Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.3, Jun. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.3.389

WannaCryptor 워머블 악성코드 확산 방식 연구*

박 태 환,[1†] 이 호 웅,[2] 신 원[3‡]
[1]㈜안랩 (연구원), [2]호서대학교 (교수), [3]동명대학교 (교수)

Propagation Modeling of WannaCryptor Wormable Malware*

Tae Hwan Park,[1†] Howoong Lee,[2] Weon Shin[3‡]
[1]AhnLab, Inc. (Researcher), [2]Hoseo University (Professor),
[3]Tongmyong University (Professor)

요 약

독특하게도 WannaCryptor는 사용자 데이터를 암호화하고 이를 복구하려면 돈을 요구하는 랜섬웨어임에도 불구하고 Windows 운영체제의 공유 폴더 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.

ABSTRACT

WannaCryptor is a type of ransomware which encrypts users' personal data or files and demands ransom payment in order to regain access. But it peculiarly spreads by itself like a Internet worm using Windows vulnerabilities of shared folder. In this paper, we analyzed and estimated the spread of WannaCryptor focusing on the wormable spread features different from the existed ransomware. Thus we observed its behaviors in virtual environments, and experimented the various spreads of WannaCryptor based on our prediction modeling.

Keywords: WannaCryptor, Ransomware, Prediction model, Wormable malware

I. 서 론

일반적으로 신뢰할 수 없는 사이트, 스팸메일, 파일공유 사이트, 네트워크를 통해 유포되는 랜섬웨어는 몸값(ransom)과 소프트웨어(software)의 합성어로 시스템을 잠그거나 데이터를 암호화하여 사용자가 사용할 수 없도록 한 후 이를 인질로 금전을 요구하는 악성 프로그램을 말한다[1]. 그 중 세계적인 피해를 유발하여 WannaCry 또는 WannaCrypt 등 여러 이름으로 불리는 WannaCryptor 랜섬웨어는 문서 파일을 암호화하여 이를 인질로 금전을 요구하는 방식은 다른 랜섬웨어와 유사하다. 그러나 클릭 또는 실행과 같은 사용자의 동작에 의해 확산하는 일반적인 랜섬웨어와는 달리, WannaCryptor는 Windows 운영체제의 SMB (Sever Message Block) 취약점을 악용하고 악성코드를 감염시킨 후 IP 주소를 스캐닝하여 네트워크를 통하여 다른 취약한 시스템으로 확산하는 형태를 가진다[2][3]. 이러한 WannaCryptor 랜섬웨어의 확산 방식은 자기 자신을 복제하여 인터넷으로 확산하는 인터넷 웜 확산과 같은 방식인데, 기존 랜섬웨어의 동작과 확산의 한계를 뛰어넘는 새로운 방식이라 할 수 있다. 또한, 확산 과정 중 발생하는 패킷은 네트워크에 오버헤드

Received(02. 13. 2020), Modified(1st: 03. 27. 2020, 2nd: 04. 09. 2020), Accepted(04. 14. 2020)
* 이 논문은 2019학년도 동명대학교 연구년지원에 의하여 연구되었음
† 주저자, taehwan.park@ahnlab.com
‡ 교신저자, shinweon@tu.ac.kr (Corresponding author)

를 초래할 뿐 아니라 WannaCryptor 희생자가 새로운 공격자가 되어 특정 네트워크 환경을 대상으로 하는 분산 서비스 거부 공격과 유사한 효과를 유발할 수도 있다.

본 논문에서는 기존 연구가 악성코드의 세부 동작을 중심으로 진행되고 있는 것에 탈피하여 거시적 관점의 네트워크 환경에 따른 WannaCryptor 확산 예측을 수행하고자 한다. 먼저 2장에서는 기존 악성코드 확산 모델링과 이를 응용한 WannaCryptor 모델링에 대하여 살펴보고, 3장에서 동작을 분석한다. 4장에서 네트워크 환경의 WannaCryptor 확산 예측 모델링을 통하여 실제 환경을 고려한 시뮬레이션을 수행한 후 마지막 5장에서 결론을 맺는다.

