**Zero Day Vulnerability**

**By- Vishal Srivastava, EEE, 2nd Year**

If you think that by installing the latest security software and using common sense while browsing you’ve won the battle against malware, then I suggest that you think again. The biggest flaw of security is in security itself and most hackers are aware of it.

Professional applications that we all use are made up of thousands of lines of code. When you write so much code, it becomes tough to make sure that it is free of bugs. Most developers try to make the software run and execute properly before selling it but they don’t properly debug it. Most of the time, a simple bug will just make the application crash but once in a while, that bug makes entry from the outside possible.

Good developers are in the habit of releasing patches or updates to fix security issues in their code. However, they need to be made aware of the fact that a glitch exists in their code before they can correct it. This means someone has to run the program in such a way that it’s not meant to be used and find a glitch in it. Then, the glitch needs to be reported to the developer. The developer needs to find out the solution to the glitch and return a patch for it which needs to be installed by the user. All this takes time and hackers know and exploit this.

Zero Day is that dark period in which the hacker knows about the glitch and has written exploits for it but the developer doesn’t know about it and hence there is no patch for it. It is a really horrific situation as the hacker can extract any amount of information from the computer system without the user knowing about it and even if the user finds out, there is no solution readily available for it.

It gives the hacker an upper hand. Enlisted below are the steps in a Zero Day attack-

1. Vulnerability is introduced in software
2. Attacker finds the vulnerability
3. Attacker writes an exploit for it
4. Vulnerability is discovered and software developer starts working on it
5. Vulnerability is disclosed to the public
6. Anti-Virus Signatures are released
7. Developer works on a patch
8. Developer deploys a patch
9. User installs the patch and vulnerability is fixed

The problem with Zero Day is, the first 3 steps last usually 10 months on an average. That’s 10 months of vulnerability that the user was not expecting. Also, when the vulnerability is known, the number of attacks on the user increases by a power of 10 as more hackers uses the same exploit.

So, how does one stay protected from it? Some helpful pointers are listed below:

* Always report any bug found in the software. If you don’t report it, no one will.
* Always keep your software up to date. Just keeping the antivirus up to date won’t be sufficient. Having the latest version of the software really helps

In reality, there is no foolproof method of protection but every step taken for security helps in staying protected.