CSS PLATINUM

Monthly Security Newsletter.

Welcome to Charter Season!

After a tumultuous year, the start of the new charter season brings huge excitement to the CSS Platinum team!

We are looking forward to joining our partner ACREW in Porto Montenegro from 15th June. CSS Platinum will attend the 3-day event, including a Captains briefing, workshops and various social activities.

You will be delighted, or slightly unnerved, to see that Cyber McNasty has been invited back for a guest spot in our newsletter! After his show stopping performance in our 'Under the Radar' event, it seems people want more McNasty! See tips and tricks from our very own sinister Cybercriminal below or watch the YouTube event video here.

Stat attack:

51%

Of data breaches are caused by remote access with third parties.

$1 Million

Bribe that Tesla employees were targeted with to place ransomware on the network.

15%

Of people use their pets names as passwords!

GIBRALTAR INSIGHT

If a cyber-criminal were to steal something of yours, you would know. Right? But would you?

In the good old days, before computers and devices, our world was dominated by tangible, physical things. It was there, present, in our hands, at our fingertips. You would know whether a thing was present or missing. We now live in an increasing digital environment, with more things becoming virtual.

Learn how cybercriminals can steal from you and not leave any tracks in our full article on www.cssplatinum.com/news

CSS PLATINUM

Monthly Security Newsletter.

Cyber McNasty's Insider Tips & Tricks

Did I get you with my little RAT hack last month?

This is a vicious little hack which uses search engine poisoning techniques to install a Remote Access Trojan (RAT) on devices.

This hack targeted anyone looking for templates to create documents, e.g. governance docs, invoicing & compliance templates. The target then clicks a link to a professional looking template but is unknowingly redirected to a site to download a fake PDF with the RAT attached to it! Once the RAT is active, we can remotely install other malicious software such as ransomware or just get a foothold in the network.

To avoid this happening to your system, make sure that your antivirus is updated and set to scan files downloaded from the internet and always obtain templates from reputable source. Read the full story here.

Poor Password Security Leads to Water Treatment Facility Hack

Now this one was close to causing some serious damage. Access was gained to a water treatment facility with an aim to increase sodium hydroxide to dangerous levels in the water system. An operator noticed in time to stop it.

So how was it done? Computers connected to the control system had Team viewer which was used to access the control system. These computers were running legacy 32-bit versions Windows 7 AND shared the same password for remote access AS WELL as being connected directly to the Internet without any firewall protection! Full article here.

If you don't keep computers, devices, and applications, including industrial control systems (ICS) software, patched and up to date, or use two-factor authentication with strong passwords you will be exposed! I've noted that Microsoft Windows 7 has reached end-of-life on January 14, 2020 – this will give me a host of opportunities!

Mac Attack: Worst Hack in Years hits Apple

This was big news! Hackers identified a flaw in Apple MacOS's Gatekeeper feature. Gatekeeper allows only trusted apps to be run by ensuring that the software has been signed by the App Store or by a registered developer and has been scanned for malicious content.

The flaw enabled hackers to develop an application that would deceive the Gatekeeper service and get executed without any security warning! It involves packaging a malicious shell script so that the malware could be double-clicked and run like an app - Full story here.

Whilst the flaw has been fixed by Apple, those who HAVE NOT updated their Operating System will remain vulnerable. The longer you wait the more at risk you are.

Luckily help is at hand, CSS Platinum have Cyber McNasty under full control. If you want to understand more about how to protect you and your organisation from cyber-attacks, contact us at support@cssplatinum.com