On 20 March 2020 the FBI issued an alert warning of the threat to the healthcare sector from malware that was being deployed in supply chain attacks. At a time when healthcare organisations across the globe are dealing with the COVID-19 pandemic, cyber attacks against these organisations have the potential to cause significant harm including the loss of life.

Key: Increasing sophistication

Critical Vulnerabilities
Although not yet exploited in the wild, critical vulnerabilities are regularly identified in medical equipment which, if compromised could be catastrophic and lead to loss of life. Vulnerabilities, such as ‘Sweyntooth’, ‘Bluekeep’ and ‘MDhex’, could allow attackers to crash critical devices such as pacemakers or glucose monitors.

Supply Chain
The FBI has released three advisories so far this year warning of supply chain attacks on the healthcare sector using the ‘Kwampirs’ malware. The FBI have indicated that the threat actors gained access to hospitals via supply chain attacks against both software and hardware products. Furthermore, some of the software packages compromised by the Kwampirs actors include programs used for management of Industrial Control System components in hospitals.

Ransomware
This year has seen numerous ransomware attacks focused on healthcare organisations. These can have a critical impact on patient care, in some cases seriously disrupting life saving treatment. In response, Interpol issued a Purple Notice in April, alerting police in all its 194 member countries to the heightened ransomware threat to healthcare organisations.

Malware
Attacks from Emotet and Trickbot remain a serious threat to healthcare organisations having targeted them extensively in 2019. These attacks can facilitate ransomware, and steal sensitive data. This threat is compounded by the fact that many healthcare organisations continue to use outdated and unsupported software.

DDoS Attacks
In late March the US Health and Human Services Department was subjected to a DDoS attack which appeared to be driven purely by malice. The increasing use of medical Internet of Things (IoT) devices also makes healthcare organisations more vulnerable to DDoS attacks, where infected devices can be used in botnets to launch coordinated attacks.

Phishing
Attackers are exploiting fear and uncertainty around the COVID-19 pandemic to deliver malware using COVID-19 themed phishing emails. Research has indicated that since the start of January the number of phishing emails being sent has spiked by over 600%, with many of these using a coronavirus theme.

Mitigations
Healthcare organisations should implement a least-privilege policy on their web servers as well as introducing a demilitarized zone (DMZ) between the corporate systems and the web-facing applications. Additionally, organisations should consider disabling remote access to administration panels as well as avoiding the use of default authentication credentials. The use of a reverse proxy to restrict accessible URLs to only trusted sources is also recommended. Remind individuals to refrain from opening emails and attachments from untrusted or unfamiliar sources. If possible, block or monitor file types that are not normally needed for business operations (e.g. ISO files) or should not be delivered as email attachments (e.g. SCR files).