



GET METAMASK

ECOSYSTEM



Crypto Security Report: July 2024

Featuring recognition for MetaMask's HackerOne bug bounty program, WazirX's \$230 million multisig hack, Squarespace domain-takeover attacks, an Ethereum.org mailing list breach exposing 35,000 users, and FBI warnings on rising crypto job scams.



Luker

🕒 7 minutes

📅 August 1, 2024



METAMASK

July 2024

Security Report

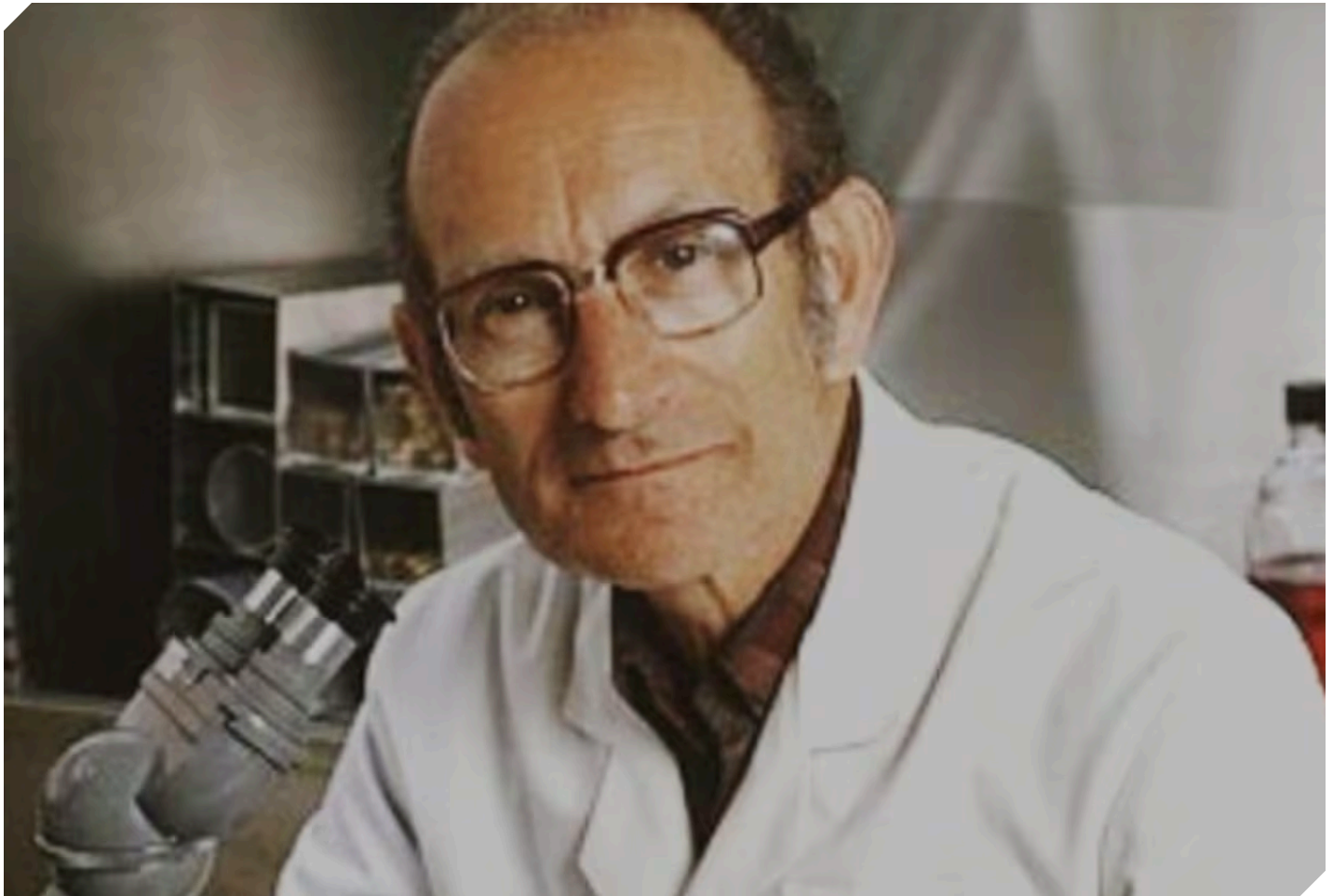


Each month, MetaMask Security Director Luker reports on the latest c emerging risks that you need to know about.

