SentinelOne's Cybersecurity Predictions 2023 | What's Next?

December 14, 2022
by SentinelOne

2022 was a sobering year for us all. Riding on the back of the COVID pandemic of the previous two years, we entered a new reality with war returning to Europe in a way not seen since 1945. And yet along with tanks, missiles, and the targeting of civilians and civilian infrastructure came a new battlefront: cyber warfare with wipers being used to hit targets inside and outside the physical battleground.

Meanwhile, new attack surfaces came to the fore, as cybercriminals began to understand how to exploit identity for access and cloud workloads for assets, privilege escalation and lateral movement.

It's not been all bad. Evolving security technologies like XDR are helping organizations to fill the gaps in visibility, join the dots in defense, and hunt for hidden threats in the enterprise. Law enforcement at home and abroad has been capturing and incarcerating more cybercriminals than ever before, while also closing the doors on some of the darknet's worst illicit markets.

But defenders are still playing catch up, a point not lost on our experts who, below, offer their predictions for what we can expect in cybersecurity 2023. Our predictions last year weren't far off the mark, so as we look forward to another year in the trenches of cybersecurity, here's what our researchers and thought leaders see in their crystal balls.

Driving Painful Lessons Home

2022 has been a year of painful lessons precisely because the most intense threats weren't technically advanced or mind-bending feats of cyber wizardry. Instead, they were mundane, pragmatic, and wildly successful. This year was largely populated by asymmetrical threat actors– hacktivists of all stripes, youthful petty criminals, and an increasingly fragmented ransomware ecosystem.

Infosec dark humor held that ransomware groups were 'technical debt collectors'– attaching an eye watering price tag to unpatched systems, misconfigurations, and generally underserved networks. It seems that we collectively underestimated the true depth and breadth of that technical debt as a wider swath of lower tier threat actors show us the results of living on a diet of fruit so low-hanging as to have rotten on the pavement.

Cells of youthful SIM swappers and source code hoarders, best referred to as 'disorganized crime', have successfully hacked their way across scores of noteworthy well-resourced companies. They've embraced a pragmatic approach to operations– abusing the nebulous web of dubious 'trusted' parties that serve the customer-facing requirements of larger corporations. Whether through social engineering, stolen and borrowed credentials, or the financially-motivated shortrun insider, attackers have enjoyed all that excessive privileges across unsegmented service VPNs can net them.

The cumulative effect? A near endemic failure of SMS 2FA as a security measure. As we enter 2023, we need to accept that hardware multi-factor authentication, short lived sessions, and severely curtailed account privileges aren't nice-to-have paranoid bells and whistles. They are now the entry threshold of the aspirational standard of corporate security.

The ransomware ecosystem continues to shift, experiment, and fracture. The most notable incident is the 'Conti Rica' affair, where a ransomware group held an entire government for ransom. In 2023, our tracking will have to become more granular– moving away from the notion of monolithic ransomware cartels to acknowledge the prevalence of smaller affiliate groups (often engaged with multiple RaaS brands).

Perhaps at that level of observability, we'll be quicker to note attempts to use ransomware as a flimsy cover for nation-state activity– as in the case of Iran 'ransoming' Albanian governmental institutions. This last facet jives with the abuse of an increasingly populated field of hacktivists (of varying degrees of authenticity) emerging to represent different sides of hot conflicts and societal tensions via overrated DDoSes and underrated hack-and-leak ops whose long-term effects are entirely unforeseeable.

The cybersecurity industry enjoys cutting its teeth on advanced threats and sophisticated techniques that challenge the collective braintrust to find new solutions. But 2022 has forced us to pay attention to the state of disrepair of our networked fabric. Without a sizable, conscientious collective effort, we should brace ourselves for a 2023 that drives those painful lessons well beyond our tolerance.
Juan Andres Guerrero-Saade, Sr. Director of SentinelLabs

Cybersecurity Only Works When "It Just Works"

2022 has been a year where, compared to previous years, the cybersecurity market has adapted not just to the threat landscape but perhaps more strongly to how security teams want to use cyber-security products. This is something I expect to see much more of in 2023.

