한국컴퓨터정보학회 동계학술대회 논문집 제27권 제1호 (2019. 1)

# 악성코드 동향에 따른 새로운 방어 전략 연구

박재경O, 이형수*
O*한국폴리텍대학 서울강서캠퍼스 정보보안과
e-mail: {jakypark, hslee01}@kopo.ac.krO*

# A Study of New Prevention Strategy According to the Trend of Malicious Codes

Jae-kyung ParkO, Hyung-Su Lee*
O*Dept. of Information Security, Korea Polytechnics College

● 요 약 ●

본 논문에서는 2018년에 성횡한 악성코드에 대한 피해 사례를 살펴본 후 이를 적극적으로 대응하기 위한 방안을 살펴본다. 특히 가상통화 거래소에 대한 해킹 사고 및 가상화폐에 대한 지속적인 해킹 시도가 탐지되면서 관련 소식들이 언론에 지속적으로 보도되었다. 또한 이와 관련하여 PC 및 서버 자원을 몰래 훔쳐 가상통화 채굴에 사용하는 크립토재킹 공격기법도 함께 주목받았다. 랜섬웨어 부문은 갠드크랩 관련 보도가 대부분을 차지할 정도로 국내에서 지속적으로 이슈가 되었다. 또한 미국 법무부에서 최초로 북한 해커조직의 일원을 재판에 넘기면서 해커 그룹에 대한 관심이 집중되기도 했다. 2018년 전반적으로 이러한 가상통화 거래소 해킹, 크립토재킹, 랜섬웨어, 해커 그룹의 4가지 키워드를 도출하였으며, 이 중 해커 그룹은 북한과 중국의 경우를 나누어 총 5가지 주제를 통해 악성코드에 대한 주요 이슈들을 살펴본다. 본 논문에서는 이러한 악성코드의 공격을 근본적으로 해결할 수 있는 방안으로 클라이언트 측에 USB형태의 BBS(Big Bad Stick) 하드웨어를 통하여 제안하는 환경을 제안하고 안전한 서비스가 제공됨을 증명하여 본 연구가 새로운 보안성을 갖춘 시스템임을 보인다.

**키워드:** Maleare, Prevention, Security Strategy, Malicious Code, CCN

## I. Introduction

2018년에 가장 주목받은 사이버 공격은 '랜섬웨어'와 '가상화폐 해킹' 이다. 지난 12월 8일 과학기술정통부 주관으로 한국인터넷진흥원을 포함한 보안 기업들이 2018년 7대 사이버 공격 전망을 발표했다. 그 중 랜섬웨어와 가상화폐 해킹이 포함돼 있었다.

랜섬웨어는 사용자가 자신의 시스템에 접근을 인질로 삼는 공격이다. 사용자는 해커에게 금전 대가를 지급하기 전까지 해당 시스템에 접근할 수 없다. 2018년 상반기에 랜섬웨어가 큰 주목을 받은 이유는 워너크라이와 패트야 때문이다. 작년 5월 워너크라이로 인해 150개국의 30만대 기기가 랜섬웨어 피해를 보았고, 이어 7월에는 패트야로 2,000여 기관이 피해를 보았다.

가상화폐 해킹도 큰 이슈였다. 가상화폐 시세가 급등하면서, 이를 노리는 해킹이 급증한 것이다. 비트코인의 경우, 2018년 한 해 동안 시세가 20배 이상 폭증했다. 1월 시세는 100만 원가량이었는데 12월에는 2,000만 원을 넘어선 것이다. 가상화폐 지갑을 노리거나, 개인기기를 가상화폐 채굴로 이용하는 공격이 많았다. 랜섬웨어와 가상화폐 해킹은 사이버 공격 패러다임을 변화시키고 있다. 개인을 대상으로 한 사이버 공격이 많아질 것이라는 의미이다. 기존에는 특정 기관을 대상으로 한 사이버 공격이 많았다. 해킹의 가장 큰 목적은 '금전 이득'인데, 개인 대상으로는 이를 달성하기에 충분치 않았기 때문이다. 그러다 보니 공격 수법도 정교했다. 지능형 지속 공격 (APT - Advanced Persistent Threat)은 특정 대상을 목표로 장기간에 걸쳐서 가하는 사이버 공격이다. 특정 대상의 관련 정보 수집은 물론이고, 여러 해커가 모여서 침투 방법을 끊임없이 논의한다. 그런데 랜섬웨어와 가상화폐 해킹은 개인을 대상으로도 금전 이익을 충분히 얻을 수 있게 한다. 랜섬웨어의 경우, 개인의 컴퓨터와 데이터를 인질로 금전적인 대가를 요구해서 이익을 얻을 수 있다. 가상화폐의 경우, 개인 가상화폐 지갑을 탈취하거나 기기를 채굴로 활용해서 금전 이익을 얻을 수 있다. 정리하면, 랜섬웨어와 가상화폐 등장으로 개인 대상으로 한 해킹이 늘어나고 있다. 개인의 보안 수준은 기관과 비교했을 때 상당히 낮다. 대규모 보안 장비를 갖춰서 사내 네트워크를 보호하는 기관과 달리, 개인은 고작해야 기기에 설치한 백신이 전부이다. 그러므로 개인 대상 시스템 침투 시에는 정교한 사이버 공격 수법이 필요 없다. 단지, 악성코드를 가장 많이 감염시킬 방법이 최선의 전략이다. 많이 감염시킬수록, 얻을 수 있는 금전 이익이 더 커지기 때문이다. 이러한 전략에 가장 적합한 공격 수법은 '익스플로잇 (Exploit)'이라고 할 수 있다. 익스플로잇은 시스템 취약점을 악용해

