ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 6, pp. 231-236, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.6.231

사물인터넷 환경에서의 VPN-Filter malware 기술과 대응방법

김승호[1], 이근호[2*]
[1]백석대학교 정보통신학부 학생, [2]백석대학교 정보통신학부 교수

VPN-Filter Malware Techniques and Countermeasures in IoT Environment

Seung-Ho Kim[1], Keun-Ho Lee[2*]
[1]Student, Division of Information Communication, Baek-seok University
[2]Professor, Division of Information Communication, Baek-seok University

요 약 최근 정보통신기술의 빠른 발전에 따라 새로운 유형의 취약점 및 공격 기법들이 수없이 생겨나고 사회적인 물의를 일으키고 있다. 본 논문에서는 2018년 5월경 Cisco 위협 정보팀인 Talos Intelligence가 새롭게 발견한 대규모 사물인터넷 기반 botnet을 구성하는 'VPN-Filter'의 공개된 표본을 분석하여, 현시대의 사물인터넷 기반 botnet의 구성 방식과 공격방식에 대하여 살펴보고 해당 자료를 바탕으로 VPN-Filter와 접목해 VPN-Filter의 공격 시나리오와 공격 취약점의 특징에 대해 이해하고 VPN-Filter 악성코드를 이용한 Botnet 구성의 핵심이 되는 C&C Server 연결방식의 원인을 제거하기 위해 EXIF 메타데이터 제거 방식을 통한 해결방안을 제안하여 미래에 다가올 4차 산업혁명 시대의 사이버 보안에 기여하길 기대한다.

주제어 : 융합, VPN-Filter, 봇넷, 악성코드, 보안, IoT 장비

Abstract Recently, a wide variety of IoT environment is being created due to the rapid development of information and communication technology. And accordingly in a variety of network structures, a countless number of attack techniques and new types of vulnerabilities are producing a social disturbance. In May of 2018, Talos Intelligence, the Cisco threat intelligence team has newly discovered 'VPN-Filter', which constitutes a large-scale IoT-based botnet, is infecting consumer routers in over 54 countries around the world. In this paper, types of IoT-based botnets and the attack techniques utilizing botnet will be examined and the countermeasure technique through EXIF metadata removal method which is the cause of connection method of C & C Server will be proposed by examining the characteristics of attack vulnerabilities and attack scenarios of VPN-Filter.

Key Words : Convergence, VPN-Filter, botnet, malware, security, IoT device

1. 서론

2018년 5월경 시스코(Cisco) 위협 정보팀인 탈로스 인텔리전스(Talos Intelligence)에 의해 발견된 러시아 정부의 후원을 받는 것으로 의심되는 정교한 모듈식 악성코드 프로그램인 'VPN-Filter'는 최근 특정 IoT 기기를 대상으로 악성코드를 감염시켜 전 세계적으로 약 500,000 ~ 1,000,000대가량의 IoT 장치를 감염시킨 것으로 추정되고 있다[1].

* This research was supported by Basic Science Research Program through the National research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A3B03935976) and was supported by Korea Sanhak Foundation
*Corresponding Author : Keun-Ho Lee(root1004@bu.ac.kr)
Received October 22, 2018 Revised November 20, 2018
Accepted December 20, 2018 Published December 28, 2018

이번 발견된 악성코드인 'VPN-Filter'는 과거 2014년 우크라이나와 폴란드를 표적으로 공격하여 이름을 떨친 악성코드인 블랙에너지(Black Energy) 악성코드[2]와 정확히 일치하는 복사본도 포함되어 있다고 한다[1]. 그러므로 이번 'VPN-Filter'를 통해서 2015년 블랙에너지의 정전 사태와 같은 막대한 피해가 일어날 수 있다는 가능성이 없다고 말할 수 없는 것이다.

또한 해당 악성코드는 서비스 제공 업체와 일반 사용자를 구분하지 않고 공격을 통해 제어할 수 있는 특징이 있어[3] 다른 악성코드에 비해 더 위협적이다.