Ⅱ. 악성코드 확산 모델링

2.1 기존 연구

Zou 등[4]은 인터넷 웜의 스캐닝 방식에 따라 웜 확산의 성능을 분석하였는데, 인터넷 IP 주소 공간에 대해 무작위 스캐닝을 수행하는 RCS(Random Constant Spread) Worm의 동작에서부터 다음 식을 유도하여 인터넷 환경의 웜 확산을 설명하였다. 여기서, β는 웜 확산율, η는 웜의 단위 시간당 평균 스캐닝 수, Ω는 웜이 스캐닝할 수 있는 전체 호스트의 주소 공간(IP 주소), N은 감염 가능한 전체 취약 호스트 수, $I(t)$는 시각 t에 감염된 호스트 수를 나타낸다.

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

Two-factor Worm Model[5]에서는 확산의 오버헤드를 고려하여 고정된 확산율 β 대신 시간에 따라 변화하는 함수 $\beta(t)$로 나타내었다. 여기서, β_0는 초기 확산율이고 ϕ는 감염 호스트 비율에 따라 확산율 감소분을 반영한 값이다. 만약 $\phi=0$라면 확산율은 $\beta=\beta_0$로 고정되고 RCS Worm에 해당한다.

$$\beta(t)=\beta_0(1-\frac{I(t)}{N})^{\phi}$$

한편, 균일한 속도로 전송되는 단일 네트워크가 아니라 Fig. 1과 같이 서로 다른 속도의 Network

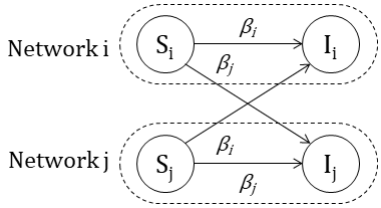


Fig. 1. Malware propagation on heterogeneous networks

i, j가 연결되어 있고 인터넷 웜이 각각의 네트워크에서 각각의 속도로 확산한다면 t시점의 감염 호스트 수는 다음과 같다[6]. 여기서, $I_x(t)$는 네트워크 x에서 t시점의 감염된 호스트 수를 나타내고, $S_x(t)$는 네트워크 x에서 t시점의 취약 호스트 수로 $N-I_x(t)$와 같다.

$$\frac{dI_i(t)}{dt}=\beta_i(t)I(t)\frac{S_i(t)S_i(t)}{N}+\beta_i(t)I(t)\frac{S_j(t)S_j(t)}{N}$$
$$=\beta_i(t)I(t)\frac{[S_i(t)S_i(t)+S_j(t)S_j(t)]}{N}$$
$$\frac{dI_j(t)}{dt}=\beta_j(t)I(t)\frac{S_j(t)S_j(t)}{N}+\beta_j(t)I(t)\frac{S_i(t)S_i(t)}{N}$$
$$=\beta_j(t)I(t)\frac{[S_i(t)S_i(t)+S_j(t)S_j(t)]}{N}$$

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

2.2 WannaCryptor의 확산 모델링

2019년 5월 공개된 CVE-2019-0708은 보안이 취약한 컴퓨터에 원격 접속한 후 공격자가 임의의 코드를 실행할 수 있는 취약점이다. Microsoft사는 이 사실을 공개하면서 "the vulnerability is wormable"이라고 표현하였다[7]. 이러한 워머블 취약점을 악용하는 악성코드에는 WannaCryptor, Petya 랜섬웨어가 있다. 여기서 워머블 악성코드는 특정 보안 취약점을 이용하는 악성코드가 인터넷 웜과 같은 방식으로 확산하는 악성코드를 말한다. 즉 악성코드 자신의 고유한 동작은 그대로 수행하지만, 확산 방식은 인터넷 웜과 같은 방식을 사용하는 것이다. 워머블 악성코드의 확산은 인터넷 웜처럼 자기 자신을 복제하여 인터넷을 통해 매우 빠른 속도로 확산할 수 있고, 막대한 피해를 끼칠 수 있다. 이는 사용자의 동작에 의해 한계를 가지는 트로이목마, 랜섬웨어, 루트킷과 같은 악성코드가 기존 방식의 한계를

뛰어넘는 매우 효과적인 확산 방식이 될 수 있다.

