# WannaCryptor 랜섬웨어 확산 예측 모델 연구

박태환*, 김경백**, 신원***

* ㈜안랩, ** 전남대학교 전자컴퓨터공학부, *** 동명대학교 정보보호학과

# A Prediction Model for the Spread of WannaCryptor Ransomware

Tae Hwan Park*, Kyung Baek Kim**, Weon Shin***

* AhnLab, Inc.

** Div. of Electronics and Communication Engineering, Computer and Information, Chonnam National University

*** Dept. of Information Security, Tongmyoung University

**요 약**

WannaCryptor는 사용자 데이터를 암호화하여 돈을 요구하는 랜섬웨어임에도 불구하고 Windows 운영체제의 공유폴더 취약점을 이용하여 스스로 확산하는 인터넷 웜과 같은 특징을 가진다. 본 논문에서는 기존 랜섬웨어와는 차별화되는 WannaCryptor의 확산 방식에 초점을 맞추어 확산을 분석하고 예측한다. 이를 위하여 가상 환경에서 동작 실험을 진행하였고, 확산 예측 모델링을 통하여 다양한 환경에서 WannaCryptor 확산의 양상을 분석하였다.

## I. 서론

랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램을 말한다[1]. 일반적으로 랜섬웨어는 신뢰할 수 없는 사이트, 스팸메일, 파일공유 사이트, 네트워크를 통해 유포되는데, 사용자의 동작이 수반되는 경우가 대부분이다. WannaCry, WannaCrypt 등 여러 이름으로 불리는 WannaCryptor 랜섬웨어는 다양한 문서 파일을 암호화하여 이를 인질로 금전을 요구하는 방식은 다른 랜섬웨어와 유사하다. 그러나 사용자의 동작에 의해 확산하는 기존 랜섬웨어와는 달리, WannaCryptor는 Windows 운영체제의 SMB(Sever Message Block) 취약점을 이용하여 악성코드를 감염시킨 후 접속 가능한 IP 주소를 스캐닝하여 네트워크 통해 다른 시스템으로 확산하는 형태를 가진다[2][3].

이러한 WannaCryptor 랜섬웨어의 확산 방식은 과거 자기 자신을 복제하여 네트워크로 확산하는 인터넷 웜 확산과 동일한 방식으로 기존 랜섬웨어 확산의 한계를 뛰어넘는 매우 효과적인 방식이다. 또한, 확산 과정 중 무한하게 발생되는 패킷은 네트워크에 오버헤드를 초래할 뿐 아니라 WannaCryptor의 희생자가 새로운 공격자가 되어 다른 시스템을 사용불능으로 만듦으로써 결과적으로 특정 네트워크 환경을 대상으로 하는 분산 서비스 거부 공격과 유사한 효과를 유발할 수도 있다.

본 논문에서는 기존 연구가 WannaCryptor 랜섬웨어의 세부 동작에만 초점을 맞추고 있는 것에 탈피하여 거시적 관점에서 WannaCryptor 확산에 초점을 맞추어 네트워크 환경에 따른 확산 예측을 하고자 한다. 먼저 2장에서는 기존 악성코드 확산 모델과 WannaCryptor 동작에 대하여 살펴보고, 3장에서는 네트워크 환경에서 WannaCryptor 확산 예측 모델링을 통하여 실

제 환경을 고려한 시뮬레이션을 수행한 후 마지막 4장에서 결론을 맺는다.

## II. 확산 모델링과 WannaCryptor 동작

### 1. 악성코드 확산 모델링

Cliff C. Zou 등[4]은 인터넷 웜의 스캐닝 방식에 따라 웜 확산 방식의 성능을 분석하였는데, 인터넷 주소 공간, 즉 IP 주소에 대해 무작위 스캐닝을 수행하는 RCS(Random Constant Spread) Worm의 동작에서 다음 식을 유도하여 인터넷 환경의 일반적인 웜 확산을 설명하였다.

