호스트 기반의 암호화폐 포렌식

MaJ3stY

saiwnsgud@gmail.com

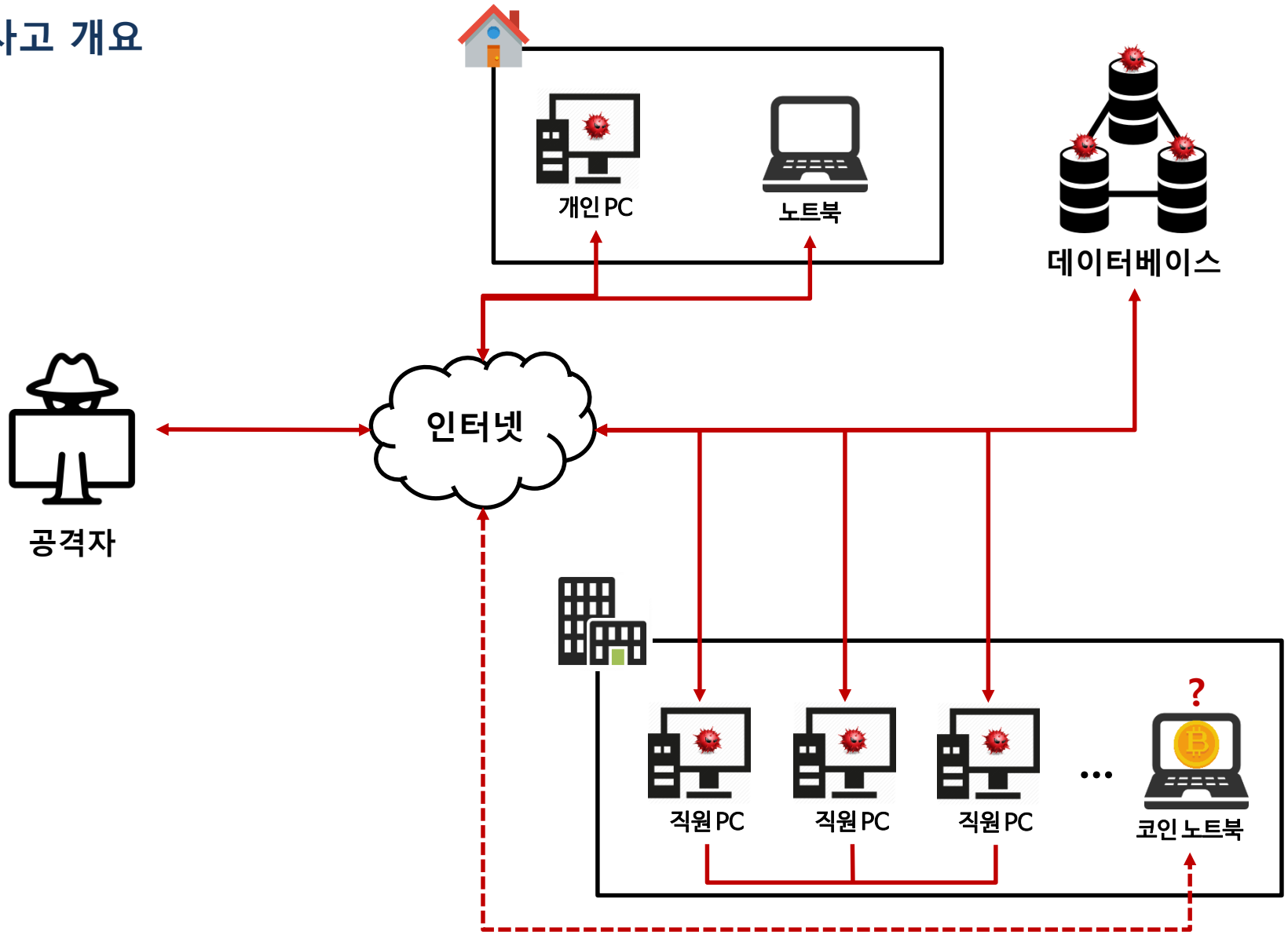
http://maj3sty.tistory.com

Rather be dead than cool.

