Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.3, Jun. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.3.501

효율적인 APT 대응 시스템 운영 모델

한 은 혜,† 김 인 석‡
고려대학교

Efficient Operation Model for Effective APT Defense

Eun-hye Han,† In-seok Kim‡
Korea University

요 약

진보하는 IT의 혁명적인 기술 발전에 따라 사이버 보안에 대한 위협과 보안 사고는 함께 증가하고 있다. 지난 수년 동안 큰 규모의 APT 보안 사고가 국내와 해외에서 다수 발생 하였다. 특히 보안 사고에 대한 피해 사실을 해당 조직 내부에서 스스로 알기 전에 외부에서 전달되는 정보에 의해 알게 되는 경우가 더 많다. 4차 산업혁명 등 진보하는 IT 발전과 함께 생성되는 민감한 데이터의 규모는 점점 더 커져가고 있고 데이터를 보호하기 위해 고비용을 투자하여 주요 데이터를 암호화하고, 접근을 통제하고, 여러 보안 장비의 정보를 수집하여 이상 징후를 찾아내기 위한 SIEM을 구현하는 등 많은 보안 대책을 세우고 있다. 하지만 극도로 지능화된 APT의 경우 내부 침투 사실을 인지하는 것조차 파악하기 어려운 것이 현실이다. 이러한 진보된 APT의 보안위협은 소규모, 대규모 기업 및 공공 기관을 포함하여 전 업계에 큰 부담이 아닐 수 없다. 본 논문에서는 사이버킬체인 체계에 맞추어 주요 취약점 현황을 분석하고 이러한 취약점에 대한 효과적인 대응 방안을 연구하여 운영 조직의 업무 환경과 운영 인력을 고려한 효율적인 APT 대응 운영 모델을 제시하고자 한다.

ABSTRACT

With the revolution of IT technology, cyber threats and crimes are also increasing. In the recent years, many large-scale APT attack executed domestically and internationally. Specially, many of the APT incidents were not recognized by internal organizations, were noticed by external entities. With fourth industrial revolution(4IR), advancement of IT technology produce large scale of sensitive data more than ever before; thus, organizations invest a mount of budget for various methods such as encrypting data, access control and even SIEM for analyzing any little sign of risks. However, enhanced intelligent APT it's getting hard to aware or detect. These APT threats are too much burden for SMB, Enterprise and Government Agencies to respond effectively and efficiently. This paper will research what's the limitation and weakness of current defense countermeasure base on Cyber Kill Chain process and will suggest effective and efficient APT defense operation model with considering of organization structure and human resources for operation.

Keywords: APT, Sandboxing, Web Proxy, Cyber Kill Chain, Real-time Filtering

I. 서 론

1.1 연구배경 및 목적

특정 목표를 타깃(target)으로 정하여 오랜 시간에 걸쳐 보안 장비들을 우회하고 악성코드 자신을 지능적으로 숨김 후 은밀히 지속적으로 공격을 수행하여 여러 단계에 걸쳐 목표 시스템에 접근, 활동 거점을 마련한 후 기밀 정보를 수집해 드러나지 않도록 천천히 지속적으로 정보를 빼돌리는 형태의 공격으로 막대한 피해를 주고 있는 '지능적 지속 위협(Advanced Persistent Threats, 이하 APT)' 공격은 차세대 보안위협으로 지목되고 있다.

Received(02. 21. 2017), Modified(05. 08. 2017), Accepted(05. 22. 2017)
† 주저자, nonehan@solupia.co.kr
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

APT 공격은 기본적으로 고도의 보안 취약점 기술을 활용하면서 사회공학적 기법까지 동원한 지능적(Advanced)인 공격 방식이다. 제로데이 취약점이나 루트킷 기법과 같은 지능적인 공격기법을 동시다발적으로 이용하고 인지하기 어려운 허위 상황을 실제처럼 꾸며 접근하는 방식으로 인간의 허점을 노려 표적에 은밀히 침투 하는 사회공학적 기법을 동시에 사용한다. 또한, APT 공격은 완벽한 상황을 만들기까지 수년간을 기다리는 정도로 길게 지속적(Persistent)으로 이루어지는 것이 특징이다. 보안 탐지를 피해 은밀히 활동해야 하기 때문이다. APT 공격은 목표로 삼은 시스템에 활동 거점을 마련한 뒤 정보를 탈취하기 위해 꾸준히 해당 시스템에 물리적인 공격을 가한다. 마지막으로 APT 공격은 확실한 목표(Targeted)를 가지고 있다. APT는 특정 정보를 빼내기 위한 목적으로 제조된 경우가 많다. 그래서 가치 있는 고객정보를 가진 기관이나 기업이 APT의 공격 대상이 되고 있다.

APT 공격은 다양한 보안장비와 정보보호 관리체계를 구축·운영하고 있더라도 조기 식별 및 대응이 어려운 위협이다[1]. 최신 보안 기술이 반영된 여러 단계의 보안 솔루션을 구축하여 운영 중인 기관이나 기업에서도 APT 공격의 목표가 되어 개인정보 탈취 이외의 여러 가지 피해(내부 정보 유출, 금전적 피해, 전산망 마비 등 치명적인 유·무형 피해)가 발생 하고 있다.

2016년 최근 공격 형태를 살펴보면 공격 대상 목표물에 따라 대상 목표물에 맞춤화 된 새로운 공격 도구를 생성할 수 있는 툴까지 제공되어 맞춤형 APT(Personalized APT)가 점점 증가하고 있는 상황을 봤을 때 그 동안 APT를 탐지하기 위해 사용했던 침해지표기반분석대응(IoC : Indicators of Compromise) 방식은 쇠퇴할 것이라고 전망하고 있다[12][13]. SIEM(Security Information and Event Management) 시스템을 도입하여 운영하는 기업이나 기관의 운영 담당자 관점에서는 여러 시스템의 주요 정보를 통합하였으나 수집된 대량의 데이터에서 활용 가능한 정보를 추출하기 위해서는 그에 맞는 잘 만들어진 시나리오가 필요하고 그럴 위한 적합한 시나리오 설계가 가능한 분석 전문가를 확보하는 것은 가장 어려운 과제가 되고 있다.

본 논문에서는 최근 발생한 APT 피해 사례를 사이버킬체인(Cyber Kill Chain)의 7단계 대응 전략에 대입하여 기존 보안 대응 체계의 취약한 부분을 분석하고 이에 대한 대응을 보다 효과적으로 할 수 있는 SSL에 대한 가시성 확보, in-line 방식의 Real-Time(실시간) 분석 및 차단의 적용, 화이트리스트 기반의 프로세스 통제, 최종 정보유출에 대한 대응 등의 기술적 보완 대책을 도출하고자 한다. 이를 통해 대규모 금융기업이나 대기업에서 갖추고 있는 전문화된 보안 체계와 전문 보안 인력으로 대응하는 침해지표기반분석대응 방식이 아닌 대규모 기관부터 중소규모의 금융, 기업까지 효율적으로 APT 대응을 할 수 있는 운영 모델을 제시한다.

1.2 연구방법 및 구성

본 연구의 구성은 제Ⅰ장에서 연구배경 및 목적 과 연구방법에 대해서 기술하고 제Ⅱ장에서 사이버킬체인과 APT 공격 대응 환경을 분석과 AHP 평가 모델에 대한 연구를 기술한다. 제Ⅲ장에서는 보다 효율적인 APT 방어 대응을 위한 구체적인 방법을 제시한다. 제Ⅳ장에서는 의사결정 모델을 제시하고, 사례를 통해 검증한다. 제Ⅴ장 결론에서는 본 연구의 시사점에 대해서 기술한다.

본 연구에서는 APT 대응 현황에 대한 자료 수집을 위해 국내 50개의 금융회사 및 기업 보안담당자 설문을 통해서 자료를 수집 하였다. 50개의 기관은 작은 규모부터 큰 규모까지 다양한 규모로 이루어져 있고, 그 중 20개 기관을 대상으로 FGI(Focus Group Interview)를 통하여 문제점을 도출하고 APT 공격 방어를 위한 운영 효율성에 영향을 미치는 평가요인을 선정 하였다. 선정된 평가 요인은 다기준 의사결정(MCDM : Multiple Criteria Decision Making)시 사용되는 AHP 모델[16]을 사용하여 결과를 분석 하였다.

