The Long Con

Pig Butchering, Drainers and Job Scams

Luker

Director of Security, Metamask

The Most Depressing Talk at Devcon

Section 1

Social Engineering

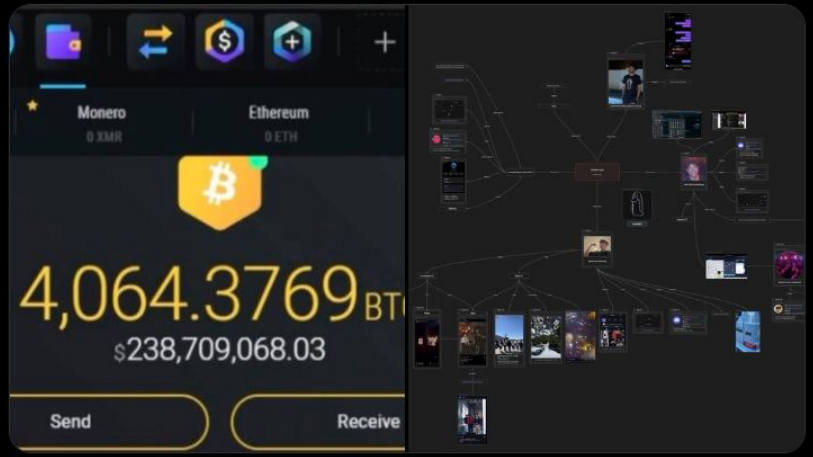
Social Engineering

- 98% of all cyber attacks involve social engineering.
- Everyone can be a target, regardless of experience.
- In September 2024, IC3 reported over 69K crypto-related complaints with more than $5.6B in losses.

Social Engineering

ZachXBT
@zachxbt

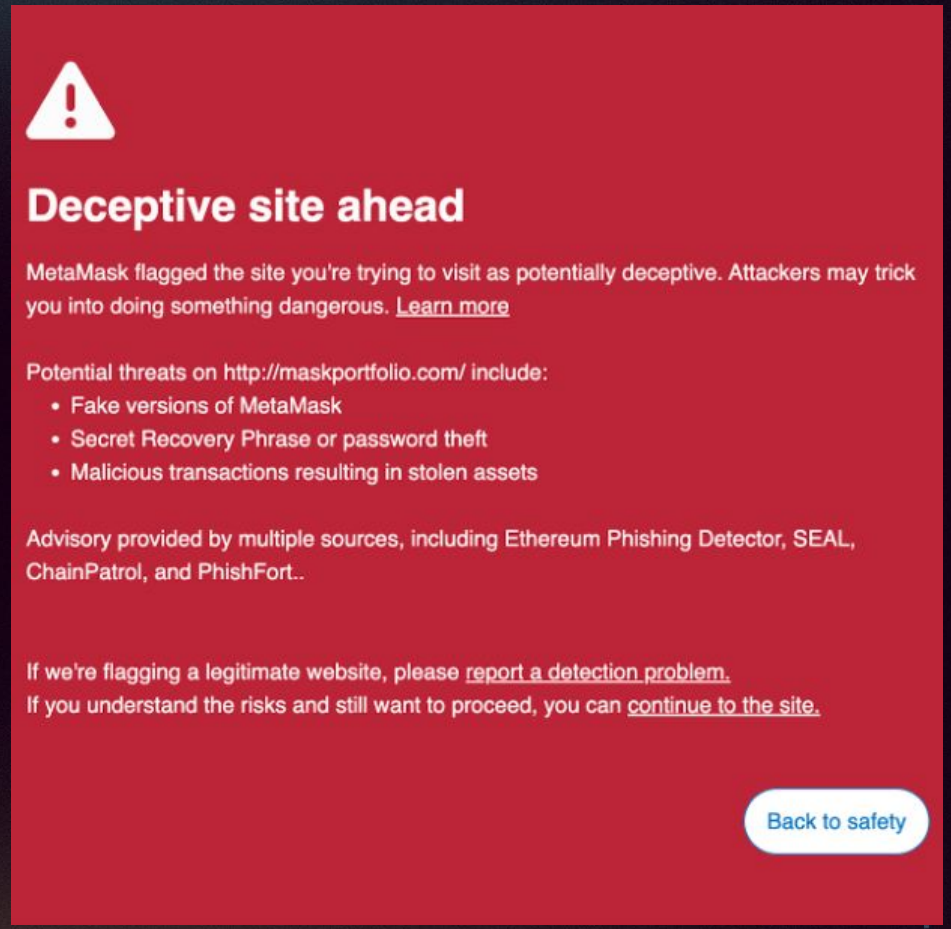
1/ An investigation into how Greavys (Malone Iam), Wiz (Veer Chetal), and Box (Jeandiel Serrano) stole $243M from a single person last month in a highly sophisticated social engineering attack and my efforts which have helped lead to multiple arrests and millions frozen.



