Documentation et analyse de la menace
ENSIBS, 2022-2023

Gimme Your Cryptoz

Axie Infinity, Intrusion ciblée et Cybercriminalité d'état

Ronan Mouchoux
Spécialiste en Analyse de la menace cyber

École d'ingénieurs
ensibs
Université Bretagne Sud

Présentation de l'intervenant

XRATOR
CONQUER YOUR RISK

- *Plateforme de gestion des risques*
- *Services:*
  - *Gestion des risques*
  - *Threat modeling*
  - *VAPT & Red Team*
  - *Conseil stratégique*

École d'ingénieurs ensibs : Université Bretagne Sud

Manager du module « Intelligence Cyber»

ESSEC BUSINESS SCHOOL

Manager externe du module « Security Strategy »

utt UNIVERSITÉ DE TECHNOLOGIE TROYES

Intervenant en analyse de la menace et criminologie numérique

RONINTEL
Cyber Threat Knowledge Management

2019-2021 TAL pour l'analyse de la menace

KASPERSKY lab

2017-2019 Analyse de la menace

SEKOIA

2015-2017 Analyse de la menace

AIRBUS DEFENCE & SPACE

2013-2015 Analyse de la menace

LA POSTE

2008-2013 Réseau & Sécurité

iut Saint Malo réseaux & télécoms

Réseau et Télécom (2008-2010)

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Réseau et Télécom (2010-2013)

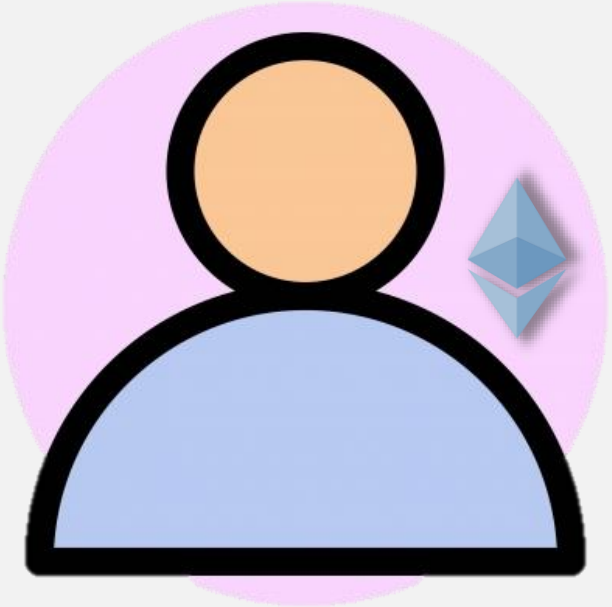
le cnam

Criminologie (2015-2016)

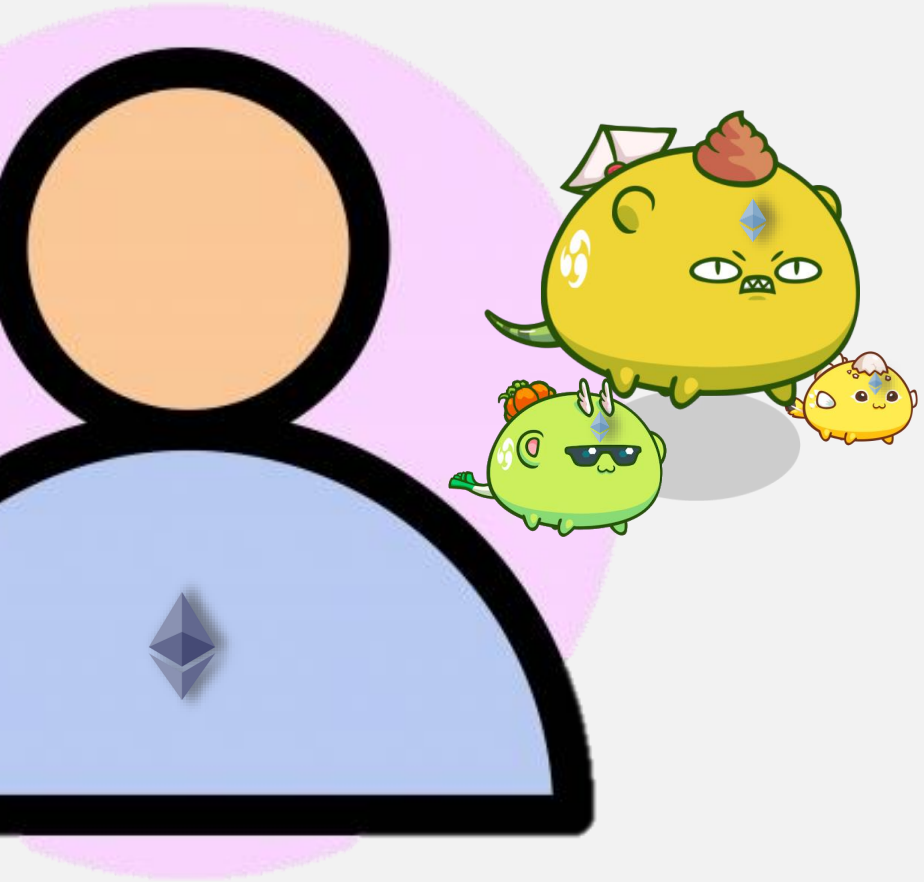
Axie Infinity - collect, breed and battle pets