Ⅱ. 선행연구

2.1 Cyber Kill Chains (Lockheed Martin)

2.1.1 Lockheed Martin의 Cyber Kill Chain

APT는 그 자체가 공격자가 충분한 시간과 자원을 갖고 고도화된 기술과 사회공학적 기법을 이용하고 있기 때문에 이런 공격을 악성코드 사전 유입 단계에서 100% 막겠다는 방어 전략은 불가능하며 모든 조직의 보안 전략은 이러한 외부 공격이 내부로 유입이

가능하다는 상황을 반드시 고려해야 한다.

군수 업체인 록히드 마틴(Lockheed Martin Corporation)에서는 사이버킬체인(Cyber Kill Chain)이라는 개념을 정의 하였다[2]. 사이버 공격을 프로세스 상으로 분석하여 각 공격 단계에서 조직에게 가해지는 위협 요소들을 파악하고 공격자의 목적과 의도, 활동을 구분하여 단계별로 완화시킬 수 있는 대응책으로 조직의 방어성 향상을 확보하는 전략을 제시 하고 있다. 2013년 미국 Target사의 정보유출 사고 관련 미국 상원위원회 상무 과학 교통위원회(Committee on Commerce, Science, and Transportation)에서 발표한 자료[20]에서도 사이버킬체인을 참조하여 APT 사고를 분석하고 있다.

사이버 킬 체인 전략의 목적은 APT 공격 활동을 파악하기 위한 기준을 수립하고 기존 인프라 방어 장치를 이용해 어떻게 대항할 수 있는가에 대한 전략으로 공격자의 첨단 공격의 구성요소를 파악함으로 공격자들의 지속적인 활동에 단계적인 대응 체계를 갖추어 공격의 성공 확률을 낮추는데 있다.

2.1.2 Cyber Kill Chains의 단계

록히드 마틴의 사이버킬체인[2]에서 정의하고 있는 공격자의 공격 활동은 정찰(Reconnaissance), 무기화(Weaponization), 전달(Delivery), 악용(Exploitation), 설치(Installation), 명령과 제어(Command & Control), 목적달성(Action on objectives)과정의 총 7단계로 이루어진다.

사이버 킬 체인의 기본 요소를 이해하게 되면 다음과 같은 사실을 알 수 있다. 첫째, 사이버 킬 체인에서 제시한 7단계의 순서에 따라 공격을 진행 하게 된다. 둘째, 7단계의 최종 목표를 달성하기 전까지는 공격에 성공하지 못한 것이다. 결국 방어하는 입장에서는 이러한 7단계의 어느 단계에서든지 공격을 차단할 수 있게 된다면 결국은 공격자의 목표 달성을 방어할 수 있는 기회가 있다는 것이다. 7단계의 공격 내용을 NTT Security에서[3] 다음과 같이 설명하고 있다.

① 정찰(Reconnaissance): 목표물을 정하고 대상을 식별하여 정보를 연구하는 내용으로 이 과정은 대상 목표물의 공격에 활용할 수 있는 이메일 주소와 같은 정보를 인터넷으로부터 수집하고 사회적 관계 정보까지 획득할 수 있는 SNS 등의 다양한 여러 경로들을 활용하거나 그 외에 다양한 기술들을 활용하여 정보 수집을 하게 된다.

② 무기화(Weaponization) : 알려진 취약점 중 패치 되지 않은 취약점(Adobe PDF 문서의 취약점 또는 Microsoft Office 문서의 취약점 등)을 알려진 취약점을 악용하는 익스플로잇을 활용하여 사용자에게 전달되어 유인할 수 있는 무기를 만든다.

③ 유포(Delivery) : 목표물 대상 사용자에게 발송하는 이메일의 파일 또는 링크 첨부, 웹사이트 링크, USB 미디어 장치 등 다양한 형태로 제작된 무기를 전달하게 된다. 최근 백신이나 보안 프로그램의 패치 기능에 대한 취약점을 이용하는 방식 등 보다 고도화된 방법도 증가 하고 있다.

④ 취약공격(Exploitation) : 대상 목표물에 전달된 무기(익스플로잇)가 구동되면서 공격자가 악의적으로 제작한 코드가 실행되어 대상물의 취약점을 이용하여 의도된 공격 방법이 활성화 된다.

⑤ 설치(Installation) : 공격자가 지속적으로 대상 목적지를 장악할 수 있는 백도어(Backdoor)나 원격접근(Remote Access) 가능한 악성 프로그램을 설치한다.

⑥ 명령과 제어(Command and Control) : 공격자가 대상물을 제어할 수 있는 통신 채널(Command and Control)이 생기면서 의도적인 수동 조작 가능해지고 내부 목표에 접근 할 수 있게 된다.

⑦ 목적달성(Actions on Objectives) : 공격자는 목표 데이타를 수집, 암호화, 전달까지 성공하여 목표한 결과물을 획득할 수 있게 된다.

2.1.3 사이버킬체인의 단계 별 대응 방안

NTT Security에서는 사이버킬체인에 대한 대응 전략[4]을 Center for Internet Security (CIS)에서 정의한 Critical Security Controls (CSC)와 매핑[5] 하여 각 단계별 방어 전략을 제시하고 CSC 기준을 참고하여 어떠한 대응을 할 수 있는지 [표 2]과 같이 제시하고 있다.

CIS는 위험한 사이버 공격을 차단하기 위해 CSC 항목을 우선순위별로 구분, 총 20개 항목으로 정의하여 널리 보급하고 있다. 이러한 각 항목은 세계 각국에서 최고의 전문가들에 의해 개발되고, 개선되고 검증되었다. 1번부터 5번까지의 CIS 컨트롤을 적용하는 조직은 약 85%의 사이버 공격 위험을 줄일 수 있

Table 1. The Center for Internet Security (CIS) Critical Security Controls

CSC No.	Description
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protections
CSC 8	Malware Defense
CSC 9	Limitation and Controls of Network Ports, Protocols, and Services
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 16	Account Monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

Table 2. The Attacker Kill Chain and Critical Security Controls

Phase	Critical Security Controls	CSC Item
Reconnaissance	Limit Reconnaissance and reduce the attacker's ability to enumerate the target's footprint	6,9,11,12,20
Weaponization	Interpret potential weaponization based on available information to disrupt future stages	3,9,17,19
Delivery	Identify activity as hostile and interrupt the delivery of malicious content, forcing the attacker to change tactics	3,6,7,11,13,17
Exploitation	Focus controls to minimize exploitation opportunities, reducing vulnerabilities, forcing the attacker into alternate or noisier attacks	3,4,8,17
Installation	Inhibit the installation of malware and other actions, interfering with the attacker's ability to establish and maintain persistent access	3,4,8
Command and Control	Disrupt the attacker's ability to retain long-term remote access and end his hostile access	3,5,6,9,16
Actions on Objectives	Disrupt the attacker's ability to locate, access and extract sensitive information	3,13,14,19

고, 모든 20개 항목의 CIS 컨트롤을 구현하면 94 %의 위험 감소시킬 수 있다고 한다. 이러한 20개의 항목 중 사이버킬체인에 대응하는 항목은 〔표 1〕와 같다.

