Malware Tracker [static + dynamic analysis]

Decode the Vinself Trojan payload, also known as GIF89a as it uses a GIF image header as obfuscation. A new version of Vinself seen in the wild in 2015 appears to encode some victim identification or other data in the first 28 bytes. Data is encoded using the xor look-ahead cipher.

The POST URL does not contain any data, but consists of a date/time ([Reference](#))
Sample: POST /W880/T19R17Q16/I2010L11O14/

Paste the hex of the beacon content (not the POST url) below, any spacing will be automatically stripped. The GIF89a can be included as it will be automatically stripped as well.

Hex data:

Submit