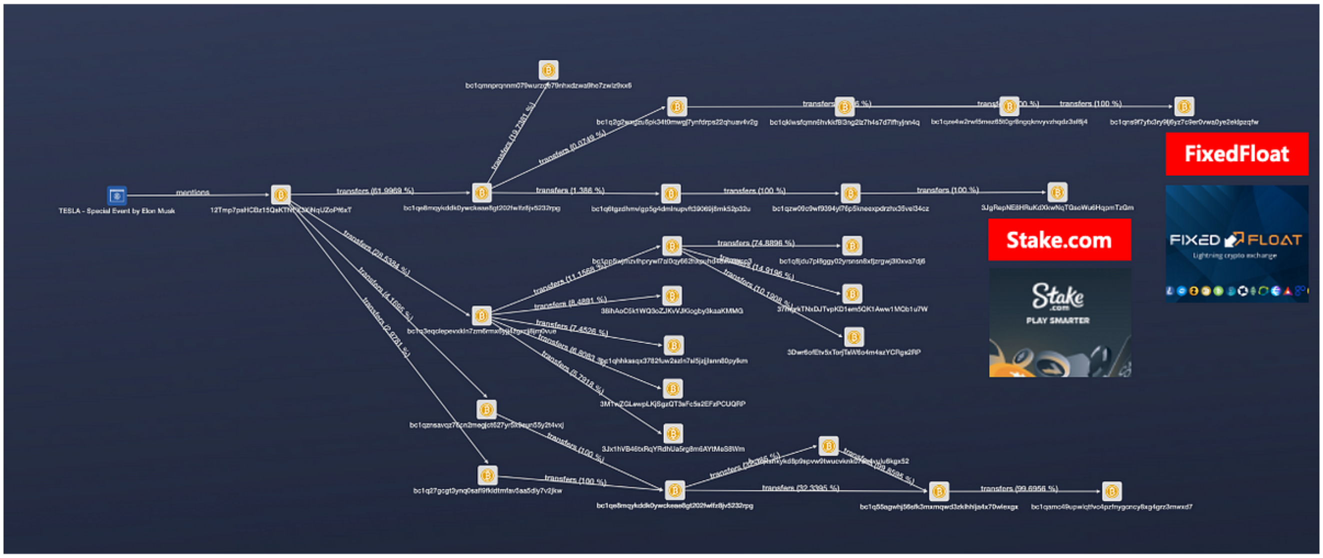
Detailed Analysis of Cryptocurrency Phishing Through Famous YouTube Channel Hacking

medium.com/s2wblog/detailed-analysis-of-cryptocurrency-phishing-through-famous-youtube-channel-hacking-cd40de8dce6f

S2W

March 24, 2023



S2W

Mar 20

.

19 min read

Author: HOTSAUCE | S2W TALON

> **Last Modified** : Mar 20, 2023

Executive Summary

최근 정부 기관의 공식 유튜브 채널을 비롯한 게임 유튜버 , 성우 유튜버 등 구독자 수가 많은 유튜버들을 대상으로 피싱 메일을 발송하여 계정을 해킹하는 사례가 늘어나고 있음.

> 관련 기사 > (2022–09–24) 머니투데이, “머스크가 왜 나와?” 정부·방송 공식 유튜브 ‘해킹’, 무엇을 노렸나”

- 해킹된 유튜브 채널들은 일론 머스크 라이브 스트리밍을 통해 비트코인 / 이더리움 등 암호화폐를 자신의 주소로 전송하면 두 배로 돌려준다는 피싱 페이지로 접속을 유도하고 있음.
- 일론 머스크, 트럼프 등 유명인사를 사칭하여 암호화폐 피싱 페이지로 접속을 유도하는 케이스는 2020년 부터 존재했으며, 최근에는 유튜브 시청자가 많아지면서 더욱 많은 피해자들에게 접속을 유도하기 위해 유튜브 채널 해킹을 통한 홍보 방법을 사용하고 있음.
- 암호화폐 피싱 사이트에서 참여자들의 입금 내역이라며 실시간으로 업데이트되는 트랜잭션들은 랜덤 문자열을 생성하여 HTML에 렌더링하는 형태로 구현되어 있으며, 실제로는 존재하지 않는 가짜 트랜잭션 및 암호화폐 주소로 확인됨.
- 최근 발생한 인피쉰 유튜브 해킹 사건을 기준으로 피싱 사이트 분석과 암호화폐 추적을 진행함.
- 피싱 사이트는 최소 69개 이상 운영되고 있음.
- 피해자들이 입금한 자금은 암호화폐를 사용하여 결제하는 카지노 사이트 stake.com과, FixedFloat 거래소로 전송된 내역이 확인됨.

Detailed Analysis

1. 유튜버 계정 해킹을 통한 암호화폐 피싱 사이트 홍보

최근 과 스타크래프트 게임 유튜버 , 성우 유튜버 등 구독자 수가 많은 유튜버 계정을 탈취된 뒤 일론머스크가 출연하는 비트코인 홍보 영상을 송출하고 있음.

