Incident response example – 13-Dec-2021

Introduction

At 1100 on the 29-Oct-2020 it is noted from a client, that a possible cyberattack on their webpage has taken place, specifically on Wordpress – Apache powered webpage, dedicated to journalism and day to day living blog.

The elements described as follows, are a preliminary analysis and don't have a definite character as such, they should be understood as a temporary, providing a framework for the decision making process to protect the integrity of the information, ensure the confidentiality and promote the availability of the information for the client that requests this service.

To take into account, all the information regarding the client was anonymized to keep critical information safe. Only the methodological and technical aspect remained as an example of the work that I have performed.

Preliminary analysis

Object of analysis: Domain

Registered: NIC Argentina[1]

After entering the domain: “Example.com” through the browser (google.com) it can be perceived a that a strange stext string was added in the meta description tag[2], as follows:

> *70157円（プレシャスブラック） dynabook dynabook T55/FB (新品未使用)東芝 スマホ、タブレット、パソコン ノートパソコン PT55FBP-BJA2 PT55FBP-BJA2*

Language was determined as “Japanese”, and translated provides the following:

> *70157 yen (precious black) dynabook dynabook T55 / FB (new unused) Toshiba smartphones, tablets, personal computers Laptops PT55FBP-BJA2 PT55FBP-BJA2…*

After searching this same text string, it was corroborated that it could be found on several internet domains and that this is a wide-spread keyword. Most of these are related to the online sale of computers. It is also interesting to note, that there were even domains from Hungary involved, indexed with japanese text[3].

Dynabook Inc. in particular, is a business dedicated to the manufacture of laptops, and the model PT55 is on sale actually, oriented to the japanese market[4] where it is originary (Dynabook[5] was subsidary of Toshiba Inc.)

Inside the HTML code, an interesting chain can be found:

> *ポケモンカードゲーム SMH GX ...*

This was translated as:

> *Pokemon card game SMH GX*

In light of the information provided, it was considered that this attack was probably a directed attack to a vulnerable webpage, adding this text chain to be automatically read by the search engine. The purposes for this, was probably to increase the position of a certain webpage or product in regards to the SEO (Search Engine Optimization) so the algorithms of the search engines position them better.

In the case of a sales webpage, the net worth would be really positive, as they would avoid paying for a SEO manager and also would increase the revenue due to more sales due to the better exposure.

