

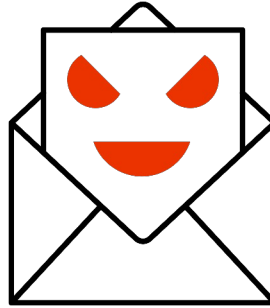
Cascading Spy Sheets

Exploiting the Complexity of Modern CSS for
Email and Browser Fingerprinting

Leon Trampert, Daniel Weber, Lukas Gerlach, Christian Rossow, Michael Schwarz

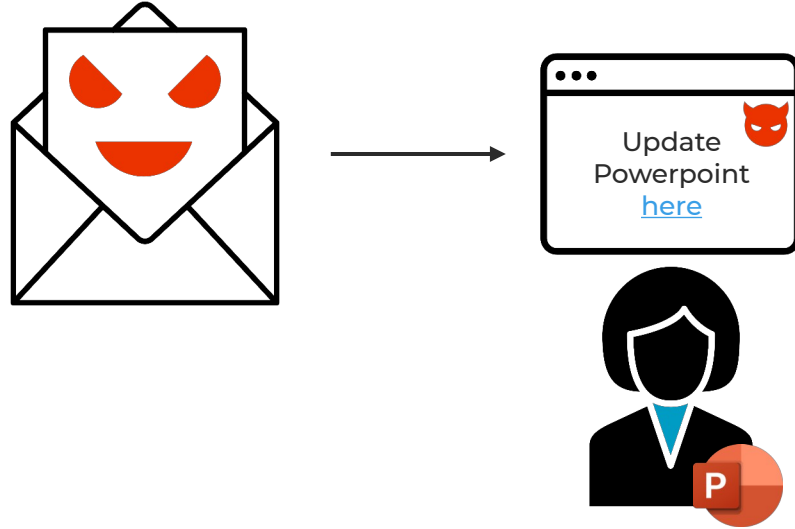


Hidden Phishing Emails



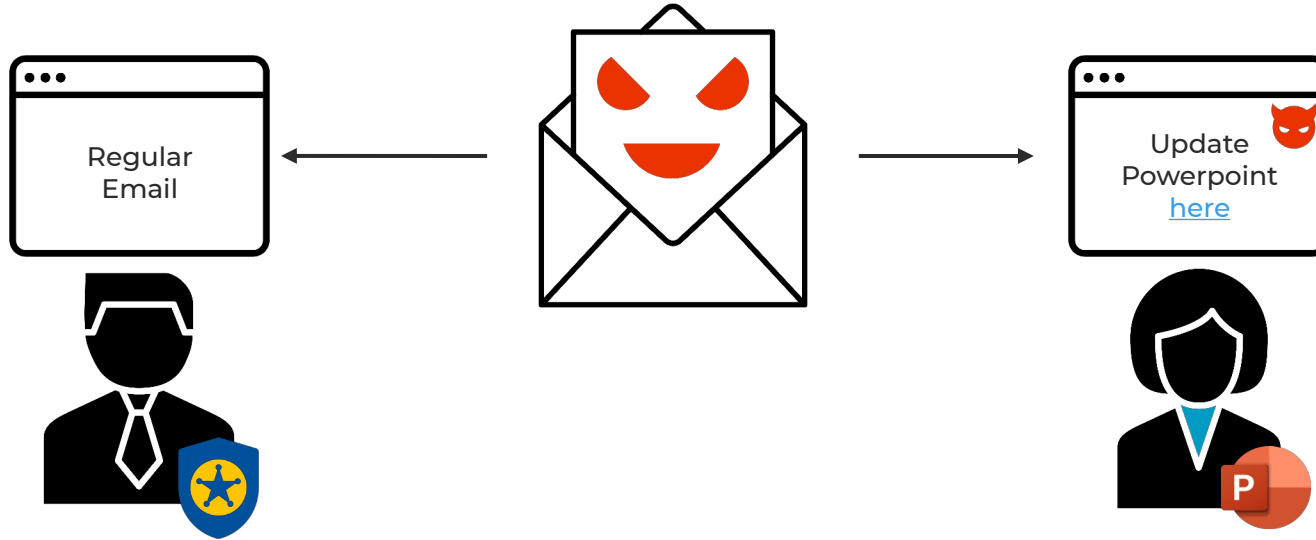


Hidden Phishing Emails





Hidden Phishing Emails





Browser Fingerprinting



Browser Fingerprinting





Browser Fingerprinting



`<script>`





Browser Fingerprinting

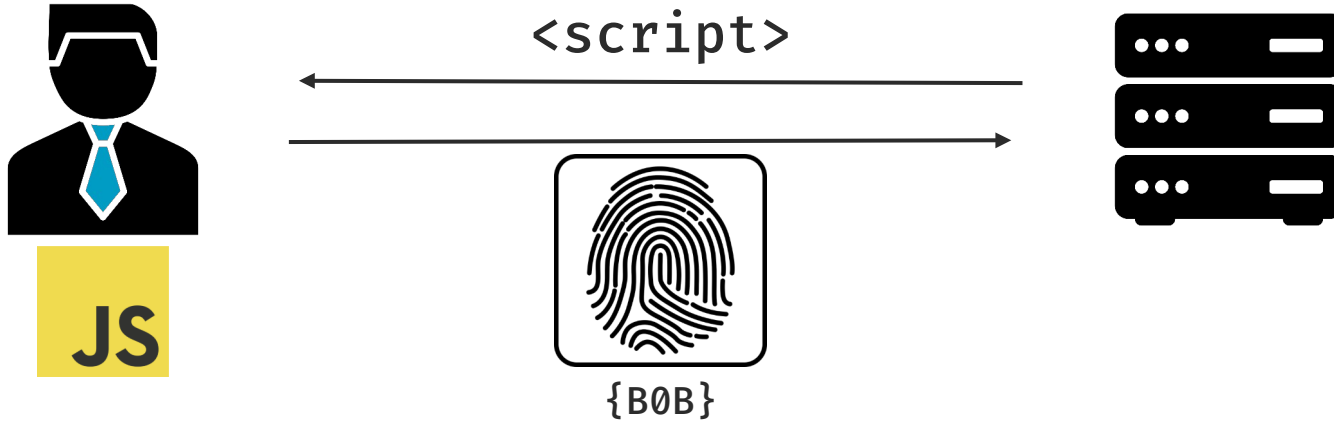


`<script>`





Browser Fingerprinting





Current techniques rely on JavaScript!



Contexts without JavaScript



Contexts without JavaScript



Tor Browser



Contexts without JavaScript



Tor Browser



NoScript



Contexts without JavaScript



Tor Browser



NoScript



Email Clients

Contexts without JavaScript



Tor Browser



NoScript



Email Clients

Can we fingerprint here?