본 논문에서는 4차 산업 시대의 IoT 보안을 위하여 필요한 정보보안의 요소와 다양한 사이버 공격 중 하나인 Botnet이 무엇이며 어떤 피해를 볼 수 있는지 알아보고 VPN-Filter에 대한 공격 원인과 EXIF 메타데이터 제거 방식을 통한 대응 방법을 제안한다.

2. 관련 연구

2.1 botnet

botnet은 보안이 취약한 컴퓨터를 스스로 찾은 후 시스템이 침입하여 보이지 않는 곳에서 은밀하게 작동하여 사용자도 모르게 컴퓨터 시스템에 명령 및 제어를 할 수 있는 원거리 해킹 프로그램을 의미하는 'bot'과 'network'의 합성어로 'bot'에 의해 감염되어 'network'에 연결된 장치들의 집단을 의미한다[4].

botnet은 통신 방법에 따라 구성 요소와 구조에 약간의 차이가 있다. botnet의 통신 방법은 크게 2가지로 직접 명령과 제어를 받는 botnet과 P2P 기반의 botnet으로 나눌 수 있다[5].

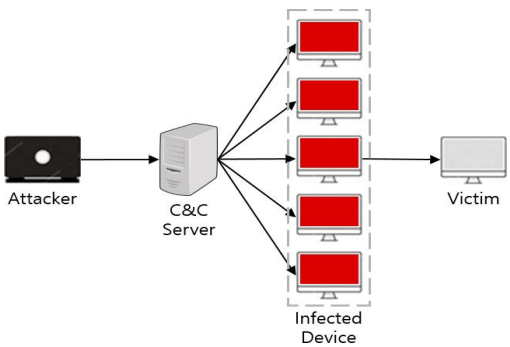

Fig. 1. General structure of direct command and control botnets

Fig 1과 같이 직접 명령과 제어를 받는 botnet은 C&C (Command & Control) Server를 이용한 방식으로 감염된 좀비 디바이스들이 C&C Server에 직접 연결 혹은 분산 연결되어 감염 디바이스의 상태를 꾸준히 전송한다.

두 번째 방식은 Fig 2와 같이 P2P 기반 botnet으로 분산식 감염 디바이스를 이용하여 봇넷을 보호하고 원활한 통신이 유지되게 하는 방식의 botnet이다.

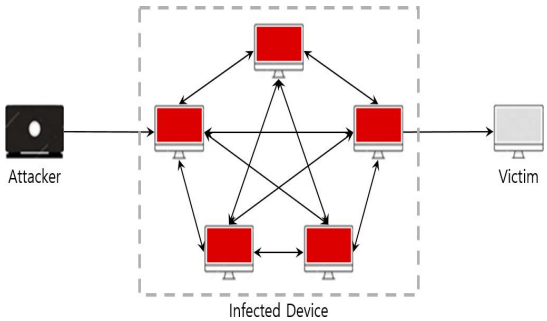

Fig. 2. General structure of P2P-based botnets

2.2 botnet을 이용한 공격 기법

2.2.1 DDoS 공격

분산 서비스 거부 공격(distributed Denial of Service attack)이라 불리는 해당 기법은 DoS 공격의 주목적인 시스템 또는 서버를 공격해 해당 장비의 자원을 소비하게끔 하여 정상적인 역할을 수행할 수 없는 상태로 만드는 기법으로 Fig3을 보면 알 수 있듯이 여러 대의 감염 디바이스로 동시에 공격함으로써 더욱 효과적인 공격을 시도하는 기법[6]으로 DDoS 공격은 공격 타겟의 계층에 따라 3~4계층은 대역폭 소진 공격, 7계층은 서비스/애플리케이션 마비 공격으로 크게 두 가지로 분류된다[7].

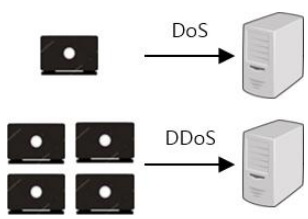

Fig. 3. Differences between DoS and DDoS

DDoS 공격은 작게는 하나의 서버 크게는 인터넷 전체를 마비시킬 수 있다. 그 예로 2002년 DNS backbone DDoS 공격으로 인해 13개의 DNS root server 중 9개에

서 서비스 중단이 보고되었다. 그리고 이 공격은 2007년에 재발하여 두 개의 DNS root server가 중단된 적이 있었다[8].