WannaCryptor는 Fig. 2와 같이 Network x, y에서 감염된 호스트 I는 로컬 네트워크에서는 β_1의 확산율로, 다른 네트워크에서는 β_2의 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. 여기서 로컬 네트워크는 IP 주소 대역을 공유하는 네트워크인데 일반적으로 같은 라우터를 공유한다. 예를 들어 C 클래스 IP 주소를 가진 경우에는 a.b.c.0에서 a.b.c.255까지를 로컬 네트워크로, B 클래스 IP 주소를 가진 경우에는 a.b.0.0에서 a.b.255.255를 로컬 네트워크로 가정한다.

이종망 환경에서 서로 다른 속도로 확산하는 인터넷 웜 확산 특성[6]에 착안하여, WannaCryptor가 Network x, y에 확산한다고 가정하면 t시점의 감염 호스트 수는 다음 식을 통하여 구할 수 있다. 여기서, 다른 표기는 앞의 식과 동일하나 $\beta_1(t)$는 로컬 네트워크에서 확산율 함수를 나타내고, $\beta_2(t)$는 외부 네트워크에서 확산율 함수를 나타낸다.

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

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

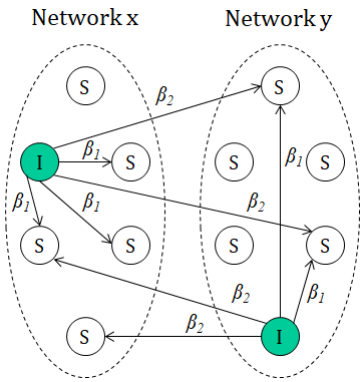


Fig. 2. Localized scanning of WannaCryptor

Ⅲ. WannaCryptor의 동작 분석

3.1 WannaCryptor의 동작

PC가 WannaCryptor에 감염되면 두 가지 동작을 차례로 수행한다. 첫 번째 단계는 공격자가 설정해 둔 특정 URL(http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 등 다수)에 접속을 시도한다. 만일 이 URL에 접속이 안 될 경우, 두 번째 단계에서 네트워크를 통한 확산과 파일 암호화 동작을 수행한다. 또한, PC가 부팅할 때마다 자동 실행될 수 있도록 Windows 운영체제 서비스 항목에 Windows 운영체제 정상 서비스 이름과 유사한 mssecsvc 2.0 서비스를 생성하고, 악의적으로 제작한 mssecsvc.exe를 실행한다.

여기서 mssecsvc.exe는 2개의 스레드가 동작하는데, 첫째 스레드는 WannaCryptor에 감염된 PC의 IP 주소를 확인하고 동일한 서브넷의 각 호스트 및 IP 주소에 SMB 프로토콜을 위한 TCP 445 포트 연결을 시도한다. 둘째 스레드는 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 EternalBlue를 사용한다. 참고로 MS17-010 보안 취약점에 대한 MS 보안 패치는 2017년 3월에 제작/배포되었다. WannaCryptor의 세부 동작은 Fig. 3과 같다[2].

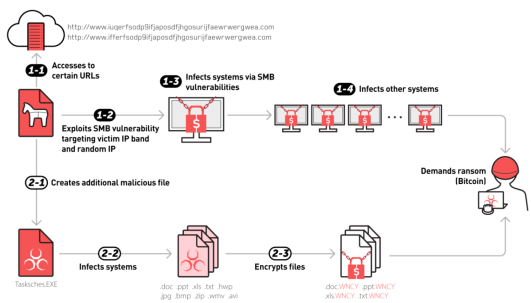


Fig. 3. Operating process of WannaCryptor

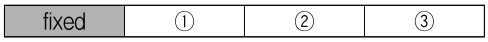
3.2 WannaCryptor의 확산 방식

WannaCryptor의 로컬 스캐닝 방식은 지금까지

알려진 랜덤 방식이 아니라, 클래스 대역에 따라 상위 비트를 고정하고, 하위 비트에 대해 순차적으로 스캐닝을 진행하는 것을 확인할 수 있었다. C 클래스 IP 주소에서는 상위 24비트는 고정되고 하위 8비트에 대해 1에서 254까지 순차적으로 진행된다. 예를 들어, IP 주소가 192.168.1.x 로 구성된 로컬 네트워크에서는 ① 부분이 순차적으로 증가하면서 192.168.1.1, 192.168.1.2, 192.168.1.3, …, 192.168.1.254의 형태로 진행되어 취약한 호스트의 수에 따른 확산 속도 차이만 존재한다.

