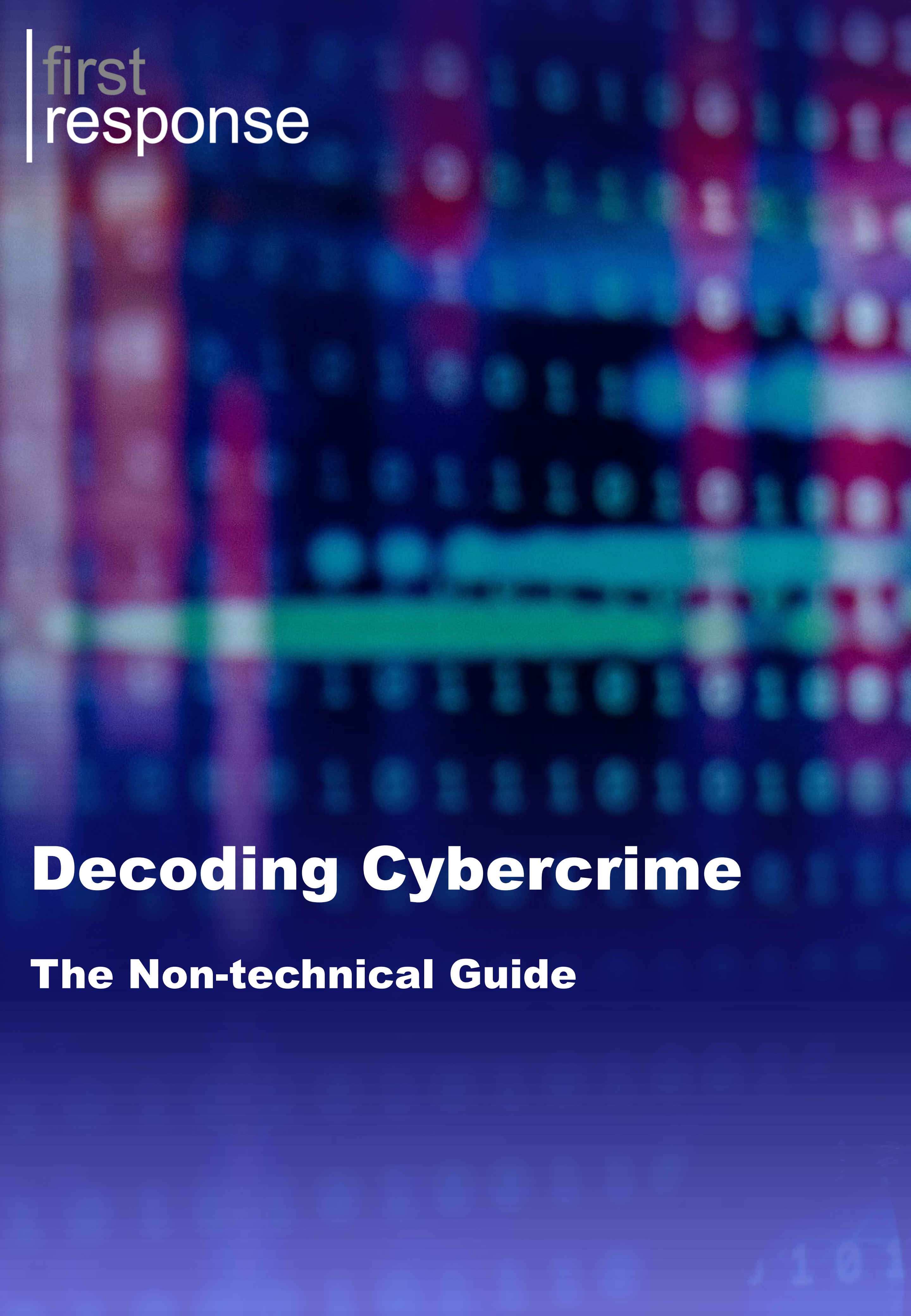
