ProtectUK

Terrorist Cyber Threat

ProtectUK publication date
07/08/2024

Cyber attacks against UK businesses take a number of forms and vary significantly in scale and complexity. Hostile attacks against UK cyberspace are considered a Tier 1 national security risk.

Terrorist Cyber Threat Headline Assessment

Hostile attacks against UK cyberspace are considered a Tier 1 national security risk.

Cyber attacks against UK businesses take a number of forms and vary significantly in scale and complexity. Ransomware is currently the most significant cyber threat facing the United Kingdom, with the potential to be as harmful as traditional state-sponsored espionage.

It is likely that terrorist cyber activity against the UK is limited to social media and website defacement. Terrorists have shown a relatively sophisticated degree of knowledge in this regard.

With the internet becoming even more integral to the success and growth of UK businesses, it is highly likely this will create more vulnerabilities for hostile cyber actors to exploit.

There is difficulty in attributing hostile cyber activity to specific named terrorist groups or their supporter networks.

The nature of online activity and the ability to anonymise or obfuscate one’s identity means unless a specific group openly claims to have conducted an attack, terrorist cyber activity is not always identifiable.

What is a cyber attack?

Hostile attacks against UK cyberspace is considered a Tier 1 national security risk, alongside

international armed conflict, terrorism and natural disasters. Tier 1 risks are judged by the National Security Council to be the highest priorities for UK national security.

Cyber attacks are malicious and deliberate attempts by individuals or organisations to breach the information system of another individual or organisation.

Usually, the attacker seeks some type of benefit from disrupting the victim's network. The motivations for such attacks can vary significantly, but often include the desire for monetary gain or ideological motivations.

There are a broad range of cyber attacks, including:

- **Backdoor Trojans** - Backdoor Trojans are malicious software programs designed to give unwanted access to an individual. Once activated the individual can send commands or leverage full control over a compromised computer. Backdoor malware and viruses bypass authentication procedures to access systems and to prevent their presence from being detected.
- **Cross-site scripting (XSS) attacks** - Cross-site scripting attacks occur when attackers execute malicious code within a victim's browser. Upon the initial execution of code, the site usually is not fully controlled by the attacker. Instead, the attacker attaches their malicious code on top of a legitimate website, essentially tricking browsers into executing their malware whenever the site is loaded.
- **Denial-of-service (DoS)** - This is where an attack floods a system's resource, overwhelming it and preventing responses to service requests, which reduces the system's ability to perform. An attack becomes a 'distributed denial of service', referred to as "DDoS", when it comes from multiple sources, compared to just one.
- **DNS tunnelling** - Domain Name System (DNS) tunnelling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. It is a method that provides attackers a back channel to extract or steal data.
- **Phishing** - Phishing is a method whereby attackers attempt to trick users into doing 'the wrong thing', such as clicking a link that will unknowingly download malware. Although commonly associated with email, this method can be utilised by other means such as text message or social media.
- **Ransomware** - Ransomware is a form of malicious software that freezes or takes control of the victim's data, with control only being released back to the victim once they have paid the attacker a nominal "ransom" fee.
- **SQL injection** - Structured Query Language (SQL) injection is one of the most common web hacking techniques. It works through the injection of malicious code in SQL statements via web page input. It usually occurs when users are asked to enter a username and instead give

a SQL statement that attaches and runs itself on the SQL database.

Cyber terrorism

It is likely that terrorist cyber activity against the UK is limited to social media and website defacement.

It is almost certain most terrorist groups and their supporters lack sufficient knowledge and technical capabilities to conduct significantly disruptive cyber attacks against UK businesses and infrastructure. In the absence of the ability to cause widespread damage or disruption, terrorists and their supporters have adopted more limited goals, such as social media and website defacement. For example, in 2017 a hacking group associated with supporters of the Islamic State group conducted a website defacement campaign targeting NHS websites in the UK.

Daesh supporter network social media defacement

Also known as the 'Islamic State in Iraq and the Levant', or ISIL (in line with government guidance), the group is now referred to by the Arabic acronym Daesh, which is used by opponents of the group because of its similarity to the Arabic verb “da’asa”, to trample underfoot.”

In 2020, research by the Institute of Strategic Dialogue identified a decentralised network of Daesh supporters exploiting vulnerabilities in social media to spread Daesh propaganda. The network used a number of relatively sophisticated techniques to ensure their content evaded detection., including:

- **Account Hijacking** - seizing accounts from other users, using applications to intercept password reset text messages from the platform.
- **Content Masking** - overlaying ISIS content with the branding of mainstream media outlets to prevent identification and bypass Facebook’s hashing technology.
- **Link Sharing** - sharing links to extremist content on websites en masse in comment threads on social media.
- **Coordinated Raids** - members of the network organised and carried out 'raids' on other Facebook pages to hijack comment threads and trending hashtags.
- **Exploiting Text Analysis** - making use of 'broken text' (like 'b roke_n text') format or specialised fonts to evade detection from Facebook’s automatic text analysis.