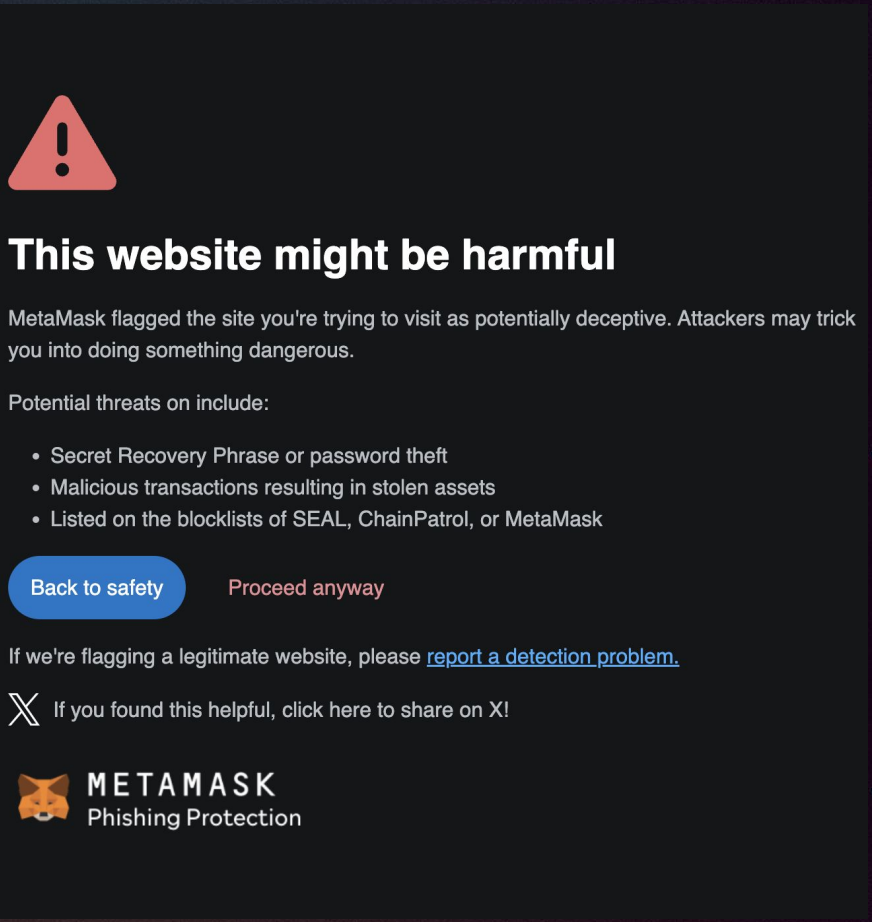
6:03 AM · Sep 19, 2024 · **7.6M** Views

These security groups and projects are all working together...

... to put in guardrails to warn users when they're about to do something dangerous...



... to put in guardrails to warn users when they're about to do something dangerous...
... now in Dark Mode™



Social Engineering Tips!

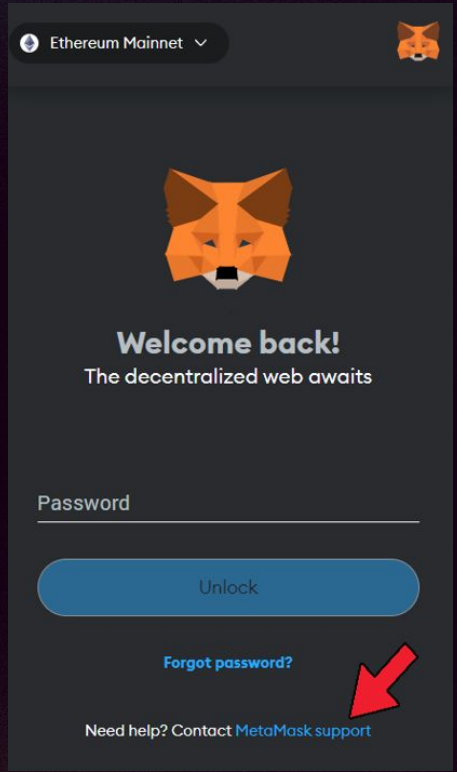
Tips for Users:

- Support is never going to contact you
- Never ever trust support links from social media, forums, or unsolicited email
- If “support” does contact you, exit that conversation, then contact support yourself through a *verified contact method*.

Social Engineering Tips, Part 2!

Tips for Developers:

- Clearly communicate to your users what the official channel is to contact support.
- Consider putting this link in a *very obvious* place in your product.



Section 2

Drainers

Drainers

Code written specifically to maximise the value of digital asset theft

- Employing various strategies to steal various asset types
- Sometimes involves custom smart contract logic
- Usually obfuscated JavaScript, sometimes compiled to WASM.

Typically distributed as a service

- We have various actors; the drainer vendors, affiliates, others

Code written specifically to maximise the value of digital asset theft

- Employing various strategies to steal various asset types
- Sometimes involves custom smart contract logic
- Usually obfuscated JavaScript, sometimes compiled to WASM.

Drainers: Key Activities and Tactics

Account Takeover

- X accounts: @SECGov (Jan2024), @Azuki (Jan2024), @DOHgovph (Apr2023), @VitalikButerin (Sept2023)

Phishing

- Typosquatting domains, brand impersonation domains, NFT airdrops with malicious metadata

Supply Chain Attacks

- Npm: @lottiefiles/lottie-player (Oct2024), @ledgerhq/connect-kit (Dec2023)

Drainers: Impact

- The drainer is packaged so it’s easy and quick to spin up for a campaign
- With various strategies employed, they can target many different Defi profiles with one campaign
- They are prevalent and consistent at targeting users

Drainers: Notable Incidents

Trader lose$ $1.28m in P… and other altcoins to Inferno Drainer-linked wallet

$1.28M

By Rony Roy October 14

Edited by Dorian Batycka

$55M

Crypto trader loses $55M in DAI to phishing attack using Inferno Drainer kit

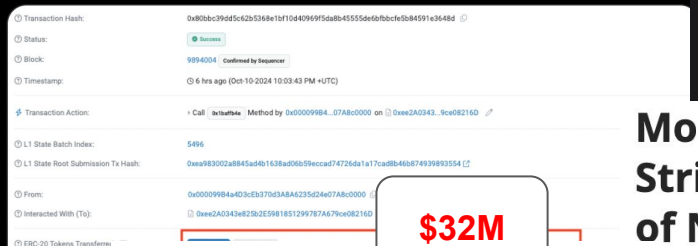
The attacker has reportedly converted some of the stolen assets into Ethereum.

Oluwapelumi Adejumo
Aug. 21, 2024 at 12:45 pm UTC

PeckShieldAlert
@PeckShieldAlert

$35M

#PeckShieldAlert The address 0xEab2E...a393 has been drained 15,079 $fwDETH (worth ~$35M) signing a #phishing permit signature



Crypto Wallet …ffers $32 Million Loss in spWETH Due to Phishing Scam

$32M

2 mins

By Lynn Wang
28 September 2024, 17:44 GMT+0000

Updated b…
28 Septe… GMT+00…

MS Drainer Scam H… Hard, $3M in Crypto Stolen on Christmas

$3M

Scammers use MS Drainer to drain $3M in crypto on Christmas Day, highlighting the evolving cyber threats in cryptocurrency.

