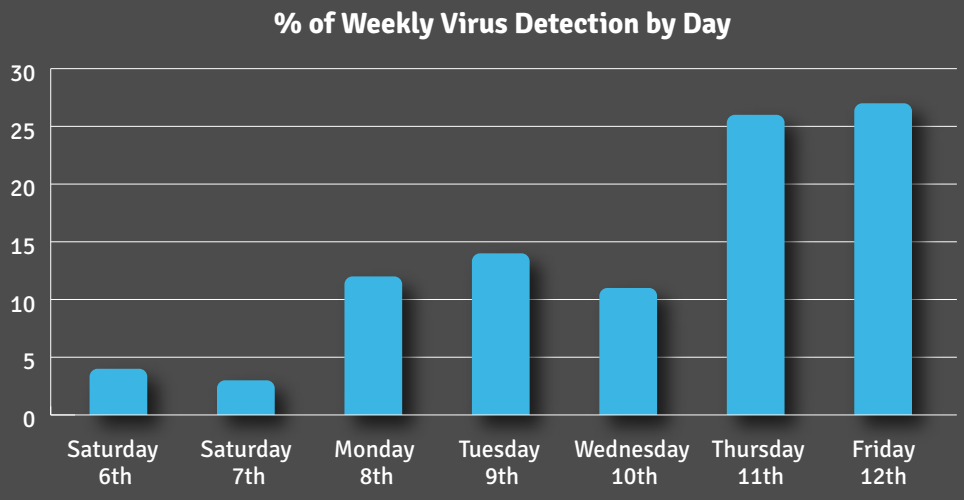
mailsphere

Securing your email

A Security Necessity

Email security is essential for the 21st century organisation. Without an effective email security solution in place your organisation risks being affected by the worst of the malicious activities reported in the news today.

The recent global cyber security threat from WannaCry is believed to have begun with an email and an attachment that should not have made it to the unfortunate recipient.



The above chart shows the total volume of viruses detected by Mailsphere across the week commencing 6th May through to 12th May when the WannaCry outbreak was globally reported. The Mailsphere perimeter identified an incease in emails containing malicious code or illegal attachments on the Thursday and Friday when the threat was identified.

Without an effective email security solution in place your organisation risks being affected by the worst of the malicious activities reported in the news today

Viruses and Attachments

The most obvious suspect for email security is in attached files. Mailsphere operates a strict default policy that prevents any scripts or executables being transmitted by email. This is not a configurable option - the exceptional cases where a script or executable file needs to be transmitted by email is possible through the use of secure encrypted file compression where the recipient is required to unlock with a shared password.

Unfortunately, some email providers still allow these file types to be transmitted freely. The only safe action is to remove this risk entirely as zero day threats and new variants are identified in the industry too frequently.

The anti virus analysis takes feeds from multiple providers. These feeds use traditional signatures and heuristic analysis to detect threats in attachments. If a compressed file is detected the contents are unpacked and analysed to ensure malicious code is not being hidden.

Common spam

The annoyance of spam doesn't need to be highlighted but, while the effect it has on us doesn't change, the content or methods used by the spammers is constantly being updated.

As such it is imperative to employ advanced spam analysis in your email security, that is proactively being updated to identify the most recent styles of spam occurring throughout the globe.

A Mailsphere monitors bad practices by email marketing companies, evidence of acquired email lists being used, new top level domains being misused by spammers as well as over 500 different points of analysis across DNS configuration, MIME or HTML properties and content analysis.

Mailsphere operates a strict default policy that prevents any scripts or executables being transmitted by email

Phishing

A common method of phishing is when the sender pretends to be a known brand or person known by the intended recipient.

Mailsphere uses dedicated analysis to prevent well known brands from being used in phishing attempts. Through ongoing research Mailsphere has found that phishing is often regionally targeted and as such our solution for the UK and Irish market offers increased protection beyond other global providers.

Spoofing

When an attacker attempts to deliver email using an email address from the targets domain this is referred to as spoofing. This is easily detected by Mailsphere as a strict policy of authorised end points is registered with each managed domain.

It is possible to add 3rd party services that may send email on behalf of your organisations domains but any source outside of this scope will be rejected with a 'Relay Denied'.

Mailsphere uses dedicated analysis to prevent well known brands from being used in phishing attempts

CEO Fraud / Whale Phishing

Phishing comes in many shapes and sizes but the tactics used in "CEO Fraud" against the executive or accounting team can be particularly challenging due to how well engineered they are.

A typical CEO fraud will pass all content checks and bayesian filters as they are written to look like an authentic email. It is common for a new domain name to be registered that looks very similar to the targets own domain name. The perpetrator will be keen not to leave a paper trail back to themselves so they often use domain registries with poor practices. Mailsphere holds a blacklist of these registries and monitor emails from domains that are resolved by these name servers.

In addition to this internal blacklist Mailsphere works with other third party domain checks with domain age used to calculate the level of trust associated with a domain name. Once combined with domain registry checks Mailsphere can identify whether it is a new domain from a low trust registry or if it's a domain that can be trusted but just happens to have been registered at a registry with poor practices.

In addition to these checks on the sender, Mailsphere also applies dedicated analysis of the email content. Four specific areas are tested, covering over one hundred indicators, to identify whether the content is a type of CEO Fraud.