CSS – Deep Dive



Cascading Style Sheets (CSS)

```
button {  
  color: red;  
  background-image:  
    url(/pattern.png);  
  width: calc(100% - 20px);  
}  
  
@media (min-width: 720px) {  
  button {  
    width: 100%;  
  }  
}
```



Cascading Style Sheets (CSS)

```
button {  
  color: red;  
  background-image:  
    url(/pattern.png);  
  width: calc(100% - 20px);  
}  
  
@media (min-width: 720px) {  
  button {  
    width: 100%;  
  }  
}
```

1. Properties



Cascading Style Sheets (CSS)

```
button {  
  color: red;  
  background-image:  
    url(/pattern.png);  
  width: calc(100% - 20px);  
}  
  
@media (min-width: 720px) {  
  button {  
    width: 100%;  
  }  
}
```

1. Properties
2. Functions



Cascading Style Sheets (CSS)

```
button {  
  color: red;  
  background-image:  
    url(/pattern.png);  
  width: calc(100% - 20px);  
}  
  
@media (min-width: 720px) {  
  button {  
    width: 100%;  
  }  
}
```

1. Properties
2. Functions
3. Selectors



Cascading Style Sheets (CSS)

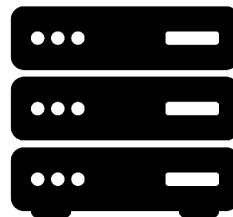
```
button {  
  color: red;  
  background-image:  
    url(/pattern.png);  
  width: calc(100% - 20px);  
}  
  
@media (min-width: 720px) {  
  button {  
    width: 100%;  
  }  
}
```

1. Properties
2. Functions
3. Selectors
4. @-rules



CSS-to-Server Communication

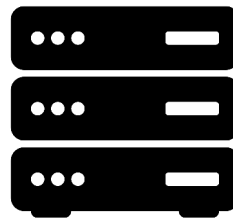
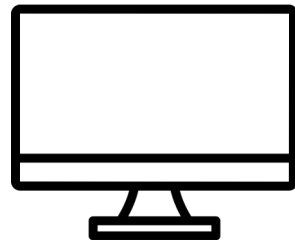
```
button {  
  background-image:  
    url(/small.png);  
}  
  
@media (min-width: 720px) {  
  button {  
    background-image:  
      url(/large.png);  
  }  
}
```





CSS-to-Server Communication

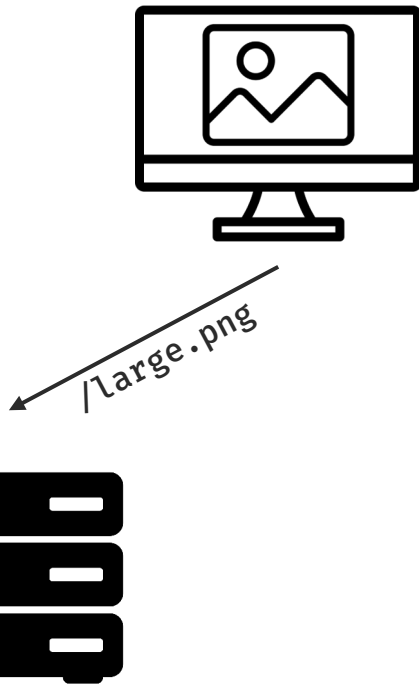
```
button {  
  background-image:  
    url(/small.png);  
}  
  
@media (min-width: 720px) {  
  button {  
    background-image:  
      url(/large.png);  
  }  
}
```





CSS-to-Server Communication

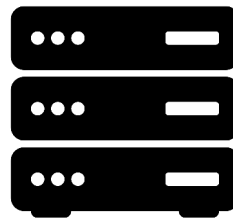
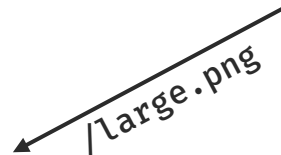
```
button {  
  background-image:  
    url(/small.png);  
}  
  
@media (min-width: 720px) {  
  button {  
    background-image:  
      url(/large.png);  
  }  
}
```





CSS-to-Server Communication

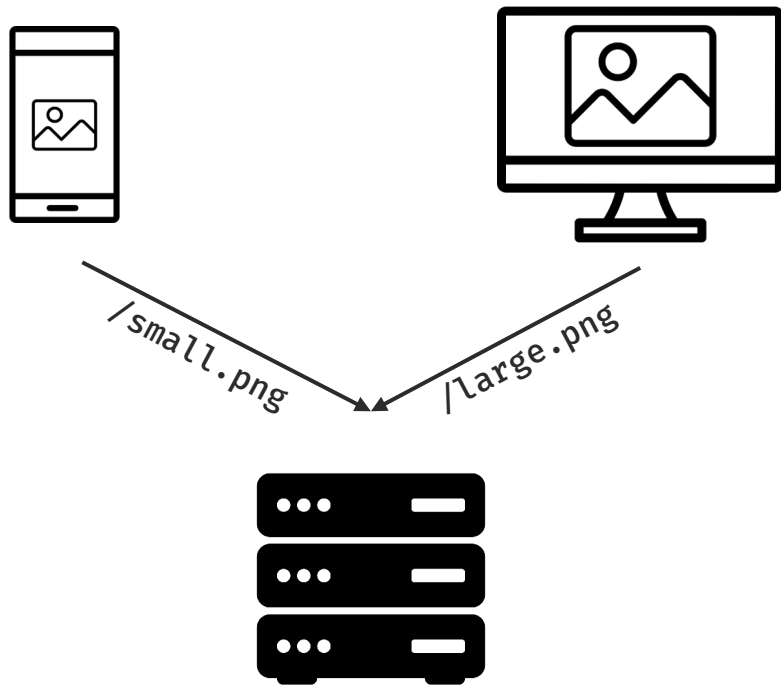
```
button {  
  background-image:  
    url(/small.png);  
}  
  
@media (min-width: 720px) {  
  button {  
    background-image:  
      url(/large.png);  
  }  
}
```





CSS-to-Server Communication

```
button {  
  background-image:  
    url(/small.png);  
}  
  
@media (min-width: 720px) {  
  button {  
    background-image:  
      url(/large.png);  
  }  
}
```





Fingerprinting with @rules



@container

```
@container (width > 400px)
{
  p {
    font-size: 16px;
    background-color: blue;
  }
}
```



@container

```
@container (width > 400px)
{
  p {
    font-size: 16px;
    background-color: blue;
  }
}
```

@container allows querying the **width** of a container element.



