JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 11, pp. 143-150, November 2025
https://doi.org/10.9708/jksci.2025.30.11.143

Study on the Preemptive Smishing Crime Tracking Method with Honey-pot Spyware

Woo Jin Jung*, Seong-Cho Hong**, Ah Reum Kang***

*Student, Dept. of Cyber Security, Pai Chai University, Daejeon, Korea
**Research Professor, SMART ICT Convergence HRD Center, Pai Chai University, Daejeon, Korea
***Professor, Dept. of Cyber Security, Pai Chai University, Daejeon, Korea

[Abstract]

This study criticized the limitations of existing post-incident smishing detection methods in preventing and tracing attacks and proposes a preemptive smishing crime-tracking method to overcome them. The proposed approach leverages the flexible structure of PDF files to create honeypot spyware PDFs disguised as legitimate documents, which, upon execution by an attacker, immediately perform system information collection, keylogging, and network transmission. This six-stage tracking scenario was validated through experiments on a testbed simulating a real-world environment, demonstrating its feasibility at every step. Consequently, this work establishes a practical foundation for shifting the smishing response paradigm from reactive detection to preemtive prevention.

▸ **Key words**: Smishing, Honeypot Technology, Spyware Tracking, Cybersecurity, Preepmtive Response

[요 약]

본 연구는 기존의 사후 대응 중심 스미싱 탐지 방식이 범죄 예방과 추적에 한계를 지니고 있음을 지적하고, 이를 극복한 능동적 스미싱 범죄 추적 방법론을 제안한다. 제안한 방법론은 PDF 파일의 유연한 구조를 활용하여 정상 문서로 위장한 허니팟 스파이웨어 PDF 파일을 생성하고, 공격자가 이를 실행하는 즉시 시스템 정보 수집·키로깅·네트워크 전송 등의 기능을 수행하도록 설계되었다. 제안된 시나리오는 6단계의 과정을 포함하며 실제 환경과 유사한 테스트베드에서의 실험을 통해 모든 단계의 실행 가능성을 입증했다. 이를 통해 스미싱 범죄 대응 패러다임을 사후 탐지에서 사전 예방으로 전환할 수 있는 실용적 기반을 마련했다.

▸ **주제어**: 스미싱, 허니팟 기술, 스파이웨어 추적, 사이버보안, 능동적 대응

• First Author: Woo Jin Jung, Corresponding Author: Ah Reum Kang
*Woo Jin Jung (2284057@pcu.ac.kr), Dept. of Cyber Security, Pai Chai University
**Seong-Cho Hong (scv.hong@pcu.ac.kr), SMART ICT Convergence HRD Center, Pai Chai University
***Ah Reum Kang (armk@pcu.ac.kr), Dept. of Cyber Security, Pai Chai University
• Received: 2025. 08. 18, Revised: 2025. 10. 28, Accepted: 2025. 11. 05.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

스마트폰의 급속한 보급과 모바일 인터넷 사용량의 증가는 새로운 형태의 사이버 범죄인 스미싱(smishing)의 급격한 확산을 야기하고 있다. 스미싱은 SMS(short message service)와 피싱(phishing)의 합성어로, 문자메시지를 통해 개인정보를 탈취하거나 악성코드를 유포하는 신종 사기 수법이다. 대한민국의 스미싱 범죄 현황은 우려할 만한 수준에 도달했다. 한국인터넷진흥원(KISA) 자료에 따르면, 2022년 스미싱 탐지 건수는 약 3만 7천 건에서 2023년 50만 건으로 크게 증가했으며, 2024년에는 219만 건을 넘어서는 급증세를 보였다. 이처럼 단 2년 사이에 약 60배 이상의 증가율을 기록하였다[1]. 전 세계적으로도 스미싱 범죄는 심각한 사회적 문제로 대두되고 있다. 미국에서는 2020년 초 COVID-19 팬데믹으로 인한 전국적인 격리 조치 초기 2주 동안 국민의 44%가 사기 전화와 문자메시지 증가를 경험한 바 있다[2]. 또한, Proofpoint의 2024년 피싱 현황 보고서에 따르면, 15개국 8,550명 대상 설문조사 결과 2023년 한 해 동안 응답 조직 중 71%가 최소 한 차례 이상의 피싱 공격을 경험했다[3].

스미싱 공격의 양상은 날로 정교해지고 있다. 초기의 단순한 문자메시지 방식에서 벗어나, 최근에는 Fig. 1.과 같은 민생과 직결된 이슈를 활용한 고도화된 수법이 등장하고 있다.

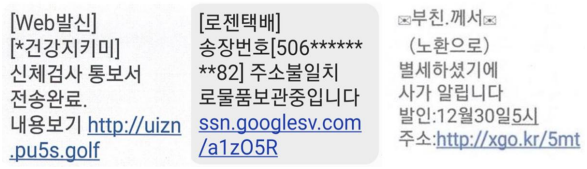

Fig. 1. Recent Examples of Smishing Messages

'민원24', '쓰레기 무단투기 범칙금', '교통범칙금 과태료 부과 통지' 등 공공기관을 사칭하는 사례가 급증하고 있으며, 심지어 '아버지 별세 부고장'과 같은 감정적 요소를 악용하는 수법까지 나타나고 있다[4].