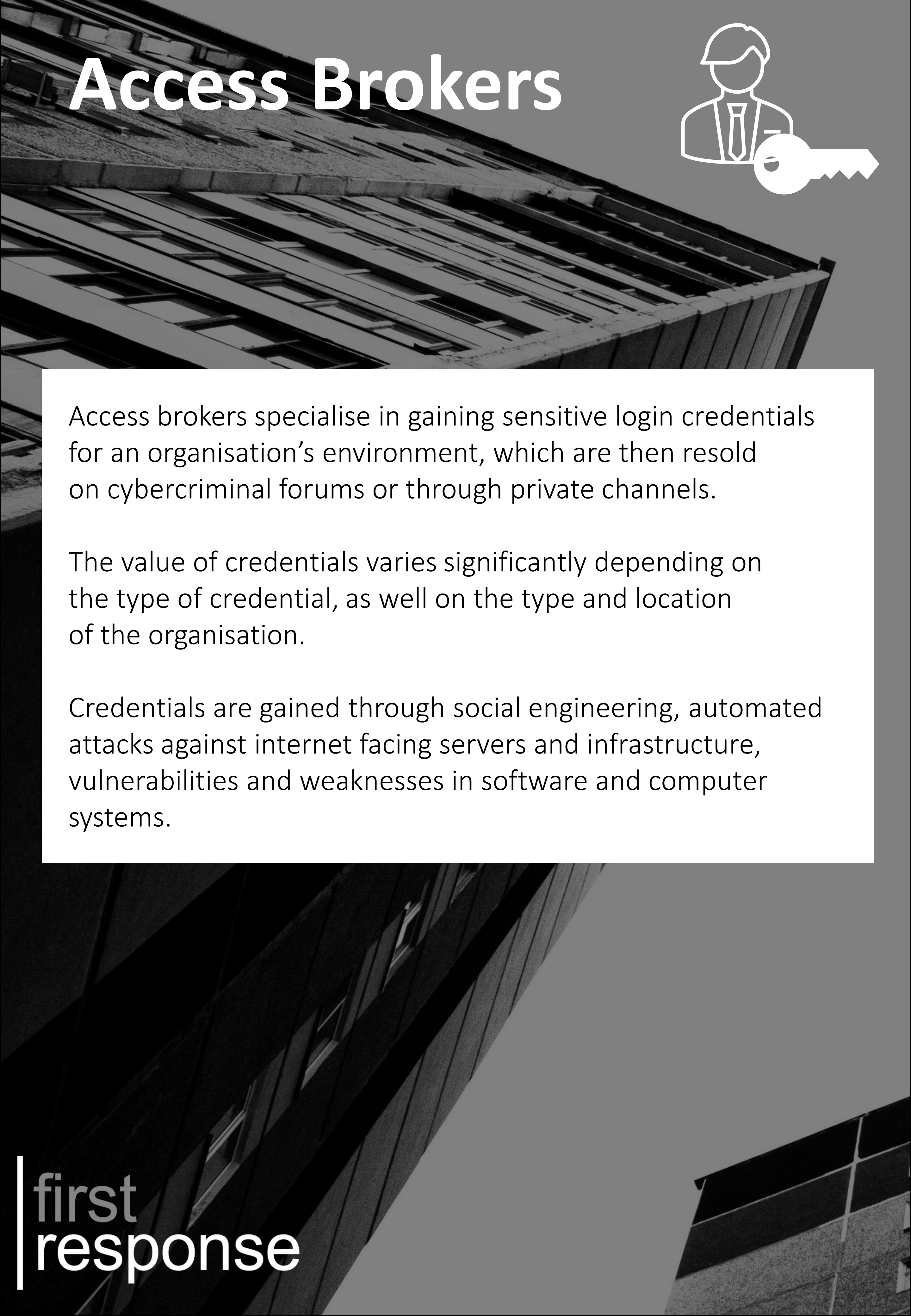
first response



