

# WannaCry 랜섬웨어 공격

10조 김지현 박서윤 정세진



# 목차

1. WannaCry 랜섬웨어 공격 개요
2. WannaCry 버전별 발전 과정 및 주요 변화
3. 감염 경로와 피해 사례
4. 온체인 자금 추적
5. 자금 세탁 및 현금화 과정
6. 배후와 기술적/법적 대응
7. 결론 및 시사점

# WannaCry 랜섬웨어 공격



# 사건 개요

- 2017년 5월 12일, 150개국 20만 대 이상의 컴퓨터 감염
  - SMB 프로토콜의 취약점을 악용한 대규모 사이버 공격
  - 비트코인을 대가로 데이터 복구를 요구

# 랜섬웨어 특징

- 네트워크 웜(Worm) 방식으로 전파
  - 빠른 확산 속도와 큰 피해 규모

# WannaCry 버전 및 주요 특징

1

# WannaCry 1.0

초기 버전으로, Kill Switch 도메인 발견으로 확산이 차단

2

# WannaCry 2.0

Kill Switch가 제거되어 보안 패치 미적용 시스템에서 지속적으로 확산

3

# 감염 시 주요 특징

- 파일 암호화 및 금전 요구
  - 시간에 따른 요구 금액 증가
  - 신원 보호 불가능
  - 복호화 실패 사례 다수

## Wannacry 1.0

nictar (cran WannaCry: ((@file / (lost @electool))  
 rfections = [!ble:  
 der tier (amendment consuetion all0),  
 satien as criticise (treez / (cm)),  
 datien. f'xallies.  
 Blaer lat = Lattee:  
 der leek: im & **L**eave (lecting (imb (cad))),  
 der leat = '(lose Lettere &mplo (ice0)). );  
 der leek:  
 der tler (toller (carikel));  
 new Lam: (lat **U**ccusur) = ),  
 new dae: / (lettificier (es) (ort (al));  
 deat (soerclere deal (ection) / **now** = / (brilidg);  
 new etier ((. **cyre0**),  
 der leek / c **Getidission**)  
 der leat = 'airfect Mat (sact, (el));  
 ).  
 derly:  
 flerrine: z());  
 der lte: (lont (ent));  
 der tiae: & comalction (one));  
 der tiam: (/ ilieb);  
 der eler # **ansle**/ -car (or/ear (al));  
 der clear = be cerilister Abclop);  
 new );  
 ),  
 Exlected the **cerored**;  
 car leear = chal};  
 car leat (feet C6obitcat emcer/leay);  
 & der (**Ab**ortion:  
 new leut (oill: = (305,11)).  
 new leut: Elm illiny ();  
 new dan: centibition (teririerstierion, catly);  
 new lam: = :al (ectal));  
 ner leat (in al and(cer madion, (el));  
 )).  
 der tiae: (falle (oatll));  
 der lse: (omsticke (hieb, (k)rb); (coset; cm)),  
 ner (mantiat imriation for the (aleiou));  
 ).  
 dan: (dokt ecticy (.  
 der tlier (lection:  
 der tiae (terivatier leeterestierion (ly));  
 der clear (**2680** (slckey);  
 der tter (lasy (tial));  
 ).  
 ctder lky:  
 der tiae: (le ols aut tenlor (leal));  
 ).  
 der eres:  
 der tlier (lar is (ar (ben/len));  
 der (mattior cilementierens/correction /le);  
 ).  
 der tter for elied:  
 der tiae = htlion,Se (eal),  
 der le alimit (cader Cerler Interdatitator());  
 ).

Wannacry 2.0

asterachov: (Comics;  
 author (entertainer:emitting ~~december~~ will);  
 artist ~~met~~ criticizes best/(com));  
 artist: /"selfies";  
 character = Callie;  
 war time: war ~~in~~ **America** (territory (e; (e0));  
 war click: in ((war location ~~not~~ listed));  
 dear use:  
 Com tiles: (titles (cared));  
 dear ~~law~~ = **troop** );  
 dear ~~law~~ (law/ (erictor (at((el, el));  
 dear (cannot law/call/ection/ **path**) = (law/lo  
 dear ~~law~~ (ettice:  
 dear lev: /r **GulFrassoso**  
 dear ~~law~~ = (refers ~~not~~ ((fact, Gob));  
 ).  
 Bartly:  
 Fidetiles: **ad**).  
 der tier: ((ant (ent));  
 der class: **Geonhition** (en0));  
 der clew: (elbow);  
 der other **WUllms/Letericarroll**);  
 der tiles: ((reccisies **#blow**);  
 ).  
 ).  
**(start an Disease)**:  
 der tiles = bbs;  
 far lacer (Ent (SNblet, tarconclition);  
**dest** (CDDirection:  
 new dev: (bill: = EBB, 1());  
 new dev: (far tiles; ());  
 new day: commitment (lacer/Perfection, tel  
 near ~~law~~ = (at (el));  
 new item: (far ~~discipline~~ (el));  
 ).  
 der tiles: (inkles (smill));  
 far ~~law~~: (elilial: (horrley, toct/one);  
 user:commitin: (raction in (orchard (llor  
 ).  
 least (real (altin);  
 dest (Amification:  
 dev class: ((enstlerfer ericeriestertion);  
 der team: (**EBO** (ilella));  
 der other easy (elal));  
 ).  
 Carter tiles:  
 cast four = in color (aw, tom (esla));  
 ).  
 asterion:  
 der tiles: (far ~~law~~ (steal/les(b));  
**dest** ~~law~~: ((let ictler ~~conierion~~ (lere (  
 ).  
 der ~~law~~ (r ~~galle~~;  
 der ~~law~~ = llcine; => (el);  
 user (cm: ~~salt~~ ~~anobtiserior~~ iocctletier (es  
 ).  
 © Dan Rossoff Licensing

