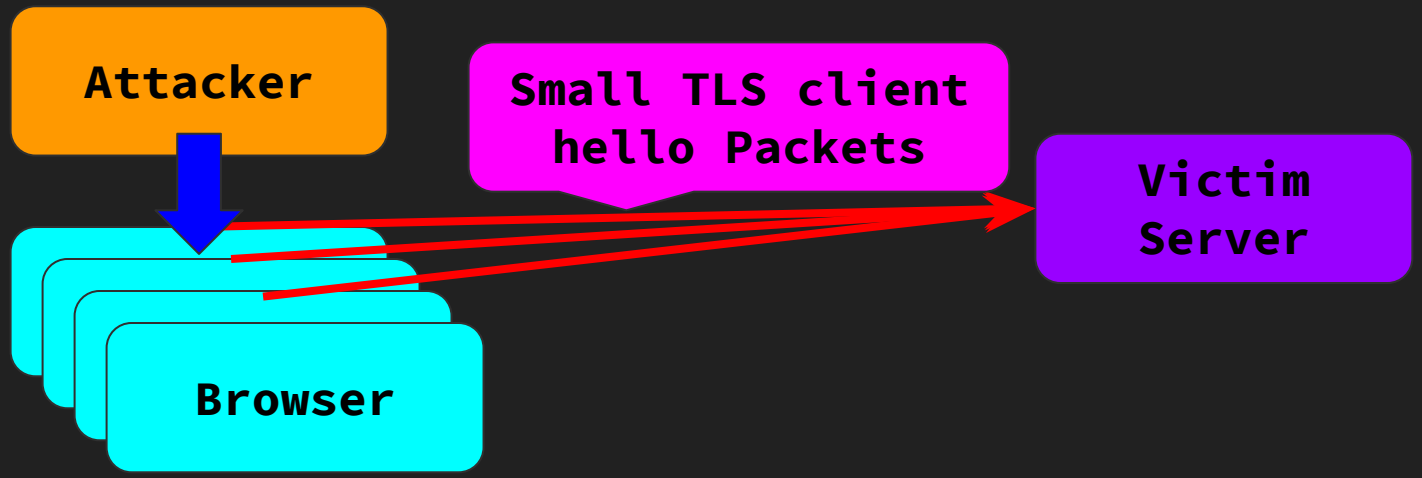
DDoS: Bandwidth exhaustion



DDoS: Bandwidth exhaustion



DDoS: Bandwidth exhaustion



DDoS: Bandwidth exhaustion

DDoS: Bandwidth exhaustion

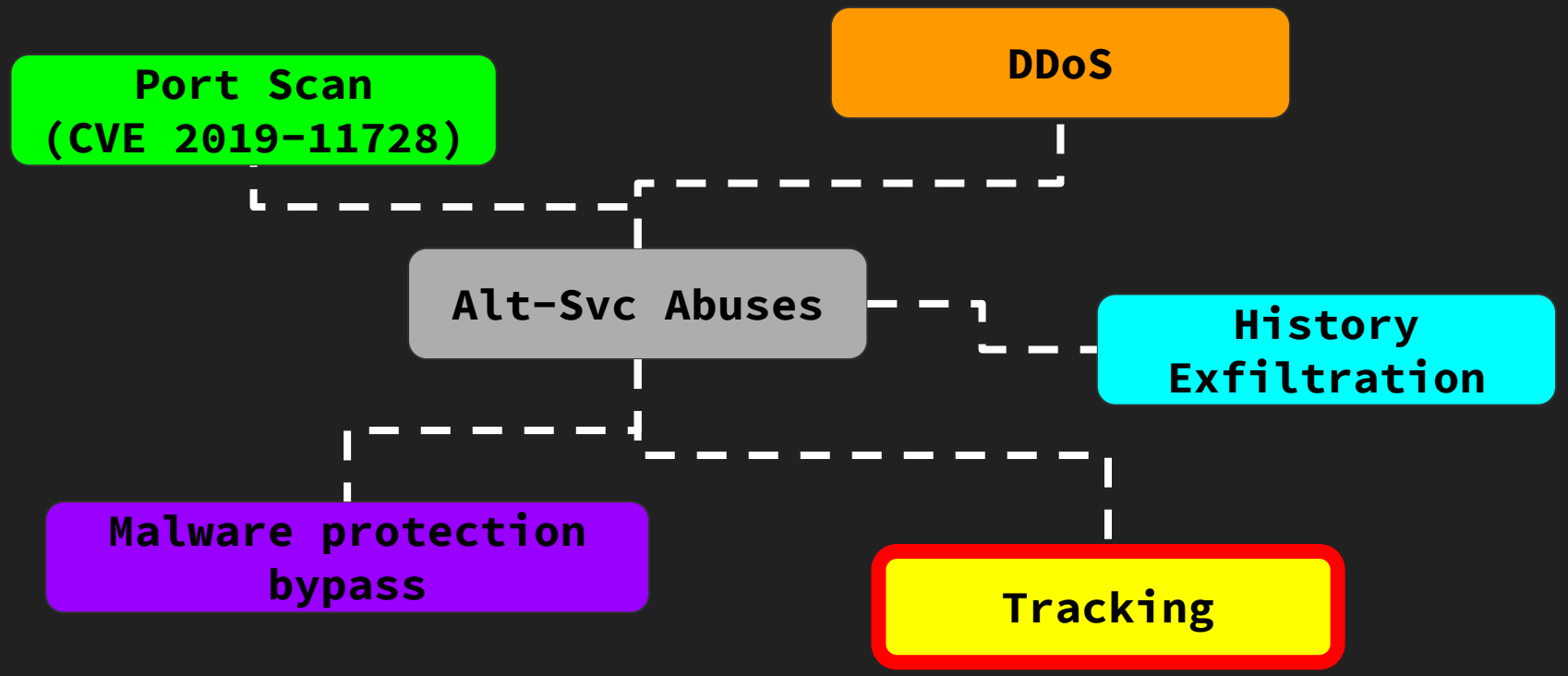
