사이버 범죄 대응

윤철희 경찰대학 치안정책연구소 연구관

1. 머리말

최근 사이버 범죄는 채널의 다양성, 정보 실시간 접근성, 인터넷 익명성과 확산성을 악용하여, 범죄 목적으로 양산된 사이트 혹은 블로그 및 소셜 네트워크 등을 통해 동시다발적으로 이루어지고 있다. 그리고 온라인상의 범죄는 지능형 사이버 범죄와 결합된 융합형 사회공학적 공격으로 발전하였고, 서비스형 랜섬웨어라 불리는 사업형랜섬위어(Rass)로까지 진화해 그 피해도 더욱 커지고 있다. 더욱이, 디지털 매체의 증가로 인해 사이버 범죄 원인의 예방과 분석도 어려워지는 새로운 문제에도 직면하고 있는 시점이다.
본 고에서는 우리 사회가 지속적으로 해결해 나가야 하는 과제인 지능형 APT와 결합된 사회공학적인 랜섬웨어 공격과 최근 급부상하고 있는 가상자산 관련 사이버 범죄 동향과 대응을 집중적으로 다루고자 한다.

2. 최근 사이버 범죄 발생과 대응 기술 동향

최근 2년간 주요 사이버 보안의 키워드는 단연 랜섬웨어와 가상화폐 기반의 범죄라 할 수 있다. 초국가적 접근 영역과 막대한 파급력을 가진 인터넷 및 소셜 네트워크에서 공유·유통되는 사이버 범죄 정보, 가짜뉴스, 자살방조, 온라인 마약거래, 해킹, 온라인 사기, 스미싱 등이 새로운 형태로 진화하고 있는 것이 현재 국내·외 사이버 범죄 환경의 모습이다. 여기에 더해 특히 2022년에는 락비트(LockBit), 콘티(Conti), 블랙캣(BlackCat), 데드봇(Deadbolt) 등 랜섬웨어가 사회공격기법을 기반으로 한 새로운 서비스형 랜섬웨어 공격으로 진화하여 위협을 받았고 또한, 가상자산과 관련하여 플래쉬 론(Flash Loan)공격, 스마트계약(Smart Contract) 취약점, 개인키 유출, 전자지갑 탈취, 가상화폐 탈취 등의 가상화폐와 디지털 자산을 둘러싼 공격 이슈도 있어왔다.

2.1 사회공학공격과 결합한 서비스형 랜섬웨어 공격

과거의 1세대 랜섬웨어인 락커 계열과 크립토 계열은 단순하게 로그인이나 접근을 차단하고, 잠금 해제에 필요한 코드를 받기 위해 돈을 요구하는 방식과 데이터 및 정보를 암호화하고, 복호화키를 받으려면 돈을 낼 것을 요구하는 방식이었다. 이후 좀 더 진화된 2세대 랜섬웨어는 이중 갈취를 목적으로 발전하였고, 방식은 다음과 같다. ① 공격자들은 암호화 이전에 이미 데이터를 확보하고, ② 데이터를 암호화 한 상태에서, 요구 금액을 지불하지 않을 경우 정보를 ③ 다크웹이나 웹사이트에 공개하여 순차적으로 금액을 지불하게 유도한다.

이후의 3세대는 랜섬웨어 공격과 디도스를 혼합하여 금전을 요구하는 랜섬디도스 방식으로 진화하였다. 결국 기업을 타켓으로 하는 랜섬 공격으로 다중 협박을 목적으로한 랜섬웨어라 할 수 있다. 최근에 모습을 보이고 있는 4세대 랜섬웨어 공격은 서비스형 랜섬웨어 공격으로, 기존 랜섬웨어 제작자들이 전문지식이 없는 개인과 관련 조직에게 랜섬웨어 배포 키트나 제작 툴을 판매하여, 직접 공격을 하지 않고도 수익을 거두는 방식을 보이고 있다. 즉, 랜섬웨어는 악의적인 비즈니스 서비스형 모델을 택하며 지속적으로 진화하고 있는 실정이다.