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)],\ \beta = \frac{\eta}{\Omega}$$

여기서, $\beta$는 웜 확산율, $\eta$는 웜의 단위 시간 당 평균 스캐닝 수, $\Omega$는 웜이 스캐닝할 수 있는 전체 호스트의 주소 공간(IP 주소), $N$은 감염가능한 전체 취약 호스트 수, $I(t)$는 시각 $t$에 감염된 호스트 수를 나타낸다.

서로 다른 네트워크 $i$, $j$가 연결되어 융합망이 구성되어 있고 각각의 속도로 웜이 확산된다면 $t$시점의 감염 호스트 수는 다음 식과 같다[5].

$$\begin{aligned}\frac{dI_i(t)}{dt} &= \beta_i(t)I(t)S_i(t)S_i(t)/N + \beta_i(t)I(t)S_j(t)S_j(t)/N \\ &= \beta_i(t)I(t)\left[S_i(t)S_i(t) + S_j(t)S_j(t)\right]/N \\ \frac{dI_j(t)}{dt} &= \beta_j(t)I(t)S_j(t)S_j(t)/N + \beta_j(t)I(t)S_i(t)S_i(t)/N \\ &= \beta_j(t)I(t)\left[S_i(t)S_i(t) + S_j(t)S_j(t)\right]/N\end{aligned}$$

단, $\frac{dI(t)}{dt} = \frac{dI_i(t)}{dt} + \frac{dI_j(t)}{dt}$

여기서, $I_x(t)$는 네트워크 $x$에서 $t$시점의 감염된 호스트 수를 나타내고, $S_x(t)$는 네트워크 $x$에서 $t$시점의 취약 호스트 수로 $N - I_x(t)$와 같다.

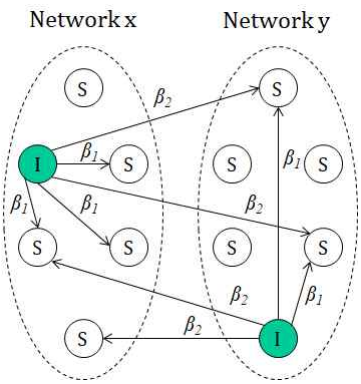


Fig. 1 Localized scanning of WannaCryptor

WannaCryptor는 Fig. 1과 같이 Network x와 y에서 감염된 호스트 I는 로컬 네트워크에서는 $\beta_1$의 확산율로, 다른 네트워크에서는 $\beta_2$의 확산율로 확산한다. 이러한 확산 방식은 동일 네트워크에 같은 운영체제를 설치하여 사용하는 경우, 하나의 호스트가 취약하여 WannaCryptor에 감염된 경우 인근의 다른 호스트들도 감염될 확률이 매우 높아진다는 것을 의미한다.

융합망에서 서로 다른 속도로 확산하는 웜 확산 특성에 착안하여 WannaCryptor가 네트워크 $x$, $y$에 확산한다고 가정하면 $t$시점의 감염 호스트 수는 다음 식을 통하여 구할 수 있다.

$$\begin{aligned}\frac{dI_x(t)}{dt} &= \beta_1(t)I(t)S_x(t)S_x(t)/N + \beta_2(t)I(t)S_y(t)S_y(t)/N \\ &= I(t)[\beta_1(t)S_x(t)S_x(t) + \beta_2(t)S_y(t)S_y(t)]/N \\ \frac{dI_y(t)}{dt} &= \beta_1(t)I(t)S_y(t)S_y(t)/N + \beta_2(t)I(t)S_x(t)S_x(t)/N \\ &= I(t)[\beta_1(t)S_y(t)S_y(t) + \beta_2(t)S_x(t)S_x(t)]/N\end{aligned}$$

단, $\frac{dI(t)}{dt} = \frac{dI_x(t)}{dt} + \frac{dI_y(t)}{dt}$

여기서, 다른 표기는 앞의 식과 동일하나 $\beta_1(t)$는 로컬 네트워크에서 확산율 함수를 나타내고, $\beta_2(t)$는 외부 네트워크에서 확산율 함수를 나타낸다.