DDoS: Bandwidth exhaustion

DDoS: Bandwidth exhaustion

DDoS: Bandwidth exhaustion

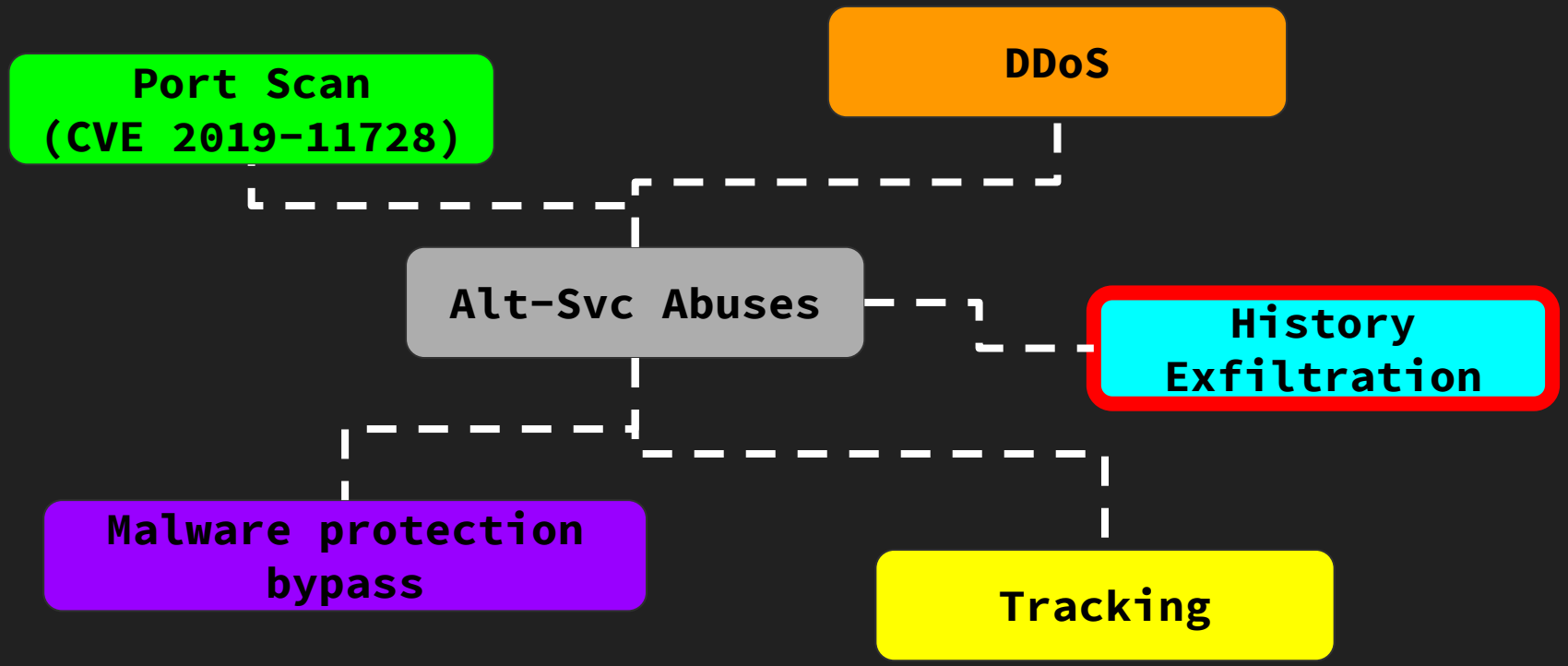
DDoS: Bandwidth exhaustion

- SMTP, HTTPS, etc. (any TLS speaking servers).


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

