CSS PLATINUM

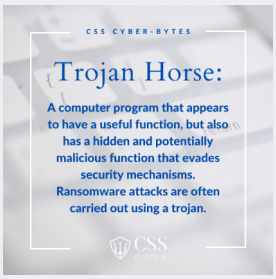
Monthly Security Newsletter.

January's Edition: Happy New Year!

As we kick-off 2021, one of the biggest security breaches in the modern era is still having an impact across the globe after a cybercriminal organisation infiltrated SolarWinds software using Malware and Trojan Horse hacking techniques.

Cyber-attacks on this scale can have disastrous consequences for organisations and individuals. It's the reason why the IMO has implemented the ISM Code Maritime Cyber Risk Management regulations this month. Learn more about the regulations and their potential impact on the maritime communities here.

Cyber Bytes Glossary.



Our aim at CSS Platinum is to inform about cyber-threats and how to protect our maritime and superyacht communities.

SolarWinds hack: The biggest cyber-attack yet?

SolarWinds reported the hack of their network and management software by "a highly sophisticated, targeted cyber-security attack by an outside nation-state". SolarWinds software is used by numerous government agencies and approximately 300,000 customers worldwide.

How did they do it?

Hackers infiltrated the SolarWinds Orion software update platform; they used "trojan horse" malware to enter a top-level server used to build the SolarWinds software updates. The cybercriminals infiltrated the very source of SolarWinds software updates, all subsequent rollouts were infected with the malicious code and attacked thousands of separate networks worldwide.

One of the organisations impacted by this highly sophisticated hack was Microsoft, leading them to respond with an unprecedented response across its Windows systems to counteract the cyber-attack which had already infiltrated customers networks through software updates rollouts.

Are you protected?

The Cybersecurity and Infrastructure Security Agency (CISA) have advisory information click here to read. The U.S. Coast Guard has urged all Marine Transportation System stakeholders using impacted versions of SolarWinds to take immediate actions to mitigate any risks of compromise.

CSS Platinum are the maritime industry cyber-security specialists, speak to one of our team for a free consultation call in January to discuss any concerns or queries you have. Email the team directly on support@cssplatinum.com

CSS PLATINUM

Monthly Security Newsletter.

How much are you worth on the dark web?

Currently email and password combinations for Microsoft Office 365 accounts, owned by high-net-worth individuals worldwide, are being offered for sale on a dark web forum for between $100 to $1500 per account. Criminals are purchasing these details in order to commit 'Business email compromise (BEC) fraud' whereby they log in and request colleagues make payments at their request. BEC fraud accounted for 50% of the cybercrime losses reported in 2019 to the FBI.

The easiest way of preventing criminals from exploiting compromised account details is to use two-step verification (2SV) or two-factor authentication (2FA) for your online accounts. Having this enabled means that even if criminals manage to obtain login details, they will be unable to access the account without the 2SV/2FA verifier.

Want to know if your accounts have been hacked? Find out with https://haveibeenpwned.com - this free site will check if your email account has ever been compromised, if so, ensure you change the passwords immediately, review any other accounts that are linked and implement verification as per the steps in this article for additional level of security.

If you are concerned about the level of your individual, organisational or vessel security, CSS Platinum can provide a review service to help you assess, understand and target any vulnerabilities. Contact the team at support@cssplatinum.com

Could your crew be targeted through Social Engineering?

2021 is predicted to see an increase in coordinated social engineering cyber-attacks. Social engineering uses information gained on an individual or organisation to build bespoke profiles and use that data for targeted attacks. Whether the subsequent cyber-attacks take the form of Phishing emails or Smishing text messages, the attacks are more successful due to the use of information scaped from the internet.

The Maritime industry has seen specific targeting of crew members. A phishing email about a fine or a Smishing text around a vaccination: the aim of these attacks will be to compromise security controls by gaining access to user credentials (i.e. passwords) that are then used to access the systems onboard the yacht.

To keep crew, and ultimately the yacht, safe from criminal attempts it is important that all crew (regardless of position) receive awareness training regarding cyber-security. Training means individuals can recognise and report cyber-attacks, gain additional understanding and be able to implement security protocols to protect themselves and systems onboard a yacht.

95%

of all attacks targeting networks are caused by successful phishing

97%

of users do not report phishing emails to their management

£170 Million

of fines relating to GDPR breaches were issued in 2020

MARITIME CYBER LICENCE

Have you trained your crew to recognise a suspect email or text? CSS Platinum provide cyber awareness training to protect staff and organisations whilst delivering compliance. Gain your Maritime Cyber Licence – to learn more click here.