이처럼 랜섬웨어 사이버 범죄는 막대한 범죄수익을 목표로 사업형으로 서비스하는 서비스형 랜섬웨어(RaaS, Ransomware as a Service)모델 형태로까지 진화하였다. Hive, LockBit, Conti, REVil 등 서비스형 랜섬웨어 운영 조직들은 Colonial Pipeline, Kaseya, JBS Foods 등 큰 규모의 공격을 감행하기도 하였다. 이러한 랜섬웨어 운영 조직은 체계화된 조직과 금액 협상 능력을 통해 공공, 금융, 제조, 교육, 국방 등 다양한 산업군으로 공격 범위를 확대하고 있고, 앞서 언급했듯이 현재는 RaaS 생태계로 확장하여 디스코드, 텔레그램, 와이어 등 폐쇄형 메신저 기반으로 불법 데이터 거래, 자금 세탁, 크리덴셜 거래, 공격도구 거래 등 사이버 공격의 새로운 생태계를 조성하고 있다.

더욱이 문제가 되는 것은 최근 랜섬웨어들은 윈도우 환경뿐만 아니라 리눅스 및 임베디드 시스템 등을 겨냥한 크로스 플랫폼 지원을 확대하고 있으며, 공급망 공격이나 보안솔루션 무력화, 복구 및 백업파일 삭제 등 공격 기법을 다양하게 진화시키고 있다는 점이다. 기존의 단순 데이터 암호화를 넘어 정보도용(data Infostealer), 자료암호화(data Encription), 다중협박(Multi Extortion) 형태로 발전하고 있고, 특히 귀신(Gwisn), 매스스캔(Masscan) 등은 랜섬웨어는 한국이라는 특정 국가만 공격하는 공격으로서, 단순한 금전적 목적 외의 다른 목적에 따라 국가 기반의 사이버 공격 도구로 활용되고 있음도 알 수 있다.

2.2 랜섬웨어 피해 방지와 예방 노력

랜섬웨어는 사회공학적 방법과 지능형 APT를 융합, 타켓을 정하여 지속적으로 집요하게 공격하므로 사실상의 대응 방법은 예방뿐이라고 할 수 있다. 그렇기 때문에, 전산 담당자 뿐만 아니라 개개인도 반드시 사용하는 컴퓨터의 시스템 패치, 의심스러운 이메일 첨부파일 필터링, 사용하는 네트워크망의 확인, 주기적 백업, 주기적인 비밀번호 변경 등을 실행해야만 한다. 그리고 좀 더 적극적인 예방을 위해 랜섬웨어 공격 기술 세부 내용과 침해지표 등을 분석해서 대응 안내하는 <표 1>과 같은 분석정보를 항상 참고해야 한다.

다음은 랜섬웨어와 의심스러운 사이트 등을 모니터링하는 방안을 나열하였다.

2.2.1. 랜섬웨어 공격 예방과 서피스 웹의 정화

랜섬웨어의 유형별 범죄속성 유사도 분류를 위해서는 웹사이트의 보안 위협도 측정을 통한 서피스 웹사이트 보안위험 분석이 필요하다. 일반적으로 웹사이트 보안위험에 대해서는 정적분석과 동적분석을 사용하는데, 최근에는 유사도 해시 기반 웹사이트 보안위험 분석과 Machine Learning 기반 웹사이트 보안위험 분석 방법도 제시되고 있다. 웹사이트 보안위험 분석기술은 점검속도, 제로데이 악성코드 분석 가능성, 분석결과의 정확성이 주요 목표이다. 웹사이트 위험

<표 1> 침해지표 사례

Indicator type	Indicator
IP	86.194.156[,]14:2222
URL	77.75.230[.]128/17820.dat
URL	myvigyan[.]com/m1YPt/300123.gif
URL	hxxps://a1revenue.co[.]uk/SQ.php?TSI=5
URL	hxxps://gpshelpline.com/EAUD.php?NSII=10
URL	hxxps://limpiotucompu[.]com/OSIQ.php?ELIEAOSMT=1
URL	hxxps://smartvizx[.]com/UE.php?AISESCTISEBYUN=4
URL	hxxps://babarbrotherscargo[.]com/RO.php?NI=1
URL	hxxps://rjll.org[.]pk/TUEI.php?CUM=3
URL	hxxps://isoatte[.]com/LOTV.php?NTUEDRSE=8

출처: secui 보고서

도 측정을 통해 웹사이트 위험도를 측정하여, 랜섬웨어 방지를 위한 침해지표 등을 작성할 수 있는 준비자료 등을 생산할 수 있다.

