Dossier Bybit

Le plus gros hack de l'histoire de la finance

Le 21 février 2025, Bybit, une plateforme d'échange de crypto-actifs[1] (plus communément appelées « cryptomonnaies »), a été victime d'un détournement (un hack) sans précédent. Les attaquants ont détourné 1,46 milliard de dollars en crypto-actifs soit près de 2 fois plus que le deuxième plus grand hack sur Ronin Network en mars 2022 avec 624 millions de dollars volés, marquant un tournant dans l'histoire de la sécurité des plateformes d'échanges.

Ce hack est tout simplement la plus grosse opération de détournement de fonds cyber de l'histoire de la finance. Les experts d'Orange Cyberdefense vous proposent de découvrir les tenants et les aboutissants de cette crise d'envergure.

À titre de comparaison avec les piratages via ransomware, la plus importante cyber-rançon connue du grand public versée à des cybercriminels s'élève à 75 millions de dollars. Le hack de Bybit est également plus important que celui orchestré par le groupe de cybercriminels Carbanak ciblant les distributeurs de billets pour détourner entre 500 millions et 1 milliard de dollars dans le monde entre 2013 et 2015.

Cet article revient en détail sur cet événement, les vulnérabilités exploitées, les techniques des attaquants, et les leçons à tirer pour l'industrie.

Voir aussi : Sécurité de la Blockchain : idée reçue ou fait établi ?

[1] Crypto-actifs : actif numérique émis sur une Blockchain

Le contexte de la cyberattaque

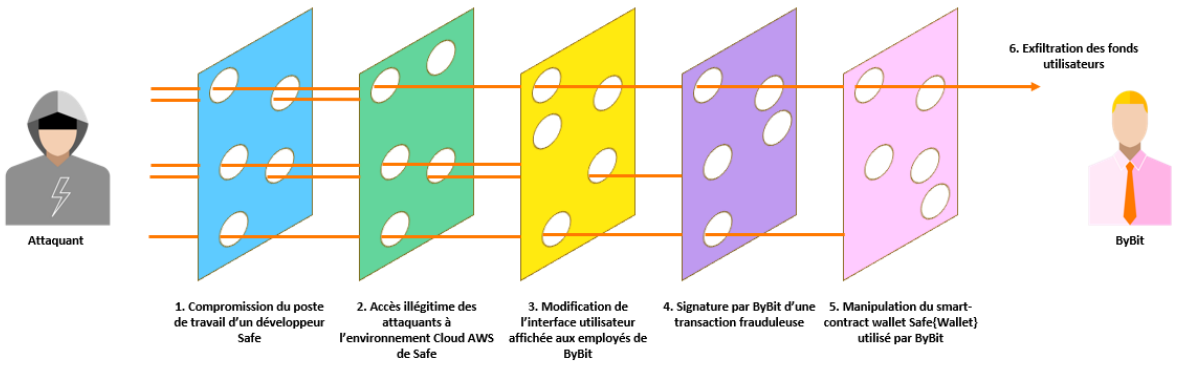
Au moment de la publication de cet article, les premiers rapports post-mortem ont été publiés par Bybit et ses partenaires. Il reste cependant encore des zones d'ombre quant à certains aspects de l'attaque.

Bybit utilise un portefeuille numérique (ou wallet[2]) dit « multisig » (multi-signatures) pour sécuriser ses fonds. Il nécessite plusieurs clés privées détenues par des personnes différentes pour effectuer une transaction[3], ce qui évite qu'une seule personne puisse avoir le contrôle total sur le portefeuille, limitant le risque. Ce wallet multisig est développé et proposé par l'entreprise Safe et est baptisé Safe{Wallet}.

Le 21 février 2025, 3 collaborateurs de Bybit (incluant leur CEO, Ben Zhou) ont signé une transaction qu'ils pensaient de routine. Mais en réalité, ils étaient en train de signer une transaction frauduleuse créée par l'attaquant.
Après l'analyse forensique préliminaire, la thèse d'une attaque ciblant l'infrastructure de Safe{Wallet} est privilégiée.

Les attaquants sont parvenus à compromettre le système d'information de Safe afin de modifier l'interface utilisateur de Safe{Wallet} qui s'affichait pour les signataires de Bybit. Cela leur a permis de réussir leur attaque sans avoir à compromettre les clés privées [4]des utilisateurs directement, alors même que ces derniers utilisaient un « hardware wallet [5]» pour les sécuriser. Il est toutefois important de noter qu'un tel système de gestion des clés privées n'est pas suffisant pour une entreprise disposant d'un si important montant d'actifs sous gestion.

Il s'agirait donc d'une supply-chain attack. Ce type d'attaque consiste à cibler un fournisseur ou un tiers pour compromettre l'organisation cible. Ici, les attaquants ont compromis un tiers de Bybit impliqué dans la fourniture du service sur crypto-actifs afin d'atteindre leur cible finale : le portefeuille de crypto-actifs de Bybit.



Cette attaque témoigne de l'urgence de la convergence entre la sécurité du Web3[6] et la sécurité dite « traditionnelle ». Car les attaquants n'utilisent plus uniquement des méthodes d'attaques propres au secteur, et parce que la typologie d'attaquants entre ces deux mondes tend à converger.

Si cette attaque semble sophistiquée, elle a en réalité vraisemblablement démarré par une « simple » ingénierie sociale ciblant les employés de Safe, permettant la compromission de l'environnement cloud AWS de l'entreprise. C'est l'enchaînement d'étapes par l'attaquant qui rend cette attaque complexe.

[2] Wallet / portefeuille numérique : outil (généralement une application ou une extension sur navigateur) permettant de stocker, envoyer et recevoir des crypto-actifs.

[3] Transaction : opération enregistrée sur une blockchain, comme un transfert de fonds, de données, ou l'exécution d'un smart-contract.

[4] Clé privée : « Code secret » permettant d'accéder et de gérer un wallet. Suite de caractères confidentielle représentant la propriété d'un wallet.

[5] Hardware wallet : dispositif physique sécurisé pour stocker des clés privées hors ligne.

[6] Web3 : nouvelle génération d'internet décentralisé basé sur la blockchain.

Étapes de l'attaque

1. Le PC d'un développeur de l'entreprise Safe a été compromis. Un malware y a vraisemblablement été introduit.

2. L'attaquant a utilisé ses accès à la machine du développeur pour récupérer un accès au tenant AWS de Safe (via l'utilisation d'un identifiant compromis ou d'une clé API),

3. Cela a permis à l'attaquant d'accéder au bucket S3 d'AWS, contenant le code de l'interface utilisateur de Safe{Wallet}. Il a ainsi pu y injecter du code malveillant (payload JS) le 19 février 2025 à 15:29:25 UTC. Ce payload permettait de manipuler l'interface utilisateur, pour faire croire à la victime qu'il signait une transaction légitime, alors qu'il s'agissait en réalité d'une transaction frauduleuse.

4. Ce code malveillant a été déployé un peu de moins de 48h avant que l'équipe de Bybit n'interagisse avec leur wallet multisig pour une opération de routine, le 21 février 2025 à 14:13:35 UTC. En exécutant cette transaction, Bybit a permis aux attaquants d'accéder aux fonds de l'entreprise.

5. Moins de 2 minutes plus tard, à 14:15:11 UTC, l'attaquant a exfiltré plus d'1,4 milliard de dollars en ETH.

6. Au même moment, ils ont restauré l'ancienne version de l'interface utilisateur pour effacer leurs traces sur le tenant AWS de Safe.

Nous analyserons dans la suite de cet article le mode opératoire détaillé de l'attaquant et les mesures de sécurité qui auraient permis d'éviter cette attaque.

La plus grosse cyberattaque de l'histoire du secteur

Chaque année, plusieurs milliards de dollars de crypto-actifs sont dérobés lors de piratages. Jusqu'alors, le principal vecteur d'attaque employé par les attaquants était l'exploitation de vulnérabilités présentes dans le code des smart-contracts[7].
Mais ces dernières années nous constatons une évolution dans les méthodes d'attaque du secteur : au fur et à mesure que le niveau de sécurité des smart-contracts s'améliore, les attaquants se tournent vers un autre vecteur d'attaque, en compromettant les clés privées ou les portefeuilles des entreprises et des utilisateurs, quitte à user de l'ingénierie sociale.

C'est ce qu'il s'est passé pour Bybit, ayant permis aux attaquants de dérober plus de 500.000 ETH (incluant des ETH natifs [8]et des LST[9]), soit plus de 1,4 milliards de dollars au moment de l'attaque. Cette attaque dépasse très largement le précédent plus important hack du secteur : celui ayant visé le réseau Ronin Network en mars 2022 et ayant coûté plus de 600 millions de dollars au moment de l'attaque.

Avec plus de 2,2 milliards de dollars volés en 2024, les crypto-actifs sont une cible de choix pour les cybercriminels, malgré la forte traçabilité qu'implique la technologie de la Blockchain, rendant difficile l'utilisation des fonds volés.
Le poids du cybercrime on-chain[10] (c'est-à-dire « sur la Blockchain ») reste cependant à relativiser face coût du cybercrime dans le monde estimé à 10.000 milliards de dollars en 2025.

[7] Smart-contract : programme exécuté sur une blockchain.

[8] ETH natifs : Ether, l'actif natif de la blockchain Ethereum.

[9] LST : Liquid Staking Tokens, jetons représentant des ETH stakés.

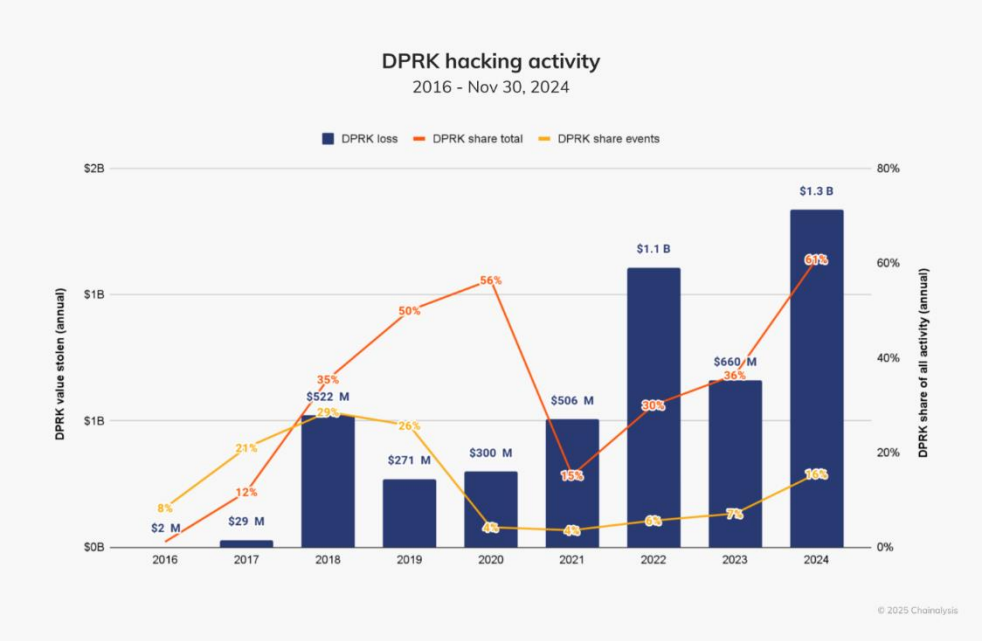
[10] On-chain : enregistré directement sur une blockchain.