서 사이버 공격을 감행하는 수법이다. 개인 대상 공격이 많아질 것으로 예상하기 때문에, 악성코드 배포가 쉬운 '익스플로잇'이 2018년 최대 사이버 위협이 되었다.

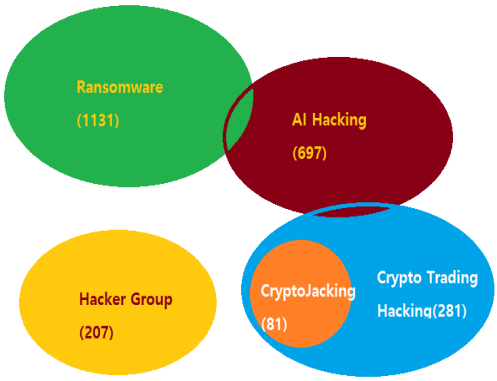


Fig. 1. Keyword in Cyber Hacking

## II. The Proposed Scheme

본 논문에서 제안하고자 하는 시스템은 기존의 전통적인 서비스 구성은 해킹을 근본적으로 피할 수 없는 구조를 가지고 있으므로 인해 아무리 많은 보안장비를 서버 앞에 설치를 하더라도 취약점이 발생하면 해킹을 당할 수 밖에 없는 구조이다. 따라서 근본적으로 해킹이 불가능한 구조를 만들어 해킹을 원천차단하고 하는 것이 본 논문의 목표이다.

랜섬웨어 부문에서는 2분기까지 널리 악용된 갠드크랩 랜섬웨어가 더욱 진화된 모습으로 변신을 거듭하며 3분기에도 독보적으로 많이 언급되었다. 7월에는 NSA 툴에 탑재된 이터널블루(EternalBlue) 취약점을 활용하는 변종이 나타났고 북한 폰트파일로 위장하여 유포된 바 있으며, 9월에는 공정거래위원회를

사칭하는 유포 방식이 발견되었다. 일부 버전에서는 안랩의 V3 Lite 제거를 유도하는 기능도 발견된 바

있다. 갠드크랩은 10월 2일 5.0대 버전까지 발견되면서 끊임없이 변종들이 나타나고 있다. 이를 위해 본 논문에서는 별도의 클라이언트 시스템을 활용하여 클라이언트를 통해 해킹을 완벽하게 방어하는 방안을 제안한다.

## III. Conclusions

위에서 설명한 바와 같이 기존의 서비스의 구조를 변경하고 특정 프로토콜을 통해 암호화 통신을 수행할 경우 기존의 해킹방법으로는 해킹자체가 이루어지지 않는 시스템을 제안하였다. 본 시스템을 통해 보다 안전한 형태의 서비스가 이루어질 것이라고 판단한다.

## REFERENCES

[1] Jae-Kyung Park, Young-Ja Kim, "A Design of Client BBS System for Secure HVA", Journal of The Korea Society of Computer and Information Vol. 23 No. 9, pp. 73-80, September 2018.

[2] Sung-Jin Kim, Jae-Kyung Park, "Strengthening Authentication Through Content Centric Networking" Journal of The Korea Society of Computer and Information Vol. 22 No. 4, pp. 75-82, April 2017.

[3] Jay-Kyung Park, Won Joo Lee, Kang-Ho Lee, "A Study on the Isolated Cloud Security Using Next Generation Network" Journal of The Korea Society of Computer and Information Vol. 22 No. 11, pp. 41-48, November 2017.

[4] Hyung-Su Lee, Jae-Pyo Park, Jae-Kyung Park, "A Network Transport System Using Next Generation CCN Technology" Journal of The Korea Society of Computer and Information Vol. 22 No. 10, pp. 93-100, October 2017.