2.2.2 암호화폐 채굴

암호화폐란 P2P 네트워크 환경에서 상호 인증되어 안전이 보장된 거래를 위해 암호화 기술을 사용하는 전자화폐를 뜻한다[9]. 대표적으로 비트코인(Bitcoin)[10]과 이더리움(Ethereum)[11], 리플(Ripple)[12]등이 가상화폐의 일종이다.

암호화폐 채굴을 이해하기 위해서는 블록체인 기법을 이해해야 한다. 블록체인 기법은 Fig 4와 같은 방식으로 실행되는데 '공공거래장부' 형태로 해당 네트워크에 참여한 사용자를 노드라 하는데 노드 모두가 기록 및 관리를 통하여 위변조를 방지하는 기법이다. 이렇게 온라인상에서 거래 데이터가 기록되는 장부를 '블록'이라 하고 이러한 '블록'들이 모여 시간이 지남에 따라 순차적으로 연결되어 '체인' 구조가 되어 블록체인이라 불리는 것이다[13].

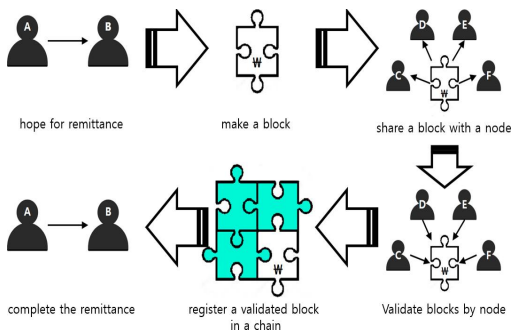

Fig. 4. Blockchain technique schematization

이때 채굴이 의미하는 바는 블록을 생성하고 체인에 등록하는 행위 즉, 블록체인을 유지하는 대가로 암호화폐를 지급받는 행위인 것이다.

공격자는 이러한 블록체인의 특성을 이용하여 botnet을 통하여 각각의 감염 디바이스를 노드화 시켜서 계속해서 블록을 생성 및 체인에 등록을 시키고 그 보상으로 암호 화폐를 공격자 본인이 받아간다. 또한, 암호 화폐의 특성상 노드가 많을수록 더 높은 보안성과 더 높은 희소성을 통해 암호 화폐의 가치를 높인다.

최근에는 랜섬웨어가 아닌 2018년 3월경 'Dofoil'이라는 이름의 트로이목마 악성코드 변종이 발견돼 약 48만대의 감염 디바이스를 만들어 악성코드 채굴을 시도한 사례도 있다[14].

2.2.3 악성코드 유포

악성코드 유포는 botnet을 구성하고 효과적으로 활용하기 위해서는 필요한 과정이라 볼 수 있다.

악성코드는 멀웨어(malware)라고 불리기도 하면 컴퓨터 바이러스(virus), 웜(worm), 스파이웨어(spyware), 백도어(backdoor) 등 컴퓨터 사용자에게 피해를 주기 위한 모든 종류의 악성 프로그램을 뜻한다[15]. 위에서 설명한 DDoS나 암호화폐 채굴을 위한 프로그램 모두 악성코드라 할 수 있다.

시간이 흐르고 컴퓨터의 성장이 더해질수록 다양한 종류의 악성코드가 생겨나고 있는데 그 예시로 위에서 설명한 암호화폐 채굴이나 컴퓨터의 모든 파일을 암호화하여 풀어주는 대가로 암호화폐를 요구하는 프로그램인 랜섬웨어(Ransom Ware) 또한 최근에 생겨난 악성코드라 할 수 있다[16].

3. VPN-Filter 공격

3.1 공격 시나리오

해당 악성코드는 2016년부터 전 세계에 은밀하게 널리 유포되고 있었으며 현재에도 지속해서 감염 영역을 넓혀가고 있다. 특히, 대다수 피해자가 우크라이나 지역으로 밝혀졌고 피해자의 IP에서 데이터 유출이 의심되는 증거가 포착되었다.