기술적 관점에서도 스미싱 공격은 더욱 정교해지고 있다. 단순한 링크 클릭 유도에서 벗어나, 악성 앱 설치 유도, 개인정보 직접 입력 요구, 금융 앱 접근 권한 탈취 등 다단계 공격 기법이 사용되고 있다. 또한, 짧은 URL 서비스를 악용하여 악성 링크를 숨기고, 소셜 미디어 플랫폼을 통한 확산 등 다양한 채널을 복합적으로 활용하는 추세이다[5].

그러나 기존의 스미싱 대응 방식은 대부분 사후 대처에 초점을 맞추고 있어, 이미 발생한 피해를 복구하거나 범죄자를 추적하는 데 한계가 있다[6]. 본 연구는 이러한 한계를 극복하기 위해 허니팟(honey-pot) 기술과 스파이웨어(spyware) 기법을 결합한 스미싱 범죄 추적 방법을 제안한다. 제안하는 방법은 스미싱 공격이 발생하기 전에 범죄자의 행동을 모니터링하고 추적할 수 있는 능동적인(preemptive) 접근법을 통해, 스미싱 범죄의 예방과 조기 탐지를 가능하게 한다.

본 논문은 다음과 같이 구성된다. 2장에서는 스미싱과 관련된 선행 연구들을 살펴보고, 그 한계점과 한계점을 극복하려는 방안으로써 능동적 스미싱 대응에 대해 설명한다. 3장에서는 제안하는 허니팟 스파이웨어를 활용한 능동적 스미싱 범죄 추적 방안에 대해 상세히 기술한다. 4장에서는 테스트베드 환경에서 허니팟 스파이웨어를 활용한 추적 시나리오 검증을 구현하여 나타내며, 끝으로 5장에서는 결론 및 향후 연구방향을 제시하였다.

II. Related Work

2.1 Smishing

스미싱은 SMS와 피싱의 합성어로, 문자메시지를 통해 수행되는 사이버 공격의 한 형태이다. 스미싱은 공격자가 합법적인 기관이나 서비스를 사칭하여 피해자를 속이고, 악성 링크 클릭이나 개인정보 입력을 유도하여 민감한 정보를 탈취하거나 악성코드를 설치하는 공격 기법이다[5].

스미싱 공격은 전통적인 이메일 피싱과 구별되는 몇 가지 고유한 특성을 가지고 있다. 첫째, 모바일 디바이스의 제한된 환경으로 인해 사용자가 URL의 진위를 확인하기 어렵다는 점이다[7]. 둘째, SMS의 즉시성과 개인적 특징으로 인해 사용자가 메시지를 신뢰할 가능성이 높다는 점이다[6]. 셋째, 모바일 환경에서는 전통적인 보안 솔루션의 효과가 제한적이라는 점이다[7].

Timko 등의 연구에서는 스미싱 메시지의 구성 요소를 발신자(sender), 주체(entity), 방법(method), 행동 유도(call to action), 시나리오(scenario)로 분류하였다[8]. 이러한 분류는 스미싱 공격의 패턴을 이해하고 탐지 시스템을 개발하는 데 중요한 기초 자료를 제공한다.

2.2 Existing Smishing Countermeasures

현재까지 제안된 스미싱 대응 방식은 크게 세 가지 범주로 분류할 수 있다. 콘텐츠 기반 탐지, 행동 기반 분석, 그

리고 하이브리드 접근법이다.

콘텐츠 기반 탐지 방법은 SMS 메시지의 텍스트 내용을 분석하여 악성 메시지를 식별하는 접근법이다. Jain과 Gupta는 규칙 기반 프레임워크를 제안하여 스미싱 메시지의 특정 패턴과 키워드를 식별하는 방법을 개발했다[9]. 그러나 이 방법은 사전 정의된 규칙을 사용하여 의심스러운 메시지를 필터링하지만, 새로운 공격 기법에 대한 적응력이 제한적이라는 한계가 있다.

기계학습 기반 접근법은 최근 들어 주목받고 있는 방법이다. Diksha Goel의 연구에서는 텍스트 정규화 기법을 적용한 콘텐츠 기반 분석을 통해 96.2%의 탐지 정확도를 달성했다[5]. 이 연구는 SMS 텍스트에서 자주 사용되는 슬랭(slang), 약어(abbreviation) 등을 표준 형태로 변환하여 기계학습 분류기의 성능을 향상시켰다[5].

하이브리드 딥러닝 접근법도 최근 연구되고 있다. 한 연구에서는 양방향 게이트 순환 유닛(Bi-GRU)와 합성곱 신경망(CNN)을 결합한 하이브리드 모델을 제안하여 스미싱 공격 탐지 성능을 향상시켰다[7]. 이 모델은 세 개의 다른 SMS 데이터셋을 사용하여 훈련되었으며, LIME(local interpretable model-agnostic explanations)을 활용하여 모델의 의사결정 과정에 대한 설명 가능성을 제공했다.

