Digital Intelligence

BAE SYSTEMS

2023 Cyber Predictions

BAE Systems Digital Intelligence's Adrian Nish, Head of Cyber; James Muir, Threat Intelligence Research Lead and Miriam Howe, Lead Cyber Consultant, lay out their 2023 cyber predictions.

2023 could be the year 'the world is held to ransom'

"Over the last few years, ransomware attacks have risen in both sophistication and frequency. We've seen targets move from individual consumers, to small businesses, to large enterprises. In 2022, we even saw entire countries being held to ransom, including attacks on Costa Rica and Montenegro that crippled multiple government services.

"Today's ransomware criminals are getting bolder, homing in on large organisations that deliver critical value to society. As this landscape evolves, it is not outside the realm of possibility that 2023 could be the year that cyber criminals hold 'the whole world to ransom'; from exploiting flaws in widely-used operating systems, to supply chain attacks in software used globally, to targeting international critical national infrastructure.

"Getting ahead of attackers is therefore paramount. This will involve collaboration between public and private sectors, sharing knowledge and working together to detect and respond to potential threats." **Adrian Nish, Head of Cyber**

Adversarial AI reaches a tipping point to become a real world concern

"There is still little evidence around the use of AI for launching cyber attacks. A more concerning aspect to consider, however, is the field of adversarial AI, whereby target AI systems are exploited as part of an attack.

"In 2023, it is possible that this type of threat will reach a 'tipping point', moving from being mainly an academic matter to a real-world concern. We can expect to see more attempts from cyber criminals to poison training data and confuse AI systems with special inputs.

"One way an adversarial AI attack could lead to real-world consequences is if vulnerabilities are found in widely-used AI frameworks or codebases. It is likely that attackers will develop easy-to-use tools to exploit these vulnerabilities, potentially opening up a whole new class of attack. How and when this may happen remains unclear, but the creation of new security policies to mitigate potential threats will become increasingly important." **James Muir, Threat Intelligence Research Lead**

Developments within the cyber insurance market will have serious, knock-on impact effects

"In 2022, the rising threat of ransomware attacks led many insurers to raise premiums and reassess coverage. Going into 2023, Lloyd's of London announced that its insurance policies will no longer cover losses from state-sponsored cyber attacks, effective from March. We can expect these dynamics to heavily impact organisations. Many will find themselves without appropriate coverage and be required to use emergency incident response services outside of their existing arrangements.

"The change in cyber insurance policy could also affect government-led attribution of cyber attacks to state entities, which is often a challenging task in itself. All of these factors combined means that if a NotPetya style incident were to occur, the repercussions could be severe." **James Muir, Threat Intelligence Research Lead**

Energy security and cybersecurity to converge

"As more focus is placed on building a more sustainable future, the motivations for energy-related cyber attacks will likely increase across the entire threat landscape. At the low end of sophistication, we have already seen numerous scams related to energy bills, including fake emails or texts to steal individuals' personal information. At the high end, the potential for state actors to disrupt energy networks looms large in certain regions.

"As companies across the globe look to green agendas and innovation in 2023 and beyond, new opportunities for threat actors will doubtless arise. Next year, we could see actors find other links between energy security and cyber security, such as espionage efforts into green technology or energy policy, along with environmental hacktivism." **James Muir, Threat Intelligence Research Lead**

Retaining and upskilling mid-level cybersecurity employees will be a top priority

"In recent years, the cyber skills shortage has had a serious impact on organisations' abilities to mitigate emerging digital security risks. As the public and private sectors have collaborated to bridge the gap, we have seen more programmes - such as CyberFirst Girls - dedicated to helping young people from all backgrounds enter into cybersecurity careers.

"While these efforts are very welcome, many organisations are also struggling to find and retain people with mid-level experience. To truly bridge the cybersecurity skills gap we also need to look at upskilling employees at all levels of their career. In 2023, it is likely that we will see an increasing number of learning and development programmes aimed at mid-level employees." **Adrian Nish, Head of Cyber**

The UK government will evolve its cyber capabilities in line with the National Cyber Strategy

"The publication of the National Cyber Strategy a year ago embedded cyber power as a key thread throughout the UK government's vision for the future. Since then, we've seen government stakeholders engaging with confidence on their cyber objectives.

"In 2023, we expect that there will be greater focus on stretching and evolving the UK's existing cyber capabilities, which will mean entrenching partnerships and joining up effects across government. As success cannot be achieved by the government alone, we expect there will be a concerted effort to engage and co-opt industry across a spectrum of pursuits and through a range of tools and incentives.

"We can also expect to see more consolidation of cyber and the electromagnetic activities and an integration of this military concept with other cyber pursuits across Defence and government." **Miriam Howe, Lead Cyber Consultant, BAE Systems Digital Intelligence**

5G rollouts will widen the attack surface

"Predicting the direction of travel for the 5G threat landscape is not a straightforward task. The 5G standard itself offers significant security improvements compared to its predecessors like 4G and LTE. But the infrastructure required to implement full 5G rollout – with increased dependence on IT, as well as virtualisation and cloud infrastructure – could increase the attack surface and expose vulnerabilities.

"When looking at radio access networks (RAN), for example, security researchers have pointed to poorly configured virtualised environments in existing OpenRAN deployments, including numerous issues in Kubernetes configurations.

"On the core network side, as the rollout and implementation of new features becomes more complex, it is possible that we'll see security misconfigurations that impact wider 5G networks. Adopters of 5G must therefore pay greater attention to the risks surrounding 5G security, with specific high-threat use cases – such as military scenarios – having been discussed in whitepapers this year, including CCDCOE's research report on Military Movement Risks From 5G Networks." **James Muir, Threat Intelligence Research Lead**

BAE SYSTEMS

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

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