first response

Ransomware in Plain English

Ransomware

Phishing Email

Brute Force / Password Guessing

Exploiting Software or System Vulnerabilities

Exposed Credentials

Gain Persistent Access

Lateral Movement

Reconnaissance

Obtain Administrator Privileges

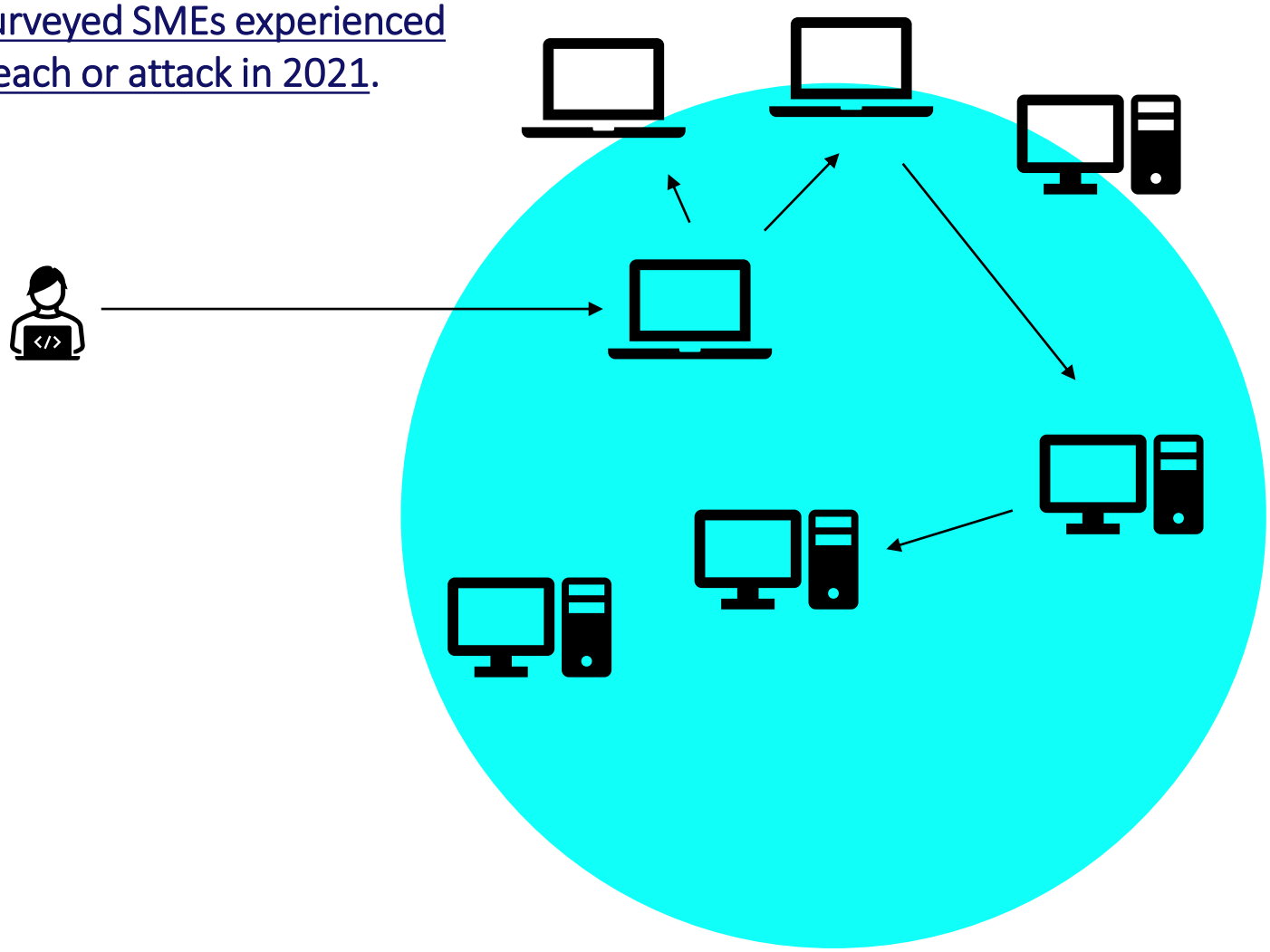
Data Exfiltration & Destroy Backups

Ransomware Deployed & Data Encrypted

What's Your Ransomware Strategy

Criminal groups are increasing the use of ransomware as a means to extort organisations