Few-shot 학습 기법을 활용한 접근법도 제안되었다. 최근 연구에서는 Gemma-2B, Phi-3 mini, Qwen3.5-3B와 같은 소형 언어 모델을 활용하여 몇 개의 라벨링된 예시만으로 스미싱 메시지를 분류하는 방법을 개발했다[10]. 이 방법은 모바일 환경에서의 프라이버시 보호와 경량화된 온디바이스(on-device) 추론을 가능하게 한다.

크로스 디바이스(cross device) 솔루션도 연구되고 있다. Kanaoka와 Isohara는 AR 글래스(glasses)를 활용하여 다양한 디바이스에 표시된 URL을 이미지 분석을 통해 탐지하는 방법을 제안했다[11]. 이 접근법은 스마트폰뿐만 아니라 노트북, 텔레비전, 벽면 등에 표시된 URL에 대해서도 스미싱 탐지가 가능하다.

2.3 Existing Limitations

기존 스미싱 대응 방식들은 여러 가지 근본적인 한계점을 가지고 있다. 첫째, 사후 대응 중심 스미싱 대응 방식의 한계이다. 대부분의 기존 연구는 이미 발생한 스미싱 공격을 탐지하고 차단하는 데 초점을 맞추고 있어, 공격이 발생하기 전에 예방하거나 범죄자를 추적하는 능력이 제한적이다[6]. 둘째, 정확도와 오탐률의 문제이다. 사용자 연구에 따르면, 참가자들이 가짜 메시지를 식별하는 정확도는 67.1%에 불과했으며, 진짜 메시지를 구별하는 정확도는 43.6%로 더욱 낮았다[6]. 이는 기존 시스템들이 높은 오탐률을 가지고 있음을 시사한다. 셋째, 언어적 다양성과 진화하는 공격 기법에 대한 적응력 부족이다. 스미싱 공격자들은 지속적으로 새로운 기법을 개발하고 있으며, 특히 COVID-19과 같은 사회적 이슈를 악용한 공격이 증가하고 있다[12]. 기존의 규칙 기반이나 정적 기계학습 모델들은 이러한 새로운 패턴에 신속하게 대응하기 어렵다. 넷째, 모바일 환경의 제약사항이다. 모바일 디바이스의 제한된 컴퓨팅 자원과 배터리 수명으로 인해 복잡한 탐지 알고리즘을 실시간으로 실행하기 어렵다[7]. 또한 모바일 인터페이스의 특성상 사용자가 URL의 진위를 확인하기 어렵다는 근본적인 문제가 있다[7]. 다섯째, 국제적 협력과 법적 프레임워크의 부재이다. 스미싱 공격은 종종 국경을 넘나들며 발생하지만, 국제적인 협력 체계와 통일된 법적 프레임워크가 부족하여 효과적인 대응이 어렵다.

기존 연구들과 비교하여 본 연구가 가지는 차별점은 다음과 같다. 기존 연구들이 수동적인 탐지와 차단에 초점을 맞춘 반면, 본 연구는 허니팟 기술을 활용하여 스미싱 공격자를 능동적으로 유인하고 추적하는 방법을 제안한다. 이는 범죄 예방과 사전 대응을 가능하게 하는 능동적 대응을 기초로 한 접근법이다. 본 연구는 허니팟 기술과 스파이웨어 추적 기법을 결합하여 스미싱 공격자의 행동을 모니터링할 수 있는 새로운 방법론을 제시한다. 이는 기존의 콘텐츠 기반 분석이나 단순한 행동 분석을 넘어서는 종합적인 접근법이다. 마지막으로, 기존 연구들이 기술적 효과성에만 초점을 맞춘 반면, 본 연구는 실제 운용 환경에서의 법적 제약사항을 고려한 설계를 포함한다. 이는 실시간 모니터링의 법적 한계를 인식하고 주기적 로그 전송 방식을 통해 이를 해결하는 실용적 접근법이다.

2.4 Preemptive Smishing Response

기존의 스미싱 대응 방식은 피해가 발생한 후에 대처하는 반응적(reactive) 접근법에 의존하고 있어 근본적인 한계를 가지고 있다. 사후 대응 방식은 이미 발생한 피해를 복구하거나 범죄자를 추적하는 데 상당한 시간과 자원이 소요되며, 그 과정에서 추가적인 피해 확산을 막기 어렵다는 문제점을 가지고 있다.

스미싱 공격의 특성상 범죄자들은 짧은 시간 내에 다수의 피해자를 대상으로 공격을 수행하며, 공격이 탐지되면 즉시 공격 인프라(infra)를 변경하여 추적을 회피한다. 이러한 상황에서 전통적인 사후 대응 방식으로는 범죄자의 신속한 대응에 효과적으로 대처할 수 없다.

