Cybereason 2022 trends and predictions

By Lior Div, issued by Cybereason

29 Nov 2021

The changing of the leaves and the brisk fall mornings around Boston are a sign that 2021 is nearing its end. It's a time that I like to reflect on the year gone by and think about the potential for the new year. In the world of cybersecurity in particular, the end of the year brings an avalanche of predictions for what the threat landscape will look like in the year ahead. It's a fun end-of-year tradition, but it can also provide valuable insight into coming trends to help defenders be prepared for what's on the horizon.

'Predictions'

As I review predictions from previous years and look at some of the 2022 predictions that are already hitting the internet, I have noticed that a lot of them are not really predictions – they are just a list of buzzwords or topics that are already gaining momentum that someone has put together to 'predict' that those things will still be relevant next year. Things like AI/ML, cloud computing, the cybersecurity skills gap, and ransomware are not really predictions but instead blatantly obvious. Of course, those things will continue to get attention, but it doesn't take a security expert or any special insight to "predict" that.

Beyond the buzzwords

To borrow a poker metaphor, those topics are table stakes. Looking ahead to what Cybereason and our customers need to be aware of for 2022, it's important to keep those things in mind, but let us consider the broader threat landscape – and what we are seeing in terms of emerging attacks and current threat research – to identify key risks that defenders need to prepare for.

2022 cybersecurity predictions

With that in mind, here are the risks that stand out as unique above and beyond the buzzwords:

RansomOps – The new kill chain

Ransomware as a threat is already established and well known. Ransomware attacks occur on a daily basis and 2021 has seen multiple ransomware events that have had a significant impact. The risk that doesn't get enough attention and that defenders need to understand is that ransomware has evolved.

It started out as a variant of traditional malware – just a different way for threat actors to make a profit when compromising a target. What we see today is not that simple. We now have ransomware cartels – like REvil, Conti, DarkSide, and others – and ransomware is not a piece of malware, but rather comprehensive ransomware operations, or RansomOps, where the execution of the ransomware itself is just the final piece of a much longer attack chain.

There is too much focus on the ransomware executable, or how to recover once an organisation's servers and data are already encrypted. That's like fighting terrorism by focusing only on the explosive device or waiting to hear the 'boom' to know where to focus resources.

RansomOps take a low and slow approach – infiltrating the network and spending time moving laterally and conducting reconnaissance to identify and exfiltrate valuable data. Threat actors might be in the network for days, or even weeks. It's important to understand how RansomOps work and be able to recognise Indicators of Behaviour (IOBs) that enable you to detect and stop the threat actor before the point of 'detonation' when the data is actually encrypted, and a ransom demand

is made.

Supply chain – Amplifying reach of attacks
This also doesn't feel like much of a 'prediction' at face value. IT professionals are very familiar with the concept of a supply chain attack thanks to the SolarWinds attacks. You need to have a broader perspective on the concept of supply chain, though. It is not always a function of compromising a device or application that is then distributed to others down the chain.

It would be more accurate to call it 'low hanging fruit'. SolarWinds is one example of a threat actor finding a way to compromise one company and leveraging that attack to allow them to compromise the customers of the initial target. Our research into DeadRinger and GhostShell illustrates examples of a different approach with a similar outcome. Threat actors gained access to telecommunications providers, which then enabled them to access and monitor communications for customers of those providers.

In both cases, the concept is the same. There is a growing trend of threat actors realising the value of targeting a supplier or provider up the chain in order to compromise exponentially more targets downstream. Rather than attacking 100 or 1,000 separate organisations, they can successfully exploit one company that unlocks the door to all the rest. It is the path of least resistance.

The attacks we have seen have been part of cyber espionage campaigns from nation-state adversaries. Those attacks will likely continue, and we will see a rise in cybercriminals adopting the strategy as well. Companies that act as suppliers or providers need to be more vigilant, and all organisations need to be aware of the potential risk posed from the companies they trust.