- 웹사이트 보안위험 정적분석

웹사이트에 은닉된 악성코드를 점검하기 위해 소스코드에 대해 정적 분석을 할 수 있다. 웹사이트에 은닉된 랜섬웨어 악성코드는 난독화된 코드로 되어 있기 때문에 디코딩을 하여 점검한다. 기존 웹사이트에서 유포하고 있는 악성코드를 시그니처로 변환하여 탐지패턴으로 등록을 한다. 이후 분석 대상 웹사이트을 크롤링으로 수집하여 등록된 시그니처로 웹사이트의 소스를 점검한다. 점검 시간이 다른 분석 방법에 비해 적게 걸리기 때문에 많은 점검 대상을 탐지하는데 효과적이다.

- 웹사이트 보안위험 동적분석

동적분석은 악성코드를 실행하여 PC에서 행위를 분석하는 방법이다. 사용자 PC와 동일한 가상화 머신에서 주로 분석한다. 웹사이트에 접속하여 악성코드를 다운로드한 후 가상 PC에서 추가 파일 생성, 레지스트리 변경, 네트워크 연결 시도와 같은 비정상적인 행위를 탐지하게 된다. 동적분석을 통해서 웹사이트에서 다운로드된 악성코드와 명령제어서버(C&C, Command & Control)에 대한 정보를 수집한다. 일반적으로 동적분석은 점검 시간이 비교적 오래 걸리지만, 정적분석으로 탐지하기 어려운 제로데이 악성코드를 분석할 수 있다는 장점이 있다.

2.2.2 해시기반 웹사이트 보안위험 분석

웹사이트에 은닉된 악성코드에는 유사도 해시방법을 적용할 수 있다. 유사도 해시 값으로 랜섬웨어 악성코드에 대한 해시코드를 생성하면 유클리드 거리 측정법과 같은 유사도 값을 도출하여 악성 파일과 유사한지를 확인할 수 있다. 많은 악성코드에 유사도 해시함수를 적용하여 악성 여부를 분류하는 데에는 K-NN의 방법이 쓰인다.

2.2.3 ML(Machine Learning) 기반 웹사이트 보안위협 분석

서피스 웹의 많은 웹사이트를 대상으로 보안위협을 탐지하기 위해서 ML(machine learning) 학

습을 통해 대응하고 있다. ML을 이용한 탐지시스템은 확장자가 EXE, DLL 형태의 PE(Portable Executable) 구조 실행파일을 학습하고, 역시 정상적인 문서 파일, 스크립트 등 비실행 파일(Non-PE) 구조도 학습한다. 이후 점검 대상이 되는 웹사이트에 은닉된 파일에 대하여 악성 파일과의 유사도를 점검하는 방식으로 구현한다.

3. 가상자산을 이용한 범죄와 대응

3.1 가상자산 범죄 동향

블록체인의 높은 보안성에도 불구하고 가상통화가 해킹되거나, 불법 자금이 가상통화로 유통되는 등 가상통화와 관련된 범죄가 증가하고 있다. 2021년 1-11월 사이 가상자산을 이용한 범죄자금 은닉이나 세탁 등 가상자산과 관련된 국내범죄 피해액은 3조 87억 원(경찰청, 윤창현 의원)에 이르고, 데이터 플랫폼 기업 체이널리시스의 '2022 가상자산 범죄 보고서'에 따르면 세계 불법가상자산 거래 금액은 16조 7930억 원(140억 달러)에 이를 정도로 증가하였다. 특히, 가상통화가 범죄에 이용되는 경우 범죄자는 가상통화의 현금화를 위해 가상통화를 가상통화 거래소에 입금한 후 거래소 내부 거래를 통해 현금화하는 방식을 사용하고 있는데, 사회적으로 큰 문제가 되고 있는 보이스피싱 범죄조직 역시 자금 세탁을 위하여 기존의 환전소, 구매대행 등의 방식을 최근에는 가상자산을 이용하여 자금을 세탁하는 방식으로 진화하는 모습을 보이고 있다.

3.2 불법 가상자산의 추적

가상자산은 거래 내역을 공개함으로써 송신자 지갑주소와 수신자 지갑주소 간 거래는 특정할 수 있다. 그러나 그 지갑주소가 누구인지는 특정할 수 없다. 범죄조직이 수사기관의 추적을 피하기 위해 믹싱이나 토큰 기반 가상자산끼리 교환하는 유니스왑(Uniswap) 방식 등을 이용하기 때문에, 가상자산에 대한 전문 지식이나 분석 노하우가 없는 수사관들이 이를 추적하는 것이 매우 어렵다.