능동적 스미싱 대응의 필요성은 다음과 같은 측면에서

강조된다. 첫째, 조기 위협 탐지를 통한 예방적 보안이 필요하다. AI 기반 예측 분석을 통해 지진, 홍수, 산불 등에 대한 조기 경보 시스템이 개발된 것처럼, 스미싱 공격에 대해서도 사전 예방적 접근이 가능하다. 둘째, 행동 분석을 통한 범죄자 추적이 중요하다. 기존의 콘텐츠 기반 탐지와 달리 공격자의 실제 행동 패턴을 실시간으로 모니터링함으로써 더욱 정확한 위협 식별이 가능하다.

해외 선행 연구에서는 능동적 스미싱 대응에 관한 몇몇 시도가 이루어지고 있다. Algarni은 범죄 발생 전 잠재 위협을 식별하고 예방 조치를 마련하는 접근법을 강조하였으며, Svensson과 Chen 등도 조기 탐지 기술을 통해 스미싱 공격을 사전에 차단하는 방안을 다루었다[13][14][15]. 이들은 잠재적 위협 신호의 조기 발견과 행동 분석을 통해 보다 정밀한 탐지가 가능하다고 보았다.

또한 허니팟 스파이웨어 기술을 활용한 기만(deception) 기반 보안이 효과성이 입증되고 있다[16]. 허니팟 스파이웨어는 공격자를 유인하여 그들의 행동을 분석할 수 있는 통제된 환경을 제공하며, 이를 통해 수집된 정보는 사법 기관의 수사에 중요한 증거로 활용될 수 있다. Crag은 허니팟 스파이웨어와 같은 기만 기술을 활용하여 공격자를 유인·분석함으로써 능동적 대응을 실현하는 방식을 제안하였다[17].

국내에서는 이와 같은 능동적 스미싱 대응 연구가 미흡한 실정이며, 본 연구는 해외에서 제안되고 있는 허니팟 스파이웨어 기반 능동 대응 기법을 중심으로 공격 행위에 대한 실시간 분석과 선제적 차단을 목표로 하고 있다. 이를 통해 스미싱 공격의 빠른 전파를 효과적으로 막고, 범죄자 추적 및 증거 수집에 유의미한 기여를 하고자 한다.

2.5 Honeypot

허니팟(honeypot)은 사이버보안 분야에서 공격자를 유인해 탐지 및 분석하는 데 사용되는 기만 기반 보안 메커니즘이다. 공격자가 매력적으로 여길 수 있는 취약점이나 가치 있는 정보를 가진 것처럼 보이는 시스템을 의도적으로 구성하여 공격자의 주의를 끌고, 이들이 허니팟에 접근하는 모든 활동을 모니터링하고 기록한다. 정상적인 사용자는 허니팟에 접근할 이유가 없으므로, 허니팟에 대한 모든 접근 시도는 악의적인 행동으로 간주할 수 있다. 따라서 거짓 긍정(false positive) 없이 순수한 공격 활동만을 포착할 수 있다는 장점이 있다.

본 연구에서 제안하는 허니팟 스파이웨어를 사용한 능동적 스미싱 범죄 추적 방법론은, 그 의도 및 목표하는 대상과는 별개로, IP 등 타인의 정보를 당사자의 동의 없이 무단으로 수집하게 되는 결과를 도출하게 된다. 따라서 현행법상 민간 차원의 사용은 그 의도와는 별개로 「정보통신망법」 및 「개인정보보호법」에 저촉된다. 사법기관 또한 이러한 법률적 제약에서 벗어날 수는 없으나, 허니팟이라는 환경에 침입해서 정보를 탈취한 범죄자 대상이라는 조건과 엄격한 관리·감독 아래 제한적으로 사용이 가능하기에 각별한 주의가 필요하다.

III. The Proposed Method

3.1 Experimental Environment

본 연구의 실험 환경은 허니팟 스파이웨어의 안전하고 효과적인 테스트를 위해 격리된 네트워크 환경에서 구축되었다. 크게 허니팟 시스템, 가상화된 공격자 시스템, 가상화된 사법기관 C&C(command & control) 서버로 구성되어 있으며, 이는 후술할 스미싱 범죄 추적 시나리오를 재현하면서도 보안성을 보장하는 테스트베드를 제공한다.

허니팟 시스템은 실제 사용자의 모바일 환경을 정교하게 모방하도록 설계되며, 공격자들이 매력적인 표적으로 인식할 수 있도록 의도적으로 보안 취약점을 포함한다. 약한 비밀번호, 오래된 버전의 운영체제, 패치하지 않은 애플리케이션 등이 설치되어 있어 공격자들이 쉽게 침투할 수 있는 환경을 제공한다. 또한 가짜 개인정보, 페이로드가 포함된 신분증 PDF 파일, 금융 정보 등의 미끼 데이터가 배치되어 있어 공격자의 관심을 끌고 지속적인 공격을 유도한다. 가상화된 공격자 시스템은 Windows 10 Professional(64bit)이 설치된 가상머신으로 구성되었으며, Adobe Reader 9.2 버전이 설치되어 있다. 가상화 플랫폼으로는 VMware Workstation Pro 17.0을 사용하였으며, 이는 네트워크 격리, 스냅샷 기능을 제공하여 안정적인 가상머신 관리가 가능하다. 가상화된 사법기관 C&C 서버는 Windows 10 Professional(64bit)과 Wireshark가 설치된 가상머신으로 구성되어 스파이웨어로부터 전송되는 데이터를 수집하고 분석하는 기능을 제공한다.