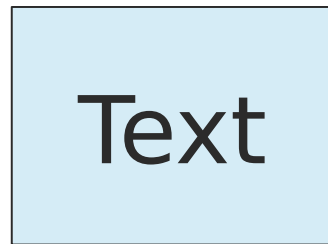
@container

```
@container (width > 400px)
{
  p {
    font-size: 16px;
    background-color: blue;
  }
}
```

@container allows querying the **width** of a container element.



250px



500px



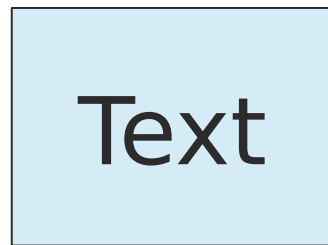
@container

```
@container (width > 400px)
{
  p {
    font-size: 16px;
    background-color: blue;
  }
}
```

@container allows querying the **width** of a container element.



250px



500px

How is this useful?



Width Measurements!



Width Measurements!

Browse... No file selected.

Durchsuchen... Keine Datei ausgewählt.

Client Language



Width Measurements!

Browse... No file selected.

dd . mm . yyyy 

Durchsuchen... Keine Datei ausgewählt.

mm / dd / yyyy 

Client Language

Browser / OS



Width Measurements!

Browse... No file selected.

dd . mm . yyyy 📅

The quick brown fox jumps...

Durchsuchen... Keine Datei ausgewählt.

mm / dd / yyyy 📅

The quick brown fox jumps...

Client Language

Browser / OS

Fonts



Fingerprinting with Functions



Math Functions – Architecture

```
calc(1px * (pi * pi + pi))
```





Math Functions – Architecture

```
calc(1px * (pi * pi + pi))
```



13





Math Functions – Architecture

```
calc(1px * (pi * pi + pi))
```



13



13.0104



Fingerprinting Plugins

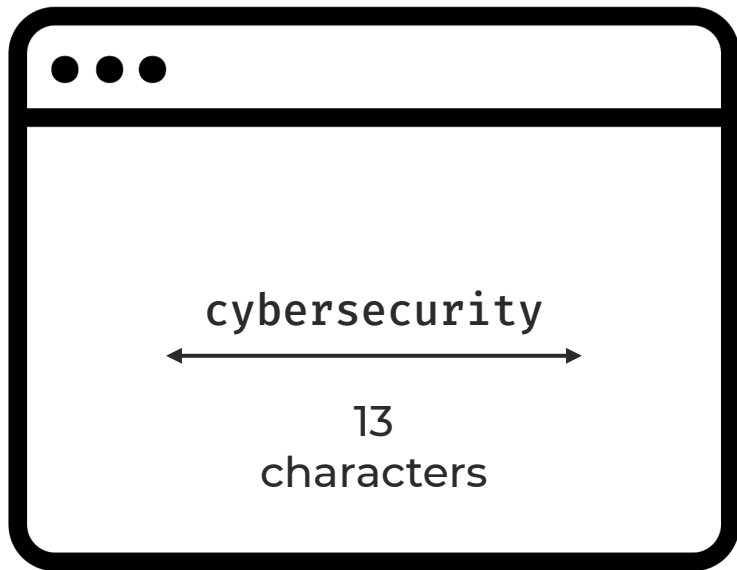


Plugin Detection – Google Translate



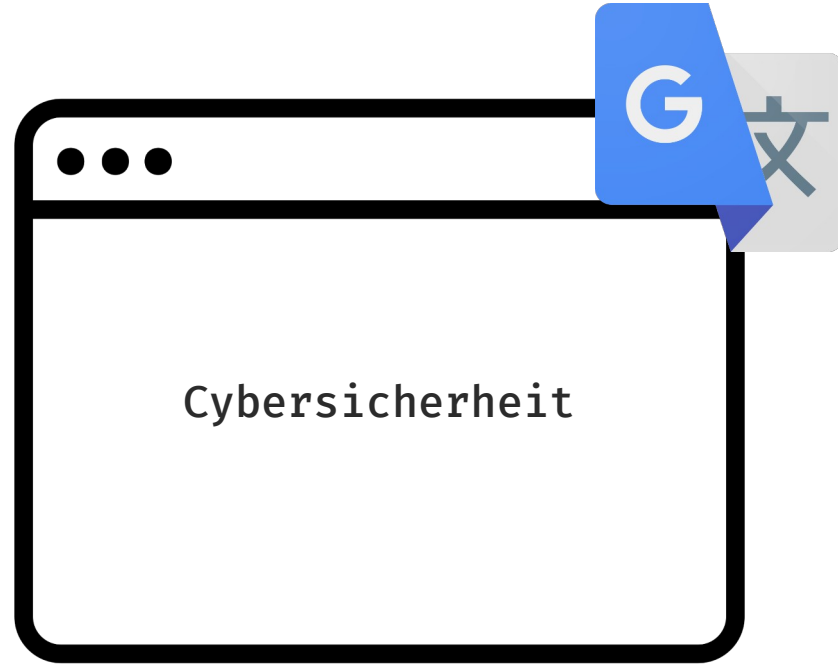
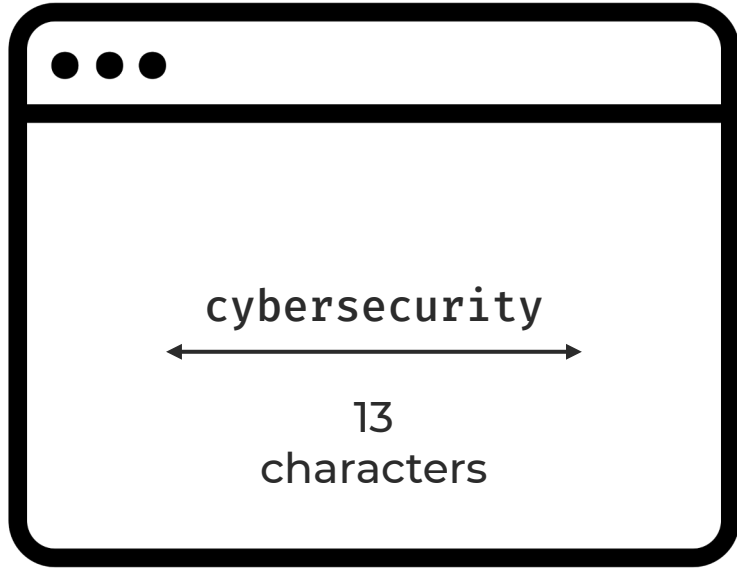


