IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

In the Midst of COVID-19 we are Seeing a Pandemic of Cyber Attacks

Adrian Taylor

Adrian Taylor
EMEA Vice President
A10 Networks

Biography

Adrian Taylor is the EMEA Vice President at A10 Networks (https://www.a10networks.com) and an established sales leader with over 25 years' experience in developing global and multinational accounts, across a wide range of emerging networking technologies. Joining A10 Networks in September 2018, Adrian is responsible for driving growth through direct customer engagements, as well as leveraging channel, service provider and technology partnerships.

Before moving into his new role, Adrian spent over three years leading software sales at Brocade, which was later acquired by Pulse Secure. Prior to this, he spent 13 years in senior positions at Cisco, where he first developed a strong understanding of cloud computing, while managing teams across EMEA and Russia, and driving a large proportion of channel and cloud sales for the business.

Always one for a challenge, Adrian likes to push the limits within his role and explore new ways of driving A10 Networks' product sales forward, while finding new and disruptive routes to market.

Keywords Cybersecurity, Phishing and DDoS attacks, Cybersecurity innovation, International cyber espionage
Paper type Research

Abstract

With 2020 dominated by the start of the COVID-19 pandemic, there was also a sharp rise in cybercriminal activity. From simple phishing attacks to one of the largest DDoS attacks ever recorded, we saw the cyber threat landscape evolve and grow.

The challenges arising from these cybersecurity developments – including COVID-19 – continues to have long-term implications in 2021 and beyond. In this article, the author discusses some of the most pressing cybersecurity trends we expect as we start emerging from the pandemic.

Introduction

With 2020 dominated by the start of the COVID-19 pandemic, there was also a sharp rise in cybercriminal activity[1]. From simple phishing attacks to one of the largest DDoS attacks ever recorded, we saw the cyber threat landscape evolve and grow. At the same time, we also saw a rapid growth in the tech and cybersecurity industry. From the continued global 5G roll out to the exponential growth of the Software-as-a-Service (SaaS) industry, there were many positive developments amidst the gloom of a worldwide health emergency.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The challenges arising from these cybersecurity developments – including COVID-19 – continues to have long-term implications in 2021 and beyond. To this end, here are some of the most pressing cybersecurity trends for the year ahead.

Cybercrimes will experience a surge

It was a busy year for both attackers and hackers in 2020, as well as for cybersecurity personnel defending against the plethora of attacks to which they were subjected. There was a rise in anti-government cyber activities, a prominent example of which was the attack on FireEye,[2] allegedly by a foreign nation state-sponsored entity, where multiple tools were stolen for use in subsequent attacks.

This year, such attacks have shown to be more frequent and very specific regarding who they target. International cyber espionage has been a main motivator for cyber attacks; we see security vendors being attacked and compromised at an even greater pace. Even the attacks which happened in 2020, like the FireEye or Sunburst attack that targeted the SolarWinds supply chain, will have long-lasting effects. Investigators suspect, for example, that up to 250 organizations may have been compromised in the SolarWinds attack.

Such attacks will not only create opportunities for newer attacks, or variants/ branches of the existing ones, but have also driven cybersecurity innovation in 2021.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The intelligent edge will be weaponized

One of the major innovations driven by 5G is the implementation of multi-access edge computing (MEC). Building intelligence into the edge will boost the availability and efficiency of 5G networks. However, keeping global cybersecurity trends in mind, we can see that the intelligent edge might be hijacked by attackers for launching different kinds of attacks, both on the mobile core networks as well as on victims outside of the realm of the service provider that has been compromised. If nothing else, MEC can be used for propagating malware into different networks for drone recruitment in IoT botnets.

Low-volume DDoS attacks will be more frequent

In 2020, even though we saw one of the largest DDoS attacks ever recorded, targeting one of the biggest names in tech, a large number of DDoS attacks went unnoticed because, even though the frequency of these attacks were very high, their size was not. These high-frequency, low-volume attacks have kept the security industry busy in 2021 and may be instrumental to disabling security infrastructures or just acting as smokescreens for larger malware attacks as demonstrated in last year's Sunburst attack.

Five million DDoS weapons will be added to the global DDoS arsenal

A10 Networks has observed that the number of DDoS weapons doubled from around six million at the end of 2019 to 12.5 million in 2020. This trend will remain the same in 2021 as more IoT devices come online with each passing day, with an expected addition of at least five million weapons.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The large number of DDoS weapons will also enable attackers to launch another record-breaking DDoS attack in 2021. We will have to wait and see whether it will be made public by the victims of such attacks. 2021 needs to be the year of Zero Trust implementation.

2020 was the year of understanding what the Zero Trust model is in a practical sense. Throughout the year, we saw security vendors align their solutions with the Zero Trust model. These were adjusted as more became clear on what it means to be a Zero Trust user, device, or network, and the policy changes necessary for a successful implementation. As the COVID-19 pandemic fast-tracked the move to a SaaS model, as swathes of the global population worked from home, the importance of Zero Trust security has gained critical importance.

Organizations now understand that Zero Trust is not a specific device or vendor, but rather a series of strategic policy and practical changes that help enable better security. A successful implementation requires good understanding of what the Zero Trust model is, as well as the many diverse solutions that need to work in unison to enable its implementation.

We believe that the concept of Zero Trust has reached a level of maturity and clarity where it will become the go-to security model for all types and sizes of organizations. Sophisticated attacks like Sunburst has illustrated the need for effective Zero Trust implementation.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

SASE adoption will accelerate

Since 2020 forced most of the workforce to work remotely, attackers have been experimenting with new ways of exploiting security loopholes and shortcomings exposed by these rapid changes. This accelerated and will continue to accelerate the development and adoption of Secure Access Service Edge (SASE) solutions.

However, since the move to the cloud is not an overnight transition, many organisations still have most of their resources hosted on-premises. They will continue to struggle with maintaining the remote work model as reverting back to business as it was is no longer a popular strategy.

This, however, might be temporary as the world has now experienced a pandemic and many organizations have already started moving their businesses from on-premises to the SaaS-based model, with the trend only being accelerated by COVID-19. In summary, SASE will be an essential part of the enterprise security infrastructure as we move throughout 2021 and beyond.

2020 taught us that vigilance in cybersecurity cannot be taken for granted. As we continue to face new and persistent threats of all shapes and sizes, we need to face these threats with the best of our collective abilities. It is through collaboration that we will see innovations in cybersecurity develop at a speed like we have never seen before.

Reference

[1] Gewirtz, D (14 September 2020), “COVID cybercrime: 10 disturbing statistics to keep you awake tonight”, ZDNet. Available at https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/

[2] Sanger, D. and Perlroth, N. (8 December 2020), “FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State”, The New York Times. Available at: https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html