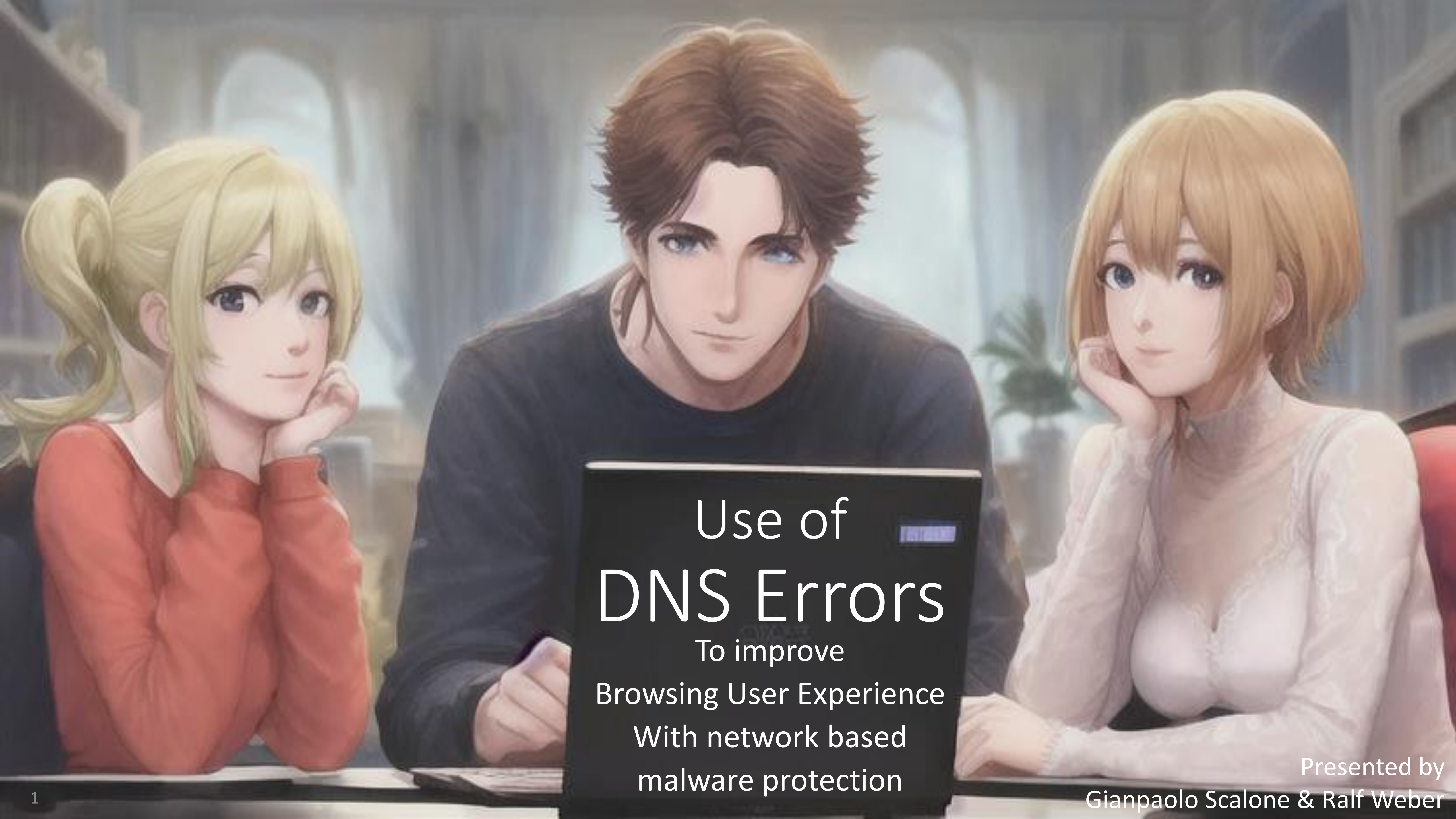


Use of DNS Errors

To improve Browsing User Experience With network based malware protection

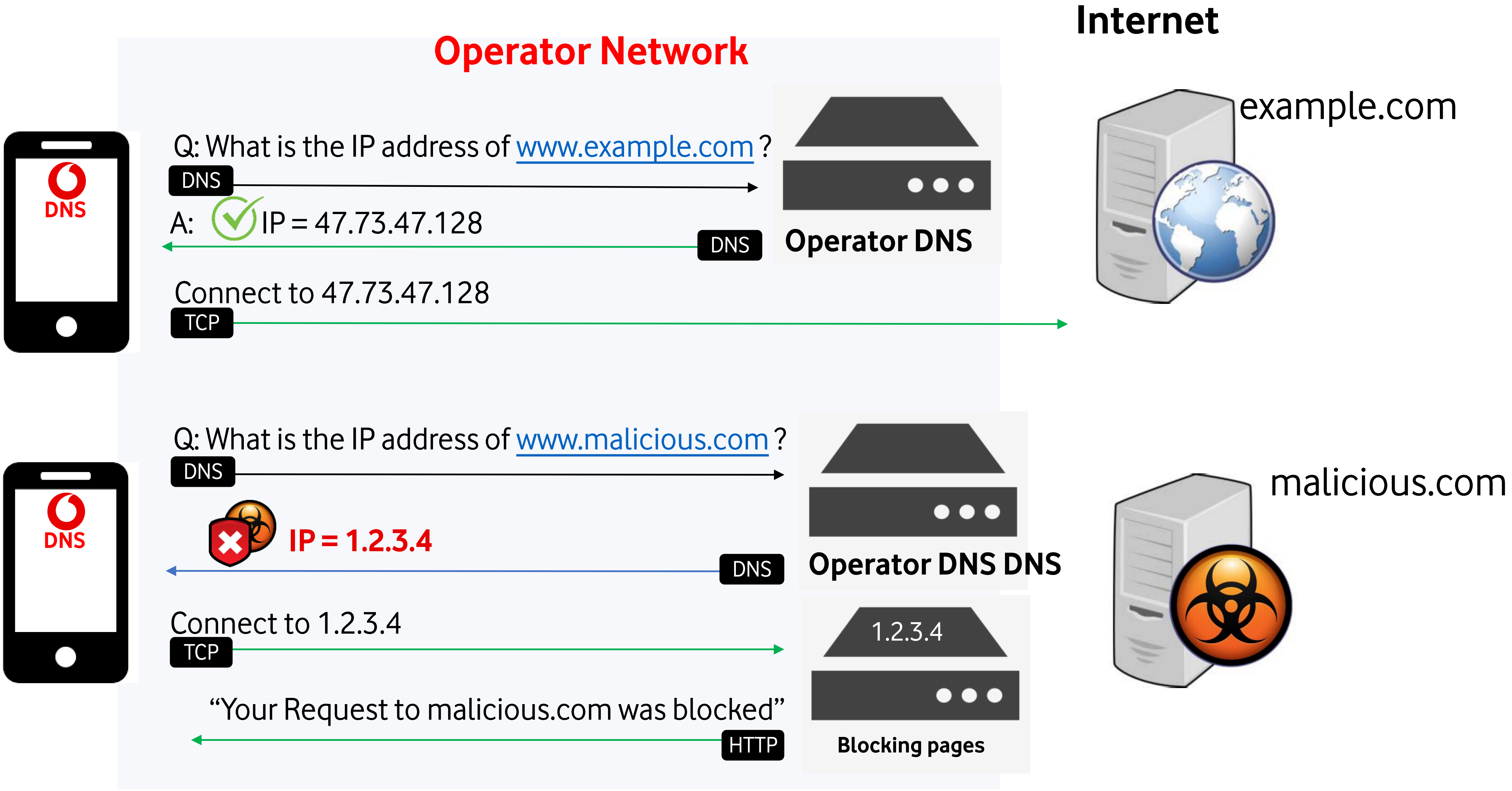
Presented by
Gianpaolo Scalone & Ralf Weber

Blocking user experience

For customers with Network based security products

(e.g. Vodafone Secure Net)

Traffic flow for network based anti malware service



Internet

Operator Network

Q: What is the IP address of www.example.com ?

DNS

A: ✓ IP = 47.73.47.128

DNS

Operator DNS

example.com

Connect to 47.73.47.128

TCP

Q: What is the IP address of www.malicious.com ?