1. 분석 주제 설정
2. 비트코인 코어 소개
3. 암호화폐 관련 공격
4. wallet.db 중심의 비트코인 코어 실험
5. 향후 실험 주제

분석 주제 설정

침해사고 개요



침해사고 개요

- **상황) 비트코인 코어만 설치되어 있는 노트북에서 wallet.db에 저장되어 있던 코인이 공격자의 지갑으로 송금!!!**
  - 비트코인 코어만 사용하기 위해 구매한 노트북
  - 인터넷, 이메일 열람 한 행위 등 **일반적인 사용자 행위는 존재하지 않음(!)**
  - 비트코인 코어 동기화 때만 인터넷 연결

- **분석 가능한 것들**
  - 노트북
  - 노트북이 연결했던 네트워크
  - ?

분석 주제 설정

- **분석 초점 설정 → 만약, 호스트에 접근 했다면?!**
  - 호스트는 어느 네트워크에 연결 했을까?
  - wallet.db 파일이 유출되었을 가능성은?
    - ✓ 유출되었다면 다른 곳에서 코인이 송금됐을까? (가능할까?)
  - wallet.db 파일은 암호화(비밀번호)가 되어 있었을까?
  - wallet.db는 처음부터 공격자의 지갑 파일이지 않았을까?

- **분석 초점 설정 → 만약, 호스트에 접근하지 않았다면?!**
  - 비트코인 코어에 원격 취약점이 존재할까?
  - 원격에서 wallet.db 파일을 가져가거나, 거래를 일으킬 수 있는 방법은?

