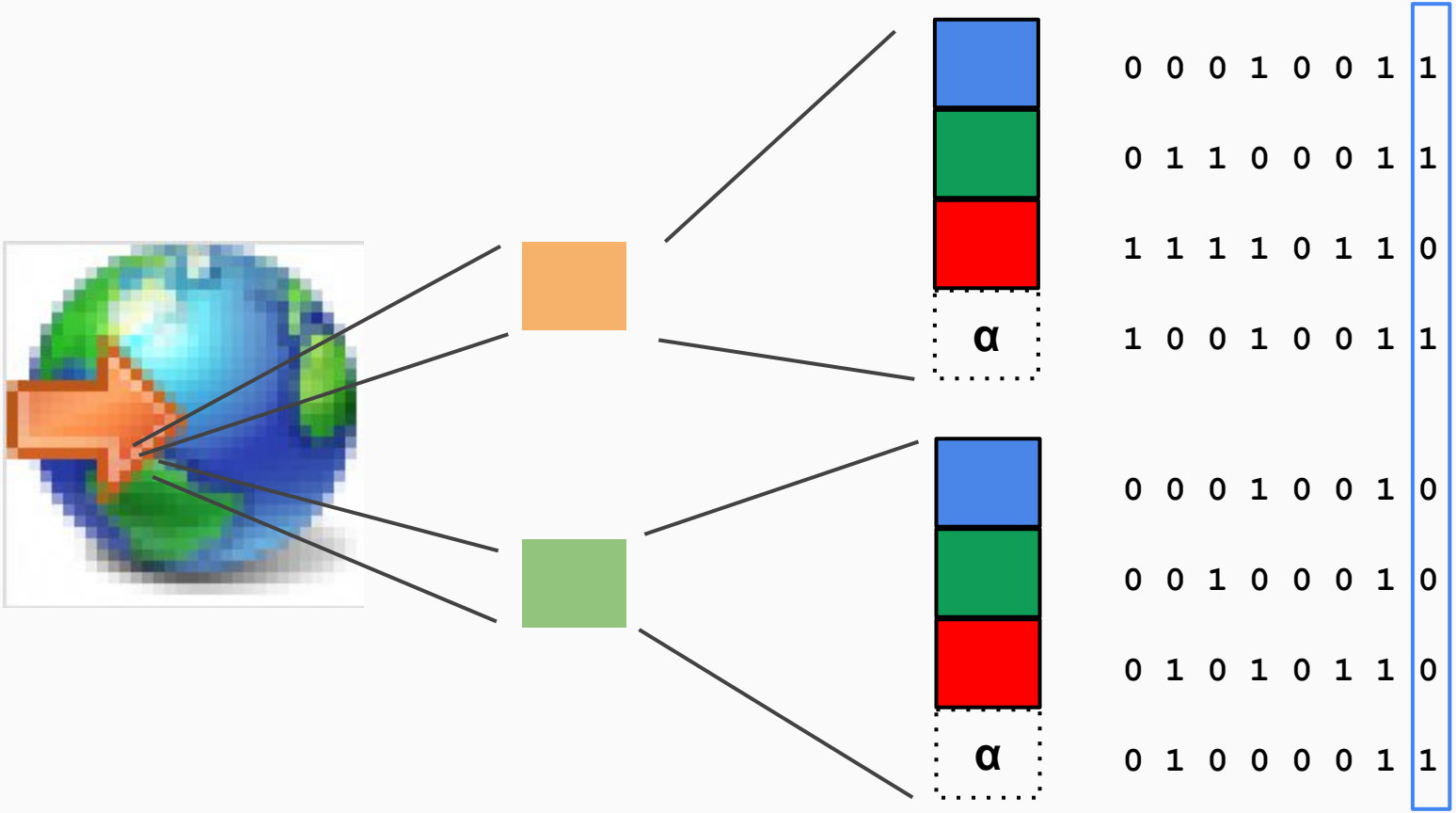
Stegoloader

Malware using steganography to hide next-stage code

Pierre-Marc Bureau
Chris Dietrich

Least Significant Bit Steganography



Stegoloader Image Processing

PNG Image

