클러스터링을 이용한 랜섬웨어에 사용된 비트코인 주소 분석

김보선, 신무곤, 이민성, 백의준, 김명섭
고려대학교 컴퓨터정보학과
{boseon12, tm0309, min0764, pb1069, tmskim}@korea.ac.kr

Clustering-based Analysis of Bitcoin Addresses Used in Ransomware

Boseon Kim, Mu-Gon Shin, Min-Seong Lee, Ui-Jun Baek, Myung-Sup Kim
Korea University Computer and Information Science

요 약

비트코인은 사토시 나카모토에 의해 개발된 암호화폐로 블록체인 기술을 기반으로 만들어진 온라인 암호화폐다. 비트코인의 거래는 P2P 기반 분산 데이터베이스에 의해 이루어진다. 비트코인의 거래량이 증가하며 블록체인의 특성을 악용한 사례가 나오고 있다. 비트코인이 등장하며 컴퓨터 시스템을 감염시켜 파일을 암호화한 후 대가로 비트코인을 요구하는 랜섬웨어로 인한 피해가 증가하고 있다. 본 논문은 비트코인 트랜잭션을 통해 랜섬웨어 관련 주소와 정상 주소를 k-means 알고리즘을 적용하여 비교하고 분석한다.

Ⅰ. 서 론

최근 컴퓨터 시스템을 감염시켜 파일을 암호화하여 사용하지 못하도록 하고, 이 암호를 풀어주는 대가로 금전을 요구하는 랜섬웨어로 인한 피해가 매년 꾸준히 증가하고 있다. 랜섬웨어는 몸값(Ransom)을 의미하는 단어와 소프트웨어(Software)의 합성어로, 이메일 혹은 업데이트로 위장하여 사용자의 디바이스 내에 침입한 후 데이터를 암호화하여 대가를 요구하는 악성 프로그램을 말한다[1].

비트코인은 2009년 사토시 나카모토라는 가명의 프로그래머가 개발한 암호화폐다[2]. 기존 화폐와 달리 정부나 중앙은행, 금융기관의 개입 없이 개인 간(P2P)의 거래가 가능하다. 비트코인이 등장하기 이전의 랜섬웨어는 해커가 대포통장을 사용하여 추적이 가능했지만, 비트코인이 등장한 이후로는 비트코인으로 몸값을 지불하게 되면서 랜섬웨어 유포자의 추적이 어려워졌다. 한국 랜섬웨어 침해대응 센터에 의하면 피해액은 2015년 1000억 원에서 2016년 3000억 원, 2017년 7000억 원, 2018년 1조 2500억 원, 2019년 1조 8000억 원으로 급증한다. 2016년, 100억 원 이상의 비트코인을 몸값으로 지급한 것으로 추정한다. 이는 2015년 30억 원 정도의 비트코인을 몸값으로 지불한 것과 비교해 1년 사이에 3배 이상 증가한 것이다. 랜섬웨어는 비트코인을 통해 전 세계 해커들에게 최대의 수익원으로 자리 잡고 있다. 이는 역설적으로 랜섬웨어에 감염될수록 비트코인 지불액도 증가하며 비트코인 시장이 커짐을 말한다.

본 논문은 비트코인 트랜잭션을 통해 랜섬웨어 비트코인 주소와 정상 주소를 비교하여 분석한다. 본론에서 데이터 수집 및 분석 과정을 설명하고 결론에서는 해당 연구를 정리하고 향후 연구 방향을 제시한다.

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2018R1D1A1B07045742)과 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00539-003,블록체인의 트랜잭션 모니터링 및 분석 기술개발)

Ⅱ. 관련 연구

[3]은 비트코인 트랜잭션 네트워크에서 이상 탐지 방법을 제안한다. 비트코인 트랜잭션 네트워크에서 생성된 사용자와 트랜잭션을 노드로 하는 2개의 그래프에 k-means 알고리즘으로 클러스터링하고 LOF(Local Outlier Factor)로 데이터 포인트의 편차를 측정한다. 사용자 그래프를 통해 의심스러운 사용자를 감지하며, 트랜잭션 그래프를 통해 의심스러운 거래를 감지한다. 비정상 사용자와 비정상 거래를 모두 파악하며 의심스러운 거래가 의심스러운 사용자에게 속해야 한다는 점에서 일관성이 있는지 확인한다.

