MOORE STEPHENS

Cyber security

R&D tax

PRECISE. PROVEN. PERFORMANCE.

Hacking – get to know your enemy

As the world moves closer to a unified digital solution for industries such as banking, social media and news, more and more personal and private data is being generated. In fact, 90% of the world's data has been created within the last two years. Every new day produces 2.5 quintillion bytes of data – equivalent to 10 million blue-rays. The vast majority of this data is meaningless, but hidden within it lie highly confidential files containing trade secrets and financial records.

Companies recognise the importance of securing their data. While an estimated $55bn was spent on cyber security in 2014. We've become used to reading news headlines reporting large scale 'hacks' on major corporations and other organisations, these range from WikiLeaks uncovering countless highly confidential documents, to Sony having potentially 70 million of its customers' bank details stolen. Apple, TalkTalk, Vodafone, Virgin, JP Morgan Chase, Blizzard and eBay have also suffered large scale hacks. So how do these attacks still happen when so much money is spent on security?

Key hacking techniques

Hacking is performed by someone exploiting weaknesses in a computer system or computer network. Although hackers have many weapons at their disposal when it comes to mounting attacks, major techniques used include:

Denial of Service (DoS\DDoS)

A denial of service attack aims to take down a site or server by flooding it with a huge amount of traffic. Hackers set up fake computers, or 'bots', to issue standard requests to open the target website. They can make tens of thousands of requests in a few seconds. The server is unable to process all the traffic in real time and finally crashes, taking out a layer of security and allowing the hackers to access data stored by the website (usually user details, bank accounts, email address, etc.). This technique is one of the most common attacks used to take large websites offline, employed successfully against websites run by CNN, Dell, Amazon and even the Pentagon.

Trojans

Aptly named after the wooden horse used by the Greeks during the siege of Troy, a trojan virus is malicious software (malware) that disguises itself as legitimate software. It's usually inadvertently installed by a PC user who intended to download a different software application or who downloaded an attachment from an email. Once installed on the victim's computer, the trojan virus can send data from the victim to the hacker. For example, a 'keylogger trojan' records every stroke on a keyboard and then sends it to the hacker in order to steal passwords and other sensitive pieces of information. New trojans are always being developed, keeping the hackers a step ahead of anti-virus software. One of the most famous attacks was the 'Storm' trojan of 2007, which affected an estimated 10 million computers. Millions of dollars were spent in an attempt to contain the threat.

Waterhole attacks

A 'waterhole' or 'watering hole' attack targets a particular group of end users (such as members of an organisation, industry or region). The attacker 'guesses' or 'observes' which websites group members often use and infects one or more of them with links to malware, so enabling it to disrupt computers and steal information without the user even knowing. Eventually, some member of the targeted group gets infected. This is a relatively new strategy and is harder to predict and stop.

Essential defensive measures

Hackers clearly pose a major risk to organisations, but they don't always succeed. You can strengthen your defences by implementing a number of protective measures. These include:

- always completing required software updates for your operating system and web browser;
- making sure all computers have a firewall installed;
- changing passwords regularly;
- installing up-to-date anti-virus software;
- installing anti-spyware/adware programs onto your system;
- deleting emails from unknown sources;
- training employees in order to raise awareness of hacking threats and the warning signs to look out for.

The many faces of the modern hacker

Hackers come in many forms. Some are simply modern criminals out to make financial gain. Others – known as 'hacktivists' – have more complex motives and goals, as explored on screen in the 1995 techno-thriller Hackers and Golden Globe-winning TV series Mr. Robot. Hacktivism is the subversive use of computers and computer networks to promote a particular, often political, agenda. The most famous hacktivist group, called Anonymous, became known for a series of well-publicized publicity stunts and attacks on government, religious, and corporate websites. But hacktivists also operate alone, outside groups, driven by their own personal agendas and motives.

Conclusion: we are all vulnerable

Large organisations invest millions in trying to secure their servers and improving network infrastructure. Some even employ 'ethical hackers' to test their security systems and identify any weaknesses. But they still get attacked and some fail to maintain adequate defences to keep their data secure. So how can smaller companies even hope to stay protected?

The truth is, there are no guarantees of safety, no matter how large or small your organisation. Hackers keep developing new forms of attack and security systems have always been reactive. Unless this changes, we will all always be vulnerable. But accepting this is a vital prerequisite for building your defences against hackers. Avoid complacency by understanding your weaknesses and staying aware of the evolving nature of the hacker threat.

Eyad Hamouieh – Partner
eyad.hamouieh@moorestephens.com

Moore Stephens LLP
150 Aldersgate Street, London EC1A 4AB
T +44 (0)20 7334 9191
www.moorestephens.co.uk

We believe the information in this factsheet to be correct at the time of going to press, but we cannot accept any responsibility for any loss occasioned to any person as a result of action or refraining from action as a result of any item herein. Printed and published by © Moore Stephens LLP, a member firm of Moore Stephens International Limited, a worldwide network of independent firms. Moore Stephens LLP is registered to carry on audit work in the UK and Ireland by the Institute of Chartered Accountants in England and Wales. Authorised and regulated by the Financial Conduct Authority for investment business. DPS38584 January 2018