DNS

IP = 1.2.3.4

DNS

Operator DNS DNS

malicious.com

Connect to 1.2.3.4

TCP

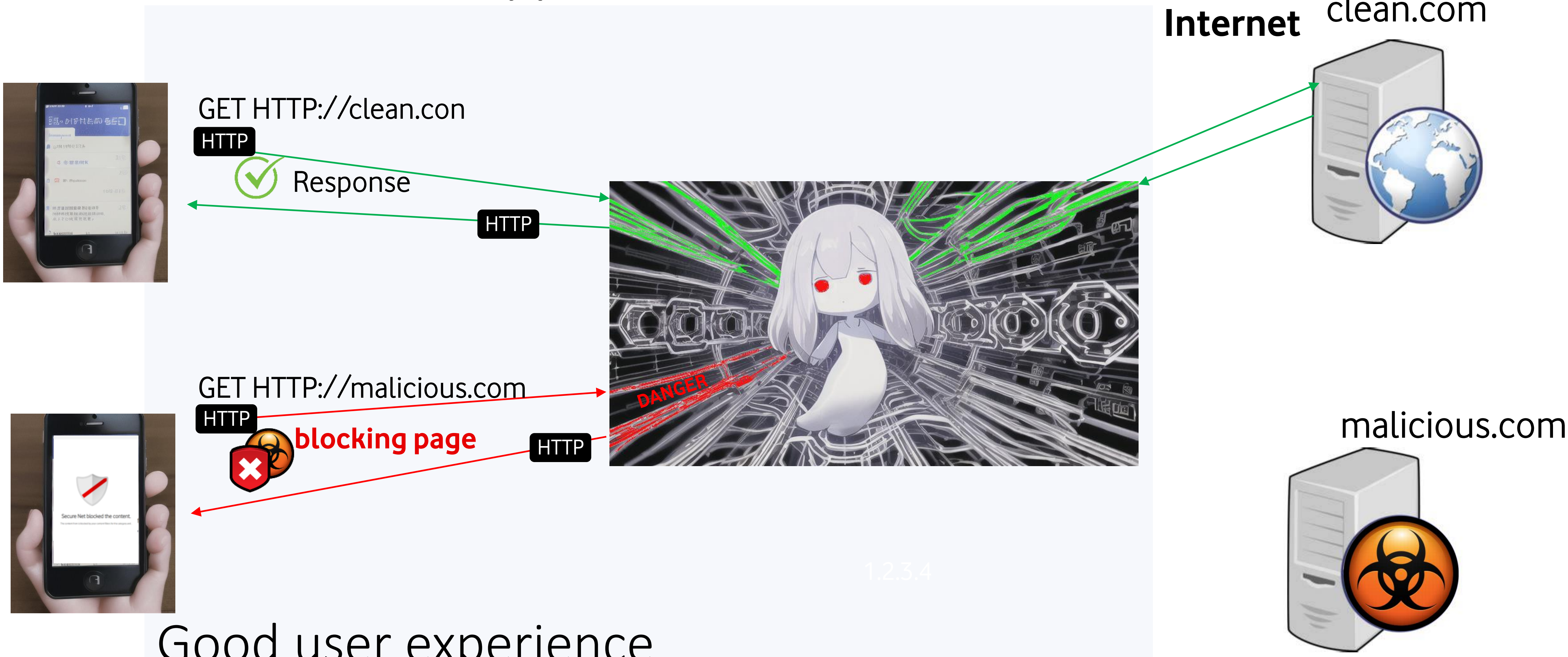
1.2.3.4

“Your Request to malicious.com was blocked”