Tracking

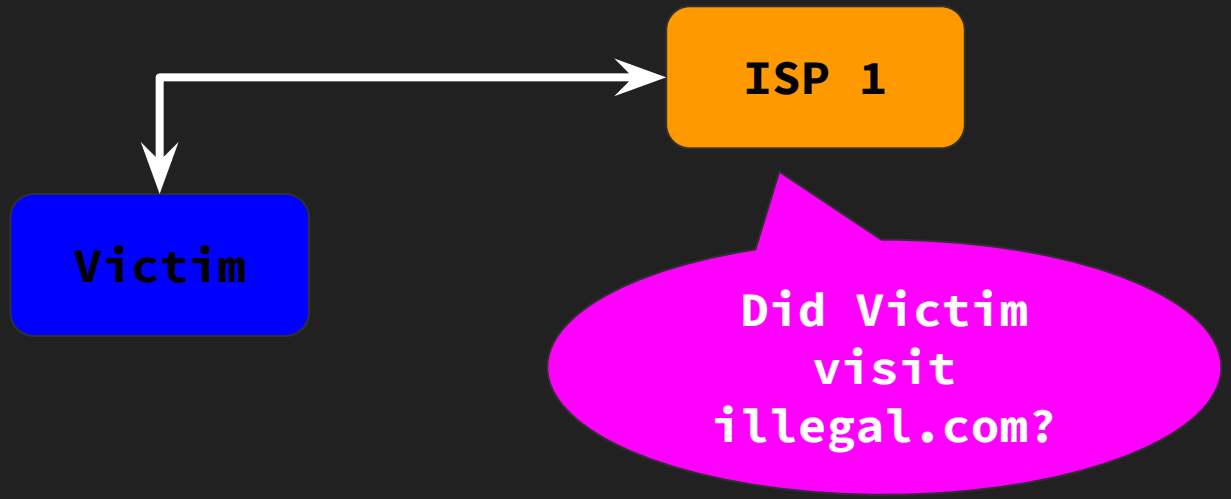
- Alt-Svc mapping is cached by browser.
- Specify unique value for each user to track.
- Works 1st and 3rd party, bypassing known tracking blockers.