네트워크 구성은 VMware의 가상 네트워크 기능을 활용하여 완전히 격리된 환경을 구축하였다. 허니팟 시스템(192.168.10.0/24), 가상화된 공격자 시스템(192.168.20.0/24), 가상화된 사법기관 C&C 서버(192.168.30.0/24)로 설정하여 세그먼트를 분리하고 외부 인터넷 연결은 완전히 차단하여 실제 악성코드나 공격 도구가 외부로 유출되는 것을 방지하였다.

본 테스트베드는 실제 스미싱 공격 환경과의 높은 유사

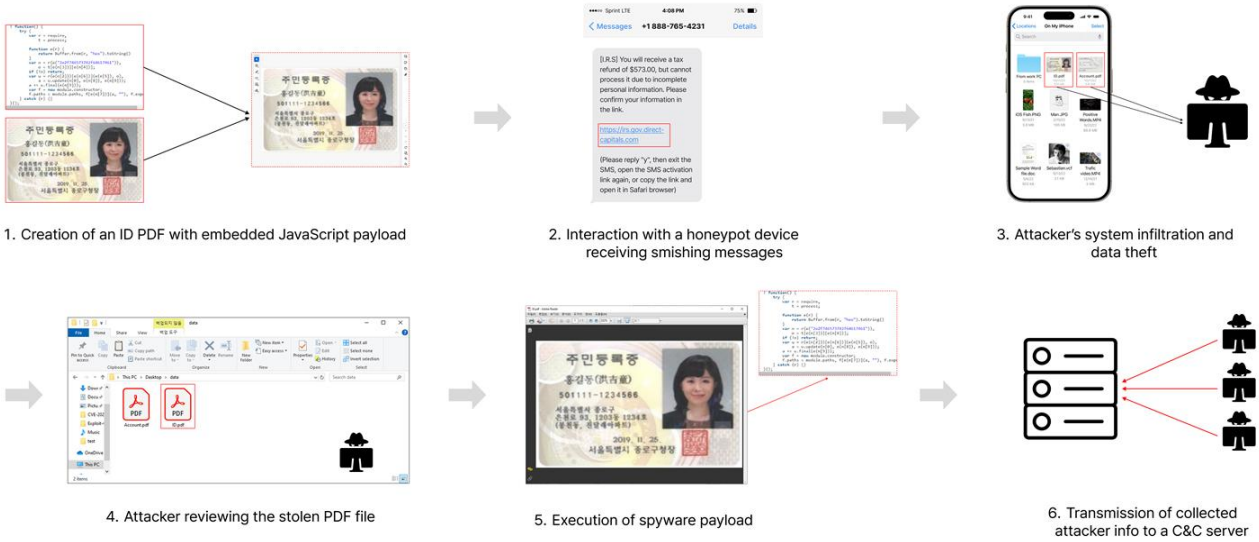

Fig. 2. Proposed Smishing Crime Tracking Scenario

성을 확보하기 위해 최신 스미싱 공격 패턴을 반영하였다. 허니팟 시스템은 안드로이드 운영체제 기반의 모바일 환경을 에뮬레이션하며, 짧은 URL 변조, 악성 앱 설치 유도, 개인정보 탈취 등 실제 공격자가 사용하는 기법을 재현하였다. VMware 기반 가상화 기술을 활용해 네트워크 세그먼트를 분리함으로써 허니팟, 공격자, 사법기관 각 시스템 간 상호작용을 실제와 유사하게 구현하였으며, 네트워크 격리와 스냅샷 기능으로 실험 환경의 복원과 반복 실험이 용이하도록 설계하였다. 또한, 네트워크 트래픽과 시스템 호출 로그를 구조화하여 정밀 분석 및 재현 가능성을 확보하였고, 최신 공격 동향을 반영해 지속적으로 업데이트할 계획이다. 이를 통해 본 테스트베드는 신뢰도 높은 실험 환경으로서 스미싱 공격 탐지 및 대응 연구에 최적화된 기반을 제공한다.

3.2 Proposed Smishing Tracking Scenario

본 연구에서 제안하는 스미싱 범죄 추적 시나리오는 Fig. 2.와 같다.

첫 번째 단계에서는 스파이웨어 페이로드(payload)가 삽입된 신분증 PDF 파일을 제작한다. 먼저 실제 신분증과 유사한 외관을 가진 PDF 문서를 생성하여 공격자의 의심을 최소화한다. 이 문서 내부에는 자바스크립트 기반의 페이로드가 은밀하게 삽입되며, 이는 PDF의 복잡한 구조를 활용하여 탐지를 회피한다. 삽입되는 스파이웨어는 Windows Powershell 명령을 포함하는 PDF 객체를 활용하여 시스템 접근 권한을 획득한다.

