Netacea's 2022 Cyber Predictions

NETACEA

Each year Netacea's Threat Research team forecasts the top cyber-trends for the following 12 months. We've predicted trends across the cybersecurity landscape and geopolitical technology to help your business stay one step ahead of cyber-attackers in 2022.

Four Cybersecurity Predictions

1 Attackers will continue to take advantage of supply chains and third parties

2021 has seen several supply-chain attacks – where an attack was launched against an organization and then cascaded to other organizations with whom the original target had a relationship. We expect this trend to continue as companies diversify their supply chains to increase resiliency in the face of unpredictable global events. Attackers are keen to use this method as by compromising one supplier with relatively weak security they can then amplify this attack into breaches of multiple related organizations, some of which may have much stronger security models.

2 Ransomware attacks to grow in volume

Ransomware will continue to be a popular choice of attack and is expected to grow in both sophistication and number. The financial returns are significant, with the average cost of these sorts of attacks rising significantly in 2020-21. Similarly, attackers are developing the so-called 'ransomware marketplace' where specializations are developing, such as brokers selling access to compromised networks and offering Ransomware as a Service (RAAS). The financial severity of ransomware attacks is being recognized by companies offering cyber-insurance, with increasing premiums and decreasing coverage to offset their own losses.

3 Cell phones create new opportunities for attackers

Cell phones are an ever-ubiquitous part of the information technology landscape. However, the increase in applications and developments in hardware creates new opportunities for attackers. From a physical tech perspective, the rollout of 5G and increase in the power and capabilities of such phones will allow for new and faster avenues for attacks against mobile devices, whilst increasing the value to attackers when they are compromised. Similarly, the myriad of applications people install creates new opportunities for security breaches by convincing users to download malicious apps or through apps that are not properly secure. As cell phones become increasingly important in day-to-day life, used for everything from banking to shopping, attackers are incentivized to compromise them. With their increased capabilities, compromising mobile devices means attackers can now more easily use them as a launchpad or botnet for future attacks. All being said, we predict attackers will generally focus on application programming interfaces (APIs) over the next year.

4 APIs increasingly become attack vector

Many businesses are setting out on a path of API discovery and implementing protection to secure their APIs. This is in response to an increasing number of traditional cyber-attacks (for example, the growing amount of malware that now targets cloud API services) as well as business logic attacks that seek to profit from insecure devices. We expect this trend will continue, with attackers exploiting the little understood and often insecure APIs.

Four Bot-Related Predictions

1 Scalper bots lower barrier to entry

We've seen the number and sophistication of scalper bot attacks rise in 2021. The scalper bot ecosystem is developing rapidly and becoming professionalized, with more advanced groups registering themselves as formal companies. We've observed 'bot' training and tutorials being offered to people, as well as scalping tools being designed with ease of use in mind. As such, the barrier to entry is lower, and as more people start using scalper bots, we're observing a greater investment of time and skill into bot tooling and techniques. The more unskilled people use bots and become familiar with them, the more they'll realize and understand the gains, further compounding the issue.

2 Bots set their sights on new targets

As bots become an increasingly popular attack vector, they'll start exploiting business logic vulnerabilities in other industry verticals that haven't seen extensive bot attacks in the past. For instance, we've found more bot developers offering their skills to those who want to profit from NFTs (non-fungible tokens). Sniper bots, such as those stalking eBay, are being developed and employed to rapidly purchase and resell NFTs. We expect to see bot attackers diversifying their attack vectors over the coming year in order to maximize their profits.

3 Residential proxy networks will be utilized more

Companies are increasingly trying to prevent business logic attacks that bots can exploit, and one of the most common ways of trying to control the attacks is to simply block the IP (internet protocol) addresses where the attacks originate. As awareness of business logic attacks and bots increases, we've seen more organizations take this step. Attackers have responded to this by using lots of proxies, sometimes as many as one per HTTP request, to try to bypass such restrictions.

Companies are growing wise to this and are trying to block legitimate proxy services they know in order to limit these attacks. In response to this, adversaries have, and will continue to, make use of residential proxies. These are proxy networks where a bot attacker routes their traffic through home computers and mobile devices to make the traffic look legitimate. Sometimes this is with the knowledge and permission of the device owners and other times, it isn't. Often, companies are reluctant to block large swathes of IPs associated with private residences for fear of blocking legitimate customers, and so have little answer to this type of attack.