2.2 APT 피해 사례 연구

2.2.1 A사 APT 공격 및 정보유출 과정

실제 발생한 APT 피해 사례 중 사회적으로 큰 이슈가 되었던 미래창조과학부에서 보도한 A사의 피해 사례[16]에 의하면 A사의 APT 공격은 〔그림 1〕 와 같은 단계로 이루어 졌음을 알 수 있다

2016년 5월 A사의 한 직원(A직원)은 업무시간 중에 사내 PC에서 네이버 웹 메일을 접속하여 자신의 동생 메일계정에서 발송된 한 통의 메일을 수신한다. 메일에는 '우리가족.abcd.scr'이라는 이름으로 스크린세이버(화면보호기) 파일이 첨부되어 있었고 직

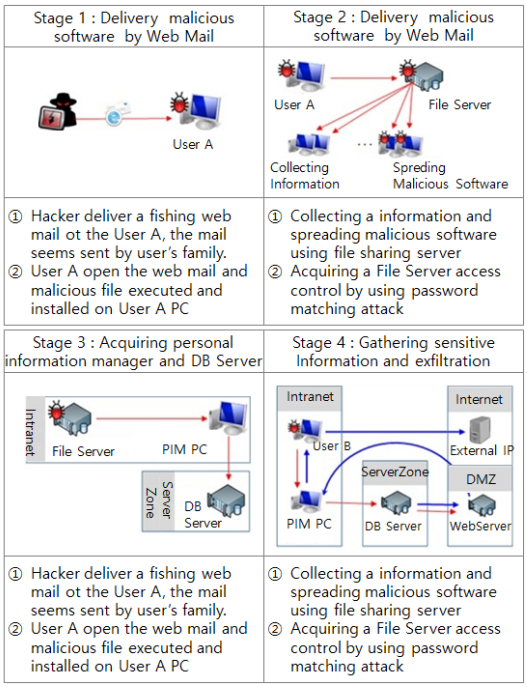

Fig. 1. APT Scenario by Ministry of Science, ICT and Future Planning [16]

원은 아무 의심 없이 다운로드하여 스크린세이버 파일을 실행 한다.

직원(A직원)이 다운로드한 스크린세이버 파일에는 'ielowutil.exe' 악성파일이 숨겨져 있었고 파일이 실행됨과 동시에 악성파일은 PC에는 설치된다. 이 악성파일은 공격자의 명령제어(Command and Control) 서버와 통신 역할을 하게 된다.

직원(A직원) PC에서 파일공유 서버로 악성코드를 전이 시키고 또 다시 파일공유 서버를 통해 여러 PC에 악성코드를 확산시키며 내부정보를 수집했다.

수집한 내부 정보를 이용하여 최종적으로는 개인정보 취급자 PC를 장악하여 DB서버로 접근, 그 이후 다른 직원(B직원) PC를 이용하여 DB로부터 웹서버 유출된 정보를 개인정보 취급자 PC 그 이후 다른 직원(B직원) PC를 거쳐 외부로 정보를 유출 하였다.

최초 악성코드가 유입되는 단계부터 최종 개인정보가 유출되기까지의 과정에서 진행된 각 단계별 공격에서 방어하지 못했던 취약한 부분을 도출 하면 [표 3]과 같이 정리 된다.

2.2.2 A사 APT 공격과 사이버킬체인

최초 직원(A직원)의 PC에 침투하여 내부에서 개인정보를 취득하고 최종 개인정보를 유출할 때까지의

Table 3. Attack Phase and Weakness (Study Case of A Company)

Attack Phase	Weakness
Delivering email thru Naver Web Mail	- Social Engineering Toolkit - Attacker has enough information about the victim - Spear phishing attack
Read the email from the Naver web mail	- Web mail reading was allowed by security policy - Naver Web mail service on HTTPS Encryption - Existing Send-box can not analyze HTTPS
download file and execute	- download screen saver file and execute it with out doubt - src file run with hidden malware execution of msoia.exe
ielowutil.exe process	- Command & Control (C&C) Server communication - C&C connection was encrypted by SSL
malware spreading	- spreading malware, increase victims thru file-server
DB Access	- controling DB manager PC and access Database - evasion DB access control system
download customer data from the DB	- downloading customer data to the web server - move the customer data to the victim(B employee) - avoiding DB access control
transfer user data to the attacker	- transfer user data to the attacker by HTTPS - stolen data was encrypted one more by attacker

APT 공격에 사용된 악성코드 관련 정보는 다음과 같다.

1) 악성코드 전달(DROP) 경로

- %USERPROFILE%\AppData\Local\\Microsoft\Office\15.0\msoia.exe /update
- md5:133a436ddb128520d5061e020f09cb16
- 진단명:Agent.Backdoor.921600.ce

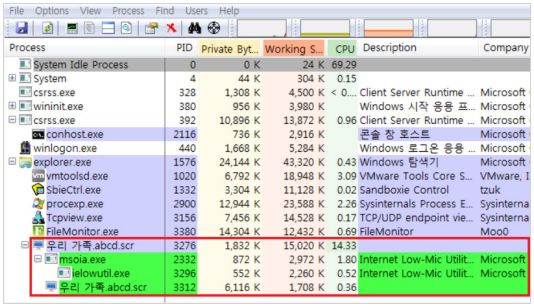

Fig. 2. Process monitoring of msoia.exe

2) 드랍된 악성코드 복제경로

- %USERPROFILE%\AppData\Local\Microsoft\InternetExplorer\IECompatData\ielowutil.exe /autostart
- md5:133a436ddb128520d5061e020f09cb16
- 진단명:Agent.Backdoor.921600.ce

3) 추가 모듈 다운로드

- ielowutil.exe 이용 iehmmapi.dll 다운로드
- iehmmapi.dll 메모리로 로드

Table 4. Attack Scenario with Cyber Kill Chain (Study case of A company)

Phase	Intrusion
Reconnaissance	gathering victim's information
Weaponization	Spear phishing file with screen saver
Delivery	mail.naver.com (SSL) phishing email
Exploitation	msoia.exe
Installation	ielowutil.exe
Command and Control	C&C (SSL)
Actions on Objectives	Exfiltration Customer's personal information (SSL)

4) C&C 연결 (SSL)

- 190.185.124.125:443, 온두라스
- 202.137.244.198:443, 호주
- 220.132.191.110:443, 대만

2.3 AHP 의사결정 방법론 연구

본 연구에서는 효율적인 APT 운영 모델에 반영하기 위한 핵심 항목을 선정하기 위해 다양한 유형의 의사결정 문제에 폭넓게 활용되어 지고 있는 Saaty(1980)의 AHP는 의사결정 방법론[18]을 사용하였다. 복수의 대안에 대한 복수의 평가기준이 존재하는 다기준 의사결정 문제(Multiple Criteria Decision Making: MCDM)를 해결하기 위해 사용하는 대표적인 기법으로 다양한 분야에 활용되어 지고 있다.

AHP의 분석방식은 주어진 의사결정 문제에 대해 목표를 수립하여 평가요인과 대안으로 구성되는 여러 요소를 여러 단계의 계층(Hierarchy) 구조로 모델링한 후 각 계층 내 의사결정 요소 간의 쌍대비교(Pairwise Comparison)를 수행함으로써 최종 우선순위를 도출하게 된다. AHP는 다양한 유형의 MCDM 문제 해결 연구에 효과적으로 사용되고 있고 이석원 등[24]은 AHP 의사결정 방법론을 사용한 많은 사례들을 연구하고 검증하여 금융회사 서버 Privilege 계정 운영방식 결정 모델을 연구하는데 사용하였다. 이러한 AHP 의사결정 방법론의 수행하는 절차를 정리하면 [표 5]의 내용과 같이 8단계의 절차로 이루어진다.

Table 5. AHP Process

Phase	Scenario and week point
1	- Defining the decision problem
2	- Modeling the Hierarchy
3	- Collecting data from experts
4	- Employing the pairwise comparison
6	- Estimating relative weights of elements
7	- Calculating the degree of consistency
8	- Calculating the mean relative weights

III. APT 공격 대응 환경에 대한 분석

사이버킬체인 모델을 기반으로 2.2 절의 피해 사례를 분석한 〔표 4〕의 사항에서 정리한 APT 대응에 반드시 포함되어 져야 하는 필수 핵심 사항인 SSL에 대한 대응과 샌드박싱 기술에 의존하고 있는 APT 대응 환경에 대한 위험성은 반드시 인지해야 한다.

3.1 SSL에 대한 위험성

SSL(Secure Socket Layer) 기술은 인터넷 활용에 있어 일상생활과 밀접하게 연관되어 각종 민감한 정보가 보다 광범위 하게 활용 될 수 있도록 큰 기여를 하고 있다. 각종 쇼핑몰, 뱅킹, 기업 간 거래 등의 중요 데이터에 대한 기밀성, 무결성, 인증, 부인방지를 보장하도록 하여 그 사용범위가 점차 광범위 해져가고 있다. 이미 글로벌에서 광범위하게 사용되는 주요 웹 서비스(구글, 야후, 트위터와 페이스 북 등)들은 기본 서비스를 암호화 통신인 HTTPS로 전환 한지 여러 해가 지났고 많은 금융관련 서비스도 이미 암호화된 방식으로 서비스를 하고 있다.