Une attaque orchestrée par la Corée du Nord

Après l'attaque, les regards se sont rapidement tournés vers Lazarus, le groupe de hackers affilié à la Corée du Nord, et plus précisément à un sous-groupe nommé TraderTraitor. Certains des portefeuilles utilisés par les attaquants avaient en effet déjà été rattachés à ce groupe.

Ces derniers sont particulièrement actifs dans les hacks impliquant des vols de crypto-actifs. Lazarus était déjà actif dans le vol de monnaies fiduciaires[11], avec pour objectif principal de contourner les restrictions mises en place à leur encontre pour leur limiter l'accès au dollar et aux autres devises.

Et pour cause, Chainalysis estime à 1.3 milliards de dollars les fonds volés par des groupes affiliés à la Corée du Nord en 2024 dans l'écosystème crypto-actifs, soit plus de 60% des fonds volés sur la période.



Source : $2.2 Billion Stolen in Crypto in 2024 but Hacked Volumes Stagnate

Avec ce seul hack de Bybit, Lazarus vient donc de dépasser leurs « performances » de l'année 2024.

Lazarus n'en est cependant pas à son coup d'essai. Nos analystes ont en effet lié le groupe de cybercriminels aux activités de ransomware depuis 2017, avec WannaCry[12].

Lors de leurs campagnes ciblant le secteur des crypto-actifs, Lazarus commence généralement ses attaques par une phase d'ingénierie sociale. Ils utilisent par exemple de faux profils de recruteurs sur LinkedIn ou l'envoi d'emails pour approcher les entreprises cibles avec une pièce jointe contenant un malware, exploitant le manque de sécurité opérationnelle des entreprises du secteur.
Cela leur permet ensuite de s'introduire sur le système d'information de l'entreprise.

Depuis 2024, une autre méthode en plein essor consiste à infiltrer un employé, en réalité un hacker affilié à la Corée du Nord, directement au sein de l'entreprise cible. Sous couverture, il mène l'attaque de l'intérieur, contournant ainsi les protections périmétriques.

La méthode précise d'ingénierie sociale utilisée lors de l'attaque contre Bybit, visant un développeur de l'entreprise Safe, reste inconnue à l'heure de la rédaction de cet article.

[11] Monnaie fiduciaire : monnaie traditionnelle émise par une autorité reconnue, comme l'euro ou le dollar.

[12] WannaCry : ransomware ayant causé une cyberattaque mondiale en 2017.

L’analyse on-chain des transactions a également permis de relier les portefeuilles utilisés par Lazarus à plusieurs autres attaques récentes sur lesquelles le groupe était également suspecté :
- Hack contre Poloniex[13], 120 millions de dollars dérobés le 10 novembre 2023 ;
- Hack contre BingX[14], 43 millions de dollars dérobés le 20 septembre 2024 ;
- Hack contre Phemex[15], 73 millions de dollars dérobés le 23 janvier 2025 ;

Pire encore, des groupes affiliés à la Corée du Nord sont suspectés d’avoir réalisé deux autres attaques récentes ciblant également les wallets multisig Safe{Wallet} d’entreprises :
- Hack contre WazirX[16], 234 millions de dollars dérobés le 18 juillet 2024 ;
- Hack contre Radiant Capital[17], 50 millions de dollars 16 octobre 2024 ;

Les fonds volés lors de ces piratages sont ensuite, entre autres, utilisés pour financer le programme d’armement nord-coréen. Près de la moitié des fonds servant à financer ce programme proviennent en effet d’activités cybercriminelles.

Pour autant, malgré leurs compétences et leur détermination, le groupe Lazarus éprouve des difficultés à blanchir l'intégralité des fonds volés, limitant ainsi leur capacité à contourner les sanctions internationales.

[13] Poloniex : plateforme d'échange de crypto-actifs.

[14] BingX : plateforme d'échange de crypto-actifs.

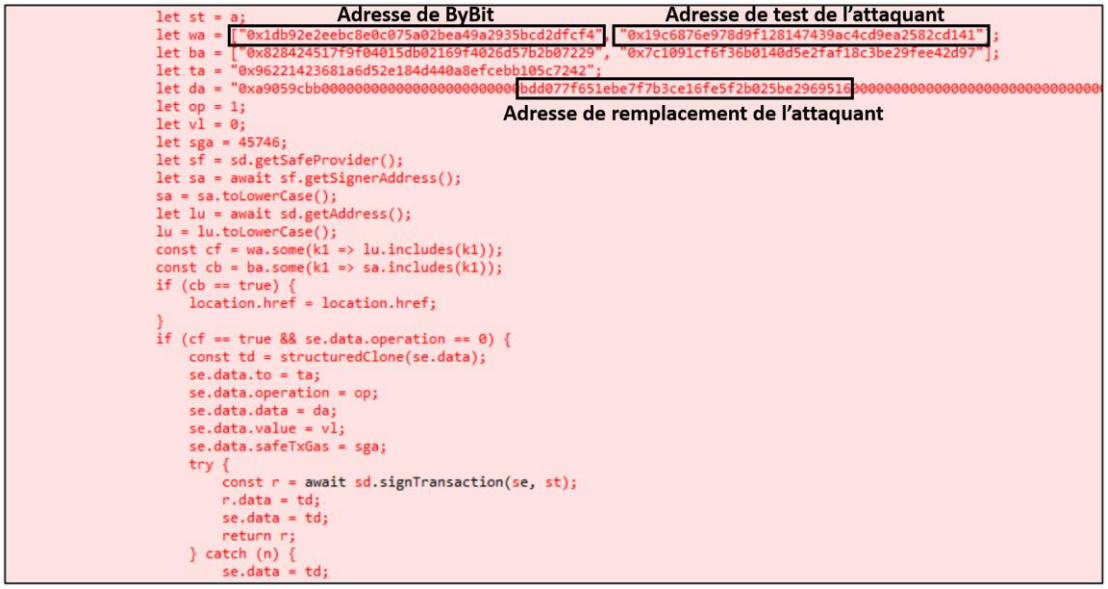
[15] Phemex : plateforme d'échange de crypto-actifs.

