

Introduction

IMAGINE!!!!

Your company's vital financial information is stolen by an unknown person!

Your day to day operations are monitored by an outsider from a remote location!

All the e-mails you correspond are viewed by your competitor!

ARE YOU RESPONSIBLE FOR THIS????

DO YOU KNOW?

None of the Anti-Virus / Anti-Spy / Intrusion Detection Systems would completely stop confidential information leakage.

According to survey, for every 100 Spyware / Malicious programs produced every week, less than 5 signatures of AntiVirus / AntiSpy are added.

Need

- The most dangerous type of threats allows an attacker to cause program flow anomalies during program execution, leading to arbitrary code execution on the victim computer.
- Malicious code can propagate very fast and cause severe network disruption and data loss even before it can be identified.
- Can you detect that the product you purchased/downloaded is not tampered?

Risks Involved

Unauthorized access to confidential information.

Sensitive data may be corrupted due to malicious content.

Possibilities of peer to peer file sharing due to malicious content.

Crash of applications by Time bombs.

Network crash due to worms.

Our Solution

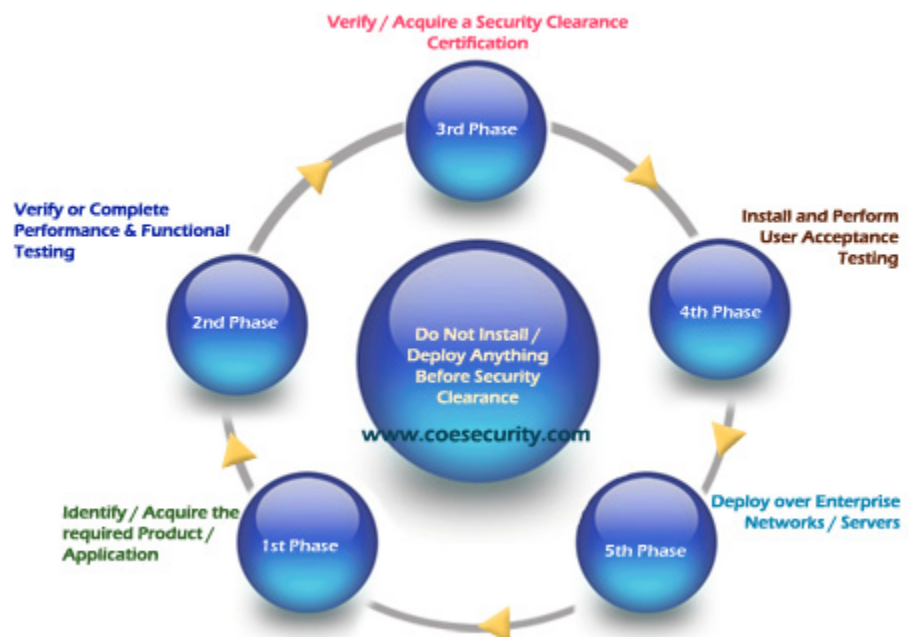
At COE Security, we strive to provide solutions for combating threats which plague an Enterprise.

Solutions are provided through a complete assessment of the software product wherein we apply various innovative techniques in finding the threats existing in the product. This assessment delivers a complete picture of the security competence of the product thus enabling you to protect your organization from any unforeseen implications.

Benefits

- Identification of anomalies in the Product.
- Avoid legal hassles.
- Increase end-users productivity and satisfaction.
- Improved internal network performance and availability.
- Reduces risks involved in loss of data.

PRE-DEPLOYMENT PRODUCT SECURITY TESTING LIFE-CYCLE



Possible Threats by a Software Product

Category	Attack	Description
Malicious Software	Virus	Malicious software that causes damage to a computer system. The damage can range from repeatedly displaying a pop-message to crashing of the system and loss of important data. It duplicates itself within a computer system, potentially attaching itself to every software application.
	Spyware	It is a broad category of malicious software which intercepts or takes partial control of a computer's operation without the informed consent of that machine's owner or legitimate user.
	Worm	Propagates through a network thus hogging the bandwidth and slowing down the network considerably.
	Trojan Horse	Same as Virus or Worm, but also sometimes used to send confidential information like username and passwords, back to the perpetrator.
	Reverse Trojan (Server-to-Client)	Same as virus or worm where the server is active and the client passive. This kind of attack can bypass firewalls, IDS, anti-virus softwares, spyware removal tools, etc.
	Time Bomb	Same as Virus or Worm, but get activated only on a certain predetermined date and time.
	Logic Bomb	Virus or Worm designed to activate under certain conditions.
	Key loggers	Malicious programs that secretly capture or log all the keyboard inputs and transfer or mail them to the attackers located outside the trusted the local network.
	Backdoors / Trapdoors	Developers usually put some access points in the software they develop for easy navigation during development and testing. Backdoors / trapdoors are such system access points that are inadvertently left available even after software release.
Malfunction	Rootkits	They are a set of tools that enable the intruder to maintain his stealth after gaining access to the system. In other words, the intruder uses rootkits in order to maintain access to the remote system without the owner's knowledge.
	Software Malfunction	Malfunction in the operation of the software due to a faulty code or data.
	Hardware Malfunction	Faulty hardware.

For Further Details visit: www.coesecurity.com or Email sales@coesecurity.com