HTTP

Blocking pages

Before the encryption era

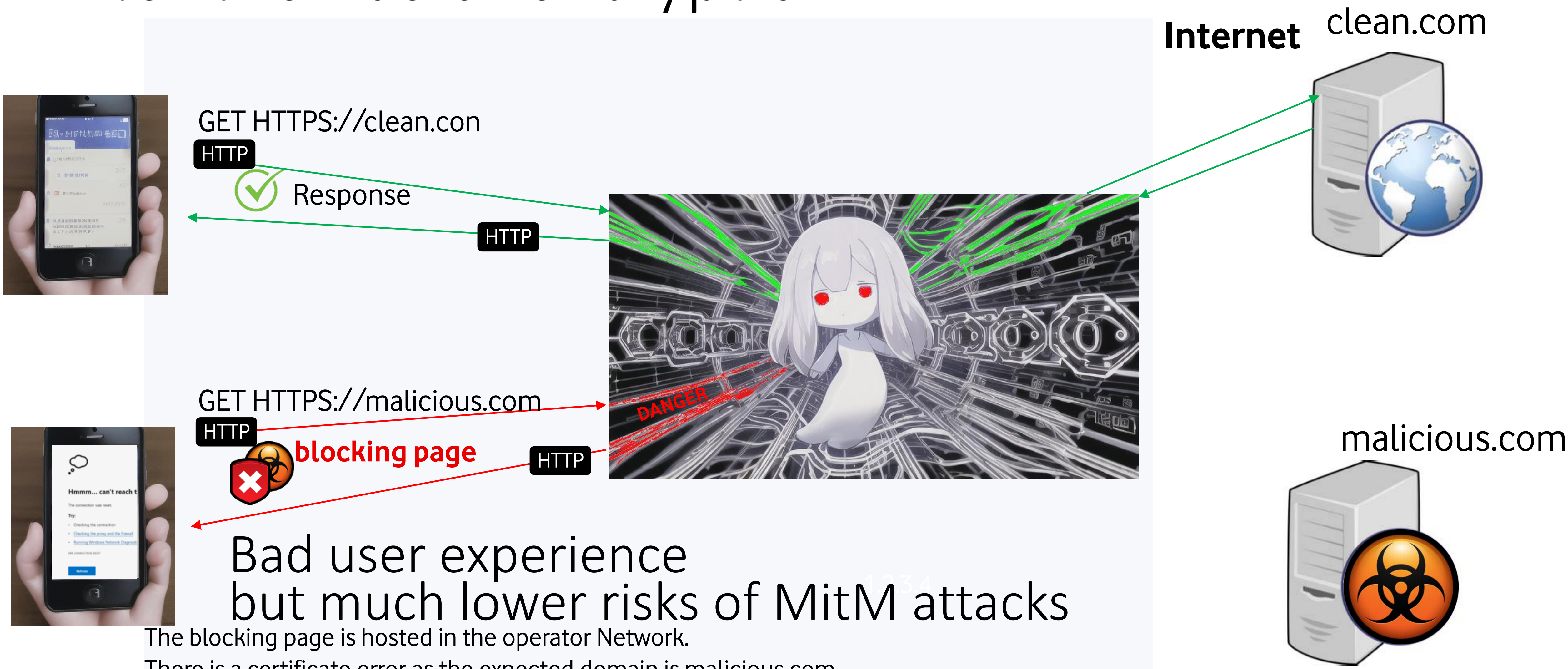


Good user experience
but high risks of MitM attacks

Our customers understood the reason of the blocking

Resulting in more customer awareness and better user experience

After the rise of encryption



Internet

clean.com

GET HTTPS://clean.con

HTTP

Response

HTTP

GET HTTPS://malicious.com

HTTP

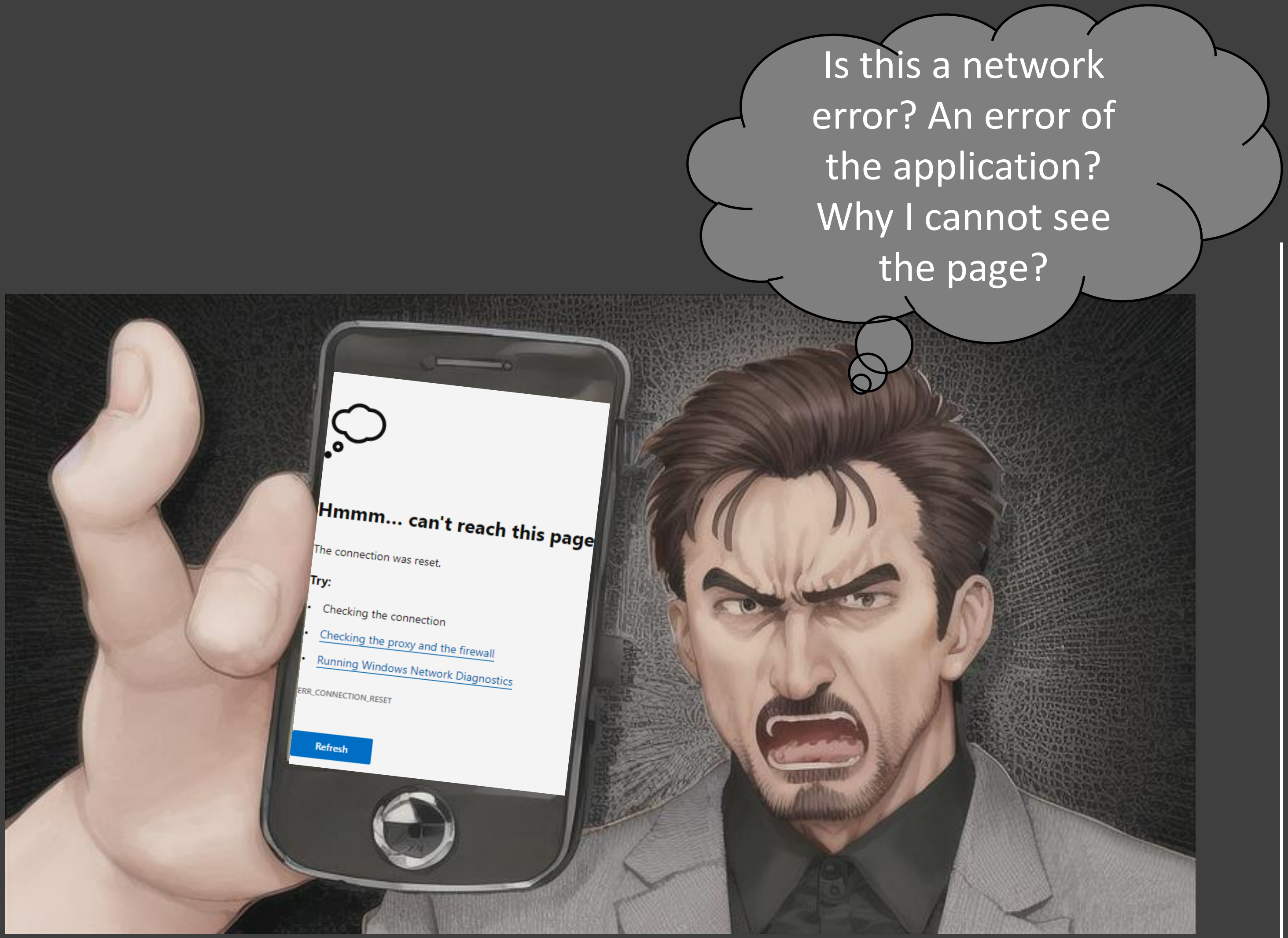
blocking page

HTTP

malicious.com

Bad user experience
but much lower risks of MitM attacks

The blocking page is hosted in the operator Network.
There is a certificate error as the expected domain is malicious.com
but the effective domain belongs to the operator,
so a browser error is presented instead of the blocking page


Is this a network error? An error of the application? Why I cannot see the page?
Hmmm... can't reach this page
The connection was reset.
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_RESET
Refresh

Network based blocking:

The customer doesn’t understand why he cannot reach the destination

BUT…

…with DoH there are the basis to implement a better user experience

DNS extended errors – RFC 8914 & Structured Error Data for Filtered DNS

Vodafone Network

Internet

clean.com

GET HTTP://clean.con

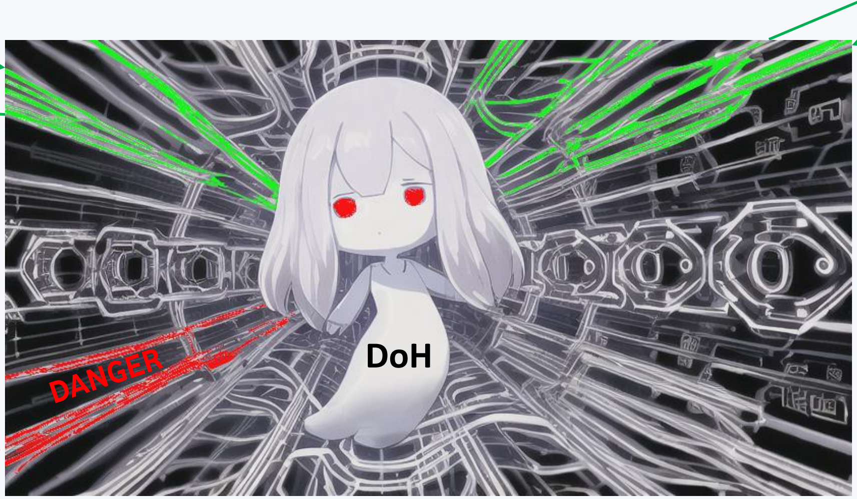
DNS

✓ Response

DNS

HTTPS

HTTPS

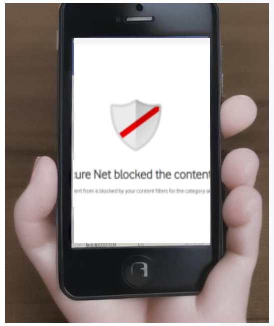


GET HTTP://malicious.com

DNS

blocking page

DNS



malicious.com

Secure NET
DNS based

Good user experience
Without risks of MitM attacks

Extended DNS Error Code 15 – Blocked

Reason: Malware C&C

Provider: Vodafone Internet Services

The DNS message contains the reason of blocking. The browser may show the blocking page via a plugin (our demo) or better via direct managent of DNS errors

Here’s how it looks under the cover

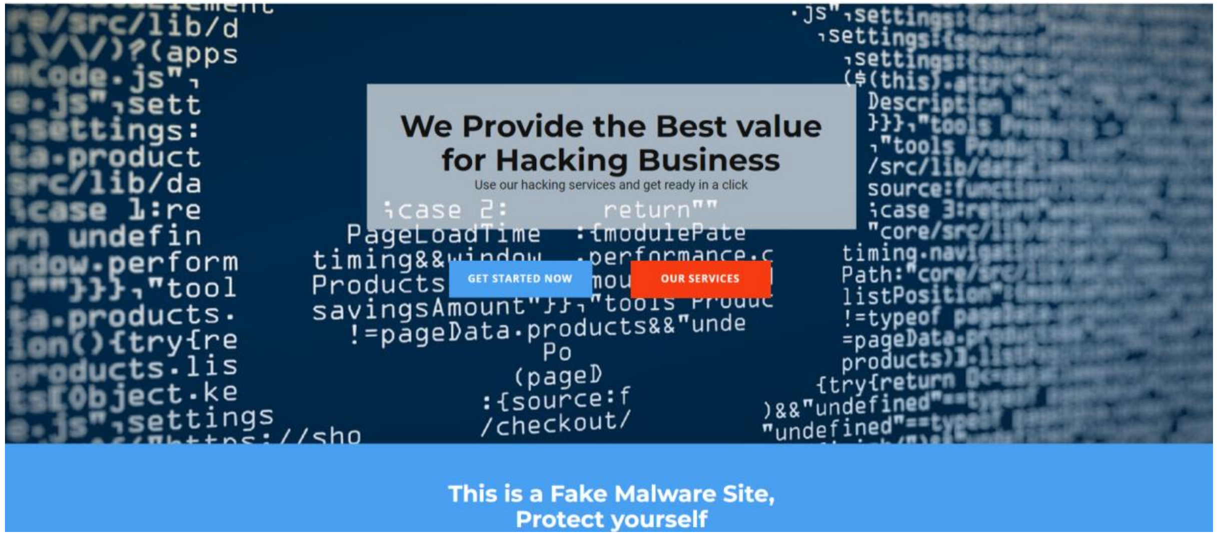
```
zsh ❯ dig malw.scalone.eu +https @cns01-euce-4haj15.002.dev.4haj15.spscld.net

; <<>> DiG 9.18.9 <<>> malw.scalone.eu +https @cns01-euce-4haj15.002.dev.4haj15.spscld.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 24987
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; EDE: 17 (Filtered): ({ "c": ["https://blocking.vodafone.com/blockpage?list=malwarecc"], "s": 1,"j": "Malware
C&C", "o": "Vodafone Internet Services" })
;; QUESTION SECTION:
;malw.scalone.eu.             IN       A

;; Query time: 72 msec
;; SERVER: 2a01:7e01::f03c:93ff:fe27:dfba#443(cns01-euce-4haj15.002.dev.4haj15.spscld.net) (HTTPS)
;; WHEN: Wed Mar 15 07:31:05 CET 2023
;; MSG SIZE  rcvd: 179
```

Thanks to RFC 8914 & Structured Error Data for Filtered DNS now it is possible to enrich DNS errors with the reason of blocking

We have designed a plugin for the Chrome browser that can intercept the DNS request and in case of blocking read the extended DNS error and show the proper blocking page