[16] WazirX : plateforme d'échange de crypto-actifs.

[17] Radiant Capital : protocole de finance décentralisée.

Analyse technique de l'attaque contre Safe et Bybit

L'analyse forensique a révélé que le payload JS utilisé par l'attaquant est le suivant :



Ce payload nous révèle que Bybit a été directement ciblé par cette attaque : le script permettant de manipuler l'interface ne pouvait se déclencher que lorsque l'adresse de Bybit (l'adresse cf4) était impliquée. Ce script fonctionne également pour une seconde adresse (l'adresse 141), qui s'avère être, après analyse on-chain, une adresse de test utilisée par l'attaquant pour tester leur script quelques jours avant l'attaque.

Ainsi, le 21/02/2025, lorsque les signataires de Bybit ont tenté d'interagir avec l'adresse cf4, le script s'est déclenché, démarrant l'attaque.

L'attaque s'est produite dans la transaction suivante :
0xb61413c495fdad6114a7aa863a00b2e3c28945979a10885b12b30316ea9f072c

6 transactions constituent cette attaque.

	Transaction Hash		Method	Block	Age	From		To
	0x847b8403e8...	F	Sweep ERC20	21895251	3 days ago	ByBit Exploiter	IN	Bybit: Cold Wallet 1
	0xa284a1bc4c...	E	Sweep ERC20	21895251	3 days ago	ByBit Exploiter	IN	Bybit: Cold Wallet 1
	0xbcf316f5835...	D	Sweep ERC20	21895251	3 days ago	ByBit Exploiter	IN	Bybit: Cold Wallet 1
	0xb61413c495f...	C	Sweep ETH	21895251	3 days ago	ByBit Exploiter	IN	Bybit: Cold Wallet 1
	0x25800d105d...	B	Sweep ERC20	21895246	3 days ago	ByBit Exploiter	IN	Bybit: Cold Wallet 1
	0x46deef0f52e...	A	Exec Transact...	21895238	3 days ago	ByBit Exploiter	IN	Bybit: Cold Wallet 1

Transaction A : multisig compromis – les 3 signataires signent la transaction frauduleuse sur l'interface modifiée par l'attaquant

Transaction B : transaction de test réalisée par l'attaquant réalisée moins de 2min après la signature – l'attaquant a transféré 90$ (en USDT) depuis le wallet de Bybit pour s'assurer que le hack avait fonctionné.

Transaction C à F : transfert des ETH, mETH, stETH, cmETH vers le wallet de l'attaquant.

Etudions la transaction A, celle qui a permis le déclenchement de l'attaque.

La transaction A appelle la méthode « Exec Transaction » de Safe{Wallet}. Il s'agit d'une méthode standard de Safe{Wallet} qui prend les paramètres suivants :

Input Data:

#	Name	Type	Data
0	to	address	0x96221423681A6d52E184D440a8eFCEbB105C7242
1	value	uint256	0
2	data	bytes	0xa9059cbb000000000000000000000000bdd077f651ebe7f7b3ce16fe5f2b025be2969516000000000000000000000000000000000000000000000000000000000000
3	operation	uint8	1
4	safeTxGas	uint256	45746

Dans le cas de cette transaction :

- Le champ « to » est celle d'un smart-contract déployé par l'attaquant ;
- Le champ « data » contient également l'adresse d'un smart-contract déployé par l'attaquant ;
- Le champ « operation » est à '1' ;

En lisant le code du smart-contract Safe{Wallet}, on constate que le champ « operation » fait référence au type d'opération souhaitée par l'utilisateur : à '0', il s'agit d'un simple « call » alors qu'à '1', les actions sont déléguées à un tiers, ici le smart-contract renseigné dans le champ « data ».

```
64
65  /// @title Enum - Collection of enums
66  /// @author Richard Meissner - <richard@gnosis.pm>
67  contract Enum {
68      enum Operation {
69          Call,        // 0
70          DelegateCall // 1
71      }
72  }
```

```
function execute(address to, uint256 value, bytes memory data, Enum.Operation operation, uint256 txGas)
    internal
    returns (bool success)
{
    if (operation == Enum.Operation.Call)
        success = executeCall(to, value, data, txGas);
    else if (operation == Enum.Operation.DelegateCall)
        success = executeDelegateCall(to, data, txGas);
    else
        success = false;
}

function executeCall(address to, uint256 value, bytes memory data, uint256 txGas)
    internal
    returns (bool success)
{
    // solium-disable-next-line security/no-inline-assembly
    assembly {
        success := call(txGas, to, value, add(data, 0x20), mload(data), 0, 0)
    }
}

function executeDelegateCall(address to, bytes memory data, uint256 txGas)
    internal
    returns (bool success)
{
    // solium-disable-next-line security/no-inline-assembly
    assembly {
        success := delegatecall(txGas, to, add(data, 0x20), mload(data), 0, 0)
    }
}
```

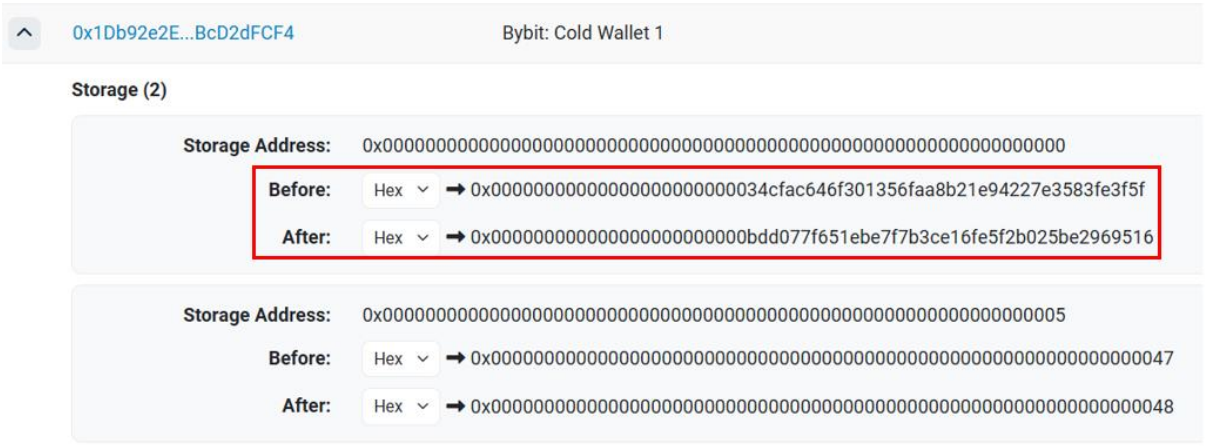
En bref, cette transaction, signée par les 3 signataires du multisig Bybit, a permis d'exécuter les fonctions présentes dans le smart-contract de l'attaquant.

Le smart-contract exécuté en question (celui-ci) contient une simple fonction permettant de modifier l'implémentation du smart-contract Safe{Wallet} de Bybit, le contrat légitime 0x34cfac646f301356faa8b21e94227e3583fe3f5f, vers le contrat pirate 0xbDd077f651EBe7f7b3cE16fe5F2b025BE2969516.

Concrètement, si les 3 signataires avaient désactivé le « blind signing[18]» sur leur hardware wallet et vérifié l'adresse de destination, ils auraient vu s'afficher l'adresse 0xbDd077f651EBe7f7b3cE16fe5F2b025BE2969516 à l'écran de leur hardware wallet, au lieu de l'adresse légitime 0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4.

Ils auraient aussi remarqué qu'ils signaient un « DelegateCall » au lieu d'un simple « Call », ce qui aurait permis d'éviter cette attaque.

On constate l'effet de cette transaction en étudiant le « storage » du smart-contract proxy[19] de Bybit :



Ainsi, la transaction a mis à jour l'implémentation du smart-contract vers celui de l'attaquant, permettant à celui-ci de récupérer l'accès aux fonds de Bybit et de les exfiltrer.

Notons enfin qu'il est possible de remonter les adresses de Lazarus jusqu'à plusieurs wallets provisionnés par des comptes sur la plateforme d'échange Binance. C'est notamment le cas pour l'adresse 9e3, liée à l'adresse 141 ayant servi à tester le script de l'attaquant avant l'attaque du 21/02.

Binance imposant la vérification d'identité à ses utilisateurs, il est alors possible de retrouver l'identité de la personne derrière l'attaque.

Cette affirmation est cependant à nuancer : les attaquants ont vraisemblablement utilisé une fausse identité ou un compte Binance volé pour provisionner ces wallets.

Suivi des fonds volés par Lazarus

L'une des principales caractéristiques de la Blockchain est sa transparence, permettant une traçabilité absolue des transactions.

Cela permet de suivre les fonds volés par Lazarus en temps réel. Pour brouiller la traçabilité, l'attaquant effectue de nombreuses transactions et disperse les fonds sur plusieurs wallets, rendant le suivi des mouvements beaucoup plus complexe pour les analystes.

La méthodologie de Lazarus est sensiblement similaire pour chacun de leurs hacks.

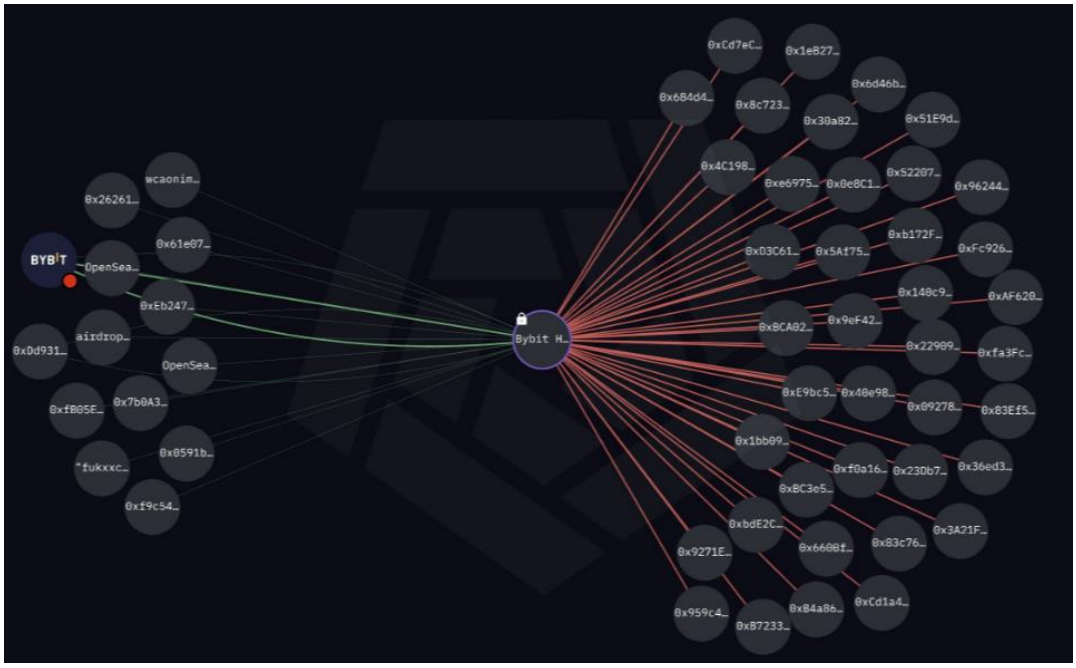
Étape 1 : premiers déplacements de fonds

