加密貨幣被盜規模創新高，揭秘駭客攻擊的類型工具及防範方法

原文：
https://www.btcc.com/zh-TW/academy/research-analysis/analyzing-cryptocurrency-hacks

今年加密貨幣被盜的規模已經創下歷史新高，駭客從加密應用程式中竊取了超過 2B 美元。在撰寫本文時，區塊鏈又出現了三起駭客攻擊，分別是Rabby wallet 、Solana 生態去中心化金融平台 Mango以及 FTX。

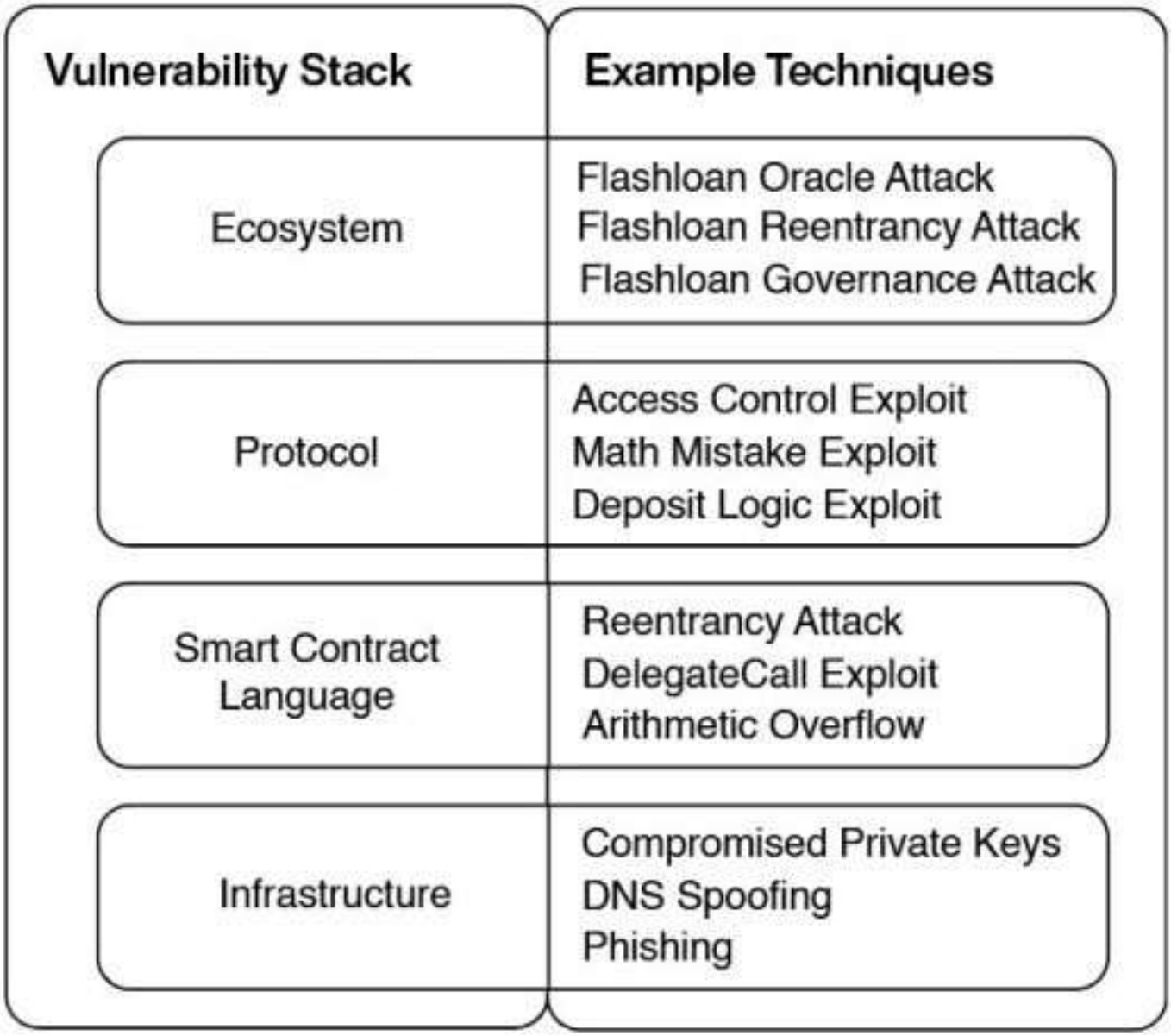
隨著加密生態系統的發展，產生的資金和效益也就越來越高，這不可避免地會吸引更多的惡意行為者，嚴重影響加密行業的安全。

本文將通過分析 100 個加密貨幣駭客攻擊事件，對加密貨幣駭客攻擊進行分類，概述迄今為止最有利可圖的黑客所使用的方法並討論加密貨幣安全的未來。

加密駭客攻擊的分類

加密應用生態系統由可互操作的協議組成，由智能合約提供支持，依賴於主鏈和互聯網的底層基礎設施。

由於堆棧的每一層都有其獨特的漏洞。我們可以根據被利用的堆棧層和使用的方法對加密駭客進行分類。



加密貨幣駭客攻擊的分類

1. 基礎設施

對基礎設施層的攻擊利用了支持加密應用程式的底層系統的弱點：它依賴於達成共識的區塊鏈、用於前端的互聯網服務以及用於私鑰管理的工具。

2. 智能合約語言

這一層的駭客利用了 Solidity 等智能合約語言的弱點。智能合約語言中存在眾所周知的漏洞，例如可重入性和錯誤的委託調用實現的危險，可以通過遵循最佳實踐來緩解這些漏洞。