B 클래스 IP 주소에서는 상위 16비트는 고정되고, 하위 16비트 중 상위 8 비트 스캐닝 완료한 후 하위 8비트로 이동한다. 예를 들어, IP 주소가 172.16.x.x 로 구성된 로컬 네트워크에서는 하위 16비트 중 ①, ② 순서로 상위바이트 완료 후 하위 바이트가 증가하는 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 클래스 IP 주소에서도 같은 방식으로 상위 8비트는 고정되고, 하위 24비트 중 ①, ②, ③ 순서로 상위바이트 완료 후 하위바이트가 증가한다.



위 분석에 따르면 WannaCryptor의 로컬 네트워크 확산은 클래스 대역이 좁게 구성될수록 효율성과 속도가 극대화되는 것을 확인할 수 있다. 즉, 로컬 네트워크의 구성형태에 따라 로컬 스캐닝의 속도 차이가 존재한다. 로컬 네트워크를 A, B, C 클래스로 각각 구성하였을 경우, 최대 설치 가능한 호스트 수와 추정 스캐닝 소요 시간은 Table 1과 같다.

Table 1. Estimated scanning time

Class	Hosts	Scanning time
A	16,777,214	about 19.4 days
B	65,534	about 1 hour 49 minutes
C	254	about 25 seconds

Ⅳ. 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 클래스 IP 주소로 구성된 네트워크를 스캐닝할 경우 IP 주소의 상위 8비트를 고정하고 하위 24비트를 바꿔가면서 스캐닝하고, 이후 32비트 IP 주소를 난수로 발생시켜서 스캐닝한다. B 클래스 IP 주소로 구성된 네트워크를 스캐닝할 경우 IP 주소의 상위 16비트를 고정하고, C 클래스 IP 주소로 구성된 네트워크를 스캐닝할 경우 IP 주소의 상위 24비트를 각각 고정하고 하위 8비트를 바꿔가면서 스캐닝한다. 둘째 WannaCryptor는 대역폭이나 네트워크 속도와 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.

WannaCryptor 악성코드 확산 실험을 수행하기 위하여 다음과 같은 가정이 필요하다.

〈가정〉

① 각 호스트는 WannaCryptor에 중복으로 감염되지 않는다.
② WannaCryptor는 스캐닝 속도가 고정되어 있으나, 취약 호스트가 속한 네트워크의 구성에 따라 확산 속도가 다르다.
③ 각 호스트의 성능, 스위치 및 라우터에서 일어나는 지연, 네트워크 장비에서 발생하는 패킷 오버헤드 등은 거시적 관점의 WannaCryptor 확산에서는 무시한다.

실험 1. 특정 네트워크 N_1의 취약한 호스트 1,000대와 그 외 취약한 호스트 9,000대 환경에서 확산 실험

위 내용을 반영하여 전체 취약 호스트 수를 $N=10{,}000$으로 동일하게 두고 초당 10회 스캐닝을 수행하는 확산 실험 결과는 다음과 같다. 여기서 로

컬 네트워크의 취약 호스트 수는 $N_1 = 1{,}000$이고 외부 네트워크의 취약 호스트 수는 $N_2 = 9{,}000$으로 둔다. Fig. 4는 로컬 스캐닝을 수행하지 않는 경우이고 Fig. 5와 Fig. 6은 로컬 스캐닝을 수행하는 경우이다.