[18] Blind Signing : Processus de signature d'une transaction sans en vérifier les détails, augmentant le risque de signer des transactions malveillantes. Il s'agit généralement d'une fonctionnalité à activer manuellement sur les portefeuilles des utilisateurs, qui simplifie l'expérience utilisateur au détriment de la sécurité.

[19] Proxy contract : smart-contract agissant comme intermédiaire pour exécuter des fonctions d'un autre contrat.

Dans les 30 minutes qui ont suivies l'attaque réussie, les attaquants ont commencé à déplacer les fonds volés sur d'autres wallets. Leur objectif : tenter de faire disparaître ces fonds.

Ils les ont alors déplacé vers plus de 50 wallets, avec 10.000 ETH par wallet.



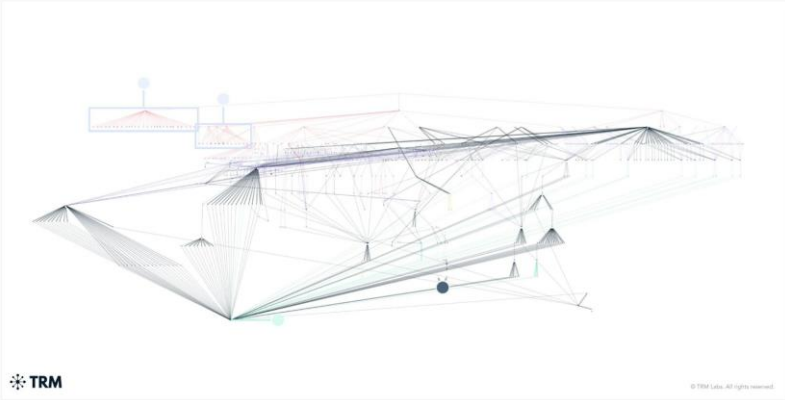
Source : Arkham

Étape 2 : des milliers de transactions

Chacun de ces 50+ wallets va à son tour réaliser des milliers de transactions vers des dizaines d'autres wallets afin de réduire encore davantage la taille de chaque portefeuille et de tenter de brouiller les pistes.

Pour complexifier encore davantage la tâche des autorités et multiplier les chances de faire disparaître les fonds, ils sont également déplacés (« bridgés ») vers d'autres blockchains, notamment sur la blockchain Bitcoin, bien qu'elle soit tout aussi traçable que la blockchain Ethereum.

Après seulement quelques jours, des milliers d'adresses sont utilisées par Lazarus pour brouiller les pistes.



Source : The Bybit Hack: Following North Korea's Largest Exploit | TRM Insights

Nous constatons d'ailleurs sur l'illustration précédente une convergence des fonds vers un nombre limité de points, notamment des plateformes de mixage de fonds et des bridges vers d'autres chaînes.

Ces adresses frauduleuses sont désormais blacklistées par de nombreux services Web3 et ajoutées au Datalake Orange Cyberdefense pour prévenir de futures menaces.

Mais s'agissant du hack le plus important de l'histoire de la finance, chaque transaction est analysée, et chaque nouveau wallet identifié est référencé par la communauté Web3. Cela permet de blacklister les wallets concernés et, quand cela est possible, de geler les fonds. Plusieurs dizaines de millions de dollars ont déjà été récupérés dans les jours suivant l'attaque.

Étape 3 : mixeurs et blanchiment

L'étape suivante dans le mode opératoire habituel de Lazarus est l'utilisation de « mixeurs » centralisés ou décentralisés pour tenter d'anonymiser les fonds. Ces outils vont « mélanger » les crypto-actifs de plusieurs sources et les envoyer vers plusieurs destinations pour tenter d'en dissimuler l'origine.

Bien que cette étape ait déjà commencé pour le hack de Bybit, il est vraisemblable qu'elle prenne des mois, voire des années, avant d'être finalisée, car la liquidité y est limitée et parce que des mouvements trop importants leur seraient contre-productifs. L'ensemble des fonds dérobés par Lazarus en 2024 n'ont en effet pas encore tous été exfiltrés vers la Corée du Nord.

La gestion de crise de Bybit

Malgré des marges d'amélioration en matière de sécurité organisationnelle, Bybit a démontré résilience et efficacité dans sa gestion de crise.

Sa réponse rapide, transparente et coordonnée a permis de limiter les impacts financiers et de préserver la confiance des utilisateurs.

Une communication immédiate et transparente

Le PDG de Bybit, Ben Zhou, s'est exprimé publiquement dans les 30 minutes suivant la découverte du hack. Cette réactivité a permis d'informer utilisateurs et partenaires en temps réel, évitant rumeurs et panique. Des points de suivi réguliers ont ensuite apporté des mises à jour claires et répondu aux préoccupations des utilisateurs.

