2021: A YEAR IN CYBERSECURITY, LESSONS AND PLANS FOR 2022

Courtesy of the team at
NaijaSecForce
nsfLABs and
TechHive Advisory

Contributors and Reviewers

Adebayo Tiamiyu

Chidi Obum

Eyitemi Egbejule

Gbolabo Awelewa

Mosimi Odusanya

Nurudeen Odeshina

Oluwole Olakanmi

Peligey Rufus

Ridwan Oloyede

Rotimi Akinyele

Seun Oyelude

Tojola Yusuf

INTRODUCTION

"Out of the depths, I cry to you, Oh Lord!" This is not only our supplication, but it also seems to be the prayer of many cybersecurity professionals throughout a year characterised by cyber attacks, ransomware attacks and data breaches. Oh yes, how can we forget the zero-day vulnerabilities? Just about 11 months ago, a team of cybersecurity and privacy professionals, under the auspices of NaijaSecForce, nsfLABs, TechHIve Advisory and some independent researchers, co-authored and documented a review of "2020: A year in cybersecurity, lessons and plans for 2021". In our exact words (see below), we questioned, "what could be the worst that could happen in 2021?"

"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?".

Well, 2021 literally told us, "hold my beer". In our local parlance, 2021 became a year where lips conjoined in hopes and prayers with the statement, "God no go shame us". Again and again, like playing a deck of Whot!® card game with a maestro, only those born in the 80s and 90s can relate. We, in the cybersecurity community, went from "General Market" to "Pick 2" and "Hold-On",... And, of course, we kept on holding on with heightened apprehension of what could be the worst that could happen. Only to get taken aback with, "here we go again". Apparently, "God no go shame us" also seems to be some organisation's cybersecurity strategy or approach towards what became an eventful 2021.