두 번째 단계에서는 연구자가 의도적으로 취약하게 구성한 허니팟 디바이스를 통해 스미싱 문자에 포함된 링크를 클릭하여 공격자로 하여금 페이로드가 포함된 신분증 PDF 파일 및 개인정보를 탈취하도록 능동적으로 유도하는 과정이 진행된다. 스미싱 공격자가 발송하는 택배 배송 알림, 정부기관 공지 사항, 금융기관 보안 업데이트 등으로 위장한 메시지가 허니팟 디바이스로 전송되면, 연구자는 의도적으로 해당 링크를 클릭한다. 이 과정에서 허니팟 시스템은 실시간으로 모든 네트워크 활동을 모니터링하며, 공격자의 접근 패턴, 사용하는 도구, 공격 기법 등을 상세히 기록한다.

세 번째 단계에서는 공격자가 피해자의 시스템에 침투하여 페이로드가 포함된 신분증 PDF 파일과 함께 다양한 개인정보를 탈취하는 과정이 진행된다.

네 번째 단계에서는 공격자가 탈취한 다양한 파일 중에서 페이로드가 포함된 PDF 파일을 열람하는 순간이 발생한다. 이는 본 연구의 핵심적인 함정 단계로, 공격자가 획득한 문서의 진위를 확인하거나 추가적인 정보를 얻기 위해 PDF 파일을 클릭하는 일반적인 행동 패턴을 활용한다. 공격자들은 일반적으로 탈취한 개인정보의 가치를 평가하기 위해 문서들을 개별적으로 검토하는 과정을 거치며, 특히 신분증과 같은 공문서는 높은 우선순위를 가진다. 이러한 행동은 공격자가 문서의 품질, 완성도, 활용 가능성을 판단하기 위한 필수적인 과정으로 인식된다.

다섯 번째 단계에서는 공격자가 페이로드가 포함된 PDF 파일을 열람하는 순간 사전에 삽입된 스파이웨어 페이로드가 실행되는 과정이 진행된다. Adobe Reader의 자바스크립트 엔진(javascript engine)을 통해 악성코드가 활성화되며, 이는 공격자의 시스템 환경으로부터 다양한 정보를 수집하기 시작한다.

최종 단계에서는 수집된 공격자의 정보가 사법기관이 운영하는 C&C 서버로 전송되는 과정이 완료된다. 이 단계는 능동적 스미싱 추적 시스템의 핵심 목표인 범죄자 식별과 증거 수집을 달성하는 단계이다. 전송되는 정보에는 공격자의 시스템 사양, 사용 중인 해킹 도구 목록, 네트워크 연결 기록, 공격 캠페인(attack campaign) 관련 데이터 등이 포함된다. C&C 서버는 이러한 정보를 분석하여 공격자의 신원 확인, 공격 조직의 구조 파악, 추가 피해 예방을 위한 정보를 사법기관에 제공한다. 이후 수집된 데이터는 법정에서 디지털 증거로 활용할 수 있는 형태로 가공된다.

3.3 Honey-pot Spyware

허니팟 스파이웨어가 포함된 PDF 파일 생성은 Adobe Reader의 Javascript 실행 환경과 PDF 문서 구조의 특징을 활용한 정교한 과정을 통해 이루어진다. PDF 파일은 유연한 파일 구조를 가지고 있어 이미지, Javascript 코드, 실행 파일 등 다양한 형태의 콘텐츠를 삽입할 수 있다는 특성을 지니고 있으며, 이러한 특성은 스미싱 범죄자로 하여금 손쉽게 접근할 수 있는 공격 벡터가 된다.

생성 과정은 먼저 실제 신분증과 유사한 외관을 가진 PDF 문서를 제작하는 것으로 시작된다. PDF 문서 내부에는 OpenAction과 같은 자동 실행 기능을 활용하여 문서가 열리는 즉시 Javascript 코드가 실행되도록 구성한다. 이때, Launch Action과 같은 자동 실행 기능을 활용하여 문서가 열리는 즉시 Powershell 명령어가 실행되도록 하여 사법기관의 C&C 서버로부터 스파이웨어를 공격자 시스템에 내려받고 실행하는 과정을 수행한다.

개발된 스파이웨어는 모듈형 구조로 설계되어 시스템 정보 수집, 키로거 기능, 네트워크 통신 등의 다양한 기능을 포함한다. 데이터 수집 모듈은 공격자의 핵심 정보를 체계적으로 수집하는 기능을 담당한다. 운영체제 정보, 설치된 소프트웨어 목록, 네트워크 설정, 하드웨어 사양 등의 시스템 환경 정보를 실시간으로 수집한다. 특히 키로거 기능을 통해 공격자의 키보드 입력, 마우스 클릭, 실행 프로그램 목록을 기록하여 공격자의 행동 패턴을 상세히 분석할 수 있다. 통신 모듈은 수집된 데이터를 암호화하여 사법기관 C&C 서버로 전송하는 기능을 제공한다. 데이터 전송 시에는 HTTP/HTTPS 프로토콜을 사용하여 일반적인 웹 트래픽으로 위장한다. 은닉 및 지속성 모듈은 스파이웨어가 시스템에서 장기간 동작할 수 있도록 보장하는 핵심 기능을 담당한다. 본 모듈은 스파이웨어를 프로세스 목록에서 숨기며 샌드박스 환경을 탐지하여 분석 시도를 차단한다.