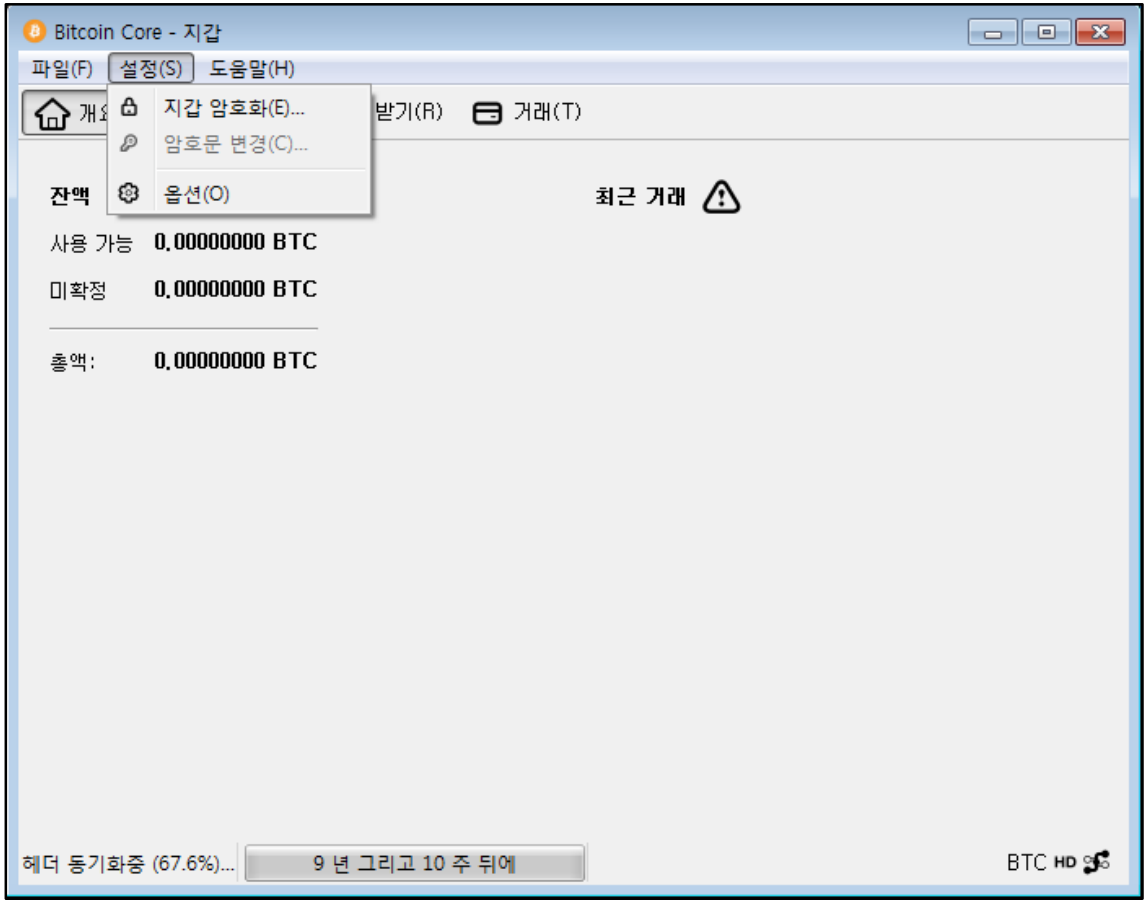
비트코인 코어 소개

비트코인 코어 소개

- **코인의 지갑 파일을 생성하는 프로그램**
  - C#과 QT Framework로 제작된 오픈소스 프로그램 → https://github.com/bitcoin/bitcoin
  - 대부분의 많은 코인 코어가 비트코인 코어를 기반으로 제작 됨
- **코어가 있어야 코인 거래가 가능**
  - 코인 지갑은 코어 동기화가 모두 완료된 후 생성
- **코어 동기화는 날이 가면 갈수록 느려짐**
  - ~~지금이 코인판에 뛰어들 때!~~

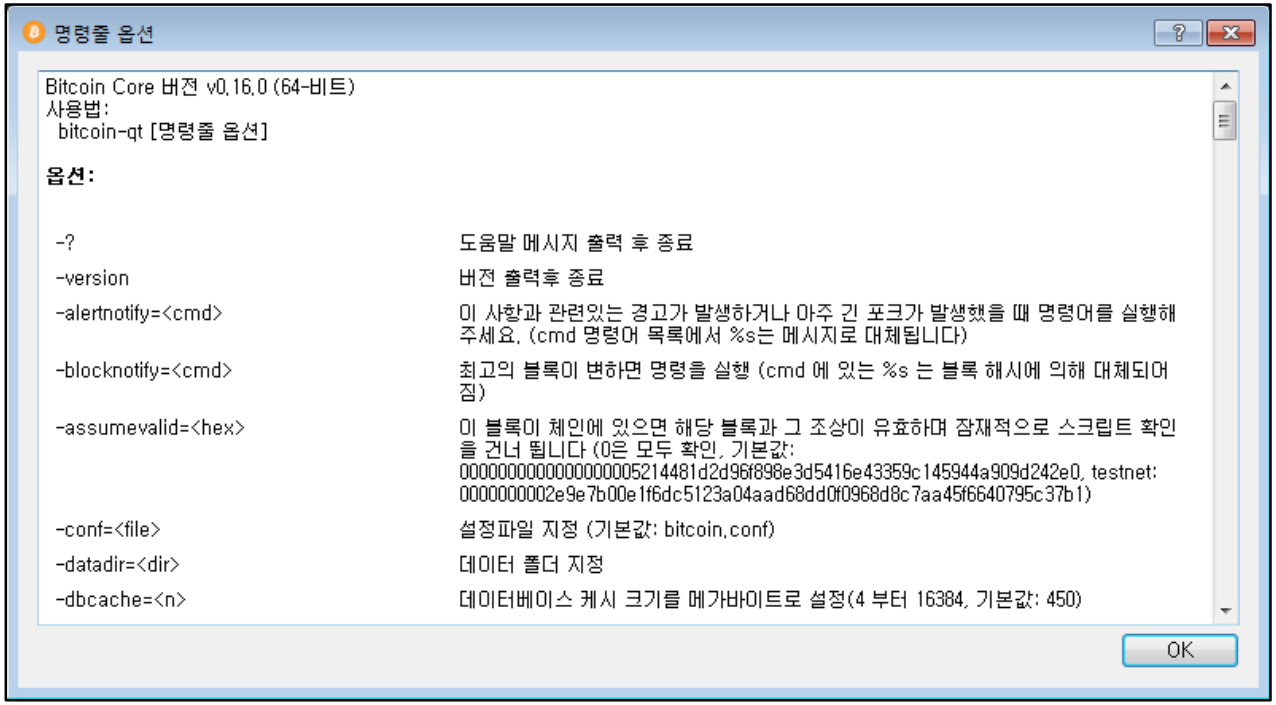
비트코인 코어 소개

- **지원 기능**
  - **지갑 관련 기능**
    - ✓ 지갑 백업
    - ✓ 지갑 암호화
    - ✓ 지갑 비밀번호 변경
  - **코인 관련 기능**
    - ✓ 코인 보내기
    - ✓ 코인 받기



