한국컴퓨터정보학회 하계학술대회 논문집 제31권 제2호 (2023. 7)

모바일 장치에 대한 멀웨어의 영향 탐색

이준호*, 박재경O
*한국폴리텍대학교 사이버보안학과,
O한국폴리텍대학교 사이버보안학과
e-mail: leejonho5177@gmail.com*, jakypark@kopo.ac.krO

A Exploring the impact of malware on mobile devices

Jun-ho Lee*, Jae-kyung ParkO
*Dept. of Information Security, Korea Polytechnic,
ODept. of Information Security, Korea Polytechnic

● 요 약 ●

모바일 멀웨어는 민감한 데이터의 도용, 기기 성능 저하, 금전적 피해 유발 등 다양한 위협을 내포하고 있으며 특히 피싱, 앱 기반 공격 및 네트워크 기반 공격과 같은 기술을 통해 모바일 장치를 악용할 수 있다. 이를 해결하기 위해 바이러스 백신 소프트웨어 및 강력한 암호 사용과 같은 보안 기술을 구현하면 모바일 멀웨어의 영향을 방지하고 완화하는 데 도움이 될 수 있다. 추가적으로 개인과 조직이 모바일 멀웨어와 관련된 위험을 인식하고 불리한 결과를 피하기 위해 이를 차단하기 위한 사전 조치를 취하는 것이 중요하다. 본 논문에서는 이러한 조치에 대한 보안 예방책을 제안하고자 하며 이를 통해 보다 안전한 모바일 환경을 갖출 수 있을 것이라 판단한다.

키워드: 모바일(Mobile), 탐지(Detection), 멀웨어(Malicious Software), 백신(Vaccine), 차단(Prevention)

I. Introduction

현대 사회에서 모바일 장치의 보급이 증가함에 따라 모바일 멀웨어(Mobile Malware)의 증가가 눈에 띄게 증가하고 있다. 모바일 멀웨어는 악의적인 의도를 가지고 설계된 소프트웨어로서, 모바일 기기의 안전과 개인 정보의 보호에 위협을 가하며, 이로 인해 개인, 기업 및 사회적 손실이 발생할 수 있다. 이에 따라, 모바일 멀웨어의 영향을 탐색하고 이에 대응하는 방안을 모색하는 것은 중요한 연구 주제가 되었다.

본 논문은 모바일 장치에 대한 멀웨어의 영향을 탐색하는 데 초점을 맞추었다. 멀웨어는 다양한 형태로 나타날 수 있으며, 악성 앱, 스파이웨어, 랜섬웨어 등 다양한 유형이 존재한다. 이러한 멀웨어는 모바일 기기의 운영체제에 침투하여 사용자의 개인 정보를 탈취하거나, 악성 코드를 실행하여 기기의 기능을 마비시키는 등 다양한 피해를 줄 수 있다.

모바일 멀웨어의 영향는 개인과 조직의 차원에서 다양한 영향을 미친다. 개인 차원에서는 개인 정보의 유출, 금전적 손실, 사생활 침해 등의 문제가 발생할 수 있다. 조직적 차원에서는 기업의 기밀 정보 유출, 고객 정보 유출, 서비스 중단 등으로 인한 금전적 및 평판적 손실이 발생할 수 있다.

본 연구의 목적은 모바일 멀웨어의 영향을 종합적으로 조사하고, 개인 및 조직에게 미치는 영향을 분석하는 것이다. 이를 통해 모바일 멀웨어에 대응하기 위한 정책 및 보안 기술 개발에 기여할 수 있을 것으로 기대된다. 연구 방법론으로는 기존의 연구 및 보고서를 검토하고, 실제 사례를 분석하여 모바일 멀웨어의 영향을 탐구할 예정이다.

이 논문의 구성은 다음과 같다. 첫째, 모바일 멀웨어의 개념과 유형에 대해 설명한다. 둘째, 모바일 멀웨어가 가져오는 개인 및 조직에게 미치는 영향을 살펴본다. 셋째, 모바일 멀웨어에 대응하기 위하여 현재 사용하고 있는 기술과 정책을 알아본다. 넷째, 본 연구의 방법론과 분석 프로세스에 대해 설명한다. 마지막으로, 본 연구의 결과와 결론을 제시하고 향후 연구 방향을 제안할 예정이다.

II. Preliminaries

1. Related works

1.1 모바일과 멀웨어의 정의

"모바일"이라는 용어는 일반적으로 스마트폰, 태블릿 및 기타 휴대용 전자 장치와 같이 이동 중에 사용하도록 설계된 장치를 지칭한다. 이러한 장치는 일반적으로 무선 연결이 가능하며 인터넷에 액세스하고, 전화를 걸고, 메시지를 보내고, 기타 다양한 작업을 수행하는 데 사용할 수 있다. 모바일 장치는 최근 몇 년 동안 점점 더 보편화되었다. "멀웨어"는 컴퓨터 시스템, 네트워크 또는 모바일 장치에 피해를 입히도록 특별히 설계된 소프트웨어를 설명하는 데 사용되는 용어이다. 여기에는 바이러스, 웜, 트로이 목마, 스파이웨어, 애드웨어 및 기타 악성 프로그램이 포함될 수 있다. 멀웨어는 민감한 데이터 도용, 장치 제어, 시스템 기능 중단, 금전적 피해 유발 등 다양한 목적으로 사용될 수 있다. 멀웨어는 종종 이메일 첨부 파일, 감염된 웹 사이트 또는 기타 형태의 사회 공학을 통해 확산된다. 아래 그림 1에서와 같이 2023년에도 여전히 5대 보안 위협에 모바일이 포함된 것을 알 수 있다. 따라서 모바일에 대한 보안 위협 제거는 무엇보다도 중요할 것으로 판단한다.

