Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

CCAOI
Cyber Cafe Association of India

Security Newsletter **15th September, 2010**

As internet is becoming an integral part of our lives, it is important that we are aware of the threats we face in the Cyberspace. The need of the hour is to be aware and adequately equipped to protect ourselves online.

Keeping this in view, with the support of ***Indian Computer Emergency Response Team (certin), Department of Information Technology, VeriSign India and Sify Technologies Ltd.*** *we are releasing our second edition of the* ***fortnightly Security Newsletter.***

Types of Online Threats

Individuals today face many threats online with their security and privacy threatened in several ways. Many of these threats seek to gain access to critical information of the individual as well as to obtain money, assets or simply, to affect the access of that individual to some specific information. Malware, viruses, spyware, phishing and e-scams are the most common threats to individuals.

Malware, Spyware and Viruses
Malware, spyware and viruses may harm the data and functioning of an individual's computer; promote online gambling and pornography sites; gather an individual's personal data, including passwords, credit card details etc.; or hijack individual computers and operate distributed attacks on other systems.

Malware or malicious software, is software designed specifically to disrupt a computer system. A Trojan horse, worm or a virus is classified as malware.

Viruses are forms of malware capable of self-reproduction and usually capable of causing great harm to files or other programs on a computer.

Spyware is malware that secretly gathers information about a user while he or she navigates the Internet. The information normally aids in advertising purposes. Spyware can gather information about e-mail addresses, passwords and credit card numbers; it may also record and send individual web browsing habits to a third party. Spyware infections occur by clicking on pop-up ads, by visiting malicious websites or by inclusion with other applications.

Phishing
Phishing is the act of tricking someone into providing confidential information or tricking them into doing something that they normally would not do or should not do. For example, one form of phishing consists of falsely claiming through e-mail to be an established and legitimate enterprise so that the recipient will surrender private information.

E-scams
"E-scam" refers to a fraud scheme that uses one or more online services like chat rooms, e-mail, message boards or websites etc. to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. E-scams are commonly associated with e-mail fraud; the commonest example is the "Nigerian letter."

VeriSign®

sify keeping you ahead

Identity theft
Identity theft is a particular threat in relation to online banking practices. Identity theft related to the use of e-banking services and technologies is not particularly associated with the developing countries. In fact, it primarily affects the developed countries, especially the US, Canada, the UK and Germany.

Online Child Abuse
Children face various threats of online child abuse in the form of Cyber bullying, child pornography, Pedophilias, Predators, Child trafficking and Sexual harassment**.**

VeriSign DNSSEC

Sept. 9, 2010

An important Internet security technology that has been more than a decade in the making took a critical step forward this year, thanks to the continued research, rigorous testing and committed efforts of technologists throughout the global Internet community.

In July, DNS Security Extensions (DNSSEC) was deployed at the root server level of the global Domain Name System (DNS). This is a critical development, as it will support DNSSEC deployments from the core of the network out to the edge, where it will benefit Internet users most.

Properly implemented, DNSSEC protects users against a particularly dangerous threat known as “DNS cache poisoning”, or more commonly, a “man-in-the-middle” attack, by allowing DNS traffic to be cryptographically signed. Because the root-server-system lies at the heart of the DNS, implementing DNSSEC at the root level provides a critical anchor to support DNSSEC deployments further out in the network.

VeriSign worked closely with the Internet Corporation for Assigned Names and Numbers (ICANN) and the U.S. Department of Commerce to implement DNSSEC on the root, drawing from experience working with other DNSSEC implementations, including, most recently, the .edu domain.

Because DNSSEC represents a significant change to the way DNS functions, it naturally creates challenges related to compatibility and capacity. That is why DNSSEC researchers have been so deliberate in pursuing a staged approach to DNSEC deployment. Each new DNSSEC implementation reveals new obstacles and new solutions – solutions that can be readily implemented to improve the effectiveness of next deployment.

VeriSign’s experience over the past year with .edu helped to illustrate the value of that approach.

VeriSign provides registry services for the .edu domain on behalf of EDUCAUSE. With a comparatively small registrant base and highly skilled technical administrators at those registrants' institutions, .edu represented an ideal environment in which to test and implement DNSSEC.

Prior to implementing DNSSEC at .edu – a process completed in August – VeriSign worked with EDUCAUSE to conduct a thorough testbed which allowed technologists to observe interactions between registrants and registrar, as well as between registrar and registry, and culminated in users being able to provision and then perform real-world DNS validations on the DNSSEC-enabled names (via test nameservers).

The testbed gave VeriSign an opportunity to address some of the continuing challenges to establishing an effective DNSSEC implementation. At a technical level, the activities in the testbed underscored the importance of understanding the more complex operational practices that come along with DNSSEC, including cryptographic-key generation and rollover.

VeriSign is committed to continuing its support for these testing activities, which are critical to the continued success of the global DNSSEC transition.

In support of this effort, VeriSign has extended the "end-to-end" testing environment to its registrar community for the .com and .net top-level domains. The aim is to provide the registrar community members with a place where they can verify their DNSSEC implementations in a controlled environment. VeriSign intends to deploy DNSSEC in the .net before the end of the year, and in .com by the first quarter of 2011.

Another resource that VeriSign is offering to registrars and other organizations comes in the form of the DNSSEC Interoperability Lab. Opened to members of the DNS and Internet communities earlier this year, the DNSSEC Interoperability Lab allows solution and service providers to determine if DNS packets containing DNSSEC information will cause problems for their Internet and enterprise infrastructure components.

The goal of the Interoperability Lab is to help identify and address potential compatibility issues throughout the DNS, from the core of the network to the end-user. Each issue the community can identify today, in a lab setting, is one less that will impact users as DNSSEC reaches global adoption. Companies like Cisco and Juniper Networks have already used the lab to test DNSSEC compatibility.

For VeriSign, all of this testing serves to further the process of implementing DNSSEC in .net and .com in a manner that provides the maximum benefit to users while causing the least confusion and disruption. As we move to implement DNSSEC in much larger, less homogenous zones, we fully expect that the number of issues we will discover will increase. But a disciplined approach will ensure that we are prepared for any eventuality.