# Security incident report

## Section 1: Identify the network protocol involved in the incident

“A lot of traffic on port 80” - port 80 is for HTTP

Protocols involved in the incident: 52444, 36086, 56378

None of them are assigned by IANA

## Section 2: Document the incident

"According to the logs, the original port of the client computer was 52444, which changed to 36086 after being redirected through the DNS domain. After downloading a malicious file from the site “yummyrecipesforme.com.http” (http - port 80), the port is set back to 52444, the original one, from which the computer again tries to connect to the site through the DNS domain. The malware redirects the computer, which this time uses port 56378, to the spoofed domain “greatrecipesforme.com”, successfully establishing the connection."

As a result, the intruder could have obtained user login credentials, infected their computers, or gained financial benefits through fraudulent product purchases.

## Section 3: Recommend one remediation for brute force attacks

I primarily recommend changing passwords across the entire company and implementing a secure password policy.

I also recommend using tools that allow real-time monitoring of login attempts from unwanted locations, networks, and ports. In this case, MFA (multi-factor authentication) can also be applied.