By Kelvin Munene Murithi
December 26, 2023

Monkey Drainer Sc… Strikes Again, Steals $800K of NFTs

$0.8M

…hing scammer made o…
…n Cr… NF…

$0

…oliver Knight
…2022 at 6:1…

Pink Drainer Hackers Drain $4.4 Million in LINK

$4.4M

Author: Wayne Jones
Last Updated Dec 29, 2023 @ 15:09

Drainers: Biz Ops

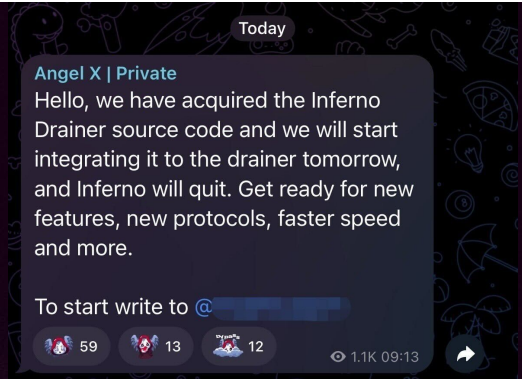
- DaaS work like traditional tech companies
- Provide support to their affiliates
- They even buyout rival drainers to acquire customers and code bases

Inferno Support today at 21:38

Hello everyone,
Today is a big day for draining as the Inferno team is delegating the entire Inferno project to the Angel team

This was a very hard decision for us, because we are really attached to our drainer but it is time for us to quit. However, we find the Angel Drainer team competent enough to maintain the drainer (while keeping our code base and features such as 200+ protocols, autoclaims, bypasses as well as many big pending updates, new panel with logs handling and many other things) as they have shown they could be trusted with handling a drainer and big hits, without ever scamming or backdooring.

All of our customers will keep the same logins as well as stats, autosplit % etc. We have worked really hard with the Angel staff to put together the best of our previously respective drainers.



Angel Drainer absorbs Inferno's toolkit, becoming a larger threat to crypto wallets

By Cryptopolitan_News

Created 23 days ago, last updated 22 days ago • 4 mins read

Drainers: Tips!

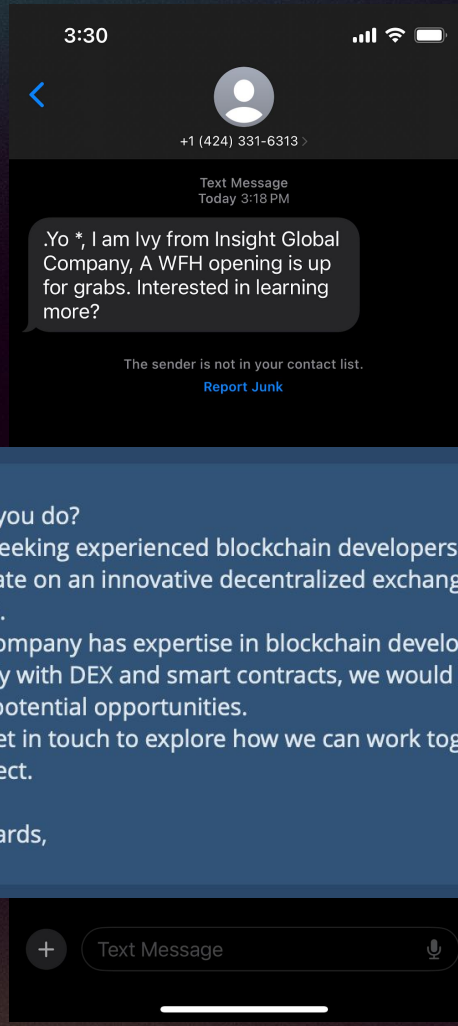
- Double check URLs
- Don’t trust unsolicited messages
- Beware of giveaways and urgent requests
- Read the transaction screen and understand it before signing
- Regularly check wallet permissions
- Use hardware wallets for cold storage

Don’t Get Drained.

Section 3

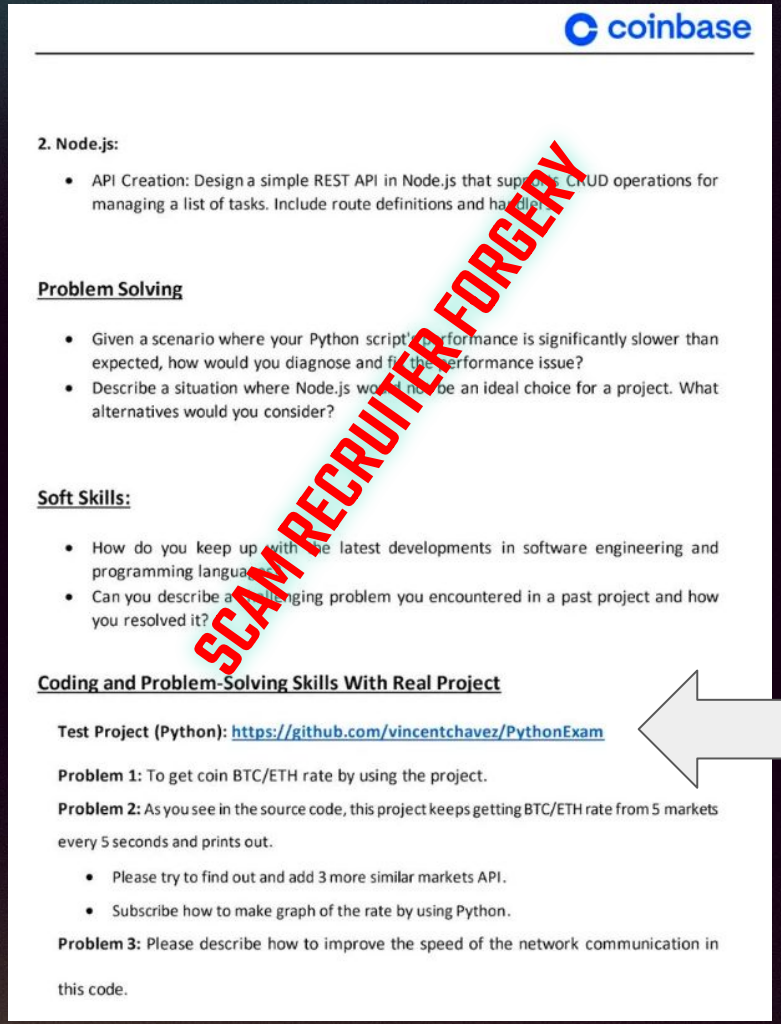
Job Scams

Scammers can pose as recruiters.