Consolidation, But Not At All Costs

The sheer number of cyber-security products covering different surfaces and use cases means that customers are looking to consolidate when and where possible. With that said, there are many sides to consolidation – security teams will not satisfied with just "buying more products from the same vendor vs multiple vendors" or "pushing everything to one data-lake" – they will demand holistic workflows, unified agents and cross-product synergies that actually deliver value that is greater than the sum of its parts when consolidating around a platform as opposed to endless point solutions.

Demand for More Vendor Collaboration

As much as we expect consolidation, customers will always end up using more than one vendor. We're already seeing security teams demand more integration and more value from the collaborations between vendors. Gone are the days when a "technological alliance" could mean little more than a shared video. In 2023 this will range from a demand for integration across more types of use-cases and standardization of data models to a very legitimate expectation that every new vendor will not only provide value on its own but also help extract more value from the existing products in the security stack

Data Retention Needs to Be Simpler, More Affordable

Despite sounding like an oxymoron – it actually makes a lot of sense. There's no argument about the importance of data. Between compliance regulations, low-and-slow attacks and the overall increase in analyst skill-level – most customers can and need to do more with security data.

The historical price and complexity of facilitating that is where change is going to come. SOCs will start looking for alternative solutions for Analytics and Data Storage that make more sense in terms of cost, scale, performance and ease-of-use. They'll be looking for improvements across the board – from "How we get the data in" to "How we can access historical data", "How fragmented the data will be" and ultimately "How much does it cost".
Yonni Shelmerdine, VP Products, SentinelOne

No One Gets to Opt Out of Cybersecurity in 2023

If there is one thing that we learned from 2022, it is that no one is immune from cyber threats. We've seen many breaches in 2022 – Lapsus$ alone breached Okta, Nvidia, Samsung, Ubisoft, T-Mobile, Microsoft, and Uber. It's hard to believe that behind these breaches, there were no well-sponsored nation-states or global cybercrime syndicates but (allegedly) a group of young hackers who met online and collaborated, not even financially motivated.

This creates a new paradigm to think about. I am not a fan of zero trust, as it is tough for organizations to implement and leaves cracks for adversaries to exploit, but trusting no one makes more sense when you look at 2022. So what should we expect in 2023? There are a few moving parts to consider.

Cost Will Be a Driving Force

The economic turmoil will pressure enterprises and organizations to save on costs and be more effective. As a result, expect more consolidation of pinpoint tools and teams and more utilization of growth and efficacy enablers like moving to the cloud.

Prediction: With less security budget, efficiency-driven products will strive. The cost will become the main consideration for cybersecurity programs.

Attacks Will Be Bigger, Louder, Faster

The attacks we've seen in 2022 are more significant than those we witnessed in 2021. This is not just a trend; the reasons remain: Vulnerable products (led by Microsoft as an operating system provider and a security vendor), the means of communication, and the speed it takes a zero-day to become an exploit.

Prediction: More organizations will be breached, more critical infrastructure will be impacted, and the cybercrime economy will continue to thrive.

We Are Entering A Golden Era of Social Engineering

As we've seen in the Cisco breach, it's enough to compromise a user to gain access to the entire network. With social networks, multi-tasking, and the evolution of devices around us, it just makes sense for adversaries to keep investing in social engineering.

Prediction: Phishing is a problem that is not solved and will continue to be a leading factor in compromising identities.
Migo Kedem, VP Growth, SentinelOne

The Disruptors Are Here, And They Aren't Going Away

2022 has been the year of disruption by non-traditional threat actors. Flaws in how teenagers exploited the way the traditional cybersecurity establishment thinks. Advances in computing power and AI will transform the effectiveness of social engineering, fraud, and active measures (information/influence operations). As governments try to get a handle on asymmetric threats, new ways of attacking the global problem will have to be used.

Deep Fakes Will Enhance Social Engineering

As we get better at defending the endpoints, threat actors will need to up their game in order to penetrate harder targets. Social engineering remains a popular vector of attack, especially as workforces continue to remain decentralized and remote. Increases in computing power and availability of AI/ML engines will accelerate the effectiveness and authenticity of social engineering attacks through audio and video.

Increased Targeting of Vaccine R&D by China

The unthinkable has happened in China–widespread dissent that is becoming more vocal and violent. Aggressive lockdowns have not made the expected impact in the spread of COVID, and the Chinese vaccines are significantly less effective than international options. For President XI Jinping, an attractive option is to enhance the efficacy of their vaccines through more aggressive theft of R&D and medical intellectual property.

Lapsu$ Shows Flaws in Adult Thinking

Migo Kedem laid out the impact of Lapsu$ and the disruption they caused. This was a group of 16-21 year olds who out thought and outwitted some of the most sophisticated cybersecurity defenses and professionals in the world. How? Because it doesn't matter how we look at the problem. It only matters how our adversaries look at the problem. Expect more attacks and disruption by younger threat actors who refuse to limit their thinking to the proverbial way of doing business.

Retasking of Intelligence Priorities

According to testimony before Congress during hearings on the SolarWinds compromise, it was estimated at last one thousand engineers and intelligence officers were involved in the design and execution of the operation. And yet there is no evidence any intelligence agency outside of Russia was able to discover this long-term campaign.

This is a glaring failure of intelligence that has become increasingly technically focused. To stop major intelligence operations, we have to develop robust HUMINT – human intelligence. And that can only come from more aggressive recruitment of agents in targeted sections of adversarial intelligence organizations. There will be retasking of intelligence priorities to identify earlier, and disrupt more aggressively, long-term operations against nations and critical infrastructure.
Morgan Wright, Chief Security Advisor, SentinelOne

No More Hiding Behind Our Macs

Indicators of what we might expect in 2023 can be read in the tea leaves of our roundup of macOS threats in 2022. The year just ending saw something rare in the macOS threat landscape become common: the inclusion of Mac payloads appearing in numerous cross-platform attack frameworks. While this wasn't entirely unheard of in the past, it was not the norm, and Mac payloads were generally poorly written, unreliable and, frankly, unsuccessful.

What's changed is the increasing popularity of two things: performative and stable cross-platform languages like Go, Kotlin and Rust, and Mac devices in the enterprise. The first makes it easier for threat actors to write Mac-compatible malware, the second gives them the motivation to get better at it.

Another trend that gathered pace in 2022 was the number of reported CVEs for macOS devices, many of which allow privilege escalation and some the ability to execute kernel code from user land processes. While a transparent bug reporting ecosystem is a good thing and long overdue regarding Apple operating systems, it has consequences for those that patch little, and patch late.

Threat actors, with or without the help of security researcher write-ups and PoCs, will increasingly pay attention to exploiting reported bugs (aka N-days) on enterprise users that fail to patch. It's not for nothing that Apple has become more aggressive in trying to force enterprises to update within 90 days.

In 2023, expect to see threat actors target macOS more successfully with cross-platform malware and to expend more effort on finding windows of opportunity to compromise unpatched Macs with known bugs. More supply chain attacks on developers and shared repositories are also likely to feature in 2023.

Deploying a native Mac security solution is the default first step to combating the increased attention of threat actors on high-interest targets like developers and senior management in 2023. Enterprises that defer upgrades and minor updates need to pay particular attention to risk assessment and their overall macOS security posture.
Phil Stokes, macOS Threat Researcher, SentinelLabs

Conclusion

Threat actors have become *collaborative* enough and malicious software and techniques *available* enough to brings us to a point where attackers are now platform and technology agnostic. Where there is a weakness, there is a way.

And yet, while 2023 will undoubtedly hold surprises none of us could predict, it's a fair bet that organizations that cover their bases, kill off the low-hanging fruit, and implement coverage across cloud, identity and endpoint will be safer than those that do not. The future is opaque to us all, but in cybersecurity we can't afford to trust to luck.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- SentinelOne is VB100 Certified | Maximizing Protection Against the Evolving Threat Landscape
- Apple's macOS Ventura | 7 New Security Changes to Be Aware Of
- Cybersecurity's Biggest Mistakes of 2022
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- Decoding the 4th Round of MITRE ATT&CK® Framework (Engenuity): Wizard Spider and Sandworm Enterprise Evaluations
- Bringing Identity to the Era of XDR