有趣的是，用於執行 6000 萬美元 The DAO 駭客攻擊的漏洞實際上是由 Least Authority 在對乙太坊的安全審計中發現的。

3. 協議邏輯

此類攻擊利用單個應用程式的業務邏輯中的錯誤。如果攻擊者發現錯誤，可以使用它來觸發應用程式開發人員無意的行為。

例如，如果一個新的去中心化交易所在確定用戶從交易所中獲得多少的數學方程式中存在錯誤，則可以利用該錯誤從交易所中獲得比本應可能的更多的錢。

協議邏輯級攻擊還可以利用現有的治理系統來控制應用程序的參數。

4. 生態系統

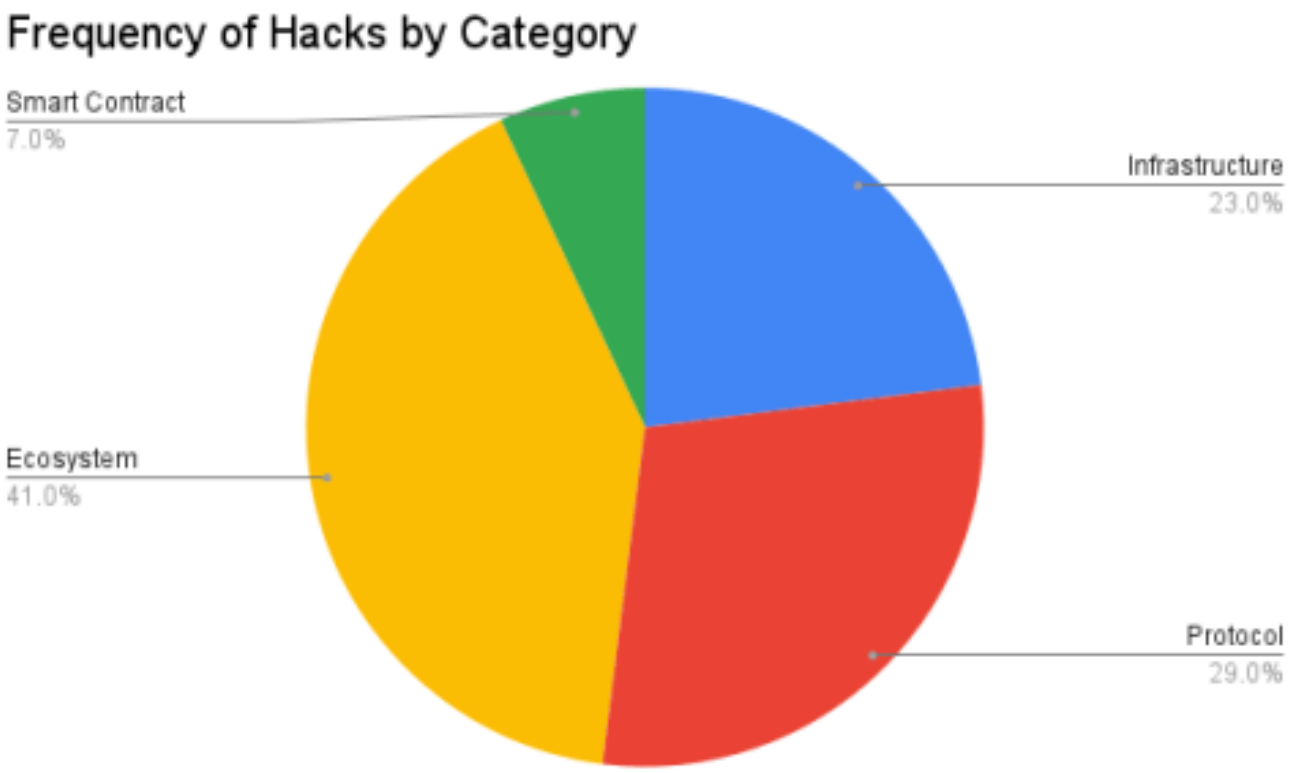
許多最具影響力的加密駭客利用了多個應用程序之間的交互。最常見的變體是攻擊者利用從另一個協議借來的資金利用一種協議中的邏輯錯誤來擴大攻擊規模。

通常，用於生態系統攻擊的資金是通過快速貸款借入的。在執行閃電貸款時，只要資金在同一筆交易中歸還，您就可以從 Aave 和 dYdX 等協議的流動資金池中藉入盡可能多的資金，而無需提供抵押品。

分析 100 起大型虛擬貨幣駭客事件

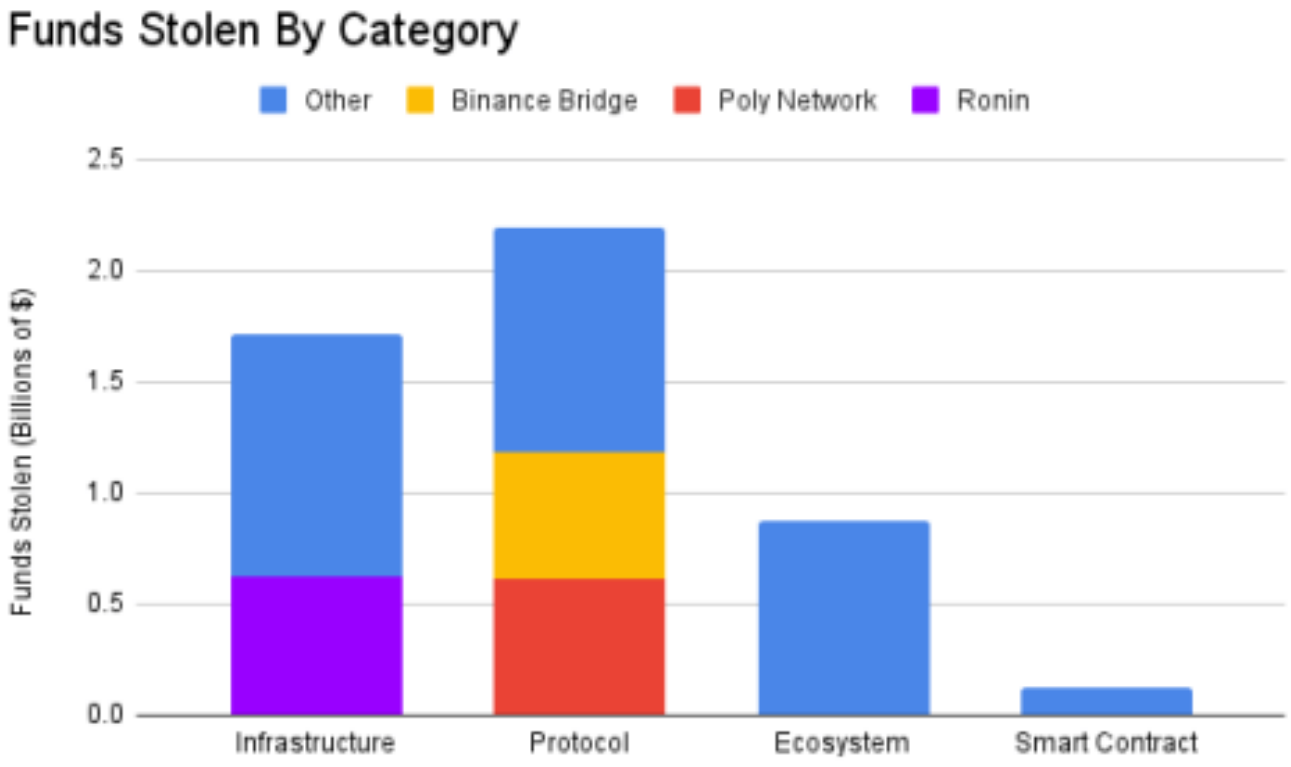
從 2020 年起，我們採集了 100 個最大的加密黑客數據集，被盜資金總計 5B 美元。

生態系統攻擊最常發生。佔樣本組的41%。協議邏輯漏洞導致的損失最大。

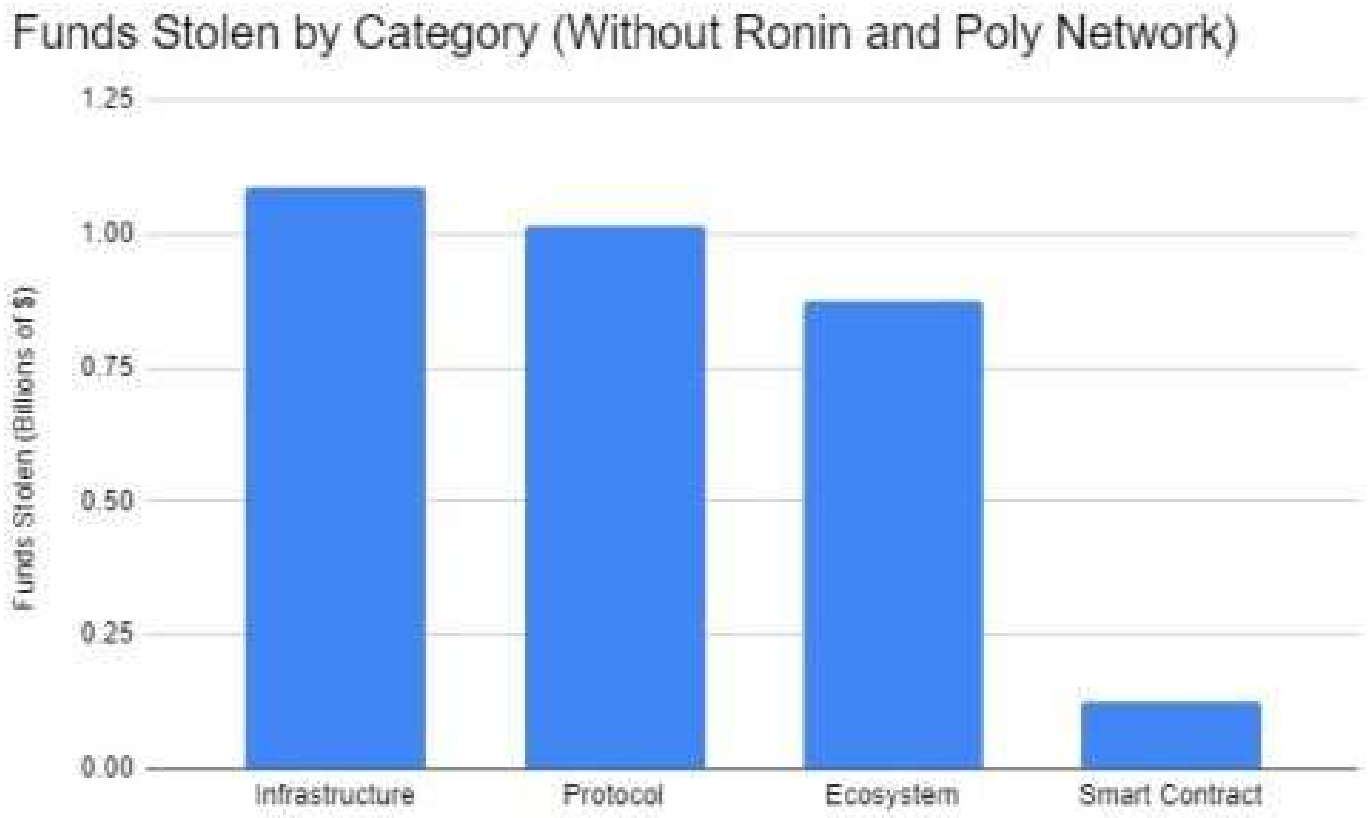


各類攻擊佔比

數據集中最大的三次攻擊，即Ronin bridge 攻擊（6.24 億美元）、Poly Network 黑客（6.11 億美元）和Binance bridge 黑客（5.7 億美元），對結果產生了巨大的影響。