Fig. 1. Security Outlook 2023 - Top 5 Cybersecurity Threats

먼저, 발전방안의 기술을 살펴보면 이해그룹의 장점과 단점을 살펴보며,

Table 1. System Environment

Item	Value
CPU Clock Speed	100 ~ 500 MIPS
Memory Size	32 ~ 256 MB
System File Size	16 MB

III. The Proposed Scheme

3.1 모바일 장치에 대한 멀웨어의 영향 및 개요

모바일 멀웨어는 민감한 데이터를 훔치고, 장치의 제어권을 탈취당하며, 기기 성능을 저하시키고, 배터리의 수명을 빠르게 저하시키는 것과 더불어 금전적 피해를 끼칠 수 있기에 개인과 조직 모두에게 중대한 위협을 끼친다 개인과 조직에 중대한위협이다. 여기서의 멀웨어란 악성 소프트웨어(Malicious Software)의 줄임말인 멀웨어는 컴퓨터 또는 네트워크를 손상 또는 파괴하거나 비도덕적인 범죄 목적으로 컴퓨터, 네트워크 또는 데이터에 무단 액세스하도록 작성된 소프트웨어 코드이다. 모바일 장치의 멀웨어는 로그인 자격 증명, 개인 정보, 금융 데이터 및 기밀 비즈니스 정보의 도용으로 인하여 신원 도용, 재정적 손실 및 평판 손상을 초래할 수 있다. 또한 멀웨어는 모바일 장치의 보안과 성능을 손상시켜 생산성의 저하를 야기할 수 있다.

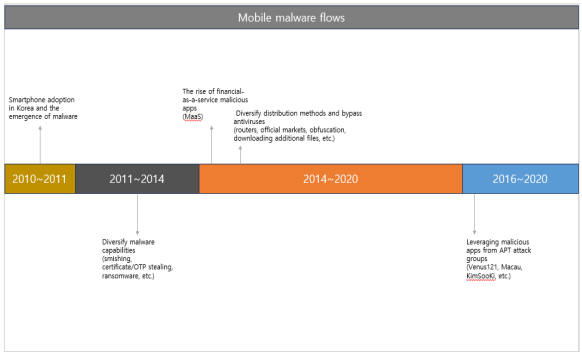

Fig. 2. Mobile malware flows

그림 2에서와 같이 스마트폰이 도입된 이후로 지속적으로 멀웨어에 대한 위협도 증가하고 있음을 알 수 있다. 또한 회사 소유 장치의 멀웨어로 인해 잠재적으로 법적 책임과 재정적 손실을 초래하는 재정적 피해로 이어질 수 있다. 따라서 바이러스 백신 소프트웨어 사용, 운영 체제 및 애플리케이션 업데이트, 앱 다운로드 및 설치 또는 알 수 없는 출처의 링크 열기 등 모바일 멀웨어의 영향을 방지하고 완화하기 위한 조치를 취하는 것이 중요하다.

3.2 모바일 멀웨어의 보안 기술

모바일 멀웨어는 다양한 기술을 사용하여 모바일 장치의 취약성을 악용하고 보안을 손상시킬 수 있으므로 개인과 조직에 상당한 위협이 된다. 피싱, 앱 기반 공격, 운영 체제 취약성, 드라이브 바이 다운로드, SMS 기반 공격, 네트워크 기반 공격, 루팅 또는 탈옥은 모바일 멀웨어가 사용하는 가장 일반적인 기술 중 하나이다. 이러한 기술은 민감한 정보를 훔치거나, 장치를 제어하거나, 다른 장치로 확산되어 신원 도용, 금전적 손실 및 명예 실추에 사용될 수 있다. 모바일 멀웨어의 영향을 방지하고 완화하려면 사용자가 이러한 기술을 인식하고 바이러스 백신 소프트웨어 사용, 운영 체제 및 애플리케이션 업데이트, 앱 다운로드 또는 열 때 주의 등 장치를 보호하기 위한 적절한 조치를 취하는 것이 중요하다.

