CERTIK

HACK3D

THE WEB3 SECURITY QUARTERLY REPORT | Q2 2022 EDITION

Securing the **Web3** World

EXECUTIVE SUMMARY

1. Over **$2 Billion** has been lost in Q1 and Q2 alone, meaning that 2022 has already lost more to hacks and exploits than the entirety of 2021. This means that 2022 is already the most expensive year for web3 by far.

2. In Q2, a total of **$308,579,156** has been lost due to flash loan attacks, making it the highest amount lost via flash loan attacks ever recorded.

3. Phishing attacks have increased by **170%** since last quarter, highlighting social media platforms as a major pain point for web3 projects.

4. CertiK Q2 Stats: **628** projects audited, **432** new clients. This brings the total number of CertiK audited projects to **3702**. CertiK also completed KYC verification for 67 projects and onboarded 78 new projects to Skynet.

> ***Over $2 Billion has been lost in Q1 and Q2 alone, meaning that 2022 has already lost more to hacks and exploits than the entirety of 2021.***

OVERVIEW

With **$870 Million** ($870,802,424) lost to hacks, scams, and exploits, Q2 continues what has been a devastating year for web3 security; A fact sharpened by the wider losses incurred by the persistent bear market.

Over **$2 Billion** has been lost in **Q1 and Q2** alone, meaning that 2022 has already lost more to hacks and exploits than the entirety of 2021. This means that 2022 is already the most expensive year for web3 by far. From these numbers, 2022 is forecast to see a **223% increase** in the funds lost to attacks when compared with 2021.

There is some cause for slight optimism given that the amount lost to attack is down by **42%** from the previous quarter, however this data is skewed by the catastrophic attack against the Ronin Network for $624 Million in late March.

Whilst marking a decline in overall attack, there has been a steep rise in the number of flashloan attacks and phishing attacks, two of the most popular hacks that, frustratingly for web3 security, can often be avoided and mitigated by the web3 security tools available.

The number and scale of rugpulls and exit scams continues to remain low when compared with the previous year. Whilst there has been a slight increase from Q1 of 2022, numbers are still far lower than the eye-watering losses seen in the previous year. However, we may have the bear market to thank for this, as rugpulls and exit scams thrive off of the newer money that pours in during a bull run.

As we emerge from Q2, the need for projects to take on a proactive, end-to-end approach to their security has never been more apparent. If one lesson can be taken from the trauma of Q2, it is that, in web3, the security of a single project and the security of the entire ecosystem depend on one another. To that end, CertiK continues to strive to secure the web3 ecosystem through honing and expanding our products that help web3 projects protect both themselves and their communities. Ultimately, it is only by implementing rigorous security measures that projects can shift from a position of reacting to attacks, to actively anticipating them, a shift that is vital to securing a stable and prosperous future for web3.

> ***“ 2022 is forecast to see a 223% increase in the funds lost to attacks when compared with 2021.***

SOCIAL MEDIA IS BECOMING THE "ACHILLES' HEEL" OF WEB3

There has been a marked increase in phishing attacks throughout Q2, with CertiK recording **290** attacks, meaning that phishing attacks have increased by over **170%** when compared with the 106 recorded in Q1 of 2022.

The vast majority of these attacks targeted projects' Discord servers, which highlights both the dependence of NFT projects on the social media platform for marketing to and engaging with their communities, but also the huge security risks that this dependence entails.

Unlike Twitter which supports account verification, social media platforms like Discord and Telegram don't. This allows hackers to clone accounts, and lay bait in the form of giveaways and "too good to pass up" token offers.

What's frustrating about these hacks from a web3 security perspective, is that the hackers are deploying the tried and tested tricks of web2 that exploit centralization and human error as a starting point, and are using this to make lateral moves to exploit web3 in turn.

In this way, the prevalence of phishing attacks shows web3's ongoing and fraught relationship with the outmoded and vulnerable infrastructures of web2. Indeed much of web3's negative reputation as a digital 'wild west' arises from the points where it relies on web2 technologies and the vulnerabilities it entails. This drives home how web3 security depends on it moving further away from, rather than returning to, the centralized practices of its predecessors.