인터넷 서비스의 안정성을 보장을 위해 사용하는 SSL의 암호화 통신의 순기능이 공격자에게는 공격활동을 숨기기 위한 방법으로 악용되기 시작하면서 점차적으로 APT 공격에 SSL 암호화 통신 활용이 급격이 증가하고 있다. 대표적으로 Zeus, China's APT1, Shylock, KINS, Upatre, SpyEye and CryptoWall 등의 악성코드(malware)는 C&C(command and control) 서버와 통신하기 위해 SSL을 사용하고 있다.

목표물에 대한 해커의 공격이 진행되면 공격대상으로부터 수집한 주요 정보들을 공격자가 획득할 수 있는 외부로 유출하는 과정에서도 역시 SSL을 활용하고 있다. 이뿐 아니라 악성코드 자체에 대한 업데이트등 필요한 대부분의 활동에 있어 가시성의 확보가 어려운 SSL을 악의적인 공격에 활용하게 된다.

3.1.1 SSL에 대한 이해

SSL은 Client와 Server간 통신하는 상호 쌍방을 인증하고〔그림 3〕 비밀키 암호(DES, 3DES, RC4)를 사용하여 데이터를 안전하게 보호하기 위해 사용하며 데이터의 위/변조를 막기 위해 메시지 인증코드(Message Authentication Code)를 사용하고 있다.

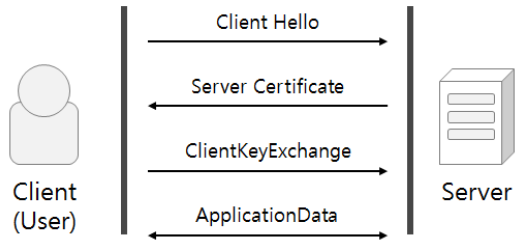

Fig. 3. Two Party Handshake

3.1.2 SSL 사용 증가에 따른 위험성의 증가

2013년 발표한 가트너(Gartner) 리포트〔7〕에 의하면 2016년 인터넷 트래픽 중 SSL이 차지하는 비중은 67%로 증가할 것이고, 2017년에는 암호화된 통신의 50%가 APT공격 등에 활용될 것으로 예측하였고 2013년 조사 당시 암호화 트래픽을 복호화 하지 않는 기관은 80%라고 분석하고 있다.

블루코트코리아〔16〕에서는 2014년 대비 SSL을 사용하는 악성코드는 58배 증가하였고 SSL을 사용하는 C&C 통신은 200배가 증가 한 것으로 발표하고 있다. 또한 전 세계에서 가장 큰 9억 엔드포인트 기반 클라우드 수집 인프라를 보유한 포스포인트사의 통계자료 에 의하면 2016년 10월 기준, 전 세계의 SSL 비중은 48%, 한국은 37%가 SSL을 사용하고 있는 것으로 집계하고 있다. 이러한 SSL의 사용율은 가트너에서 예측〔7〕 하고 있는 바와 같이 지속 증가할 것이다.

네트워크 트래픽을 분석하는 것이 네트워크의 보안 정책 전략의 핵심 요소이고 네트워크 보안을 위해 여러 가지 기술을 복합적으로 사용하고 있지만 그중 SSL 트래픽 부분은 네트워크 분석 영역에서 보이지 않는 블라인드(BLIND) 영역이 되고 있고 시대적 흐름에 따라 점차 증가할 수밖에 없는 환경이다. 이렇게 암호화된 트래픽을 분석하지 않고는 정교하게 고도화된 APT 공격에는 무방비 상태가 될 수밖에 없으며 이미 암호화된 방식으로 내부에 침투하여 활동하고 있는 악성코드를 감지하지 못하고 있을 수도 있다.

네트워크 구간에서 분석 및 관리가 불가능한 SSL 기반의 암호화된 트래픽은 HTTPS를 사용하는 웹사이트에 접속하는 내부 사용자의 인터넷 접속(Outbound)에 있어 아무런 대책 없이 APT 공격에

노출되게 하며 해커에 의해 점령당한 단말장비의 C&C 통신에 의해 악의적으로 도용이 되고 최종적으로 주요 정보가 유출되는 모든 과정에서 무방비 상태가 된다.

SSL 기반의 암호화 된 트래픽을 분석할 수 없는 문제를 극복하기 위해서는 SSL을 복호화하여 가시성을 확보 수 있는 기술이 필요한데 〔그림 4〕에서 대표적인 SSL Proxy 방식을 보여준다. SSL 분석을 위해서는 외부로 연결되는 웹 트레픽을 in-line 으로 구성하는 MITM (man-in-the-middle) 방식을 사용하게 된다.

SSL에 대한 가시성을 확보함으로서 사각지대의 암호화된 트래픽을 분석하여 APT의 위협을 감지능력을 향상 시키고 또 다른 측면으로는 APT 공경에 의해 발생되는 최종 데이터 유출에 대한 방지 능력도 더욱 강화 할 수 있게 된다.

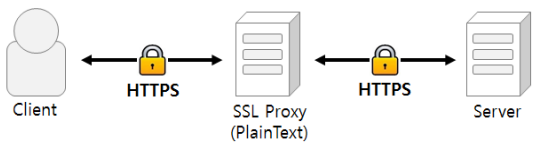

Fig. 4. SSL Interception by Proxy

3.1.3 국내 기관의 SSL 사용 현황

설문 대상 기관들의 SSL에 대한 사용 현황은 〔표 6〕과 같다. 포스포인트사의 통계자료에서 제공하는 한국의 37% SSL 비중과 유사함을 볼 수 있다.

Table 6. SSL Ratio

SSL Ratio Range	Ratio of Targets
0~20%	20.4%
~30%	29.6%
~40%	9.3%
~50%	16.7%
etc	24.1%

3.1.4 국내 기관의 SSL 가시성 분석 현황

국내 50개 기관의 설문 조사 결과 SSL에 대한 분석을 하고 있는 기관은 19개 기관인 25.9%에 해당하며 이중 13개 기관은 네트워크 DLP(N-DLP)를 구성하여 특정 웹메일(Gmail, Naver, Daum, Nate 메일 등)에 대해서만 Proxy 장비 구성하여 가시성 확보를 적용하고 있다. 그 이외 전체 SSL을 분석하고 있는 기관은 6개에 불과하다. 나머지 기관은 SSL에 대한 분석을 하고 있지 않고 이중 27.8%는 도입에 대한 계획조차 없는 실정이다. 하지만 SSL 가시성 확보에 대한 필요성을 인지하고 있는 보안담당자는 92.6%에 달하며, 이중 74%는 SSL 가시성 확보 또한 반드시 필요하다고 답하고 있다.

3.1.5 100% SSL 복호화 적용의 어려움

SSL 암호화 통신의 가시성을 확보하고 분석하기 위해서는 〔그림 5〕와 같이 사용자가 목적지 서버에 통신하는 중간 과정에 복호화 가능한 Proxy를 적용하여 기술적 복호화 구성이 가능하다.

하지만 실제 Proxy를 구현한 기업/기관의 사례들을 잘 살펴보면 운영상의 문제로 인해 실제 HTTPS 통신의 100%를 모두 복호화 하여 분석을 적용하고 있는 회사는 거의 없다.

보안을 운영하는 실무자가 체감하는 SSL 분석 적용의 어려운 점은 〔표 7〕과 같이 첫 번째는 사용자의 인터넷 사용 속도 저하에 대한 우려, 두 번째는 예외처리 운영 부담으로 정리 된다.