비트코인 코어 소개

- **지원 기능**
  - **RPC 명령 기능**
    - ✓ BlockChain
    - ✓ Control
    - ✓ Generating
    - ✓ Mining
    - ✓ Network
    - ✓ Rawtransactions
    - ✓ Util
    - ✓ Wallet



비트코인 코어 소개

- **지원 기능**
  - **기타 기능**
    - ✓ 디버그 기능
    - ✓ 거래 내역
    - ✓ 메시지 서명/확인

비트코인 코어 소개

- **비트코인 코어 특징**
  - 패스워드가 설정된 지갑은 패스워드를 해제 할 수 없다.
  - 원격에서 명령을 내릴 수 있는 RPC 명령 기능을 제공한다.
  - **Peer 목록을 관리 함**
    - ✓ 블록을 서로 나눠 갖기 위해
  - Tor Network 지원
  - 설정 파일을 생성할 때 빈파일로 생성(?)
    - ✓ 왜…?
    - ✓ 그리고 GUI 설정이 bitcoin.conf 파일보다 우선시 됨(?)
      - 왜…?

비트코인 코어 소개

- **비트코인 코어 주요 파일**

위치	파일	설명
/	banlist.dat	피어 중 블록 교환을 하지 않을 IP 목록
	bitcoin.conf	비트코인 코어 설정 파일
	debug.log	**비트코인 코어 프로그램의 운영 로그**
	fee_estimates.dat	최소 거래 수수료를 계산하는데 필요한 통계치 저장
	mempool.dat	메모리 저장되어 있던 트랜잭션 정보
	peers.dat	블록을 교환하는 IP 목록
	.cookie	RPC 원격 명령 수행 시 인증 정보가 저장 됨 - 생성: RPC 인증 시 - 삭제: 비트코인 코어 종료 시
/blocks	blk[순서를 가지는 숫자].dat	블록체인 네트워크의 데이터
/wallets	**wallet.dat**	**개인키, 트랜잭션, 지갑 주소 등이 저장**
	db.log	wallet.dat 트랜잭션 로그, 트랜잭션 성공 후 내용 삭제 되서 항상 빈 파일로 밖에 안보임

암호화폐 관련 공격

암호화폐 관련 공격

- **Bitmessage**
  - 전달 메시지(블록) 인코딩 시 취약점 발생
    - ✓ Remote Code Execution 발생
  - 그러나 비트코인 코어에는 직접적인 영향을 미치지 않음

- **KeyLogging**
  - wallet.db의 패스워드를 키로깅
  - wallet.db의 패스워드가 유출되므로 가장 큰 영향을 미침
  - 단, 호스트에 접근할 수 있어야 함

암호화폐 관련 공격

- **Memory Hacking**
  - 비트코인 송금 주소를 클립보드에서 바꿔치기
    - ✓ http://blog.alyac.co.kr/1554
  - 이것도 결국엔 호스트에 접근할 수 있어야 함

암호화폐 관련 공격

- **대부분 블록체인 위/변조와 비트코인 이중지불 관련된 공격만 연구**
  - 블록체인의 블록을 위/변조 할 수 있는가?
    - ✓ 일부 조건에서는 가능
    - ✓ 현실에선 글쎄..
  - 코인을 보내고 받는 과정에서의 딜레이를 이용해 거래를 조작할 수 있다던데...

- **그래서 한번 찾아 봄!**
  - Local Exploit: 3개
    - ✓ wallet.db
    - ✓ bitcoin.conf
  - Remote Exploit: 1개(?) → Fuzzing으로 Crash만 찾은 상태