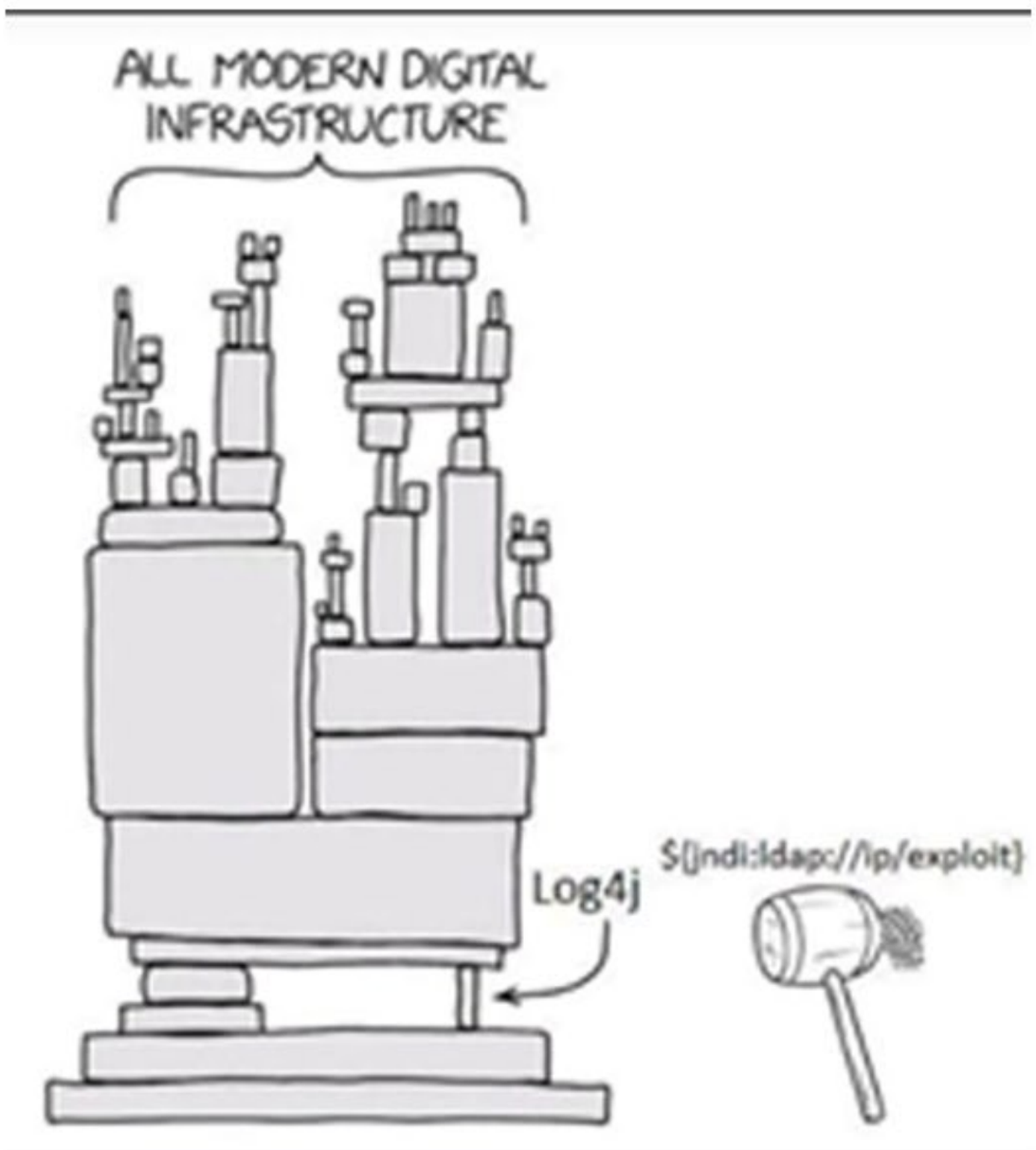
2021 REVIEW: HIGHLIGHTS

Zero-days

2021 seems to have broken the records when it comes to zero-day reports. Zero-day vulnerabilities are software flaws unknown to the vendors or cybersecurity community at large, and until they're identified and fixed, they can be exploited by attackers. There are two key things to note here, there are the zero-day vulnerabilities, and there are the zero-day exploits.

In the first week in December, when we started this article, we had to pause and deal with the log4 vulnerability (CVE-2021-44228) dubbed "Log4jShell". Alas! It was very bold of us to write a wrap-up about the 2021- year in cybersecurity when we still had two weeks till the end of the year. By the time you are reading this in 2022 or some other time in the future, there are chances that cybersecurity professionals and organisations are still dealing with the remediation or patch of this critical vulnerability. Please don't say we did not help; here is some guidance to help deal with this and a list of applications/products affected. The cybersecurity community rallied together to provide support which was quite memorable.

There were tweets, webinars, twitter spaces, organised sharing knowledge, cooperating and collaborating. The team at NaijaSecforce also had a webinar session courtesy of our United Kingdom team, innit? Speaking of the patch, did you know that Apache released a patch for this vulnerability and had to release another patch for the patch itself - crazy! But why is this categorised under zero-day? Well! There are unconfirmed reports that some attackers may have exploited this before Alibaba's cloud security team reported this on November 24. And, if by now you are still wondering what log4j is and why we have dedicated half-a-page to it, the image embedded sums it up.



What is there to write about Microsoft when the global company kept giving us a periodic dose of zero-days. Here is a laundry list of all reports of security vulnerabilities affecting Microsoft products and services. We counted about 25 which were listed as being exploited in 2021 alone. One of those that made the news was: Microsoft MSHTML Remote Code Execution Vulnerability and Windows Print Spooler Remote Code Execution Vulnerability (PrintNightmare). Also notable was HAFNIUM in March 2021, targeting Microsoft Exchange Servers with 0-day exploits. What about this story that made the news too relating to Palo Alto and Randori (a penetration testing company) that discovered a zero-day and literally sat on it without disclosing to either Palo Alto or the public while attempting to justify an "ethical" use of zero-days for security testing. Really!!!

Ransomware

The attack method for ransomware may have advanced, but the ultimate goal for ransomware, "to extort money from victims", still did not change in 2021. Last year, we wrote about the evolution of the traditional ransomware into one dubbed as "blended extortion ransomware". Yeah, the one about weaponising data (exfiltrating data before encryption) while resorting to extorting the targeted organisation with blackmail to release the confidential data publicly. 2021 was also the year of ransom demands, payments and negotiations with ransomware gangs. It seems "we don't negotiate with…" does not apply in 2021. A whopping $11 million in Bitcoin was reported to have been paid by JBS Foods, while Colonial Pipeline paid $4.4 million, which the Department of Justice later recouped. The greatest ransom demand to date seems to be with the computer giant Acer where $50 million was demanded. There is really no need to wonder why ransomware still makes the headlines in 2021 and maybe will make even more in 2022. REvil (Ransomware Evil; also known as Sodinokibi) became a household name- and was one of the most active ransomware gangs, Ransomware-as-a service (RaaS) provider or ransomware variant in 2021, affecting organisations of different sizes and government institutions. Some of the cases of REvil attacks include; Harris Federation (March), Quanta Computer Incorporated (April), JBS S.A. (May), Kaseya (July), among others.

Well, we will not give many audiences to the group than is necessary, you can read more about an interview with one of their representatives here. Alas! There were also crises within the ransomware community, including the hack-back operation by the government agencies and leaks by a disgruntled ransomware affiliate. There is no gainsaying that this may become a full-fledged industry in 2022 - we pray not.

