CYBERSECURITY

Information Sheet

Threat Actors

Tags: Cybersecurity, Attack Vectors, Threats

365 ARCHITECHS

The old idea of a hacker being a misguided kid using a computer to try to hack into a government system has evolved considerably. There are many different types of individuals and organisations who seek to gain from gaining access to your systems and data.

Threat actors are the cyber criminals working to disrupt operations, cause reputational damage or steal information from governments, organisations and individuals. They come in many guises.

The casual criminal

The cybercrime money launderers, casual criminals are often employed by highly professional criminal organisations that may initially appear legitimate. Motivated by fear or desperation, they are often the most likely to face prosecution or arrest as their role is to convert virtual stolen goods into the physical world. They tend to work from detailed training manuals provided by their employers.

The professional hacker

This is a professional employee similar in every respect to a typical lawyer, accountant or engineer with one exception. The work they perform is illegal. They are technically capable with the skills and experience to evade detection. With strong networks, professional hackers may employ teams of casual criminals.

Nation states

Nation states employ individuals to disrupt, compromise or steal information from governments, organisations and individuals. They work without fear of retribution as they are unlikely to be arrested in their country for doing the work they are engaged to do. They can be motivated by nationalism and have a high degree of technical expertise.

Activists

Political, social or religious causes motivate the activist to attack individuals and organisations that they disagree with, often by setting out to disrupt operations, steal data or harm reputations. They can claim responsibility for their actions to gain maximum media exposure, while they hide their true identity with pseudonyms.

Insiders

Insiders present unique challenges to detect. They are often trusted individuals or customers, or suppliers known by the organisation, with potentially high levels of access to systems and information. They may work together with other cybercriminals or be the victims of blackmail or extortion. Disgruntled insiders can be particularly damaging to organisations.

Child hackers

Children want to shun authority, cause mischief and impress their peers. If caught, they are unlikely to face much more than a slap on the wrist. Their skills vary widely from running scripted attacks to specific assaults on high-value targets. They may be recruited by others, such as professional hackers, nation states or activists.

About us

365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.

(07) 3393 1186 | www.365a.com.au | sales@365a.com.au