# 감염 경로와 피해 사례



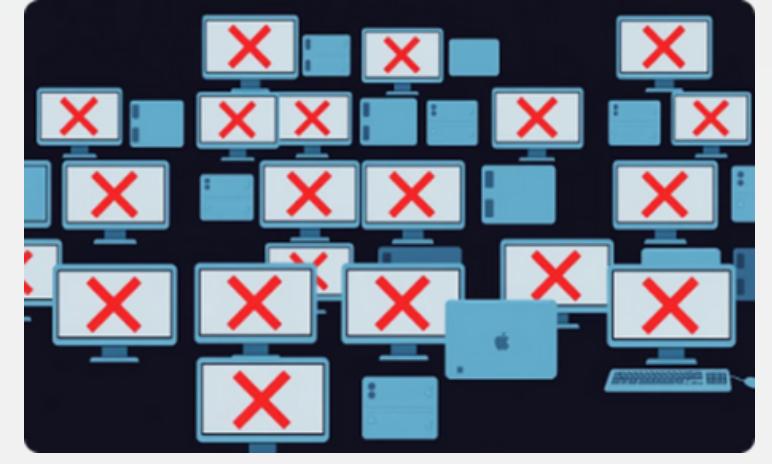
영국 NHS 마비



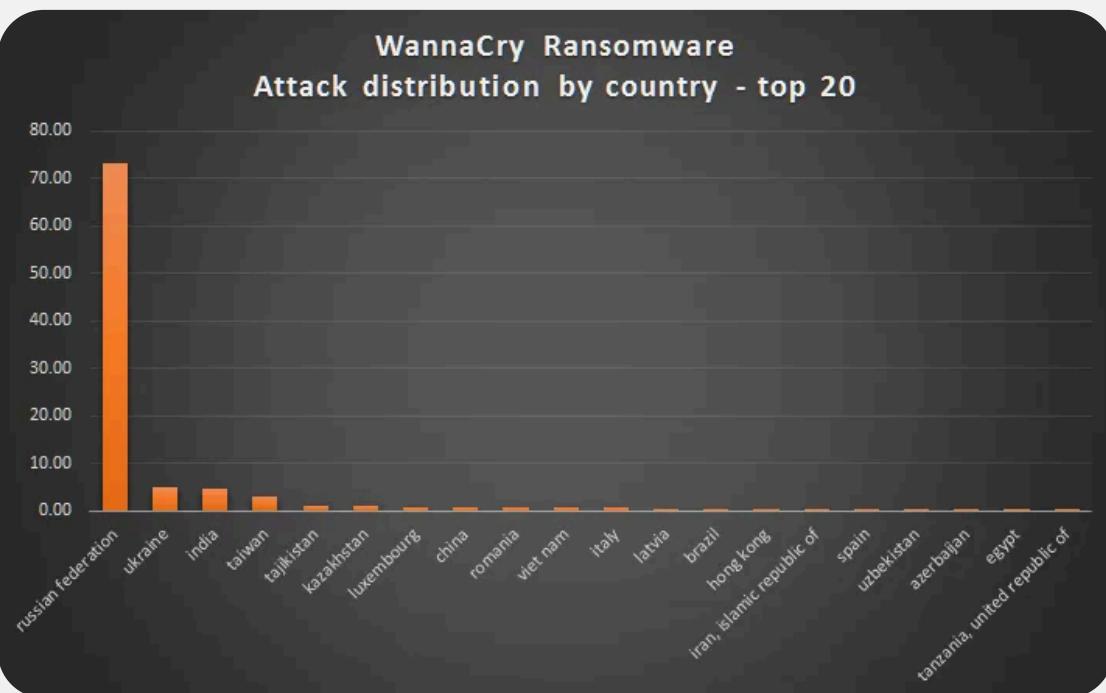
독일 철도청 피해



스페인 Telefonica,  
러시아 Megafon  
시스템 장애



중국 대학 시스템 감염

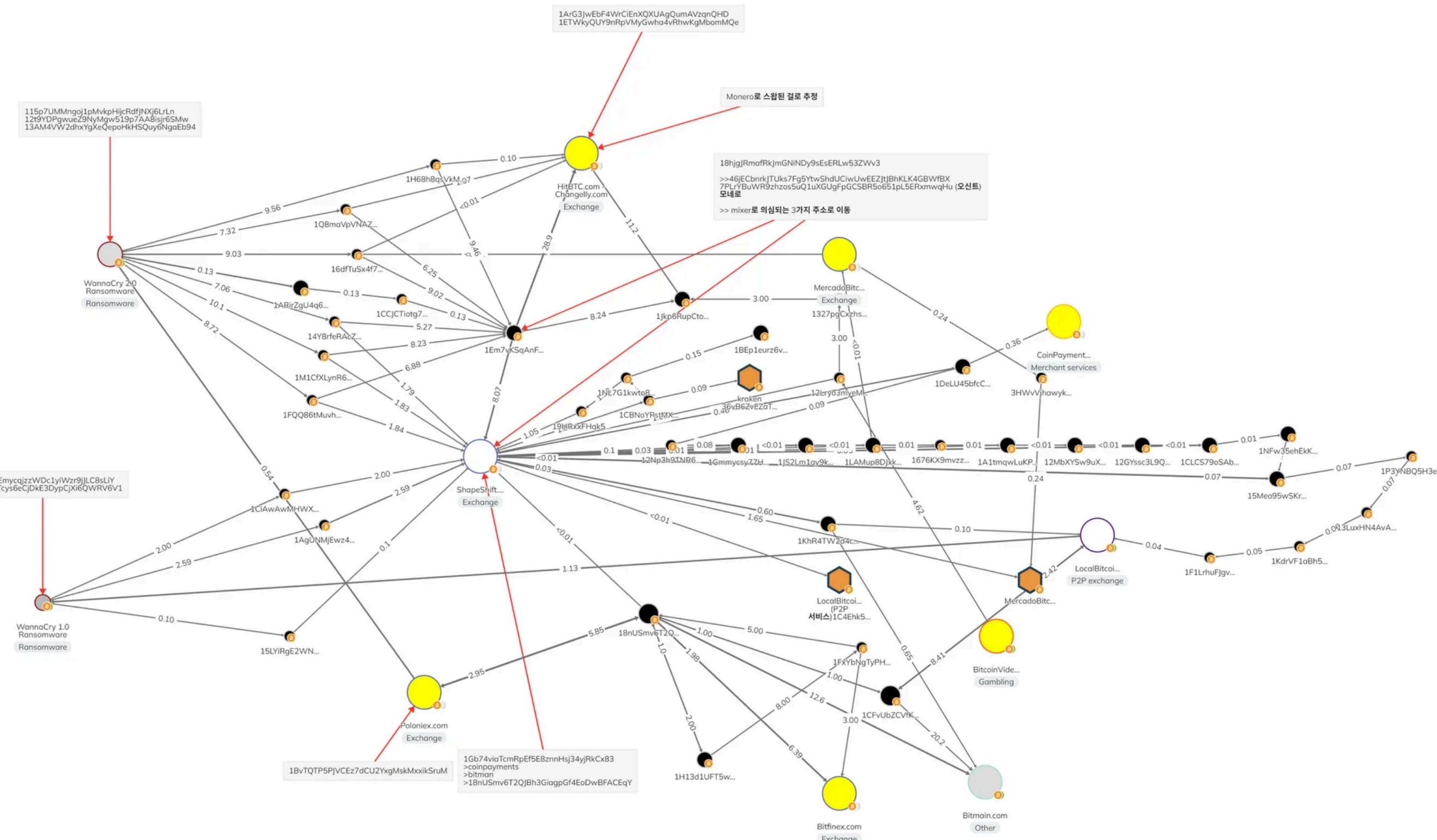


상위 20개 피해 국가



전 세계적 피해

# 온체인 자금 추적



# WannaCry 1.0 자금 흐름 분석

## 주요 주소

1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY  
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