wallet.db 중심의
비트코인 코어 실험

wallet.db 중심의 비트코인 코어 실험

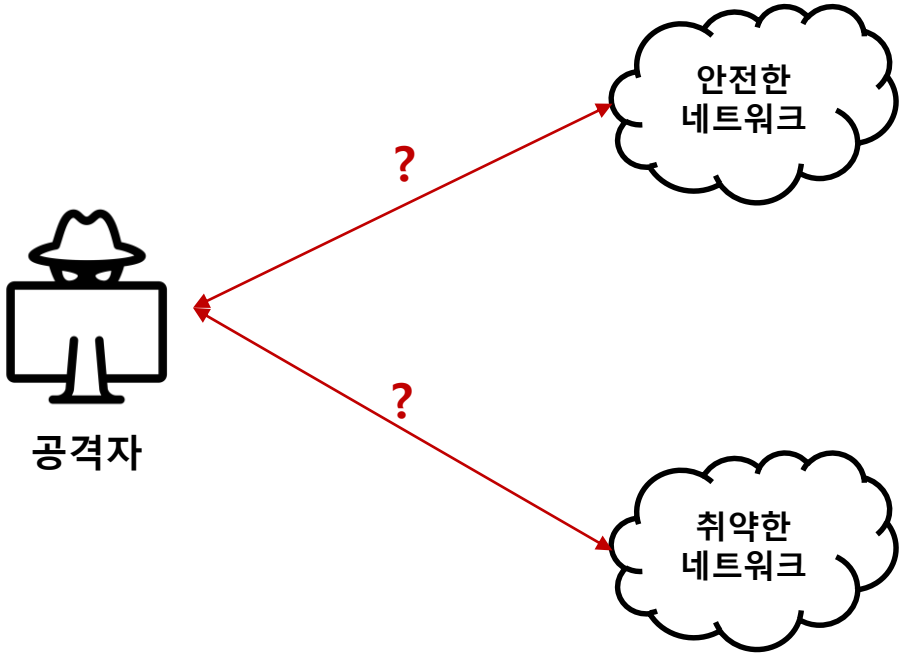
- **분석 대상**
  - Debug.log
  - 비트코인 코어의 파일 메타데이터 → 파일시스템

- **분석 방법**
  - 실제 비트코인을 보내고 받아 debug.log에 기록되는 로그들을 살펴 봄
    - ✓ 행위에 따른 로그 분석

    *** debug.log에 기록되는 시간은 UTC+0**
  - 거래가 이뤄질 때와 비트코인 코어 프로그램 사용 시 파일의 메타데이터 변화를 살펴봄

wallet.db 중심의 비트코인 코어 실험

- (호스트 접근 O) 호스트는 어느 네트워크에 연결 했을까?



wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 O) 호스트는 어느 네트워크에 연결 했을까?**
  - debug.log의 Receive 로그 분석
  - Receive 로그 Parameter
    - ✓ **User-Agent: 블록을 보낸 BitCoin Core의 명칭**
    - ✓ BitCore Version: BitCoin Core 버전
    - ✓ Blocks
    - ✓ **Us**
      - 8333 포트를 가진 IP는 블록을 전송하는 Peer
      - 40000~60000 포트를 가진 IP는 로컬 호스트 (혹은 로컬 게이트웨이)
    - ✓ Peer

wallet.db 중심의 비트코인 코어 실험

- (호스트 접근 O) 호스트는 어느 네트워크에 연결 했을까?

2017-12-18 23:27:59 receive version message: /Satoshi:0.11.2(bitcore)/: version 70002, blocks=500047, us=**61.102.68.20:50102**, peer=363
2017-12-18 23:29:32 receive version message: /Snoopy:0.2.1/: version 70001, blocks=0, us=[2001:0:9d38:6abd:872:24d0:c299:bbeb]:8333, peer=364
2017-12-18 23:34:36 receive version message: /Snoopy:0.2.1/: version 70001, blocks=0, us=[2001:0:9d38:6abd:872:24d0:c299:bbeb]:8333, peer=365
2017-12-18 23:39:38 receive version message: /Snoopy:0.2.1/: version 70001, blocks=0, us=[2001:0:9d38:6abd:872:24d0:c299:bbeb]:8333, peer=366
2017-12-18 23:41:05 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:41:05 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:41:08 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:41:10 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:41:11 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:42:13 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:44:13 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:44:49 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-18 23:46:04 socket recv error 소켓 연결에 에러가 발생했습니다. (10054)
2017-12-19 00:14:39 receive version message: /Satoshi:0.15.0/: version 70015, blocks=500051, us=[2001:0:9d38:6abd:2451:3435:950a:b106]:53710, peer=367
2017-12-19 00:14:41 receive version message: /Satoshi:0.15.1/: version 70015, blocks=500051, us=**106.245.78.249:53715**, peer=368

wallet.db 중심의 비트코인 코어 실험

- (호스트 접근 O) wallet.db 파일이 유출 되었을 가능성은?

wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 O) wallet.db 파일이 유출 되었을 가능성은?**
  - 유출 사실은 일반적인 정보유출사고 분석 관점에서 분석을 진행
  - **유출 되었다면 다른 곳에서 코인이 송금 됐을까? (가능할까?)**
    - ✓ 로컬에서 거래 했을 때와 지갑이 다른 곳으로 이동된 후 거래가 이뤄졌을 때 debug.log가 다름

(지갑 암호화 O/X)
로컬에서 거래가
이뤄졌을 경우

2018-02-19 06:57:22 **keypool** reserve 3002
2018-02-19 06:57:22 **Fee Calculation**: Fee:685 Bytes:226 Needed:685 Tgt:6 (requested 6) Reason:"Conservative Double Target longer horizon" Decay 0.99931: Estimation: (1979.93 - 3071.52) 97.25% 152.4/(152.4 0 mem 4.3 out) Fail: (0 - 1979.93) 55.85% 50.6/(50.6 0 mem 40.0 out)
2018-02-19 06:57:28 **CommitTransaction**:
CTransaction(hash=d43b32fd94, ver=2, vin.size=1, vout.size=2, nLockTime=509891)
CTxIn(COutPoint(59e48a7f77, 1), scriptSig=483045022100b0528e8ec631, nSequence=4294967294)
CScriptWitness()
CTxOut(nValue=0.00009315, scriptPubKey=76a914c9233fd0d8e04ea59ec53db2)
CTxOut(nValue=0.00363702, scriptPubKey=76a914ffd68d035fdf4403d3871fc4)
2018-02-19 06:57:28 keypool keep 3002
2018-02-19 06:57:28 **AddToWallet** d43b32fd946ab3d083c71f18317ad93cbc6ebc1df5b4c365faa23af3f434b698 new
2018-02-19 06:57:28 **AddToWallet** d43b32fd946ab3d083c71f18317ad93cbc6ebc1df5b4c365faa23af3f434b698
2018-02-19 06:57:28 **Relaying wtx** d43b32fd946ab3d083c71f18317ad93cbc6ebc1df5b4c365faa23af3f434b698

wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 O) wallet.db 파일이 유출 되었을 가능성은?**
  - 유출 사실은 일반적인 정보유출사고 분석 관점에서 분석을 진행
  - **유출 되었다면 다른 곳에서 코인이 송금 됐을까? (가능할까?)**
    - ✓ 로컬에서 거래 했을 때와 지갑이 다른 곳으로 이동된 후 거래가 이뤄졌을 때 debug.log가 다름

(지갑 암호화 X)
원격에서 거래가
이뤄졌을 경우

2018-02-19 07:23:41 **AddToWallet** 755ca3257ac7cd7b84a882945ab6841edb73e2d7a8a1e41779c36d3f6bf49031 new

wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 O) wallet.db 파일이 유출 되었을 가능성은?**
  - 유출 사실은 일반적인 정보유출사고 분석 관점에서 분석을 진행
  - **유출 되었다면 다른 곳에서 코인이 송금 됐을까? (가능할까?)**
    - ✓ 로컬에서 거래 했을 때와 지갑이 다른 곳으로 이동된 후 거래가 이뤄졌을 때 debug.log가 다름

(지갑 암호화 O)
원격에서 거래가
이뤄졌을 경우

2018-02-19 06:57:36 **AddToWalletIfInvolvingMe**: Detected a used keypool key, mark all keypool key up to this key as used
2018-02-19 06:57:36 **keypool** index 3002 removed
2018-02-19 06:57:36 **AddToWalletIfInvolvingMe**: Topping up keypool failed (locked wallet)
2018-02-19 06:57:36 **AddToWallet** d43b32fd946ab3d083c71f18317ad93cbc6ebc1df5b4c365faa23af3f434b698 new
2018-02-19 06:58:58 **AddToWallet** d43b32fd946ab3d083c71f18317ad93cbc6ebc1df5b4c365faa23af3f434b698 update

wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 O) wallet.db 파일은 암호화가 되어 있었을까?**

