nsflabs Naijasecforce TECH HIVE ADVISORY

# 2020: A YEAR IN CYBERSECURITY, LESSONS AND PLANS FOR 2021

**Courtesy of the team at**
NaijaSecForce
nsfLABs and
TechHive Advisory

nsflabs

Naijasecforce

TECH HIVE ADVISORY

## Contributors and Reviewers

Rotimi Akinyele (@infosecshinobi)

Nurudeen Odeshina (@Ibn_AbdulRahman)

Remi Akintonde (@securemi)

Ridwan Oloyede (@readeroy)

Olusegun Ajiboye (@Mister_O_A)

Tojola Yusuf (@TheTojolaBilqis)

# INTRODUCTION

2020! There have been various recounts of 2020: tales of events that unfolded – the good, but mostly the bad and the very ugly. "Ugly" is too limited a term to describe some of the events which have remained with us as you read this in 2021, or maybe until 2022 (we do not know what is to come). Nonetheless, in cybersecurity, 2020 was just like every other year. Hence, we have no doubt about 2021! What could be the worst that could happen? Cyberattacks leading to ransomware? Data breaches, or theft or loss of confidential or financial information? A critical part of the internet being unavailable; or a cyberattack leading to an unfortunate actual loss of life?. There is also the nation-state cyberattack, the associated attribution and the devastation which is still being uncovered.

# HIGHLIGHTS

Email security-related threats such as phishing and other forms of social engineering continue to be the medium adopted for most of the cyberattacks witnessed in 2020. These include those leading to Business Email Compromise (BEC), the supply-chain variant called Vendor Email Compromise (VEC) and other threats that lead up to ransomware and data exfiltration. The COVID-19 pandemic and the resulting transition to remote working also brought about remote-working threats, leakage of sensitive data and financial loss. The team at nsfLABs (an initiative of the NaijaSecForce - a team of diverse Nigeria cybersecurity professionals and enthusiasts in Nigeria and Diaspora) also uncovered, reported, and supported the remediation of several threat intels associated with organizations in Nigeria and the rest of Africa. See here and here. 2020 was also not free from Distributed Denial of Service (DDoS) attacks and other technical vulnerabilities.

> *The team at nsfLABs (an initiative of the NaijaSecForce - a team of diverse Nigeria cybersecurity professionals and enthusiasts in Nigeria and Diaspora) also uncovered, reported, and supported the remediation of several threat intels associated with organizations in Nigeria and the rest of Africa.*

## Remote Working related cyber threats

Remote working became the norm due to the pandemic requiring employees to Work From Home (WFH) or Work From Anywhere (WFA). The need for virtual meetings and collaboration became an essential organisational requirement so much that Zoom's share price skyrocketed – we hope you are not mistaken like these investors. "Zoombombing" made its way into the 2020 words of the year list – a term associated with the surge observed in the unauthorised intrusion into an online audio or video conference generally by trolls or for other malicious purposes. Here is one interesting example. Compromised Zoom credentials were also discovered in underground forums. Remarkably, as a response to the public outcry and regulatory attention, Zoom engaged cybersecurity heavyweights (former Facebook CISO Alex Stamos and Katie Moussouris) and committed to security and privacy. Other online collaborative solutions such as Microsoft Teams also had their fair share of attacks to gain employees credentials.

## Phishing Emails and Spam

According to the Anti Phishing Working Group (APWG), the number of phishing attacks increased tremendously since the beginning of the pandemic. Cybercriminals took advantage of the Fear, Uncertainty and Doubt (FUD) generated by the pandemic. There were many COVID-19 themed phishing emails sent to employees, healthcare facilities, and the unemployed, especially those whose jobs were impacted. One of the notable phishing emails was titled "COVID-19 Training for Employees: A Certificate for Health Workplaces". As at Q3, 2020, the number of unique phishing sites detected and reported was 884,530. Guess what? 3 out of 4 of these phishing sites use SSL protection – the lock sign on the URL we often advise employees to look out for to determine legitimate websites, especially during cybersecurity awareness. Business Email Compromise (BEC) was also rampant with attacks targeting organisations and employees using Google Suite and Office 365 (O365) as their messaging and collaboration solutions. The actions taken by Google and Microsoft can also be read here and here, respectively, to protect business and curb the threats.