4 Increasing professionalization of bot attackers

Across 2021, we've observed a huge influx of talent and resourcing into the bot developer and user ecosystem. Inspired by lockdown but also by the increased awareness of the low risk and high profits of bot attacks, many more people have started using bots for their own gain. This has driven many bot groups to professionalize, with many now actively recruiting employees who fulfill roles in marketing, recruitment, support, development and more.

In some cases, where the activities are legal, these bot groups have even registered themselves with governments as formal companies and pay employees to work full time. Across all types of bot attacks, we've identified segmentation of specialisms, with people choosing to specialize and fill a particular niche within the larger ecosystem, such as developing bot tools, selling supplementary services (such as information or infrastructure needed to run attacks), acting as trainers, hosting communication/ networking services, or working with developers as a consultant.

We've started to see bots being offered as a Software as a Service (SaaS) model as well. We think professionalization of bot attackers will continue into 2022 as more people become involved.

Three Geopolitical Predictions

1 Information warfare, Rhet-ops and involvement in elections

Governments have realized they can harness social media to influence democracy for their own advantage, whether by interfering with rival states through 'Rhet-ops' or manipulating public opinion within their own territories. Bots are a valuable tool in information warfare, with advanced bots able to track, repost, comment on, and even generate credible, human-sounding posts on social media spreading propaganda. These methods will only become more sophisticated and more widely used by all governments in pursuit of their geo-strategic aims.

Similarly, states will explore and possibly utilize other forms of technology (such as deep fakes) for information warfare purposes. This allows them to pursue international policy goals in a state of grey warfare (where there is no escalation to actual armed conflict, and where identification of an attacker is almost impossible).

2 Cryptocurrency will be a focal point for cyber-attacks globally

Cryptocurrency exchanges and wallets often contain significant assets that can be a great lure to attackers looking to profit from their attacks. Over the latter half of 2021, there has been an uptick in attacks related to cryptocurrencies. Sometimes these are simple social engineering attacks; other times they are much more technically advanced.

With the amount of money that can be stolen in a single successful attack – potentially running into millions of dollars – we expect to see more attacks on decentralized currencies. However, we reckon law enforcement will come down hard on cryptocurrency attacks and exploiting cryptocurrency weaknesses in order to investigate and interfere with crime. Governments might crack down on cryptocurrencies or seek to regulate them more severely in response to this trend.

3 Greater government involvement in cybersecurity

During the height of the COVID-19 pandemic, there were significant worries there may be attacks on vital healthcare infrastructure, vaccine rollouts and more. Some of these worries did manifest, with, for example, the Irish Health Service suffering a crippling ransomware attack. Besides healthcare targets, attacks on oil pipelines in the US, powerplants across the world, and many more instances triggered concerns for critical national infrastructure. This has encouraged many governments (including the USA and UK) to consider how private enterprises can help national security, how vulnerable they are to attack, and what impact this has on the public.

We think governments will become more hands on in terms of regulating security at private enterprises and helping these organizations respond to attacks. We also expect to see more international collaboration and competition in policing cyber-space. Due to the global nature of the internet, attacks often cross international jurisdictions making prosecution difficult. We expect to see more efforts by governments to establish international standards and facilitate working with one another to help investigate and prosecute digital crimes. However, we think this will lead to competition between rival states, with each trying to exert their own idea of what a common global cyber-policing effort should look like. The USA and China are likely to be the two big players in this area, with each trying to convince other states to subscribe to their own versions of a common international digital model.

Stay one step ahead of bots with Netacea

Choosing the right bot management solution is a major decision for any business. Understanding the bot landscape and the threats posed to your business is the first step in staying one step ahead of malicious actors. At Netacea we take a consultative approach, working closely with you to understand not only the threats bots pose to your business, but how our solution fits into your wider strategy and organisation.

This partnership, paired with our server-side approach and innovative Intent Analytics® technology, allows us to seamlessly integrate with your business and deliver accurate, intelligent and effective mitigation against scalper bots and beyond.

To learn more about our 2022 cyber-predictions, talk to the Netacea Threat Research team today at hello@netacea.com.

Or to book a free demo of Netacea Bot Management, visit www.netacea.com/lp/bot-protection/