### 2. WannaCryptor의 동작

WannaCryptor의 세부 동작은 다음과 같다. PC가 WannaCryptor에 감염이 되면, 두 가지 단계의 동작을 차례로 수행한다. 첫 번째 단계는 최초 공격자가 저장해 둔 특정 URL (hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 등 다수)에 접속을 시도한다. 만일 이 URL에 접속이 안 될 경우, 두 번째 단계에서는 네트워크를 통한 확산과 파일 암호화의 동작을 수행한다. 또한, PC가 부팅할 때마다 자동으로 실행되도록 하기 위하여 Windows 운영체제 서비스 항목에 Windows 운영체제 정상 서비스 이름과 유사한 mssecsvc 2.0 서비스를 생성하고, 악의적으로 제작한 mssecsvc.exe를 실행한다. mssecsvc.exe는 2개의 쓰레드가 동작하는데, 첫째 쓰레드는 WannaCryptor에 감염된 PC의 IP 주소를 확인하고 동일한 서브넷의 각 호스트 및 IP 주소에 SMB 프로토콜을 위한 TCP 445 포트 연결을 시도한다. 둘째 쓰레드는

인터넷에서 임의의 IP 주소를 생성하여 TCP 445 포트 연결을 시도한다. 포트 연결이 성공할 경우, MS17-010 보안 취약점을 통해 원격에서 LSASS.exe를 통해 악성코드를 실행한다. 특히, WannaCryptor는 원격에서 악성코드를 설치하고 실행하기 위해 MS17-010을 이용하는 Exploit Kit인 EtetnalBlue를 사용한다. 단, MS17-010 보안 취약점에 대한 MS 보안 패치는 2017년 3월에 제작/배포되었다.

### 3. WannaCryptor의 확산

WannaCryptor의 로컬 스캐닝 방식은 지금까지 알려진 랜덤방식이 아니라, Class 대역에 따라 상위 비트를 고정하고, 하위 비트에 대해 순차적으로 스캐닝을 진행하는 것을 확인할 수 있었다. C Class 대역에서는 상위 24비트는 고정되고 하위 8비트에 대해 1에서 254까지 순차적으로 진행된다.

| 고정 | 고정 | 고정 | ① |
|---|---|---|---|

예를 들어, 192.168.1.x 로 구성된 로컬 네트워크에서는 192.168.1.1, 192.168.1.2, 192.168.1.3, ..., 192.168.1.254의 형태로 진행되어 취약한 호스트의 수에 따른 확산 속도차이만 존재한다.

B Class 대역에서는 상위 16비트는 고정되고, 하위 16비트 중 상위 8 비트 스캐닝 완료한 후 하위 8비트로 이동한다.

| 고정 | 고정 | ① | ② |
|---|---|---|---|

예를 들어, 172.16.x.x 로 구성된 로컬 네트워크에서는 172.16.0.1, 172.16.1.1, ..., 172.16.255.1, 172.16.0.2, 172.16.1.2, ..., 172.16.255.2의 형태로 진행된다.

A Class 대역에서도 같은 방식으로 상위 8비트는 고정되고, 하위 24비트 중 상위비트 완료 후 하위비트가 증가한다.

| 고정 | ① | ② | ③ |
|---|---|---|---|

위 분석에 따르면 WannaCryptor의 로컬 네트워크 확산은 Class 대역이 좁게 구성된 환경일수록 그 효율성과 속도가 극대화되는 것을 확인할 수 있다. 또한, 로컬 네트워크의 구성형태에 따라 로컬 스캐닝의 속도차이도 존재 한다. 로컬 네트워크를 A, B, C Class로 각각 구성 하였을 경우, 최대 설치 가능한 호스트 수와 스캐닝 소요 시간은 다음과 같다.

| Class | 호스트 수 | 스캐닝 소요 시간 |
|---|---|---|
| A | 16,777,216 | 약 20일 |
| B | 65,534 | 약 1시간 49분 |
| C | 254 | 약 26초 |

## III. WannaCryptor 확산 실험

WannaCryptor 확산에 대한 세부 동작을 분석한 결과 2가지 사실을 확인할 수 있었다.

