COVID-19 SOCIAL ENGINEERING ATTACKS

THREAT ACTORS ARE CAPITALISING ON THE UNCERTAINTY THAT THE GLOBAL COVID-19 PANDEMIC IS CREATING TO TARGET INDIVIDUALS, ORGANISATIONS AND REMOTE WORKERS.

Mimecast has observed the following malicious activity related to COVID-19:

15%

of detected spam is linked to COVID-19 related phishing attacks

234%

increase in new COVID-19 web and sub-domains registered per day

168,000

unsafe clicks in the UK per week

Barracuda Sentinel has observed the following phishing attacks

- Scams 54%
- Brand impersonation (malware and credential phishing) 34%
- Blackmail 11%
- Business email compromise 1%

Deloitte Cyber threat intelligence has observed the following COVID-19 malware campaigns

- Malspam with attached ISO disk image file delivers LokiBot
- Malspam delivers Remcos RAT
- Attack campaign delivers Remcos RAT
- Malspam delivers Formbook
- New Patchwork malspam campaign with maldocs targeting Chinese individuals
- Malspam delivers Emotet

LORCA delivery partner Deloitte's threat intelligence has observed a significant increase in the number of COVID-19 related social engineering cyber attacks, particularly phishing, domain spoofing, waterholing and smishing attacks.

Prime locations

Early attacks targeted geographies badly affected by the COVID-19 pandemic such as North America and the UK, according to the UK's National Cyber Security Centre. However, other countries such as Japan, Italy, Indonesia, Australia, Germany and China are also beginning to be targeted.

Who's behind the threat?

The threat actors behind these attacks range from small, unknown actors to prominent threat actors and nation states. Cyber attacks from organised crime groups may also be a greater source of potential threats in the future.

The threat actors who are currently active have differing agendas, ranging from financial crime to stealing information and cyber espionage. This is reflected in the types of phishing attacks being observed by Barracuda Sentinel, such as scams, business email compromise (BEC), brand impersonation malware campaigns, credential phishing) and blackmail.

Methods and tactics

Threat actors tend to impersonate healthcare organisations, public sector bodies and financial institutions because of their perceived authority and relevance to the COVID-19 pandemic. For example, a recent campaign saw the World Health Organization being impersonated in phishing emails that purported to contain links to documents on preventative measures for COVID-19. In reality, the links took victims to malicious domains.

Cyber criminals are also conducting COVID-19 themed scams to receive payment for fraudulent COVID-19 vaccines or protective equipment. An example of this is the domain spoofing scam that impersonated the US Centres for Disease Control and Prevention website and requested bitcoin donations to fund a fake vaccine.

Similarly, a phishing campaign targeted individuals in Japan with emails claiming to be from disability welfare providers. When people downloaded a document claiming to contain information on COVID-19, an information stealing malware called Emotet was installed.

Researchers at cyber company Proofpoint recently identified an emerging brand impersonation trend where cybercriminals are waging COVID-19 financial aid themed credential phishing campaigns. These campaigns have impersonated health organisations, financial institutions and government bodies in Germany, the UK, the US and Australia to steal personal data.

Barracuda Sentinel found that threat actors seeking to blackmail individuals have also used malicious email campaigns that threaten to infect victims and their families with COVID-19 unless a ransom is paid. Examples of BEC attacks include those described by the FBI where employees at a financial institution received emails from someone posing as the CEO, requesting that a $1m payment be switched to a different date.

Cybersecurity solutions to a heightened threat

Social engineering attacks always pose a potential threat to organisations. However, the increase in fear, reliance on remote working and quantity of attacks caused by the COVID-19 pandemic is significantly increasing the susceptibility of individuals and organisations to social engineering attacks.

LORCA's members offer many services and products that could help organisations, including solutions that:

- anticipate COVID-19 related trends
- secure BYOD and CYOD devices
- bolster threat detection capabilities
- protect data from third parties that might become compromised
- develop staff awareness through smarter training

LORCA BY plexal