Decoding Cybercrime

The Non-technical Guide



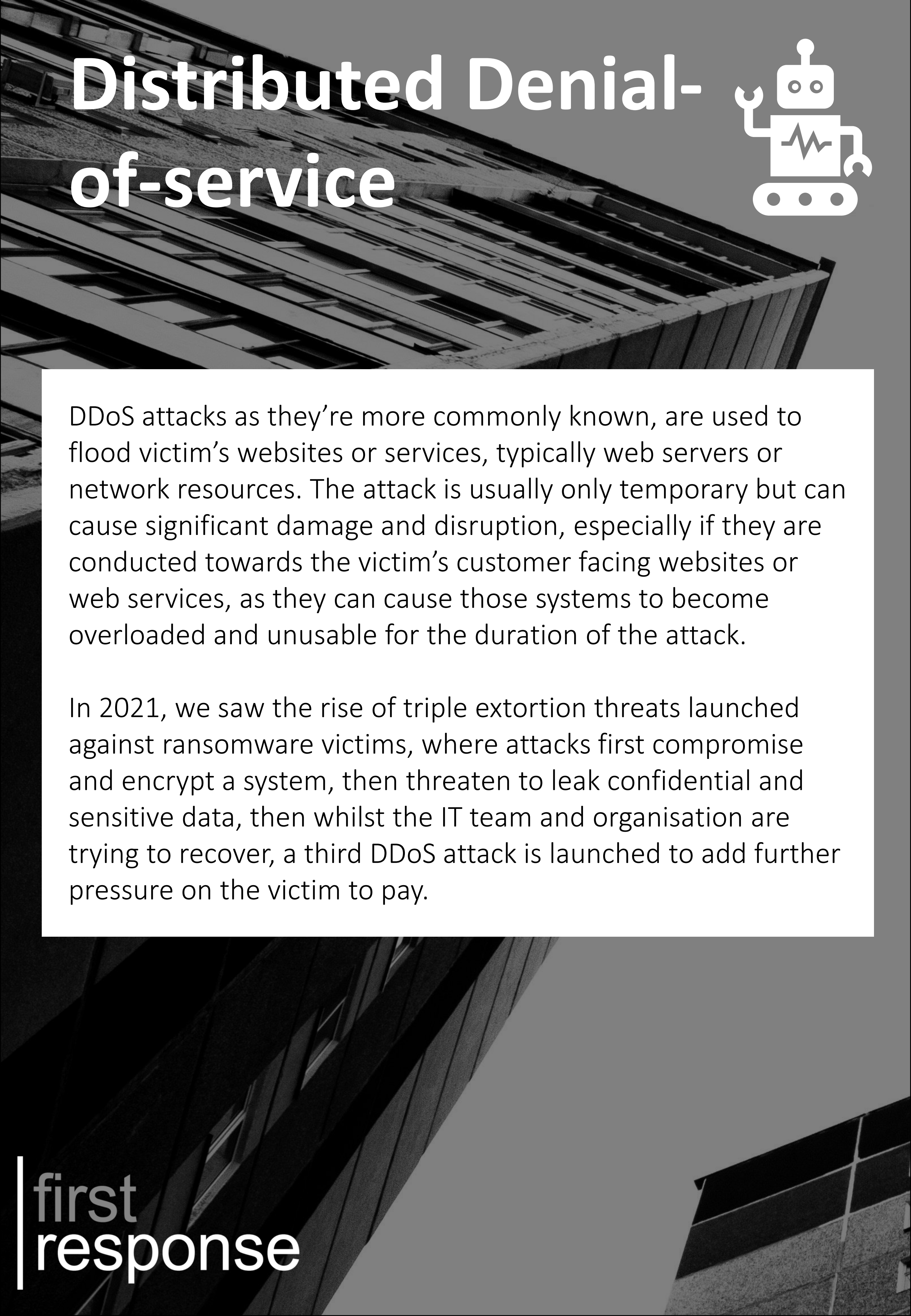
Access Brokers

Access brokers specialise in gaining sensitive login credentials for an organisation’s environment, which are then resold on cybercriminal forums or through private channels.