GET METAMASK

In July 2024, MetaMask's HackerOne bug bounty program earned praise from HackerOne's founders, while Security Lab's Zbigniew Tenerowicz and Gal Weizman took LavaMoat, LavaDome, and DOM isolation to x33fcon, BlueHatIL, and OWASP. Elsewhere, MetaMask's Realms Initialization Control proposal entered incubation. On the threat side, WazirX lost over \$230 million in a multisig exploit, a Squarespace vulnerability enabled domain takeovers across the industry, an Ethereum.org mailing list breach exposed 35,000 users to a draining attack, and the FBI warned of rising crypto job scams. The full breakdown is below, but first...

Featured STEM pioneer: César Milstein, Nobel-winning pioneer of monoclonal antibodies



César Milstein (1927–2002) was an Argentine biochemist who shared the 1984 Nobel Prize in Physiology or Medicine for developing the technique to produce monoclonal antibodies. Antibodies are the immune system's precision tools—engineered to recognize and neutralize

one specific threat—and Milstein's work made it possible to produce them reliably at scale. That idea of targeted, repeatable threat detection is exactly what m GET METAMASK g strives for.

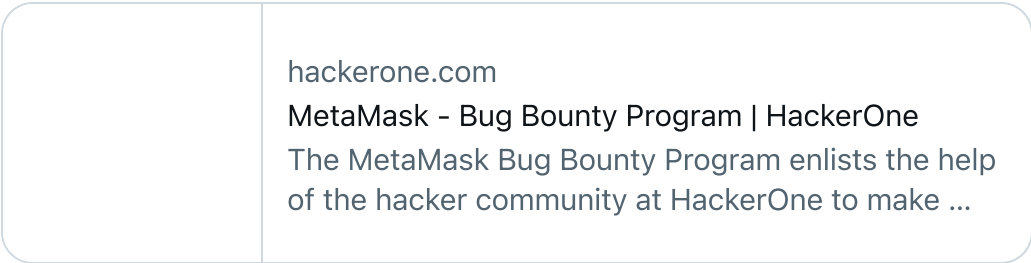
MetaMask's HackerOne bug bounty program earns founder praise

MetaMask's bug bounty program got a shout-out from both HackerOne founders, [Jobert Abma](#) and [Michiel Prins](#), for quickly adopting new policy improvements—Open Scope, which rewards reports across all of MetaMask's assets based on impact, and Fast Payment, which commits to paying out within a month of receiving a report. Over the prior 90 days, the [program](#) received 120 reports, averaged 3 days and 15 hours from submission to bounty, and paid out \$266,000 to date. MetaMask thanked its community of researchers—including pkkr, innarendrabhati, plsecurity, Nicocha30, T4lnk, René Kroka, renniepak, hackerOnTwoWheels, and redyetihacks—and invites anyone who finds a vulnerability to report it through its HackerOne program.

Jobert Abma
@jobertabma · [Follow](#)



Today [@Hacker0x01](#) is launching a big improvement to program policy pages, providing structure and remove ambiguity! Here's a great example from [@MetaMask](#): hackerone.com/metamask.



hackerone.com
MetaMask - Bug Bounty Program | HackerOne
The MetaMask Bug Bounty Program enlists the help of the hacker community at HackerOne to make ...

9:03 AM · Jul 15, 2024 

 93  Reply  Copy link

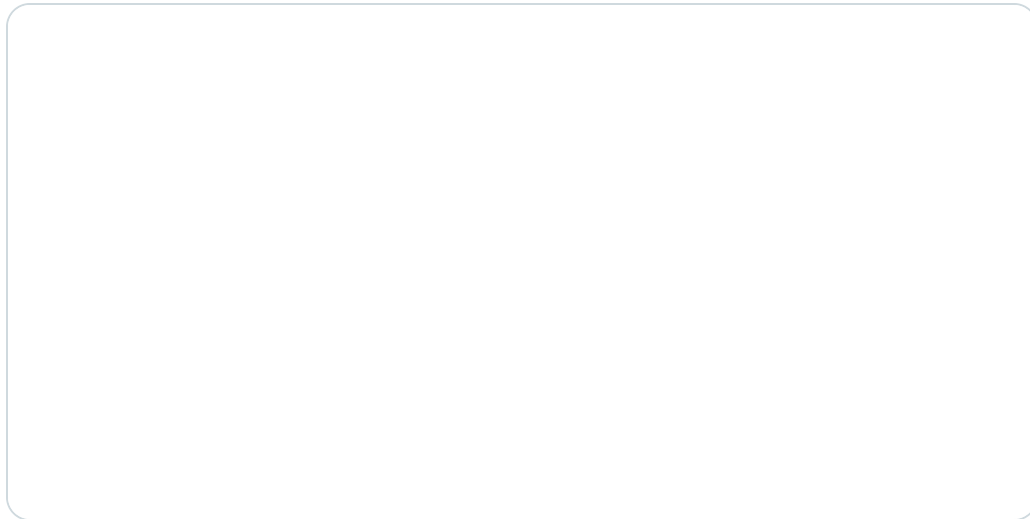
[Read 4 replies](#)



GET METAMASK

Michiel Prins@michielpriins · [Follow](#)

That was fast. Within hours of publicly releasing the new Program Declarations, [@MetaMask](#) has already adopted the Open Scope and Fast Payment declarations. Great programs move with a high sense of urgency!
hackerone.com/metamask?type=...