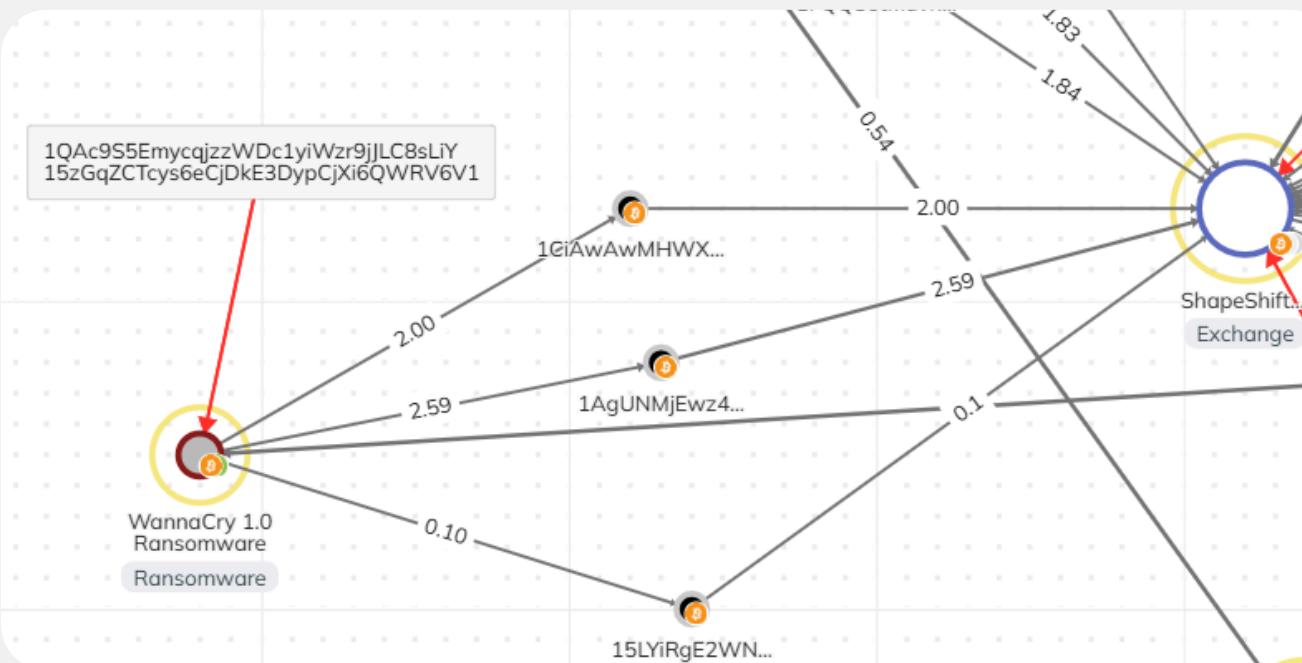
지출 거래의 change 주소:  
13JfxwBKfL8VcXgjEuVFKRjh44EvL3Lee4

1

WannaCry 1.0 Ransomware				
● Ransomware				
Cluster ID	Balance	0.175769 BTC	Transfers	29
1QAc9S5EmycqjzzWDc1yiWz...	Sent	4.687646 BTC	Withdrawals	3
Activity	Received	4.866660 BTC	Deposits	26
2017년 3월 31일 - 2020년 8월 11일	Total fees	0.003244 BTC	Addresses	3

Overview Counterparties Transfers Addresses OSINT

Address	Balance	Transactions
13JfxwBKfL8VcXgjEuVFKRjh44EvL3Lee4	0.00	2
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1	0.175769	17
1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY	0.00	14



2

## ShapeShift 이동

WannaCry 1.0 클러스터링 된 약 4.7 BTC:  
2017년 7월 19일 - 20일에 걸쳐 세 개의 주소로 이동된 후  
ShapeShift로 이동

# WannaCry 1.0 자금 흐름 분석

## Monero 스왑

ShapeShift에서 Monero로 스왑

18t3rC2d1HRwPdtRb9RvyMi6MsMda9orK9 sent 1.99980498 BTC (126.34726205 XMR)  
© OSINT

1CwJEUiPCo12zzwjxczVw5EXEa9T9pNn8k sent 0.09968241 BTC (6.326280 XMR)  
© OSINT

1936uzRAPsou9Gi4oNpTG8Hr43fUenSeX7 sent 1.08722198 BTC (68.733900 XMR)  
© OSINT

1DtGS1jRSxZH26fidS18NZ6tRQpYJxiust sent 1.5 BTC (94.85547892 XMR) to 49rJThdEQrjBiBKwvGDNpH28uWstwAMvVSYez3qYjkNWH4A8CbKRYnU82Hzmrs2a31NyDEb59hC6SBTekl  
© OSINT

**Summary**

Category	Shapeshift.io
Label	1DtGS1jRSxZH26fidS18NZ6tRQpYJxiust sent 1.5 BTC (94.85547892 XMR) to 49rJThdEQrjBiBKwvGDNpH28uWstwAMvVSYez3qYjkNWH4A8CbKRYnU82Hzmrs2a31NyDEb59hC6SBTekl
Time	none
Addresses found	1
URL	<a href="https://shapeshift.io/txStat/1DtGS1jRSxZH26fidS18NZ6tRQpYJxiust">https://shapeshift.io/txStat/1DtGS1jRSxZH26fidS18NZ6tRQpYJxiust</a>

**Text** Addresses

```
[{"status": "complete", "address": "1DtGS1jRSxZH26fidS18NZ6tRQpYJxiust", "withdraw": "49rJThdEQrjBiBKwvGDNpH28uWstwAMvVSYez3qYjkNWH4A8CbKRYnU82Hzmrs2a31NyDEb59hC6SBTekl", "incomingCoin": 1.5, "incomingType": "BTC", "outgoingCoin": 94.85547892, "outgoingType": "XMR", "transaction": "7f28d279cd01e544"}]
```

