From Web2 Security With Love

There is hope, if you know where to look.

Joe ‘dobs’ Dobson

The views and opinions expressed are my own - *not* my employer's.

Who am I?

Joe ‘dobs’ Dobson

15+ years in cybersecurity

I track bad guys in Web2 & Web3
(Threat Intelligence)

Previously:
Digital forensics
Incident response

2x startups
2x Mandiant
Now Google (who acquired Mandiant)

I'm not here to spread FUD (Fear, Uncertainty, & Doubt).

There is no Web3 without Web2.

This also means web3 security is about more than smart contracts!

Web2 has made a lot of mistakes - please learn from them.

Everyone in the cryptocurrency ecosystem is a target.

You are the front line of defense.

Hard Truth 1: You Are A Target

Builders.
Users.
Investors.
Artists.
VC partners.
Memelords.
Grandparents.

Hard Truth 2: You Are Outgunned

Cyber conflict is asymmetric. Nation states have targeted *individuals*. Cyber criminals use specialized tools for attacks that may go undetected.

Newly active wallets are targeted with malicious tokens within ***35 seconds.*** *Crypto n00bs are getting airdropped malicious tokens before they even know what a token is.*

Attackers are clever, well-resourced, and persistent. There is a reason the term “**A**dvanced **P**ersistent **T**hreat” (APT) was coined.

Hard Truth 3: Unless You Act, You'll Get rekt

Crypto is under attack. Billions of dollars have been stolen. DAOs have been hacked. Social media accounts have been hijacked.

Bugs and vulnerabilities will be found. You must find and address them before motivated attackers do.

Attackers have the element of surprise.

You must be intentional about security.

Assume Compromise

Build your systems with the expectation that they ***will*** be compromised.

Tool your systems so that you are prepared to do something when they ***are*** compromised.

Your smart contract might be bulletproof, but what about:

- Your DNS
- Your code's supply chain
- Your SIM card
- The apps on your devices

0days happen.

Web2 security has been here before.

You must *assume compromise*.

Every attack cannot be stopped.

Defense in Depth

Getting compromised ***does not*** mean getting rekt

Focus not just on ***preventing*** hacks, but ***minimizing severity***.

Defense in Depth can be applied to cryptocurrency - in particular, in the Ethereum ecosystem

The USA's National Security Agency applied Defense in Depth to Information Security

Defense in Depth

A practical strategy for achieving Information Assurance in today's highly networked environments.

Source: https://web.archive.org/web/20121002051613/https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Examples of Layered Defenses

Class of Attack	First Line of Defense	Second Line of Defense
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

Source: https://web.archive.org/web/20121002051613/https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Defense in Depth In Practice

A well-planned defensive posture can reduce intrusions and their impacts.

Centralized Crypto Exchange Example:

- Customer support is on a separate network segment than developers
- Maximum outflow in a single tx is limited to $X
  - Triggering 80% of the outflow enacts a cooldown
  - This gives Operations a chance to evaluate the large transaction(s)

Freelance Developer Example:

Isolate social media access from developer's computers with Virtual Machines or separate devices. "Decoy" wallets on machines with social media

Have An Incident Response Plan

Preparation helps you survive compromises.

Have a plan that helps defenders and costs attackers.

You want to:

- Identify a compromise earlier
- Respond faster
- Minimize the impact
- Follow a well thought-out plan

Do not make it easy on the attackers.

Understanding The Attacker Helps. A Lot.

Attribution Matters

Attribution = Understanding who is attacking you.

Script kiddies? Cyber criminals? Nation states?

Financial theft is ***a*** motivation for threat actors in web3, but not the ***only*** motivation. Others include:

- Malware delivery
- Command & control
- Misinformation
- Hacktivism

Understanding the “who” and “how” of attacks can help you prepare.

Understanding Attribution

Questions that help attribute attacks:

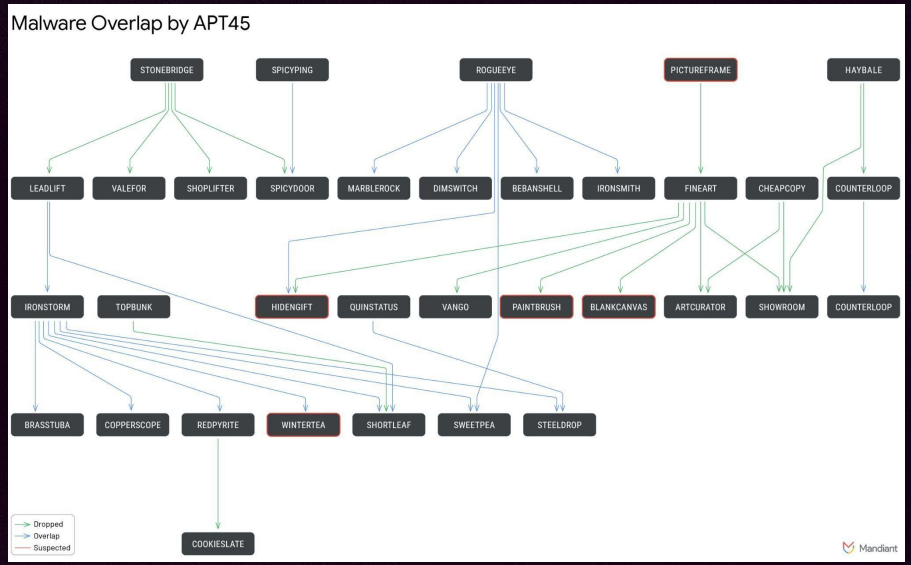
What are the tactics, techniques, and procedures (TTPs) used by attackers?