10:54 AM · Jul 15, 2024



39



Reply



Copy link

[Read 4 replies](#)

Zbigniew Tenerowicz talks defensive coding at x33fcon

MetaMask Security Lab's Zbigniew Tenerowicz is at it again! In June 2024, ZB attended x33fcon, a gathering for IT security professionals "where red meets blue," giving a [lightning talk](#) and hosting a workshop on defensive coding. It's the latest step in his push to evangelize supply chain security—the core focus of LavaMoat. Both his talk and an [interview](#) are available now.



Zbyszek Tenerowicz interview

x33fcon

GET METAMASK



Watch on

Zbigniew Tenerowicz lighting talk

x33fcon



Watch on

Gal Weizman presents DOM isolation at BlueHatIL and OWASP, and Realms Initialization Control enters incubation

Gal Weizman, also from MetaMask Security Lab, presented on DOM isolation and the LavaDome project at Microsoft's [BlueHatIL](#) and OWASP Lisbon's Global AppSec conference,

examining how the difference between securing centralized and decentralized architectures pushes the boundaries of web application security. Additionally, he r GET METAMASK ns Initialization Control proposal MetaMask presented was approved for incubation by the Web Incubator Community Group. Implementing this proposal should eventually provide a native, browser-level solution to the "same origin concern" that the Snow project originally set out to address—an important step toward securing a complex client-side web security problem.

BlueHat IL 2024 - Gal Weizman - DOM Jungle - Can We Trust The U

Microsoft Israel R&D Center



Watch on



DOM Jungle - Can We Trust The UI? - Gal Weizman

OWASP Foundation

GET METAMASK

What Can Traditional Web App Security Learn From Browser Wallet

OWASP Foundation



Watch on

Understanding DPKR group Lazarus' threat to crypto and their TraderTraitor campaign

MetaMask Security's Taylor Monahan explored a new campaign called TraderTraitor, from members of the North Korea-linked advanced persistent threat (APT) group Lazarus. TraderTraitor uses spearphishing to target employees of crypto companies and steal millions. Anyone working in the crypto industry, at any level, should consider themselves at risk, warns Monahan. Her advice: eliminate single points of failure, use hardware wallets and hardware MFA, don't run or build code from strangers, use different devices for communication versus accessing crypto, learn from others' mistakes, educate those around you, and stay skeptical.

Scammers get scammed: Pink Drainer gets address-poisoned for \$30,000

In an ironic turn, the infamous Pink Drainer scam group fell victim to an address poisoning scam, losing around \$30,000 worth of ether after being tricked into sending ether to an address that closely resembled a legitimate one. Cryptocurrency compliance firm MistTrack reported the incident, noting the irony of scammers being scammed. Pink Drainer had only just announced its retirement in May 2024 after stealing millions from crypto wallets.

Ethereum.org third-party mailing list breach exposes 35,000 to a draining attack

On July 2, 2024, Ethereum reported that its mailing list was compromised, exposing over 35,000 users to a phishing attempt. The attacker sent an email posing as a collaboration with Lido DAO, directing recipients to a site that promised high returns on staked Ethereum but was actually a drainer. The Ethereum security team quickly blocked the attack, alerted the community, and submitted the malicious link to blocklists; no losses were reported, and Ethereum began migrating email services to enhance security.

Squarespace vulnerability enables domain-takeover attacks

What happened

Researchers found that weak security defaults in Squarespace's domain registration process allowed attackers to hijack domains. Insufficient verification and the ability to change domain settings without proper authentication let them take control, redirect traffic, and potentially steal sensitive information. In its incident post-mortem, Squarespace cited OAuth-related weaknesses as the cause, said it had fixed the issue, and reported no additional compromises. After a coordinated, industry-wide response, samczsun—with MetaMask Security's Taylor Monahan, AndrewMohawk, and others—published a retrospective.

How users can protect themselves

Users should harden their Squarespace accounts by enabling two-factor authentication (2FA) and removing unnecessary contributors, and consider registrars that support hardware tokens for 2FA.