3



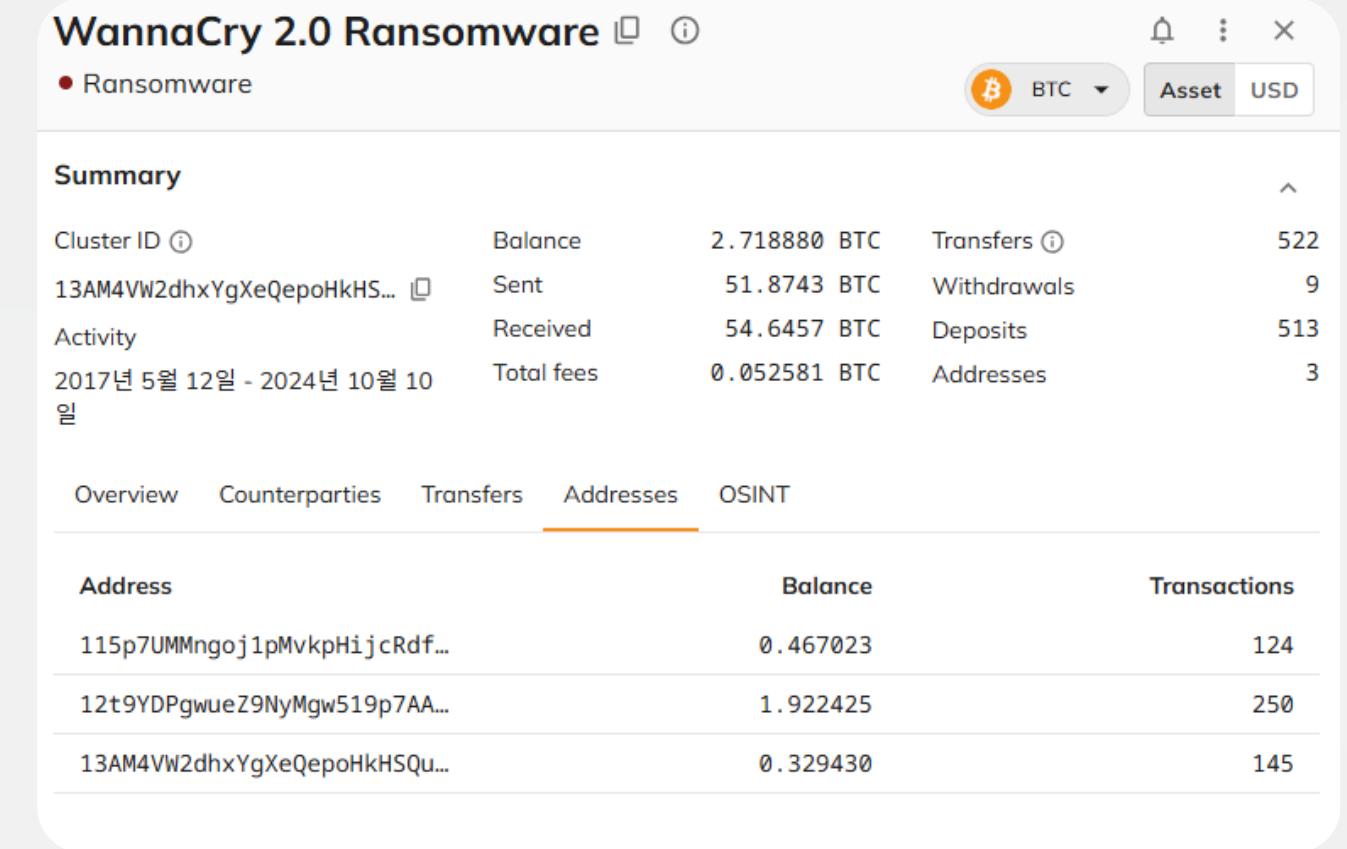
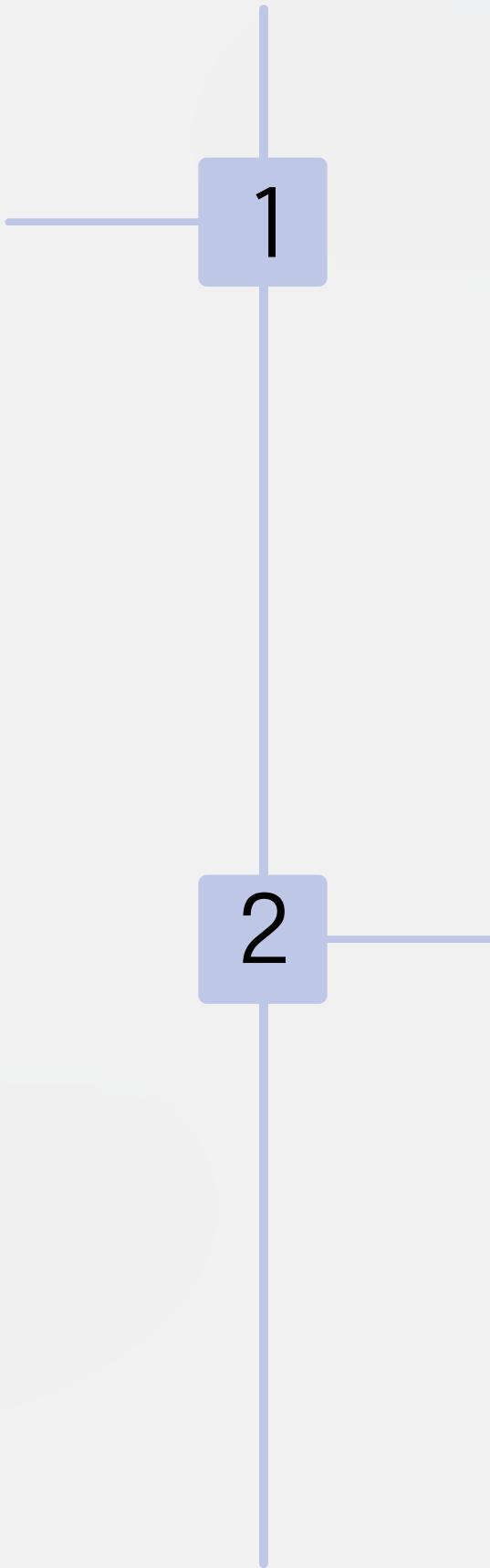
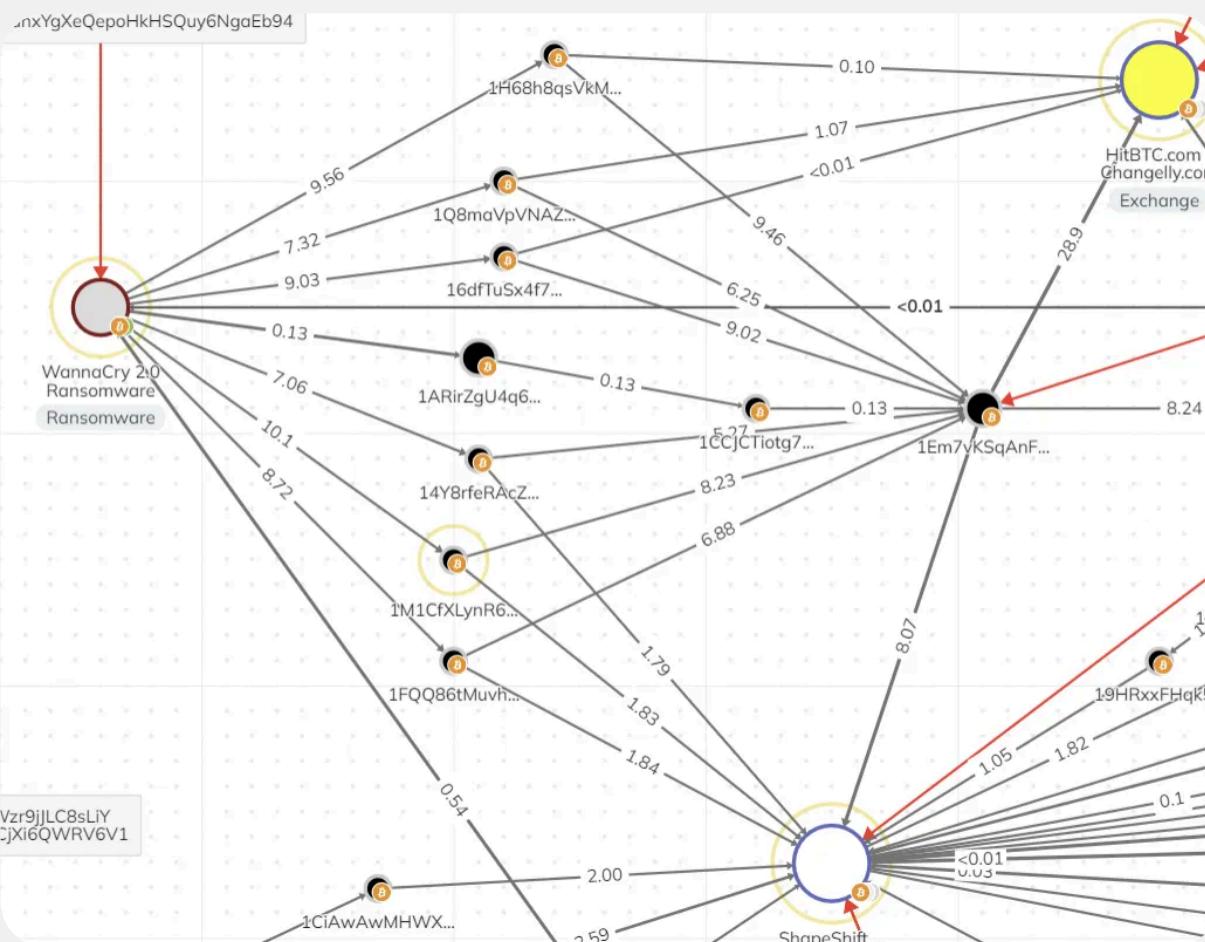
## 최종 목적지