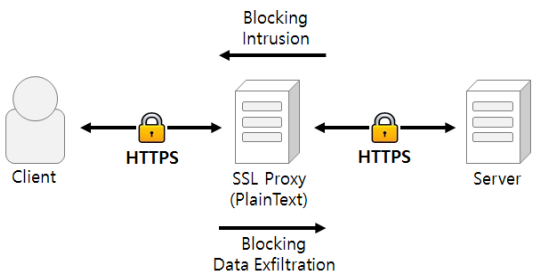

Fig. 5. Block Intrusion and Block Data Exfiltration by Proxying

Table 7. SSL Decoding Limitation

Limitation	Ratio
Latency Time	39.6%
Operation Load	35.8%
Budget	17%
etc	7.6%

1) 사용자의 인터넷 사용 속도 저하
SSL 복호화 적용을 시도했던 기업/기관에서는 HTTPS 복호화 적용 시 사용자가 느끼는 체감 속도가 저하되는 문제로 모든 HTTPS 사용에 대해 100% 복호화를 적용하지 못한다고 설명한다.

2) 예외 처리 운영 부담
대표적으로 금융회사의 웹 서비스 (인터넷뱅킹(Internet Banking), 인터넷 주식거래(Internet Stock Trading)) 및 공공서비스(Government Service))등의 웹 사이트에서는 암호화 된 HTTPS로 웹 서비스를 하고 있고 이러한 SSL기반의 HTTPS 서비스는 점차 증가하고 있다. 이러한 웹 서비스 중에는 아이클라우드(iCloud, 애플이 제공하는 클라우드 저장 공간이자 클라우드 컴퓨팅 서비스)와 같이 Proxy를 통해서 접속되는 사용자의 접속 자체를 거부하는 웹 사이트가 다수 있으며 이러한 경우는 일일이 건별로 예외처리를 해야 하는 수작업 운영 관리 대상이 된다. 이렇게 발생되는 예외에 대한 처리의 범위를 국내뿐 아니라 해외까지 고려하면 일일이 관리해야 하는 대상의 숫자는 실제로 운영 인력 및 처리에 부담을 가지게 된다.

3.2 샌드박스 기반 방어 대응 취약점

3.2.1 샌드박스 우회 취약점

대부분의 금융회사나 기업에서는 APT 방어를 악성코드 유입을 탐지하여 대응하기 위한 목적으로 네트워크 기반 또는 이메일 기반의 샌드박스 기반의 솔루션을 활용하고 있다. 하지만 최근의 악성 코드는 오래되고 알려진 기술인 샌드박스를 우회[14][25]하기 위한 회피 기능을 가지고 있고, 이러한 샌드박스 회피 문제를 극복하고 탐지 능력을 향상[26][27]시키기 위한 연구 또한 계속해서 진행 되고 있다.

3.2.2 샌드박스 탐지 시점의 문제

인터넷 사용에 대한 서비스는 실시간으로 사용자에게 서비스를 해야 하기 때문에 인터넷으로 연결되는 구간에 적용하는 샌드박싱 구성은 대부분 실시간 검사 후 차단하는 방식이 아닌 모니터링 모드로 운영하고 있다. 모니터링 모드로 운영하는 샌드박스 구성에서는 악성코드를 탐지하는 시점이 이미 악성코드가 내부로 유입 된 이후가 대부분이다.

샌드박스에서 탐지한 악성코드가 정탐인 경우에도 탐지 이후 사후 대응을 위해서는 해당 악성코드가 유입된 사용자 PC를 찾아서 해당 악성코드를 확인 후 삭제 하거나 포맷하는 등의 수동적인 운영인력이 투입되어야하기 때문에 일반적인 조직에서는 이러한 대응을 위한 운영 조직이나 대응 리소스에 큰 부담을 가지는 것이 현실이다.

3.2.3 False Positive에 대한 운영 부담 가중

샌드박스에서 탐지하는 가상환경에서의 행위기반 악성코드 분석 기술은 운영관점에서 큰 부담을 만들어 내고 있다. 샌드박스에서 발생시키는 모든 건에 대해서 보안 운영자 또는 보안 담당자가가 False Positive와 정탐의 여부를 판단해야 한다. 규모가 큰 금융 기관이나 기업에서는 의사결정을 위해 탐지 결과에 대한 분석이 가능한 분석 전문가나 관제 전문가를 두고 있지만 규모가 작은 기업이나 기관에서 현실적으로 그러한 전문가를 상시 배치하기는 것은 어려운 문제이다[14].

False Positive로 인한 경고(Alert)의 비중이 많을수록 보안 담당자는 경고 자체에 점차적으로 둔감해지게 되어 모든 건에 대해서 대응을 하지 못하게 된다. 실제 악성코드로 탐지 하였으나 정탐으로 인지하지 못하거나 너무 많은 경고를 모두 다 대응하지 못해 금감원이나 내부 감사의 지적사항이 되기 때문에 보안운영자로서의 부담은 가중될 수밖에 없다. 결국 많은 False Positive에 대한 경고는 실제 위협에 대한 즉시 인지를 방해하는 요소가 되며 정탐의 경우에도 모두 수동으로 대응해야 하는 문제에 직면하게 된다.

3.3 체류시간(Dwell Time)에 대한 고려

기업이나 기관들이 자사의 망 내부로 공격이 침투된 사실을 알게 되는 건 2014년 기준으로 공격자의 최초 침입 후 평균 205일이 지나서 이다. 2013년 229일 에 비하면 24일 가량 빨라진 것이지만 최초 침해 발생부터 발견까지 6개월 이상을 전혀 모르고 있었다는 것이다[11]. 6개월 이라는 오랜 시간 동안 공격자가 할 수 있는 공격의 범위는 우리가 알고 있는 것 이상일 것이다.

침투 이후의 체류시간(Dwell Time)이란 공격자가 내부 네트워크에 침입한 시점 이후 발견이 되어 차단되어 더 이상의 행위를 할 수 없을 시점 또는 목표한 작업을 다 끝낸 후 스스로 떠나는 시점까지의 소요 시간을 말한다. APT 방어차원에서의 목표는 이 체류 시간을 최대한 짧게 줄여 공격자가 행동할 수 있는 확산과 침해 활동을 최소화해야 한다.

결국 알지 못하면 대응조차 하지 못하기 때문에 이러한 침해 사실을 최대한 빨리 발견하기 위한 보안 체계는 반드시 필요한 대응 방안이다.

3.4 APT 공격의 진화 방향

향후 APT의 공격은 계속해서 증가하고 더 교묘해지며 역동적으로 발전할 것으로 예측하고 있다[12][13]. 공격을 위한 도구들이 상품화 되면서 공격 도구를 쉽게 구매할 수 있게 되고 이러한 공격 툴은 공격을 위해 준비하는 시간과 노력은 절약하면서 탐지와 추적이 어려워지는 맞춤화된 공격들을 만들어 내게 될 것이다. 상품화된 공격 도구들은 공격을 타인으로 위장하거나 추적을 회피하는 효과를 가지면서, 공격 시 발생하는 흔적을 줄여 탐지를 피할 수 있게 하고 특히 메모리 상주형과 파일이 존재하지 않는 형태의(fileless) 악성 코드가 증가하여 APT의 특성을 탐지해 왔던 고전적인 침해 지표에 기반 한 탐지 방법은 대응의 한계가 있을 수밖에 없다.

세계 최고의 보안 기업도 뛰어난 보안전문가도 APT에 대한 문제를 쉽게 해결할 수 있다고 자신하며 단언 하지 않는다. 오히려 그 지능화와 위험성이 IT의 발전 속도 이상으로 더 커질 것으로 예측하고 고전적인 방식으로는 APT 공격 자체를 찾아내기도 어려워질 것이라고 예측한다.

IV. APT 방어 효과를 위한 개선사항

4.1 개요

APT 공격을 방어하기 위한 사이버킬체인의 전략은 단편적인 APT 대응이 아닌 APT 공격 사이클 전체를 고려한 관점에서 APT 대응이 필요성을 말해주고 있다. 그 중에서도 다음의 다항은 반드시 고려되어야 하며 본 논문에서는 다음 사항에 대해 중점적으로 대책을 수립하고자 한다.

첫째, SSL기반의 HTTPS 암호화 통신에 대한 가시성 확보는 선택이 아닌 필수사항 이다[7].

