악성코드 유형별 공격동향

김종도[O], 이훈재[*], 이영실[**]
[O]동서대학교 일반대학원 디지털포렌식학과,
[*]동서대학교 정보보안학과,
[**]동서대학교 International College
e-mail: jongdorai@naver.com[O], hjlee@dongseo.ac.kr[*], lys0113@dongseo.ac.kr[**]

Attack Trends by Malware Type

JongDo-Kim[O], Hoon-Jae Lee[*], Young-Sil Lee[**]
[O]Dept. of Digital Forensic, Dongseo University,
[*]Dept. of Information Security, Dongseo University,
[**]Dept. of Computer Engineering English Track, International College, Dongseo University

● 요 약 ●

코로나19로 인한 비대면 사회의 발전으로 일반인들의 IT이용이 증가하였고, 우크라이나 전쟁이 장기화 됨에 따라 주요 기반시설 및 글로벌 기업을 대상으로 대규모 사이버 공격 시도가 증가할 것으로 전망된다. 사이버 공격에는 대부분 악성코드가 활용이 된다. 본 논문에서는 2022년 및 2023년 1분기 중 사이버공격에 많이 활용된 악성코드들의 특징과 동향을 파악한다.

키워드: 정보탈취형악성코드(InfoStealer), 백도어(BackDoor), 서비스형악성코드(MaaS)

I. Introduction

2019년 코로나19로 인한 비대면 사회가 발전하면서 일반인들의 IT이용이 크게 증가하였으며 유무선 인터넷 기반의 여가활동, 재택활동과 관련된 서비스들이 크게 활성화 되었다. 이에 따라 보안이 상대적으로 취약한 원격 및 재택환경을 노린 공격이 늘어났다.

과학정보기술통신부와 한국인터넷진흥원이 발표한 2023 사이버 보안 위협 전망에 따르면 우크라이나 사태가 장기화 됨에 따라 23년도에도 글로벌 해킹 조직의 활동은 증가할 것이며, 주요 기반시설이나 글로벌 기업을 대상으로 대규모 사이버 공격 시도가 지속될 것이라고 전망하였다.[1]

최근 사이버 공격에 활용된 악성코드의 유형별 통계를 살펴보면 2022년 상반기와 3분기에는 정보탈취형 악성코드가 66.7%와 55.1%로 가장 많은 비중을 차지했고, 4분기와 2023년 1분기에는 다운로더가 42.5%, 백도어가 39.8%로 가장 많은 비중을 차지하였다.[2-5]

다운로더는 자체적인 기능보다 추가 악성코드를 설치하는 것이 목적인 악성코드로, 주로 정보탈취형 악성코드를 설치한다.

따라서, 본 논문에서는 악성코드 중 정보탈취형 악성코드와 백도어의 공격동향 및 대응방안을 제시한다.

II. Types of Malware

1. Malware

1.1 정보탈취형 악성코드

정보탈취형 악성코드는 데이터 유출과 탈취를 목적으로 하며 운영체제나 프로그램에 저장된 자격 증명과 각종 정보를 탈취하는 악성코드다. RedLine Stealer의 경우 탈취한 정보를 공격자의 C&C서버(Command and Contro Server)와 연결하여 탈취한 정보를 전송하고, 공격자의 명령을 수신하여 추가 악성코드 다운로드, 지정된 명령 수행등 다양한 악성행위를 수행한다. 정보탈취형 악성코드는 탈취한 여러 가지 정보등을 활용하여 다크웹에서 판매하거나 크리덴셜 스터핑 공격을 통해 개인정보를 유출하는 등 2차 피해가 발생 할 수 있다.

1.2 백도어

백도어는 시스템에 접근하기 위한 인증 절차를 우회하여 접근할 수 있도록 하는 악성코드이다. 이를 통해 공격자가 시스템의 정보를 수집하거나 추가적인 악성코드 설치를 할 수 있고 시스템에 대한 전체적인 제어권을 획득 할 수 있는 기능이 있다. 북한 해킹조직 라자루스는 DTrack을 활용하여 인도원자력공사 (NPCIL) 네트워크를 공격하여 원자력발전소 가동을 중단시켰으며, 최근에는 독일,

브라질, 이탈리아, 멕시코, 스위스, 미국 등 디트랙을 활용한 공격을 하고 있다.[6]

2. Malware Trend

2.1 길버트 아라베디언 기법

길버트 아라베디언 기법은 유명 해커 출신 보안 컨설턴트인 길버트 아라베디언이 나눈 해커등급으로 공격 수준에 따라 Lamer등급에서 Elite등급까지 5단계로 나눈다.[7]

Lamer 등급의 경우 컴퓨터에 지식이 없는채 단순히 해커를 동경하는 사람들 뜻한다.