Plugin Detection – Google Translate



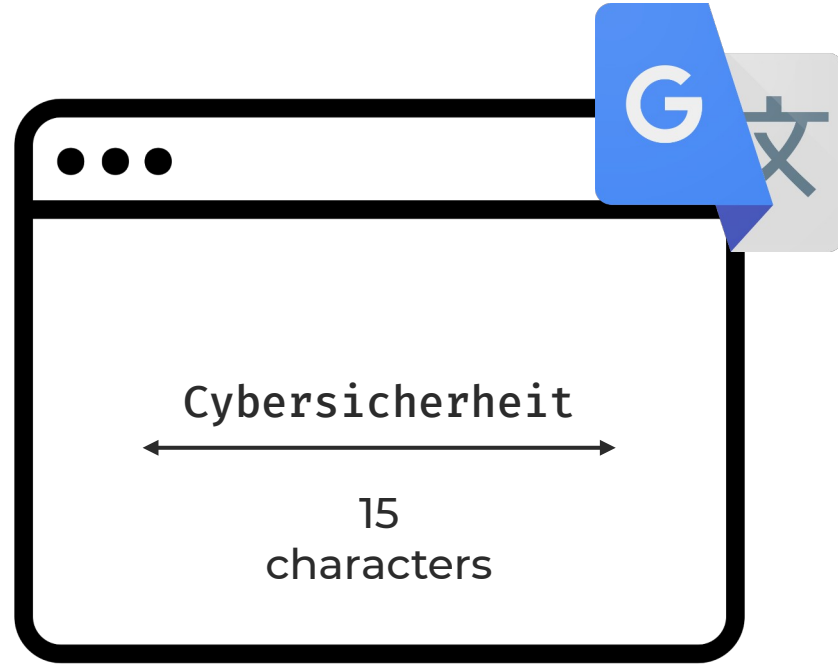
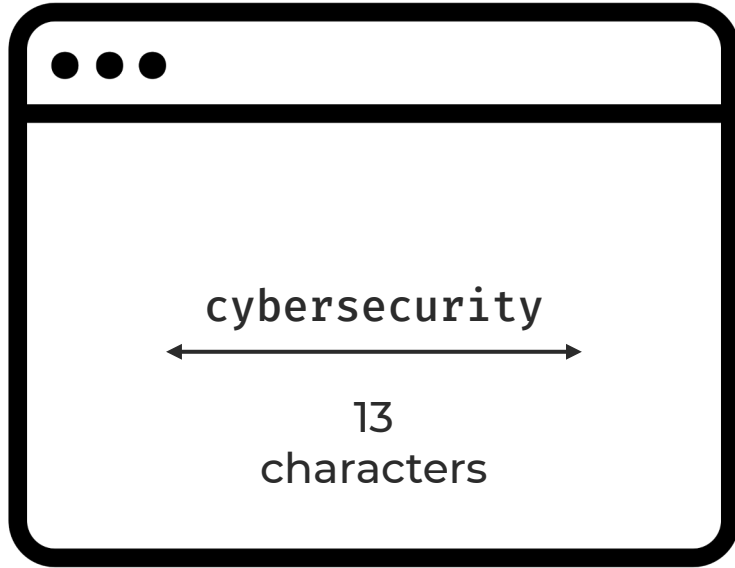


Plugin Detection – Google Translate





Plugin Detection – Google Translate





CSS Fingerprints



**System
Information**



CSS Fingerprints



**System
Information**



**Hardware
Information**



CSS Fingerprints



**System
Information**



**Hardware
Information**



**User
Information**



CSS Fingerprints



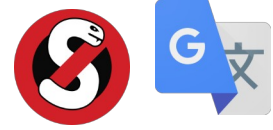
**System
Information**



**Hardware
Information**



**User
Information**



**Plugin
Detection**



CSS Fingerprints



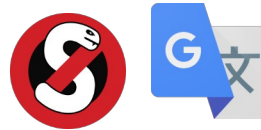
**System
Information**



**Hardware
Information**



**User
Information**



**Plugin
Detection**

It works in the browser.



What About Email Clients?



What Is an Email Client?



Webmail



What Is an Email Client?



Webmail



Desktop Clients



What Is an Email Client?



Webmail



Desktop Clients



Mobile Clients



What Is an Email Client?



Webmail



Desktop Clients



Mobile Clients



What Is an Email Client?



Webmail



Desktop Clients



Mobile Clients



What Is an Email Client?



Webmail



Desktop Clients



Mobile Clients



What Is an Email Client?



Webmail



Desktop Clients



Mobile Clients

They are essentially browsers!



HTML Emails

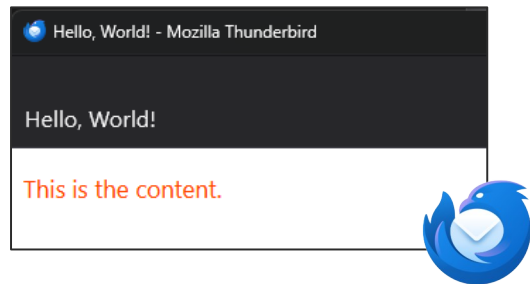
Content-Type: text/html
Subject: Hello, World!

```
<html>

  <head>
    <style>
      p { color: orangered; }
    </style>
  </head>

  <body>
    <p>This is the content.</p>
  </body>

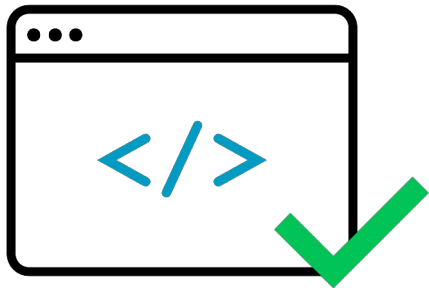
</html>
```





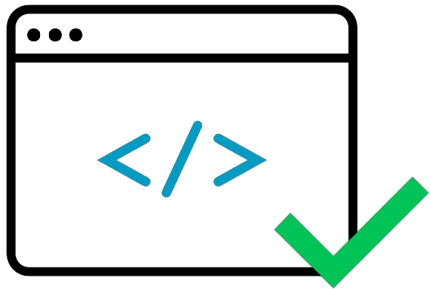
Can We Fingerprint in Emails?

Fingerprinting in Emails?



CSS Feature Availability

Fingerprinting in Emails?