그래서 수사 현장에서는 불법 가상통화 자동추적 시스템을 통해 수사관이 불법 가상 통화의 이체 흐름을 추적하고 가상통화 거래소 입금 시점을 포착하여 불법 가상통화의 동결 및 환수 등의 조치를 취할 수 있게 하는 시스템을 개발하고 있다.

일반적으로 가상통화 거래는 블록체인의 각 노드에 모두 기록되기 때문에 누구든지 확인할 수 있으나, 중앙화된 거래소의 경우 거래소 내부의 고객 간 거래 내역을 블록체인에 기록하지 않고 거래소 자체의 데이터베이스에만 기록하여 외부에서 확인할 수 없다. 이에 따라, 범죄 대상이 된 가상통화가 가상통화 거래소로 입금된 후 다른 가상통화로 환전되거나, 현금화 후 출금되는 경우 해당 거래소가 수사에 협조하지 않으면 수사에 상당한 지연이 발생한다.

그렇기 때문에 블록체인 트랜젝션 포렌식을 통해 불법 가상통화의 이체 흐름을 추적하고, 가상통화 거래소 입금 시점을 포착하여 수사관에게 알리고 거래를 동결해 환수 조치를 할 수 있게 도와주는 불법 가상통화 흐름 자동 추적 시스템개발을 위해 전문수사관과 관련기관이 협력하는 방식을 나열하면 다음과 같다.

3.2.1 가상통화 거래 추적

가상통화 거래소에 해킹 피해가 발생하면 거래소에 보관 중인 가상통화가 큰 규모로 이체되는 경우가 많으므로, 특정 금액 이상의 이체가 발생 할 경우 알림을 주어 고액이체를 탐지하게 할 수 있다. 이러한 고액이체 알림은 가상통화 거래소 주소 사이 뿐만 아니라 개인 주소 고객 간 고액 이체가 발생하는 경우에도 제공되기 때문에, 개인 간 고액 이체의 경우에도 범죄 자금 세탁 등의 부정한 목적이 의심될 경우에는 대처가 가능하다. 이 정보를 수집한 후 이상거래로 판단되는 주소를 바로 공개하거나 사용자가 검색을 통하여 확인할 수 있도록 매칭을 하면 가상통화 부정거래 추적이 가능해지기 때문이다.

3.2.2 블록체인 트랜젝션을 이용한 디지털 포렌식 적용

블록체인은 거래내역 정보를 중앙집중형 서버에서 관리하지 않고 네트워크의 참가자 즉, 노드들에 분산하여 저장하기 때문에 탈중앙화가 가능하고 해킹이 어렵다는 장점이 있다. 하지만 이런 높은 보안성에도 불구하고 가상통화가 해킹되거나 불법 자금이 가상통화로 유통되는 등 가상통화와 관련된 범죄가 증가하였다.

가상통화 거래 추적을 위해서는 풀노드를 운영하여 블록체인의 모든 거래 데이터를 데이터베이스화하여 저장하는 단계를 거쳐 데이터베이스를 분석하여 가상통화 거래소 내부 주소를 식별 후 저장하는 것이 필요하다. 그리고 이러한 데이터베이스를 기초로 불법 가상통화의 거래 흐름을 모니터링하는 단계가 추가된다. 가상통화 거래소 내부 주소로 불법 가상통화 입금이 시도되거나 입금이 완료되었다고 판단되면, 가상통화 거래소로 입금 시도 또는 입금 완료된 불법 가상통화의 거래 동결을 요청해야 하기 때문이다.

그리고 불법 가상통화 거래 흐름을 모니터링하는 단계의 경우는 미리 파악된 불법 가상통화 주소를 파악하는 것이 중요한데, 불법 가상통화거래 주소에서 다른 주소로 가상통화가 이체되었는지 여부를 추적 확인한다. 즉, 블록체인 트랜젝션 포렌식을 통해 불법 가상통화 주소가 다른 주소로 이체된 경우와 이체된 다른 주소를 추적 대상 주소에 추가하여 분석하는 단계를 거치게 된다. 앞서 언급한 대로 범죄자들은 탈취한 가상통화에 대한 믹싱과 스와핑을 통해 이동경로 추적을 어렵게 하기 때문이다.

여기서 믹싱은 이동경로 추적을 어렵게 하기 위해 불특정 다수의 지갑 주소를 뒤섞어 거래하는 기술이고, 스와핑은 범죄로 취득한 특정 가상통화를 다른 종류의 가상통화로 교환하여 추적을 어렵게 하는 기술을 말한다.

