Infiltrating your Organization

"Advanced Persistent Threat (APT) refers to a type of cyber attack designed to evade an organization’s present technical and process countermeasures. APTs are those that are specifically designed to bypass firewalls, intrusion detection systems and anti-malware programs."

- Ponemon Institute® in ‘The Economic Impact of Advanced Persistent Threats’

Some of the biggest corporate APT attacks

**Operation Aurora**

An estimated €36MN was stolen from more than 30,000 customers in over 30 banks across Europe by a Trojan based APT called Eurograbber.

Since August 2013, approximately US$ 1BN has been stolen from over 100 financial institutions by the Carbanak cyber-gang. The threat still persists.

The average cost from cyber crime per company was about US$ 12.7MN in 2014!

EMC’s security division - RSA - spent US$ 66MN to undo the damages brought about data exfiltration from its network.

Learn how ATP attackers infiltrate

APTs exploit security vulnerabilities and use that as a launching point for further incursions

91% of targeted attacks involve spear-phishing emails, making it the primary means by which APT attackers infiltrate target networks.

87% of targeted organizations fall for malicious URLs.

How do organizations defend against APT? 

The IT security budgets of most organizations are largely consumed by antivirus, firewall, and other traditional security measures. A survey of security professionals reveal:

- 94.9% of professionals employ anti-virus or anti-malware
- 92.8% of professionals employ network security technologies
- 71.2% of professionals employ intrusion prevention systems

To know more about our offerings. Please write to us at business@happiestminds.com

SOURCES: