Bullish

NEWS RELEASE

2023 Security Predictions

2023-01-25

By Kevin Fealey, Chief Security Officer

2023 will be a make-or-break year for crypto companies. Businesses that prove to their customers that they take security seriously and can operate effectively with additional oversight will thrive. Companies who haven't learned from the mistakes of 2022 will see their customers disappear. Here are my key security predictions for what to expect in 2023:

Skynet is coming

While we are likely decades away from giving control of critical infrastructure over to the machines, the practical applications for artificial intelligence (AI) are becoming real as the technology and training data sets improve. ChatGPT is already being used to create polymorphic malware, and throughout the next year, attackers will find new ways to use free and easy-to-use AI to create new security problems.

The most immediate risks from ChatGPT are social engineering and phishing. ChatGPT can be used by anyone in the world, regardless of technical skill, to create well-written, concise, and compelling scripts that entice victims to click on links, download malware (which is also created by ChatGPT), and grant unauthorized access. Expect phishing and social engineering to become even more prevalent and harder to detect over the next year.

Supply chain attacks abound

Supply chain attacks have become rampant in recent years, and that will not be changing any time soon. Most companies use thousands of third party products, from open source libraries and frameworks to SaaS platforms and smart video conferencing in their offices. Every one of these products has a risk of vulnerability and could

provide an attacker an entry point to an enterprise network or worse. Few practical frameworks exist for managing this risk, and the scale of the problem continues to grow with every procurement request.

In 2023, we will continue to see critical vulnerabilities in platforms that store or manage our data and in components deployed like scatter-shot across enterprise networks. Companies will continue to struggle to identify when they are impacted, and they will take months to fully remediate when they are.

Cryptocurrency's role in cybercrime

Crypto's ease of use makes it a preferred method for ransomware payments, and the reduced value of cryptocurrencies is unlikely to change the demand for cryptocurrency as part of ransomware schemes or other forms of fraud. Ransomware groups have invested in building tools and infrastructure to support cryptocurrency as a form of payment, and now they are well-positioned to continue to generate returns on that investment. While paying a ransom is typically not advisable, it's worthwhile for enterprises to be knowledgeable about how cryptocurrency works and to prepare for the worst case by building a relationship with a reputable cryptocurrency exchange or OTC broker. Expect cryptocurrency to continue to be discussed in relation to company business continuity and resilience in 2023.

Similarly, the costs associated with scams like "**Double-Your-Crypto**" are so low, they will always be economical for criminals. When you're tempted to generate returns that are "too good to be true" in 2023, resist the urge.

Strengthening the foundation of crypto

Institutional customers in the cryptocurrency space—who make up the majority of trading volume, especially in the 2022 bear market—have been burned one too many times from failures in their trust models. These organizations will revert to traditional due diligence experience and require things like third party independent audits and code reviews of platforms they want to leverage. This will lead to increased demand for smart contract auditors and educational content for secure smart contract developers. Ultimately benefiting the crypto security industry, this talent will help repair trust models and build a stronger, more secure foundation for the next bull market.

Crypto companies, DeFi platforms, and blockchain protocols will be forced to go "back to basics" and focus on improving hygiene, rather than expanding features, to retain customers and incentivize former customers to rejoin their platforms. This could be an opportunity for security engineers, researchers, and auditors looking to get into the blockchain space. We'll likely see new internal security roles created as well as increased demand for bug bounties, which are already very common in the industry.

Trust in the crypto industry is at an all-time low. And for good reason. There have been too many high profile losses

due to fraud, hacks, and a general lack of due diligence. Crypto companies, DAOs, and blockchain protocols in general have been an appealing target due to the often irreversible nature of transactions and short settlement times. The lack of regulation and immature best practices have resulted in poor hygiene and shortcuts throughout the industry, making many companies easy targets. However, 2023 will serve as an inflection point in the industry, and those institutions that remain in the market will be required to meet a higher standard of due diligence to maintain and attract new customers.

Customers will demand the usage of common frameworks for security governance, risk and compliance (e.g., NIST CSF, ISO 27001), and audits to show compliance with standards like GLBA, SOC2, and FSSCC.

Cyber defenders become cyber criminals

While we can expect new roles in security, audit, and governance around blockchain and crypto in 2023, the macroeconomic landscape, as well as the crypto bear market have led to layoffs and fewer jobs in general. Challenges in finding work as a defender could lead some security engineers and researchers to generate income as attackers —and some of those attackers may have inside knowledge of your infrastructure and applications because they helped build them. Agitated ex-employees are always a risk to a business, but a poor economy can greatly exacerbate the problem.