The value of credentials varies significantly depending on the type of credential, as well on the type and location of the organisation.

Credentials are gained through social engineering, automated attacks against internet facing servers and infrastructure, vulnerabilities and weaknesses in software and computer systems.

first
response

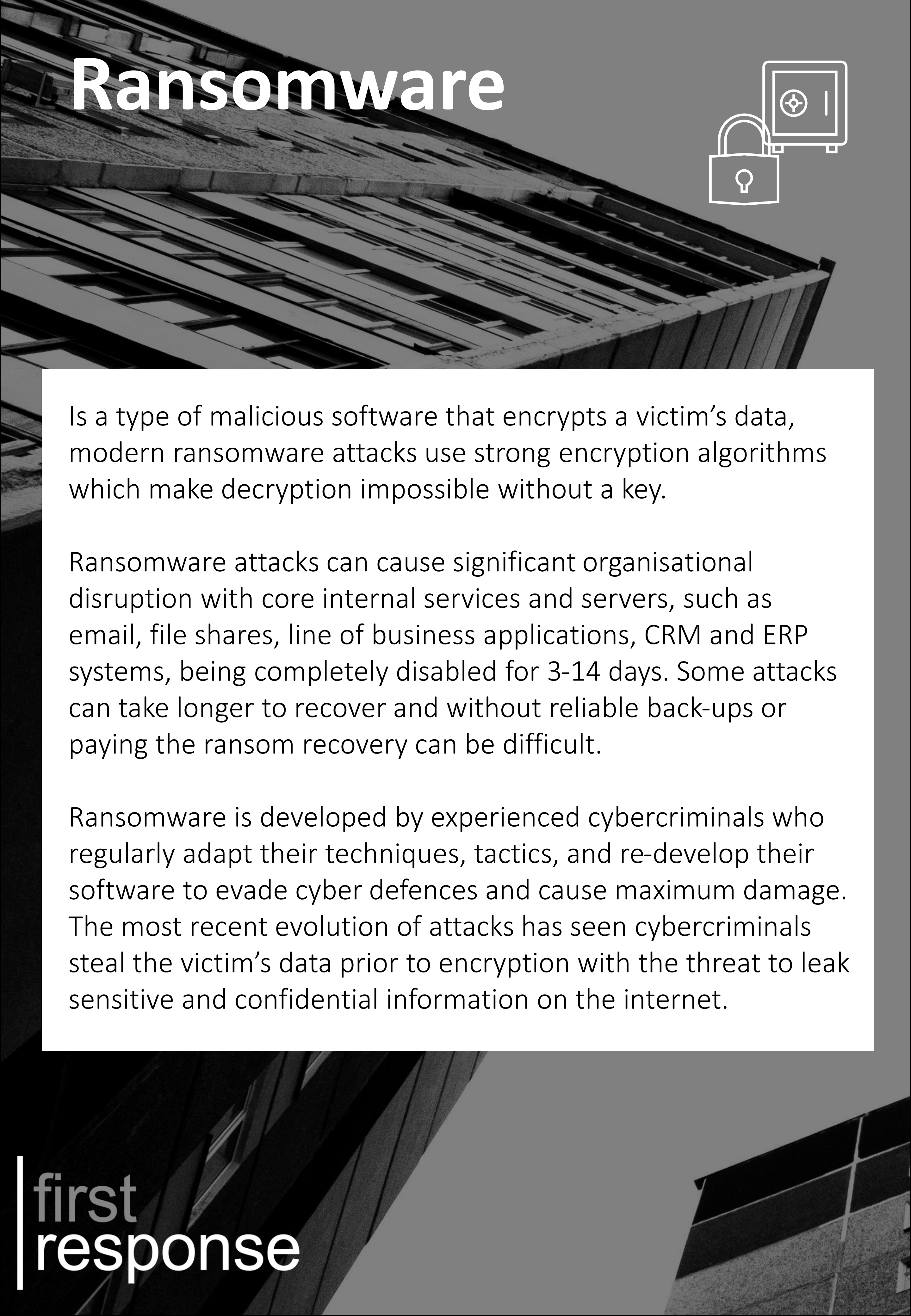


Distributed Denial-of-service

DDoS attacks as they’re more commonly known, are used to flood victim’s websites or services, typically web servers or network resources. The attack is usually only temporary but can cause significant damage and disruption, especially if they are conducted towards the victim’s customer facing websites or web services, as they can cause those systems to become overloaded and unusable for the duration of the attack.

In 2021, we saw the rise of triple extortion threats launched against ransomware victims, where attacks first compromise and encrypt a system, then threaten to leak confidential and sensitive data, then whilst the IT team and organisation are trying to recover, a third DDoS attack is launched to add further pressure on the victim to pay.