CSS Feature Availability



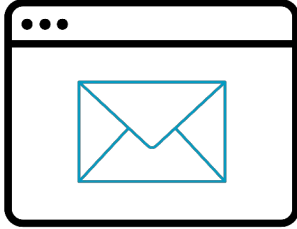
Remote Content Loading



Analysis Time



Analysis of Clients

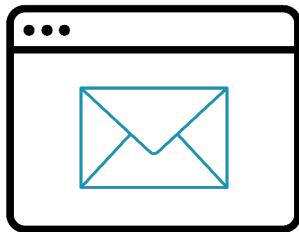


9 Webmail Clients
4 Desktop Clients
4 Android Clients
4 iOS Clients

= 21 Clients in Total

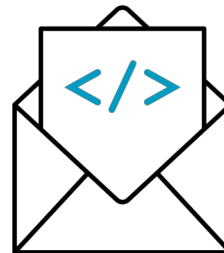


Analysis of Clients



9 Webmail Clients
4 Desktop Clients
4 Android Clients
4 iOS Clients

= 21 Clients in Total

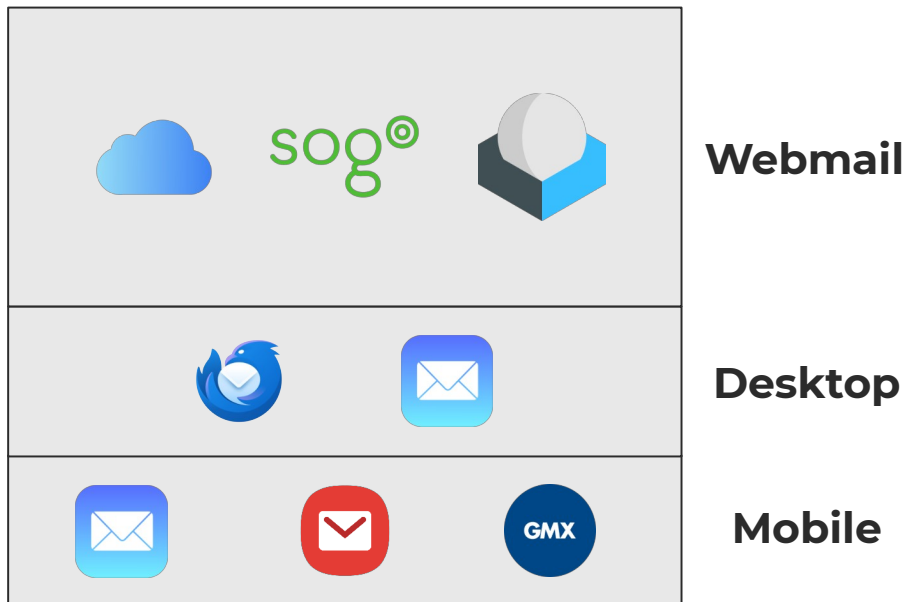


100 Test Emails

= 2.100 Emails in Total



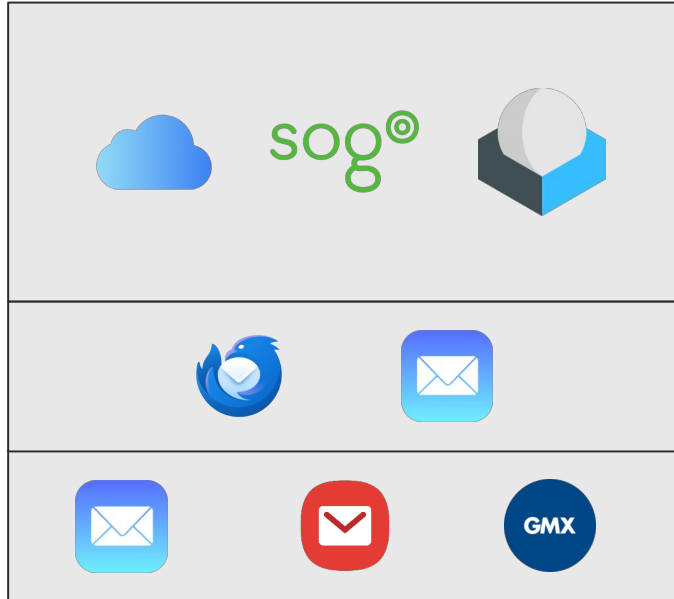
Client Behavior



Lenient Clients



Client Behavior

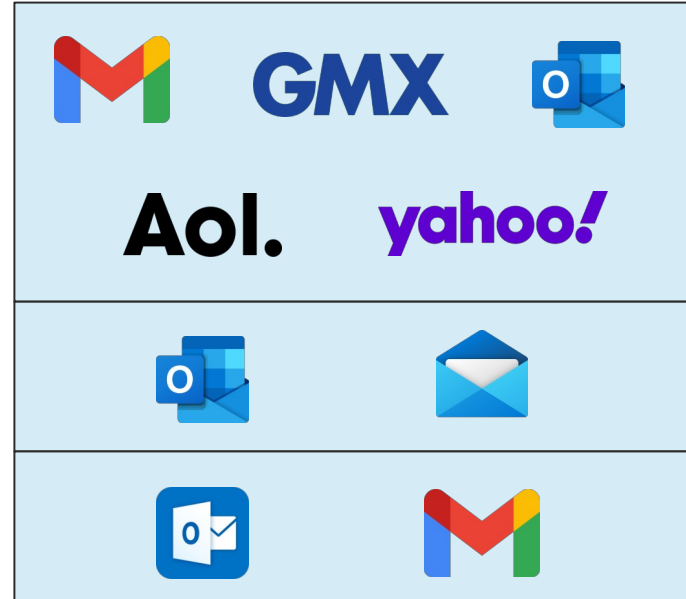


Lenient Clients

Webmail

Desktop

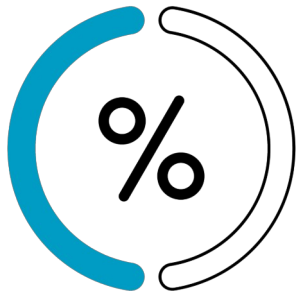
Mobile



Restrictive Clients



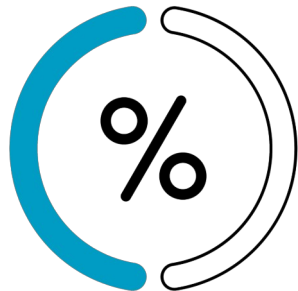
Email Client Fingerprinting



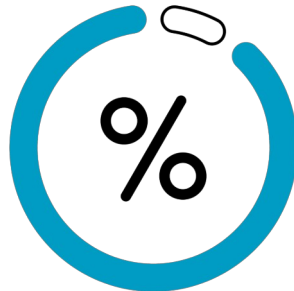
Half of clients allow **all**
techniques