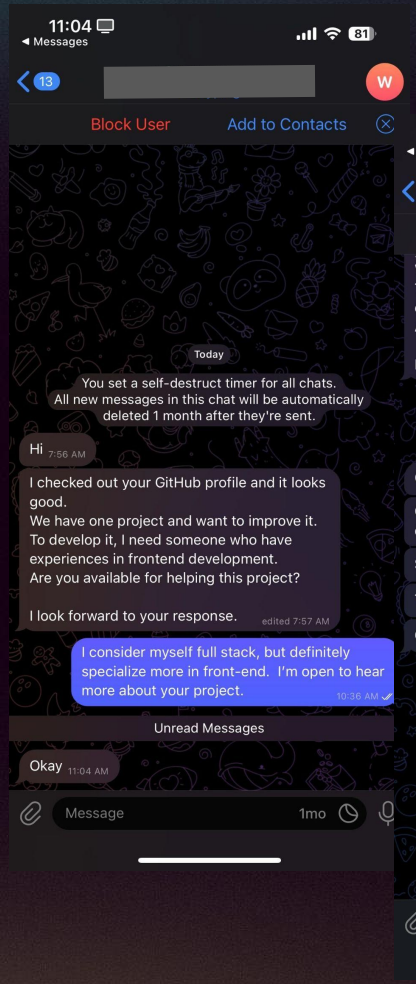


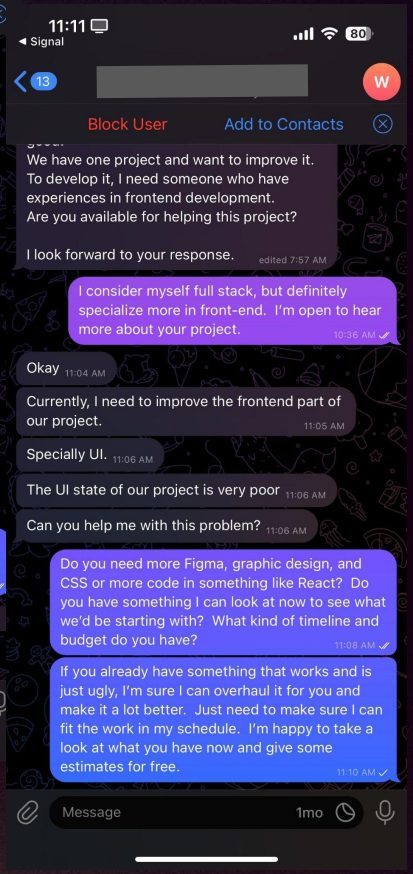
Scammers can pose as recruiters.

- Will contact via social media or messaging app
- Will direct target to a Github for a job offer, "skills test," or to help with a bug
- Target will be asked to clone a repo or download files
- From there they will compromise the target's machine and can gain entry to the AWS of the target's current company



Scammers pose as collaborators.





Job Scams Avoidance Tips!!

- Be cautious if solicited to clone or download content associated with accounts listed in GitHub's advisor

- Don't run/build code from strangers w/out sandboxing
- Use different devices for messaging versus accessing crypto
- Check to see if the the user profile is recent
- Verify to see if the user has connections in your network
- Check if the repository is recent, with few commits and stars
- Use hardware wallets/hardware MFA

Scammers pose as job seekers.

ZachXBT 
@zachxbt

1/ Recently a team reached out to me for assistance after $1.3M was stolen from the treasury after malicious code had been pushed.

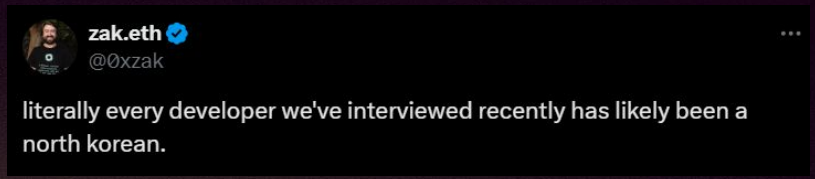
Unbeknownst to the team they had hired multiple DPRK IT workers as devs who were using fake identities.

I then uncovered 25+ crypto projects with related devs that have been active since June 2024.

