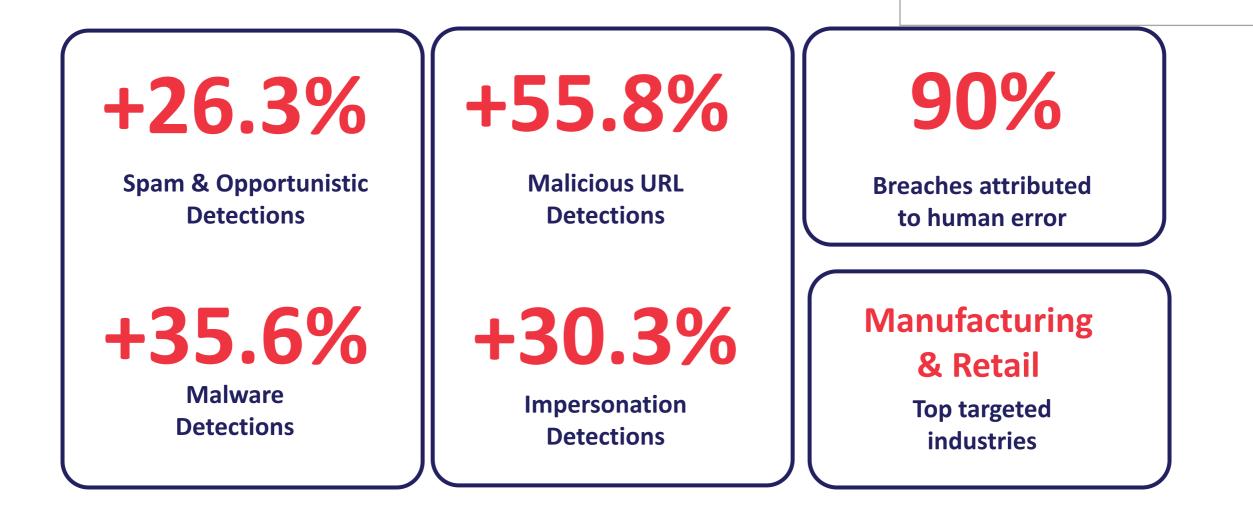
mimecast[®]

Cyber4Good Threat Intelligence

30 September 2020

AND THEN THERE WAS COVID19...



UK & European analysis

- Campaigns primarily
 Emotet driven since it reactivated.
- General level of daily activity against many verticals was significantly increased.
- Activity appeared to be normalizing over time.

Key malware components: Abracadabra AgentTesla Cryxos Emotet Logan Lokibot Nanocore Remcos Zloader **Emotet**

Reactivated on 07July

Between 29 – 31 July

Over 230,000 detections of Emotet globally.

Manufacturing and Retail/Wholesale hardest hit.

Australasia, UK and US regions impacted most heavily







Ransomware

Top 3 active since January Maze REvil/Sodin Ryuk/Conti

Increasingly delivered via exploit or the brute forcing of RDP processes/ports

Public Sector

16 July - NCSC APT 29 Targets COVID19 vaccine development.

16 September – NCSC

UK condemns Chinese cyber attacks against governments and businesses.

04 September – NCSCQakbot malware targetingUK organisations

17 September – NCSC Education Actively targeted by ransomware.