Microsoft – Living with the Microsoft risk
The simple truth is that one way or another, Microsoft products are directly involved in the vast majority of cyber attacks. Threat actors invest their time and effort identifying vulnerabilities and developing exploits for the platforms and applications their potential victims are using. Microsoft has a dominant role across operating systems, cloud platforms, and applications that make it fairly ubiquitous.

By developing software riddled with vulnerabilities and not always accepting responsibility or acting to address issues, Microsoft bears some responsibility. However, it is not always a matter of exploiting vulnerabilities. Google analysed 80 million ransomware samples and determined that 95% were Windows-based executables or DLLs. Only about 5% of the samples actually used exploits – but most of those targeted Windows as well.

Adding insult to injury, Microsoft continues to coerce customers into using its own inferior cybersecurity offerings through its predatory E5 licensing model. They are selling customers products and services that make them vulnerable, and then demanding more money to provide inadequate protection to try and defend those products and services.

Microsoft will continue to be the primary focus for cyber attacks in 2022. That isn't really a revelation. Defenders need to understand the risk of relying on Microsoft to protect them when they can't even protect themselves. Organisations that depend on Microsoft for security will find themselves making headlines for the wrong reasons.

I'm not suggesting that organisations not use Microsoft products or services, but it is important to understand the risks and have a layered approach to defending those products and services against attacks.

Cybersecurity is national security
The line no longer exists between national security and cybersecurity. Sometimes a nation-state adversary attacks a private company as part of a broader campaign. Russia did it with SolarWinds. China did it with Hafnium. Iran did it with GhostShell. Sometimes, cybercriminals launch attacks with national security implications. The flow of oil and the food supply chain were both seriously disrupted in 2021 by ransomware attacks.

What we need to be aware of as we go into 2022 is the increasing cooperation and collaboration between these threat

actors. Nation-state adversaries are not directly controlling many of these operations, but a combination of state-sanctioned, state-condoned, and state-ignored attacks create an environment where failure to act is equivalent to tacit approval and indicates that even if they are not actively working together, their objectives are often aligned.

The US government has made progress and will continue to work to improve the cyber defences of federal agencies. They will also coordinate efforts with private sector tech and cybersecurity companies, as well as nation-state allies around the world to address the Cyber Cold War, protect effectively against threats, and work together to bring threat actors to justice.

XDR – Improving protection with AI

With the shift to work-from-home or hybrid work models, the rollout of 5G wireless, and the explosion of IoT (internet-of-things) devices, virtually everything is connected today. This connectivity provides a variety of benefits in terms of productivity and convenience, but it also exposes organisations to significant risk which makes Extended Detection and Response (XDR) crucial.

The question is, “What is XDR?” Many vendors have an offering they are calling XDR, but not all XDR is created equally. There is almost universal agreement that XDR is the next thing, but the definition of what XDR is and the best way to achieve it is still being debated.

The industry will reach some consensus in 2022 and leaders will emerge as the dust settles some in the XDR market. Regardless of how we define XDR, the scope and volume of threats demands that artificial intelligence (AI) play a central role in making it effective.

Get ready for 2022

As you take time to gather with family and friends for the holidays, or just disconnect from work and recharge, hopefully these insights will help you prepare more effectively for the cybersecurity challenges you will face in 2022. The threat landscape is constantly shifting, but understanding how threat actors think and having insight into emerging trends enables you to stay ahead of the curve and defend more effectively.

ABOUT THE AUTHOR

Lior Div is the CEO and co-founder of Cybereason.

- **FBI warns US companies to avoid malicious USB devices** 18 Jan 2022
- **Cybereason 2022 trends and predictions** 29 Nov 2021
- **Cybereason Exposes Chinese Threat Actors Compromising Telecommunications Providers for Cyber Espionage** 3 Aug 2021
- **Cybereason acquires empow to enhance XDR offerings** 20 Jul 2021
- **Cybereason Secures $275 Million in Crossover Financing to Extend Global Leadership in XDR** 14 Jul 2021