baesystems.com/cyber

Cyber Security Predictions 2021

From the rise of ransomware to remote working, it is time to shore up your defences

BAE SYSTEMS

James Muir of BAE Systems Applied Intelligence lays out his 2021 cyber security predictions on ransomware, synthetic media, hacking for hire and remote working for organisations around the world.

Ransomware continues its march; policy complexities follow

The surge of ransomware attacks against organisations was **the** major cyber threat theme of 2020. We have seen more and more groups adopting the 'double extortion' model based on data theft and public victim blogs, and a 'perfect storm' of factors has contributed to the success of this criminal enterprise. We expect criminal groups to continue in this vein, evolving their tools and finding ways to collaborate. This will result in a greater number of effective attacks. We also anticipate increased use of ransomware-like attacks by unscrupulous state actors, both for financial gain, as well as for disruption under a false flag. Recent advisories by US Treasury bodies are a first sign of policy complexities to come, with legislation around ransom payment likely to emerge in a number of countries.

Financial institutions, especially those offering cyber insurance will need to watch this space closely in 2021. Whether policy measures are sufficient to stop the scourge of ransomware attacks remains to be seen; collaborative defensive and increased pursuit of the criminals are also likely to be required.

2

Synthetic media goes mainstream, and threat actors capitalise

Technological developments in synthetic media (AI-generated faces, voices, etc.) have boomed in 2020 and will continue to do so into 2021. The benefits of this could be many-fold. For example, NVIDIA has proposed an AI-based mechanism to minimise bandwidth use in videoconferencing, with impressive results. However, time has told us that threat actors are always quick to exploit technological advances to support to their goals. The immediate use of 'deepfakes' for disinformation will be in the interests of a number of different threat actors with political or subversive goals.

Synthetic media will also be increasingly used for new twists on social engineering - e.g. AI-generated faces on social media profiles, fictitious personnel at spoofed/front companies, etc., and an array of potential uses of this technology for cybercrime and fraud is likely to be seen in the wild. A scenario in which 'your CEO' requests over Zoom that a wire transfer is made, when in reality it is a real-time deepfake video overlay and audio from a cyber-criminal, is increasingly a possibility.

3

Hacking-for-hire becomes a boom industry and intrigue abounds into the 'employers'

2020 has seen a huge increase in disclosure of threat activity constituting 'hacking for hire'. Often referred to as corporate or industrial espionage, or 'mercenary' activity, an increasing number of threat groups and corresponding companies have been implicated in this.

We predict that further to the apparent nexuses for these companies in India and Russia, more groups and centres will appear. To date, organisations and individuals in legal, financial services and government sectors have been heavily targeted, but the ultimate 'hirers' of this activity remain unclear. We expect more investigative effort will shine a light on this eco-system in 2021.

4

The implications of remote working become clearer

Much has been written about the potential implications of increased remote working on organisational security, with particular attention to increased attack surface through additional devices and different connectivity mechanisms. Survey data has suggested that lack of awareness around security best practices has led to an increased rate of data breaches. There have been reports of 'WFH compromise' leading to 'organisational compromise' – although it is unclear whether these would have occurred from the office anyway.

Definitive trends in whether remote working has led to increased prevalence of specific attack paths are currently unclear. However, we expect further attention from both attackers and defenders in 2021. As a global movement to work from home has shifted the enterprise 'last mile' to include consumer network-enabled technology, 2021 shapes up to be the beginning of a new revolution in adversary tactics, tools and strategy.

Organisations go back to basics to shore up defences

'Doing the basics right' has been a mantra of many cyber security standards bodies for a number of years. Continuing a trend we saw in 2020, we expect additional emphasis on this in 2021 as organisations realise that implementation of patching regimes and appropriate authentication controls are a pre-requisite for good security – and that complex technical solutions are rarely the answer in and of themselves.

This has particular relevance for prevention of ransomware attacks, where board recognition of the threat and preparedness for attack - both in response and in ensuring that backups are functioning and resilient to attack - are vital. The transition to cloud has been undoubtedly accelerated by the COVID pandemic, further shifting monitoring away from the enterprise for early warning. The Verizon DBIR 2020 highlighted the rise of breaches due to cloud misconfigurations (pre-pandemic) – this is likely to feature heavily next year too, but is a 'basic' that should receive increased emphasis.

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 87,800 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/cyber

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai