2021年11月29日 星期一
網路與系統安全報告
108AB0735 藍珮瑈

# Ledger Supply Chain Attack

## WHAT HAPPENED?

On the 14th of July 2020, a researcher took part in Ledger bounty program and made aware of a potential data breach on the Ledger website. They immediately fixed this breach after receiving the researcher's report and underwent an internal investigation. A week after patching the breach, they discovered it had been further exploited on the 25th of June 2020, by an unauthorized third party who accessed their e-commerce and marketing database which is used to send order confirmations and promotional emails and mostly consisted of email addresses, but with a subset including also contact and order details such as first and last name, postal address and phone number. Although customer's payment information and crypto funds are safe but the attacker used the stolen data for online phishing and user extortion.

The API key which the unauthorized third party used to access a portion of e-commerce and marketing database has been deactivated and is no longer accessible.

## WHAT CAN LEAD TO IF THOSE PERSONAL INFORMATION BE STOLON?

Attacker can use those personal information which include first and last name, postal address, email address and phone number to send phishing emails and replicate USB crypto wallet drives to steal cryptocurrency from the customer.

## HOW DID THE ATTACKER DO IT?

Before analyze the accident, we review the "TAXONOMY OF SUPPLY CHAIN ATTACKS" which mention in the Chapter2.

Taxonomy for supply chain attacks. It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) assets attacked in the customer. (Threat Landscape for Supply Chain Attacks 2021)

# CASE ANALYZE

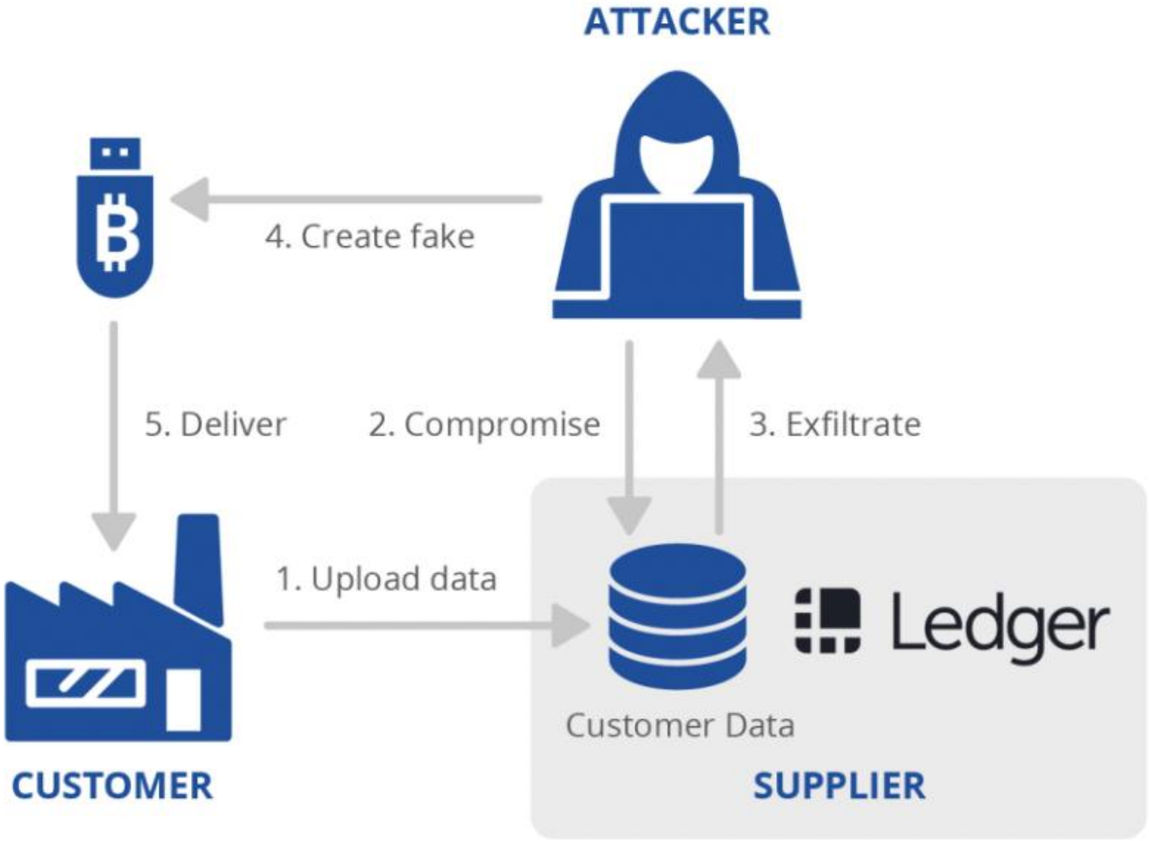
Now we’re going to using the information from “WHAT HAPPENED?” to identify the four elements in the taxonomy for supply chain attacks.

| **SUPPLIER** | |
|---|---|
| Attack Techniques Used to Compromise the Supply Chain | Supplier Assets Targeted by the Supply Chain Attack |
| Malware Infection | Pre-existing Software |
| Social Engineering | Software Libraries |
| Brute-Force Attack | Code |
| Exploiting Software Vulnerability | Configurations |
| Exploiting Configuration Vulnerability | Data |
| Open-Source Intelligence (OSINT) | Processes Hardware |
| | People Supplier |

| **SUPPLIER** | |
|---|---|
| Attack Techniques Used to Compromise the Customer | Customer Assets Targeted by the Supply Chain Attack |
| Trusted Relationship [T1199] | Data |
| Drive-by Compromise [T1189] | Personal Data |
| Phishing [T1566] | Intellectual Property |
| Malware Infection | Software |
| Physical Attack or Modification | Processes |
| Counterfeiting | Bandwidth |
| | Financial |
| | People |

“The attack on the supplier” means how the attackers got access to the supplier. In this case, attackers use API key to get the access, therefore it was by “OSINT”. Through this attack, the attackers target “Data” - the asset of the supplier, such as information about the supplier, values from sensors, certificates, personal data of customers and suppliers. After the elements for the supplier were identified in the taxonomy, we can move to how the customer was attacked. In the Ledger case is through ‘Trusted Relationship’, ‘phishing’, ‘Counterfeiting’, with the supplier that was not secured and verified. The final asset targeted in the customer was ‘Financial’, because attackers can use those personal information to send phishing emails and replicate USB crypto wallet drives to steal cryptocurrencies from the customer.

Ledger supply chain attack. The attackers found credentials of Ledger online, accessed their customers 'database and used the information to attack the customers. (Threat Landscape for Supply Chain Attacks 2021)


ATTACKER
4. Create fake
5. Deliver
2. Compromise
3. Exfiltrate
1. Upload data
Ledger
Customer Data
CUSTOMER
SUPPLIER