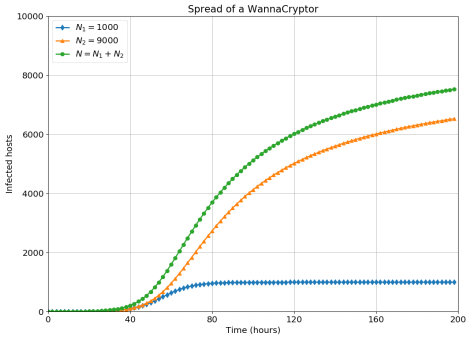


Fig. 4. The spread of WannaCryptor with random scanning

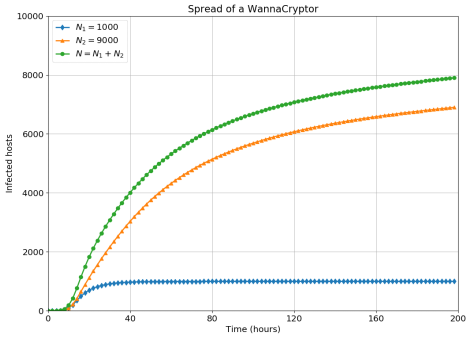


Fig. 5. The spread of WannaCryptor with localized scanning in B class network

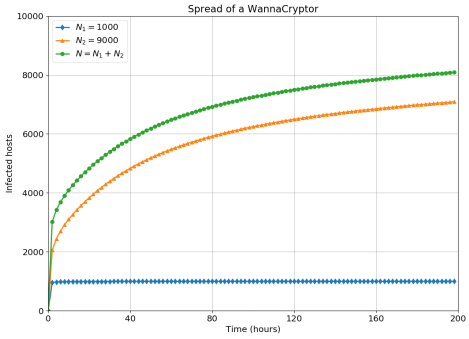


Fig. 6. The spread of WannaCryptor with localized scanning in C class network

Fig. 4는 인터넷을 대상으로 랜덤 스캐닝을 수행한 경우이다. WannaCryptor는 워머블 악성코드이므로 슬로우 스타트 특성을 보이는데, 확산 후 40시간 지점까지 아주 미세하게 확산을 진행하다 그 후 확산이 대규모로 증가하는 것을 확인할 수 있다. Fig. 5는 동일한 조건에서 $N_2 = 9{,}000$이 B 클래스 네트워크라 가정하고 로컬 스캐닝을 수행하는 경우이다. 일반적으로 워머블 악성코드와 같이 자율적으로 확산하는 악성코드의 확산은 Fig. 4와 같은 슬로우 스타트 특성을 보이는데, Fig. 5는 확산 후 슬로우 스타트 특성을 보이다가 15시간 이후 빠른 속도로 확산하는 것을 확인할 수 있다. Fig. 6은 역시 동일한 조건에서 $N_2 = 9{,}000$이 C 클래스 네트워크라 가정하고 로컬 스캐닝을 수행하는 경우이다. 일반적으로 워머블 악성코드와 같이 자율적으로 확산하는 악성코드의 확산은 Fig. 4와 같은 슬로우 스타트 특성을 보이는데, Fig. 6은 슬로우 스타트 특성 없이 기하급수적으로 확산하는 것을 확인할 수 있다.

실험 2. 특정 네트워크 N_1, N_2, N_3의 취약한 호스트 각각 1,000대, 2,000대, 3,000대와 그 외 취약한 호스트 4,000대 환경에서 확산 실험

전체 취약 호스트 수를 $N = 10{,}000$으로 동일하게 두고 초당 10회 스캐닝을 수행하는 확산 실험 결과이다. 여기서는 편의상 네트워크를 4개 네트워크로 나누고 각 네트워크의 취약 호스트 수는 $N_1 = 1{,}000$, $N_2 = 2{,}000$, $N_3 = 3{,}000$, $N_4 = 4{,}000$으로 둔다. Fig. 7은 로컬 스캐닝을 수행하지 않는 경우이고 Fig. 8과 Fig. 9는 로컬 스캐닝을 수행하는 경우이다.