둘째, 국내의 경우 대부분 샌드박스 기술을 이용한 가상화 기반의 행위분석을 이용하여 악성코드를 탐지하여 대응하는 체계가 있지만 샌드박싱 탐지에 대한 회피의 문제[14][25], 현실적인 운영성과 즉시대응에 어려운 점이 있다. 샌드박스 기술을 활용하면서 그에 대한 부족한 부분을 대응하기 위한 대책 역시 반드시 필요하다. 그 중에 하나가 웹 사용에 대한 실시간 분석/차단이 될 수 있고 또 하나는 화이트리스트 기반의 프로세스 통제이다[28].

셋째, 사회공학적 기법 공격까지 융합된 고도화된 최근 공격 형태를 볼 때 악성코드 자체의 내부 유입을 100% 막는 것은 불가능하다. 따라서 악성코드 유입이 가능하다는 전제 조건은 반드시 고려하여 최종 유출이 되는 단계 범위까지 APT 대응 범위에 포함하여 DLP(정보유출방지)에 대한 융합 대책을 반드시 고려해야 한다[29].

4.2 효율적인 SSL 분석 방법 제시

4.2.1 카테고리 기반 복호화 예외정책 구현

복호화를 적용할 수 없는 웹사이트에 대한 복호화 예외처리를 손쉽게 할 수 있는 방식을 고려해야 한다. 예를 들어 금융 분야의 카테고리(Finance Category)를 대상으로 예외처리를 설정할 수 있다면 하나하나의 인터넷 뱅킹 웹 사이트, 하나하나의 주식 트레이딩 웹 사이트를 일일이 모두 예외처리 해야 하는 업무 부담을 최소화 할 수 있다. 이러한 카테고리(category) 단위의 예외정책은 반드시 필요하다. 특히 금융 카테고리에 해당하는 사이트에는 금융거래에 필요한 개인 정보가 사용이 되므로 조직 입장에서도 해당 거래에서 사용되는 트래픽 정보를 반드시 복호화 하여 검증해야 할 필요성은 없다.

4.2.2 카테고리 정보의 자동 업데이트

끊임없이 변화하는 웹 사이트 정보를 지속적으로 업데이트하여 카테고리 분류 그룹에 자동으로 반영하는 서비스도 반드시 필요하다. 하루에도 수없이 새로 생겨나는 웹사이트 또는 사라지는 사이트 등이 자동으로 반영되어 운영자의 개입 없이 적용할 수 있다면 수작업을 최소화 하고 효율적으로 운영이 가능할 것이다.

4.2.3 서비스 지연(레이턴시-latency) 최소화

SSL 분석을 위한 Proxy 복호화 장비 구성 시 사용자의 체감 속도 저하를 최소화 할 수 있는 성능 검증 또한 반드시 필요하다. 2013년 NSS Lab, Inc. 에서[21]는 차세대방화벽을 대상으로 SSL 복호화 성능을 검증한 자료를 제공하고 있다.

4.3 실시간 위협 차단(클릭 시점의 위협 분석)

사용자에게 서비스 되고 있는 대부분의 웹 서비스들은 끊임없이 계속해서 그 안의 내용이 변화하고 있고 광고제휴, 배너(banner)서비스 등을 통해 검증되지 않은 내용이 포함되어 같이 서비스 될 수 있다. 또는 악의적 공격에 의해 침해된 웹사이트에 의도적인 악성코드를 유포할 수 있는 스크립트가 포함되어 서비스 되거나 악성코드를 유포하기 위한 경유지가 되기도 한다.

금융회사나 일반 대기업의 경우는 서비스 보안에 대한 충분한 투자와 보안 관제 운영 등을 통하여 일정 수준 이상의 검증된 안전한 웹 서비스를 할 수 있지만 작은 규모의 회사 일수록 외부로 제공되는 인터넷 서비스에 대한 보안 안정성을 보장하기에는 어려움이 있다.

이메일을 이용하여 사용자를 속이는 방식으로 사용되는 이메일 피싱(phishing) 공격이 성공하는 주원인은 게이트웨이 방식의 멀웨어(악성코드) 분석을 우회하거나 회피할 수 있는 임베디드(Embedded) 링크를 악용하고 방법을 사용하기 때문이다. 피싱 이메일에 동적 봇넷(dynamic botnet)이나 동적 코드를 서비스하는 웹사이트에 연결되어 있는 임베디드(Embedded) 링크를 사용하여 이러한 이메일 게이트웨이 방식의 방어 체계를 무력화시킬 수 있다.

4.3.1 웹 사이트 접속 통제 방식 Whitelist & Blacklist운영의 취약점

대부분의 조직에서는 내부 사용자의 웹 사이트 접속 통제를 위하여 화이트리스트(Whitelist) 또는 블랙리스트(Blacklist) 방식을 혼합하여 웹사이트 접속을 통제하기 때문에 한번 허용으로 화이트리스트에 등록된 웹사이트는 등록한 이후로는 아무런 제약이 없이 사용자에게 지속적으로 사용이 가능하게 된다. 이러한 화이트리스트에 있는 웹사이트가 침해되고 악용되어 공격의 경유지로 사용이 된다면 결국 무방비 상태가 되게 된다. 대기업이나 상위 금융기관에서는 해당 기관의 웹 서비스에 대해서는 철저한 보안을 하지만 APT 공격의 경우 사전의 치밀한 정찰 단계의 조사를 통해 협력업체나 유관 기관 등 화이트리스트에 허용이 되어 있는 주변의 취약한 경로를 찾아서 공격한다.

강찬구[9]의 연구에서도 조직 내부에 외부 목적지로 접속되는 대상 중 신뢰할 수 있는 사이트를 화이트리스트 등록하고 사용자가 접속 시 화이트리스트에 해당하는 사이트는 접속을 허용하고 그 외의 모든 사이트는 추가로 인증 하는 방식을 제시하였지만 모든 신규 사이트를 건별로 인증하고 화이트리스트에 등록하는 체계가 실제 조직 운영 환경에서 사용자 불편과 운영자 부담을 가중시키며 화이트리스트에 등록된 사이트가 침해되어 악성화 된 사이트에 대해서는 방어가 불가능하다. 실제로 지능화된 APT 공격에서는 대상 조직의 취약한 협력업체를 활용 하는 등 보다 고도화된 기술을 사용하고 있다.

조직 내 사용자가 외부로 접속하는 웹 사이트에 대해서 업무 특성에 따라 화이트리스트 또는 블랙리스트 방식으로 관리할 필요는 있으나 언제든지 해커에 의해 공격을 당할 수 있는 가능성은 늘 존재하므로 화이트리스트에 있는 대상도 매 접속하는 순간에 반드시 검증하는 절차가 필요하다.

4.3.2 위협 시나리오

① 시나리오 #1 : 사용자에게 전송된 이메일에는 특정 웹 페이지로의 링크가 포함되어 있는데 해당 메일이 전송되는 단계에서 이메일 게이트웨이에 의한 최초 검사 시에는 무해한 것으로 나타난다. 하지만 그 다음날 사용자가 그 메일을 수신하고 해당 링크를 클릭할 때는 연결되는 웹 페이지에 이미 악성 코드가 삽입되어 있다. 사용자가 메일을 열어보기 전에 준비하였던 공격으로 해당 사이트는 이미 안전하지 않은 상태가 된 것이다.

② 시나리오 #2 :사용자가 접속하는 사이트 자체에는 아무 문제가 없지만 해당 사이트에서 제공하는 배너 광고를 클릭하는 순간 해당 배너에 연결 웹 페이지 통해 악성코드를 감염시킬 수 있는 스크립트가 숨겨져 있거나 악성코드 유포 사이트로 연결되는 iFrame이 숨겨져 있다.

③ 시나리오 #3 : 사용자가 자주 접속하는 업무 사이트나 협력사 사이트가 해킹되어 사용자가 사이트 접속 시 아무런 행위를 하지 않아도 자동으로 악성코드를 감염시킬 수 있는 스크립트가 숨겨져 있거나 악성코드 유포 사이트로 바로 연결되어 지는 숨겨진 임베디드(Hidden Embedded iframe /Redirection link)링크가 바로 실행된다.