Email Client Fingerprinting



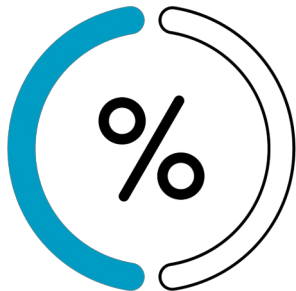
Half of clients allow **all**
techniques



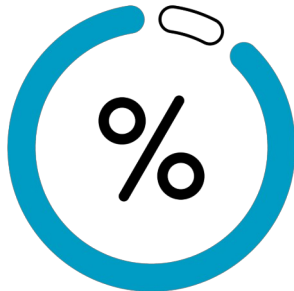
Almost all clients
allow **some**
techniques



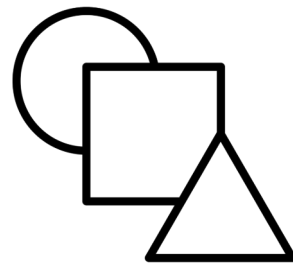
Email Client Fingerprinting



Half of clients allow **all** techniques



Almost all clients allow **some** techniques



Each client supports **different features**

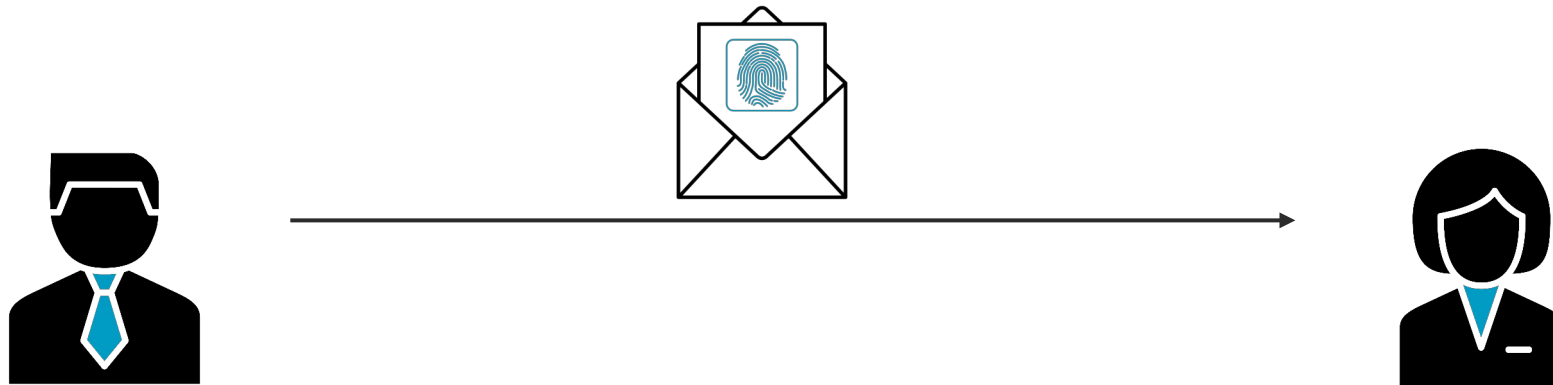


How Is Email Fingerprinting Useful?