User experience – protection disabled

the user can reach the malicious site



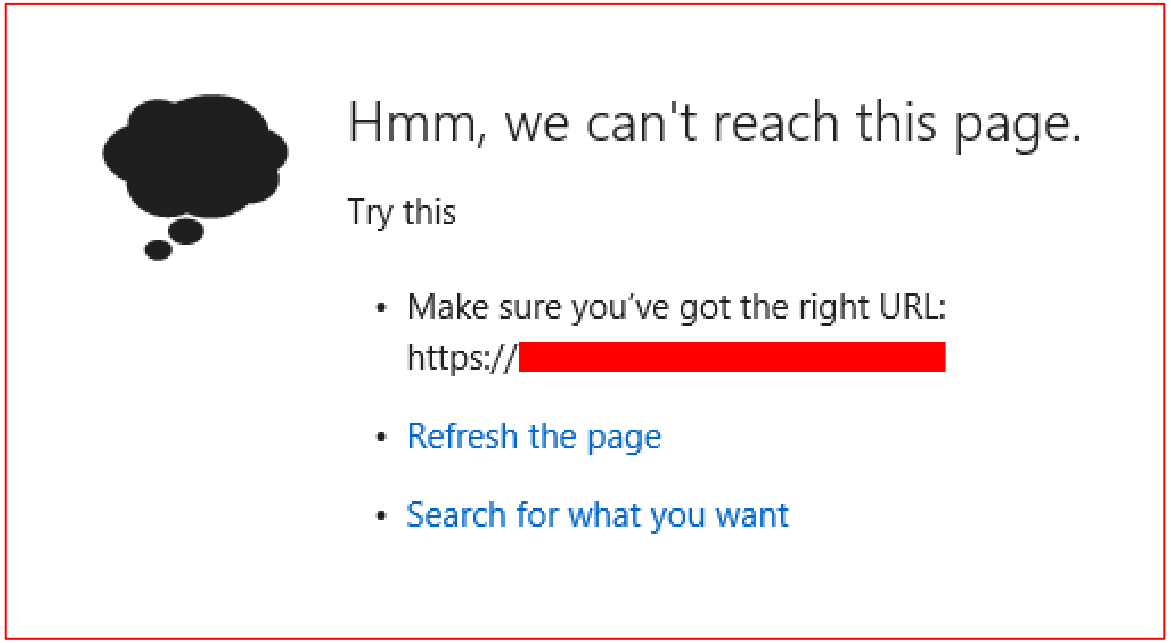
We Provide the Best value for Hacking Business

Use our hacking services and get ready in a click

This is a Fake Malware Site, Protect yourself

User experience - Protection enabled without the plugin:

Access to malicious domain is blocked but the customer doensn’t knows why



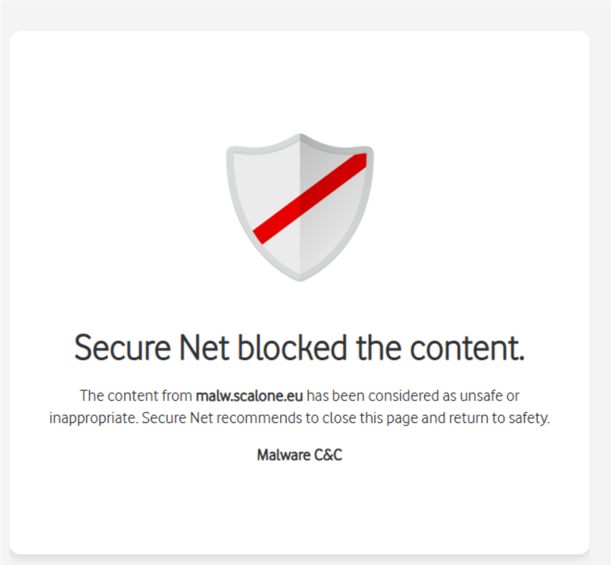
Hmm, we can't reach this page.

Try this

- Make sure you’ve got the right URL: https://[redacted]
- Refresh the page
- Search for what you want

User experience - Protection enabled with the plugin:

Access to malicious domain is blocked and an explaining blocking page is presented



Secure Net blocked the content.

The content from **malw.scalone.eu** has been considered as unsafe or inappropriate. Secure Net recommends to close this page and return to safety.

Malware C&C

The Standard allows the server-side implementation of extended DNS errors. We are presenting a plugin that shows the error, best approach would be integration in the browser, for a better user experience.

Thank you