It is a threat that shows no signs of slowing down with the average cost of a data breach totalling $4.24m, organisations of all sizes are at risk, with the National Cyber Security Centre reporting that 38% of surveyed SMEs experienced a breach or attack in 2021.



What's the Risk

In 2021 we saw the devastating affect ransomware could have on critical national infrastructure.

The Conti ransomware group, attacked the Irish Health Service Executive, reportedly requesting a ransom for $20m. Reducing the number of appointments by 80%.

The Colonial Pipeline attack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack by Darkside asking for a ransom of $4.4 million.

What we don't see are the many smaller organisations that are impacted by ransomware. With the FBI tracking more than 100 active ransomware groups.

38% of surveyed SMEs experienced a breach or attack in 2021

Source: National Cyber Security Centre Annual Review 2021, https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf

How Ransomware Spreads

Ransomware attack groups focus on two main approaches to gain access to an environment; attack an internet facing system or using a phishing email with malicious content.

Once the attack group has gained access, they will then try to push that access to its limit. Gathering credentials with the goal to gain full system access, conducting reconnaissance about the organisation and the system, pivoting or moving laterally from one system to another, finding and stealing sensitive or confidential information, exfiltrating that data, deleting or disabling backups, then finally deploying the ransomware payload and encrypting as much of the core servers and services as possible.

The encryption of servers and services will lock the organisation out of its own IT system and shut down the day-to-day operations. Without the encryption key, or reliable backups it is often impossible for the business to bring the system back online. To add further insult to injury, the threat actors will then often threaten to leak corporate information unless the ransom is paid.

Recovery can take anywhere from a few days to weeks or months.

What You Can Do

In October 2021, Lindy Cameron the chief executive of the UK's National Cyber Security Centre warned that "Ransomware presents the most immediate danger to the UK businesses and most other organisations."

Ransomware attacks can be extremely disruptive to organisations, with critical business systems often being offline from a few days to weeks or months. Make sure cybersecurity is a board-level concern and ensure there is a dedicated budget and resources are aligned.

Speak to IT partners and service providers that you work with, and ask what their experience is with dealing with ransomware attacks. Consult with cybersecurity specialists if you feel your providers lack the necessary experience or skills.

Create, document, and rehearse an incident response plan. Plans should be rehearsed on an annual basis and include both internal and external stakeholders, such as senior management, IT, HR, legal, finance, and service providers.

Develop and implement a backup plan for your organisation. Implementing offline backups that are not connected to your network or devices, can help reduce the risk of a ransomware attack leading to your backups being deleted. The recovery process for backups should be regularly tested.

Technical Measures

1. Build a reliable asset management process to identify what needs to be protected and who is responsible. This should include the identification of critical assets and determine the impact to these if affected by a ransomware attack. Ransomware attack groups will usually disable critical business systems including telephony, email communications, payment services, file servers, business applications, CRM and ERP systems.

2. Require multi-factor authentication (MFA) across the organisation. MFA can stop the use of stolen credentials from being easily reused.

3. Ensure known vulnerabilities of devices and infrastructure are regularly patched, especially with critical vulnerabilities and with security-enforcing devices on the network, such as firewalls and VPNs.

4. Ransomware attacks are usually stealthy and able to evade detection from basic antivirus and anti-malware products. So consider implementing behavioural-anomaly-based detection technologies such as Endpoint Detection and Response (EDR), or Extended Detection and Response (XDR).

5. Enforce the principle of least privilege. Administrator accounts should have the minimum permission they need to do their tasks. Ensure there are unique and distinct administrative accounts for each set of administrative tasks. Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).

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