IV. Results

본 연구의 결과는 다음과 같다. 먼저 Fig. 3.는 정상 신분증 PDF 파일(좌)과 페이로드가 포함된 허니팟 스파이웨어 PDF 파일(우)의 시각적 비교를 보여준다.

Fig. 3. Normal ID PDF file (left) and ID PDF file with payload (right)

두 문서는 시각적으로 확인했을 때 완전히 같은 문서임을 확인할 수 있다. Fig. 4.의 Windows 탐색기 비교 결과에서도 파일 크기가 모두 24KB로 동일함이 확인된다.

Fig. 4. Data size of normal ID PDF file and ID PDF file with payload

테스트베드 환경에서 수행된 실험 결과, 가상화된 공격자 시스템이 허니팟 스파이웨어가 포함된 PDF를 열었을 때 삽입된 페이로드가 즉시 실행되어 시스템 정보 수집, 키로깅, 네트워크 전송 모듈이 정상 작동하였다. 또한 수집된 로그는 설정된 주기에 따라 암호화된 형태로 C&C 서버로 전송됨을 확인했다.

본 연구는 기존의 사전 예방적 측면에서 탐지만 수행했던 기존의 연구와는 다르게[5-6][8][13-15], 더 나아가 공격자를 적극적으로 추적하고, 검거하는 데 초점을 맞춤으로써 피싱의 근본적인 원인을 해결하는 것에 기여한다는 점에서 차별성을 가진다.

V. Conclusion

본 연구는 급증하는 스미싱 범죄에 대응하기 위해 허니팟 기술과 스파이웨어를 결합한 능동적 스미싱 범죄 추적 방법론을 제안하였으며, 기존의 반응적 탐지 방식의 한계를 극복한 능동적 대응법을 통해 범죄 예방과 범죄자 추적을 가능하게 하는 새로운 패러다임을 제시했다. 제안된 6단계 추적 시나리오는 페이로드가 삽입된 PDF 파일 제작

부터 공격자 정보의 사법기관 서버 전송까지의 체계적인 과정을 구축하였으며, 허니팟 디바이스를 통한 능동적 유인 전략과 Adobe Reader JavaScript 엔진을 활용한 스파이웨어 배포 기법은 기존 연구와 차별화되는 핵심 기여점이다. 아울러 법적 제약사항을 고려한 주기적 로그 수집 방식을 설계하여 관련 법령을 준수하면서도 실용적인 운영을 가능하게 했다.

본 연구는 허니팟 스파이웨어를 사용하여 스미싱 범죄자들을 역추적하는 새로운 방향성에 대해 제안하고, 그 가능성을 살펴보는 탐색적 초기 연구라고 할 수 있다. 연구 결과, 허니팟 스파이웨어를 활용한 스미싱 범죄 역추적의 가능성을 살펴보고 제안한 6단계 추적 시나리오의 실험적 타당성을 테스트베드 환경에서 구현 및 검증하였다.

연구의 한계점은 다음과 같다. 먼저, 새로운 대응 방법을 제시하고, 이를 실험 환경에서 탐색적으로 진행한 만큼, 실제 스미싱 캠페인을 대상으로 하는 허니팟 스파이웨어 및 테스트베드 환경의 효과성을 검증하지 못해 일반화의 어려움이 존재하며, 기존의 연구 결과와 비교가 어렵다는 한계점을 가지고 있다. 아울러 Window의 Adobe Reader 하위 버전에서만 일관되게 작동하여, Linux와 macOS 등 다른 운영체제에서의 호환성 부족과 플랫폼 종속성 문제를 가지고 있다. 마지막으로, 공격자가 실행하는 Anti-Virus와 같은 탐지 시스템 회피에 대한 한계점을 가지고 있다. 향후 연구에서는 AI 기반 지능형 허니팟 시스템 구축, 크로스 플랫폼 호환성 확보, 이미지 스테가노그래피(steganography) 기법과 난독화를 적용한 탐지 회피 등을 바탕으로 발전시키고, 이를 실제 환경에 적용하여 구체적인 지표를 산출하는 것을 통해 더욱 효과적인 스미싱 범죄 추적 시스템을 구축할 수 있을 것으로 기대된다.

연구의 한계점에도 불구하고, 본 연구가 제시한 방법론은 스미싱 범죄 대응 패러다임을 수동적 탐지에서 능동적 예방으로 전환시키는 이론적 토대를 마련할 수 있었으며, 연구의 결과가 사이버 범죄 대응 분야의 실질적 발전과 사회적 안전망 구축에 중요한 기여를 할 수 있기를 기대한다.

ACKNOWLEDGEMENT

This work was supported by the PaiChai University research grant in 2025.

REFERENCES

[1] Financial Services Commission, "Watch out for cyber frauds such as smishing aimed at the Lunar New Year holiday!," Financial Services Commission, https://www.fsc.go.kr/no010101/83889.

