- Cybercrime / Artificial Intelligence

Cybersecurity threat predictions for 2021

Daily Mirror (Sri Lanka) · 11 Jan 2021 · 12 · BY RAJESH MAURYA

In 2020, we saw many rapid changes on a global scale as organisations across the world attempted to adapt to a new normal caused by the pandemic. Amid this shift, there were significant developments seen across the cyberthreat landscape.

Going into 2021 and beyond, we face another significant shift with the rise of new intelligent edges, which is about more than just end-users and devices remotely connecting to the network.

In Fortiguard Labs' threat predictions for 2021, we've estimated the strategies that we anticipate cybercriminals will leverage in the coming year and beyond. This includes but is not limited to predictions and insights on intelligent edge computing and advances in computing power, as well as the new wave of advanced threats that will undoubtedly arise as a result.

Each year at this time, we take a look at trends across the cyberthreat landscape, whether just around the corner or further afield. Predicting security threat trends may seem like more art than science but the reality is that combining a strong understanding of how threats develop and what sorts of technologies cybercriminals gravitate towards both to use and to exploit with evolving business trends and strategies helps make predictions a reasonable process.

Intelligent edge is a target

Over the past few years, the traditional network perimeter has been replaced with multiple edge environments, WAN, multi-cloud, data centre, remote worker, IOT and more, each with its unique risks. One of the most significant advantages to cybercriminals in all of this is that while all of these edges are interconnected many organisations have sacrificed centralised visibility and unified control in favour of performance and digital transformation.

Trojans evolve to target edge

While end-users and their home resources are already targets for cybercriminals, sophisticated attackers will use these as a springboard into other things going forward. Corporate network attacks launched from a remote worker's home network, especially when usage trends are clearly understood, can be carefully coordinated so they do not raise suspicions.

Advancements in social engineering attacks

Smart devices or other home based systems that interact with users, will no longer simply be targets for attacks but will also be conduits for deeper attacks. Leveraging important contextual information about users, including daily routines, habits or financial information, could make social engineering-based attacks more successful. Smarter attacks could lead to much more than turning off security systems, disabling cameras or hijacking smart appliances, it could enable the ransoming and extortion of additional data or stealth credential attacks.

New ways to leverage ransomware in critical infrastructures

Ransomware continues to evolve and as IT systems increasingly converge with operational technology (OT) systems, particularly critical infrastructure, there will be even more data, devices and unfortunately, lives at risk. Extortion, defamation and defacement are all tools of the ransomware trade already. Going forward, human lives will be at risk when field devices and sensors at the OT edge, which include critical infrastructures, increasingly become targets of cybercriminals in the field.

Spreading attacks from space

The connectivity of satellite systems and overall telecommunications could be an attractive target for cybercriminals. As new communication systems scale and begin to rely more on a network of satellite-based systems, cybercriminals could target this convergence and follow in pursuit.

Quantum computing threat

From a cybersecurity perspective, quantum computing could create a new risk when it eventually is capable of challenging the effectiveness of encryption in the future. The enormous compute power of quantum computers could render some asymmetric encryption algorithms solvable. Although the average cybercriminal does not have access to quantum computers, some nation-states will, therefore the eventual threat will be realised if preparations are not made now to counter it by adopting crypto agility.

Artificial intelligence will be key

As these forward-looking attack trends gradually become reality, it will only be a matter of time before enabling resources are commoditised and available as a darknet service or as part of open-source toolkits. Therefore, it will take a careful combination of technology, people, training and partnerships to secure against these types of attacks coming from cyber adversaries in the future.

AI technology needs to keep up

The evolution of AI is critical for future defence against evolving attacks. AI will need to evolve to the next generation. This will include leveraging local learning nodes powered by ML as part of an integrated system similar to the human nervous system. Ai-enhanced technologies that can see, anticipate and counter attacks will need to become reality in the future because cyberattacks of the future will occur in microseconds. The primary role of humans will be to ensure that security systems have been fed enough intelligence to not only actively counter attacks but actually anticipate attacks so that they can be avoided.

Organisations can’t do it alone

Organisations cannot be expected to defend against cyber adversaries on their own. They will need to know who to inform in the case of an attack so that the ‘fingerprints’ can be properly shared and law enforcement can do its work.

Cybersecurity vendors, threat research organisations and other industry groups need to partner with each other for information sharing but also with law enforcement to help dismantle adversarial infrastructures to prevent future attacks. Cybercriminals face no borders online, so the fight against cybercrime needs to go beyond borders as well. Only by working together will we turn the tide against cybercriminals.

(Rajesh Maurya is Regional Vice President, India and SAARC, Fortinet)