49rJThdEQrjBiBKwvGDNpH28uWstwAMvVSYez3qYjkNWH4A8CbKRYnU82Hzmrs2a31NyDEb59hC6SBTekl  
CbKRYnU82Hzmrs2a31NyDEb59hC6SBTeklUsdgsMm28QxdDH

# WannaCry 2.0 자금 흐름 분석

주요 주소

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw  
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94



## ShapeShift 및 Changelly 이동

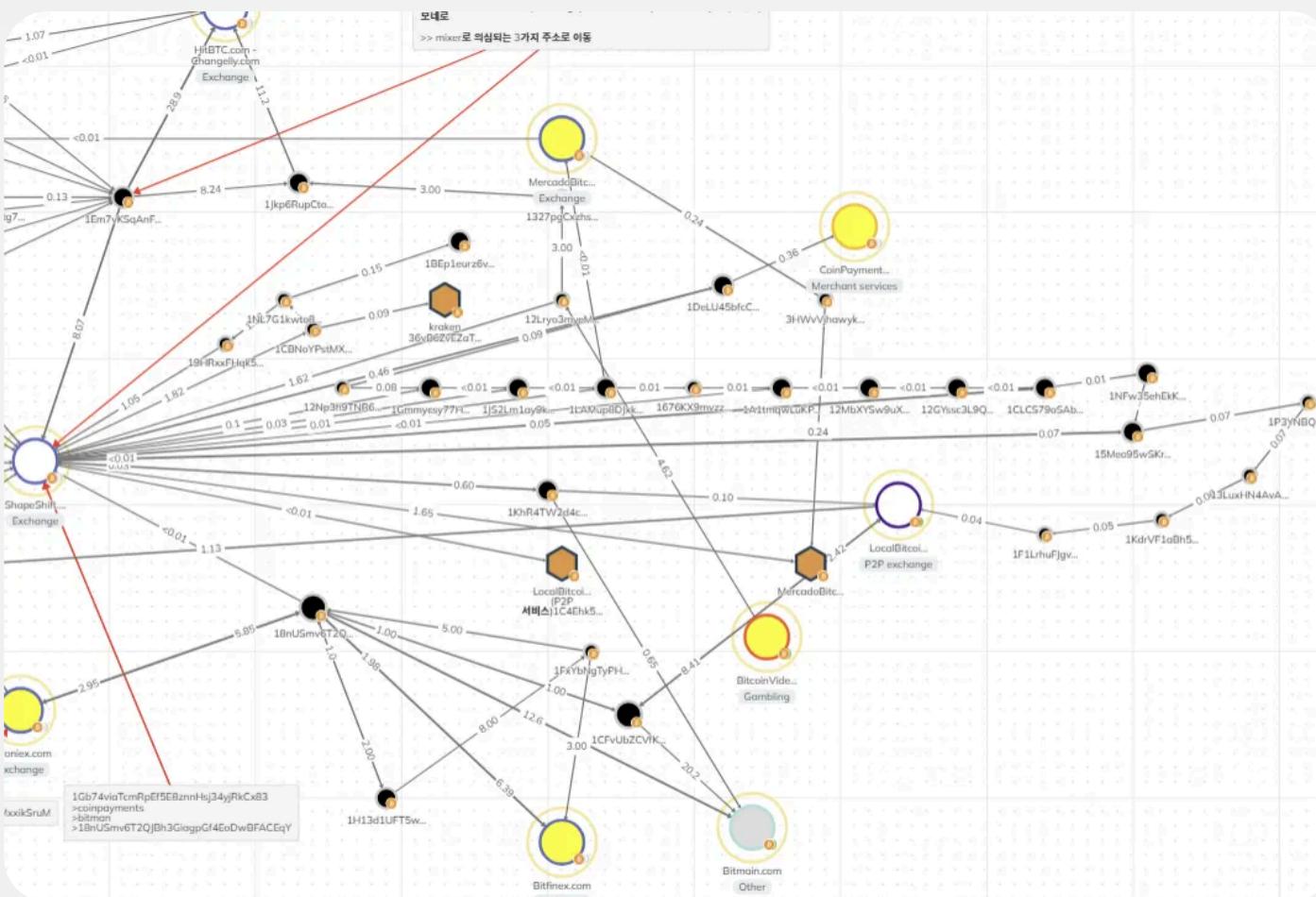
WannaCry 2.0으로 수집된 52 BTC는 여러 주소로 송신된 후 ShapeShift와 Changelly 거래소로 이동  
대부분 1Em7vKSqAnFMpejf3fSPSQdxrx99ma856h 주소로 집결된 후 두 개의 거래소로 이동