특히, 블록체인 트랜젝션 포렌식의 주요 검토사항은 믹싱과 스와핑의 증거분석 후 가상통화를 탈취한 시점부터 현재까지의 가상통화 흐름을 추적 및 가상통화 믹싱과 스와핑 행위에 대한 분석을 시각화해 가상통화 세탁 방향을 예측하는 것이라 할 수 있다.

3.3 블록체인 트랜젝션 포렌식을 위한 거래 내역 분석

3.3.1. 블록과 트랜잭션 ID (TXID)의 이해

가상자산은 송수신 데이터를 생성, 전파, 보관할 때 블록체인을 활용한다. 블록체인에서 1개의 데이터 단위를 트랜잭션이라고 하며, 트랜잭션이 불특정 개수로 묶여 있는 것을 블록이라고 한다.

블록은 고유의 순차적 정수 번호를 갖고 있으며, 바로 앞 블록 데이터의 일부와 당해 블록 데이터의 일부를 조합해 해시 처리한 후 보관하기 때문에, 사후에 과거 블록 데이터 일부를 수정하기 위해서는 뒤따르는 모든 블록 데이터를 점유해야 한다. 블록체인 기술에서 과거 블록 데이터 조작은 기술적으로 불가능에 가깝다고 알려진 이유다. 각 트랜잭션은 내부 데이터를 해시 처리하여, 다른 트랜잭션과 구분할 수 있는 고유값을 만들어내는데 이를 트랜잭션 ID(TXID)라고 한다.

3.3.2 트랜잭션 데이터 생성과 전파 과정

가상자산 소유자가 트랜잭션(거래) 데이터를 생성, 전파해서 블록에 포함되는 주요 과정은 ① 송신자가 수수료, 송신 수량, 수신 주소를 확정해 트랜잭션 데이터 생성 ② 송신자와 연결된 노드에 전파 ③ 트랜잭션 데이터를 수신한 노드는 유효성 검증 후 자신과 연결된 노드에 전파 ④ 채굴노드까지 전파 등으로 정리할 수 있다.

3.3.3 부정거래 데이터베이스 분석

가상자산 부정거래 데이터베이스 분석은 가상통화 거래소 내부 주소를 식별하여 저장한 후 가상통화 거래소 외부에 외부 주소를 생성하는 단계와 가상통화 거래소로부터 가상통화 거래소 내부의 입금 전용 주소를 발급받는 단계, 그리고 외부 주소에서 입금 전용 주소로 가상통화를 이체하는 단계로 구분한다. 입금 전용 주소로 입금된 가상통화의 흐름을 모니터링하여 가상통화가 입금되는 가상통화 거래소 중앙 관리 주소를 식별하면 중앙 관리 주소의 과거 거래 내역을 분석할 수 있다. 블록체인의 모든 거래 데이터를 분석하여 가상통화 거래소 내부 주소를 식별하면 내부 주소 추출과 불법 가상통화의 입금 시도 또는 입금 여부를 판단하는 분석, 가상통화 거래소 내부 주소로의 불법 가상통화의 입금이 시도되거나 입금이 완료되는 시점을 파악하는 분석이 가능하다. 이런 분석이 수행되면 가상통화 거래소 외부에 미리 생성된 외부 주소로부터 가상통화거래소 내부의 미리 발급된 입금 전용 주소로의 가상통화 이체를 모니터링하여, 상기 가상통화가 입금되는 가상통화 거래소 중앙 관리 주소를 식별할 수가 있다.

3.3.4 부정거래 자동추적과 국내외 거래소의 협력

가상통화 거래소 외부의 각 노드들 간 거래 정보 즉, 모든 트랜잭션 정보는 블록체인을 구성하는 모든 노드들에 분산 저장된다. 하지만 거래소 내부의 거래 정보는 거래소 내부의 데이터베이스에만 저장되기 때문에 범죄에 이용된 가상통화가 거래소 내부로 입금되어 내부 간 거래를 통해 현금화되는 경우에는 해당 거래소의 협조 없이는 수사에 상당히 어려움이 있다.