Payment address	Fake Location	Github	
0x6b94ba1528636af600dab486a217d39bb7ce21d75 0x1075ef62bfacbb44e31d7a5719e65c7d148a7d36d 0x79f69b188f1bc6b9f0d68f2f24ac34554dfe9f6cf5d 0xa771609C5C56048f146d2C794cB7DB946bF27C7 0x90cf352cDAF171d41A0DEd1d54cEDA4605047c83 0x72c70990ACdd7a5C9437000E73E7a97f921025	Canada	https://archive.ph/J347I https://archive.ph/WIu3i	0xr
0x97a1f4fA676c07ef07cD121992748bAE18ef1CdD8d	California, US	https://archive.ph/5jJfK	will
0x6188e9e7679f4e7cb337b9E5e2D918086Ce34Fc6D1 0x85e06046cf7981bae68774431099c5e2dcf074dd	Tokyo, Japan	https://archive.ph/96QVA	naok
0xef2a0324cfaa0100db9de9fef31c6e23bc4f9258	-	https://archive.ph/KMoXG	
0x8aa07899eb040f40e514b8ef8cb3b6af5d1cf7bb	Singapore	https://github.com/junkai121	jun
0xff22be4f00fc837dade564bd9659e2669f2afa620 0x4525205c6c3872691fbce7ce6453537d496d55f76 0x21e5d5afe40b32cff77c9a77dca0346d4101131d	Tokyo, Japan	https://archive.ph/mc0QZ https://archive.ph/fhKTT	kein
0x210888f2624d01fbcbc71de5bf4caf5b6dc9fa7f	Fukuoka, Japan	https://archive.ph/80EYH	devc
0xd80614fe0b54d49cf46cc861fc540fae0a05b3f7e	-	https://archive.ph/cGIGc	
0x09f90983cd2215379e440fc525e4416e9fc3fba 5JfbSn8erWLkyQrKJktMNBF3rtC1pc21Hjf93kz9rT15QHh 0xa8afe0290fb6f2f7ced0a2753de57f5fa7c9c9dd 0xfa802d9b33ec74baff62b189875c2b2d192874e0 0x7854e18f34956f7809c906fa39b62640e5d0e8a7	Michigan, US	https://github.com/call-by https://archive.ph/grgjk	jos sma
0x1043efee936903951b88db2355187 3bb67292e95	-	https://archive.ph/7lbnH	and
0x82cd7363c5b1853bc6fe6b5ae209838fc506caf3	Texas, US	https://archive.ph/tFeQG	clou
0x9de5d3158b0b83e6211c7444d94ce0c63763f574 0xf9adac8668e08693fb4e91c1062e471eb11cb6c7	-	https://archive.ph/KLBYw	lett
0xa71641a495e33bb13548a01aca5e20e083e637b 0x6fb67fb0d4fbc2f50ee9ecf774251fccde57a2da8	-	https://archive.ph/V5GsZ	ryu
ESSP3aAcW5Z59sxu69JkqyBhkX5YTH2t5b3Vhe2hxf 0x1043efee936903951b88db2355187 3bb67292e95 0x3b9A870c24905256bDE10863cb369F48933C7cC60f 0xc2b2a9c20740Ef97ee7BA7e83A811ECBbe8CB1D1	Malaysia	https://archive.ph/x0LMf	a
GrXoeqM2e9QFKSbd2SRRJVJCBVTFvuuH8eCjdLbjhpdR 0xC9054F484ed98a7Dd632EB9c09644616db3deA8C 0x2EFe21F4Fef7e737C0a3491C93dbe7D696038fe9f5 0x65b48a82ff85A429dfaf2c8B1304065A819A5394 0x184729E00e8C0fB711891 60f36dee4386cAde1F2 0x09f90983cd2215379e440fc525e4416e9fc3fba	Malaysia	https://github.com/devneser	ale
0xb94510493113053b20e5d69fb54bff37a5e38819c	Texas, US	https://archive.ph/r9TU	jam
0xb3ebf4962e4a2e1b5031911e27236253bc1afa 0xfd1b05e51653339c850c8a1bc8ac11aed91095f2a	-	https://archive.ph/Kq8Kd	
0x9db9e27080b7f8258448aa31c36e7c0937fd55f7	-	-	
0x5d8335834bfdf4c746e277e5100d7c77fc807356	-	https://github.com/issaaiinooo77	
0x97467ea9bef1c925e9c8e2e65932d0368860e2f13 0xF9cB6897a3387e10d0E52697C38D7f8bb6A1454f	Vietnam	https://archive.ph/vgsFX https://github.com/0xdoccer	rust
0xfb6d591e8216f5d096428f09b1f61114c16aab0	Singapore	https://archive.ph/nVlz9	pemb pemb

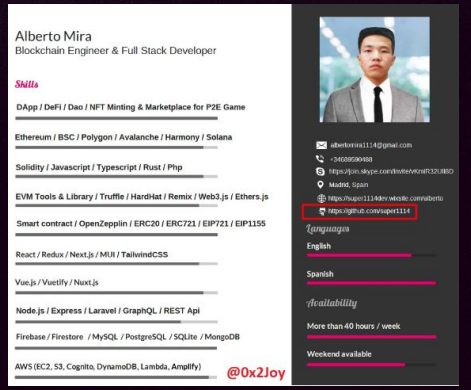
Job Scams

- US-based remote-first tech companies are being targeted
- Companies are beholden to sanctions violations laws



Job Scam Avoidance Tips!!!

- INVEST IN THOROUGH BACKGROUND CHECKS!
- Best practice: Principle of least authority
- Things to look out for:
  - No online presence or inconsistent online presence
  - Inability to answer basic questions about where they supposedly are
  - Background noise that sounds like call centers
  - Refusal to appear on camera during video calls