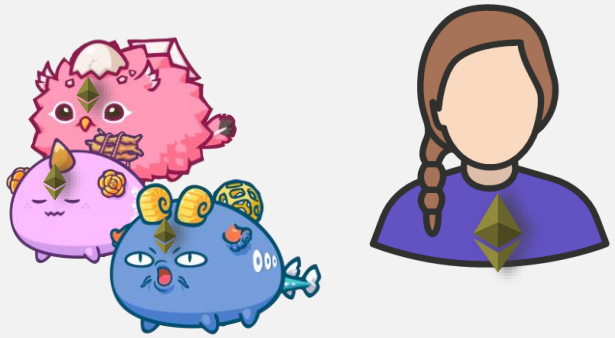
La mécanique NFT dans Axie Infinity

La mécanique NFT dans Axie Infinity



La mécanique NFT dans Axie Infinity





La mécanique NFT dans Axie Infinity

La mécanique NFT dans Axie Infinity

Smooth Love Potion – $SLP

ERC-20 Reward Token

SHARD – $AXS

ERC-20 Governance Token

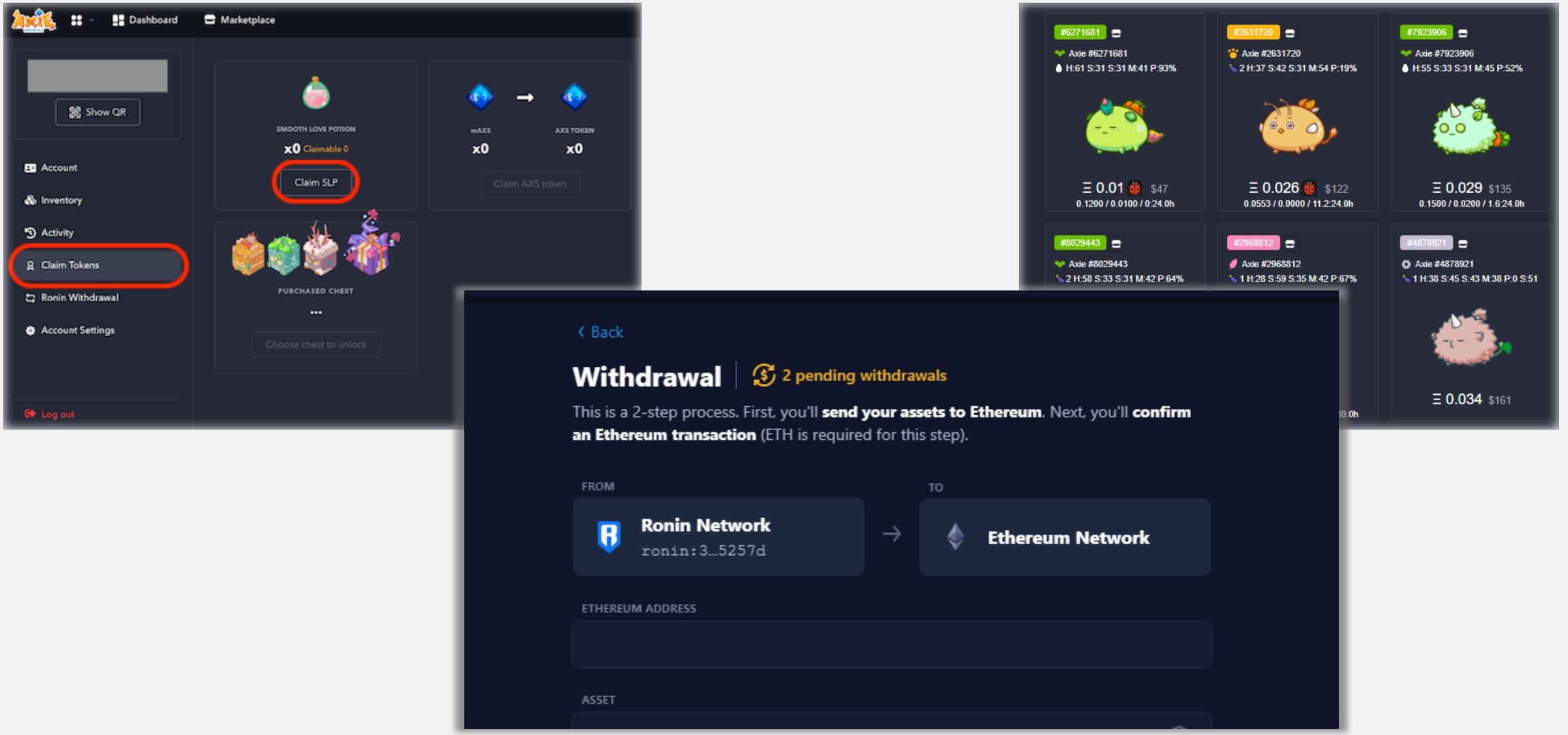
AXIE

NFT

RONIN – $RON

EVM-based Fees Token

La mécanique NFT dans Axie Infinity



La mécanique NFT dans Axie Infinity

Ronin
@Ronin_Network

The Ronin bridge has been exploited for 173,600 Ethereum and 25.5M USDC.

The Ronin bridge and Katana Dex have been halted.

9:29 AM · Mar 29, 2022 · Twitter Web App

Ronin's Newsletter

We thank you for your patience and support.

4/14/22 Updated Key Points

- Today, the FBI attributed North Korea based Lazarus Group to the Ronin Validator Security Breach.
- The US Government, specifically the Treasury Department, has sanctioned the address that received the stolen funds.
- We are still in the process of adding additional security measures bef redeploying the Ronin Bridge to mitigate future risk. Expect the brid deployed by end of month. Security comes first. The timeline is subje change based on the implementation time of several security measure
- We would like to extend a thank you to all law enforcement agencies supported us in this ongoing investigation.
- We expect to deliver a full post mortem that will detail security meas place and next steps by the end of the month.
- S our top priority, and we look forward to sharing our and the broader ecosystem. We thank you for yo

U.S. DEPARTMENT OF THE TREASURY

BOUT TREASURY | POLICY ISSUES | DATA | SERVICES | NEWS

We can do this. Find COVID-19 vaccines near you. Visit Vaccines.gov.