first
response



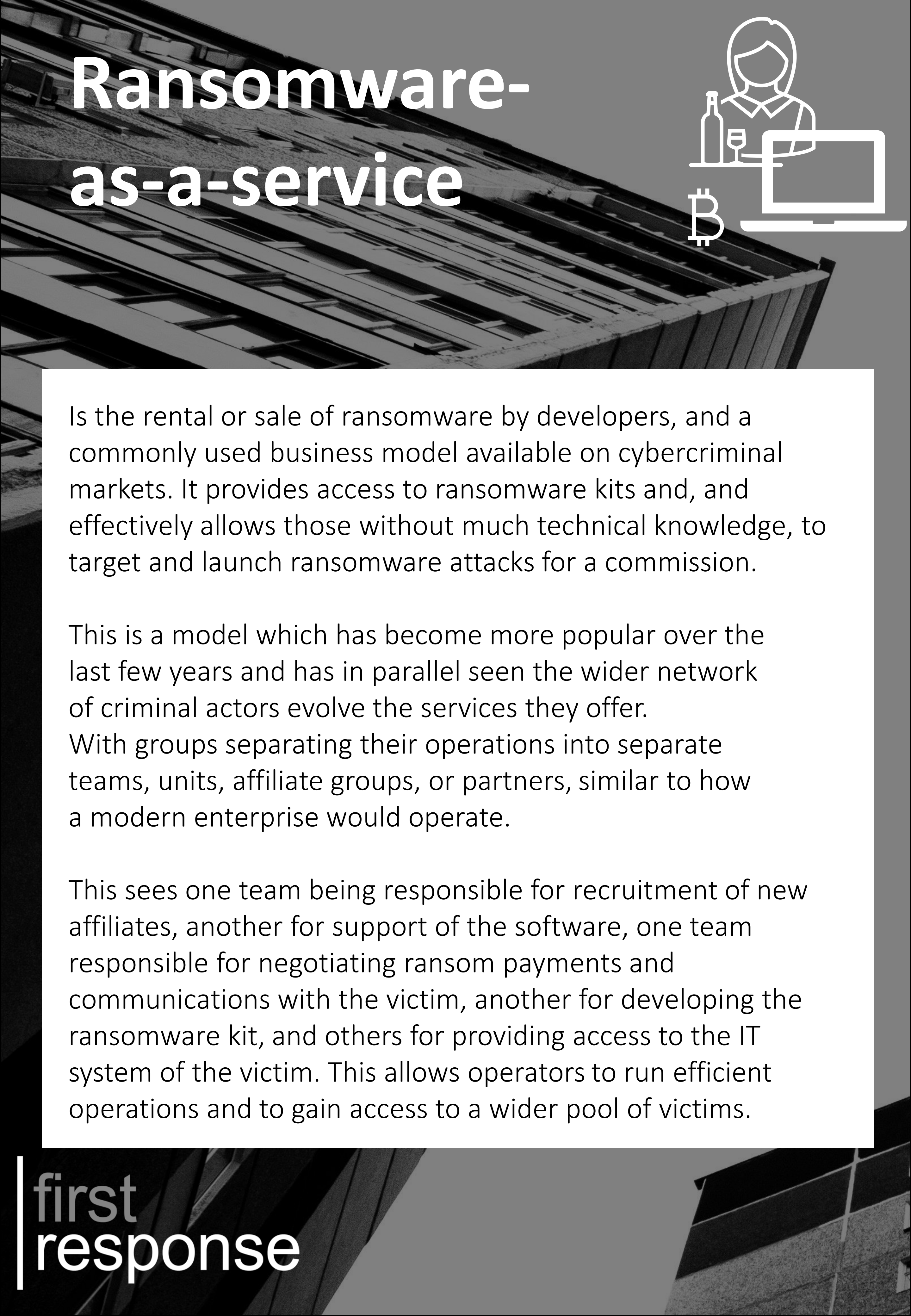
Ransomware

Is a type of malicious software that encrypts a victim’s data, modern ransomware attacks use strong encryption algorithms which make decryption impossible without a key.

Ransomware attacks can cause significant organisational disruption with core internal services and servers, such as email, file shares, line of business applications, CRM and ERP systems, being completely disabled for 3-14 days. Some attacks can take longer to recover and without reliable back-ups or paying the ransom recovery can be difficult.

