BAE SYSTEMS

2022 Cyber Security Predictions

BAE Systems Applied Intelligence's Dan Alexander (Head of Threat Intelligence) and Kyle Draisey (Senior Solutions Architect) lay out their 2022 cyber security predictions.

#1

Return of the Bank Heist

Attacks against payment systems boomed in the years following the infamous Bangladesh Bank Heist, however, in the past year or so, the number of bank heists dropped significantly. The global coronavirus pandemic is a key contributor to this, with closed borders and limited international travel hampering the ability for money mules to enter countries to retrieve stolen funds. As international travel once again becomes the norm, we expect mules to return and bank heists to follow.

#2

Ransomware Operators Move Away from Bitcoin

Ransomware has dominated the threat landscape in 2021 and is not something that is going to disappear anytime soon. Law enforcement is increasing their focus in this area, with a number of operations to disrupt and arrest the operators within 2021. In rare cases, Law Enforcement has been able to recover funds following a ransom payment through tracking Bitcoin transactions. As Ransomware operators look to avoid law enforcement, we expect them to evolve their tactics and look for more ways to make it more difficult to track and recover funds.

A logical next step to this is the movement away from using Bitcoin to other cryptocurrencies, such as Monero, where the tracing is far more difficult.

#3

A Blurred Response

In 2022, we expect cyber attackers to have an increasing focus on employee's personal devices as a stepping point before entering the target organisation. We expect to see a strong social engineering aspect, with attackers reaching out to targets through social networking and instant messaging services before delivering malware to their personal device.

This will in turn bring up challenges of where the limits of protecting an organisations truly are. Incident response teams are often limited to the boundaries of the corporate network, however, we expect this to be challenged with a need to update incident response plans and privacy concerns.

#4

Initial Access via IOT Devices

The number of Internet of Things (IOT) devices has continued to grow at a rapid pace, however, cyber criminals have yet to really take advantage of this outside of botnet assembly which is used in DDOS attacks. IOT devices are regularly found to have vulnerabilities, however, they are often excluded from an organisation's patching regime.

In 2022, we expect attackers to explore IOT vulnerabilities in more creative ways and use this as an initial access vector to access target networks.

#5

Business Email Compromise using Deepfake Voice

Business email compromise scams involve criminals impersonating c-level executives, finance teams, or even suppliers to trick employees into making large payments or changing the payment process to send funds to a scammer's bank account. Security advice has been to double, or even triple-check the requests out-of-band through an alternative means to ensure the request is genuine. This may have previously been just a walk down the corridor in the office to check, however, with many people working remotely, more and more of those verification checks are now happening over the phone, this presents new opportunities for the criminals. In 2022, we expect more criminals to utilise the rapidly developing deepfake technology to accurately impersonate the voice of the executive or finance team member making the request seem more legitimate and therefore more successful for the scammer.

#6

Purple is the New Red

Threat intelligence-led Red Teaming has become a global standard for organisations to strengthen their security postures, however, there is often a disconnect from those performing the exercise (Red Team) and those defending against it (Blue Team). This results in missed opportunities in the detection of offensive actions within networks, systems and platforms.

By having Red and Blue work closely together in Purple team allows organisations the ability to improve the effectiveness and efficiencies in network monitoring, threat hunting, and detecting vulnerabilities in a much shorter time period. In 2022, we expect more security teams to employ threat intelligence-led Purple Team practices throughout their operational and engineering lifecycles.

#7

Effort to Prevent Small Fails Turning into Mass Failure

In today's connected world, a small outage or failure can lead to serious downstream impacts, affecting products and services we all rely on day-to-day. Examples from the past year include the Colonial Pipeline ransomware incident which resulted in fuel supplies running dry in some locations in the US and the major Facebook/WhatsApp outage caused by a misconfiguration during routine maintenance.

Operational resilience is an area often talked about in the financial sector, however, we expect there to be a greater need for this across our critical national infrastructure. We expect more concerted efforts by Western Governments to ally with the non-profit and private sectors to collaborate against emerging cyber threats, but this will likely take years to turn into fruition. Therefore in 2022, we expect to see a number of initially seemingly innocuous events and failures which turn into major failures affecting the supply of goods and services we rely on.

BAE SYSTEMS

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

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