Continuité d'activité

Bybit a décidé de maintenir les retraits utilisateurs ouverts malgré l'attaque, contrairement à la pratique courante de suspension temporaire lors de tels incidents.

Bien que risquée, cette décision a permis d'éviter une panique généralisée et un "bank run[20]" prolongé. Les réserves de Bybit se sont stabilisées en deux jours, les retraits se sont normalisés, et l'expérience utilisateur est revenue à la normale par la suite, validant ainsi la pertinence de cette décision à court et long terme.

Collaboration avec les partenaires

Bybit a mobilisé ses partenaires et concurrents pour gérer la crise, renforçant sa crédibilité et illustrant la solidarité de l'industrie. Un effort communautaire significatif a également été déployé pour tracer, geler ou récupérer les fonds.

Un programme de bounty[21] de plus de 100 millions de dollars a par ailleurs été lancé pour soutenir cet effort collectif et limiter le blanchiment des fonds par Lazarus.

Réassurance sur leur résilience financière

Pour rassurer ses utilisateurs, Bybit a rapidement été transparent sur l'état de ses réserves en crypto-actifs, mis en avant son ratio de réserves 1:1 et sa preuve de réserves, assurant la sécurité des fonds clients. L'entreprise a également obtenu un prêt relais pour couvrir les pertes et maintenir les retraits sans interruption. En 12 heures, les réserves d'ETH ont été refinancées, préservant la confiance des utilisateurs.

[20] Bank Run : retraits massifs de fonds par les utilisateurs d'une plateforme, souvent en période de crise.

[21] Bounty : récompense offerte pour identifier et signaler des vulnérabilités de sécurité, ou pour aider à récupérer les fonds volés

Grâce à une gestion rapide, transparente et bien planifiée, Bybit a montré qu'une crise, même majeure, peut être efficacement maîtrisée.

"Not your keys, not your coins" ?

Ce principe largement poussé dans l'écosystème web3 fait référence aux risques liés à la centralisation : si vous ne possédez pas la clé privée, les crypto-actifs ne vous appartiennent pas. C'est ce principe qui guide des millions d'utilisateurs de crypto-actifs dans le monde à opter pour des solutions d'auto-conservation (ou « self-custody[22] »).

Il est vrai que cette attaque a été rendue possible parce qu'une partie des fonds des utilisateurs de Bybit étaient stockés sur un seul wallet appartenant à l'entreprise.

Cette affirmation est cependant à nuancer : Safe{Wallet} est très largement utilisé dans l'écosystème web3 et supporte également des activités de self-custody, que ce soit directement (par exemple en sécurisant les wallets de certains utilisateurs ou les trésoreries d'organisations décentralisées) ou indirectement (en portant l'ownership[23] de smart-contracts de la finance décentralisée[24]).

Une attaque ciblant un tel wallet multisig pourrait donc aussi cibler des protocoles décentralisés, des DAO[25], ou même des layers-2 si les bonnes pratiques de sécurité ne sont pas respectées.

C'est justement ce qu'il s'est passé en octobre 2024, lorsque le wallet multisig de Radiant Capital, un protocole de la finance décentralisée, a été compromis, permettant aux attaquants de drainer leurs smart-contracts et voler les fonds utilisateurs.

Et le terrain de jeu est suffisamment grand pour les attaquants : Safe{Wallet} sécurise aujourd'hui plus de 100 milliards de dollars dans l'écosystème.

Comment la cyberattaque aurait-elle pu être évitée ?

La principale erreur de Safe et de Bybit est également commise par de nombreuses autres organisations du secteur : ne pas penser à la cybersécurité à 360°.

Alors que la sécurité du web3 se concentre aujourd'hui, à tort, principalement sur celle des smart-contracts, ce hack nous rappelle qu'il y a de nombreuses autres considérations à avoir :

- Structurer sa sécurité, adopter une approche par les risques pour identifier et réduire les risques les plus importants comme celui-ci ;
- Contrôler la sécurité de ses tiers TIC[26] ;
- Protéger les utilisateurs contre les menaces liées aux usages d'internet et aux accès distants ;
- Sécuriser ses postes de travail ;
- Sécuriser ses environnements Cloud ;
- Sécuriser les interfaces web ;
- Mettre en place l'authentification multi-facteurs ;
- Détecter proactivement les fuites de données et d'identifiants susceptibles d'être utilisées par un attaquant ;

[22] Self-custody : gestion personnelle des clés privées et des crypto-actifs, sans intermédiaire (en opposition à la gestion via une plateforme d'échange ou de trading).

[23] Ownership : propriété ou contrôle d'un actif ou d'un smart-contract sur une blockchain.

[24] Finance décentralisée : écosystème financier basé sur des protocoles blockchain sans intermédiaires centralisés.

[25] DAO : « decentralized autonomous organization ». Il s'agit d'une organisation décentralisée, assurant généralement la gouvernance des protocoles de la finance décentralisée.

[26] Tiers TIC : Tiers fournissant un produit ou un service lié aux technologies d'information et de communication

- Sensibiliser les collaborateurs à la sécurité et aux gestes importants ;
- S'assurer de la désactivation du blind signing et vérifier la cohérence des données affichées sur son hardware wallet ;
- Renforcer la sécurité des crypto-actifs en mettant en place des processus et des solutions techniques adaptées : flux d'approbation, whitelisting, HSM, MPC, utilisation de sa propre interface, solutions « off-exchange », scripts de vérification, … ;
- Réaliser une veille en vulnérabilités pour être proactif face aux menaces émergentes du secteur ;
- Souscrire à une assurance cyber ;
- Se préparer à la crise pour ne pas la subir, et réagir efficacement ;

Comment les réglementations MiCA et DORA nous protègent

L'entrée en vigueur de MiCA et DORA marque un tournant majeur pour la régulation des crypto-actifs au sein de l'Union Européenne. MiCA encadre les plateformes en imposant transparence et protection des investisseurs, tandis que DORA renforce la cybersécurité et la résilience opérationnelle des acteurs financiers, y compris leurs prestataires.