Regulations and Guidance

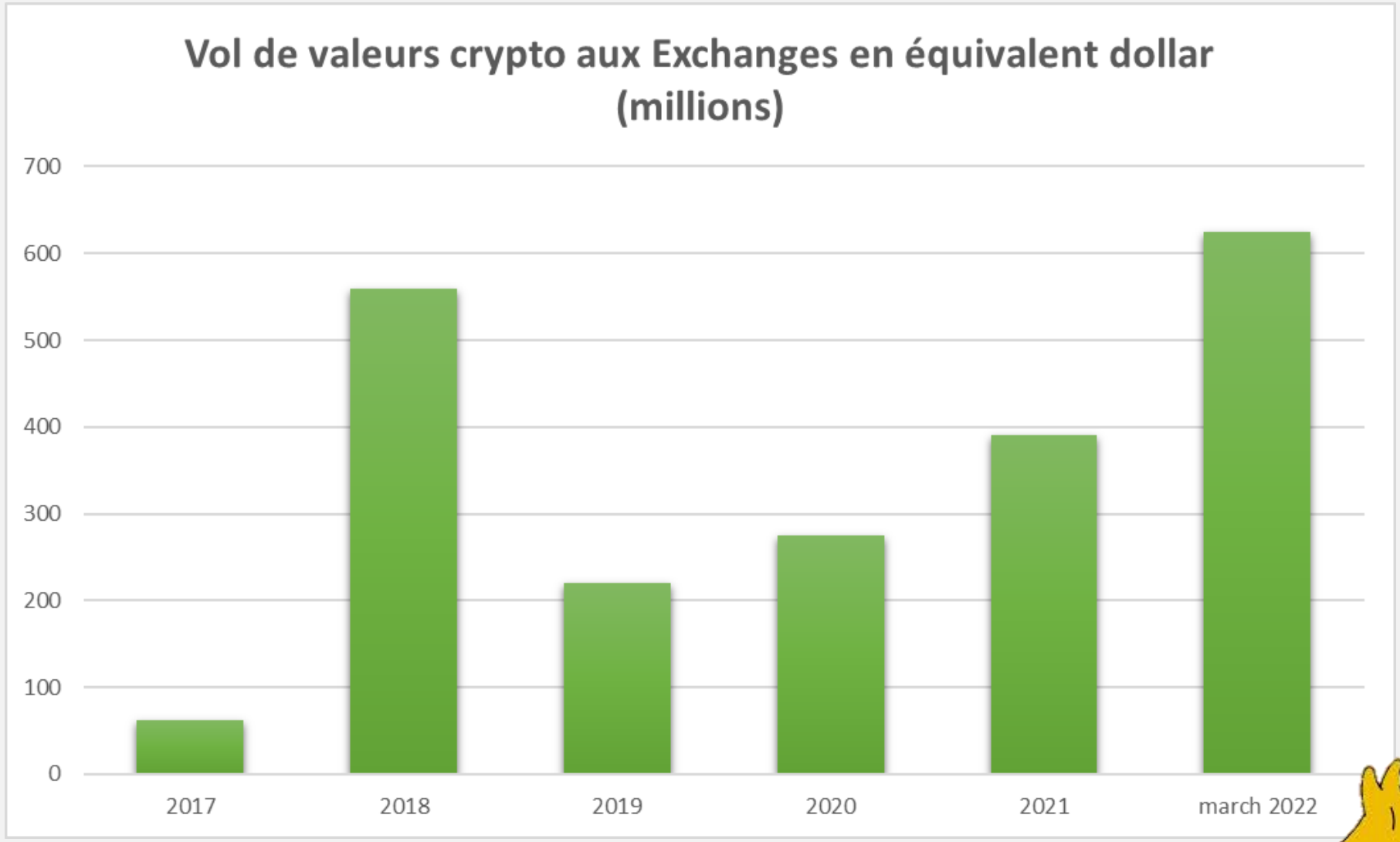
Sanctions List Updates

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following changes have been made to OFAC's SDN List:

LAZARUS GROUP (a.k.a. "APPLEWORM"; a.k.a. "APT-C-26"; a.k.a. "GROUP 77"; a.k.a. "GUARDIANS OF PEACE"; a.k.a. "HIDDEN COBRA"; a.k.a. "OFFICE 91"; a.k.a. "RED DOT"; a.k.a. "TEMP.HERMIT"; a.k.a. "THE NEW ROMANTIC CYBER ARMY TEAM"; a.k.a. "WHOIS HACKING TEAM"; a.k.a. "ZINC"), Potonggang District, Pyongyang, Korea, North; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214 [DPRK3]. -to- LAZARUS GROUP (a.k.a. "APPLEWORM"; a.k.a. "APT-C-26"; a.k.a. "GROUP 77"; a.k.a. "GUARDIANS OF PEACE"; a.k.a. "HIDDEN COBRA"; a.k.a. "OFFICE 91"; a.k.a. "RED DOT"; a.k.a. "TEMP.HERMIT"; a.k.a. "THE NEW ROMANTIC CYBER ARMY TEAM"; a.k.a. "WHOIS HACKING TEAM"; a.k.a. "ZINC"), Potonggang District, Pyongyang, Korea, North; Digital Currency Address - ETH 0x098B716B8Aaf21512996dC57EB0615e2383E2f96; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214 [DPRK3].

Responsable de plus de 50% des vols crypto depuis 2017



Hack & Pwned

Depuis les années 90

La crypto n’est qu’une victime,
le piratage n’est qu’un moyen,
l’argent n’est qu’une nécessité.

La guerre de Corée - 25 juin 1950 au 27 juillet 1953

Les ambitions nucléaires de la Corée du Nord - Marianne Peron-Doise, chercheur à l'IRSEM - 2019
(https://lelephant-larevue.fr/dossiers/les-ambitions-nucleaires-de-la-coree-du-nord/)

La bombe nucléaire gravée dans les esprits

ew York Times.

Copyright, 1950, by The New York Times Company.