Zoombombing

Zoombombing is a type of cyber-harassment in which a group of unwanted and uninvited users interrupt online meetings over video conference applications.

With the Covid-19 pandemic and the move to remote working, the use of Zoom and other similar applications to facilitate meetings became increasingly popular, leading to an increase in this type of harassment.

Zoombombing has been a notably popular methodology amongst the Extreme Right Wing (ERW) to harass individuals and communities, aiming to cause fear and distress.

With the introduction of new security features in video conference applications, instances of Zoombombing have declined but can still occur.

Ransomware

The National Cyber Security Centre (NCSC) assesses that ransomware continues to be a significant cyber threat to the United Kingdom.

Ransomware is a form of malicious software used by criminals or those who seek to extort money from victims. The software is used to freeze or take control of the victim’s data, often with a threat of said data being made publicly available, and only released back to the control of the victim once they have paid the attacker a nominal 'ransom' fee.

Although the precise costs to UK businesses from ransomware are hard to determine, a government-commissioned study in 2023 estimated that extortion is costing businesses £2.2bn per annum.

Ransomware attacks by criminals linked to Russia

In January 2023, severe disruption to the Royal Mail's overseas deliveries was caused by a ransomware allegedly linked to Russian criminals. The cyber attack affected the computer systems Royal Mail used to despatch deliveries abroad. The ransomware was claimed by ‘LockBit’ who demanded a £66 million ransom.

Also in January 2023, the Guardian newspaper suffered a ransomware attack by ‘LockBit’, where the personal data of UK staff members was accessed.

In August 2023, reportedly sensitive information belonging to the Ministry of Defence was released onto the dark web by ‘LockBit’. The data was stolen during an attack on fencing manufacturer Zaun, a supplier to the UK government.

What this means for business and the public

It is likely that should a UK business website be targeted by terrorists, this will be limited to website defacement and will have short-term reputational consequences. Although it is often very difficult to

attribute a cyber attack, UK citizens and businesses are much more likely to be targeted by criminals for financial gain than terrorists.

Cyber attacks against UK businesses are common, as highlighted in the Government's Cyber Security Breaches Survey 2023, which found that nearly a third (32%) of UK businesses had suffered from a cyber attack, with the most common methodology being phishing attempts.

Cyber security should be an important consideration when operating IT at home or in the workplace. Good practice by all users should aim to protect key devices, systems and data from theft, damage and loss.

The National Cyber Security Centre (NCSC) is the UK's technical authority for cyber threats, and provides cyber security guidance and support, helping to make the UK the safest place to live and work online.

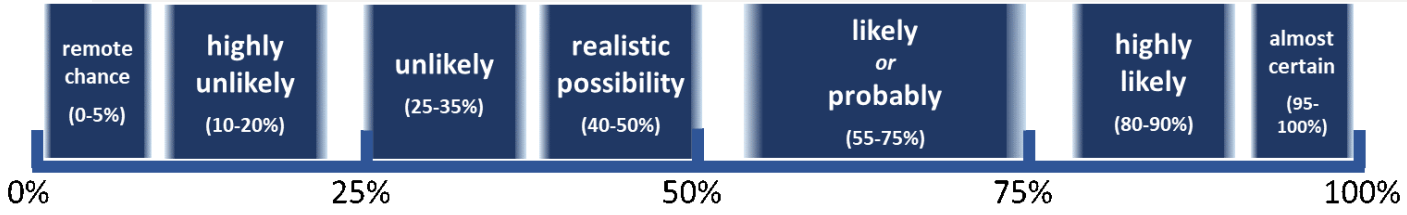
This is available for both business and the general public and can be accessed from the National Cyber Security Centre website.

Probability and Likelihood in Intelligence Assessments

When describing threats in intelligence assessments, Counter Terrorism Policing utilises the Probabilistic Yardstick.

The Probabilistic Yardstick is a tool created by the Professional Head of Intelligence Analysis (PHIA), in the UK government, to standardise the way in which we describe probability in intelligence assessments. For example, if we use the term 'likely' what we mean is 'a 55-75% chance'.

Use the scale below as a reference when reading ProtectUK Insights.



KEYWORDS

THREAT ANALYSIS
THREAT
CYBER
ATTACK METHODOLOGY
CYBER ATTACKS
CYBER SECURITY
PHISHING
NATIONAL CYBER SECURITY
TERRORISM AND CYBER THREATS
SECURITY ONLINE
NATIONAL CYBER SECURITY CENTRE

PAGE CATEGORY

THREAT ANALYSIS