Fig. 7은 인터넷을 대상으로 랜덤 스캐닝을 수행한 경우이다. 네트워크가 규모별로 나누어져 있으므로 확산 후 50시간 지점까지 슬로우 스타트 특성을 보이다가 그 후 확산이 대규모로 증가하는 것을 확인할 수 있다. Fig. 8은 동일한 조건에서 $N_1 = 1{,}000$, $N_2 = 2{,}000$, $N_3 = 3{,}000$이 B 클래스 네트워크라 가정하고 로컬 스캐닝을 수행하는 경우이다. 일반적으로 워머블 악성코드와 같이 자율적으로 확산하는 악성코드의 확산은 Fig. 7과 같은 슬로우 스타트 특성을 보이는데, Fig. 8은 확산 후 슬로우 스타트 특성을 보이다가 10시간 이후 빠른 속도로 확산하는 것을 확인할 수 있다. Fig. 9는 동일한 조건에서 $N_1 = 1{,}000$, $N_2 = 2{,}000$, $N_3 = 3{,}000$이 C 클래스 네트워크라 가정하고 로컬 스캐닝을 수행하는 경우이다.

일반적으로 워머블 악성코드와 같이 자율적으로 확산하는 악성코드의 확산은 Fig. 7과 같은 슬로우 스타트 특성을 보이는데, Fig. 9는 슬로우 스타트 특성 없이 기하급수적으로 확산하는 것을 확인할 수 있다.

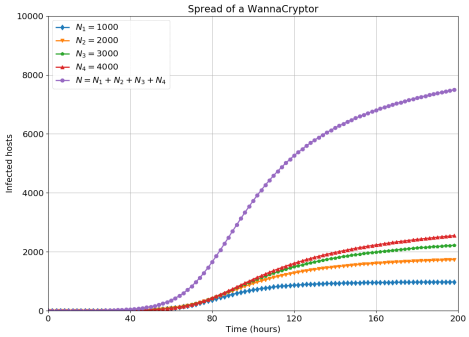


Fig. 7. The spread of WannaCryptor with random scanning 2

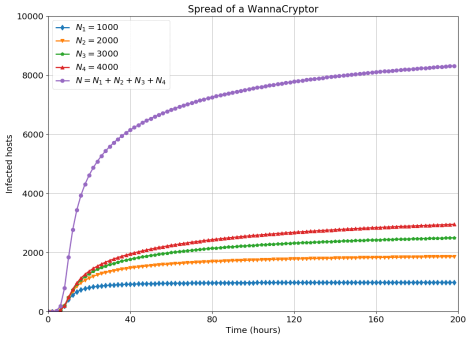


Fig. 8. The spread of WannaCryptor with localized scanning in B class network

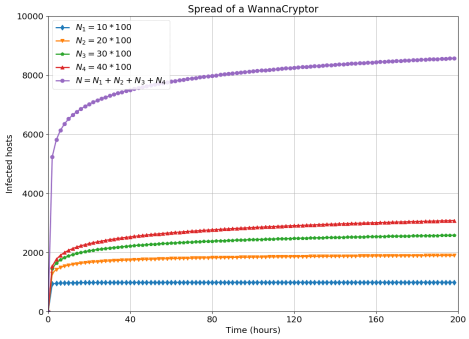


Fig. 9. The spread of WannaCryptor with localized scanning in C class network

위 실험을 통하여 얻는 결론은 다음과 같다. 첫째, 인터넷 속도가 빠르면 확산 속도도 빨라진다. 그러나 WannaCrypto는 스캐닝 속도가 고정되어 있어 인터넷 속도가 빠르다고 확산 속도가 빨라지는 것이 아니다. 둘째, 취약 호스트가 많으면 많을수록 확산 속도는 더 빨라진다. 취약 호스트끼리 시너지 효과가 있어 훨씬 빠른 속도로 확산이 진행된다. 셋째, 로컬 스캐닝을 수행하면 슬로우 스타트 특성이 거의 없어지므로 악성코드 확산은 훨씬 빠르게 진행된다. 이에 대응하기 위해서는 악성코드 확산에 대한 대응도 훨씬 빠르게 진행하여야 한다. 넷째, 로컬 스캐닝을 수행하여 취약 호스트가 없으면 다시 랜덤 스캐닝을 수행한다. 따라서 같은 네트워크에 취약한 다른 호스트가 별도로 존재하지 않는다면 다른 네트워크를 스캐닝하므로 확산 속도는 다시 떨어지는 효과가 발생한다. 반대로 이야기하면 주위에 다른 취약한 호스트들이 존재하면 첫 번째와 같이 슬로우 스타트 특성이 없어져서 확산이 더욱 빠르게 진행된다.