[2] Keepnet Labs, "Smishing Statistics 2025: The Latest Trends and Numbers in SMS Phishing," Keepnet Labs, https://keepnetlabs.com/blog/smishing-statistics-the-latest-trends-and-numbers-in-sms-phishing.

[3] Proofpoint, "2024 State of the Phish – Today's Cyber Threats and Phishing Protection," Proofpoint, https://www.globenewswire.com/news-release/2024/02/27/2835744/35374/en/Proofpoint-s-2024-State-of-the-Phish-Report-68-of-Employees-Willingly-Gamble-with-Organizational-Security.html.

[4] A. I. Jung, "Smishing Attack via Text Message Disguised as 'Recycling Violation Report' from Government24," Chosun Ilbo, https://www.chosun.com/national/national_general/2024/04/01/MCZR52XKQJBMBKEJV3SSVMBKBU/.

[5] D. Goel, "Detection and Prevention of Smishing Attacks," arXiv, 31 Dec. 2024, https://arxiv.org/abs/2501.00260.

[6] D. Timko and D. H. Castillo, "A Quantitative Study of SMS Phishing Detection," arXiv, 12 Nov. 2023, https://arxiv.org/abs/2311.06911.

[7] M. M. Islam, M. A. Hossain, and M. S. Hossain, "Enhancing Cybersecurity: Hybrid Deep Learning Approaches to Smishing Attack Detection," Systems, vol. 12, no. 11, pp. 490, Nov. 2024. DOI: 10.3390/systems12110490

[8] D. Timko, D. H. Castillo, and M. L. Rahman, "Understanding Influences on SMS Phishing Detection: User Behavior, Demographics, and Message Attributes," NDSS Symposium, pp. 1-16, San Diego, CA, USA, Feb. 2025. DOI: 10.14722/usec.2025.23027

[9] A. K. Jain and B. B. Gupta, "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment," Procedia Computer Science, vol. 125, pp. 617-623, 2018. ICSCC. DOI: 10.1016/j.procs.2017.12.079

[10] S. M. Sanjari, J. Roberts, and M. M. A. Pritom, "Poster: A Few-Shot Learning Method for SMS Phishing Detection," in Proceedings of the 46th IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 2025. [Online]. Available: https://sp2025.ieee-security.org/downloads/posters/sp25posters-final23.pdf

[11] A. Kanaoka and T. Isohara, "Beyond Mobile Devices: A Cross-Device Solution for Smishing Detection and Prevention," in Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS), pp. 6-8, Anaheim, CA, USA, August 6–8, 2023. [Online]. Available: https://www.usenix.org/system/files/soups2023-poster13_kanaoka_abstract_final.pdf

[12] Y. J. Choi and J. Lee, "The change in the methods of smishing

in South-Korea after the onset of covid-19," Journal of Legal, Ethical and Regulatory Issues, vol. 24, no. S5, pp. 1-8, 2021. [Online]. Available: https://www.abacademies.org/articles/the-change-in-the-methods-of-smishing-in-southkorea-after-the-onset-of-covid19-12776.html

[13] A. F. Algarni, "Policing Internet fraud in Saudi Arabia: expressive gestures or adaptive strategies?," Policing and Society, vol. 23, no. 4, pp. 498–515, 2013, DOI: 10.1080/10439463.2013.780220

[14] J. S. Svensson and S. Saharso, "Proactive policing and equal treatment of ethnic-minority youths," Policing and Society, vol. 25, no. 4, pp. 393–408, 2015. DOI: 10.1080/10439463.2013.875015

[15] H.-M. Chen, R. Kazman, I. Monarch, and P. Wang, "Can cybersecurity be proactive? A big data approach and challenges," HICSS, 10 pages, Waikoloa, HI, USA, January 2017. DOI: 10.24251/HICSS.2017.725

[16] O. el Kouari, S. Lazaar, and T. Achoughi, "Fortifying industrial cybersecurity: a novel industrial internet of things architecture enhanced by honeypot integration," IJECE, vol. 15, no. 1, pp. 1089–1098, Feb. 2025. DOI: 10.11591/ijece.v15i1.pp1089-1098.

[17] A. N. Craig, S. J. Shackelford, and J. S. Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis," American Business Law Journal, vol. 52, no. 4, pp. 721–787, Dec. 2015. DOI: 10.1111/ablj.12055

Authors

Woo Jin Jung is currently pursuing the B.S. degree in the Department of Cyber Security at Pai Chai University in Daejeon, South Korea. His current research interests include Artificial Intelligence, Cyber Security and Deepfake Detection.

Seong-Cho Hong received the B.S. degree in Psychology in 2014, M.S.in Criminology in 2018 and Ph.D. in Legal Psychology. Dr. Hong joined the Smart ICT Convergence Human Resource Development Center at Pai Chai University, Daejeon, Korea, as a Research Professor in 2025. He is interested in criminal behavior, need for cognition, theoretical framework and convergence research.

Ah Reum Kang received the M.S. and Ph.D. degrees in information security from Korea University, South Korea, in 2012 and 2016. She is a professor in the Department of Information Security at Pai Chai University in Daejeon, South Korea. Her current research interests include security, artificial intelligence, malware, medical data analysis, and online game security.