如果排除前三種攻擊，則基礎設施駭客攻擊是損失資金影響最大的類別。

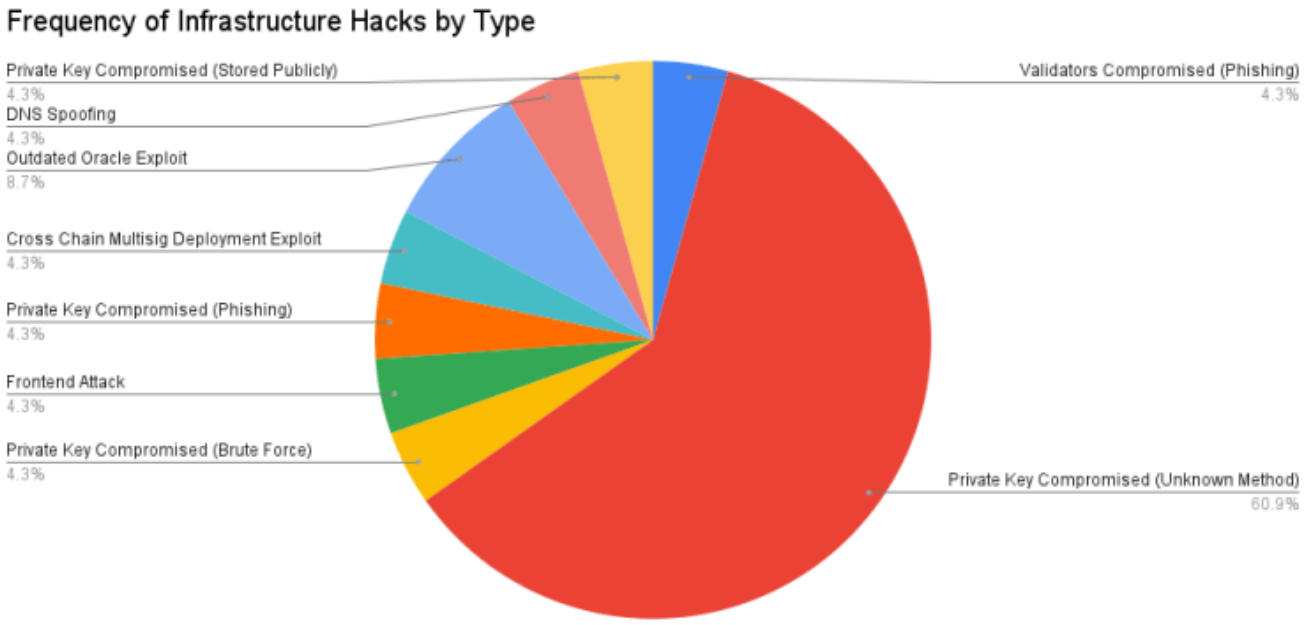


加密駭客如何執行攻擊？

---

1. 基礎設施攻擊

在樣本組中 61% 的基礎設施漏洞利用中，私鑰被未知方式破壞。駭客可能已經通過網路釣魚電子郵件和虛假招聘廣告等社交攻擊獲得了對這些私鑰的訪問權限。



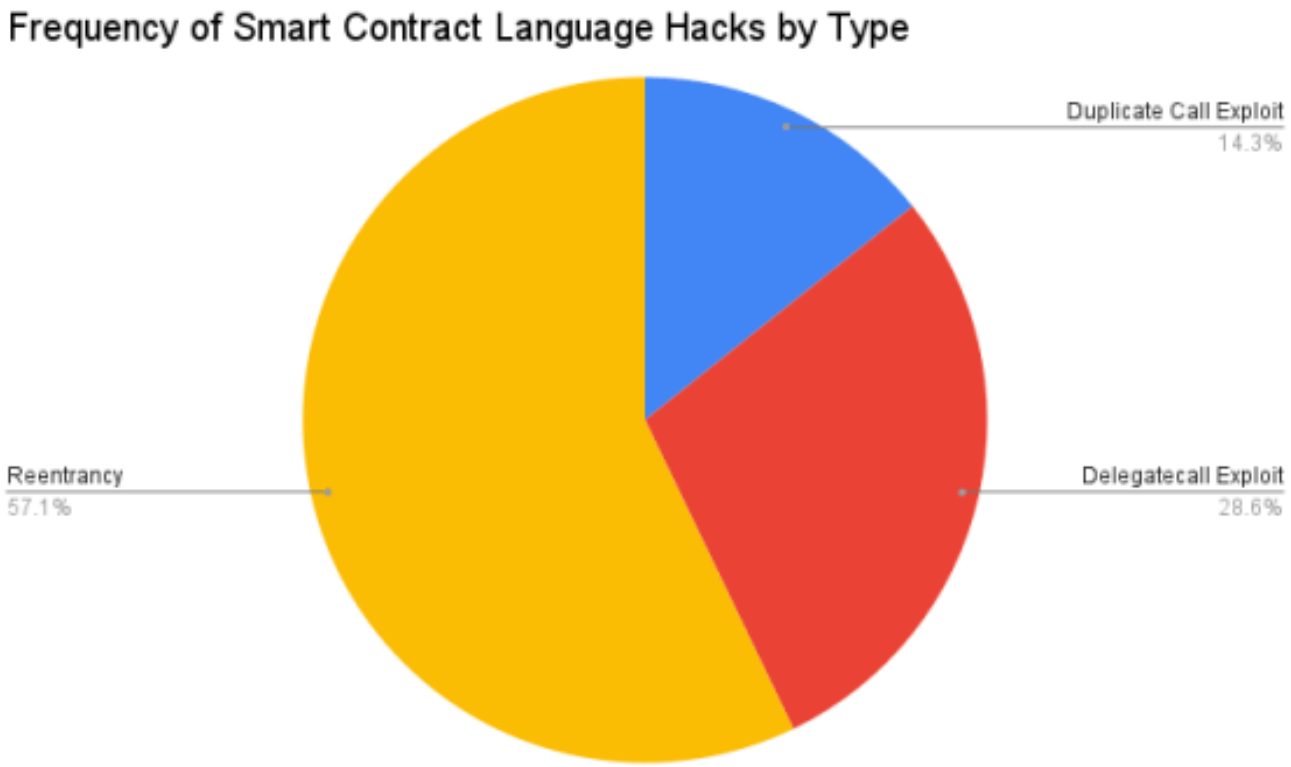
基礎設施攻擊

2. 智能合約語言攻擊

重入攻擊是智能合約語言級別上最流行的攻擊類型。

在重入攻擊中，易受攻擊的智能合約中的函數調用惡意聯繫人的函數。或者，當易受攻擊的合約向惡意合約發送代幣時，可以觸發惡意合約中的功能。然後，在合約更新其餘額之前，該惡意函數會在遞歸循環中回調易受攻擊的函數。

例如，在Siren Protocol hack 中，提取抵押代幣的功能很容易被重入並被反複調用（每次惡意合約收到代幣時），直到所有抵押品都被耗盡。



3. 協議邏輯攻擊

協議層上的大多數漏洞都是特定應用程序獨有的，因為每個應用程序都有獨特的邏輯（除非它是純分叉）。

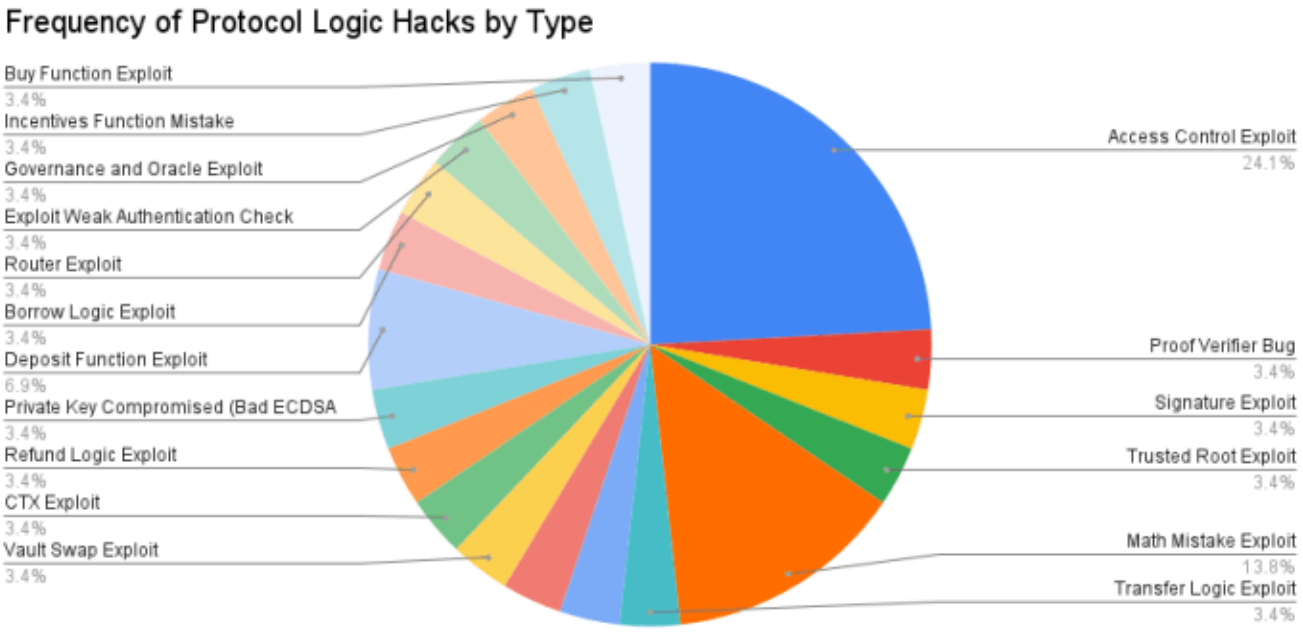
訪問控制錯誤是樣本組中最常出現的問題。例如，在Poly Network hack 中，「EthCrossChainManager」合約具有任何人都可以調用以執行跨鏈交易的功能。

