PGI SME Cyber Digest

15th March 2017

- What is an Attack Vector?
- Top 5 Vectors
- Two Thirds of Firms Infected by Ransomware in 2016
- Cybercriminals Becoming Increasingly Capable
- Hasta la 'Vista'……Windows

CESG Certified Training · CREST · TIGERSCHEME · CHECK IT Health Check Service · PCI DSS COMPLIANT · Cyber supplier to: HM Government

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com

What is an Attack Vector?

An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. They include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception. These methods involve a human operator being fooled into removing or weakening system defences.

Top 5 Vectors

Distributed Denial of Service (DDoS)

Multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack

Social Engineering

The art of manipulating people so they divulge confidential information

Spear-phishing

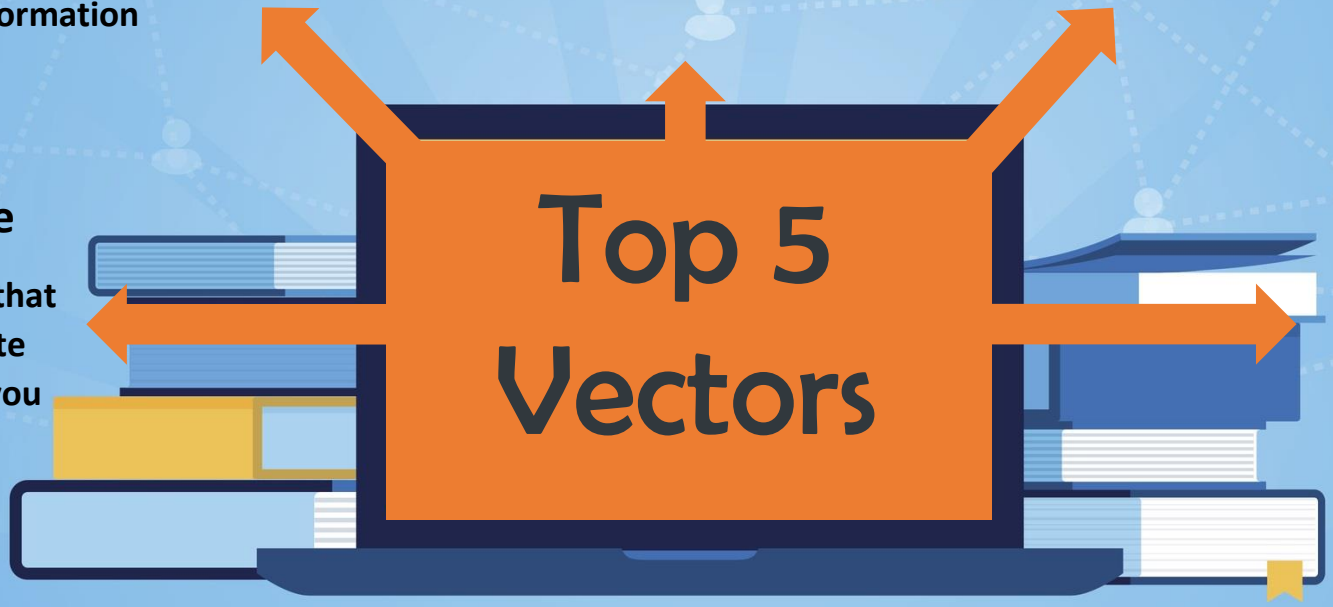
Fraudulent emails target specific organisations or people to gain access to confidential information

Ransomware

Computer viruses that threaten to delete your files unless you pay a ransom

Insiders

A malicious attack perpetrated on a network or computer system by a person with authorised system access



Cybercriminals becoming increasingly capable

Two thirds of firms infected by ransomware in 2016

A recent survey suggests 61% of organisations fell victim to ransomware last year, with 33% paying the ransom. Interestingly, 54% of those who refused to pay still managed to recover their data. At the same time, the overall percentage of organisations affected by successful cyber-attacks rose to 76%, up from 70% in 2015.

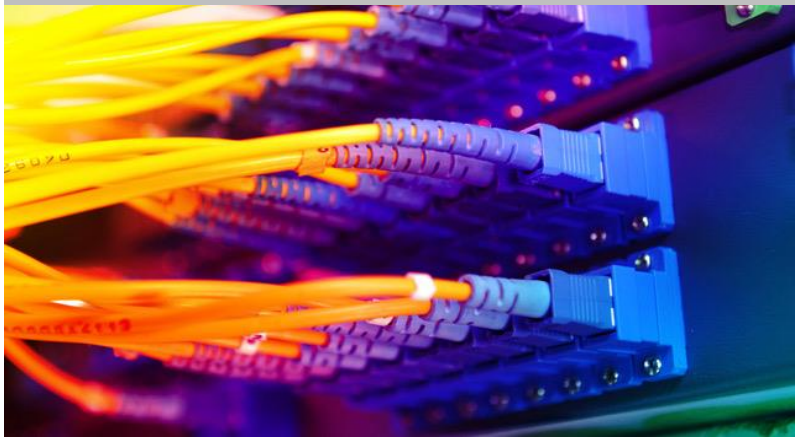
The study also highlighted a 'global cyber security skills crisis', with nine out of ten respondents indicating that their firms were suffering from a lack of talent. In fact, 51% said they are using external vendors and contractors to fill the void. One of the top concerns however, is the low security awareness among employees which has remained the top security problem for the fourth consecutive year.

According to the 2017 M-Trends report, financially motivated attackers have become just as sophisticated as threat actors who are sponsored by nation states. In the last few years, the level of sophistication exhibited by financial attackers and nation-state actors has become increasingly blurred, but researchers now argue that line no longer exists. However, it could be argued that the Dark Web has facilitated the rise of crime-as-a--service (CaaS) which has provided increased capability to the 'masses' including organised crime groups offering on-demand DDoS and bulletproof hosting to support malware attacks. CaaS is becoming increasingly commoditised and syndicates have enhanced their ability to share information and collaborate to leverage sophisticated techniques to evade detection.

Retailers can be highly lucrative targets, especially since many of them fail to ensure that their networks are segmented, allowing attackers to breach the entire environment once they have gained access to Point of Sale systems. Since these attacks can be very lucrative, cybercriminals invest a lot of effort into them. Businesses should ensure they have fundamental protections such as data and key application segregation, network segmentation, and continuous visibility and monitoring of critical systems as well as ensuring all staff have adequate threat awareness training.

Hasta la 'Vista'....Windows

Windows Vista users now have less than 30 days to migrate to a newer Windows version, as Microsoft is stopping support for the old operating system on 11 April. Systems still running Vista beyond this date will remain unprotected and will be vulnerable to attacks trying to exploit unpatched operating system vulnerabilities.



Visit Our Websites

Protection Group International:
www.pgitl.com

Protection Vessels International:
www.pviltd.com

Cyber Services:
www.pgicyber.com

Cyber Academy:
www.pgicyberacademy.com

Intelligence Services:
www.pgi-intelligence.com
www.riskportal.pgitl.com

JTip:
www.jtip.co.uk

Follow us on Social Media:

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com