OR

  - 지갑 암호화 기능을 수행하면 이에 해당하는 로그가 기록 됨
  - **지갑 암호화 후, 비트코인 코어는 반드시 종료 됨**

```
2018-02-19 08:51:21 Encrypting Wallet with an nDeriveIterations of 248916
2018-02-19 08:51:23 keypool added 2000 keys (1000 internal), size=2000 (1000 internal)
2018-02-19 08:51:23 CWallet::NewKeyPool rewrote keypool
2018-02-19 08:51:23 CDB::Rewrite: Rewriting wallet.dat...
2018-02-19 08:51:26 tor: Thread interrupt
2018-02-19 08:51:26 scheduler thread interrupt
2018-02-19 08:51:26 addcon thread exit
2018-02-19 08:51:26 torcontrol thread exit
2018-02-19 08:51:26 opencon thread exit
2018-02-19 08:51:26 Shutdown: In progress...
2018-02-19 08:51:26 net thread exit
2018-02-19 08:51:26 msghand thread exit
2018-02-19 08:51:26 Dumped mempool: 0.000501s to copy, 0.061559s to dump
2018-02-19 08:51:26 Shutdown: done
```

wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 O) wallet.db 파일은 처음부터 공격자의 지갑 파일이지 않았을까?**
  - 지갑 생성 기록과 지갑 파일의 파일시스템 메타데이터를 비교

[지갑 생성 시]	[기존 지갑 로드 시]
2017-11-21 08:58:42 init message: 지갑을 불러오는 중... 2017-11-21 08:58:42 nFileVersion = 150001 2017-11-21 08:58:42 Keys: 0 plaintext, 0 encrypted, 0 w/ metadata, 0 total 2017-11-21 08:58:42 Performing wallet upgrade to 60000 2017-11-21 08:58:44 **keypool added 2000 keys** (1000 internal), size=2000 (1000 internal) 2017-11-21 08:58:44 **keypool reserve 1** 2017-11-21 08:58:44 **keypool keep 1** 2017-11-21 08:58:44 wallet 2066ms 2017-11-21 08:58:44 **keypool added 1 keys** (0 internal), size=2000 (1000 internal) 2017-11-21 08:58:44 setKeyPool.size() = 2000	2017-11-22 03:05:50 init message: 지갑을 불러오는 중... 2017-11-22 03:05:50 nFileVersion = 150001 2017-11-22 03:05:50 Keys: 2002 plaintext, 0 encrypted, 2002 w/ metadata, 2002 total 2017-11-22 03:05:50 wallet 125ms 2017-11-22 03:05:50 setKeyPool.size() = 2000

- **wallet.db 파일의 MACB 중 MA만 수시로 변경 됨**
  - ✓ B는 파일을 옮기거나 덮어 쓰지 않는 이상 변경되지 않음

wallet.db 중심의 비트코인 코어 실험

- **(호스트 접근 X) 비트코인 코어에 원격 취약점이 존재할까?**
  - 현재까지 보고된 RCE 취약점은 없었음

- **(호스트 접근 X) 원격에서 wallet.db 파일을 가져가거나, 거래를 일으킬 수 있는 방법은?**
  - RPC 콘솔을 이용하면 원격에서 로컬 비트코인 코어의 지갑에서 코인을 송금할 수 있음
    - ✓ **단, 암호화된 지갑의 경우 패스워드가 필요함!**
    - ✓ 그리고 RPC 설정을 bitcoin.conf 파일에서 별도로 설정을 해줘야 함
      - 호스트 접근이 한번 필요한 조건
      - 서버, 아이디, 패스워드 설정 필요
      - bitcoin.conf 파일을 기본으로 생성되어 있지 않음 (사용자가 별도로 생성해야 함)

wallet.db 중심의 비트코인 코어 실험

- (기타) wallet.db 파일의 패스워드 변경이 일어나면?

2018-02-19 08:58:13 **Wallet passphrase changed** to an nDeriveIterations of 273861

- (기타) 비트코인 코어의 실행과 종료

2017-11-21 02:59:10 **Bitcoin version v0.15.0.1**

[비트코인 코어 시작]

2017-11-21 08:57:42 **Shutdown: done**

[비트코인 코어 종료]

케이스 적용

- **분석 초점 설정 → 만약, 호스트에 접근 했다면?!**
  - 호스트는 어느 네트워크에 연결 했을까? → **알 수 있었음!**
  - wallet.db 파일이 유출되었을 가능성은?