Lire aussi : Blockchain & actifs numériques : MiCA, la sécurité comme prérequis

Ces deux cadres réglementaires que sont MiCA et DORA mettent en avant l'approche par les risques, qui consiste à identifier les menaces *(par exemple, celle liée à l'utilisation d'une interface utilisateur tierce pour un service critique comme la réalisation de transfert de fonds clients)* afin de les réduire. C'est le **premier pilier de DORA**.

Mais DORA ne s'arrête pas là : le règlement européen impose l'identification et la classification des tiers TIC. L'objectif du règlement est de mettre en place des mesures de sécurité proportionnées au sein des tiers TIC critiques pour assurer la résilience des entités financières utilisatrices.

Le cadre réglementaire ne se limite pas aux obligations déclaratives : DORA impose aux prestataires de services sur crypto-actifs et à leurs fournisseurs des mesures strictes pour prévenir les risques cyber. C'est le **troisième pilier de DORA**.
DORA répond ainsi notamment à la montée en puissance de la menace étatique, dont l'attaque supply-chain est un mode opératoire fréquent, particulièrement dans le monde de la finance.

Lire aussi : Over 50% of UK Financial Firms Hit by Supply Chain Attacks in 2024

Enfin, le **cinquième pilier de DORA** prévoit un partage d'informations entre les entités financières, afin de pouvoir réagir au mieux face à une menace systémique ou face à un nouveau mode opératoire des attaquants. Cela permet d'améliorer la capacité de réaction face à des scénarios comme celui ayant visé Bybit.

Notons également que Bybit a été placé sur la liste noire de l'Autorité des Marchés Financiers (AMF) de mai 2022 à février 2024 pour non-conformité aux règles du régime PSAN. Ils ont finalement retiré de cette liste le 14 février 2025, une semaine avant l'attaque. Le régime PSAN aurait ainsi permis de limiter l'exposition des utilisateurs français à une éventuelle défaillance de Bybit.
Le régime « renforcé » de PSAN (loi PACTE) avait d'ailleurs été introduit à la suite de la défaillance de la plateforme d'échange FTX en novembre 2022 pour renforcer les exigences de sécurité envers les prestataires de services sur actifs numériques.

Conclusion

Le piratage de Bybit illustre une tendance inquiétante : un nombre d'attaques en constante augmentation dans le web3, où la menace principale devient des groupes de cybercriminels financés par des états.

Menées par des groupes comme Lazarus, ces attaques exposent la fragilité du secteur face à des adversaires bien plus avancés et matures. Il y a en effet un décalage grandissant, disproportionné, entre le niveau de maturité cyber de certains acteurs du secteur et les moyens des attaquants.

Cette attaque soulève également des questions plus fondamentales : en attaquant Safe{Wallet}, Lazarus a-t-il tenté de s'attaquer à l'un des piliers de la finance décentralisée ?
Leur technologie sécurise en effet plus de 100 milliards de dollars on-chain et porte l'ownership de nombreux protocoles de la finance décentralisée.
Dans le cas précis de cette attaque, l'attaquant s'est limité au wallet de Bybit. Mais Lazarus disposait des accès pour réaliser une attaque de plus grande ampleur, pouvant potentiellement cibler tous les utilisateurs de l'interface Safe{Wallet}, causant des dégâts systémiques au secteur.

Cette attaque intervient alors même que la finance dite « traditionnelle » converge vers l'utilisation de la Blockchain avec des cas d'usage comme la « tokenisation[27] » d'actifs financiers. Bien que le secteur financier traditionnel soit familier avec la menace étatique, l'utilisation d'une blockchain publique pour ces cas d'usage soulève des questions de sécurité additionnelles.

De manière plus générale, cette attaque constitue une prise de conscience pour l'écosystème web3 qui n'avait jamais été confronté à une attaque supply-chain d'une telle ampleur, prouvant le niveau de motivation des attaquants. Ce mode opératoire est pourtant fréquent dans l'informatique traditionnelle, comme en témoigne le cas récent ayant ciblé XZ Utils qui aurait pu avoir un impact dans le monde entier.
Et il y a fort à parier que cette attaque ne soit qu'une première étape, un « proof of concept », où Lazarus a prouvé qu'une attaque supply-chain est possible dans le web3.
Reste alors à se demander quelle sera la prochaine cible. Un wallet grand public ? Un wallet B2B ? Un client de consensus ou d'exécution[28] Blockchain ?

Sans une sécurité pensée de bout en bout et un réel pas en avant dans la maturité du secteur, la pression exercée par ces attaquants d'ordre étatique continuera de s'accentuer. Et Orange Cyberdefense se positionne comme un rempart pour une société numérique plus sûre dans le web3.

Nos experts œuvre au quotidien pour accompagner nos clients dans la prévention de ce type d'attaque, et afin de garantir une sécurité de leurs systèmes d'information de bout en bout, face à tout type de menace.

Orange Cyberdefense – 05.03.2025

[27] Tokenisation : processus de représentation d'actifs réels sous forme de jetons sur une blockchain.

[28] Clients de consensus / clients d'exécution : Logiciels constituant un « nœud » Blockchain, permettant de gérer les règles de consensus d'une Blockchain, l'exécution des transactions et le maintien de l'état d'une Blockchain.