또한, 해당 악성코드에 감염된 대다수 디바이스는 보안에 취약한 디바이스로 IPS의 범위를 벗어난 네트워크의 경계에 위치한 경우가 많고 Antivirus 패키지와 같은 보호 시스템을 지원하지 않는 디바이스들이 대부분이었다.

'VPN-Filter'의 공격 방식은 3단계로 구성되어 Fig5와 같은 흐름으로 실행된다. 1단계 공격의 주요 목적은 지속적인 공격로의 교두보를 마련하고 2단계 악성코드의 유포를 지원하는 것이다. 위에서 말한 보통의 악성코드는 재부팅으로 소멸하지만 'VPN-Filter'는 살아있는 이유이다. 자세히 살펴보자면, 1단계의 명령 및 제어 메커니즘을 통해 2단계 공격의 배포 서버(C&C Server)를 찾는데 만약 예외 상황이 발생하더라도 2단계 공격이 정해진 동작할 수 있도록 처리한다.

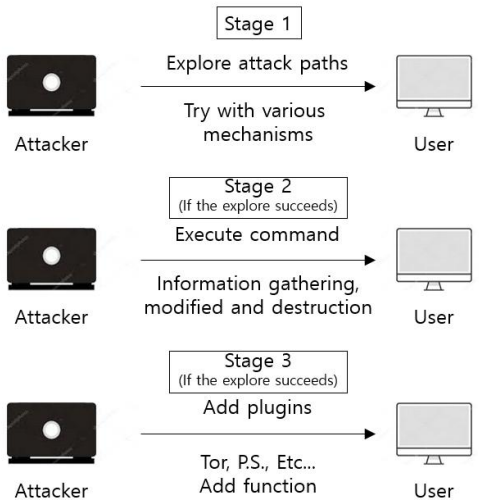

Fig. 5. schematization by attack stage

조금 더 깊게 살펴보자면 1단계 공격이 실행되면 이미지 호스팅 사이트인 'Photobucket.com'에서 EXIF 메타데이터가 포함된 이미지 파일을 다운로드를 시도하고 해당 파일의 GPS 정보를 분석하여 가장 가까운 거리의 C&C Server의 IP를 결정 및 연결을 시도한다. 연결에 실패할 경우 'toknowall.com'에서 같은 방식으로 재시도한다. 이 두 가지 방식 모두 실패할 경우 리스너를 생성하여 연결을 돕는 특정 트리거 패킷을 대기하다 탐지가 될 경우 C&C Server 연결을 시도한다.

2단계 공격은 1단계를 통해 배포된 'VPN-Filter'가 실질적인 공격을 하는 부분으로 자료수집, 변조 및 유출, 비인가 명령 실행 또는 장치 조작 등 일반적인 정보 수집 기능을 하고 있다. 또한 특정 악성코드의 경우 장비의 펌웨어를 초기의 설정으로 덮어씌우고 해당 장비를 재부팅해 장비를 마비시키는 자폭 기능도 소지하고 있다. 하지만 몇몇 2단계 악성코드의 기능을 분석한 결과 자폭 기능이 없는 악성코드라고 해도 공격자가 자폭 명령을 수행하면 언제든 해당 장비에 문제를 일으킬 수 있는 것으로 추정되고 있다.

마지막 3단계는 2단계 악성코드의 플러그인으로써, 2단계 악성코드에 별도의 기능을 추가하여 더욱 다양한 공격이 가능하게 한다. 현재까지 발견된 플러그인은 웹사이트 자격 도용, Modbus SCADA 프로토콜 모니터링이 목적인 트래픽을 수집하는 패킷 스니퍼, 2단계 악성코드의 Tor 통신을 지원하는 통신 모듈로 2가지가 발견되었다. 하지만 'VPN-Filter'를 발견한 Talos 팀에 의하면 다양한 종류의 플러그인이 존재하지만, 발견하지 못한 것이라는 말을 하여 어떠한 방식의 공격으로 우리를 위협할지 아무도 모른다.