The Good – Leak Detection



The Good – Leak Detection



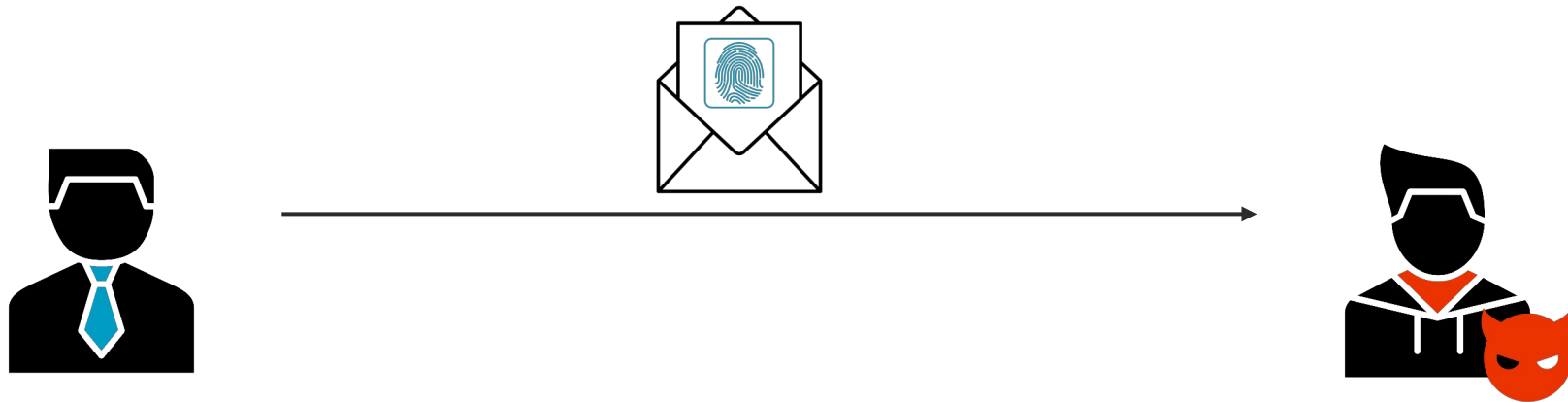
The Good – Leak Detection



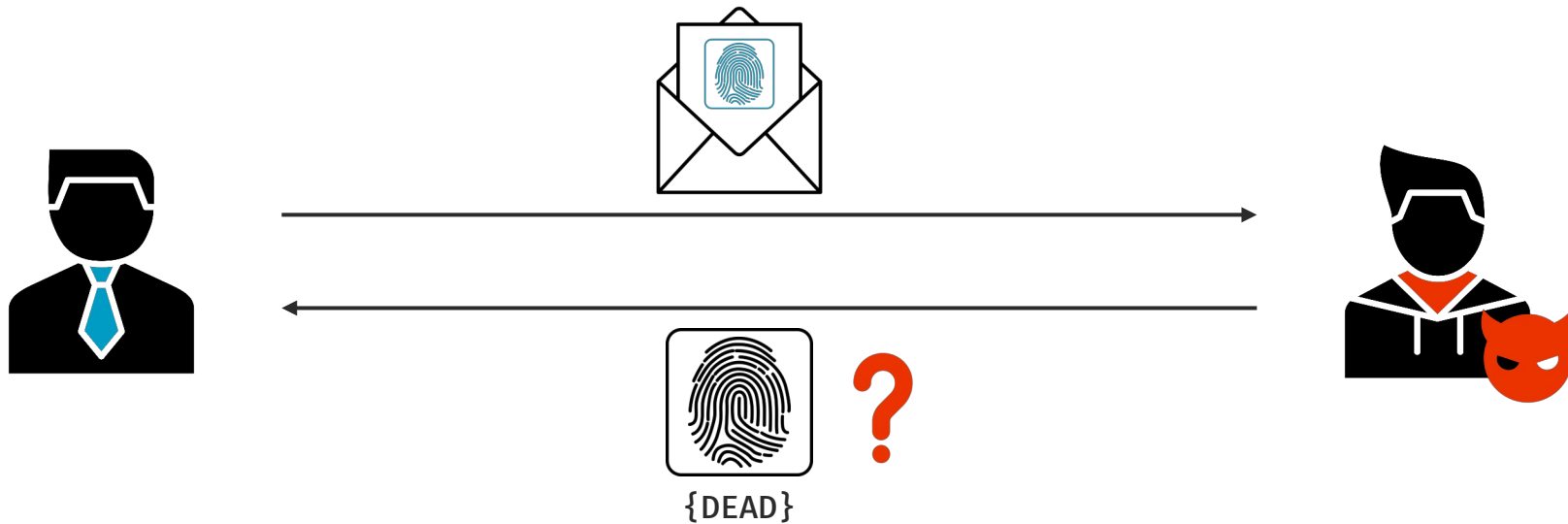
The Good – Leak Detection



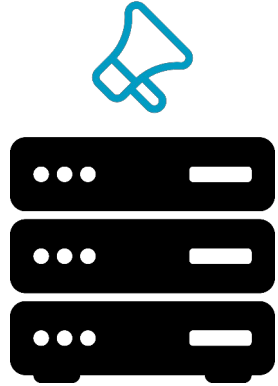
The Good – Leak Detection



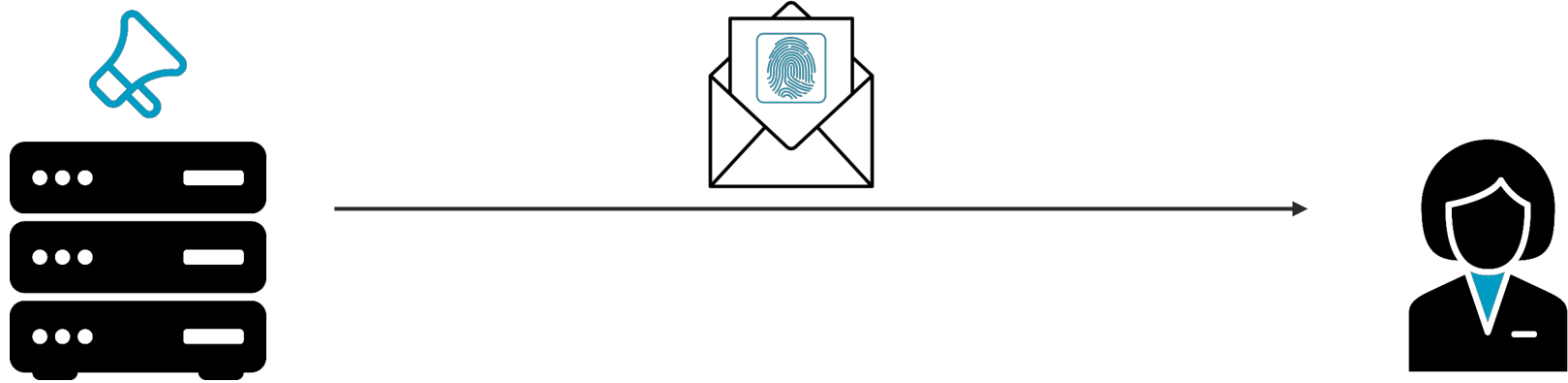
The Good – Leak Detection



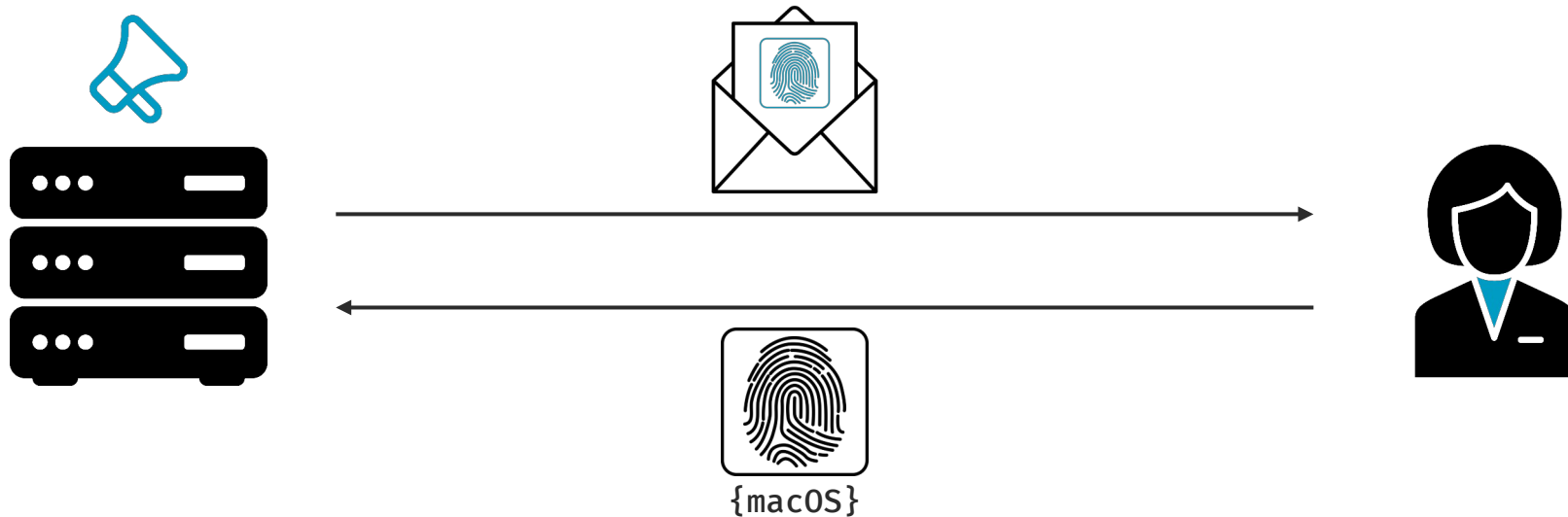
The Bad – Enhanced Tracking



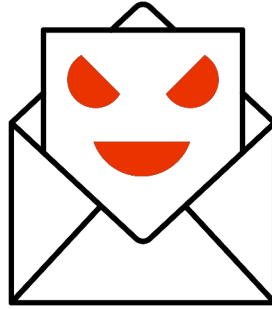
The Bad – Enhanced Tracking



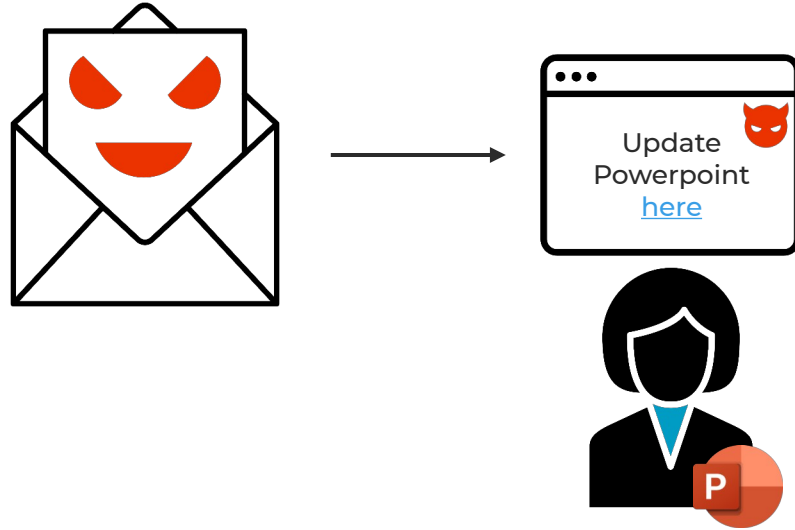
The Bad – Enhanced Tracking



