Cyber Security 2022 Landscape

Discover the most significant methods of cyber attackers of 2021 and the forecast for cyber security threats in 2022.

Cyber security: The current landscape

The Covid-19 pandemic shook the business world in a very permanent way, with many organisations forced to adapt to a hybrid model of work. As such, the reliance upon technology has increased at an exponential rate, as has the number of opportunities for cyber criminals to compromise valuable data. This is reflected by an eye-watering 600% rise in cyber crime.

The Gov UK Cyber Security Breaches Survey revealed that the effects of this rise were felt across the board.

39% of businesses suffered a cyber security breach or attack - of which:

27% stated that they experienced cyber-attack attempts roughly once a week

1/3 reported being adversely affected by an attack

1/5 reported that they experienced a financial, data or asset loss as a result of an attack

COOLSPIRiT™

www.coolspirit.co.uk

T. 01246 454 222 E. hello@coolspirit.co.uk

Barracuda

CYBER SECURITY PARTNER

The 5 biggest cyber security threats during 2021

Phishing

By impersonating a trusted brand or person, cyber criminals trick victims into revealing sensitive data or downloading malware to their device

43% of all cyber breaches resulted from a phishing attack

A more targetted and organisation-specific form of phishing, spear phishing, was the primary method of infection for more than 65% of known cyber-attacker groups.

Ransomware

As the name suggests, this attack relies upon a type of malware that encrypts data until a ransom is paid. In this instance, the attacker exploits the victim's fear of permanent data loss or exposure to the public.

There were 3x the amount of ransomware attacks in the 1st quarter of 2021 than there were in the entire year of 2019.

The average ransomware payment soared by 82% in 2021, from $312,000 in 2020 to $570,000.

Cryptojacking

Hackers trick their target into installing malware that allows the hacker to access their device. From there, the hacker is able to use their device to generate cyrptocurrency.

25% of business are estimated to have been victim to cryptojacking.

Distributed Denial of Service Attacks (DDos)

DDoS attacks prevent users from accessing the targetted website, application, server or network by sending a large volume of traffic from botnets to overwhelm it. Typically, to regain functionaility the vitcim is forced to pay a ransom.

In 2021, DDoS attacks increased by 29% - VoIP providers were disproprotionately targeted.

Network hijacking

As remote working became the norm, businesses adopted VPNs to allow their employees to work from home. Those that did not implement proper VPN security became hot targets for cyber criminals who scouted for vulnerbailities to exploit and gain access to corporate networks.

VPN attacks increased by almost 2000%.

This highlights the dire need for more effective security measures to be taken amongst the hybrid work model.

COOLSPIRiT™

www.coolspirit.co.uk

T. 01246 454 222 E. hello@coolspirit.co.uk

The Cyber Security Forecast for 2022

The 5 key cyber-attacking trends that are expected to occur in 2022:

Internet of Things (IoT) attacks

All physical objects that are embedded with technolgoies that connect to, and exchange data with other devices over the internet are referred to as the IoT. By the end of 2022, it is estimated that the IoT will grow to 18 billion objects and unsurprisingly is a big target for cryber criminals. Once they have found and exploited a vulnerability within one object, they can then spread throughout the digital system to which the object is connected. Due to the expansion of 5G services, cellular bandwidth will increase, allowing for more connectivity of digital devices and in turn, more opportunities for exploitation.

Supply chain attacks

These types of malware infection often go undetected by vendors of legitimate applications and so the damage can be widespread and fast-acting upon release. Supply chain attacks on open-source software increased by 650% in 2021 and this is sure to increase still in 2022.

Ransomware

It's predicted that last year's rise in ransomware attacks will only continue to grow in 2022 and in fact, it appears that cyber criminals are already evolving in their practices. For instance, they are now offering Ransomware as a Service (RaaS) in which they provide subscriptions to their malware programmes so that even those without the technical knowledge are able to launch ransomware attacks.

Deep fake threats

With deep fake techology, hackers are able to bypass multi-factor and biometric authentication protect and access otherwise secure data. It is plausible that as with RaaS, hackers will also monetise and provide deep fake technologies as a service to those who are willing to pay for it. The consequences of such a thing are untold, allowing these attacks to increase at a rapid rate.

Insider threats

This occurs when a former employee retains access to the corporate network or confidential data, despite having left the company. With the rate of employee turnover remaining high, the risk of insider threats is set to increase and it is believed that is the job market is to remain this way - cyber criminals will financially incentivitise employees to carry out attacks on their behalf, internally.

COOLSPIRiT™

www.coolspirit.co.uk

T. 01246 454 222 E. hello@coolspirit.co.uk

Our expert team helps you protect your most valuable asset – data

The modern world relies on technology more than ever before. As such, digital data creation has surged, simultaneously creating a larger target for criminals - presenting threats both internally and externally. If malicious activity against your assets occurs, you cannot often see it.

COOLSPIRiT is a leading provider of Cyber Security solutions, delivering disruptive, collaborative technology - while consolidating platforms to help secure your data.

COOLSPIRiT™

www.coolspirit.co.uk

T. 01246 454 222 E. hello@coolspirit.co.uk