# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| HTTP was the main protocol utilized to send GET requests to transfer malware. | |
|

| **Section 2: Document the incident** |
| --- |
| The incident began with our device hostname “your.machine” sending a request to “dns.google.domain” from port 52444 and “dns.google.domain” responding to “your.machine.52444”  Milliseconds after this, a request was sent from “your.machine.36086” to “yummyrecipesforme.com” for http. The request was acknowledged and after the handshake was completed “your.machine” requested a data push via the http GET method from “yummyrecipesforme.com”.  After the download from “yummyrecipesforme.com” on port 80 was complete there was another handshake from google dns followed by a new request to “greatrecipesforme.com.http” from “your.machine” this time using port 56378. After the handshake was completed another data push was requested from “your.machine” and “greatrecipiesforme.com” responded via http GET method. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Raise password complexity requirements across systems to prevent simple brute force and dictionary attacks. |