At the immediate level, there are a few key things that can be done to avoid such attacks. Firstly, projects need to bolster the security surrounding community managers and anyone with access to privileged accounts. This means implementing practices of decentralization such as requiring 2FA authentication and multi-sig authentication so there is no single point of failure in the project's structure, particularly at the point where the project overlaps with centralized systems such as social media.

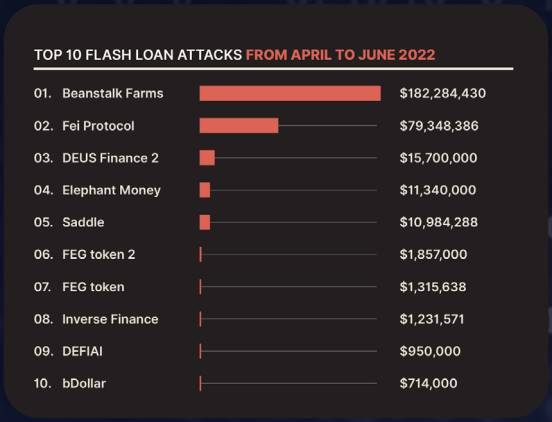
Projects also need to foster increased decentralization around accessing privileged accounts. This means requiring multiple users to authenticate identity anytime a privileged account is accessed and also renouncing any user privileges after each session.

At the other end, community education needs to improve so that members know to stay extremely vigilant against attacks. This means exercising the utmost caution whenever clicking on links, even if they are posted over official channels.

FLASHLOAN ATTACKS ARE TRENDING UPWARD

Flashloan attacks continue to be a major pain point for web3 projects, with a total of **$308,002,694** lost across **27 attacks**.

When compared with Q1 this is a staggering increase both in terms of the number of attacks, and the amount lost to each attack. The number of attacks up 66.7% from 14 attacks in Q1 to 25 attacks in Q2, and an over 2000% increase in the amount of funds lost from $14,178,471 lost in Q1 to $308,002,694 lost in Q2.



Q2's numbers are skewed by the highest profiting flashloan attack on record, in which a hacker made away with $182 Million after targeting Beanstalk Farms. This accounts for 59% of the total loss in this quarter alone. The $79 Million flashloan attack against Fei protocol also accounts for a significant portion of this. To put this in perspective, the biggest flashloan attack in Q1 was the $3 Million attack against Deus Finance. Yet even without these, Q2 has still been a far more devastating quarter than Q1 for flashloan attacks.

Looking towards the future, flashloan attacks have drastically increased in terms of both frequency and profits each quarter, and our projections are grim for the remainder of this year. Using Q1 and Q2 as baselines, we can forecast **nearly $656M in losses**, which is a 78% increase in loss over the previous year.

Only flashloan attacks that have reached a threshold of being profitable attacks, over $100k or against a highly visible or popular protocol, have been included in this report. Many attacks resulted in small losses, and many losses or attacks are lost in the noise of simple arbitrage farming by bots. It is also worth noting that flashloan attacks are rarely "just" flashloan attacks, they often involve manipulation of price oracles, bridge vulnerabilities, liquidity pair pools, and many more exploits.

> ***A total of $308,002,694 has been lost to flashloan attacks across 27 incidents.***

RUGPULLS

Rugpulls and exit scams continue to be one of the most popular forms of attack, with **$37,462,472** lost across **90** attacks. Whilst this is a 16.7% increase from Q1, Q2 still continues the sharp decline in losses to rugpulls and exit scams from the previous year. By comparison, Q2 of 2021 saw a staggering **$2,650,234,662** lost in rugpulls and exit scams.