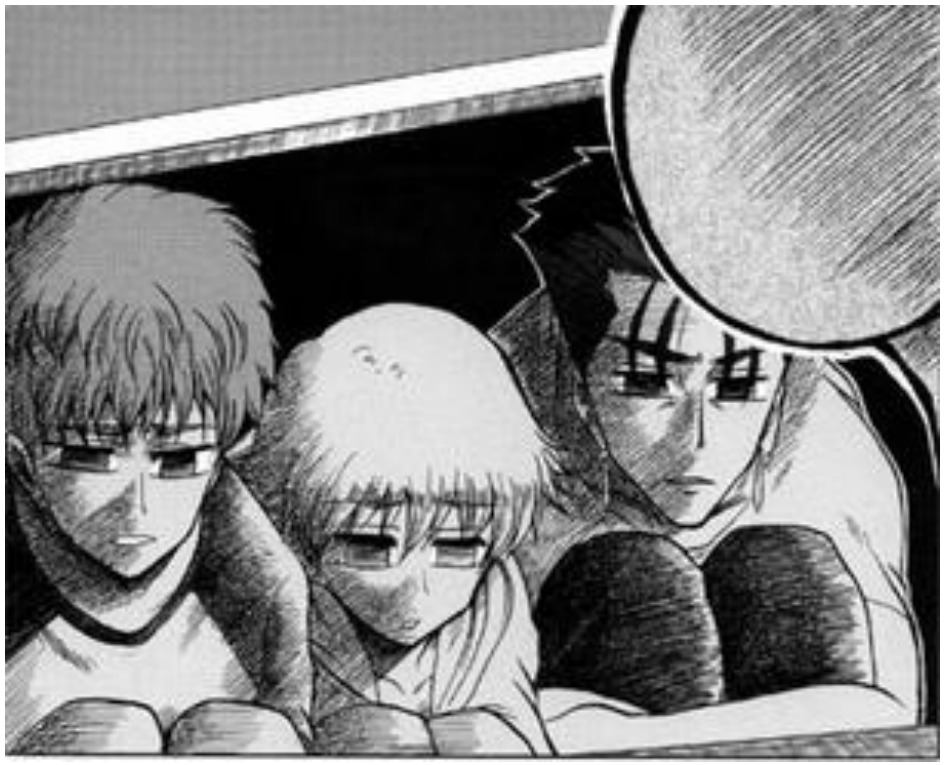
    → **있음, 지갑 파일에 비밀번호가 없을 때 원격에서 거래할 때의 로그가 다수 존재함**

    ✓ 유출되었다면 다른 곳에서 코인이 송금됐을까? (가능할까?)
  - wallet.db 파일은 암호화(비밀번호)가 되어 있었을까? → **비밀번호 설정 되어 있었음!**
  - wallet.db는 처음부터 공격자의 지갑 파일이지 않았을까? → **아니었음!**

- **분석 초점 설정 → 만약, 호스트에 접근하지 않았다면?!**
  - 비트코인 코어에 원격 취약점이 존재할까? → **존재할 수 있지만 현실 가능성 1%**
  - 원격에서 wallet.db 파일을 가져가거나, 거래를 일으킬 수 있는 방법은? → **현재까지는 없는걸로..**

케이스 적용

- **결론은, 공격자는 노트북에 접근해 비밀번호가 걸리지 않은 지갑 파일을 가져 갔다는 이야기인데...**
  - 가져갈 수 있는 시간이 대략 20분



- **어떻게 가져간 걸까 ——?**
  - 윈도우 취약점?
  - 악성코드?
  - ...?!

향후 실험 주제

향후 실험 주제

- **메모리를 대상으로**
  - **wallet.db 패스워드 찾아보기**
    - ✓ 키보드 입력 버퍼에 남아 있을 것으로 추정
  - **지갑 주소 바꿔치기**
    - ✓ 이전에 우리은행 악성코드 방식과 유사하게 코인 전송 직후에 메모리에서 상대방 지갑 주소를 공격자의 지갑주소로 변경
  - **복호화된 지갑 파일 추출**
    - ✓ 지갑의 파일이 크지 않아 메모리에 지갑 파일 전체가 load 될 것 같음

Question and Answer