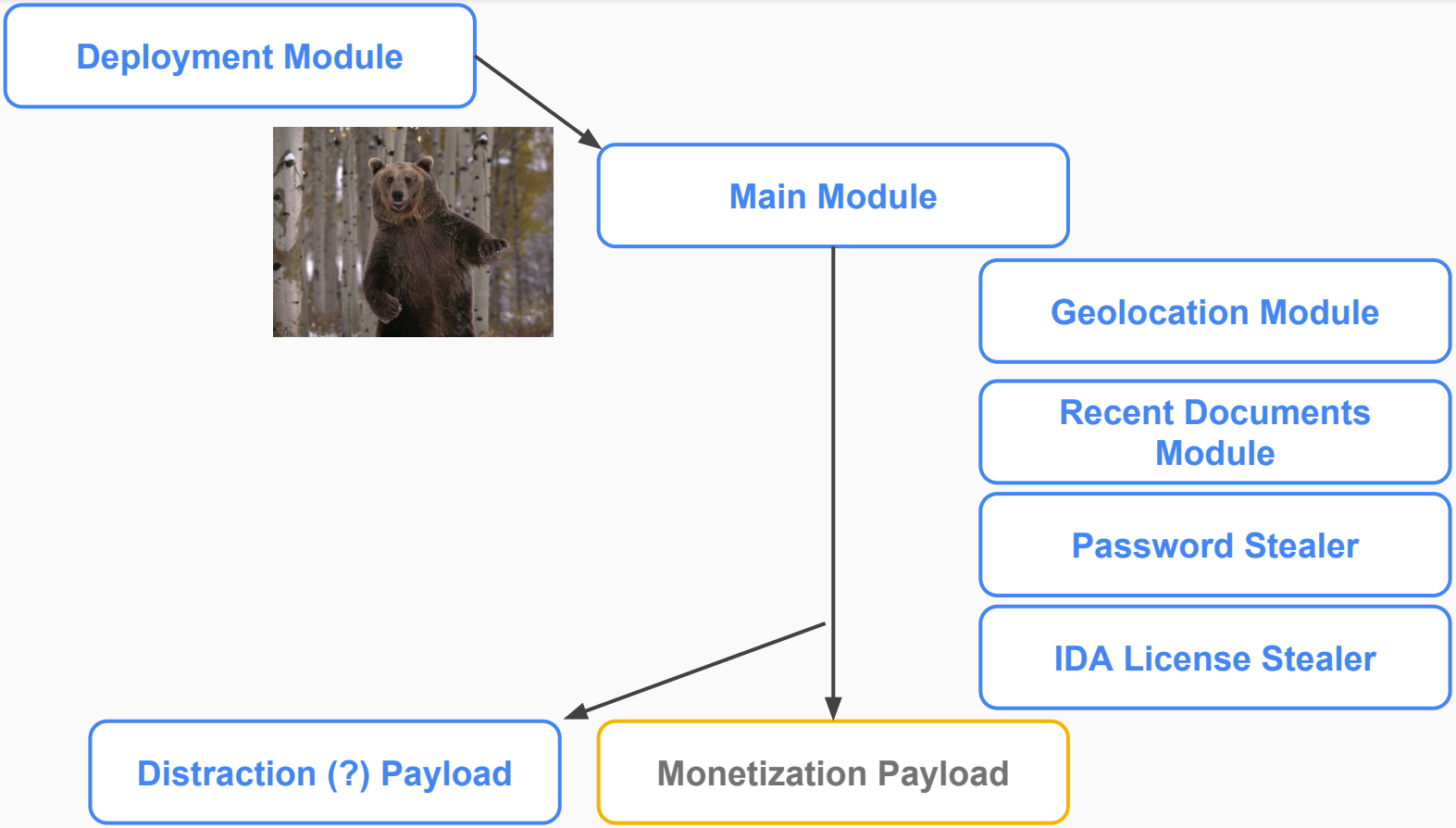
LSB extraction

RC4 decryption

Code

```
push    ebp
mov     ebp, esp
sub     esp, 24h
push    esi
push    edi
push    14h
...
```

Stegoloader Module Interaction



Thank you!

Pierre-Marc Bureau
Chris Dietrich