This story appeared on Information Security Forum at
http://www.securityforum.org
7/29/09

ISF Lists Top 10 Future Information Security Threats;
Criminal Attacks and Crimeware as a Service top Information Security Forum's Threat Horizon 2011

Cybercrime is at the top of the Information Security Forum's (ISF) Threat Horizon list for 2011, which highlights the growth of 'Crimeware as a Service' offered by criminal gangs along with infiltration into organisations for insider attacks. The other threats in the ISF's Top 5 that will present challenges for information security professionals over the next two years are weaknesses in the IT infrastructure, tougher statutory environments, pressures on outsourcing and offshoring and the erosion of the network boundary.

Mobile malware, Web 2.0 vulnerabilities, espionage, insecure user-driven developments and changing cultures with a blurring of the boundaries between work and personal life, make up the remainder of the Top 10 threats predicted in the ISF Threat Horizon report.

The Threat Horizon 2011 report draws on the knowledge and practical experiences of ISF Members, comprising some 300 of the world's largest business and public sector organisations including many of the Fortune 100 corporations. The research was carried out within a 'PLEST' framework that takes into account Political, Legal, Economic, Socio-cultural and Technology factors.

"Many of the threats in 2011 will be familiar ones that are evolving and will present new and sophisticated attacks to compliment tried and tested techniques," says Jason Creasey, head of research at the ISF. "It is also clear that the financial crisis is accelerating these changes, fuelled by increasing staff turnover and dissatisfaction along with the increased involvement of organised criminal groups that see online crime as a lucrative and low risk alternative to other nefarious activities."

Criminal syndicates are developing more sophisticated malware such as viruses and Trojans sold on a 'commercial' basis with guarantees including non-detection by commercial anti-malware software and full helpdesk support. In addition, the so-called 'crimeware as a service' model offers services such as DDOS attacks, botnet rental, malware creation and electronic money laundering. And for the more exclusive, targeted attacks, the criminal world is using techniques such as whaling - targeting high net worth individuals - and attacks tailored to individual organisations.

The ISF is already seeing a shift from indiscriminate events to highly targeted and planned attacks using a combination of social engineering and technical methods to steal identities and information for fraud. The ISF also points to evidence that criminal organisations are recruiting employees as moles or sponsoring students through their IT education and placing them into targeted organisations.

"This more sophisticated and planned approach by criminal gangs comes at time when IT budgets are under pressure and companies are also looking to outsourcing and offshoring to save money," says Creasey.

"These potential weaknesses in the IT infrastructure and third-party relationships - particularly with the advent of cloud computing - pose further threats and it is important to have the right controls in place to mitigate the risks."

"Data is now the gold, the silver and diamonds of the online world and criminals see it as a low-risk way to steal money without going anywhere near the crime scene," says Prof. Howard A. Schmidt, CEO of the ISF. "But even in today's financial climate and increased threat environment, we are better placed than ever before to meet these challenges - as long as we have the resolve to strengthen and invest in security rather than reduce it."

Schmidt also highlights the **need for more security awareness and education.**

"The new generation corporate culture driven by a younger, more techno-savvy workforce presents benefits but there new employees must also be made fully aware of information risks and the need for tighter controls that may restrict their IT freedom."

The Threat Horizon 2011 is one of over 300 authoritative reports along with information risk methodologies and benchmarking tools that are available free of charge to ISF Members. The ISF is a not-for-profit international association of some 300 leading international organisations that has already invested over US$ 100 million in research and the development of practical, business driven research, methodologies and tools in order to address information security and risk management problems.

The ISF Top 10 Threats

1. Criminal attacks

2. Weaknesses in infrastructure

3. Tougher statutory environment

4. Pressures on offshoring / outsourcing

5. Eroding network boundaries

6. Mobile malware

7. Vulnerabilities of Web 2.0

8. Incidents of espionage

9. Insecure user-driven development

10. Changing cultures