**Incident Report:** CH-15149-Defensive-What-is-the-Payload

**Date:** 10-27-2022

**Executive Summary:**

On Mon 2015-08-31 at approximately 17:58 GMT, Windows host GOOGENHEIM-PC was infected with TeslaCrypt Ransomware via the Neutrino Exploit Kit (EK) after accessing the compromised website <http://vitaminsthatrock.com/>.

**Victim Details:**

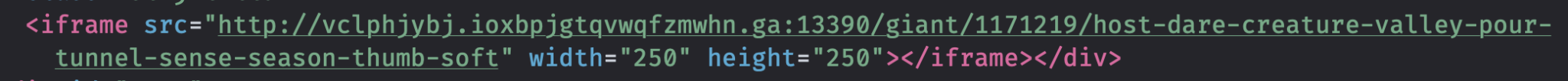
* IP Address: 192.168.137.239
* MAC Address: 00:02:a5:1c:d4:92
* Host name: GOOGENHEIM-PC

**Infection Details:**

* Exploit Kit: Neutrino EK
* Payload: TeslaCrypt Ransomware
* Origin of Infection: 64.20.39.203:80 (<http://vitaminsthatrock.com/>)

**Summary of Infection Progression:**

* Victim attempts to connect to <http://vitaminsthatrock.com/>
  + Website is compromised
  + Contains malicious Javascript code that is heavily obfuscated
  + Malicious code gets executed inside HTTP Response
    - Browser is instructed to make a request to an identified URL triggered by the <iframe> tag
      * URL = landing page for the Neutrino EK



* Contained within the HTML code of the EK landing page is an object tag that instructs the browser to:
  + - Download or update Adobe Flash Player
    - Download malicious .swf file



* Exploits contained in the encrypted .swf file are triggered based on available vulnerabilities of the infected host environment
  + Shellcode is executed
  + Malware is downloaded, decrypted, and launched

**Indicators of Compromise:**

* 17:58:19: HTTP GET /giant/1171219/host-dare-creature-valley-pour-tunnel-sense-season-thumb-soft HTTP/1.1
  + Hostname: vclphjybj.ioxbpjgtqvwqfzmwhn.ga
  + IP Address: 46.108.156.181 | Port: 13390
  + Referrer: <http://vitaminsthatrock.com/>
  + Additional Info: Location of Neutrino EK
* 17:58:21: HTTP GET /defense/eGxyaGM
  + Hostname: vclphjybj.ioxbpjgtqvwqfzmwhn.ga
  + IP Address: 46.108.156.181 | Port: 13390
  + Additional Info: .swf source file
* 17:58:31: DNS Query for ipinfo.io
  + DNS Response: 54.164.11.220 | Port: 80
  + HTTP GET /ip
  + Additional Info: IP address check by TeslaCrypt Ransomware
* 17:58:33: DNS Query for asecproteccion.com
  + DNS Response: 72.55.148.19 | Port: 80
  + Additional Info: TeslaCrypt Ransomware callback
* 17:59:28: HTTP GET giant/1171219/host-dare-creature-valley-pour-tunnel-sense-season-thumb-soft
  + Hostname: tpfnmvg.ioxbpjgtqvwqfzmwhn.ga
  + IP Address: 46.108.156.181 | Port: 35407
  + Additional Info: Ping of Neutrino EK server after payload is sent