該合約擁有「EthCrossChainData」合約，因此如果您將「EthCrossChainData」設置為跨鏈交易的目標，則可以繞過onlyOwner() 審查。

剩下要做的就是製作正確的消息來更改哪個公鑰被定義為協議的「保管人」，奪取控制權並耗盡資金。普通用戶永遠無法訪問「EthCrossChainData」合約上的功能。

注意：在許多情況下，多個協議使用相同的技術被攻擊者入侵，因為團隊分叉了一個存在漏洞的代碼庫。

例如，CREAM、Hundred Finance 和Voltage Finance 等許多Compound 分叉成為重入攻擊的受害者，因為Compound 的代碼在允許交互之前沒有檢查交互的效果。這對Compound 來說效果很好，因為他們審查了他們支持的每個新代幣的漏洞，但分叉團隊並沒有做這樣的努力。



4. 生態系統攻擊

98% 的生態系統攻擊都使用了閃電貸。

Flashloan 攻擊通常遵循以下公式：使用貸款進行大規模掉期，從而推高 AMM 上的代幣價格，而 AMM 將其用作價格饋送。然後，在同一筆交易中，使用膨脹的代幣作為抵押，獲得遠高於其真實價值的貸款。

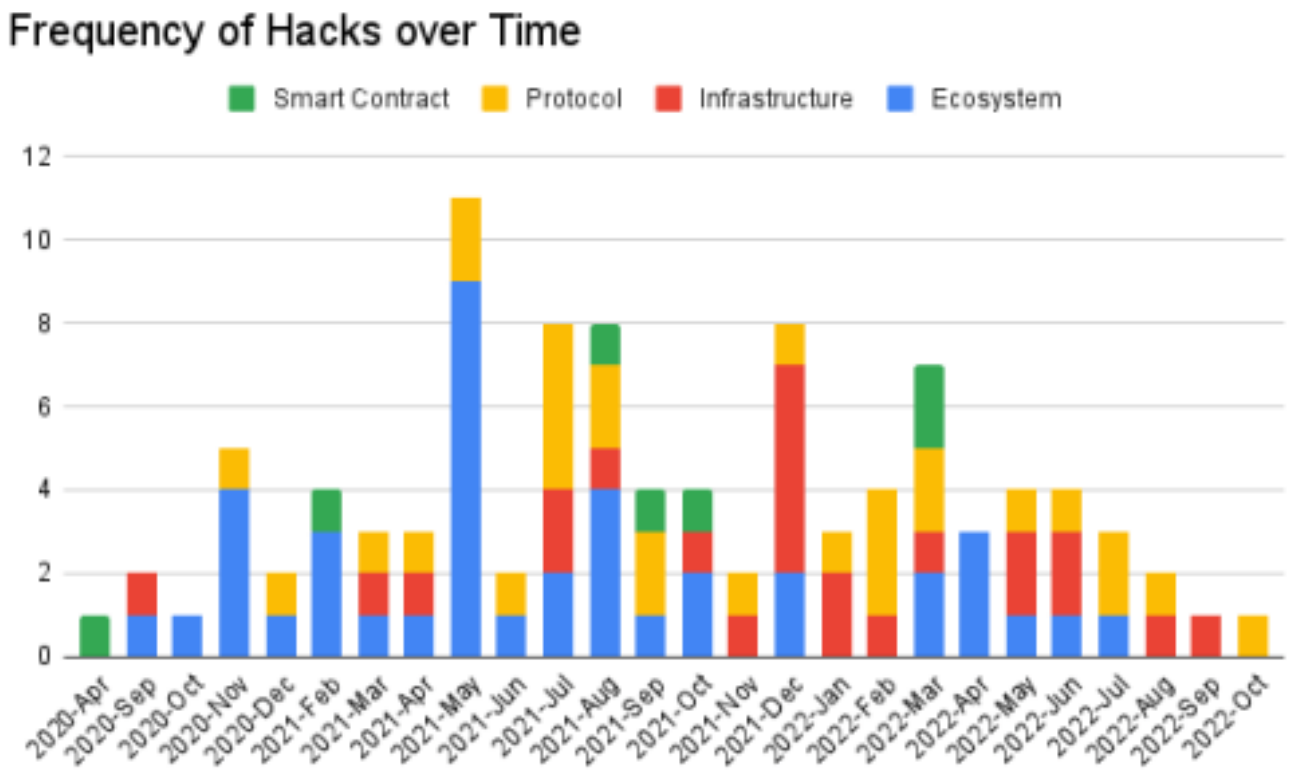
加密貨幣駭客攻擊的時間

數據集不夠大，無法從時間分佈中得出有意義的趨勢。但我們可以看到，不同類型的攻擊在不同的時間更頻繁地發生。

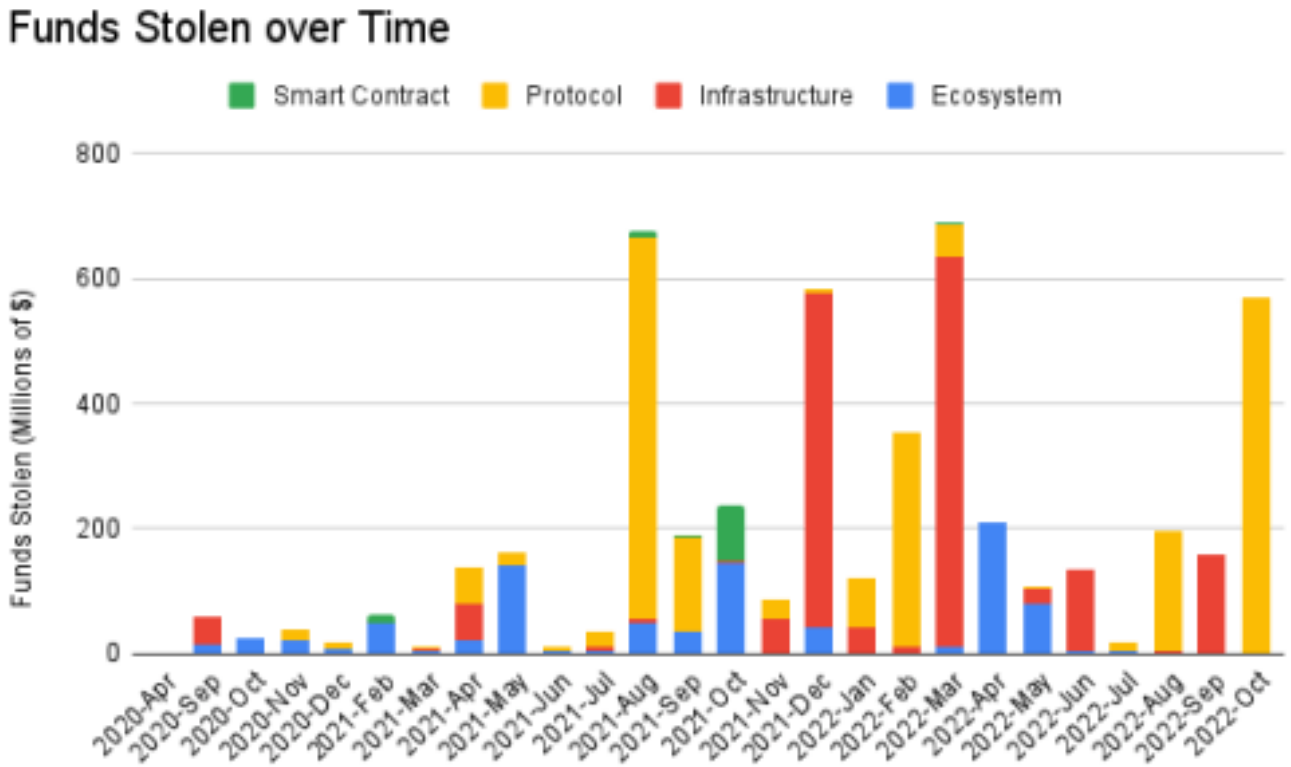
2021 年 5 月是生態系統攻擊的歷史新高。2021 年 7 月的協議邏輯攻擊最多。2021 年 12 月發生的基礎設施攻擊最多。很難判斷這些集群是否是巧合，或者它們是否是一個成功的成功案例，激勵人們專注於特定類別。

智能合約語言級別的漏洞利用是最罕見的。該數據集始於2020 年，當時該類別中的大多數漏洞利用已經

廣為人知，並且很可能很早就被發現。



隨著時間的推移，被盜資金的分佈有四個主要峰值。2021 年 8 月有一個高峰，這是由 Poly Network 駭客驅動的。2021 年 12 月，由於大量基礎設施攻擊導致私鑰遭到破壞，例如 8ight Finance、Ascendex 和 Vulcan Forged，又出現了另一次高峰。然後，由於Ronin 駭客攻擊，我們看到了 2022 年 3 月的歷史新高。最後的峰值是由 BNB bridge 被攻擊引起的。