Ransomware is developed by experienced cybercriminals who regularly adapt their techniques, tactics, and re-develop their software to evade cyber defences and cause maximum damage. The most recent evolution of attacks has seen cybercriminals steal the victim’s data prior to encryption with the threat to leak sensitive and confidential information on the internet.

first
response



Ransomware-as-a-service

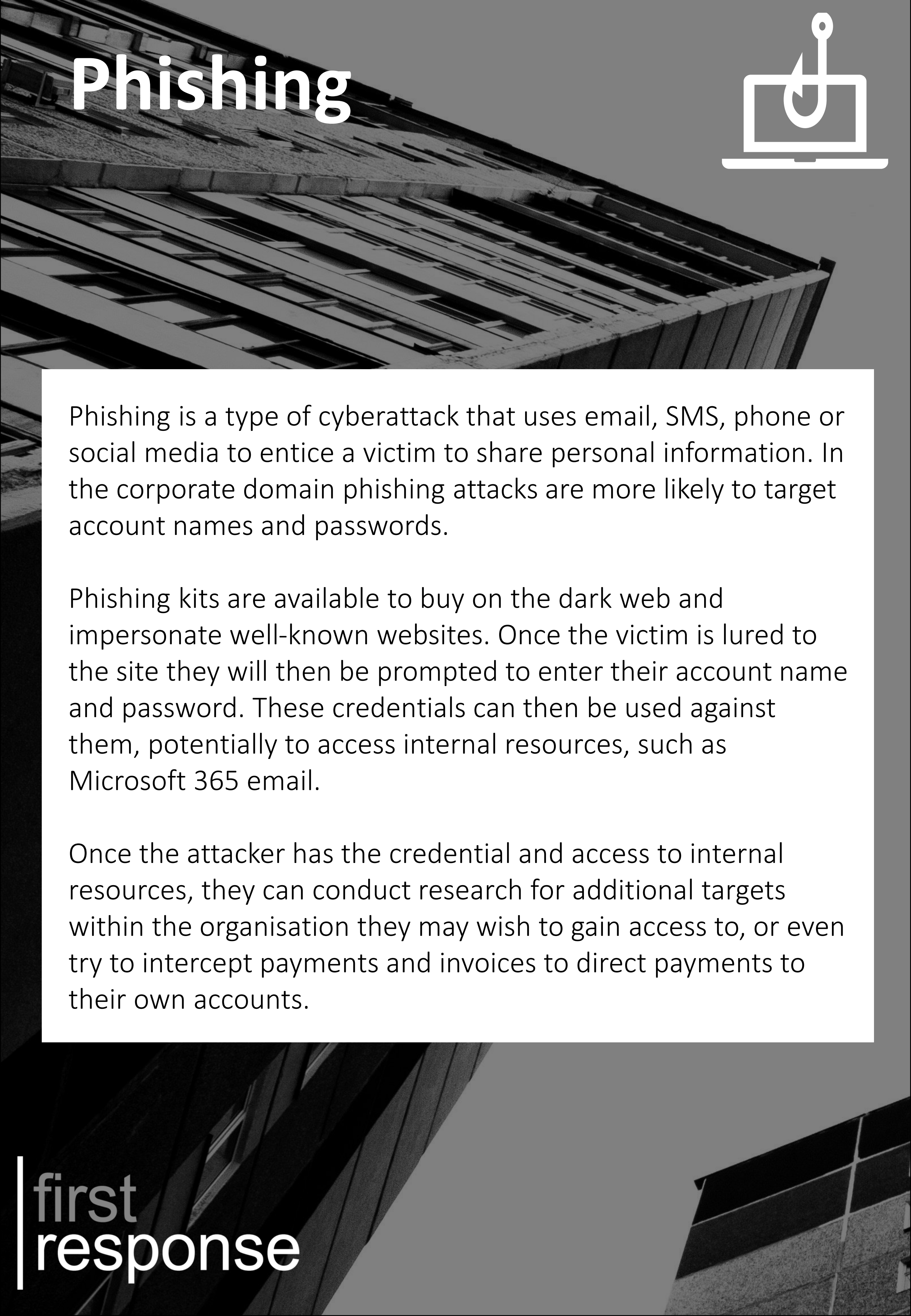
Is the rental or sale of ransomware by developers, and a commonly used business model available on cybercriminal markets. It provides access to ransomware kits and, and effectively allows those without much technical knowledge, to target and launch ransomware attacks for a commission.