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

History exfiltration

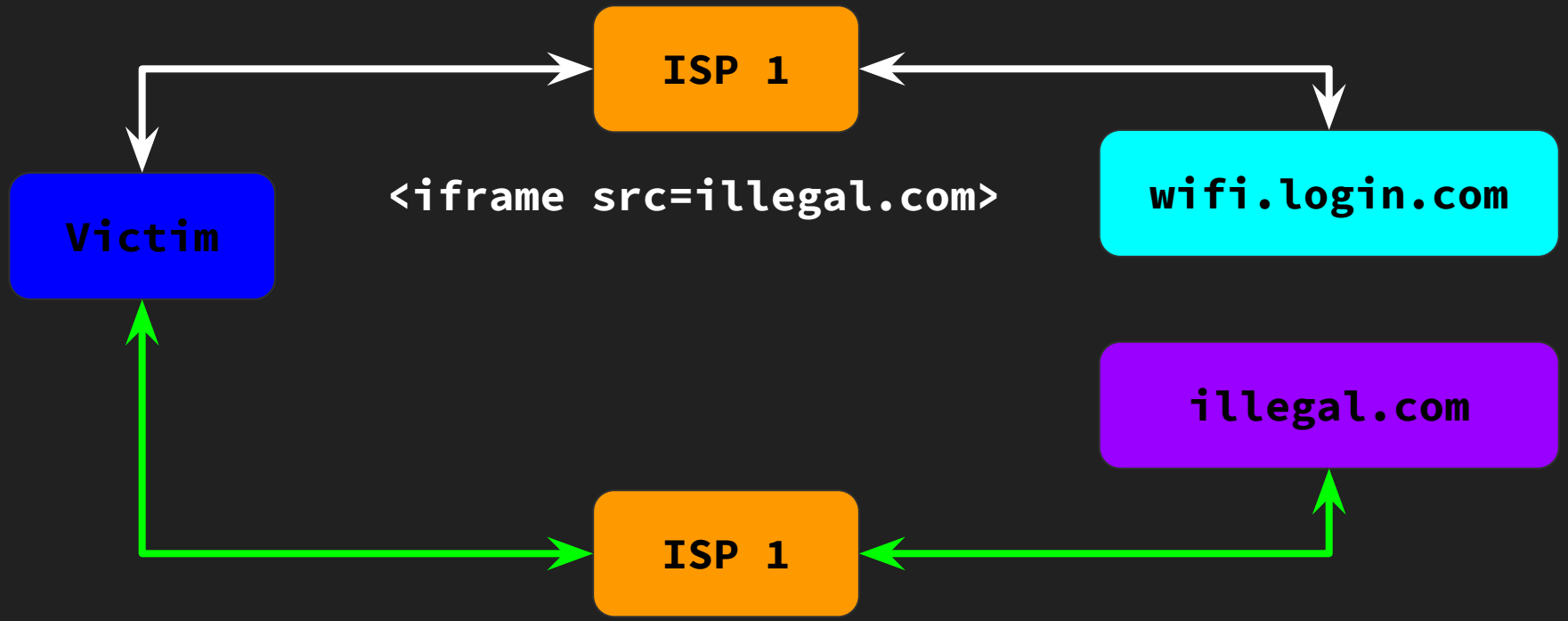
- Captive WiFi Portal
- Restaurants, coffee shops, hotels