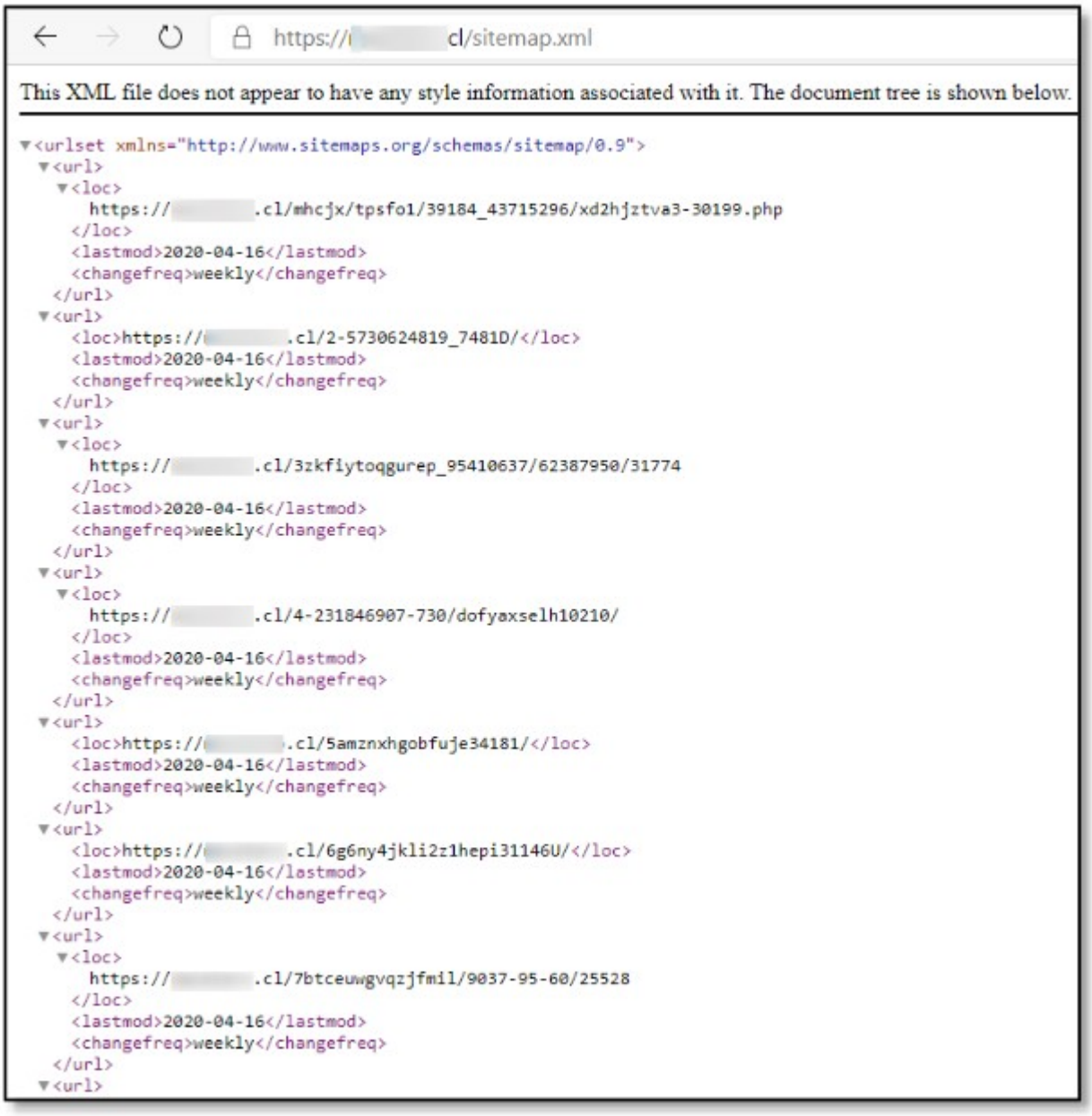
After research, this attack, was identified as the “Japanese Keyword Hack” or the “Japanese SEO hack”.

---

1 See: https://nic.ar/
2 See: https://moz.com/learn/seo/meta-description
3 See: https://montazsmagazin.hu/pec-events/zenet-hallgat-csalad-komolyzenei-matine-berlet/1554634800
4 See: https://dynabook.com/pc/catalog/dynabook/140515t75t55/index_j.htm
5 See: https://us.dynabook.com/

It was also confirmed by a CSIRT level 2 researcher[6], that it has also taken control of several webpages registered with Chile domains[7], noting the following changes in the sitemap.xml, thus confirming the nature and motivation of the attack as economic gain due to redirection to e-commerce sites.

Figure 1 sitemap.xml of compromised sites from Chile



Source: “Cybernetic Threat Analysis, Carlos Silvia Caffi, 28-Apr-2020”.

The attack itself is really interesting, due to using japanese characters that would not be understood normally in sites that are English – Spanish speaking, since most of the users would not normally search for these or even distinguish them from other languages, such as chinese or korean.

6 The complete investigation can be seen at https://www.csirt.gob.cl/media/2020/04/AN2-2020-01.pdf
7 See: https://www.nic.cl/

It was also noted that the analyzed domain (http://www.example.com) doesn’t have a valid SSL certificate (HTTP vs HTTPS) and that all information sent to the webpage woulnd’t be encryped. This provides a more easy avenue for any attacker within the local network to intercept traffic between the user and the webpage. The domain also lacks a robots.txt (the configuration file that allows / disallows a bot / spider to analyze all the information contained in the webpage).

Both are considered as a **critical** misconfiguration that should be fixed as soon as the current security issue is solved.

Conclusion: It was considered that the attack has an economical motivation from a hacker or group of hackers that are trying to increase sales or acquire hard currency using a redirection method to known japanese computer sales e-commerce sites.