3.2 VPN-Filter 공격 취약점

'VPN-Filter'는 사물인터넷 botnet을 구축하는 악성코드의 일종으로 정보 수집과 사이버 공격에 효과적인 다양한 기능을 갖춘 다단계 모듈식 악성코드이다. 사물인터넷 장비를 공격하는 악성코드는 보통 재부팅을 하면 소멸하는 데 반해 'VPN-Filter'는 소멸하지 않고 계속해서 살아있다는 것이 특징이다.

해당 악성코드는 공격자가 다양한 작전을 펼칠 수 있고 소재지 파악이 힘든 광범위한 인프라를 구현하는 것이 주요 목적이며 공격적 기능으로는 감염된 장비를 통과하는 정보를 수집, 파괴, 변조시키고 지속적인 잠복이 가능케 함으로 공격자가 어느 때에나 해당 장비의 기능에 장애를 일으킬 수 있다는 점에서 매우 치명적인 위험이 될 수 있다.

또한, 대부분의 감염 디바이스가 인터넷에 연결되어 있고 대부분 디바이스가 악성코드 방지 기능이 내장되어 있지 않아 방어가 매우 어렵고 일반 사용자들이 피해를 복구하기 위해서는 기술적 역량이 필요하기 때문에 스스로 해결하는 것도 불가능에 가깝기 때문에 미리 감염되기 전 보안에 힘쓰는 것이 중요하다.

4. VPN Filter 공격 대응기법

'VPN-Filter'를 사전에 방지하기 위해서 그리고 감염이 되었다면 어떻게 해야 하는가에 대해서 알아보려 한다.

위의 시나리오를 살펴보면 1단계에서 총 3가지 방식을 통하여 연결을 시도하는데 EXIF 메타데이터 분석을 사전에 차단하여 C&C Server의 연결을 어렵게 함으로써 제어권이 빼앗기는 것을 방지하는 방법을 제시하고자 한다.

우선 VPN-Filter 악성코드가 EXIF 메타데이터를 활용하는 방법은 Fig 6과 같이 사진의 GPS 정보를 토대로 위도 및 경도를 분석하여 가까운 C&C Server에 연결을 시도하는 방식이다.

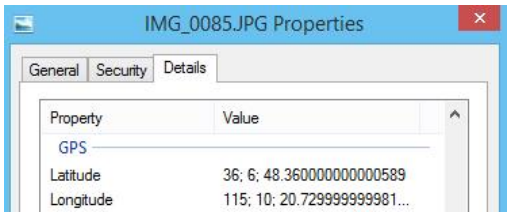

Fig. 6. GPS data in picture files

여기서 인터넷 서비스 제공자들이 업로드된 사진 파일의 EXIF 메타데이터의 GPS를 제거하는 기능을 제공하는 것이다. 이는 지능형 범죄, 예를 들어 GPS 추적을 통한 스토킹 등 지능형 범죄 또한 방지할 수 있게 된다.

인터넷 서비스 제공자들은 간단한 프로그램으로 EXIF 메타데이터를 제거할 수 있다.

```
import piexif

filename = "sample.jpg"

data = piexif.load(filename) # Dict with metadata
piexif.remove(filename)
empty = piexif.load(filename) # No metadata
```

Fig. 7. Example of a simple EXIF metadata removal python program

Fig 7에 작성된 소스를 보면 python으로 제작된 간단한 프로그램이지만 다른 언어로도 서버 구축 환경에 따라 간편하게 구현할 수 있다.

5. 결론

최근 사물인터넷 환경이 상용화 되면서 환경의 변화에 따른 새로운 방식의 공격 기법들이 생겨나고 있다. 'VPN-Filter' 악성코드는 그중 하나로 제조사가 제공하는 최신 보안 패치를 하지 않았거나 보안 설정 강도가 낮은 네트워크 장비들이 주요 타겟으로 공격을 시도하였고 이에 대응하기 위해서는 네트워크 장비 제조사의 꾸준한 보안 솔루션 제공을 위하여 노력해야 하고 사용자는 그 솔루션을 장비에 적용하여 해당 악성코드의 1단계 공격인 공격로 탐색 성공을 사전에 차단하는 것이 중요하다.