Elite 등급의 경우 시스템에 존재하는 취약점을 찾아 아무런 흔적을 남기지 않고 해킹할 수 있는 수준의 해커를 뜻한다.

2.2 서비스형 악성코드

기존의 사이버공격은 소프트웨어 엔지니어링, 보안 및 네트워킹에 대한 지식이 있어야 공격을 수행할 수 있었다. 하지만 서비스형 악성코드가 나타나면서 Lamer등급의 해커도 일정 금액을 지불하면 사이버 공격을 할 수 있게 되었다.

서비스형 악성코드는 악성코드를 판매할 뿐만 아니라 구체적인 사용방법이나 멘토링을 악성코드 구매자에게 서비스를 제공하는 형태로 발전하고 있다.

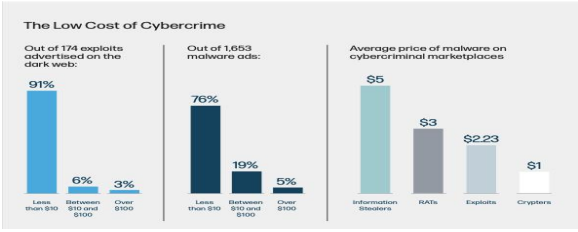

Fig. 1. DarkWeb MaaS Market Stats

'FIg 1'은 HP Wolf Security가 분석한 다크웹이나 해킹 포럼에서 유통되는 서비스형 악성코드들의 시세 통계이다.[8]

서비스형 악성코드의 비용을 살펴보면 평균 10달러 미만으로 구매가 가능한 것으로 나타났다.

III. Conclusions

본 논문에서는 사이버공격에 많이 활용된 악성코드의 유형별 기능과 최근 동향을 살펴보았다.

다크웹에서 서비스형 악성코드의 시장이 형성 및 확대되면서 무차별적으로 악성코드를 유포할 가능성이 커졌다.

이러한 악성코드를 유포하는 방법 중 대부분은 스팸메일 발송과 변조된 상용 프로그램 업로드 등이 있다.

이러한 악성코드에 대응하기 위해서는 운영체제 및 사용 프로그램의 최신 업데이트 적용 및 백신 프로그램의 실시간 탐지 활성화, 변조된 상용 프로그램 미사용, 정기적인 백업 등 기술적인 대응 보다는 사용자의 보안교육이 필요하다.

ACKNOWLEDGMENT

이 논문은 2023년 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (해양 디지털 항로표지 정보협력시스템 개발 (3/5) (20210650))

REFERENCES

[1] ICT Information Sharing & Analysis Center, "2023 Cybersecurity Threat Outlook Report," Jan 2023.

[2] AhnLab, https://blog.ahnlab.com/2516

[3] AhnLab Security Emergency Response Center, "Malicious Code Threat Statistics for Q3 2022," ASEC REPORT, Vol. 108, pp. 3-10, .Q3 2022.

[4] AhnLab Security Emergency Response Center, "Malicious Code Threat Statistics for Q4 2022," ASEC REPORT, Vol. 109, pp. 3-11, .Q4 2022.

[5] AhnLab Security Emergency Response Center, "Q1 2023, what is the most threatening malware?," ASEC REPORT, Vol. 110, pp. 3-11, .Q1 2023.

[6] Kaspersky, https://www.kaspersky.com/about/press-releases/2022_andariel-a-lazarus-subgroup-expands-its-attacks-with-new-ransomware, Aug 2022

[7] AhnLab, https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=19236

[8] HP Wolf Security, "The Evolution of Cybercrime: Why the DarkWeb is Supercharging the Threat Landscape and How to Fight Back," AN HP Wolf Security Report, pp. 12-14, July 2022.