

## Protect Briefing – 25/10/2016



## Do you realise the danger a DDoS attack poses?

After the recent DDoS attack on Dyn, which led to a number of high profile companies being affected, the threat of DDoS is once again in the spotlight. This informative slideshow examines five DDoS myths and details what you really need to know about this type of attack.

To view the article visit [ITBusinessEdge](#)

## Ransomware is now big business

Are virtual currencies and the dark web a catalyst for this type of crime? This article explains how, and why, instances of ransomware have exploded over recent years.

Read the article at [ITPro](#)

[No more ransom](#) is a project involving law enforcement and IT Security companies from around Europe who have joined forces to disrupt cybercriminals who distribute ransomware. Their website offers advice on preventing yourself becoming a victim of this type of crime and also offers support if you have been a victim of ransomware, including decryption tools.



The Cyber Essentials scheme provides business' with clarity on good practice within cyber security.

Find out more [here](#).

CYBER AWARE 

On the 6<sup>th</sup> of October 2016 the government's cyber security awareness website Cyber Streetwise changed its name to Cyber Aware. By working with partners to deliver consistent messages, Cyber Aware aims to maximise the impact of the cross-sector effort to drive the adoption of secure online behaviours. The new Cyber Aware logo will provide a visual link of this co-ordinated approach.

To visit the new Cyber Aware website click [here](#)



**METROPOLITAN  
POLICE**

**TOTAL POLICING**

NEW  
SCOTLAND  
YARD

## 2017 – What to expect

As technology continues to improve and innovate how will the cybercrime landscape evolve in 2017?

We have already seen the IoT being used in a massive DDoS attack against critical ISP infrastructure and ransomware allegations have risen significantly in 2016 but what other attack vectors should we be concerned about in the months and years to come?

An article on the [Techrepublic](#) website discusses a number of these areas and what to expect in the future.

## GDPR, are you ready?

The General Data Protection Regulation is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union.

The regulation was adopted in the EU on 27 April 2016. It enters into application on the 25 May 2018 after a two-year transition period and, unlike a [Directive](#), it does not require any enabling legislation to be passed by governments.

Although the UK has voted to leave the EU it is highly likely that the GDPR will remain in force in the UK, particularly for organisations holding data relating to individuals living in other EU member countries.

For more information visit [ico.org.uk](#)

## What is DMARC?

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email standard that makes it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender, and what to do if it isn't. This makes it easier to identify spam and phishing messages, and keep them out of peoples' inboxes.

### DMARC

- checks inbound emails came from where they say they came from using a combination of [Sender Policy Framework](#) (SPF) and [DomainKeys Identified Mail](#) (DKIM)
- tells the recipient's email service what to do with emails that fail the check
- asks recipient email services to send back reports of where email is coming from

DMARC is one of many tools that can be used to prevent email spoofing, phishing and spam emails.

For more information visit [dmarc.org](#)



## **Briefing Dissemination**

This document has been given the protective marking of NOT PROTECTIVELY MARKED and may be disseminated outside of law enforcement with no restrictions. Please feel free to circulate it within your business or to other partners.

If you know anyone else who would like to receive this briefing please send us their e-mail address and we will add them to the distribution list. If you no longer wish to receive this bulletin please let us know at the email address below.

Any comments or queries please email the FALCON Cyber Protect team at:

**CyberProtect@met.police.uk**