# WannaCry 2.0 자금 흐름 분석

# Monero 스왑

- ShapeShift로 이동한 13.53 BTC는 모두 Monero로 스왑
  - Changelly로 이동한 38.33 BTC 역시 대부분 Monero로 스왑된 것으로 추정

3

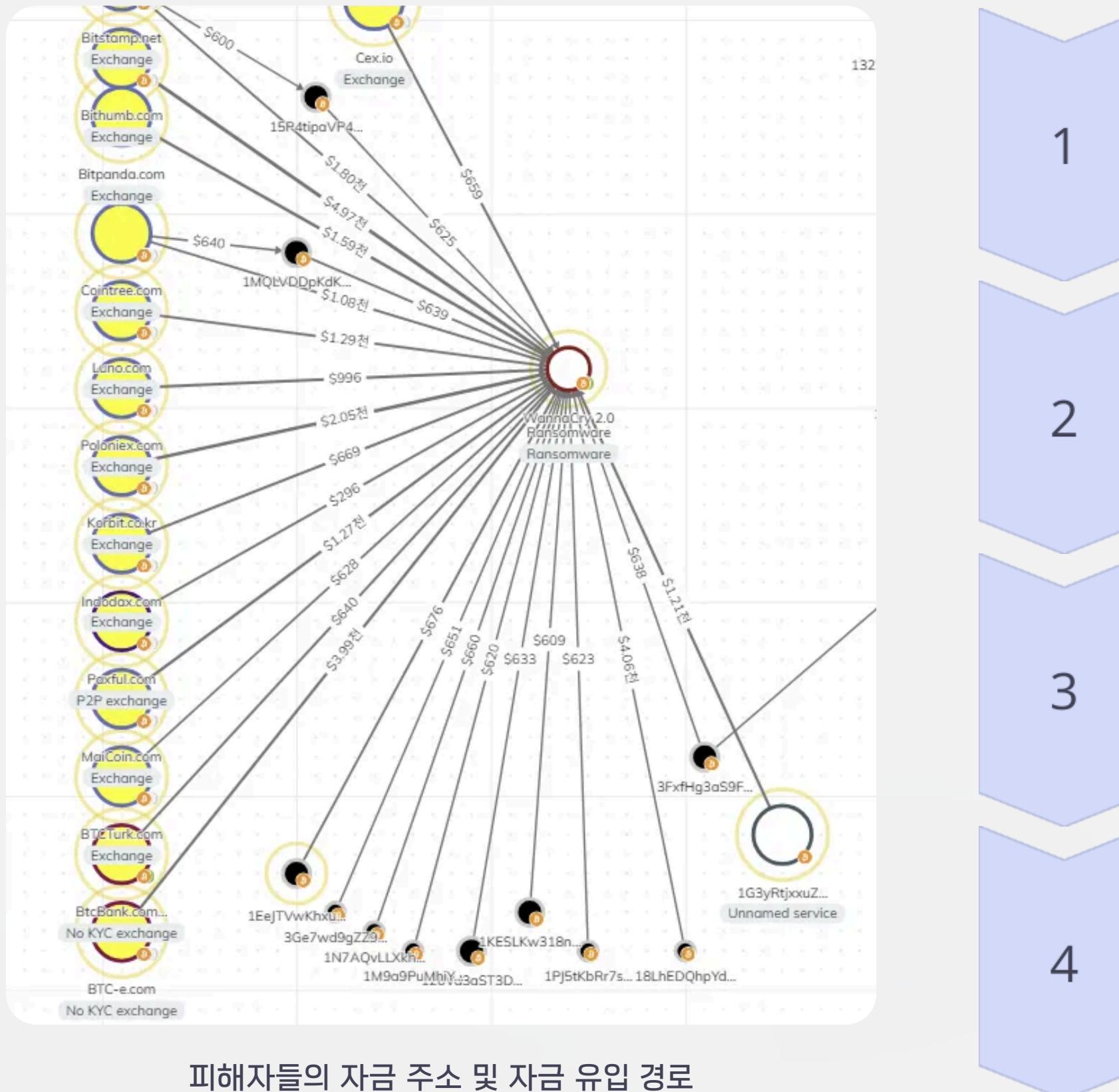


2017-08-03 09:53:03 (2017-08-03 09:58:07)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.73614387 BTC</span>	6377c5c8db1d72f09...34a61b8e853a8270
prev 9.462641 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.7359328 BTC next 7.72649713 BTC next
2017-08-03 09:42:48 (2017-08-03 09:47:04)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.67870289 BTC</span>	79aa721be73b5f854...2132d810d41dae91
prev 5.26702985 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.67849182 BTC next 3.58832696 BTC next
2017-08-03 09:36:49 (2017-08-03 09:37:20)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.80450345 BTC</span>	95d36a6926639ba50...a1e8d8be1b13cb40
prev 9.02445824 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.80429238 BTC next 7.21995479 BTC next
2017-08-03 09:26:32 (2017-08-03 09:27:33)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.03844 BTC</span>	3b11006791e57cd3d...dc87fc7c3aff9689
prev 3.21521353 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.03822893 BTC next 2.17677353 BTC next
2017-08-03 09:18:25 (2017-08-03 09:21:03)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.81640947 BTC</span>	f7866ba8bea329e80...2f977eb71664841
prev 5.031623 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.8161984 BTC next 3.21521353 BTC next
2017-08-03 08:15:53 (2017-08-03 08:28:51)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.79250367 BTC</span>	fd77ae2b63adbac9e...efa4375d9f7da78a