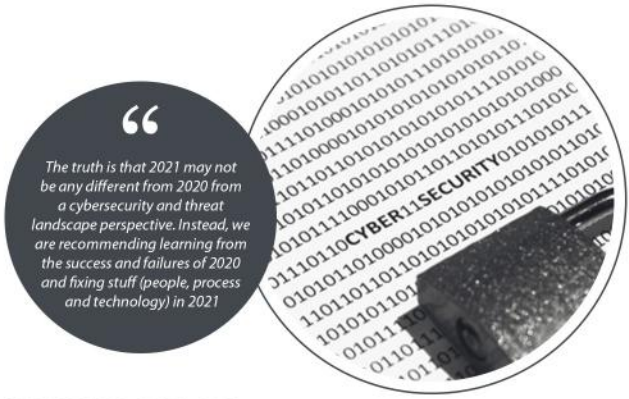
*"As at Q3, 2020, the number of unique phishing sites detected and reported was 884,530. Guess what? 3 out of 4 of these phishing sites use SSL protection – the lock sign on the URL we often advise employees to look out for to determine legitimate websites, especially during cybersecurity awareness*

## Ransomware

2020 was characterised by several ransomware attacks propagated by both known and new ransomware operators. The extent of the reach knew no bounds – see this list from the European Union Agency for Cybersecurity (ENISA) threat landscape. Educational institutions, government agencies and municipalities, hospitals and Health Management Organisation (HMOs), and other private organisations were targeted. According to this report, ransomware had a terrific year. A notable difference was that ransomware actors were more particular about weaponising data. This includes situations where the sensitive company information and/or data was exfiltrated before encrypting it. Victims chose not to pay for a decryption key, attackers threatened, and publicly released the stolen information. Personal and sensitive health records were not spared in these ransomware operators' steal and shame tactics. The IBM Security X-Force termed this blended extortion-ransomware attacks. Even if organisations can restore the encrypted files from an offline unencrypted backup, the threat actors have a copy of the data that may be dumped publicly or shared with a competitor(s). In addition to the loss of data and regulatory fines, the organisation would need to repair a damaged reputation. It is a bad-bad situation.

## National Security and Attribution

It is easy to get one's head entangled in the web of revelation of cyber-attacks by supposedly state-sponsored or nation-state attackers with a devastating global impact.? There are still dark clouds surrounding the chaos happening, the extent of which is being uncovered daily. If you read about SolarWinds, then, that is what this is about. Late in 2020, it was reported that malicious actors slipped malicious code into the solution used by several organisations, including critical government agencies worldwide. There is a term for that, "backdoor". This is also not the first case where a top-tier cybersecurity firm would be impacted where attackers targeted red-teaming tools used for offensive security assessments. A simple description is provided here. What would have been a quiet holiday period quickly degenerated into Solorigate, impacting several organisations, departments and agencies. As of December 31st, we read that it might have also impacted Microsoft. While Russia is being fingered in all of this by what Chris Roberts calls armchair attribution, it is noteworthy to mention that there has been tremendous collaboration to understand, respond and recover from this attack. It may or may not be necessary to mention the ruse associated with the US elections – but that has little to do with cybersecurity.




# RECOMMENDATION

That is 2020 in a nutshell! 2021 may not be any different; from the remote-working threats that have trailed us into 2021 because of the pandemic and lockdown; to the phishing, spam and seemingly innocuous emails filled with malicious URLs attachments; the cyber-attacks leading to downtime, data breaches, data exfiltration and ransomware. It would be a great read to say 2021 will be devoid of all of these. Or to do a trend of what to expect in 2021. The truth is that 2021 may not be any different from 2020 from a cybersecurity and threat landscape perspective. Instead, we are recommending learning from the success and failures of 2020 and fixing stuff (people, process and technology) in 2021. Let 2021 be about what we should do and what we should do positively differently.

## People

While multi-factor authentication should be the default for everyone and every organisation right now, there is a need to further take this a notch, not with more technology and shinning boxes or cloud solutions but with security awareness leading to acculturation for employees. Recall the security incident with Twitter Inc. of July 2020? Yes! That was social engineering at play. Internally and within organisations, let the primary focus of simulated phishing assessment gradually shift to behavioural changes, uncovering and rewarding employees who report phishing emails rather than the shaming of those who failed the test. The remarkable outcome of impactful awareness, employee engagement, well-being and satisfaction at the workplace should not be trivialised. Neither should insider threat be underestimated. Have you extended awareness to your partners, vendors, contractors within your supply chain and third-party service providers? Beyond those legal controls such as contracts, confidentiality clauses and NDAs, invest a little in ensuring that at the minimum, you extend periodic security awareness to them – that might be your saving grace or theirs for a Vendor Email Compromise (VEC). Summarily, know your vendors the same way you know your assets, especially from procurement, services, and payments.

## Messaging and collaboration

Email continues to be a primary vector for sophisticated cyber attacks. Attacks are typically delivered by seemingly benign emails which contain a weaponised attachment or a link to a malicious website. As a consequence, a multilayered approach is required to protect an organisation from these malicious emails, attachments, and URLs. In addition to the configuration of DMARC, SPF and DKIM (read a guide here), organisations employ email gateways to help address both inbound and outbound threats. Employees are the last line of defence for all other emails that make it past your technical defences – it is critical to train them to report suspicious emails. Messaging and collaboration solutions such as GSuite and O365 come with some of these controls which may be used in combination with offerings by other email gateway security providers. Features may include email/attachment quarantining, and sandboxing,, protection from malicious URLs, and browser isolation. There might also be a need to plan for email continuity during downtime, especially with the increasing dependence on the cloud services for messaging and collaboration. This could be in the form of a hybrid infrastructure or an email continuity solution.