> 관련 기사 > 대한민국 정부 유튜브 계정 털렸다… 일론 머스크는 왜?

유튜브 계정을 해킹 후 암호화폐 피싱 사이트 홍보에 사용한 건 2019년 부터 식별되기 시작 했으며 국내 뿐만 아니라 해외에서도 빈번히 일어나고 있음. 특히, 사망한 뒤 관리되고 있지 않던 유튜브 계정도 탈취된 사례가 존재하여 이슈가됨.

> 관련 기사 > Reckful: Dead YouTuber hacked by bitcoin scammers

- 피싱 사이트를 홍보하는 근본적인 목적은 암호화폐 편취이며 일론 머스크, 도널드 트럼프 등과 같은 많은 재력을 보유한 유명인이 이벤트를 하는 것 처럼 속인 뒤 임.
- 사기 과정에서 유튜브 로고, 유튜브 채널명을 변경한 뒤 실시간 라이브 영상을 틀어 유튜브 메인 화면에 노출시켜 시청을 유도하고 있으며, 도메인은 일론머스크, 트위터, 아크인베스트 등 유명인이나 기업 이름을 Typosquatting하여 사용하고 있음.

그림 1. 트위터 Typosquatting 도메인 twitterchiefp[.]com 을 사용한 암호화폐 피싱 사례

- 이와 같은 암호화폐 편취를 목적으로 한 사기성 피싱 사이트는 과거부터 존재했으며 다크웹 상에서 최소 2020년 10월 부터 활동한 이력이 확인됨.
- 비트코인 주소를 기준으로 교차분석한 결과 각각의 케이스에서 동일한 주소를 사용한 이력이 발견되었고, 초기 비트코인 트랜잭션 사기에서 도널드 트럼프 사칭, 일론 머스크 사칭으로 변화된 것으로 확인됨.

표 1. 비트코인 사기 사이트의 피싱 방식 변화
그림 2. 암호화폐 피싱 사이트 교차 분석

- 위 사례의 피싱 사이트에 언급 되어있는 비트코인 주소 8개의 거래 이력을 조사한 결과 457건의 트랜잭션이 확인되었으며, 약 0.75 BTC의 피해 금액이 입금됨.
- 이러한 형태로 사기가 가능하다는 것을 확인한 사이버 범죄자들은 더욱 많은 유저들에게 접속을 유도하기 위해 유튜브 채널 해킹을 통한 홍보 방법을 사용하는 것으로 추정됨.

표 2. 비트코인 피해 금액

1.1. 정부 기관 유튜브 공식 채널 해킹

(2022–09–03) 우리나라의 정부에서 공식적으로 운영하는 유튜브 채널 “대한민국정부”와 공공기관 “한국관광공사” 계정이 탈취된 뒤 채널명이 SpaceX Invest로 변경 되었으며 일론머스크가 출연하여 비트코인을 홍보하는 영상이 송출됨.

그림 3. 피싱을 위한 이더리움 & 비트코인 라이브 스트리밍
라이브 스트리밍에서는 테슬라와 유명 미국 투자사 아크인베스트를 사칭하여 암호화폐 피싱사이트 tsla-arkinvest[.]info 로 접속을 유도하고 있음.

그림 4. 피싱을 위한 이더리움 & 비트코인 라이브 스트리밍

1.2. 유명 유튜버 채널 해킹

Case 1 : “인피쉰” 유튜브 채널 해킹

- (2023–02–04) “인피쉰” 유튜버의 계정이 해킹당해 채널명과 프로필 사진이 “Tesla Pull”로 변경됨.
- 유튜브 채널 운영자가 빠르게 인지하기 어려운 새벽 시간대에 변경되어, 다음날 아침에서야 해킹 사실을 인지하였고 계정 복구 절차를 진행함.

그림 5. 인피쉰 유튜버 계정 해킹 전(좌) / 후(우)
기존 업로드되었던 모든 영상이 비공개로 바뀌고 일론 머스크의 라이브 스트리밍 영상이 업로드됨.

그림 6. “인피쉰” 유튜버 계정 해킹 후 일론 머스크 라이브 영상 스트리밍
실시간 라이브 영상을 틀어 유튜브 메인 화면에 노출시켜 시청을 유도하고 있으며, 도메인은 일론머스크가 경영 중인 테슬라의 공식 도메인을 Typosquatting한 teslafuture[.]com 을 사용함.