**samczsun** @samczsun · [Follow](#)[GET METAMASK](#)

After spending the last four days helping teams recover and secure their Squarespace domains, we believe the vulnerability has finally been patched

A big thank you to [@tayvano_](#), [@AndrewMohawk](#), and numerous others for jumping in and saving the day

securityalliance.notion.site

A Squarespace Retrospective, or How to Coordinate an Industry-Wide...

July 14, 2024 — samczsun, tayvano, AndrewMohawk

10:01 AM · Jul 15, 2024

**346****Reply****Copy link**[Read 22 replies](#)

WazirX loses over \$230 million in a multisig exploit

India-based crypto exchange and trading platform WazirX suffered a cyberattack on one of its multi-signature (multisig) wallets, **losing over \$230 million**. The wallet, managed through Liminal's digital asset custody service, required multiple signatories—three from WazirX and one from Liminal—but the attack exploited a discrepancy between what Liminal's interface displayed and the transaction's actual contents, likely swapping the payload to transfer

control to the attacker. The incident is a reminder that custodial solutions central withdrawal of funds, whereas only the user controls funds with self-custodial wallets. [GET METAMASK](#) [tina a bounty](#) worth up to \$23 million to help identify, track, and recover the stolen funds.

FBI warns of rising cryptocurrency job scams

In June 2024, The Federal Bureau of Investigation (FBI) [released a public service warning](#) about cryptocurrency job scams, where fraudsters pose as legitimate employers to lure victims into fake job opportunities. This month, the agency [followed up with a more in-depth look into how these job scams work](#) and what to look out for. They often involve convincing victims to set up cryptocurrency accounts or transfer funds, ultimately stealing their money. The FBI advises job seekers to be cautious of unsolicited job offers, verify the legitimacy of employers, and avoid sharing personal or financial information with unverified sources. Victims of such scams are encouraged to report the incidents to the FBI's Internet Crime Complaint Center (IC3). Beyond scams that target job seekers, businesses should also watch for attacks during the interview process and insider threats—a risk underscored by reports of North Korean operatives attempting to pose as [remote IT workers](#) and [fake job-interview malware targeting Macs](#).

MetaMask's July 2024 Crypto Security Report covered recognition for its HackerOne bug bounty program, the WazirX multisig exploit that lost over \$230 million, and a series of threats spanning a Squarespace domain-takeover vulnerability, an Ethereum.org mailing list breach, and rising cryptocurrency job scams. Browse previous editions of the [MetaMask Crypto Security Report](#) for more threats, trends, and tips for staying safe across the ecosystem.

Subscribe to Alpha for market alpha straight to your inbox

Email address

protected by reCAPTCHA

SUBSCRIBE

Learn about our privacy practices in our [Privacy Notice](#).

[GET METAMASK](#)[ECOSYSTEM](#)[INSIGHTS](#)[SECURITY](#)

Luker

Jen Luker, known by most as just Luker, is the Director of Product Security at Consensys, where she leads the frontline defenders who protect millions of users from vulnerabilities, emerging threats, and malicious actors across decentralized tech. An active participant in the Ethereum ecosystem since 2017, she has held key roles including Editor at ETHNews and Project Manager at MyCrypto. Luker is a regular speaker at industry conferences, the author of MetaMask's monthly Crypto Security Report, and an official ETH Security Badge holder as designated by The DAO. She's also a passionate advocate for continuous education and security awareness as essential pillars for the future of Ethereum and blockchain technology.

[Read all articles](#) →

Latest articles

[All news](#) →





What are bitcoin treasuries and how do they work?

A guide to how corporate bitcoin treasuries work, from convertible bonds and fair value accounting to the risks this model carries.



What is a bitcoin ETF?

Learn about bitcoin ETFs: how creation and redemption mechanism works, what spot and futures ETFs each hold, and where ETF exposure ends and direct ownership begins.





What is a Bitcoin wallet?

Bitcoin wallets store Private Keys that control BTC addresses. Compare software vs hardware, custodial vs self-custodial, and SegWit vs Taproot address formats.



- Trade
- Swap
- Money
- Buy NEW
- Predict
- Developer
- Perps NEW
- View the Docs
- View MetaMask
- Buy NEW
- Transaction Shield
- Earn
- Agent Wallet NEW
- Explore prices
- Supported Wallets
- Explore conversions
- Connect
- Solana Price
- Shiba Inu Price



GET METAMASK

Bitcoin services
Bitcoin wallet
Best crypto cards
Contact



What is Polymarket?

Crypto tax news

How to buy cryptocurrency?
Privacy Policy
How to sell bitcoin?
Terms of Use

Contributor License Agreement

Sitemap

Accessibility

Manage Cookies

©2026 MetaMask • A Consensys Formation