What malware is used? How was it delivered? What does it do? Who uses it? Is it shared across threat groups?

What does the attacker's infrastructure look like? Is there a domain? How long has it been registered & active?

These questions also apply to smart contracts & on-chain activity!

An example of tracking the relationships between different families of malware used by a single threat group:



Source: https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

Attribution Matters

Attribution helps Ethereum.

Understanding ***who*** is attacking you helps to understand ***what*** they are doing (or did), ***how*** and ***why***.

How can the ecosystem prevent attacks?

Dwell time represents the period an attacker is on a system from compromise to detection, and in 2023 the global median dwell time is now 10 days, down from 16 days in 2022.
-A quote from Mandiant on their 2023 MTrends report

Source:
https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024

All that said...

There is hope.

You don’t have to go it alone.

The industry is decentralized. So is cryptosecurity.

You are the frontline of defense - this also means that you have information that can help the community.

Trusted sharing is key to the health of the ecosystem.

ISAC = **I**nformation **S**haring & **A**nalysis **C**enter
SEAL-ISAC
Crypto-ISAC

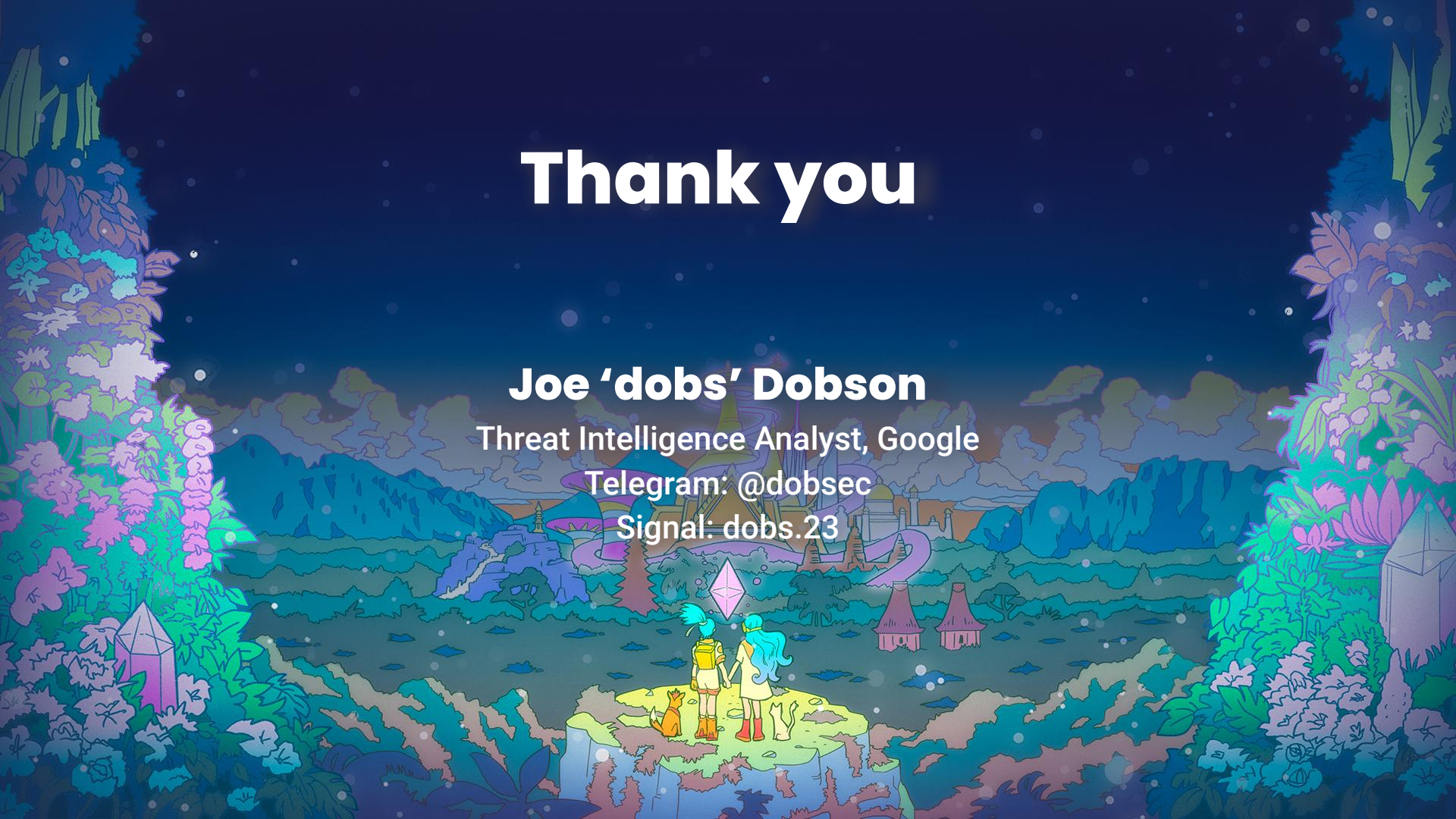
Moving Forward

Web3 is young, innovative. *Don't repeat the mistakes of the past.*

Think about security. Be intentional about it.

Web3 security can look different (DAOs investing in security for developers)

Be innovative. Consider building something to support or enhance security.


Thank you
Joe ‘dobs’ Dobson
Threat Intelligence Analyst, Google
Telegram: @dobsec
Signal: dobs.23