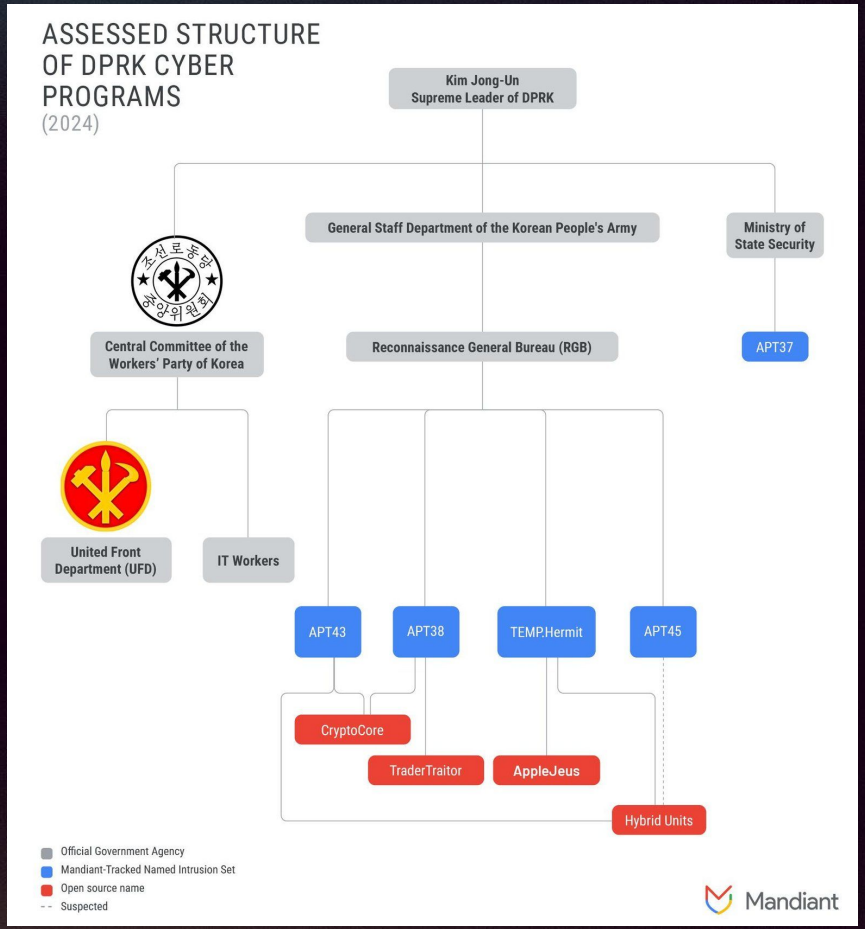
Job Scams

TraitorTrader
Targets: CEXs and bridges via their engineers and devops.
Tactics: Impersonates recruiters or hiring managers. Utilizes job offers, technical job tests to deliver malware via malicious Github repos or npm packages. Previously used malicious trading apps. Then escalates from to fully rekt company & infra.

SquidSquad/DangerousPW/CryptoCore
Targets: Founders, CEOs, fund managers, admin keys
Tactics: Impersonates a VC and using a fake video call or fake Google Doc to land a remote-access trojan. Will also write super custom malware to compromise keys—especially admin keys.

Contagious Interview
Targets: Anyone in crypto, esp. those working in crypto.
Tactics: More general-purpose malware / infostealer. Steals from unsuspecting individuals via outreach on job forums, Linkedin, Upwork, Braintrust, etc.

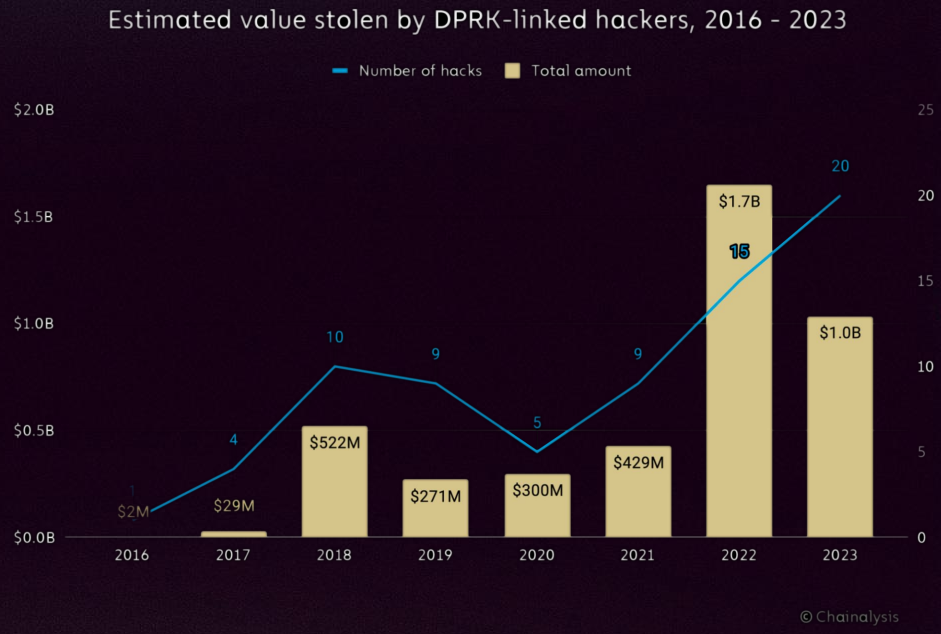
Job Scams


ASSESSED STRUCTURE OF DPRK CYBER PROGRAMS
(2024)
Kim Jong-Un
Supreme Leader of DPRK
General Staff Department of the Korean People's Army
Ministry of State Security
Central Committee of the Workers' Party of Korea
Reconnaissance General Bureau (RGB)
APT37
United Front Department (UFD)
IT Workers
APT43
APT38
TEMP.Hermit
APT45
CryptoCore
TraderTraitor
AppleJeus
Hybrid Units
Official Government Agency
Mandiant-Tracked Named Intrusion Set
Open source name
Suspected
Mandiant

Job Scams

“North Korea’s launch of yet another intercontinental ballistic missile (ICBM) in February of 2023 displays unprecedented advancements in technological capability, defying expectations for a country under strong United Nations (UN) sanctions. North Korea has developed such capabilities in part by stealing billions in cryptocurrency.”

- *Georgetown Journal of International Affairs*



Job Scam Facts!

- In March 2024, the UN estimated that these IT workers are generating between $250M-$600M every year for the DPRK
- Some estimates are over 50% applicants across crypto industry are dprk
- “Wagemole,” is the term for where threat actors seek unauthorized employment with organizations with potential for both financial gain and espionage