④ 시나리오 #4 : 사용자가 접속하는 상용사이트가 해킹당하거나 배너광고 등에 포함되어 있는 악성 스크립트에 의해 실제 실행파일등의 다운로드와 실행과정 없이 메모리에서 바로 실행되어 악성코드에 감염된다.

4.3.3 In-Line 방식의 Real Time 분석 차단의 필요

4.3.2에서 나열한 위협 시나리오를 방어하기 위해서는 사용자가 웹사이트를 접속하기 위해 클릭하는 그 순간 해당 웹사이트의 웹페이지 내용이 사용자의 브라우저에 도달하기 전, 웹페이지 안의 유해한 내용(악성 스크립트, 악성사이트로의 Redirect, 난독화 코드)이 있는지를 판별하여 유해한 내용은 제거하고 사용자에게 서비스 될 수 있어야 한다[18]. 이러한 구성은 SSL 복호화 분석 시 적용하는 Proxy에서 구현하는 방식과 동일한 MITM (man-in-the-middle) 기법을 이용한 방식으로 구현이 가능하다. in-line 구성으로 웹 콘텐츠의 악성여부를 판별하여 Real-time의 방어 체계가 필요한 보안 위협은 [표 8]과 같다.

세계적으로 알려진 여러 보안 연구소 등에서 이미 분석하여 공개된 멀웨어 일지라도 시그니처 기반의 백신, 정적인 보안 게이트웨이와 방화벽 기술에서 방어에 실패하는 이유는 방어 체계를 회피하기 위한 멀웨어 난독화, 인코딩, 암호화 등의 회피 기술이 적용되어 수개월 수년이 지난 후에도 여전히 방어하지 못

Table 8. Real-Time Protection Categories

Item	Deceription
Malicious Lures	the sites that leat to various types of threats - Breaking news, Celebrity gossip, Popular topics,Social media
Phishing	Phishing site is fake website whose look and feel are almost identical to the legitimate one typically carried out by directs users to enter personal information - email spoofing, instant messaging
Malicious Embedded iFrame	It used for delivery a malware, bots, eploits and other threats - compromised sites, advertising banner
Evasive Malware	One of the most critical challenges, downloading malware such as trojans, worms, spyware and utilizes evasion techniques - obfuscation, encoding, polymorphism, compression, packing, encryption
Bot Networks (botnet)	Internet-connected computers autonomously communicating coordinate their actions by (C&C) or by passing messages to one another - launch attacks, install malware, click fraud - steal victim's information, generate spam
Exploits	Taking advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior - compromised website, iframes & redirections - dynamic payload modification
Spyware	Gathering information from a victim, exfiltrate data and control the victim. it evade anti-virus and anti-malware, it is not an infected file but the code running on memories - carries the initial malicious code, extract the malware payload - call-home for additional malware payload
Malicious Redirection	web sites that contain redirections to threats such as fake AV, bots and other malware. - social networking websites, watering holes - fake plug-ins, fake certificates, obfuscated Javascript
Non-Binary Obfuscated Threats (web-borne)	Utilized various types of obfuscation to hide malicious threats - compromised sites

하고 공격이 성공 하게 된다. 이를 해결하기 위해서는 다음과 같은 보안위협을 방어할 수 있는 방법을 갖추어야 한다[18].

① known and unknown 바이너리(binary) 위협의 실시간 탐지와 차단
② known and unknown 알려지거나 알려지지 않은 web-borne(non-binary) 위협의 실시간 탐지와 차단
③ 탐지 중심이 아니 사이버 보안 킬 체인에 걸쳐 확장된 범위의 보호 제공
④ 인바운드(inbound) 및 아웃바운드(outbound) 악성 트래픽의 탐지와 차단

4.4 unknown 프로세스 검증 및 Whitelist 및 Blacklist 기반의 프로세스 통제

사이버 킬 체인의 전제조건은 내부로 유입되는 악성코드가 유입단계에서 100% 차단이 어렵다는 것을 전제로 하고 있다. PC에서 실행되는 모든 프로세스에 대해서 유효성을 검사하고 검증된 프로세스를 Whitelist로 운영하는 방식은 조직을 안전하게 보호할 수 있다[23]. 50개 기관의 설문조사 결과도 90.7%의 보안 담당자가 Whitelist 및 Blacklist 기반 프로세스 통제가 효과적일 것이라고 생각하거나 이미 도입하여 운영 중 또는 도입 검토한 경험이 있다. 프로세스를 통제/허용하기 위해서는 프로세스의 해쉬정보를 기준 값으로 관리하여 악의적으로 활용되는 동일 프로세스를 구별[23]하여 통제해야 한다.

4.4.1 프로세스 검증 절차

PC에서 프로세스가 실행이 되는 시점에 해당 프로세스를 검사하여 검증된 Whitelist에 있는지 우선 확인하고 이후 악성 프로세스로 알려진 시그니쳐 DB화 비교하여 악성 프로세스는 즉시 실행을 차단하도록 한다.

4.4.2 알려지지 않은 프로세스에 대한 사전 승인

일차적으로 악성 프로세스에 대해서는 즉시 차단을 하고 또한 검증된 알려진 프로세스에 대해서는 사용을 허용하지만 의심스러운 프로세스에 대해서는 사용자의 승인 또는 보안팀의 확인 후에 적용하는 절차를 마련하는 것 또한 APT 위험성을 최소화 하는데 효과적일 수 있다.

4.5 Network/Endpoint 정보 유출 Screening 활동과 정보유출 통제

APT 공격의 경우 목표하는 바가 분명하기 때문에 마지막 공격의 완성단계는 해당 조직에 물리적인 피해를 가하거나 가치 있는 정보를 획득하여 기업이나 기관의 외부로 정보를 유출하여 공격자가 확보하는 것이 최종 단계가 될 수 있다. 이중 정보유출을 목적으로 하는 경우가 더 많은데 최종 목적을 달성하지 못하도록 APT대응에는 정보유출방지를 위한 대응이 반드시 필요하다[22]. 설문조사 답변한 96.3%의 보안담당자가 APT에 의한 정보유출 방지를 위한 DLP와의 상관관계가 중요하다고 하였다.

4.5.1 SSL가시성 확보를 통한 Network/Endpoint 정보유출 Screening 및 정보유출통제

정보유출을 통제하기 위해서 대부분의 기관에서는 네트워크 구간의 정보유출방지(Network DLP) 시스템과 PC단말에서의 정보유출방지(Endpoint DLP) 시스템을 갖추고 있지만 공격자가 암호화 통신을 이용하거나 사용자 PC의 단말보안 프로그램에서 인식할 수 없는 방식을 이용하면 해당 유출을 인지하지 못할 수 있다. 3.1.2에서 언급한 바와 같이 SSL 암호화 통신이 증가하는 추세이고 악의적인 공격은 암호화 통신을 악용하는 형태가 증가하고 있기 때문에 최종 네트워크 DLP 관점에서의 암호화 통신에 대한 가시성 확보는 반드시 필요하다. 일반적인 국내 금융 및 기업에서 적용하고 있는 네트워크 DLP의 적용은 정보유출에 대한 사전 차단 정책 보다는 로그를 남겨 사후 감사하는 용도로 사용하고 있고 그 중 SSL에 대한 가시성 확보는 운영성을 고려하여 Gmail, Naver, Nate, Daum, Yahoo 메일에 대해서만 제한적으로 적용하는 것이 일반적이다.

Table 9. Network DLP& SSL Decoding

Network DLP Mode		Ratio
Blocking	Real-Time Blocking	32.7%
	Monitoring Only	57.6%
SSL Proxying	All Traffic	7.4%
	For some web mail	22.2%
	Planing in Future	70.4%

〔표 9〕의 Network DLP의 적용 현황에 대한 설문조자 내용을 살펴보면 대상 50개 기관 중 실시간 차단을 적용하고 있는 기관은 32.7% 이고 SSL에 대한 전체 가시성을 확보하고 있는 기관은 7.4%에 불과하다.