This is a model which has become more popular over the last few years and has in parallel seen the wider network of criminal actors evolve the services they offer.
With groups separating their operations into separate teams, units, affiliate groups, or partners, similar to how a modern enterprise would operate.

This sees one team being responsible for recruitment of new affiliates, another for support of the software, one team responsible for negotiating ransom payments and communications with the victim, another for developing the ransomware kit, and others for providing access to the IT system of the victim. This allows operators to run efficient operations and to gain access to a wider pool of victims.

first
response

Phishing



Phishing is a type of cyberattack that uses email, SMS, phone or social media to entice a victim to share personal information. In the corporate domain phishing attacks are more likely to target account names and passwords.

Phishing kits are available to buy on the dark web and impersonate well-known websites. Once the victim is lured to the site they will then be prompted to enter their account name and password. These credentials can then be used against them, potentially to access internal resources, such as Microsoft 365 email.

Once the attacker has the credential and access to internal resources, they can conduct research for additional targets within the organisation they may wish to gain access to, or even try to intercept payments and invoices to direct payments to their own accounts.

first
response

About First Response

Established in 2013, First Response is a cybersecurity, digital forensics, and incident response company. Working with SMBs, SMEs & MSPs to protect their organisations and accelerate cybersecurity maturity. This is through outcome-focused consultancy and services incl. managed cybersecurity services (endpoint, network, mobile & cloud), and secure infrastructure design.

Our technical specialists comprise respected security and investigative professionals from a diverse set of backgrounds, including police cyber-crime units, the security services & enterprise network specialists.

We are headquartered in London with offices in Manchester and Rome, from where we assist our clients around the world. We also help organisations navigate the complex issues surrounding systems breaches, server compromises and data loss. Working with a wide variety of clients including banks, law firms, energy & manufacturing companies and public sector bodies.

first
response

Contact

Email: info@first-response.co.uk
Tel: +44(0) 20 7193 4905
Web: https://first-response.co.uk/

first
response