LATE CITY EDITION
Becoming fair and cold today. Continued fair and cold tomorrow.
Temperature Range Today—Max., 41; Min., 32
Temperatures Yesterday—Max., 39; Min., 30
Full U. S. Weather Bureau Report, Page 41

NEW YORK, FRIDAY, DECEMBER 1, 1950. Times Square, New York 18, N. Y. Telephone Lackawanna 4-1000 FIVE CENTS

PRESIDENT WARNS WE WOULD USE ATOM BOMB IN KOREA, IF NECESSARY; SOVIET VETOES PLEA TO RED CHINA

NEW DEFENSES SET

Allies During Lull Form a Line Thirty Miles Above Pyongyang

AIR BASES ARE ABANDONED

U. S. Marines Encircled Near Reservoir in Northeast Beat Off Attacks by Chinese

U. N. MOVE BALKED

Russia Bars Resolution for the Withdrawal of Chinese in Korea

NEXT STEP IN ASSEMBLY

U. S. Plans to Refer Motion to Veto-Free Body Next Week —New Version Sifted

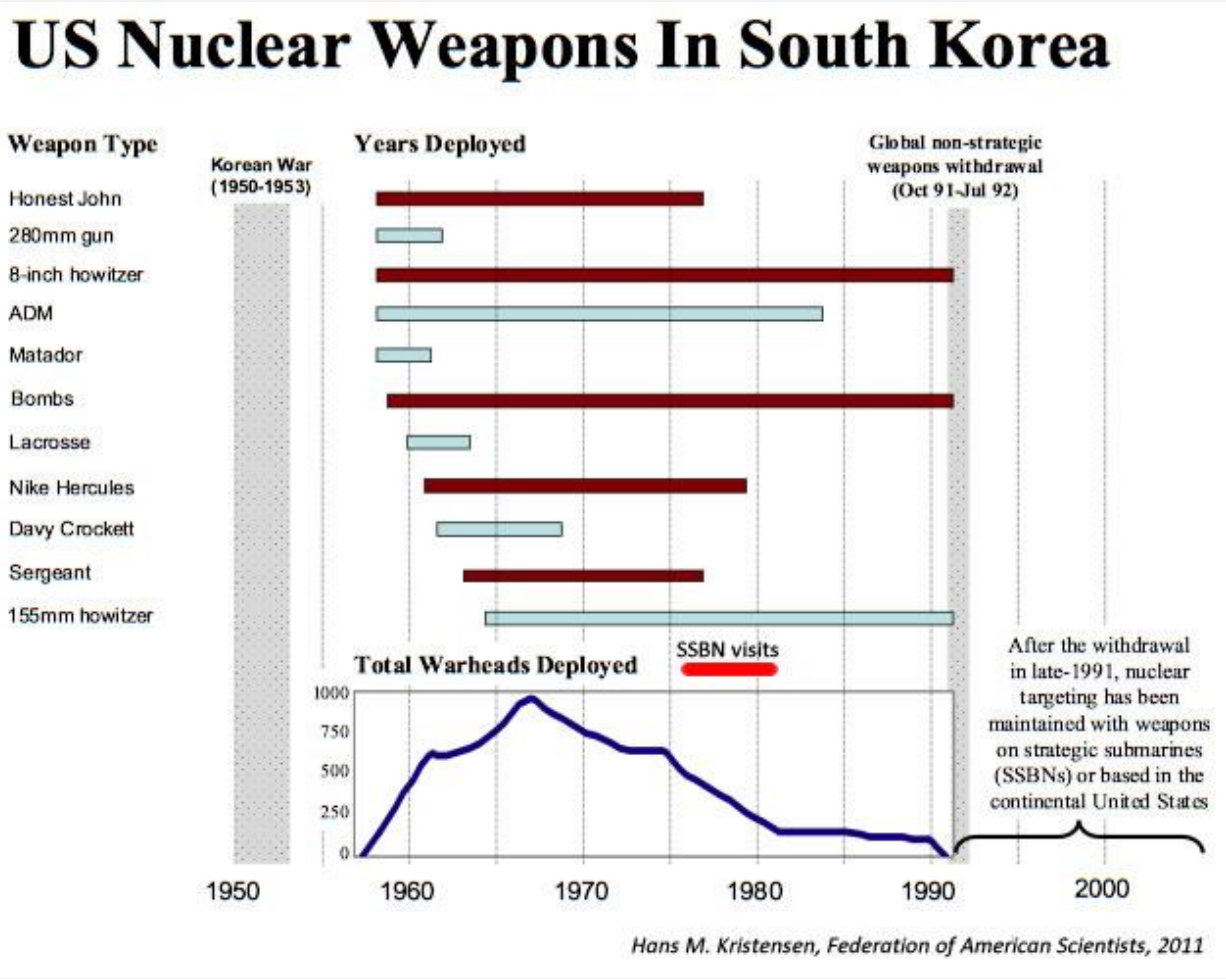
TRUMAN REPEATS STATEMENT TO PRESS

TRUMAN GIVES AIM

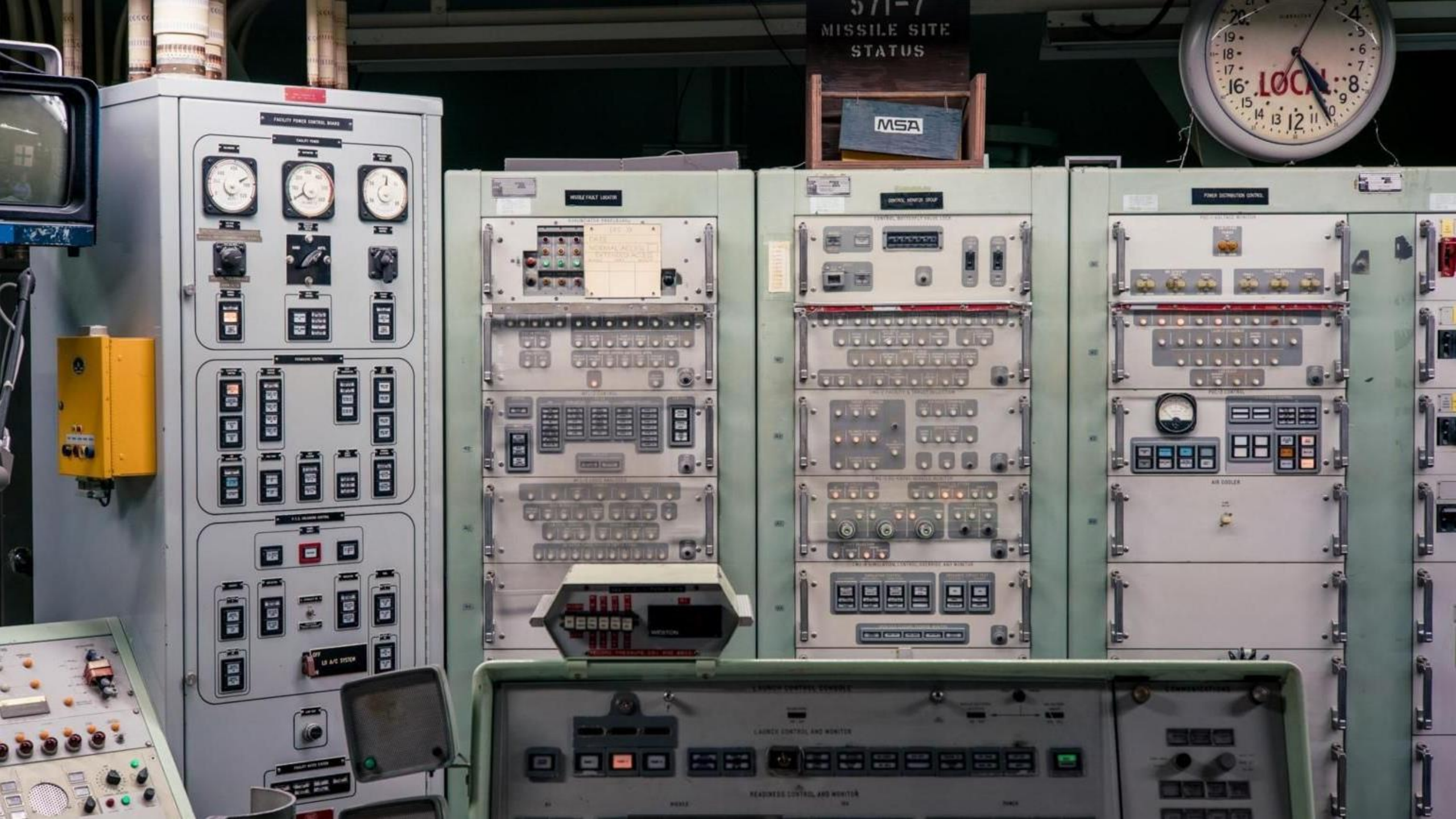
'Just, Peaceful World' Is Goal, --Moscow and Peiping Are Told

BACKS M'ARTHUR, ACHESON

President Says U.N. Action Will Be Pushed and U. S. and Allies Bolstered to Meet Crisis



US Deployment of Nuclear Weapons in 1950s South Korea & North Korea's Nuclear Development- Lee Jae-Bong - 2009
(https://lelephant-larevue.fr/dossiers/les-ambitions-nucleaires-de-la-coree-du-nord/)


MISSILE SITE
STATUS
MSA
LOCAL

1965

“North Korea built its first computer with vacuum tubes in 1965, with engineers trained in France.” – NYT, 2015-01-19

1980 – Création d'un réacteur nucléaire Magnox à Yongbyon
Production du plutonium utilisé dans le 1er essai de 2006

1984 – Création du Mirim College – Automated Warfare Institute
100 diplômés par an en guerre électronique