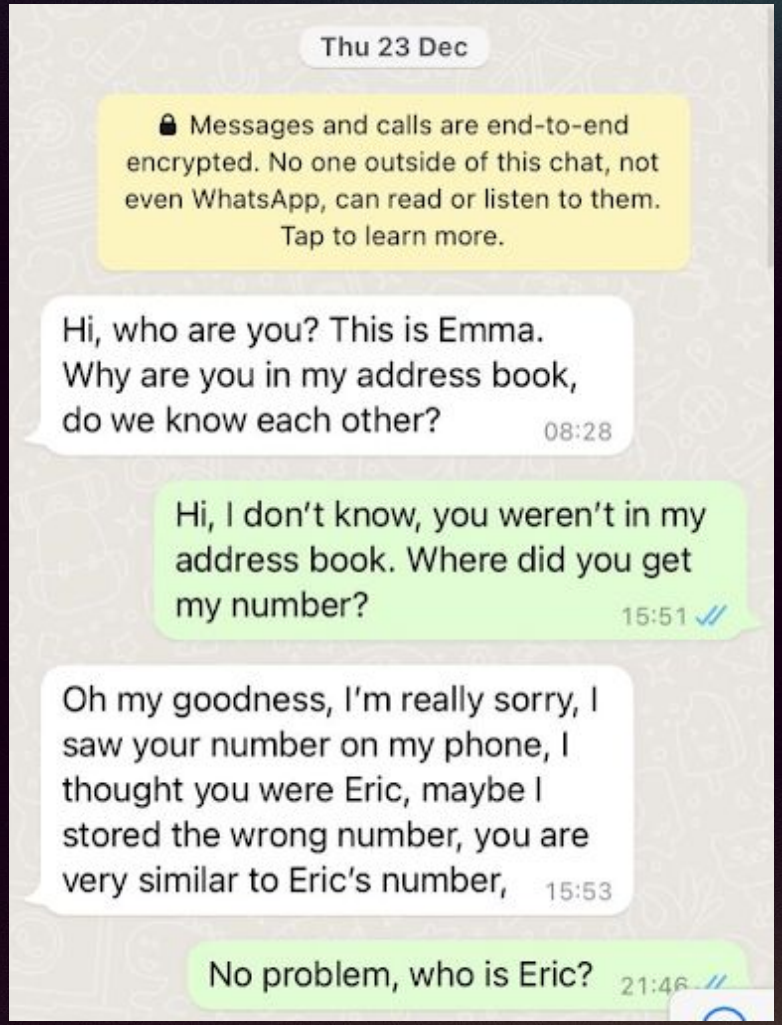
Section 4

Pig Butchering

Pig Butchering

What is “Pig Butchering?”

- 杀猪盘 (sha zhu pan) - *rough translation: pig slaughtering game*
- “Fattening up” the victim (pig) over time before the final theft.



The beginning of the process is not always obvious.

Pig Butchering

Confirmation Bias

- The tendency to interpret new evidence as confirmation of one's existing beliefs or theories

Pig Butchering

Romance Scams

- Targets loneliness and the fear of struggling

Pig Butchering

Steps:

- Presentation
- Grooming
- Pressure Tactics
- Cutting Off

Pig Butchering

A fake platform can be quite convincing.

Pig Butchering

- The scammer is not operating alone
- The majority of these scams are conducted by criminal rings / organized crime syndicates
- Scammers are trained on tactics to gain trust and extract value. They have quotas

Pig Butchering

This is where the talk begins to get dark.

