Ransomware:
What SMBs should know

Ransomware is one of the biggest threats to businesses today, and with new attacks hitting the news on a daily basis, the risk can seem overwhelming. But what actually is ransomware, and how can businesses protect themselves? In this series, we will take an in-depth look at ransomware, highlighting specific methods of attack such as email compromise, vulnerabilities and the Remote Desktop Protocol, delving into supply chain attacks, and giving advice on how businesses can mitigate the risk .

What is ransomware?

Ransomware is a type of cyberattack that seeks to encrypt, prohibit or severely restrict access to the victim's data, device or entire systems until ransom demands have been met and the user's data is restored. The damage caused can be severe and widespread. The largest ransomware attack to date – **WannaCry** – affected more than 230,000 computers across 150 different countries back in 2017.

Ransomware today is commonplace, and has been exacerbated by the current hybrid work trend. Between January 2020 and June 2021, there have been an incredible 71 billion ransomware attacks worldwide. While no one is safe, **SMBs have increasingly become attractive targets for attacks**. This is because, although they hold plenty of valuable customer and financial data, they often lack the robust security measures employed by large corporations. What also exacerbates the situation is that because they don't see themselves as potential targets, they are less likely to back up their data.

While we have seen several variants of ransomware since its emergence in 1989, they can generally be broken down into four main types:

- **Screen locker ransomware**, which blocks access to your device through a screen locker
- **PIN locker ransomware**, which changes your device's PIN code, rendering its content and functionality inaccessible
- **Disk coding ransomware**, which encrypts the MBR (Master Boot Record) and/or critical file system structures, preventing you from accessing your operating system
- **Crypto-ransomware**, which encrypts the files on your disk

How does it work technically?

As employees have moved to working from home and accessing internal company systems and services via Remote Desktop Protocol (RDP), and there's an increasing trend of employees **bringing their own devices to work (BYOD)**, cybercriminals have leveraged this as a vector to deliver ransomware as well as other malicious threats. However, this isn't the only vector being used. Malspam and phishing campaigns delivering dodgy documents, malicious macros, harmful hyperlinks and botnet binaries also remain popular.

Then there are cybercriminals who run **ransomware as a service (RaaS)** schemes to gain access to a machine via known vulnerabilities and then move laterally across the network, before deciding where to encrypt. Others conduct supply-chain attacks to access entire IT ecosystems. By commandeering popular managed service provider (MSP) platforms and productivity tools, threat actors can unleash ransomware across multiple networks at scale.

How does it work psychologically?

Ransomware works by **placing pressure on its targets**. This could be the pressure of reputational damage, business outages or even legal and financial penalties. Its effectiveness has led to hundreds of millions of dollars ending up in the accounts of cybercriminals. Recent ransoms, such as the $70 million demanded by Sodinokibi in the Kaseya attack or the $40 million paid by CNA, demonstrate the scale of the problem in 2021.

Unfortunately, this has led to a vicious circle. As large sums flow into the coffers of ransomware gangs, it allows them to further develop their RaaS business model and onboard numerous new affiliates.

Don't become a statistic

Ransomware turns an unfortunate malware incident into **psychological warfare that aims to force victims to act against their own will and best interests**. Realizing you have become a victim generally doesn't take long. Ransomware will usually inform you of its presence soon after affecting your devices by displaying a ransom note on your screen, adding a text file to the affected folders, or changing the file extension of the encrypted files. Operators rarely stay in the shadows for long.

Make sure you don't become a statistic. As with many things in life, prevention is better than the cure. To minimize the risk of ransomware, ensure you don't cut corners. Implement a comprehensive security solution for proactive protection.