Indonesia Web Defacement Attacks Analysis for Anti Web Defacement

IGN Mantra

Informatics Engineering, FTI, Perbanas Institute
Jl. Perbanas, Setiabudi, Kuningan, Jakarta 12940
Tel. (021) 525 2533, Fax. (021) 522 8460
ignmantra@gmail.com, ign.mantra@perbanas.id

Abstract*—Web Defacement attacks in Indonesia are getting worse, many web servers are attacked by the attackers around the world and also from local itself. As the number of web servers is increasing in defacement, the authors want to investigate further on this web defacement attacks. Analysis of web defacement Indonesia who want to investigate in large part 5 Domain Name Server (DNS) that is .go.id (government), .co.id (commercial), .or.id (organization), .net.id (internet) and .Ac.id (academic). Web Defacement action appeared briefly growth increase, it could be triggered by the increasing skill of young people, teenagers in hacking, web defacement tools easily get it on the internet, laptops and tablets are increasingly sophisticated, many hackers community, which increases the amount of book hacking, web server built still using a content management server (CMS) and many other causes, so it needs to be further investigated. Methodology is performed descriptive statistical analysis of the amount of each ter-DNS web defacement. The results of the descriptive analysis will be used for anti web defacement of the web groups. Knowing the desired output is statistically the greatest of all five parts of the government, commercial, organization, academic and internet domain, the next output is find out the cause of this web defacement in Indonesia and conduct anti web defacement to various causes.

Keywords: attacks, web defacement, anti web defacement, descriptive analysis, commercial, government, organization, internet, academic, domain name server (DNS).

I. Introduction

Web Defacement or so-called Gravity Web, in book [1], the hacking activities are heavily utilized by young children today anywhere in the world, because with a web defacement, and the popularity of their existence directly uphill and a thumbs-up among the bad hackers and underground, the faster they work me break down and hacked the computer systems of others riding their caste. What exactly is a web defacement activities this? Because this activity has begun to disrupt and harm it would require more in-depth research on the subject of this web defacement.

In Journal [2], Defacement or Gravity Web site is an institutional web strike activity, this streak could be in the form of colorful, inject swear words undue (blasphemy), the proclamation of the word hacker suppose hacked by Dr. Kruzz, or just replace the original web with pirated web hacker.

II. The Problems

1. There is no standard in protecting web defacement attacks or anti web defacement in Indonesia.
2. To the diversity of forms and web programming carried by each programmer and web administrators.
3. There is no detailed description of an Indonesia web defacement are attacked from both outside and within the country.

III. Research Objectives

1. To make the clear standards to protect web defacement attack Indonesia called anti web defacement.
2. To make the clear standards for the handling of web defacement incident Indonesia.
3. To provide a detailed description of an Indonesia web defacement are attacked from both outside and within the country.
4. To reduce and prevent the occurrence of web defacement, if this happens it will interfere with the performance of the web and *online* transactions on various web sites, of course, the economy will also be affected.
5. The Institutions such as governments, banks, private and academic sector can do the preventive measures based on the Anti Defacement, Standard Operating Procedure, Guidance and incident handling management to reduce and protect their *online* business.

IV. Methodology

Methodology that will be used in this research is constructive research, analysis of web defacement by hackers that attacked, making Indonesia a detailed description of a web attack data published by zone-h.org and ultimately create standards for anti-web defacement (SOP) and incident handling. Database obtained from the download and analysis of the database and then perform categorization as a data .go.id, .co.id, or.id, .ac.id and .net.id. Once complete, the data is posted to excel and be the summation and sorting.

V. Discussions

In book ([3],[4]), The purpose of web defacement hackers do vary, according to the records while there are 5 goals of this activity:

1. Hacker pursue fame, usually hackers and hacker teams vying for the system to break down the identity of the web server and put them on a web page (home page) or sub-page, with the hopes of anyone who opens the web so their identity can be read clearly, an example : web site defacement FBI, CIA, CNN etc.
2. A hacker and a hacker team has a specific mission of the organization who take shelter under it, this team has a goal of peace with the expectation that sites were hacked to read their messages and immediately implement anything they want from the message, for example: the NGO Green Peace , there are a few sites hacked in the name of green peace, as peace mission they prohibit and stop the killing of whales in the pacific ocean, and their participants hacked site that sells the whale meat.
3. Hackers Anonymous 3 has a unique way of conveying its mission to the government does not like, normally an anonymous participant hacking site (web defacement) of the government and paralyzed services in them for days or even weeks. This would never happen in a variety of sites in our neighboring country of Malaysia, has more than 40 Web services down by the Malaysian government made the anonymous participants.
4. The next generation Hackers have money oriented goals and demolish or deface Web sites a person / company to profit and the action. Hackers like this usually work alone, less likely to have friends and are sometimes paid for defacing a website and paralyze the target.
5. Hacker Hero this one action defacement as it went along with the others who attacked first, or part of it as offense and the reason is not clear, for example, a hacker feud between Indonesia and Malaysia have lasted long, who first sparked unclear , but once there is a problem and provocation then the hackers in the two countries attacking each other and paralyze websites of each country and government. There is no element of compulsion and orientation of the money, merely went along and wants to knock down the site was used as a target country.

In book [5], Deface is a technique to replace or insert a file on the server, this technique can be done because there is a hole in the security system that is in an application.