3.3 모바일 장치의 멀웨어 감염 방지: 모범 사례 및 전략

증가하는 모바일 멀웨어의 확산은 개인과 조직에 심각한 위협이 되므로 멀웨어를 차단하고 감염을 방지하기 위한 효과적인 전략을 채택하는 것이 중요하다. 멀웨어를 효과적으로 차단하려면 사용자는 가장 일반적인 감염 벡터를 이해하고 모바일 장치 보안을 위한 모범 사례를 구현해야 한다. 여기에는 바이러스 백신 소프트웨어 사용 및 최신 상태 유지, 알 수 없는 소스에서 앱 다운로드 또는 링크

열기 방지, 운영 체제 및 애플리케이션 정기적 업데이트, 모든 계정에 대해 강력하고 고유한 암호 사용이 포함된다. 또한 조직은 모바일 장치 관리 솔루션을 구현하여 보안 정책을 시행하고 잠재적인 위협이 있는지 장치를 모니터링하며 위반 시 데이터를 원격으로 지울 수 있다. 또한 사용자 교육 및 인식 캠페인을 사용하여 모바일 멀웨어 및 감염 방지 방법에 대한 지식을 높일 수 있다. 이러한 전략과 모범 사례를 구현함으로써 개인과 조직은 멀웨어 감염 위험을 크게 줄이고 중요한 정보가 손상되지 않도록 보호할 수 있다. 다음 표 2은 모바일 장치의 보안 조치에 대해 나열하고 있다.

Table 2. Security measures strategy topics

Category	Action Description
Use an antivirus	Installan antivirus-enabled app
User training	User education and awareness campaigns
Disable unauthorized apps	Prevent downloading apps or opening links from unknown sources
Update	Regularly update your operating system and applications
Periodic checks and backups	Periodically check user phones and back up key data

위의 표의 내용 중에서 가장 중요한 사항은 주기적 점검 및 백업이라고 판단하며 본 논문에서는 이 부분에 대한 중요성을 강조하고 싶다. 그림 3과 같이 모바일 환경에서 랜섬웨어의 피해를 예방하기 위해 5가지의 수칙을 준용하기를 권고하고 있으며 그 중 가장 중요한 사항은 주기적인 백업이라고 판단한다.

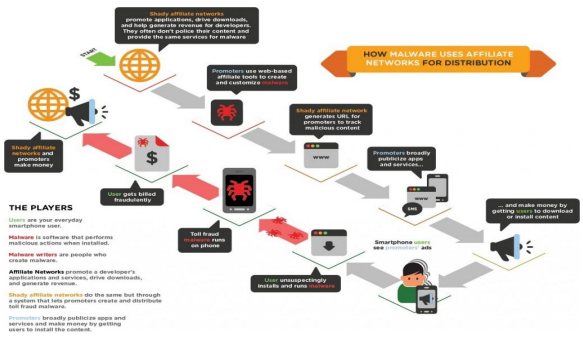

Fig. 3. Most affecting and Active Malwares on Mobile Devices

이를 위해 모바일 환경에서는 다양한 백업을 제안하고 있으며 이 중 클라우드 백업을 다중으로 할 것을 권고하고 싶다. 백업의 종류로는 아래의 목록 같이 여러 종류들이 있다.

- 로컬 백업
- 클라우드 백업
- 스냅샷 백업

이 중에서 사용자가 가장 쉽게 접근할 수 있는 방안은 클라우드 백업이라고 판단한다.

IV. Conclusions

모바일 멀웨어는 금전적 손실, 평판 손상, 민감한 정보 손상을 유발할 수 있으므로 개인과 조직에 중대한 위협이 된다. 멀웨어는 다양한 기술을 사용하여 피싱, 앱 기반 공격, 운영 체제 취약성, 드라이브 바이 다운로드, SMS 기반 공격, 네트워크 기반 공격, 루팅 또는 탈옥을 포함하여 모바일 장치의 취약성을 악용할 수 있다. 이러한 기술은 데이터 도용, 장치 제어, 성능 저하, 배터리 소모, 다른 장치로의 확산 및 재정적 피해로 이어질 수 있다. 모바일 멀웨어의 영향을 방지하고 완화하려면 사용자가 위험을 이해하고 바이러스 백신 소프트웨어 사용, 운영 체제 및 애플리케이션 업데이트, 앱 다운로드 방지 또는 알 수 없는 출처의 링크 열기와 같은 모바일 장치 보안에 대한 모범 사례를 구현하는 것이 중요하다. 강력하고 고유한 암호를 사용하다. 또한 조직은 모바일 멀웨어로부터 보호하기 위해 모바일 장치 관리 솔루션, 사용자 교육 및 인식 캠페인을 구현할 수 있다. 이러한 전략과 모범 사례를 채택함으로써 개인과 조직은 멀웨어를 효과적으로 차단하고 감염 위험을 줄이며 중요한 정보가 손상되지 않도록 보호할 수 있다고 판단한다.

REFERENCES

[1] Ryosuke Kokado "A Countermeasure against Ransomware and Their Implementation" Proceedings of the Computer Security Symposium 2020 pp. 926-931, october 2020.

[2] Hwang, Dong-Ryeol. "A Study on Ransomware Response System." D. Dissertation, Hanser University Graduate School, 2018. Chungcheongnam-do, South Korea

[3] Jung, Heeja. "Real-time integrated network file management system in cloud computing environment." D. thesis, Honam University Graduate School, 2014.

[4] Wuk Chitrapanjaknit. "Detection and classification of code obfuscation and native code-based malware on Android." Master's thesis, Kyungmyeong University, 2018. Daegu, Korea