21st September 2016

Cyber Matters

Your essential guide

In this issue

- Hacktivists Go For Gold
- Dridex Trojan Returns
- Jargon Buster: SQL & Trojan
- Sage Employee Arrested
- US to Handover DNS

01704 542 420
info@p-ccomms.com

Hacktivists Go For Gold

The Brazilian hacktivist group, AnonOpsBR, have reportedly posted a Pastebin link on its Twitter profile (@anonopsbrazil) to an apparent dump of employee contact data stolen from the Olympic Broadcasting Service (OBS). OBS is the arm of the International Olympic Committee responsible for distributing official images of the Games. It is believed the compromise was achieved via a SQL injection on the website. The data dump allegedly include OBS employees' and freelancers' legitimate names, job titles, email addresses, and both mobile phone and landline numbers as well as some links to potentially sensitive PDF documents supposedly stored on the company's main website. However, the compromise did not affect the broadcast of the Olympic Games because the IT environment for OBS's field operations were segregated from its web presence.

Dridex Trojan Returns

Dridex, one of the most prolific Trojans in recent years, is ramping up its activity once again after coming to a near stop some two months ago. Earlier this year Dridex started distributing the Locky ransomware, but since June, distribution has been very low. Most recently, however, researchers have observed a spike in Dridex distribution suggesting a new, larger campaign. The spike in distribution is focused on targeting financial services and manufacturing organisations. While most of the campaigns observed since June have been aimed mainly towards Switzerland, the UK, Australia, and France were also targeted. The recent shift to more targeted distribution suggests Dridex actors are still looking to monetize the malware by targeting a smaller number of large organizations, many in financial services.

Jargon Buster: SQL & Trojan

SQL injection is a type of web application vulnerability in which an attacker is able to submit a database SQL command that is executed by a web application, exposing the back-end database. A SQL injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. It allows an attacker to access, alter or delete data stored in the back-end database.

What is a Trojan?

A Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cybercriminals and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cybercriminals to spy on you, steal your sensitive data, and gain backdoor access to your system. Unlike computer viruses and worms, Trojans are not able to self-replicate.

Sage Employee Arrested

Recently it was reported that employee details from up to 280 UK businesses may have been compromised after software company Sage Group suffered a data breach. Sage, which supplies accounting and other financial software to 3 million small and medium-sized business customers globally, was investigating an incident of “unauthorised access to customer information”, which was made using internal login details. Initial reports suspected an insider was responsible rather than an external attack. Whilst the motive remains unclear, this provides a timely reminder of the threat posed by insiders.

US to hand over DNS

The US National Telecommunications & Information Administration (NTIA) has announced that it is ready to cede control over the Internet domain name system (DNS) infrastructure to the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization effective October 1, 2016. The DNS is basically a directory for internet-connected devices that helps translate domain names to numerical IP addresses. In other words, it is responsible for holding and pairing web addresses or its URL to its respective servers. DNS is a foundational piece of the internet, which has been under the control of the state for the last 20 years. The handover won’t change anything for the 3.5 billion people connected to the internet because US control has been largely administrative. The shift will likely go unnoticed by everyday users and businesses despite its political complications.

Thank you for downloading this guide.

Please feel free to contact us on the details below if you have any questions or comments, or would like advice on any of your own cyber security issues.

01704 542 420
info@p-ccomms.com