1990 – Création du Korean Computer Center (KCC)
Centre de R&D en technologie de l'information

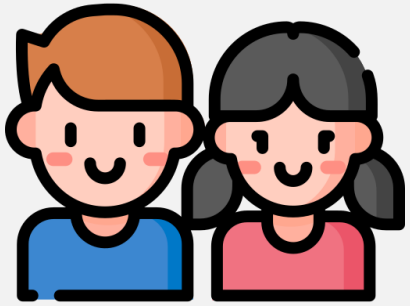
1994 – Formation cyber de 15 Nord Coréen à l'Académie Militaire de Pékin
Ils sont les piliers du nouveau Bureau des renseignements extérieurs

Pirate informatique, un cursus d’élite

Ecole obligatoire, universelle et gratuite entre 5 et 15 ans

Pirate informatique, un cursus d’élite

Maternelle
(1 an)



Primaire
(4 ans)

Collège
(6 ans)

100%

Taux d’alphabétisation à 15 ans
(revendiqué)

Pirate informatique, un cursus d'élite

Primaire

- Être premier de la classe
- Excellence en mathématique
- Excellence en science appliquées

Collège

Keumseong 1 et 2

(6 ans)

- Cursus avancée (maths, code, …)
- Competition : IMO, ICPC

Universités

Kim Chaek | Kim Il Sung

(3 ans)

- Programmation avancée
- 1 an obligatoire en Chine ou en Russie («sécurité offensive avancée»)
- Entre 100 et 2500 recrues par an au GRB (effectif cyber : 1000-7000 personnes)

Source : *North Korea recruits hackers at school*, Aljazeera - 2011

Pendant ce temps en occident

« Axe du mal » (2002) et invasion de l’Irak (2003)

Embargo économique après le premier test nucléaire de 2006

Pirate informatique, un travail de groupes

Bureau 121 (GRB)
Equipe **:** Andariel
Détection : 2009
Ciblage : Rançonnage Corée du Sud

Ministère de la sécurité d'état
Equipe **:** APT37
Détection : 2012
Ciblage : Espionnage industriel

Lab 110 (GRB)
Equipe **:** Kimsucky
Détection : 2012
Ciblage : Espionnage & Vol

Lab 110 (GRB)
Equipe **:** HERMIT
Détection : 2013
Ciblage : Espionnage

Bureau 180 (GRB)
Equipe **:** APT38
Détection : 2014
Ciblage : Vol Banque & Crypto