Critical National Infrastructure Attacks

2021 had its fair share of cyberattacks against critical infrastructures affecting the energy, health, I.T., and food sectors. The Canadian Signals Intelligence Agency reported about 235 ransomware cases, and more than half were against critical infrastructure. In Q3 2021 alone, there were 68 cyberattacks against healthcare facilities globally. As you read earlier, Colonial Pipeline (one of the largest U.S. pipeline operators) was one of the targets of this cyberattack (another case of the prevalence of ransomware) that led to the shutdown of the supply of gas within the United States. Colonial Pipeline closed its operations on May 7th after the malicious Darkside group exfiltrated about 100GB of data from the company's network before locking computer systems with ransomware and demanding payments. Colonial's response to the attack includes taking systems offline to contain the attack, which temporarily halted pipeline operations and affected I.T. systems. This attack had numerous effects on the organisation and the lives of everyday people and the economy: Colonial Pipeline took some of its operations offline, leading to a temporary shut down of its pipelines to prevent the spread of ransomware. As a result, the demand for fuel rose because supply was not met due to the shutdown. The fuel shortage affected transportation, including the airlines, as there were disruptions at the airports. Buyers started to buy fuel out of panic leading to long queues at the filling stations. The pump price of fuel rose by 6 cents on each gallon, leading to inflation, and it was also reported that this had a ripple effect on the financial market.

We meat again! In June 2021, they came for our food. JBS Foods, the largest meat supplier globally, was also hit by ransomware. This attack affected its Canadian, U.S., and Australian business operations. REvil was also confirmed responsible for the attack, leading to meat shortage and increased demands. Supermarkets and fast food outlets supply networks were also affected.

Supply Chain Attacks

In one of the most classic cases of supply chain attacks, in July 2021, hackers accessed Kaseya's customers' data and demanded ransom. Kaseya produces software used to manage companies' I.T. networks and devices. The REvil gang launched a zero-day attack on the company's VSA. While the company was trying to fix and patch, REvil hijacked Kaseya's security update and released a fake update to Kaseya's customers, which infected the customers' systems with malware. After that, a ransom demand for $70 million was made. Like Solarigate, around 1,500 businesses in different countries were affected, including the U.K., South Africa, Canada, New Zealand, Kenya, Indonesia, Sweden. These businesses include downstream customers, as was obtainable with the SolarWinds attack. A trusted software update ended up becoming an attack vector which led to, among others, about 800 Sweden COOP grocery stores temporary closure due to their inability to access their cash registers. In total, about 1000 companies' servers and workstations became encrypted. Since most of these customers were themselves Managed Service Providers (MSPs), their customers were also affected by the attack.

Phishing Emails and Scams

According to the Anti Phishing Working Group (APWG) 2021 quarterly reports, phishing emails remain an active threat vector. The number of phishing attacks as of the third quarter of the year has doubled from early 2020, and the volume of attacks in July 2021 was the highest in reporting history. One of the noticeable differences from last year was increased phishing against cryptocurrency targets such as cryptocurrency exchanges and wallet providers. For example, one of those phishing campaigns targeted Coinbase (the world's second-largest cryptocurrency exchange with about 68 million users), for which, about 870 credentials were harvested before the phishing domain was taken offline.

National Security and Attribution

In April 2021, research sponsored by H.P. focused on Nation States, Cyberconflict and the Web of Profit. One of the report's key findings is that nation states are engaging with and profiting from the cybercrime economy, shaping the character of nation-state conflicts. While accurate attribution remains a challenge, nation states deny accusations of sophisticated attacks whose magnitude can only be attributed to espionage or cyber warfare. There are also indications of 'stock-piling' of zero-day vulnerabilities through covert channels such as 'atypical' buyers acting on behalf of nation-state actors. While on the topic of zero-days and nation-states, we are wondering, just as you are, why Alibaba is (as at when we wrote this) being reprimanded for not reporting the log4j zero-day to the government first. 2022 may surely be an interesting year concerning national security and attribution. In anticipation of what is to come, please grab tea or coffee to sip while reading Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Until then, it seems like we have been talking too much about this, so fem!