가상통화 거래소는 일반적으로 고객에게 입금처리를 위해 입금 전용 주소를 미리 생성하여 발급하거나 요청시 발급하여 고객에게 제공한다. 따라서 고객은 입금 전용 주소를 발급받으면 가상통화를 입금 전용 주소에 이체하게 되고, 입금전용 주소에 이체된 가상통화는 일정 시간 경과후 중앙 관리 주소에 이체된다. 이후 가상통화 거래소는 입금된 모든 가상통화주소를 중앙 주소에 이체한다. 지갑주소가 과연 누구의 것인지를 특정하는 것은 블록체인 기술의 특성상 불가능하기 때문에 현금으로 출금하기 위해서는 반드시 필요한 거래소의 협력이 필요하다.

4. 맺음말

최근 사이버 범죄는 서비스형 랜섬웨어라 불리는 사업형 랜섬웨어(Raas)를 통해 그 피해가 막대하게 일어나고 있다. 조직화된 해킹 그룹들이 서비스형 랜섬웨어를 제작 배포하여 공격 횟수와 피해 규모가 나날이 늘어가고 있으며, 범죄 피해 금액은 가상자산으로 지불받아 추적을 피하고 있다. 교묘하고 조직적으로 발전하고 있는 랜섬웨어에 대한 지속적인 모니터링이 필요하고, 또한 이를 불법 가상통화로 환전하려는 사이버범죄행위를 추적해야 한다.

현재 국내 수사기관은 불법 가상통화 자동 추적 시스템 구축을 위한 연구개발 등을 진행하고 있으며, 국내외 거래소와 협력도 추진하고 있다. 이를 통해 가상자산 부정거래 방지 플랫폼을 구현, 가상통화의 주소정보와 사용자 정보를 매칭하여 처리하고, 모든 주소에 대한 거래 데이터를 투명하게 공유할 수 있게 하는 방안을 추진 중이다. 앞으로 국내외 거래소가 협력을 강화하여 가상자산 부정거래 시도를 차단하고, 인공지능 기반 부정거래 판단 알고리즘 이용을 확대해야 할 필요가 있다. 이렇게 되면 부정거래 탐지 프로세스 강화와 신속한 모니터링 및 대응의 부담을 덜고, 수사력을 집중하여 사이버범죄에 대응할 수 있으리라 기대된다.

[참고문헌]

[1] Ryan Francis, '서비스로 제공되는 랜섬웨어, 그 종류와 대응 방안' ITWORLD, 2016.

[2] Josh Fruhlinger, '더 교묘하고 더 악랄해진' 2020 랜섬웨어 공격 5종, ITWORLD, 2020.

[3] 우성희, '차세대 랜섬웨어의 공격유형과 대응방안' 한국정보통신학회 2020년 춘계 종합학술대회 논문집

[4] 문기운 외 '최신 랜섬웨어 동향 및 발전 방향', 정보보호학회지 제32권 제3호, 2022.6

[5] S. J, Park 'Blockchain Paradigm and Fin Tech Security', Information And Communications Magazine, Vol.34, No.3, pp. 23-24, March, 2017.

[6] S.G. Kang, H.J. Bae, S.H. Lim, Y.S.. Lee, 'A Study on the Vulnerability and Countermeasures of Bitcoin', Proceedings of the Korean Society of Computer Information Conference, Vol 25. No.2, pp. 124-127, 2017.

[7] Kuyoung Shin, Jinchel Yoo, Changhee Han, et al., 'A study on building a cyber attack database using Open Source Intelligence(OSINT)', Convergence Security Journal 19(2), pp. 113-133, 2019.

[8] Kim, KH., Lee, DI., Shin, YT. (2018). Research on Cloud-Based on Web Application Malware Detection Methods. In: Park, J., Loia, V., Yi, G., Sung, Y. (eds) Advances in Computer Science and Ubiquitous Computing. CUTE CSA 2017 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore.
https://doi.org/10.1007/978-981-10-7605-3_130

[9] Yong-Joon Lee, Se-Joon Park, and Won-Hyung Park,'Military Information Leak Response Technology through OSINT Information Analysis Using SNSes', Security and Communication Networks, 2022. https://doi.org/10.1155/2022/9962029

[10] G. Tan, P. Zhang, Q. Liu, X. Liu, C. Zhu, and F. Dou, 'Adaptive Malicious URL Detection:

Learning in the Presence of Concept Drifts,' 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), NewYork, NY, USA, 2018, pp. 737-743, doi: 10.1109/TrustCom/BigDataSE.2018.00107.
[11] K. Nandhini, and R. Balasubramaniam, 'Malicious Website Detection Using Probabilistic Data Structure Bloom Filter,' 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 311-316, doi: 10.1109/ICCMC.2019.8819818.

※ 출처: TTA 저널 제206호