Bureau 325 (GRB)
Equipe **:** CERIUM
Détection : 2020
Ciblage : Pharmaceutique

Pirate informatique, pas que du piratage

Lab 110 - Bureau 35

Information des leaders

Bureau 39

Blanchiment d’argent

Bureau 91

Capitalisation de l’espionnage

Lab 110 - Bureau 414

Espionnage humain

Bureau 128

Manipulation humaine

Bureau 180

Collecte clandestine de
Moyens financiers

Palmares célèbre

Piratage de Sony, 2014 (vengeance)

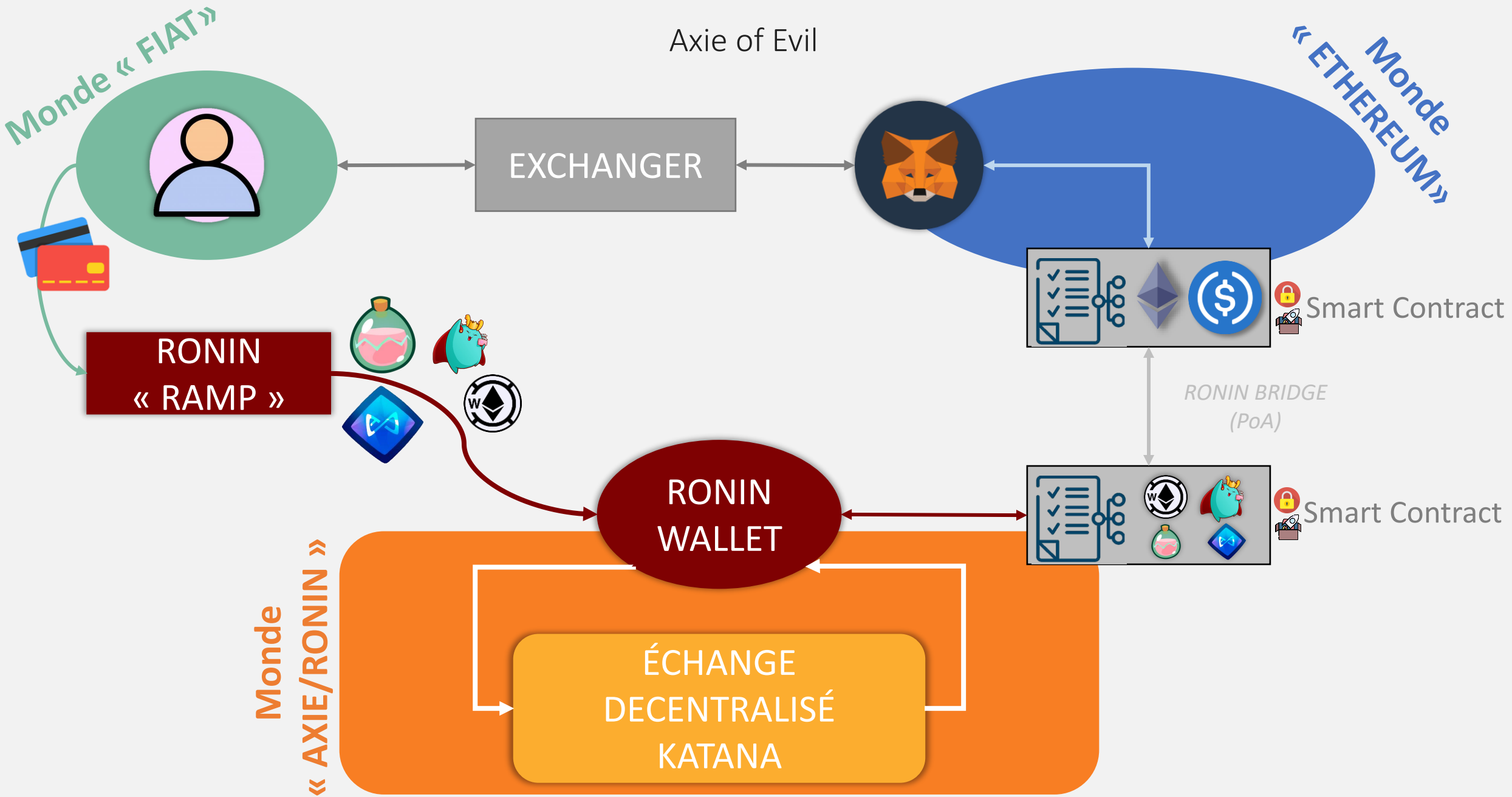
Banque Centrale du Bangladesh, 2016
(vol de 81 millions de dollars)