첫째 로컬 네트워크와 그 외 네트워크의 스캐닝 범위가 다르다. WannaCryptor는 로컬 스캐닝을 수행하여 로컬 네트워크와 그 외 네트워크에서 확산율이 다르다. 이는 취약한 호스트를 물색하는 스캐닝의 범위가 달라서 발생하는 현상인데[2], 실제 실험한 바에 따르면 로컬 네트워크에서 A Class 대역으로 구성된 네트워크를 스캐닝 할 경우 IP 주소의 상위 8비트를 고정하고 하위 24비트를 바꿔가면서 스캐닝하고, 이후 32비트 IP 주소를 난수로 발생시켜서 스캐닝한다. B Class 대역으로 구성된 네트워크를 스캐닝 할 경우 IP 주소의 상위 16비트를 고정하고, C Class 대역으로 구성된 네트워크를 스캐닝 할 경우 IP 주소의 상위 24비트를 각각 고정하고 하위 8비트를 바꿔가면서 스캐닝한다.

둘째 WannaCryptor는 대역폭이나 네트워크 속도에 관계없이 매초 10회의 스캐닝을 수행한다. 로컬 네트워크에 있는 취약 호스트를 찾아내기 위해 SMB 프로토콜을 사용하여 접속을 시도한다. 로컬 네트워크의 취약 호스트 스캐닝을 시도한 후 모두 완료되면 랜덤한 외부 네트워크 주소에 SMB 프로토콜 접속을 시도한다.

위 내용을 반영하여 전체 취약 호스트 수를 $N=10{,}000$으로 동일하게 두고 초당 10회 스캐닝을 수행하는 확산 실험 결과는 다음과 같다. 여기서 로컬 네트워크의 취약 호스트 수는 $N_1=1{,}000$이고 외부 네트워크의 취약 호스트 수는 $N_2=9{,}000$이다. Fig. 2는 로컬 스캐닝을 수행하지 않는 경우이고 Fig. 3은 로컬 스캐닝을 수행하는 경우이다. 일반적으로 웜과 같은 자율적인 확산하는 경우 Fig 2와 같은 슬로우 스타트 특성을 보이는데, Fig 3은 훨씬 빠른 속도로 확산하는 것을 확인할 수 있다.