History exfiltration

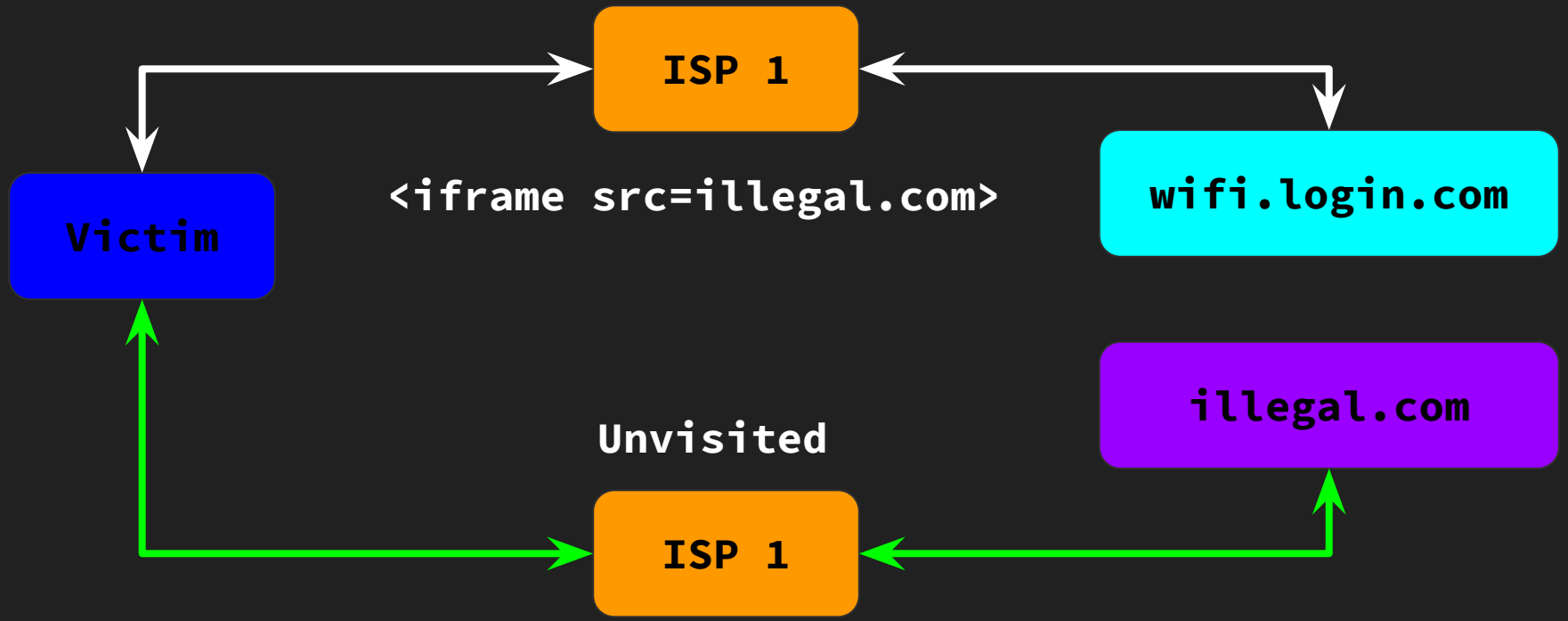


History exfiltration

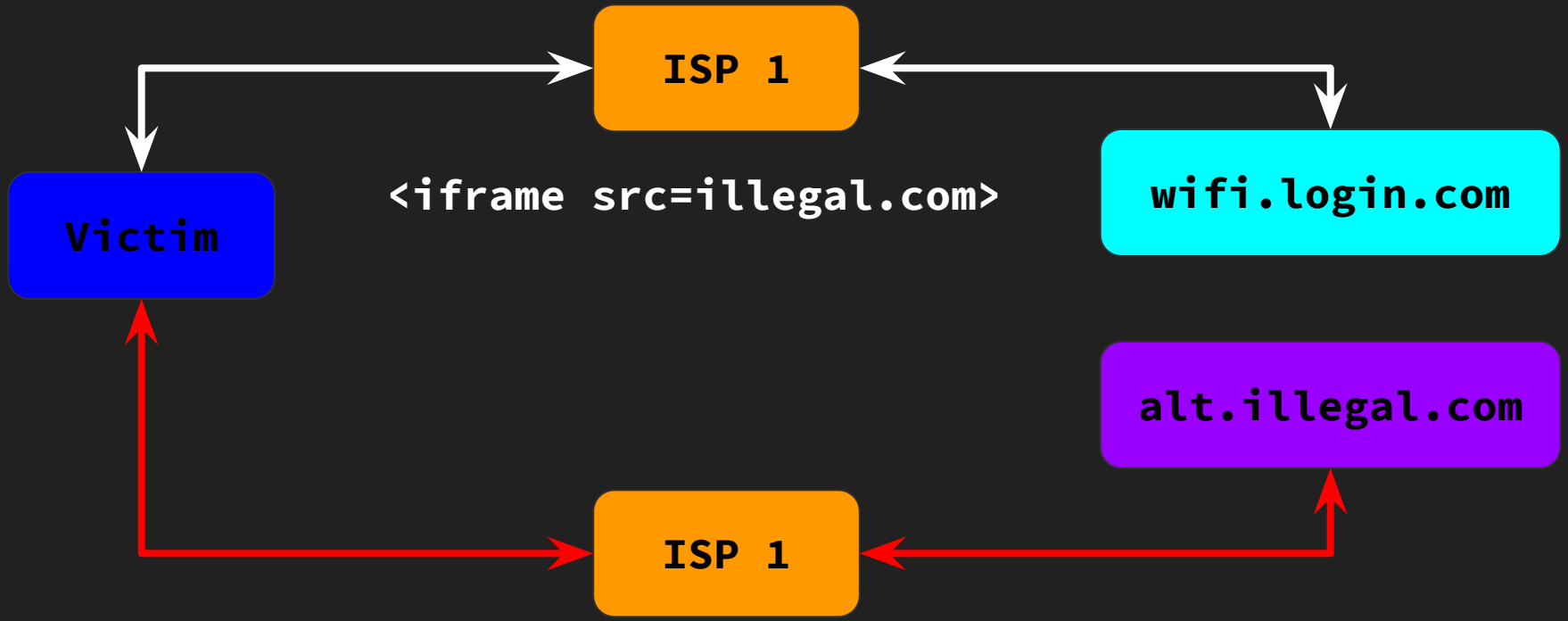
History exfiltration



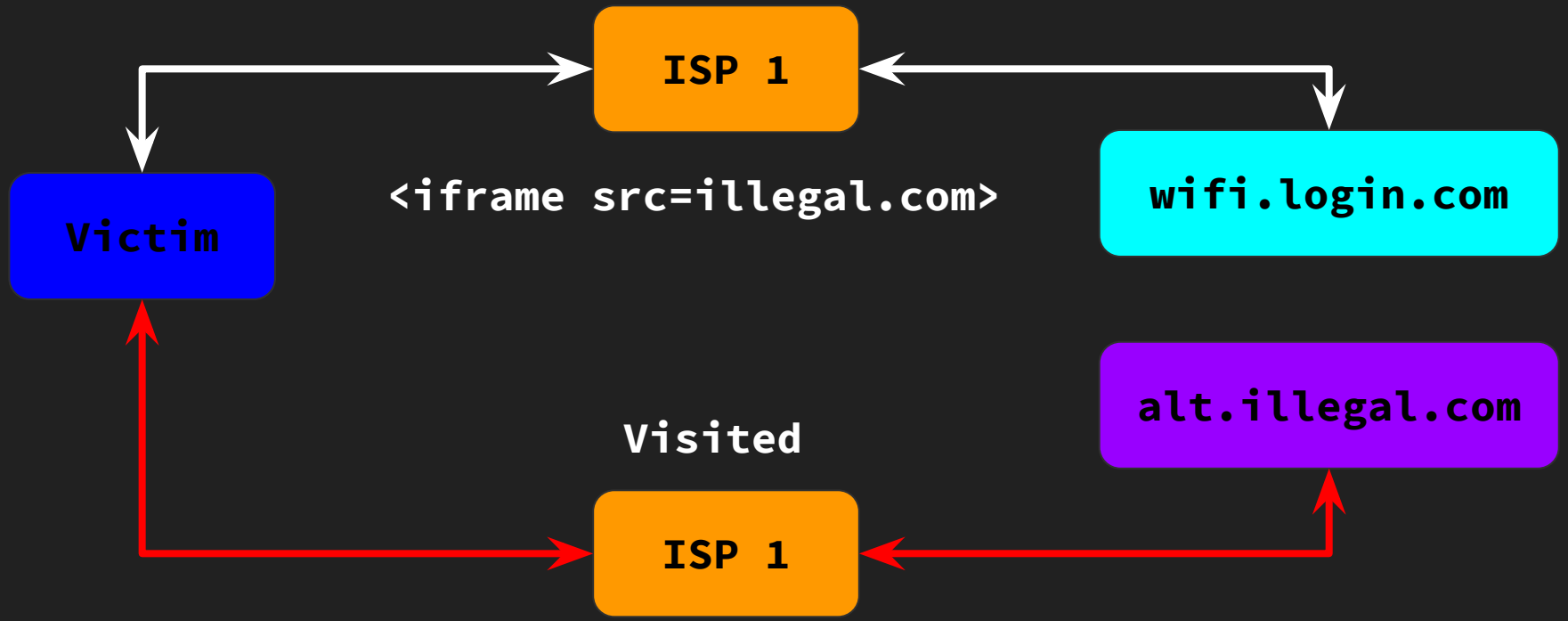
History exfiltration



History exfiltration



History exfiltration



Mitigations

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

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

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

Industry response

	Firefox	TOR	Chrome	Brave
Port-Scan				
DDoS				
Malware protection bypass				
Tracking				
History exfiltration				

Fixed	In process	Unpatched	Unaffected

Conclusion

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

References

- Icons made by Smashicons from Flaticon is licensed by CC 3.0 BY
- Icons made by Freepik from Flaticon is licensed by CC 3.0 BY
- Http Icon #286170 made by Icon Library

Questions?