bithumb

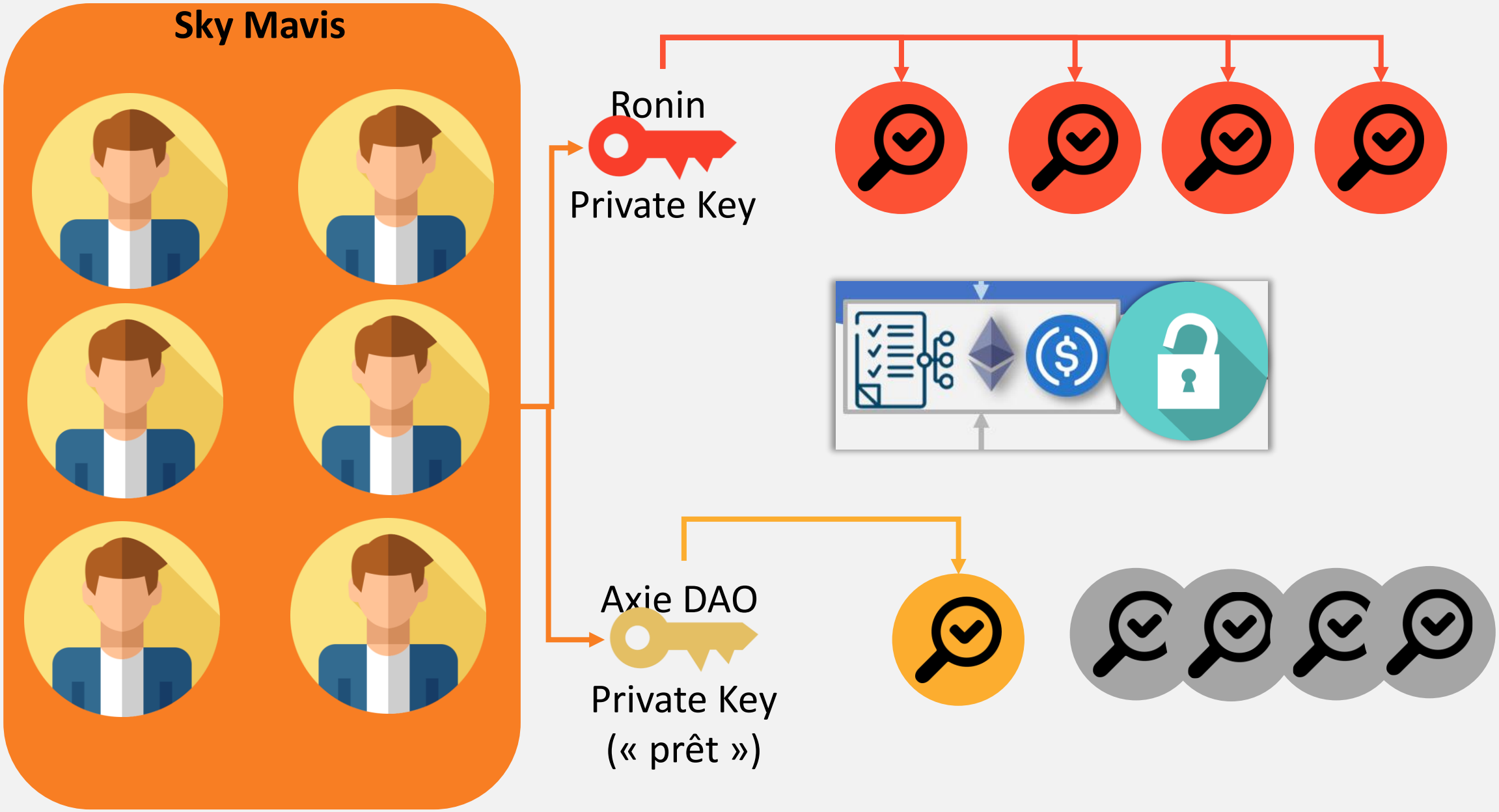
Quatre piratages de Bithumb entre 2017 et 2019
(vol 65 millions équivalent dollars)

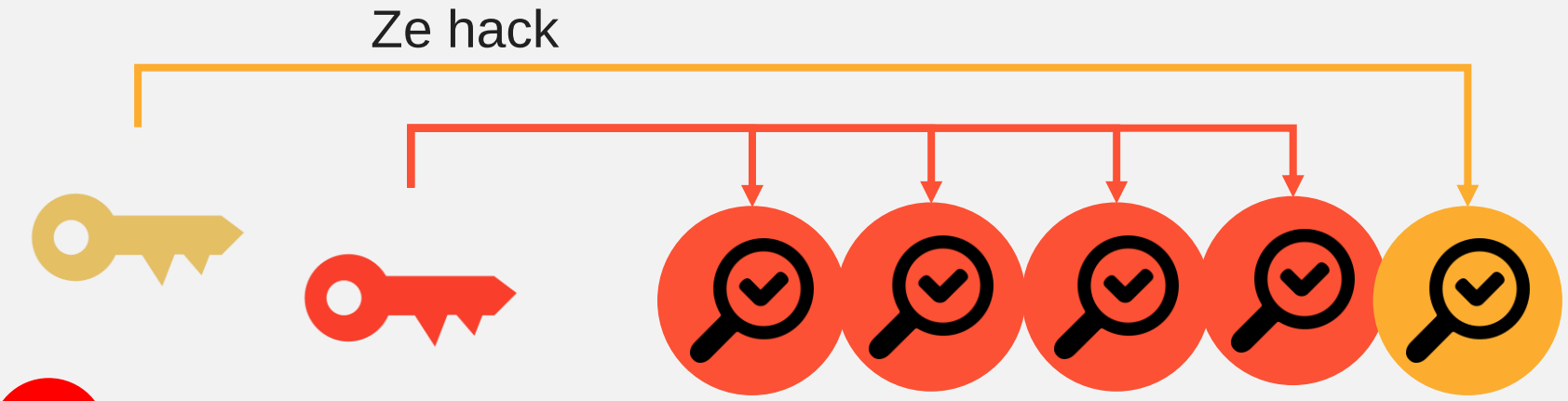
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

Axie of Evil


Monde « FIAT »
EXCHANGER
Monde « ETHEREUM »
Smart Contract
RONIN « RAMP »
RONIN BRIDGE (PoA)
RONIN WALLET
Smart Contract
Monde « AXIE/RONIN »
ÉCHANGE DECENTRALISÉ KATANA

Proof of Evil





2 Saisie des clés

1 Manipulation humaine

(Social engineering)

hihihi

3 Forge d'une transaction

4 Validation malveillante de la transaction

(« 51% attack»)

5 Déblocage des 173 600 ETH et 25,5 millions USDC

En résumé

La technologie blockchain repose sur l’informatique.
Elle est implémentée par et pour des humains.
N’oubliez pas les bonnes pratiques.