Whilst this decline is of course welcome, it is likely a consequence of the persistent bear market. As the flow of new money entering the web3 economy dries up, so do the kinds of uneducated investors who are likely to fall prey to the wild promises of bad faith projects. By contrast, the average web3 investor weathering the so-called 'crypto-winter' is both harder to dupe, and a lot less willing to part with their hard-earned funds. Add to this the devastating events that occurred in Q2 such as the collapse of Terra, Three Arrows Capital and insolvency issues with Celsius, and it is no wonder that we have not seen a rush of new investors entering the space.

Whether this drop in rugpulls continues once we move into a better market remains to be seen and will depend on both increased investor education, and also better cultures of transparency and accountability around project teams. To that end, CertiK has introduced CertiK KYC, which provides verification checks for project teams using a combination of AI technology and human checks. Doing so is key to both saving investor funds, but also securing the web3 ecosystem as a whole. Look out for the KYC badge on CertiK's leaderboard for projects that have undergone this process.

> ***"There has been a total of $37,462,472 lost to rugpulls across 90 attacks.***

MAJOR EXPLOITS

Exploits comprise a broad category of hacks in which attackers target vulnerabilities that are specific to a project's code or its intersection with other infrastructures. In contrast to other categorizations, hacks that come under major exploits are more tailored to a specific project and, as a result, harder to group. Sometimes it may be a case of compromised multi-sig passwords, other times hackers will target bugs and vulnerabilities in code, exploiting minting functions, reentrancy problems, or flaws in the ways that oracles are used.

Given the breadth of this category, there have been fewer attacks than when compared to other more narrow categories that occurred this quarter. However, they are also disproportionately represented amongst the more devastating attacks, with 7 of the top ten most lucrative attacks classed as exploits, and 50% of the top ten attacks exploiting bugs in the projects' underlying code.

Q2 saw over **$520 Million** lost to exploits over **39** attacks. This is a marked decline in losses when compared with Q1 – **down 57% from $1.2 Billion**– yet surprisingly no decline in the number of attacks, which actually slightly increased from 33 to 39. Much of this difference is accounted for by the seismic $624 Million attack on the Ronin Network which accounts for over half of the losses to exploits in Q1. However, even without the Ronin Attack, the average funds lost per exploit is down from 19 Million to 13.3 Million.

> ***Q2 saw over $520 Million lost to exploits over 39 attacks.***

In fighting to secure web3, CertiK provides a number of tools designed to help projects take an end-to-end approach to their security.

The CertiK Security Leaderboard – with a total of 1956 completed and on-boarded projects at the end of 2021 – allows web3 users to leverage the expertise of our auditing and security teams in order to equip themselves with a deeper knowledge of security risks. These users push the whole ecosystem to new heights, while we provide the data that helps them make informed decisions.

Skynet actively monitors hundreds of web3 platforms in real-time, using a combination of on-chain transaction monitoring and off-chain data such as social sentiment to ultimately arrive at a comprehensive security analysis. Skynet Premium – unveiled in 2021 – integrated continuously-evolving machine learning to grow in lockstep with the constantly shifting smart contract risk environment, getting more and more advanced as it encounters new threats and vulnerabilities. The Premium platform includes an analytics dashboard which enables enterprise clients to monitor and manage their risk in real-time.

CertiK's Security Oracle allows developers to leverage real-time security scores provided by a decentralized network of nodes to ensure that their contract's interactions with other smart contracts meet an acceptable level of security. This allows developers to take advantage of the powerful interoperability of web3 while protecting their own contracts against failures of third-party dependencies.

SkyTrace is an intelligent, intuitive tracing tool to help analyze and visualize transaction data across Ethereum and BSC wallets. This tool provides actionable insights into identifying and tracing suspicious flows to and from one's own personal wallet or a project's team wallet.

CertiK KYC provides identity verification for project teams which includes an ID authenticity inspection using AI-based detection systems, as well as liveness checks to ensure the individual is indeed real and matches the ID. In addition to a liveness check during the ID verification process, CertiK will also do a live video call with each team member to verify their identity and other parameters as needed. As team anonymity increasingly enables high-risk behaviors, CertiK KYC helps to build accountability around projects to enable investors to move forward in trust.