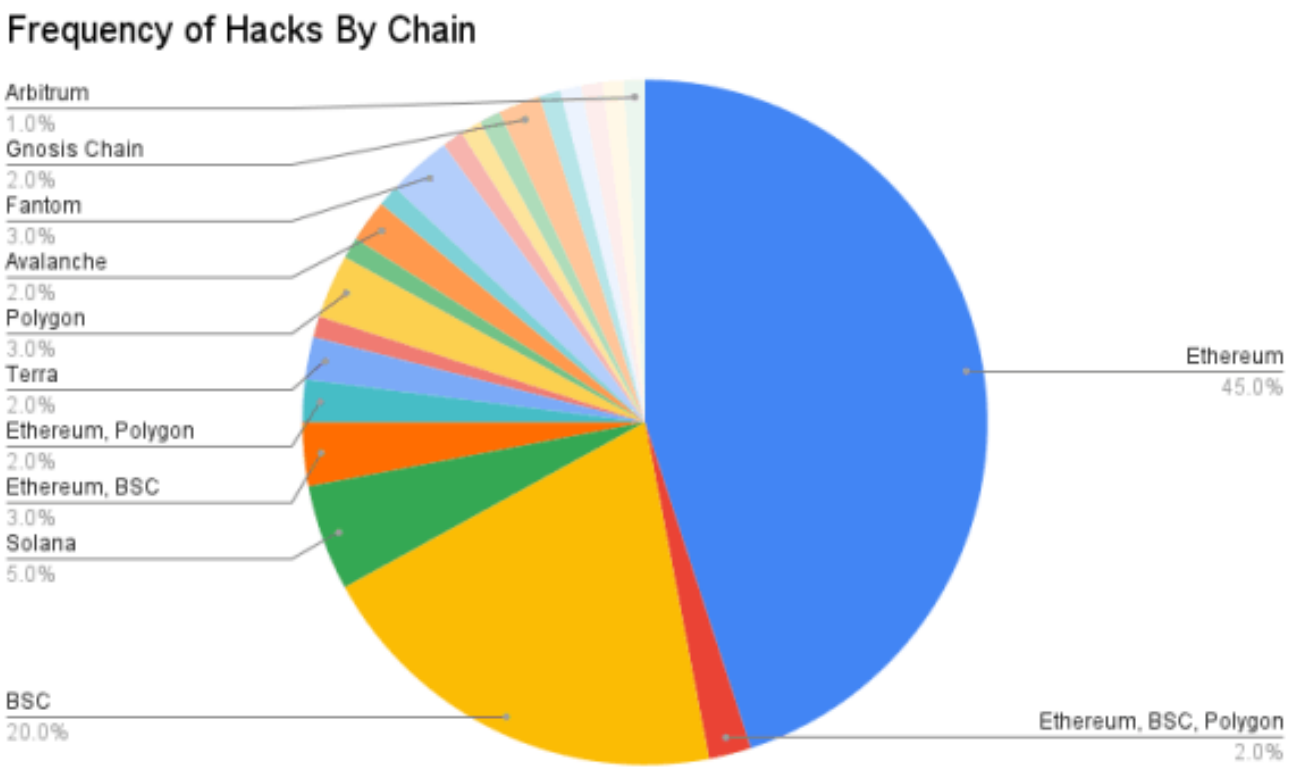


不同鏈的駭客攻擊

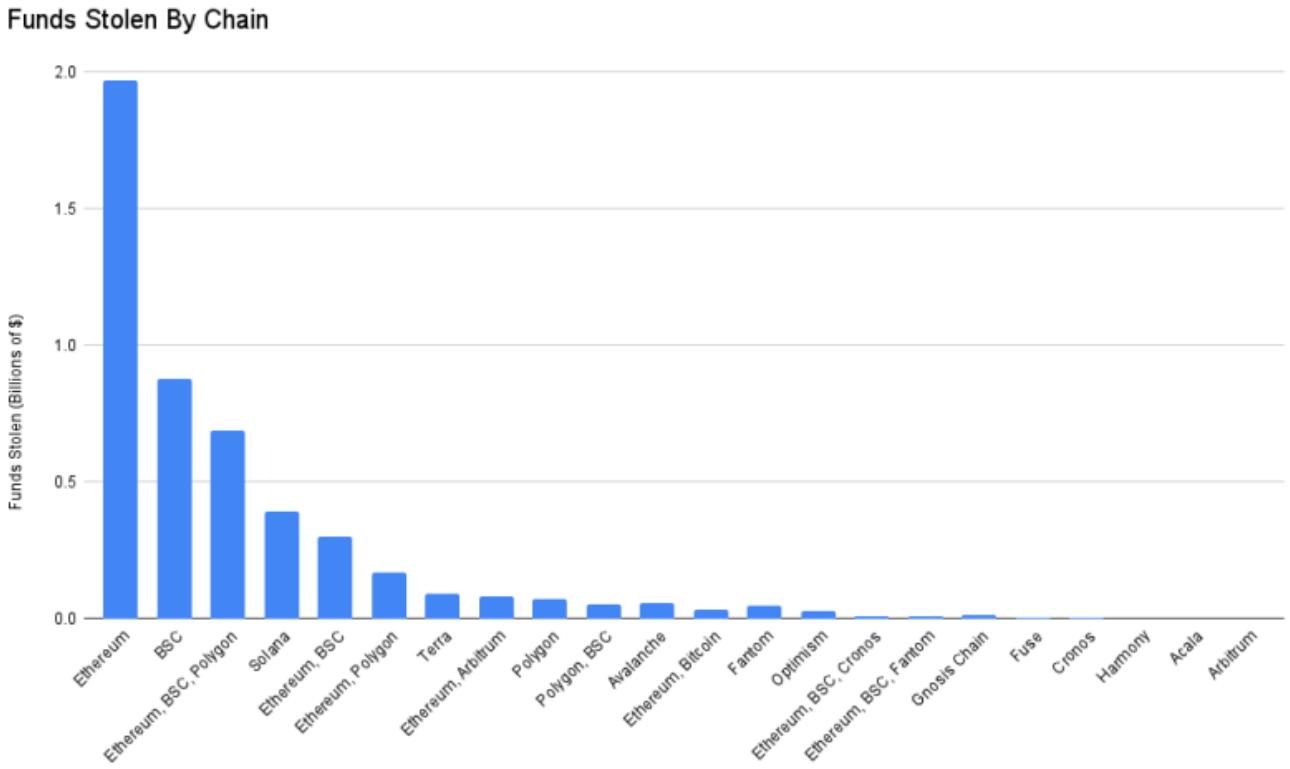
根據託管資金被盜的合約或錢包的鏈來分割數據集。乙太坊的駭客數量最多，佔樣本組的45%。幣安智能鏈（BSC）以20% 位居第二。

造成這種情況的因素有很多：