Les erreurs de Sky Mavis

1. **Un risque dans la conception connu mais non géré**
   Un faible nombre de nœuds validateurs (9) avec un seuil trop bas (5)

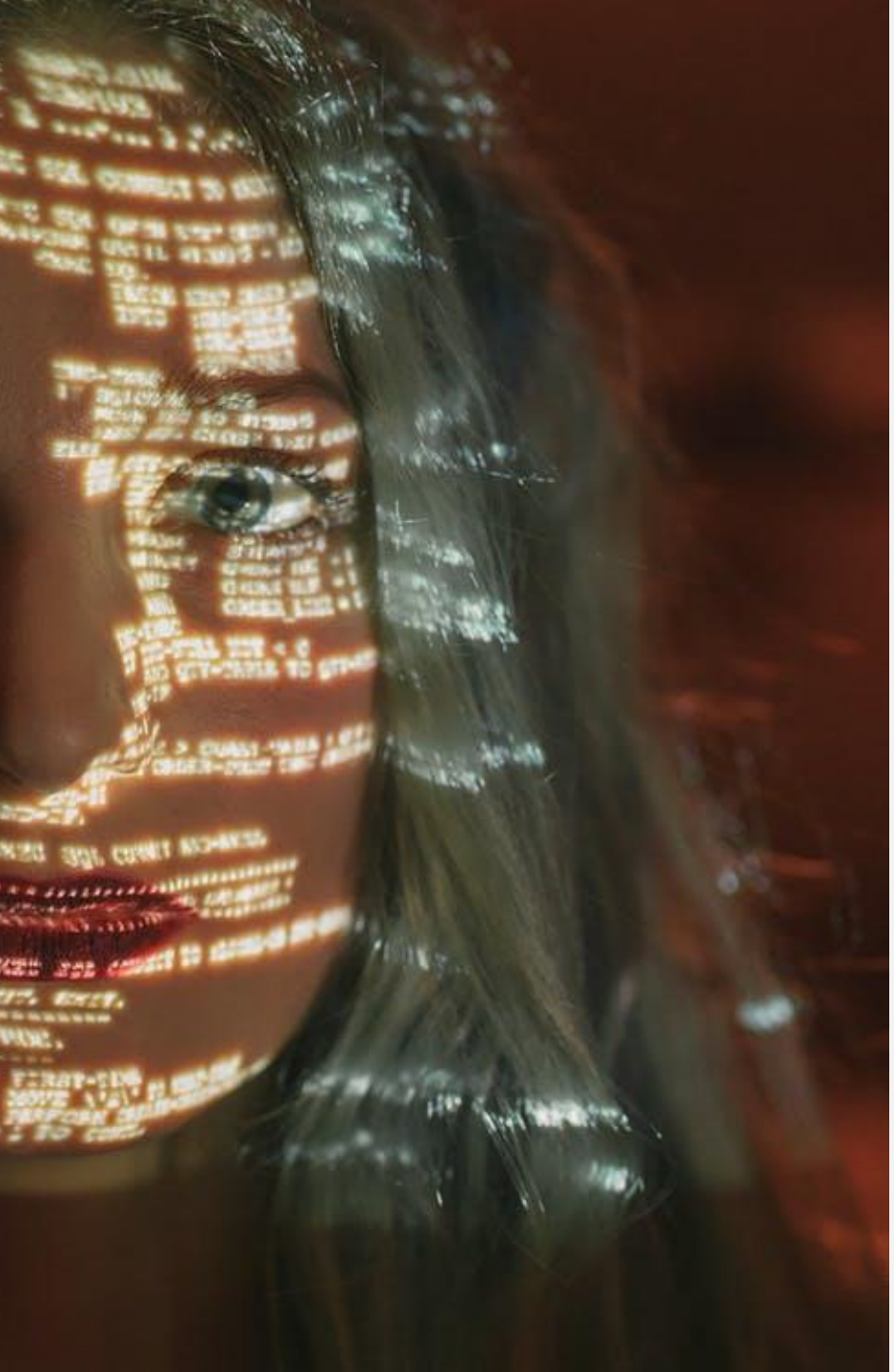
2. **Un raccourci temporaire qui perdure**
   La « backdoor » (Axie DAO) n'a pas été révoquée après usage

3. **Une clé privée accessible sans multi-authentification**
   La procédure de gestion des secrets vitaux est lacunaire

4. **Une sensibilisation des employés trop faible**
   Les informaticiens sont tout aussi manipulables … voire plus

5. **Une surveillance d'actions suspectes absentes**
   Le retrait de tous les fonds est un scénario de risque à considérer

6. **Aucune cartographie des risques de l'écosystème**
   Un écosystème DEFI est ouvert à tout le monde… Tout. Le. Monde.



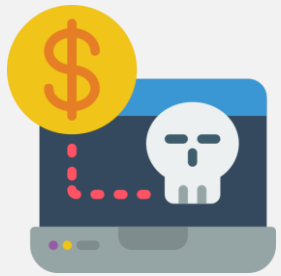
La blockchain repose sur l'informatique

Les « nodes » sont des serveurs qu'il faut patcher

Les « smart contract » sont des logiciels qu'il faut auditer

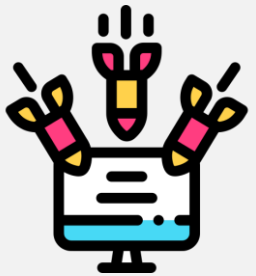
Les acteurs crypto sont des entreprises qu'il faut sécuriser

Malware



Arnaque

Phishing



DDOS

Usurpation

Exploitation

Complicité

Déni

Si ce n’est Kim, cela peut être un autre

DAFOM
Faux portfolio manager

TokenAIS/CryptAIS
Fausse « IA » crypto

AlticGo/Esilet
Faux signal crypto

CreAI Deck
Faux « IA »exchange

Celas Trade Pro

JMT Trading

Union Crypto

Kupay Wallet

CoinGoTrade

Dorusio

Ants2Whale

Quelques pièges tendus aux particuliers par les KimBoyz

Quelques conseils universels

Protéger les terminaux avec des solutions de sécurité à jour, ce sont vos coffres-forts

Méfiez vous des approches alléchantes et protégez vos secrets

Auditez votre code, évaluer votre écosystème et vos parties tierces

Utilisez des logiciels réputés avec des mises à jour de qualité

Bugs ? Hack ? La qualité et la sécurité sont des signes de l'attention portée à l'utilisateur

La blockchain sécurise son périmètre. Sécurisez le votre.


École
d'ingénieurs
ensibs :
Université Bretagne Sud