## Alerts, Log, Monitoring and Detection

The key to an effective response to cyber-attacks is the timely detection of the attack. One of the key features of recent cyber-attacks and data breaches is the mean time between the initial access and the exfiltration process (see MITRE ATT&CK) when most of the organisations detected a compromise of their systems or a foothold within the organisation. The importance of alerts, collecting meaningful logs, real-time analysis and investigation of events and incidents cannot be overstated – that could be the difference between a successful cyber-attack and a security incident. Deploying appropriate tokens/canaries and monitoring mechanisms could be the key to uncovering a breach. It is also essential to monitor the right things so as not to be overwhelmed by logs. We would love to say that every log counts, but that would be at the expense of storage. Know your assets, log what is relevant with alerting, and keep your logs protected. There are tons of intelligent open-source and proprietary solutions that can be used, but know this, a Security Operation Centre (SOC) is not a Security Incident Event Management (SIEM). It is not always about the Benjamins SIEM.

## Alerts, Log, Monitoring and Detection

This is where we recommend everything else that is equally or more important than the items recommended above. From identifying and knowing your assets; to the timely patching of vulnerabilities such as this; to maintaining backups of systems (also as a great defence against ransomware attacks); maintaining basic endpoint security controls (anti-malware, host-based firewalls); to network segmentation and protection; to other security and privacy controls that are often termed the "fundamentals" or the "basics". These fundamentals make all the difference amidst all the sophisticated attacks employing seemingly novel techniques and tactics.

# CONCLUSION

2020 dealt the world blow after blow from a cyber-attack point of view. Impacted organisations that survived were not necessarily those with improved cybersecurity posture, but organisations that have transitioned and incorporated cybersecurity resilience into their operations. This refers to the ability to continuously deliver on their objectives, despite adverse cyber events we witnessed in 2020. Simply put, they prepared for, responded to and recovered from the devastating cyber-attacks. Even though 2021 may not be any different from a threat, tactics and techniques stance, and being resilient, organisations need to prepare for what is to come by learning from the lessons of what is today. This necessitates a shift from cyber resiliency to being ANTIFRAGILE – cyber antifragility.

**PS**: If you are having one heck of a day in 2021, here is a good read of someone's day. We need to be thankful that every day is not like this.

# REFERENCE

All references are embedded as links.

nsflabs

nsfLABs is Nigeria's first private computer emergency response service working with citizens, public entities & private organizations to contain cyber threats and to build a more secure and resilient infrastructure for the Nation.
nsfLABs is a NaijaSecForce initiative.
Wanting to bridge the enormous divide between C-level, mid-level and entry level security professionals in the Nigerian Cybersecurity industry, NaijaSecForce(Nigeria's largest cybersecurity community), was formed. The group has since evolved from networking remotely and in person, to playing capture the flag (CTF) contests, knowledge sharing through the community channels and meet-ups, recommending junior professionals for their next gig and of course, our signature event: the annual NaijaSecCon Conference.

**Contact:** *info@cybersecurity.ng*

Naijasecforce

We understand how daunting it may be to get into the information security field or find a niche for yourself after learning the ropes. NaijaSecForce provides a platform for newbies and experts alike to interact in a mutually respectful space and openly share ideas, research materials and provide technical guidance for ethical hacking, cryptography, cyber risk management, reverse engineering, cloud security and malware analysis.
We meet monthly to discuss and share knowledge, ideas, threats and intels. We also organize a yearly NaijaSecCon Conference. Nigeria Cybersecurity Conference (NaijaSecCon) is Nigeria's first of its kind 100% annual technical Cyber security Conference that uniquely merges information about the latest and relevant threats from a Nigerian context with live technical demonstrations and hands-on workshops.
Annually, NaijaSecCon attracts over 300 cybersecurity professionals from various industries including Financial Services, Insurance firms, Telecommunications, Oil and Gas, conglomerates, Tech Start-ups, Financial Technology (FinTech) companies, other privately-held organizations and also government Ministries, Department and Agencies (MDAs).

**Contact:** *info@naijaseccon.com*

TECH HIVE ADVISORY

TechHive Advisory Limited is a technology advisory firm which provides advisory and support services to private and public organisations with regards to the intersection between technology, business, and law. We focus on how emerging and disruptive technologies are altering and influencing the traditional way of doing things while acting as an innovation partner to our clients. These new technologies often birth new challenges requiring regulations to balance the benefit of innovation and the rights and freedoms of users. Our experience and capability extends across startup advisory, privacy and data protection, data ethics, cybersecurity, intellectual property management and emerging technologies. We ensure our advice serves our clients well by having an excellent understanding not only of their business, but of the markets in which they operate.

**Contact:** contact@techhiveadvisory.org.ng