Ⅱ. 본론

본 장에서는 비트코인 블록 및 트랜잭션 데이터 수집과 랜섬웨어 주소 분석 방법에 대해 언급한다.

A. 비트코인 블록 및 트랜잭션 데이터 수집

본 절에서는 실험에 사용된 데이터에 대해 언급한다. 데이터는 본 연구팀이 수집한 2009년부터 2011년 비트코인 블록 데이터와 Kaggle에서 수집한 2009년부터 2011년 랜섬웨어 주소 데이터 셋을 사용한다.

B. 데이터 전처리

본 절에서는 수집한 트랜잭션 기준의 데이터를 주소 기준의 데이터로 변환한다. 데이터 기준 변환 과정은 그림 1과 같다.

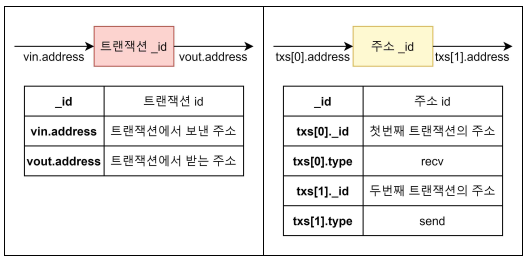

그림 1 데이터 전처리

C. 특징 추출

본 절에서는 주소 기준 데이터에서 추출한 21가지 특징을 설명한다. 다음 표 1과 같다.

항목	의미
all_count	전체 거래 횟수
all_amount	전체 거래 금액
all_amount_mean	전체 거래 금액 평균
all_amount_std	전체 거래 금액 표준편차
all_activation_period	전체 거래 시간
all_activation_mean	전체 거래 시간 평균
all_activation_std	전체 거래 시간 표준편차
send_count	보낸 거래 횟수
send_amount	보낸 거래 금액
send_amount_mean	보낸 거래 금액 평균
send_amount_std	보낸 거래 금액 표준편차
send_activation_period	보낸 거래 시간
send_activation_mean	보낸 거래 시간 평균
send_activation_std	보낸 거래 시간 표준편차
recv_count	받은 거래 횟수
recv_amount	받은 거래 금액
recv_amount_mean	받은 거래 금액 평균
recv_amount_std	받은 거래 금액 표준편차
recv_activation_period	받은 거래 시간
recv_activation_mean	받은 거래 시간 평균
recv_activation_std	받은 거래 시간 표준편차

표 1 데이터 설명

항목	정상주소		랜섬웨어 주소	
	평균	표 준 편 차	평균	표 준 편 차
all_count	2.28	24.27	7.66	235.54
all_amount	210.15	6641.99	407.82	19527.14
all_amount_mean	100.8	3270.62	150.29	4675.53
all_amount_std	0.91	188.73	3.96	319.72
all_activation_period	7.27	45.09	11.84	37.31
all_activation_mean	12178.23	6037.48	14754.82	2437.01
all_activation_std	3.49	22.2	4.37	13.24
send_count	0.89	11.22	2.44	115.5
send_amount	103.88	3320.13	200.4	9761.85
send_amount_mean	100.84	3271.73	147.98	4677.09
send_amount_std	0.8	180.74	3.38	303.73
send_activation_period	0.76	9.45	7.06	30.33
send_activation_mean	385.32	2388.73	1702.02	4791.44
send_activation_std	0.31	3.85	2.48	10.58
recv_count	1.38	14.18	5.22	121.06
recv_amount	106.28	3323.41	207.41	9767.28
recv_amount_mean	102.76	3272.14	150.23	4674.73
recv_amount_std	1	192.76	3.98	321.46
recv_activation_period	1.22	11.91	10.07	37.04
recv_activation_mean	740.24	3270.1	2256.77	5401.63
recv_activation_std	0.46	4.55	3.19	11.77