Defacer website in book ([6], [7]) can change the look of partly or wholly dependent willingness defacer and holes that can be entered, but if he was desperate, defacer will perform a denial of service (DoS) attack is to send fake requests to the server redundant servers so that the work is slow and gradually and the server will crash down. To be able to do a web defacement, defacer do the following phases:

a. Looking for weaknesses in the security system, find a gap that can be entered to conduct exploration on the target server. He will do the scanning on the operating system, service pack, service is enabled, ports are open, and so forth. Then analyzed the gap which can be entered.
b. Hacking into a victim server. This technique uses multiple tools, the file to be inserted, files are created deliberately to exploit the copy-right. Upon successful entry, the hands can defacer ransacked server.

Observations of web defacement statistics Indonesia in 5 groups with 5 domains Indonesian grouping ie, .co.id (company), .go.id (government), .or.id (organization), .Ac.id (academic) and net id (network), this statistical data taken in January 2014 until July 2014 as follows:

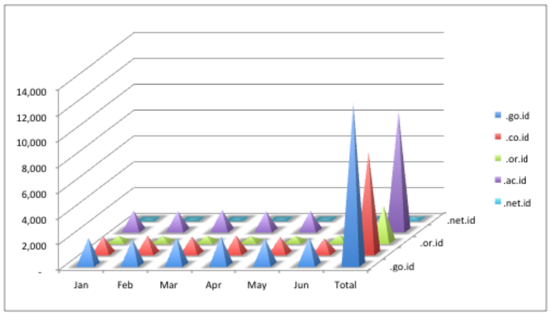

Fig.1. Indonesia Web Defacement Attacks Indonesia 2014

TABLE I.

INDONESIAN WEB DEFACEMENT ATTACKS.

Domain Name	.go.id	.co.id	.or.id	.ac.id	.net.id	
Jan	2,094	1,311	473	1,538	28	
Feb	1,979	1,377	449	1,507	27	
Mar	2,115	1,308	471	1,582	27	
Apr	2,208	1,399	447	1,502	26	
May	2,052	1,287	469	1,517	27	
Jun	2,117	1,185	527	1,586	30	
Total	**12,565**	**7,867**	**2,836**	**9,232**	**165**	**32,665**

Defacer website [8] can change the look of partly or wholly dependent willingness defacer and holes that can be entered, but if he was desperate, defacer will perform a denial of service (DoS) attack is to send fake requests to the server redundant servers so that the work is slow and gradually and the server will crash down. To be able to do a web defacement, defacer do the following phases:

a. Looking for weaknesses in the security system, find a gap that can be entered to conduct exploration on the target server. He will do the scanning on the operating system, service pack, service is enabled, ports are open, and so forth. Then analyzed the gap which can be entered.
b. Hacking into a victim server. This technique uses multiple tools, the file to be inserted, files are created deliberately to exploit the copy-right. Upon successful entry, the hands can defacer ransacked server.

Anti Web Defacement

Note that gathered ([9], [10]) to fight the hackers from doing Web Defacement activity, there are several ways Anti Web Defacement writers analytical results such as:

1. The administrator must often monitor the use of the Web Server, the slightest change should be known by the web admin, so if there is defacement, the admin should emergency surgery to stop the web server.
2. There are several software tools provided by the developer to protect web servers from defacement as an example: RemoteIntegrity Website Scanner, Npust Anti Spyware, Shadow Server, Anti-Keylogger, Anti NetCut 3, Advanced Anti Spy, etc.. All of these tools are useful to withstand attacks by hackers in action try to deface web that we use. These tools will alert the web administrator of our web site are in scanning hacker, trace / log activity scanning a web server.
3. Web Admin should have a contingency plan in case of web defacement attack, one of the ways is the page that dideface replaces all the original page, in order to be restored to their web sites and web hacker does not display the hacking messages.
4. Do not use the default password of the application used to create web design and web uploader (FTP), it is very dangerous and prone to the web to dideface.
5. If an admin has more capabilities (high skill), can implement secure web with https://domainname.com etc, but not all institutions can do this, at least they should have their own web server to be able to implement it, when hosting busy-busy sharing with the hosting provider, it will be difficult in the implementation.

6. Conclusions

Web Defacement happens every day in Indonesia hit several groups such as the domain name .go.id, .Ac.id, .co.id, or.id, .net.id, defacement of data collected have not decreased and is likely to increase. To anticipate this needs to be done to make Web security and anti SOP for special web defacement Indonesia. Because the anti-web defacement activity is still very little needs to be made and SOPs be developed easily and efficiently so that it can be used as guidance by the web administrator in the area. There are several things that need to be adhered to at least a web defacement wane.

REFERENCES

[1] Scambray, Joel., Shema, Mike., andSima, Caleb., Hacking Exposed Web Applications, 2nd Ed. (Hacking Exposed), 2006.

[2] Kruegel, Christopher, Vigna, Giovanni, “Anomaly detection of web-based attacks” in CCS’03 Proceedings of the 10th ACM conference on Computer and communications security, pp. 251-261, 2003.

[3] EC-Council.,Ethical Hacking and Countermeasures: Web Applications and Data Servers, 2009.

[4] Mintz, Anne P., Benham, Amber., Edwards, Eli.,Fractenberg, Ben., Web of Deceit: Misinformation and Manipulation in the Age of Social Media, 2012.

[5] Cross, Michael, *Developer's Guide to Web Application Security*, 2007.

[6] C. Chou, David, Yurov, Kiril, “Security Development in Web Services Environment” in Computer Standards & Interfaces, Vol.27 Issue 3, ACM, March 2005.

[7] Hope, Paco.,Walther., Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast, 2008.

[8] Department of Commerce, U.S., Guidelines on Securing Public Web Servers, 2014.

[9] Sullivan, Bryan.,Liu, Vincent., Web Application Security, A Beginner's Guide, 2011.

[10] Stuttard, Dafydd.,Pinto, Marcus., The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 201