Website Defacements

Krishna Kumar B

Definition:

- A website defacement is an attack on a website that changes the visual appearance of the site.
- A message is often left on the webpage. Most times the defacement is harmless, however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware.

Website Defacement:

- Impacts upon both content and image of the affected site
  - Visitors may gather incorrect information
  - May cause lasting damage to reputation
- Commonly achieved by exploiting poorly configured or incorrectly maintained systems
  - Vulnerability alone may be a reason that a site gets defaced

Objectives behind Website Defacement:

- Defacements may be done in an effort

  -- to publicly “strike a blow” against a perceived enemy
  -- to attract public attention to a cause, an “injustice” or an entity
  -- to reduce public confidence in the security of a system and its trustworthiness for use for sensitive purposes
  -- simply because the defacer finds doing defacements to be “fun”

- To achieve most of these ends, defacements done by a hacker/cracker **must be noticed**.

Decomposing A Web Site Defacement:

- A web site defacement consist of four key elements:

  1) A system with a vulnerability is identified and exploited, allowing unauthorized access by a malicious third party

  2) Existing web pages are modified or replaced with new text or graphics

  3) Something that an attacker might hope to accomplish as a result of a web site defacement

Sample Defaced Page:

Sample Defaced Page:

Mirror saved on: 2013-09-15 17:53:08

Notified by: lafanga **Domain:** http://www.vhscap.kerala.gov.in/VHSECMSControl2012/admin/ **IP address:** 210.212.239.56

System: Linux **Web server:** Apache Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2013-09-15 17:53:08

Types of hackers

- Professional hackers
  - Black Hats – the Bad Guys
  - White Hats – Professional Security Experts
- Script kiddies
  - Mostly kids/students
    - User of tools created by black hats,
      - Impress their peers
- Underemployed Adult Hackers
  - Former Script Kiddies
    - Couldn't get employment in the field
    - Want recognition in hacker community
  - Hack as a mechanism to promote some political or ideological purpose
  - Usually coincide with political events

Cyber Targets:

- Military Networks
- Government Systems and Websites
- Ecommerce and Financial Institutions
- Telecommunication Companies
- Others

Active Hackers in Indian Cyber Space:

- Ashiyane Digital Security Team
- Muhammad Bilal
- h4x0r HuSsY
- BD BLACK HAT
- BD GREY HAT HACKERS
- Romantic
- 3xp1r3
- Hunter Gujjar

Recent Trends:

- Specific exploits:
  - SQL injection Attacks:
  - Remote File Inclusion (RFI) Attacks:
    - Executing remote files in the target web site
  - Use of webshells
  - Exploitation of the weakest link in a co-hosted environment
- Poor design of web applications
  - Javascript hacks
  - PHP/ASP hacks
  - Content Management Softwares

Handling Defacement Incidents:

- Source:
  - Through Defacement Mirror sites;

    - Zone-H, Mirror-H
  - Through Email;
  - Pastebin & other websites
- Domain:
  - .in (ccTLD)
  - Indian Origin (TLD)

Important Things to be Obtained:

- Domain details
- IP Address & Location
- OS, Webserver details
- Defacer information
- Snapshot of the Defaced page.
- Source code of the Defaced page.
- Reasons for Defacement

Defacement Analysis:

- Source:
- Logs
  - Web server Logs
    - Access Log
    - Error Log
  - IDS/IPS Firewall Logs
- Tools:
- Sawmill
- Deep Log Analyzer
- WebLog Expert

Log Management

- Rotation
- Central Log management
- Security

Logs can be effectively managed by establishing policies & procedures, prioritization, creation of Infrastructure and effective operational process

Centralized Log Management & Benefits

Centralized logging server receives all syslog messages from all systems across the network including network devices like router, firewall & IDS/IPS.

Benefits :

- ✓Log messages from all sources could allow for better co-relation of attacks across different platforms
- ✓Central logging server can be placed in a separate segment behind firewall for secure storage
- ✓Hackers won't be delete logs after breaking into a public server
- ✓Real time alerts can be generated using tools
- ✓Easier backup policy , file permissions

Best Practices

- Use latest version of Web server, Database Server, Hypertext Processor (PHP).
- Apply appropriate updates/patches on the OS and Application software when available.
- Conduct complete security audit of web application, web server, database server periodically and after every major configuration change and plug vulnerabilities found.
- Apply Security Information and Event Management (SIEM) and/or Database Activity Monitoring (DAM) solutions.
- Search all the websites hosted on the web server or sharing the same DB server for the malicious webshells or any other artefact.
- Change database passwords of all the accounts available in the compromised database server.

Best Practices

- ✓Block the IP addresses if any suspicious traffic observed from the IP
- ✓Develop signature based prevention techniques to certain known attack patterns observed in the log
- ✓Periodical Review & Audit of application logs for any suspicious attempt to exploit the vulnerabilities.
- ✓Urge service providers to record logs separately for your service in shared hosting to provide logs whenever necessary.
- ✓Host Government website in India only for better follow ups.
- ✓Plug the application specific vulnerabilities.
- ✓Keep track of widely used Web shells & automated attack tools footprints in the logs.
- ✓Use File Integrity checking tools for automatic monitoring of changes in the files and directory structure.

Thank You