표 2 정상 주소와 랜섬웨어 주소 간 통곗값 비교

D. 랜섬웨어 주소와 정상 주소 특징

본 절에서는 주소 기준 데이터를 통해 랜섬웨어 주소와 정상 주소의 21가지 특성을 비교한다. 랜섬웨어 주소가 정상 주소보다 대체적으로 보내거나 받는 모든 거래를 더 많이 하고 표준편차도 크다. 또한 랜섬웨어 주소가 거래기간이 더 길다. 이를 통해 랜섬웨어 주소는 자주 많은 양을 긴 시간동안 거래한다는 것을 알 수 있다. 이러한 통계적 차이는 클러스터링을 통해 정상과 랜섬웨어를 구분할 수 있는 가능성을 제시한다.

E. K-means Clustering

본 절에서는 K-means 클러스터링을 이용하여 정상적인 주소와 랜섬웨어에 관련된 주소를 분석한다. K-means 알고리즘은 주어진 데이터를 k개의 클러스터로 묶는 알고리즘이다[4]. n 개의 d-차원 데이터(x1, x2,…, xn)가 주어졌을 때, n 개의 데이터 오브젝트들을 각 집합 내 오브젝트 간 응집도를 최대로 하는 k(≤n) 개의 집합 S={S1, S2, …, Sk}으로 분할한다. 다음 수식 1과 같다.

$$\operatorname{argmin} \sum_{i=1}^{k} \sum_{x \in S_i} \| x - \mu_i \|^2 \quad (1)$$

#클러스터	1	2	3	4	5	6
클러스터 내 RA개수/전체 RA 개수	51.5	11.2	2.7	3.7	0.5	30.4
클러스터 내 RA 개수/클러스터 내 전체주소개수	13.3	33.3	1.5	15.1	11.8	9.6

표 4 클러스터 별 랜섬웨어 주소 포함 비율

*RA : 랜섬웨어 주소

클러스터링 결과, 1, 2, 6번 클러스터에 전체 랜섬웨어 주소 중 90% 이상이 속하며 3, 4, 5번 클러스터에 적은 수의 랜섬웨어 주소가 속하는 것을 통해 정상적인 주소와 랜섬웨어 주소는 구별할 수 있는 확실한 특징을 가지는 것을 알 수 있다. 특히 2번 클러스터 내 전체 주소 중 30% 이상의 랜섬웨어 주소가 속하며 이는 2번 클러스터가 다른 클러스터에 비하여 랜섬웨어 주소의 특징을 잘 나타낸다고 볼 수 있다.

Ⅲ. 결론

본 논문은 랜섬웨어에 관련된 트랜잭션과 비트코인 트랜잭션을 주소 기준의 데이터로 처리하여 분석하였다. K-means 알고리즘을 적용하여 정상적인 주소와 랜섬웨어 주소가 가장 많이 포함된 클러스터를 비교하였다. 결과적으로 랜섬웨어 주소는 정상 주소와 비교했을 때, 구별할 수 있는 명확한 특징을 가지는 것을 확인할 수 있었다. 또한 클러스터링을 통해 랜섬웨어 주소의 특징을 가장 잘 나타내는 클러스터를 추출할 수 있었다. 하지만 대부분의 랜섬웨어 주소들이 속한 클러스터 내에 높은 비율의 정상 주소가 섞여있는 문제점이 있다. 따라서 본 논문에서 제시한 주소들의 특징 외에 랜섬웨어 주소를 더 잘 구별 가능한 추가적인 특징들을 추출하여 분석할 예정이다. 또한 랜섬웨어를 포함한 비트코인에서 발생하는 다른 불법거래들을 분석할 예정이며 주소 관점이 아닌 트랜잭션 관점에서도 분석을 수행하고자 한다.

참 고 문 헌

[1] 박은후, et al. 2019 국내· 외 주요 및 신규 랜섬웨어 동향 분석. 정보보호학회지, 2019, 29.6: 39-48.

[2] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[3] PHAM, Thai; LEE, Steven. Anomaly detection in the bitcoin system-a network perspective. arXiv preprint arXiv:1611.03942, 2016.

[4] JAIN, Anil K. Data clustering: 50 years beyond K-means. Pattern recognition letters, 2010, 31.8: 651-666.