해킹의 새로운 국면을 맞이할 시기가 도래하여 과거 보안 분야도 중요했지만, 미래 4차 혁명에 더욱 중요한 기술이자 반드시 존재해야 할 기술로써 자리를 잡게 될 것으로 예상된다. 또한 정부 차원에서의 정보보안 인식에 관한 정책을 수립함으로써 전 국민에게 보안 인식을 심어 주어야 할 의무가 있다고 생각되며 일반 사용자도 자신의 정보와 안전한 인터넷 생활을 즐기기 위해 각자의 노력이 필요하다.

REFERENCES

[1] W. Largent. (2018). *New VPNFilter malware targets at least 500K networking devices worldwide.* California : Cisco.

[2] H. J. Bak, S. B. Yang, J. K. Jang & Y. H. Jeon. (2016). A Study on the Cyber Attack against Social Infrastructure and the Security Countermeasure. *Journal of Korean Society for Internet Information, 17(1),* 285-286.

[3] http://www.igloosec.co.kr/BLOG_VPNFilter%20%EC%95%85%EC%84%B1%EC%BD%94%EB%93%9C%20%EB%B6%84%EC%84%9D%20%EB%B3%B4%EA%B3%A0%EC%84%9C?searchItem=&searchWord=&bbsCateId=47&gotoPage=1

[4] S. Saad, L. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, J. Felix & P. Hakimian. (2011). Detecting P2P botnets through network behavior analysis and machine learning. In Privacy, Security and Trust (PST), *2011 Ninth Annual International Conference.* (pp. 174-180). IEEE.

[5] Y. Fan & N. Xu. (2014). A P2P Botnet Detection Method Used On-line Monitoring and Off-line Detection. International *Journal of Security and Its Applications, 8(3),* 87-96.

[6] J. S. Lee, D. W. Kim, W. H. Park & K. H. Kuk. (2009). A Study on Analysis and Response of DDoS Cyber Terror Based on Network. *Jouranl of Information and Security, 9(3),* 43-51.

[7] I. S. Lee & S. Y. Lee. (2018). A Study on Implementation of DDOS Attack Simulator in Cloud Computing. *The Journal of Korean Institute of Communications and Information Sciences, 2018.6,* 1384-1385.

[8] Y. G. Park. (2013). Analysis of DDoS Attack Trends through Cyber ??Shelters. *KISA, Internet & Security Focus, 2,* 28-38.

[9] J. H. Joo, H. C. Youn, J. S. Oh & T. H. Kim. (2018). A Study on Cognitive Dissonance in the Understanding of Blockchain and Crpytocurrency. *The Journal of the Korea Contents Association, 2018(5),* 73-74.

[10] bitcoin.org

[11] www.ethereum.org

[12] ripple.com
[13] H. Y. Kim. (2018). Analysis of Security Threats and Countermeasures on Blockchain Platforms. *Korean Institute of Information Technology, 16(5),* 103-112.
[14] Microsoft. (2018). *Behavior monitoring combined with machine learning spoils a massive Dofoil coin mining campaign.* Washington : Microsoft
[15] H. S. Seo, J. S. Choi & P. H. Chu. (2009). Design of Classification Methodology of Malicious Code in Windows Environment. *Journal of The Korea Institute of Information Security and Cryptology, 19(2),* 83-92.
[16] S. H. Hong & J. A. Yu. Ransomware attack analysis and countermeasures of defensive aspects. *Journal of Convergence for Information Technology, 8(1),* 139-145.

김 승 호(Kim, Seung Ho) [학생회원]

・2018년 3월 ~ 현재 : 백석대학교 정보통신학부
・관심분야 : 융합 보안, 시스템 보안, 웹 보안, 인공지능
・E-Mail : bayster0508@naver.com

이 근 호(Lee, Keun Ho) [정회원]

・2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
・2010년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
・2006년 9월~2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장
・관심분야 : 이동통신 보안, 융합 보안, 개인정보보호, IoT 보안, 블록체인
・E-Mail : root1004@bu.ac.kr