Ⅴ. 결 론

본 논문에서는 최근 심각한 문제가 되는 랜섬웨어 중 WannaCryptor에 대한 동작 분석과 함께 확산 예측 모델링을 수행하였다. 이를 위하여 관련 연구를 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 환경보다는 폐쇄망 환경에서 치명적인 피해를 줄 수 있다는 것이다.

특히 워머블 악성코드로서 WannaCryptor는 한계를 가질 수밖에 없는 기존 랜섬웨어의 확산 방식에 새로운 방향성을 제시함으로써 향후 등장할 워머블 악성코드로 인하여 막대한 피해가 예상되고 있다. 따라서, 악성코드 분석 및 대응 전문가는 악성코드 제작자들이 효율적인 공격을 수행하기 위해 다양한 응용기술들을 적용해 가고 있다는 점을 늘 염두에 두어야 할 것이다. 방어자의 관점에서 악성코드의 세부적인 동작에 초점을 맞추어 악의적인 의도와 행위를 분석하는 것도 중요하지만, 공격자들이 적용한 확산 방식을 참고하여 거시적 관점에서 확산 속도를 지연시킬 방법들과 확산의 유형을 조기에 인지하는 방법들

을 함께 고민하는 것이 필수적이다.

본 논문의 연구 결과는 날로 고도화되는 새로운 방식의 랜섬웨어 확산 대응 방안을 마련하는 데 있어 기반 연구로 활용할 수 있을 것이다. 이를 기반으로 향후 다양한 방법으로 확산을 시도하는 악성코드 확산 예측 모델링에 대한 깊이 있는 연구와 거시적 관점의 대응에 관한 연구도 함께 진행되어야 한다.

References

[1] Definition of Ransomware, https://www.krcert.or.kr/ransomware/information.do

[2] AhnLab, "WannaCryptor Ransomware Analysis," ASEC Tech Report, https://www.ahnlab.com/

[3] KISA, "WannaCry Analysis Special Report," KrCERT Report, https://www.krcert.or.kr/

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

[5] Cliff C. Zou, Weibo Gong, and Don Towsley, "Code Red Worm Propagation Modeling and Analysis," in Proceedings of the 9th ACM conference on Computer and communications security, pp.138-147, Nov. 2002.

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

[7] Prevent a worm by updating Remote Desktop Services (CVE-2019-0708), https://msrc-blog.microsoft.com/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

[8] VIPRE Labs, "Wannacry Technical Analysis," https://labs.vipre.com/wannacry- technical-analysis/

〈저자소개〉

박 태 환 (Tae Hwan Park) 정회원
2016년 8월: 한양사이버대학교 컴퓨터공학과 졸업
2020년 2월: 전남대학교 정보보안 협동과정 석사
2002년 10월~현재: ㈜안랩 시큐리티대응센터(ASEC) 대응팀장
〈관심분야〉 악성코드, 사이버시큐리티 동향

이 호 웅 (Howoong Lee) 정회원
1998년: 호서대학교 컴퓨터공학과 졸업
2000년: 인하대학교 전자계산공학과 석사
2000년: ㈜안랩 입사
2011년~2014년: ㈜안랩 시큐리티대응센터(ASEC) 센터장
2015년~2017년: ㈜안랩 연구소장
2018년~2020년 2월: ㈜안랩 CTO(최고기술책임자)
2020년 3월~현재: 호서대학교 컴퓨터정보공학부 조교수
〈관심분야〉 디지털 융합보안, 인공지능, 블록체인

신 원 (Weon Shin) 종신회원
1996년 2월: 부경대학교 전자계산학과 졸업
1998년 2월: 부경대학교 전자계산학과 석사
2001년 8월: 부경대학교 전자계산학과 박사
2002년 3월~2005년 1월: ㈜안랩 선임연구원
2005년 3월~현재: 동명대학교 정보보호학과 교수
〈관심분야〉 소프트웨어 보안, 악성코드 확산 대응, 디지털포렌식