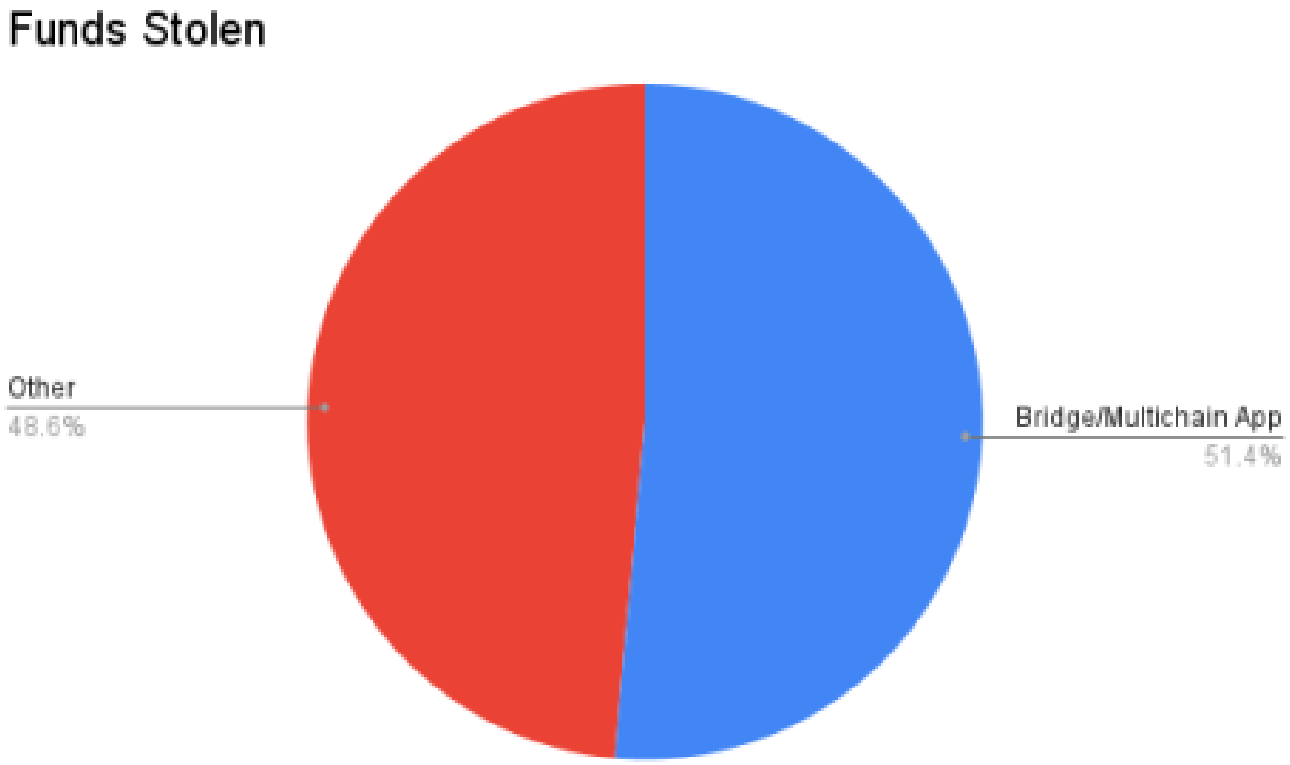
1. 乙太坊和 BSC 的鎖定總價值（存入應用程序的資金）最高，因此對於這些鏈上的攻擊者來說，獎金的規模更大。
2. 大多數加密開發人員都知道 Solidity，這是乙太坊和 BSC 上選擇的智能合約語言，並且有更複雜的工具支持該語言。