prev 7.05953352 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.7922925 BTC next 5.26702985 BTC next
2017-08-03 07:56:51 (2017-08-03 08:05:33)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.83289567 BTC</span>	b0f788ea6f24dbf7d...05ffac34145a5247
prev 10.05800019 BTC	WannaCry 2.0 peeling ↗ ShapeShift BTC to XMR ⓘ WannaCry 2.0 peeling ↘	1.8326845 BTC next 8.22510452 BTC next
2017-08-03 07:44:14 (2017-08-03 07:51:04)	<span style="background-color: red; border-radius: 5px; padding: 2px;">-1.92761448 BTC</span>	340b14c7a7857a96f...0df1a35688845d16

## 2차 이동

그 외 일부 비트코인은 여러 트랜잭션을 거쳐 소액으로 분할하여  
MercadoBitcoin, Bittrex, LocalBitcoins, CoinPayment 등  
다양한 거래소 및 P2P거래로 송금

# 자금 세탁 및 현금화 과정



## Chain-hopping

암호화폐를 다른 암호화폐로 교환하여 추적을 어렵게 만듦

## Monero 전환

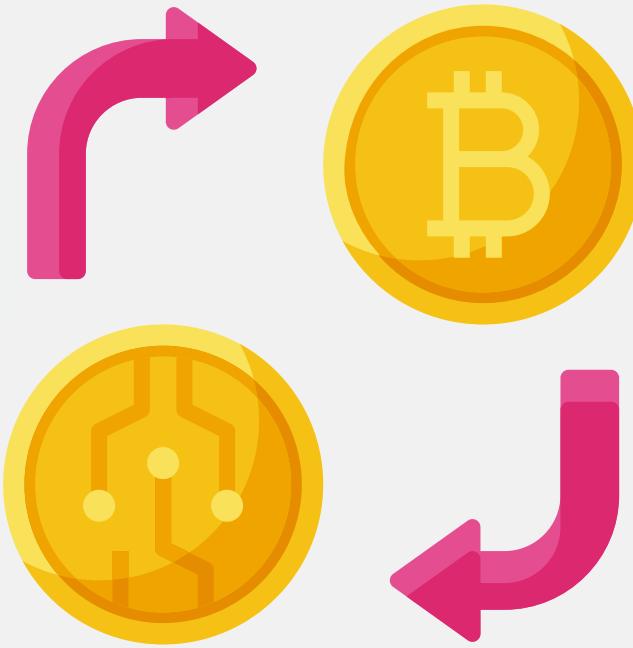
익명성이 높은 Monero로 전환하여 추적을 더욱 어렵게

## 소액 분할

자금을 소액으로 분할하여 다양한 거래소로 송금

## 현금화

# ShapeShift와 Changelly 사용 이유



## 코인 스왑 가능

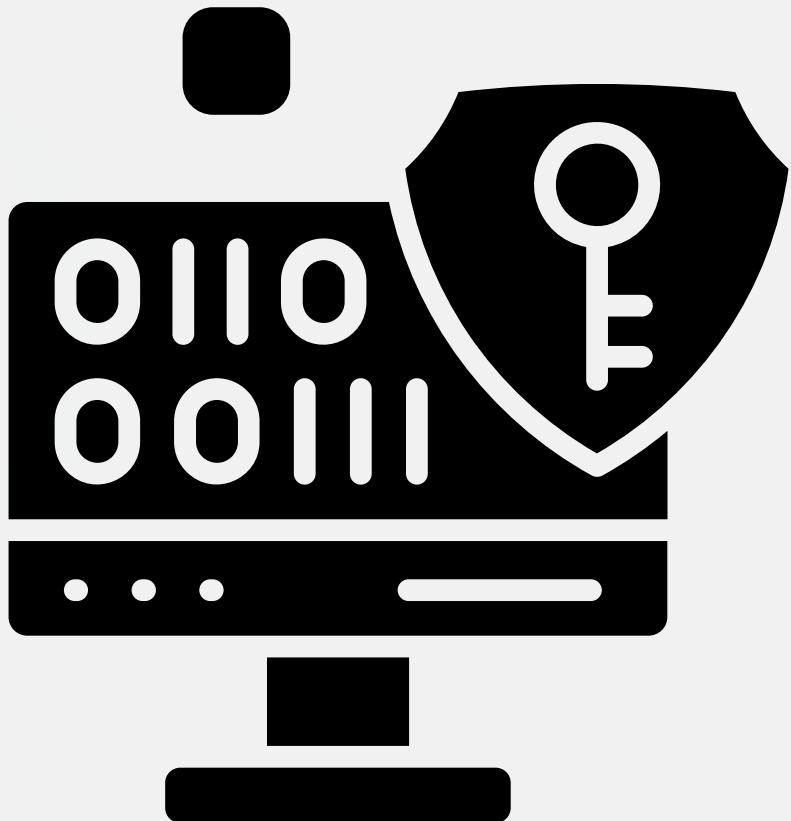
비트코인을 다른 암호화폐로 손쉽게  
교환 가능



## 낮은 인증 절차

- KYC(신원 인증) 절차가 없거나  
매우 간소화되어 익명성이 보장됨
- 당시 거래소는 사용자 정보를 요구하지 않음

# 체인호핑 (Chain-hopping) 기법



## 난독화 방식

암호화폐를 다른 암호화폐로  
교환하며 자금 흐름을 숨기는 방법



## 추적 방지

다양한 암호화폐를 연속으로 교환해  
자금의 출처와 목적지를 알아내기 어렵게 만듦

# Monero 전환 이유



## 익명성 중시 암호화폐

Monero는 사용자 거래 내역이 공개되지 않아 흔적을 남기지 않음



## 추적 어려움

고도로 강화된 프라이버시 기술로  
자금 흐름을 식별 불가



## 공격자들이 선호

랜섬웨어 공격에서 자주 사용되는  
암호화폐

# 배후 및 기술적/법적 대응



라자루스 그룹(북한 연계 해커 조직) 추정  
자금 확보 / 경제 제재 우회 목적

## 기술적 연계 증거

- WannaCry 코드와 Lazarus 도구 간 공통 코드 발견
- SSL 구현에서 75개 암호화 시퀀스 일치
- WannaCry 변종 감염 시스템에서 Lazarus 독점 도구 확인
- 공격에 사용된 IP 주소가 중국에서 북한 정찰총국이 사용하는 범위에 해당