그림 7. 암호화폐 피싱 사이트 접속 유도 (출처 :

Case 2 : “남도형의 블루클럽” 유튜브 채널 해킹

- (2023–02–06) “남도형의 블루클럽” 유튜버의 계정이 해킹당해 채널명과 프로필 사진이 “Tesla US” 로 변경됨.
- 반다이남코 게임사를 사칭한 스피어피싱 메일이 사용되었으며, 이메일을 통해 Lumma Stealer 악성코드가 설치됨.
- (참고) S2W 위협분석센터(TALON) 위협분석팀에서 작성한 상세 분석 보고서

> (2023–02–28) S2W Medium — Lumma Stealer targets YouTubers via Spear-phishing Email

그림 8. “남도형의 블루클럽” 유튜버 계정 해킹 전(좌) / 후(우)

1.3. 암호화폐 피싱 사이트 홍보

- 해킹된 유튜브 채널들은 라이브 스트리밍을 통해 비트코인 / 이더리움 등 암호화폐를 자신의 주소로 전송하면 두 배로 돌려주겠다는 피싱 페이지로 접속을 유도하고 있음.
- 예를 들어 0.1 비트코인을 전송하면 즉시 0.2 비트코인을 돌려 받는 구조라고하며 한정 이벤트인 것 처럼 홍보하고 있음.

그림 9. 암호화폐 피싱 사이트 — teslafuture[.]io

2. 피싱 사이트 분석

2.1. teslafuture[.]io

송금 유도 방식

- 피싱 사이트는 실시간으로 참여자들이 입금한 금액에 따라 2배의 금액을 돌려주는 것 처럼 트랜잭션이 계속해서 업데이트되고 있음.
- 해당 사이트를 통해 피해자가 giveaway 주소에 돈을 전송하도록 유도하고 있음.

그림 10. 암호화폐 피싱 사이트
입금 내역 조회 및 실시간 트랜잭션 현황

- 암호화폐 피싱 사이트에서 참여자들의 입금 내역을 조회할 수 있음.
- 실시간으로 업데이트되는 트랜잭션들은 랜덤 문자열을 생성하여 HTML에 렌더링하는 형태로 구현되어 있음.
- 트랜잭션 확인 결과, 실제로 존재하지 않는 가짜 트랜잭션 및 암호화폐 주소로 확인됨.
- 해당 테이블은 마치 실시간으로 업데이트 되는 것 처럼 보이나 화면에 표시되는 내용은 피싱 사이트에 포함된 자바스크립트(assets/script.js)에 의해 임의의 문자열 조합으로 랜덤하게 생성되고 있는 의미없는 문자열 조합로 확인됨.

그림 11. LIVE 테이블

3. 유튜브 계정 탈취 수법

유튜브 계정 탈취를 위해 공격자들은 유튜버들을 대상으로 실제 업무 관련 메일과 매우 흡사한 형태의 피싱 메일을 발송하거나, 스틸러 악성코드를 활용하는 등의 방법을 사용하고 있음.

3.1. 인포스틸러 악성코드 활용

스틸러에 감염되어 유출된 계정들 중 유튜브 채널과 구독자를 보유한 Google(YouTube) 계정만 별도로 구매 / 판매함.

그림 12. 스틸러 악성코드에 감염되어 유출된 계정들 중 유튜브 채널 보유한 계정 판매

3.2. 유튜브 채널 구매

많은 사람들이 피싱 페이지로 접속하도록 유도하기 위해 구독자 수가 많은 유튜브 채널을 구매함.

그림 13. 유튜브 채널의 계정 구매

4. 암호화폐 주소 분석

teslafuture[.]io 피싱 사이트를 피봇팅한 결과 동일한 형태의 피싱 사이트 75곳이 확인됨. (상세 주소 목록은 Appendix 참조)

표 3. 암호화폐 피싱 사이트에서 사용된 도메인, IP, 암호화폐 등 정보
해당 사이트들에서 공통적으로 사용된 입금 주소는 다음과 같음.피싱 주소에 입금된 피해자들의 금액은 암호화폐를 사용하여 결제하는 카지노 사이트 stake.com과, FixedFloat 거래소로 전송된 내역이 확인됨.

그림 14. 암호화폐 트랜잭션 분석
암호화폐 피싱에 사용된 Bitcoin, ETH(USDT), DOGE 주소에 입금된 피해금액은 현재 시세 (2023–03–17) 기준으로 한화 에 달하는 것으로 확인됨.

표 4. 암호화폐 피싱 주소에 입금된 피해금액

Conclusion

- 공격자들은 더욱 많은 사람들이 피싱 사이트에 접속하도록 유도하기 위해 유명 유튜버 및 정부 기관의 유튜브 채널 등을 해킹하는 방법을 사용하고 있음.
- 코인을 무료로 나눠 준다며 입금을 요구하는 행위는 99.9% 사기 행위라고 봐도 무방하며 최근 유행하고 있는 일론 머스크 사칭 유튜브 채널, 피싱 도메인 등에 접속에 주의가 필요함.

Appendix

IP

```
199.195.250[.]129192.236.154[.]108188.120.237[.]203176.9.52[.]166154.85.45[.]88185.40.
```

Domain

```
teslaking.ioteslatop.ioteslabuy.ioteslatrend.ioteslahigh.iorichtesla.ioteslabest.iotes
```

Cryptocurrency Address

```
bc1qqgtkca3m5tjflf75f4eqvka4ktxglcpk6vycxf,Bitcoinbc1qlpt8lm0hsjggytkmeka63tt4klu355an
```