Cryptocurrency, Crypto-exchange attacks and NFTs

In what was reported as the largest crypto hack in history, about $600 million worth of crypto tokens was stolen (and returned?) in an attack targeted at the cross-chain Decentralised Finance (DeFi) platform - Poly Network. How did this happen? Mismanagement of the access rights between two important smart contracts makes it possible for the undisclosed attacker to transfer tokens and move them to external wallet addresses. Have you heard of "rug pulls"? Well, thanks again to crypto! Rug pulls are a relatively new scam type particularly common in the DeFi ecosystem, in which the developers of a cryptocurrency project — typically a new token — abandon it unexpectedly, taking users' funds with them. There you go! Rug pulls accounted for about 40% of all cryptocurrency scams in 2021. Some of them even used some of the world trends and well-known personalities, influencers and celebrities to pull off these schemes, such as the Squid Game tokens. There is also the ruse about Non Fungible Tokens (NFTs) which we are not sure what to make of - see a quick FAQ about NFTS.

Recommendation

Well! That is it! 2021 in a nutshell! Just another year in cybersecurity. As stated last year in our report, we do not know what is to come. 2021 has proved to be significantly different from 2020 in terms of not necessarily the techniques and tactics, but rather, the scale and sophistication of cyberattacks, exfiltration and data breaches, and the targeted industries - we did see a lot of cryptocurrency-targeted attacks. Even though 2022 may not be different from 2021 (we know we said this last year, too), our recommendation is still learning from the success and failures of 2021. What can and should we do better as a community?

People

We saw collaboration and cooperation a lot towards the end of 2021. The whole world needs love, more especially the cybersecurity community. Irrespective of the area of focus, we need each other to deal with the menace and onslaught of the threats unleashed on a daily, weekly and monthly basis. An African proverb quipped about one of the best ways to eat an elephant is not only by devouring it piece after piece but by soliciting the community to join in. There is a need for security practitioners to engage more and support open-source projects. There is much improvement required within that space. Also, let us not beat each other down; organisations and their people dealing with cyberattacks have a lot to deal with (if you have been there, you will know); it is important to be mindful at the very least and be supportive. We are not sure about you, but Twitter became an active medium for cybersecurity threat intelligence, information broadcast, dissemination and a collaboration platform (Spaces). Do review those you are following to benefit from this. Lastly, do not forget to grab a cuppa TEA (Security Training, Education and Awareness) for all your stakeholders (internal and external).

Third-Party Risks

There is a need to transition how organisations deal with 3rd-party service providers or external service providers, especially the critical ones. The Zero-trust concept should extend beyond technology and architecture into ways of thinking about risks associated with 3rd-party dependencies across people, applications, infrastructure and services. Assume compromise (whether it is in the case of acquisition of proprietary applications, patch or a software update, use of outsourced personnel including contractors and consultants, among others.), assess what will impact your organisations (perform risk assessment) and determine what you can do to mitigate that risk. In summary, we envisage that this will be a primary determinant in the organisation's engagements with vendors for business deals and mergers and acquisitions.

Processes and Technology

You probably have read that security is not a technology problem. Today, some of the failure to address security problems is not a result of technological limitations but rather organisational issues. Nonetheless, we had a bunch of recommendations relating to Messaging and Collaboration (because email is still an active threat vector) and Alerts, Logs, Monitoring and Detection from last year's report. Please look here, as they are still relevant to what we should be doing in 2022. It is also time to re-think organisational strategies (especially resilience) towards severe cybersecurity incidents such as ransomware and other cybercrimes - think of operational playbooks, technology architecture, especially for organisations that have adopted a cloud-delivery approach. We will also not bury our heads in the sand concerning security and privacy compliance (data protection and privacy regulations). Organisations can use them effectively to improve processes to help address some of the security and privacy risks.

Cyber Hygiene

This is where we recommend everything else that is equally or more important than the items recommended above; patch early and as often as is feasible, isolate critical and sensitive systems and data, filter emails, keep on maintaining backups of systems (not entirely a great defence against ransomware attacks we described above but will still do); maintain basic endpoint security controls (anti-malware, host-based firewalls), enable detection and notification for maintained logs and review, among other measures. Finally, lest we forget, multi-factor authentication should now be a standard. These fundamentals make all the difference amidst sophisticated attacks that employ seemingly novel techniques and tactics.

Conclusion

2021 dealt the world blow after blow from a cybersecurity threat point of view. What is that saying about 'do not beat a dead horse'? Well, the cybersecurity community and most professionals kept on being rammed up to the very end of 2021. Even as we complete this on the very last day of the year, we are not sure what will happen in the last few hours or what we will wake up to tomorrow and in 2022 in general - only God knows, and that is how the story goes.

Going by the significant difference between 2020 and 2021, we all need to recover from the devastating cyber-attacks of 2021 and then prepare for and plan to respond to whatever 2022 has in store - we hope it is going to be a much milder year. But hopes, wishes and dreams are not enough in response to the ever-evolving and sophisticated cybersecurity threats, tactics and techniques. Organisations need to prepare for what is to come by learning from the lessons of what is today.

P.S.: If you have 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