## 공격 도구의 증거

- EternalBlue 취약점(미 NSA 유출 기술) 활용

# 배후 및 기술적/법적 대응



## 기술적/법적 대응

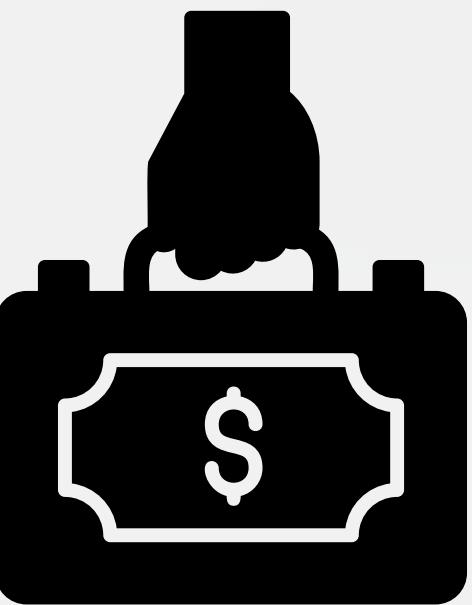
- Kill Switch 도메인 발견
- WannaKey 및 Wanakiwi 복구 도구 개발
- MS17-010 긴급 보안 패치 배포
- 국제적 협력을 통한 보안 강화
- 미국 법무부는 라자루스 소속 박진혁에 대한 공식 기소 발표

# 결론 및 시사점



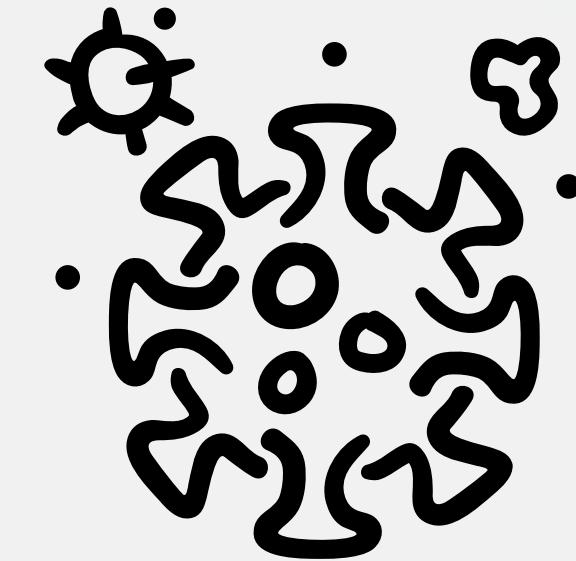
## 자금 세탁 수법 분석

- Chain-hopping
- 소액 분할
- 익명 거래소 활용



## 자금 흐름 분석

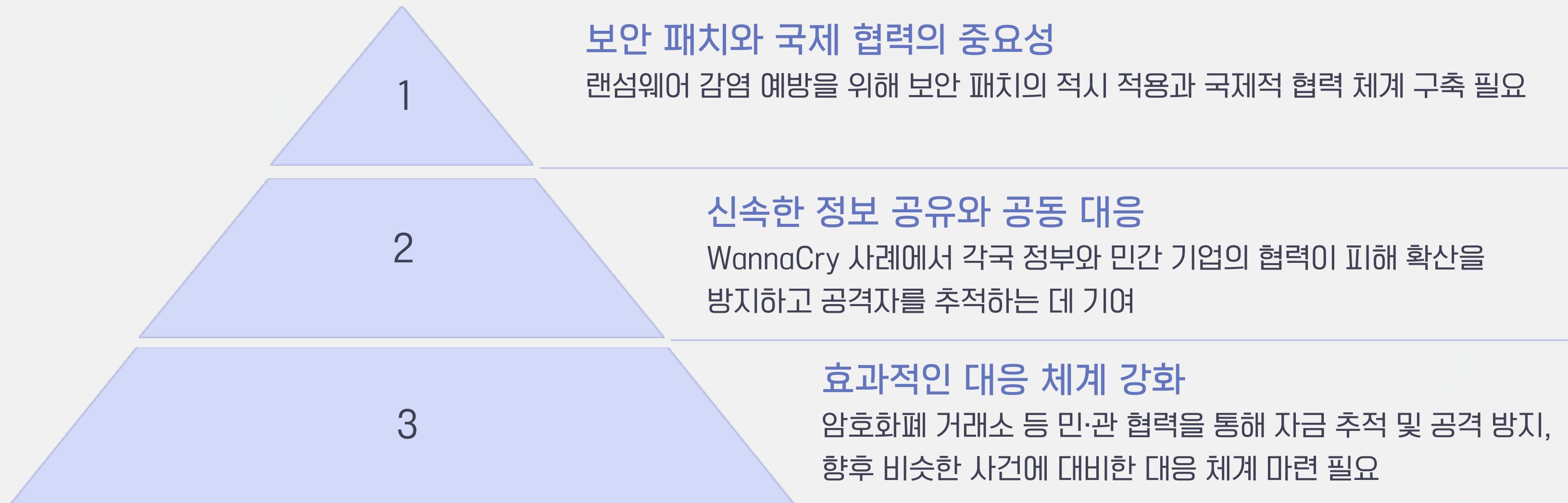
- 자금 흐름 파악
- WannaCry 1.0:  
약 4.7 BTC → ShapeShift 거래소 → Monero로 전환
- WannaCry 2.0:  
약 52 BTC → ShapeShift 및 Changelly → Monero로 전환
- 난독화 기술 사용



## 피해 규모 및 여파

- 150개국에서 약 20만 대의 컴퓨터가 감염
- 전 세계 총 피해액  
약 40억 달러

# 결론 및 시사점



**감사합니다**