乙太坊被盜的資金量最大（20 億美元），BSC 位居第二（8.78 億美元）。乙太坊、BSC 和 Polygon 上的資金被盜的黑客在一次事件中排名第三（6.89 億美元）。這主要是因為 Poly Network 攻擊事件。



涉及跨鏈橋或多鏈應用的駭客（如多鏈交換或多鏈借貸）對數據集有巨大影響。儘管只佔事件的10%，這些攻擊者佔了25.2 億美元的被盜資金。



在加密領域中如何防止黑客入侵？

對於威脅堆棧的每一層，我們可以使用一些工具來及早識別潛在的攻擊向量並防止攻擊發生。

1. 基礎設施

大多數大型基礎設施攻擊都涉及駭客獲取敏感信息，例如私鑰。遵循良好的運營安全(OPSEC) 實踐並進行經常性威脅建模可降低發生這種情況的可能性。擁有良好OPSEC 流程的開發人員團隊將：

- 識別敏感數據（私鑰、員工信息、API 密鑰等）
- 識別可能的威脅（社交攻擊、技術漏洞、內部威脅等）
- 識別現有安全防禦中的漏洞和弱點
- 確定每個漏洞的威脅級別
- 創建並實施計劃以減輕威脅
- 智能合約語言和協議邏輯

2. 模糊測試

像Echidna 這樣的模糊測試工具可以測試智能合約如何對大量隨機生成的交易做出反應。這是檢測特定輸入產生意外結果的邊緣情況的好方法。

3. 靜態分析

靜態分析工具，如Slither 和Mythril，自動檢測智能合約中的漏洞。這些工具對於快速挑出常見的漏洞是很好的，但它們只能抓住一組預定義的問題。如果智能合約有一個不在工具規範中的問題，它將不會被看到。

4. 形式驗證

形式驗證工具，如Certora，會將智能合約與開發人員編寫的規范進行比較。該規範詳細說明了代碼應該做什麼及其所需的屬性。例如，開發貸款應用程序的開發人員會指定每筆貸款都必須有足夠的抵押品支持。

如果智能合約的任何可能行為不符合規範，正式驗證者將識別該違規行為。

形式化驗證的弱點是，測試只和規範一樣好。如果所提供的規範沒有考慮到某些行為，或者過於寬鬆，那麼驗證過程將無法捕獲所有的錯誤。

5. 審計和同行評審

在審計或同行評審中，一個受信任的開發者小組將測試和評審項目的代碼。審計員會寫一份報告，詳細說

明他們發現的漏洞以及如何修復這些問題的建議。

讓第三方專家審查合約是識別原團隊所遺漏的漏洞的一個好方法。然而，審計師也是人類動物，不可能發現所有的東西。另外，還必須對此信任，如果審計師發現了問題，他們會告訴你，而不是自己去利用它。

6. 生態系統攻擊

令人沮喪的是，儘管生態系統攻擊是最常見和最具破壞性的變體，但工具箱中並沒有多少工具適合防止這些類型的攻擊。

自動化安全工具專注於一次發現一個聯繫人中的錯誤。審計通常無法解決如何利用生態系統中多個協議之間的交互。

Forta 和Tenderly Alerts 等監控工具可以在發生可組合性攻擊時發出預警，以便團隊採取行動。但在閃電貸攻擊期間，資金通常在單筆交易中被盜，因此任何警報都來得太晚，無法防止巨額損失。

威脅檢測模型可用於在內存池中查找惡意交易，其中交易位於節點處理之前，但黑客可以通過使用flashbots 等服務將交易直接發送給礦工來繞過這些檢查。

加密安全的未來如何？

相信最好的團隊將從將安全視為基於事件的實踐（測試-> 同行評審-> 審計）轉變為一個持續的實踐過程。他們將：

- 對主代碼庫的每個添加運行靜態分析和模糊測試。
- 在每次重大升級時運行形式驗證。
- 使用響應操作（暫停整個應用程序或受影響的特定模塊）設置監控和警報系統。
- 讓一些團隊成員專門負責制定和維護安全自動化和攻擊響應計劃。
- 安全性不是一組要填寫和擱置的複選框。安全工作不應在審計後結束。在許多情況下，例如Nomad bridge hack，漏洞利用是基於審計後升級中引入的錯誤。

此外，加密安全社區應對駭客攻擊的流程將變得更有條理和精簡。每當發生駭客攻擊時，貢獻者就會湧入渴望提供幫助的加密安全群組聊天，但缺乏組織意味著重要的細節可能會在混亂中丟失。我看到未來其中一些群聊會轉變為更結構化的組織：

- 使用鏈上監控和社交媒體監控工具快速檢測主動攻擊。
- 使用安全信息和事件管理工具來協調工作。
- 獨立的工作流，有不同的渠道來溝通白駭客工作、數據分析、根本原因理論和其他任務。

結語

以上就是關於加密貨幣駭客攻擊事件的所有內容了，希望對各位讀者有所幫助。

在了解了這些駭客攻擊的分類和原因後，作為投資者我們也需要了解如何防止自己受到加密貨幣詐騙，保護自己的加密安全。以下是辨別幣圈詐騙的方法，在進入幣圈前請務必進行查看：

這些加密投資者是真的嗎？一文教你避開90%的虛擬貨幣詐騙！

5種常見數字貨幣詐騙 新手應該如何防範？

NFT防盜指南丨如何保護自己的NFT資產安全？

加密安全丨預防加密貨幣所被駭指南

T-SET事件詳解，我們應該如何避開加密貨幣騙局

Pi 幣是詐騙嗎？該項目存在什麼風險？

如果你想了解更多加密貨幣的資訊，可以進入 BTCC **學院** 及 **資訊** 頁面進行查看。