**Reconnaissance Report of ForManMills**

**Scope:**

Reconnaissance is the first crucial step to launch a successful hacking attack. It enables an attacker to become familiar with basic, or not so basic information about a company. For example, information such as: Corporate culture, terminology, employee information, trading secrets, technology, and so forth. Conversely, reconnaissance can also be utilized as a wakeup call to help companies protect confidential information online. It is in the same line of idea that I develop the following reconnaissance findings about ForManMills or [www.formanmills.com](http://www.formanmills.com), one of Philadelphia’s largest local retail stores, using search bar commands.

The following report is divided into two parts:

**Part I** – Reconnaissance Information and **Part II** – Mitigation Strategy Recommendations.

**Part I** – Reconnaissance Information

First, a simple WHOIS search via <http://www.networksolutions.com/> reveals an array of network information about FMM. Information such as: Registry Domain ID 720897\_DOMAIN\_COM-VRSN, corporate headquarters: 12808 Gran Bay Parkway West, Jacksonville, FL 32258, Admin Email: [p32ep7r49gy@networksolutionsprivateregistration.com](mailto:p32ep7r49gy@networksolutionsprivateregistration.com), domain creation date 1997-12-31T05:00:00Z,

name of servers: NS1.NXLKHOST.COM and NS2.NXLKHOST.COM.

Next, DNSstuff.com confirms servers and IP information such as: **Created date :**1997-12-31T05:00:00Z,

**updated date :**2015-01-28T23:42:27Z and **WHOIS server:**whois.verisign-grs.com.

Moreover, <http://www.ip-tracker.org/> helps uncover additional material about FMM’s DNS server, IP Addresses and server names. See below.

IP Address: 156.154.64.25 [IP Blacklist Check] Reverse DNS: 25.64.154.156.in-addr.arpa Hostname: ns1.hostingsvcs.com Name servers: ns3.hostingsvcs.com >> 156.154.66.25 ns1.hostingsvcs.com >> 156.154.64.25 ns2.hostingsvcs.com >> 156.154.65.25 ns4.hostingsvcs.com >> 156.154.67.25

Furthermore, analyzing [www.formanmills.com](http://www.formanmills.com) domain through <http://www.accessify.com/f/formanmills.com> discloses page size, programing languages and other poor results of technology resources that FMM relies upon (More detailed information are shared via slides).

Lastly, a Google hack of **Site:formanmills.com -www.formanmills.com** of the company unveils several more critical data. For example, people can understand that FMM is utilizing Monster.com and Indeed.com for recruiting purposes. This is something that can help determine when the retail store is experiencing shortage in staff in a certain area. In addition, this hacking query can help identify the type of personal information FMM collects from job applicants via <http://formanmills.com/corporatecareers/apply-page.htm>. Other websites that FMM either owns or associates with are also publicly displayed with this Google search command.

“**Google Cache**” would beat FMM’ website security to successfully access Formanmills.com’s text format without leaving a footprint in the hosting server logs. This is something that would make it difficult to track down an attacker after hacking into the website.

**Part II** – Mitigation Strategy Recommendations

A good analysis report constitutes of not only finding potential problems, but at least offer good mitigation methods too. The following are essential steps managerial decision-makers at FMM can take to ensure an effective first line of defense of its website. First, it would be a clever idea to think like a hacker. In other words, study and use the similar methods as attackers, but in an ethical fashion. Secondly, it would be critical that the company evaluates and tests its systems regularly. Next, FMM should rely on multiple systems such as Intrusion Detection Systems (IDS), Firewalls, apply vulnerability scanner programs (Nessus would be a good choice), etc. in order to maintain safer online presence. Last of all, make it a FMM culture to consider IT Security as a vital part of its network because refrain from doing so would lead to catastrophic problems. The clear advantage of applying these is to ensure a better first line of defense and safer online presence against hackers. On the other hand, implementing these are associated with disadvantages such as: Give up critical network or PII information to third party testers, systems could be difficult and costly to maintain, also systems crash or failure of production environment.