Pig Butchering

- Kidnapping

Pig Butchering

- Kidnapping
- Trafficking

Pig Butchering

- Kidnapping
- Trafficking
- Ransom

Pig Butchering

- Kidnapping
- Trafficking
- Ransom
- Forced Labor

Pig Butchering

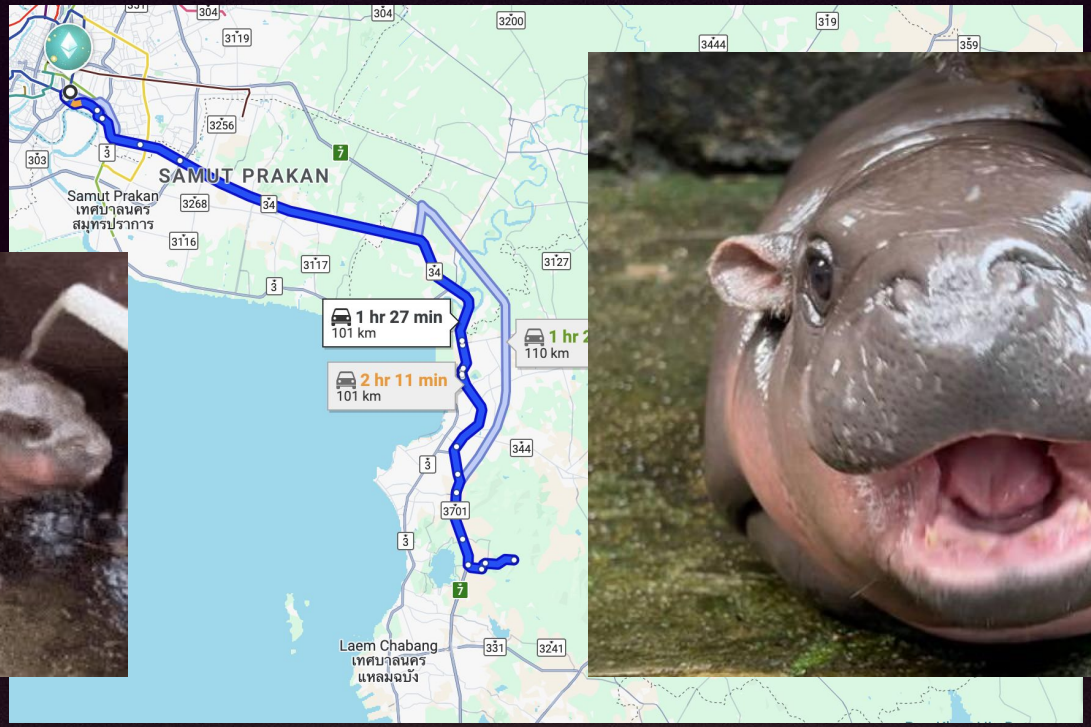
Pig Butchering

KK Park, Myanmar

Pig Butchering

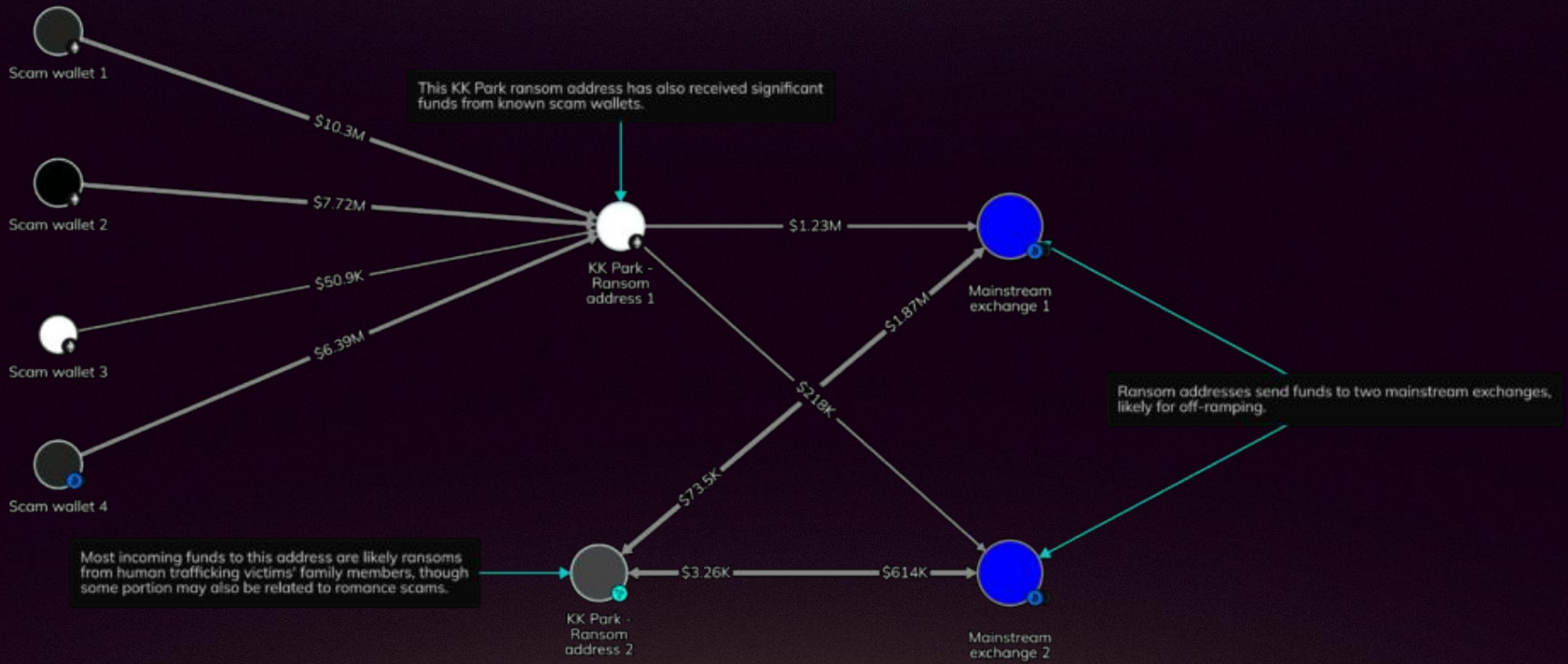
KK Park, Myanmar

Pig Butchering



Moo Deng, Khao Kheow Open Zoo

Pig Butchering

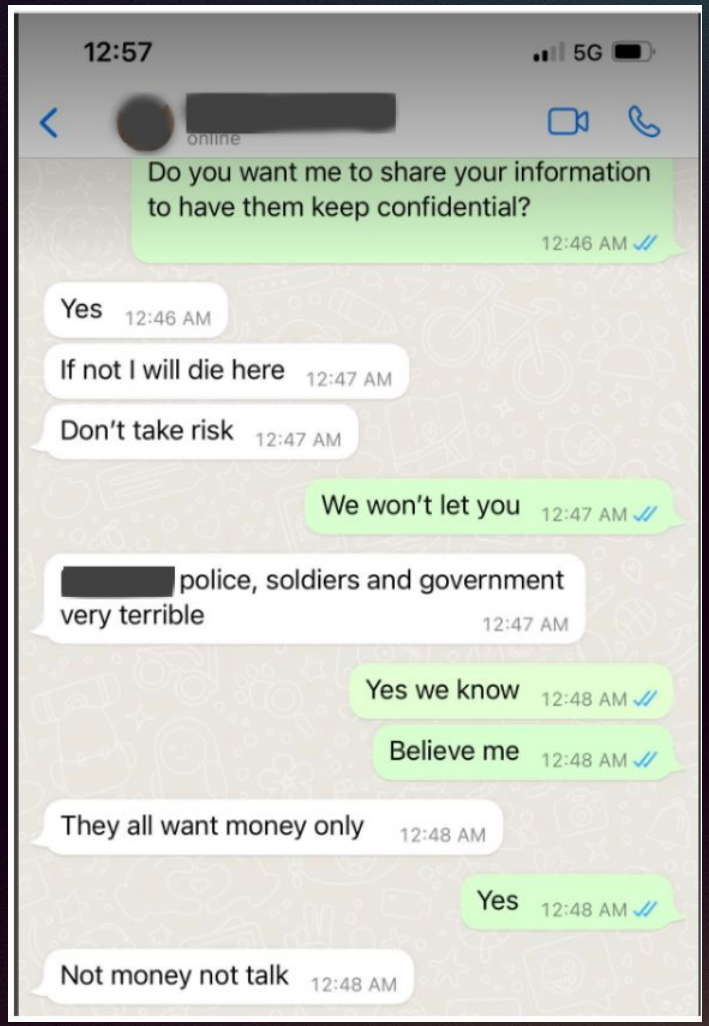


Chainalysis published this graph by Eric Heintz, Global Analyst at the Global Fusion Center of the International Justice Mission.

Pig Butchering

TRIGGER WARNING

Pig Butchering



"I was taught how to hit on them for about three or four days. After being friends for about a week, you go in for the 'kill'.' I wondered when I scammed them, would they become penniless, would they face hardship."

Pig Butchering

Global Advance Projects (GAP)

globaladvanceprojects.org

Partner with us to 'bridge the GAP from captivity to freedom'.

WE ADVOCATE ON BEHALF OF VICTIMS OF HUMAN TRAFFICKING FOR FORCED CRIMINALITY AND WE PROVIDE THEM WITH:

- FOOD
- SHELTER
- COMPASSION
- EMERGENCY AID
- RESOURCES
- STRATEGIES

That deserves a Unicorn Chaser.

That's All, Folks!

Luker

Director of Security, Metamask

luker@consensys.net

slides by Moo Deng - #hippo4lyfe