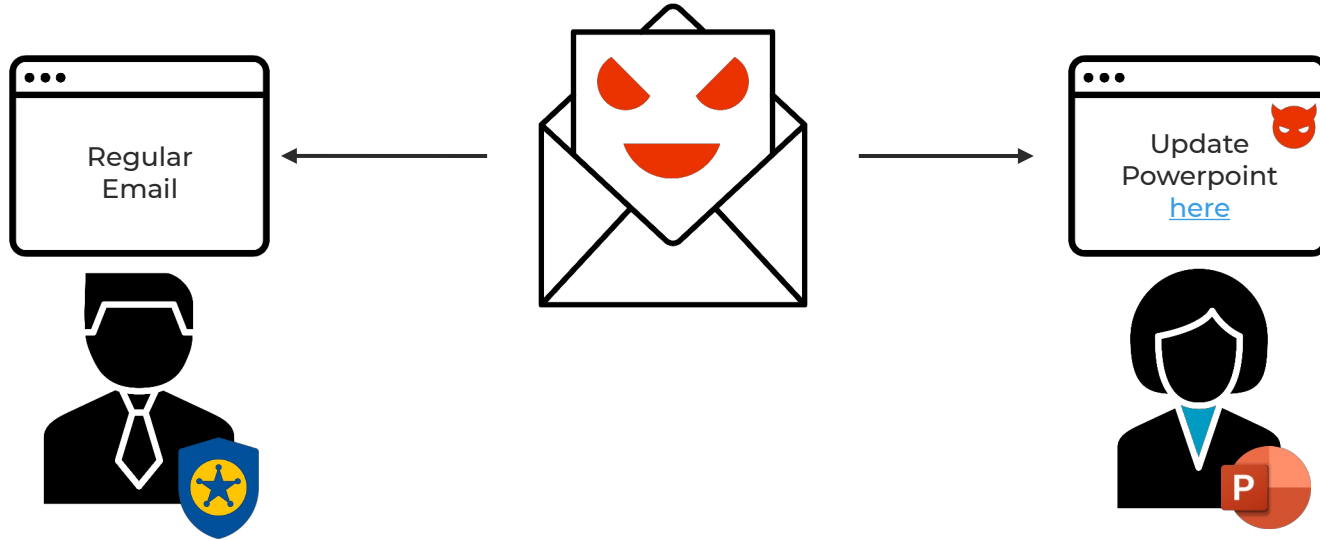
The Ugly – Spear Phishing



The Ugly – Spear Phishing



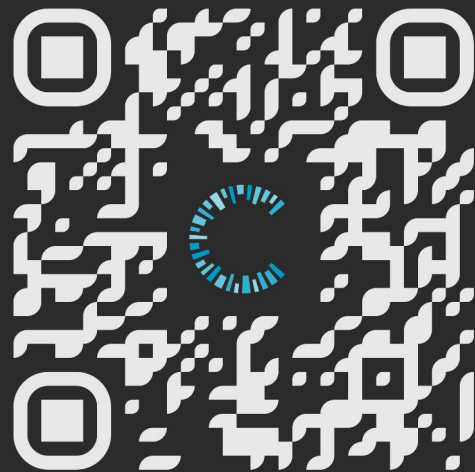
The Ugly – Spear Phishing





Wrapping Things Up

Takeaways

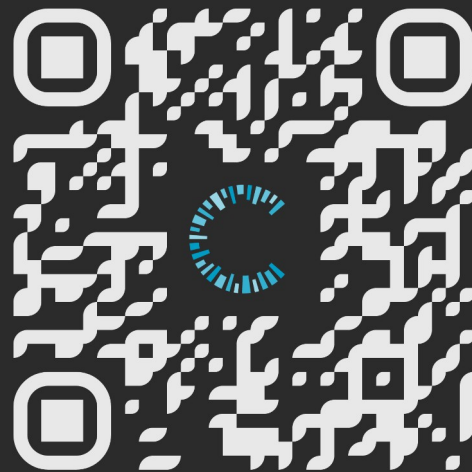


s.roots.ec/spy-sheets



Takeaways

1. Stylesheets (CSS) alone can be used for Fingerprinting.

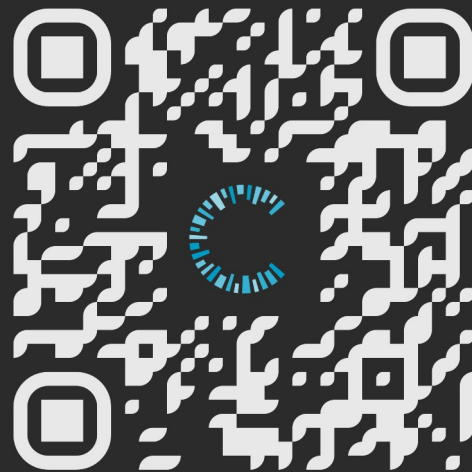


s.roots.ec/spy-sheets



Takeaways

1. Stylesheets (CSS) alone can be used for Fingerprinting.
2. CSS-based Fingerprinting can even be used in emails.



s.roots.ec/spy-sheets