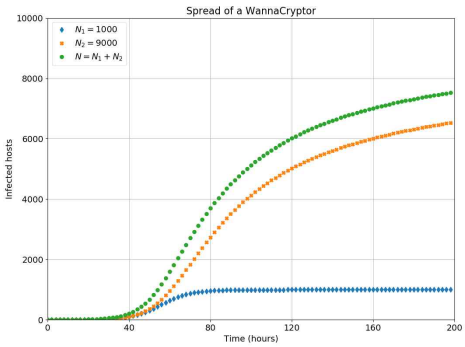


Fig. 2 The spread of WannaCryptor with random scanning 1

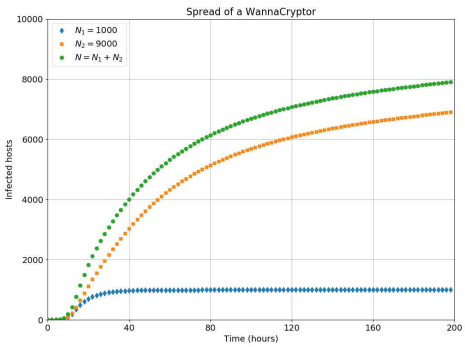


Fig. 3 The spread of WannaCryptor with localized scanning 1

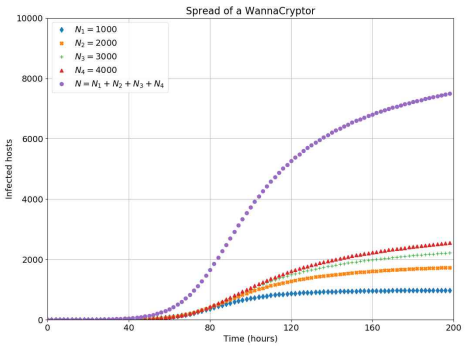


Fig. 4 The spread of WannaCryptor with random scanning 2

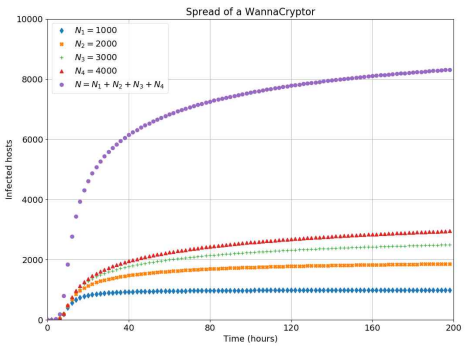


Fig. 5 The spread of WannaCryptor with localized scanning 2

전체 취약 호스트 수를 $N$=10,000으로 동일하게 두고 초당 10회 스캐닝을 수행하는 확산 실험 결과이다. 여기서 4개 네트워크로 나누고 각 네트워크의 취약 호스트 수는 $N_1$=1,000, $N_2$=2,000, $N_3$=3,000, $N_4$=4,000이다. Fig. 4는 로컬 스캐닝을 수행하지 않는 경우이고 Fig. 5는 로컬 스캐닝을 수행하는 경우이다.

앞의 실험과 마찬가지로 Fig. 4는 슬로우 스타트 특성을 보이는데, Fig. 5는 훨씬 빠른 속도로 확산하는 것을 확인할 수 있다.

## IV. 결론

악성코드 분석 및 대응 전문가는 악성코드 제작자들이 효율적인 공격을 수행하기 위해 다양한 응용기술들을 적용해 가고 있다는 점을 늘 염두에 두어야 할 것이다. 방어자의 입장에서 악성코드의 세부적인 동작에 초점을 맞추어 악의적인 의도와 행위를 분석하는 것도 중요하지만, 공격자들이 적용한 확산 방식을 참고하여 거시적 관점에서 확산 속도를 지연시킬 수 있는 방법들과 확산의 유형을 조기에 인지할 수 있는 방법들을 함께 고민하는 것이 필수적이다.

본 논문에서는 최근 심각한 문제가 되고 있는 WannaCryptor 랜섬웨어에 대한 동작 분석과 함께 확산 예측 모델링을 수행하였다. 이를 위하여 관련 연구에 대하여 살펴보고, 실제 네트워크 환경에서 발생 가능한 확산을 실험하였다. WannaCryptor가 적용한 로컬 네트워크에 대한 스캐닝 후 악성코드를 확산하는 방식은 과거 네트워크 웜의 무작위 IP 주소에 대한 확산 방식과는 달리 공격대상을 제한함으로써, 빠른 속도로 피해를 확산시킬 수 있었음을 확인할 수 있었다. 특히, 이런 확산 방식은 인터넷 환경 보다는 폐쇄망 환경에서 치명적인 피해를 줄 수 있다는 것이다.

본 논문의 결과는 날로 고도화되는 새로운

방식의 랜섬웨어 확산 대응 방안을 마련하는데 있어 기반 연구로 활용할 수 있을 것이다. 이를 기반으로 향후 다양한 방법으로 확산을 시도하는 악성코드 확산 예측 모델링에 대한 심도있는 연구와 거시적 관점의 대응에 대한 연구도 함께 진행되어야 한다.

## [참고문헌]


[1] 랜섬웨어(Ransomware) 정의, https://www.krcert.or.kr/ransomware/information.do

[2] AhnLab ASEC, "WannaCryptor Ransomware Analysis", 2017.

[3] KISA KrCERT, "WannaCry Analysis Specail Report", 2017.

[4] Cliff C. Zou, Don Towsley, Weibo Gong, "On the Performance of Internet Worm Scanning Strategies", Elsevier Journal of Performance Evaluation, vol. 63, no. 7, pp. 700-723, 2006.

[5] Weon Shin, "Mobile Worm Propagation in Analysis on Heterogeneous Mobile Networks", Telecommunications Review, vol. 23, no. 2, pp. 224-234, 2013.

[6] Panda Security, “WannaCry Report”, 2017.

[7] VIPRE Labs, "Wannacry Technical Analysis", 2017.

[8] Hitachi, "Network infection by WannaCry", 2018.