4.5.2 unknown 목적지 전송에 대한 통제와 전송되는 DATA 검증

APT 공격에 대한 최종 방어 단계로 데이터가 전송되는 목적지를 확인하여 대상 목적지가 불분명한 unknown인 경우에는 우선적으로 데이터 전송을 차단해야 한다. 또한 해커에 의한 자체 암호화를 사용하기 때문에 DLP에서 가시성을 확보하여 분석하지 못하는 임의적 암호화 데이터 전송을 차단하는 것 또한 효과적이다. 내부 업무에 필요한 데이터 전송 시에는 DLP에서 차단하지 않도록 사전 승인과 허용 정책 적용에 대한 절차를 두도록 한다.

4.5.3 A사 사고사례에 대한 방어 시나리오

2.2에서 연구하였던 A사 사고사례를 4장에서 설명하고 있는 개선사항을 도입하여 방어체계를 수립하면 〔표 10〕에서 정리한 내용과 같이 사이버킬체인 모델의 Delivery, Exploitation, Installation, C&C(Command and Control), Actions on Objectives의 3단계부터 7단계까지의 단계에 걸쳐 방어할 수 있는 체계가 갖추어 진다. 3단계부터 7단계 중에 어느 한 단계에서만이라도 차단을 할 수 있어 Kill Chain에 성공한다면 공격자는 최종적인 정보유출 등의 목표를 달성하지 못하게 된다.

4.6 AHP 의사결정 모델을 이용한 검증

효율적인 APT 대응 시스템 운영 모델을 수립하고 그에 대한 효과성을 검증하기 위해 보안 기획업무 또는 보안 운영업무 실무 담당자를 대상으로 2016년 10월, 11월, 12월에 걸쳐 3차례의 설문조사를 실행하였다. 1차 설문조사에서는 50개 기관을 대상으로 APT대응 현황 실태를 조사 하였고 2차 설문조사에서는 50개 기관 중 실제 APT 관련한 업무를 수행하고 있는 14개 금융기관과 6개의 기업의 보안 실무자를 대상으로 설문조사를 수행하여 AHP 계층 모델 수립을 위한 세부 항목을 정의하였다. 3차 설문조사에서는 구성된 AHP 계층 모델에 대한 항목별 쌍대비교 평가를 하고 이를 바탕으로 평가 항목에 대한 가중치를 도출하였다.

Table 10. Attack Blocking with Cyber Kill Chain (Study Case of A Company)

Phase	Intrusion	Method	Block
Reconnaissance	gathering first victim's personal information	-	-
Weaponization	Spear phishing file with screen saver	-	-
Delivery	mail.naver.com (SSL) phishing email (download and execute the .src file)	Real-time Detecting (src file verification and dropping it over mail.naver.com SSL)	YES
Exploitation	msoia.exe	whilelist execution control (verification of new execution file of msoia.exe)	YES
Installation	ielowutil.exe	whilelist execution control (verification of new execution file of ielowutil.exe)	YES
Command and Control	C&C (SSL)	Real-time Detecting and Dropping (dropping session with unknown destination by SSL)	YES
Actions on Objectives	Exfiltration Customer's personal information (SSL)	Real-time Detecting of Dropping by DLP (Exfiltration Data sending to unknown destination over SSL, Exfiltration Data was unknown encrypted and cannot verify by DLP over SSL)	YES

4.6.1 AHP 계층 모델 수립

APT 대응에 필요한 항목들을 선정하기 위한 2차 설문조사는 1차적으로는 이미 기관에 적용하여 사용하고 있는 APT 대응 요소들을 인터뷰를 통하여 도출하였고 2차적으로는 해당 기관에 구현되어 있지는 않으나 앞서 제시했던 4.2에서부터 4.5항목의 개선사항들에 대해서 상세 설명을 한 이후 향후 적용 한다면 효과적일 수 있는 항목들을 설문을 통해 선별하여 총 14개의 세부항목을 정의하였다. APT 대응을 위한 상세 항목들을 선정하는 단계에서 설문 조사를 시행한 총 20개 기관의 현황을 정리하면 〔표 11〕과 같다.

Table 11. Criteria for APT Defense and Current Status of Organizations

Top Criteria	Sub Criteria	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Network APT	Sandboxing of malicious file	O	O	X	O	O	X	O	O	O	O	O	X	X	O	X	X	X	O	O	O
	Real-time Malicious Context Filtering	X	X	X	X	X	O	O	X	X	X	X	X	△	X	X	X	X	X	X	X
	N-APT SSL Visibility	X	X	X	X	X	O	O	X	X	X	X	X	X	X	X	X	X	X	X	O
	unknown destination blocking	X	X	O	X	X	O	O	X	X	X	X	X	X	X	X	X	X	X	X	X
Endpoint Security	Virus Vaccine	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
	Process Monitoring	X	X	X	X	X	O	X	O	X	X	X	O	X	X	X	O	X	X	X	X
	Process blocking base on Whitelist	X	X	X	O	X	O	X	X	X	X	X	O	X	X	X	X	X	X	X	X
Data Loss Prevention	Logging and Screening	O	O	O	X	O	△	△	O	O	O	O	O	O	O	△	△	O	O	O	O
	Real-time blocking for DLP	X	△	△	△	X	△	△	X	X	△	X	O	X	X	X	△	X	△	X	X
	unknown destination exfiltration blocking	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	unknown encryption file blocking	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	NDLP SSL Visibility	X	X	△	△	X	X	X	X	X	X	X	X	△	△	X	X	X	X	X	X
Enterprise Security Management	ESM Screening	O	O	O	O	X	X	X	X	X	O	X	X	X	X	X	X	X	X	X	X
	SIEM Screening	O	O	O	O	X	X	O	O	X	O	O	X	O	O	O	X	X	O	O	O

Table 12. Selecting Factors by Survey

Top Criteria	Sub Criteria	Definition
Network APT	Sandboxing of malicious file	Behavior analysis of suspicious file
	Real-time Malicious Context Filtering	Filtering a malicious contents on Real-time context analysis
	N-APT SSL Visibility	SSL Proxying and Decoding for APT analyze
	unknown destination blocking	Verifying where communication channel comes form
Endpoint Security	Virus Vaccine	Signature base detecting
	Process Monitoring	monitoring process execution and follow up if it's suspicious
	Process blocking base on Whitelist	define the process whilelist if it was verified and un-verified process will be block when it runs
Data Loss Prevention	Logging and Screening	Screening which data is going out from the organization
	Real-time blocking for DLP	it will be useful to real time block capability base on the DLP policy not only monitoring
	unknown destination exfiltration blocking	if the destination is suspicious DLP can block the transfer
	unknown encryption file blocking	if the DLP cannot recognize Data than block the transfer
	NDLP SSL Visibility	SSL Proxying and Decoding for DLP
Enterprise Security Management	ESM Screening	IDS, IPS, FW event analyzing
	SIEM Screening	real-time analysis of alerts generated by network and applications
Management	Operation Load	considering of operation
	Budget Load	considering of Budget

설문을 통해 도출한 세부 항목은 〔표 12〕과 같이 네트워크 APT, Endpoint 보안, 정보유출방지, 관제 분야의 14개 항목과 그 이외 고려가 필요한 운영성과 비용성에 해당하는 관리 요소 2개 항목을 추가, 총 16개의 항목으로 정의하여 2계층으로 구분하고 해당 내용을 반영한 AHP 계층 모델 〔그림 6〕을 수립하였다.

4.6.2 AHP 계층 모델 설문 조사 및 유효성 평가

3차 설문조사에서는 〔그림 6〕의 계층모델을 바탕으로 각 계층과 항목에 대한 척도를 조사하는 설문지를 준비하여 20개 기관의 실무 보안 담당자들을 대상으로 조사를 진행하였다. 설문으로 취합된 평가 내용을 쌍대비교로 계산하여 도출된 가중치가 논리적으로 일관성을 유지하는지 검증하기 위하여 Saaty〔16〕가 개발한 '일관성 비율(CR, Consistency Ratio)' 값을 사용하여 검증하였다. 일관성 비율이 0.1이하일 때 쌍대비교행렬은 일관성이 있으므로 일관성 비율이 0.1 이상인 설문지의 설문자에게 평가 이론에 대해 다시 설명하고 설문지 평가 값을 재평가하여 분석에 반영하였다.

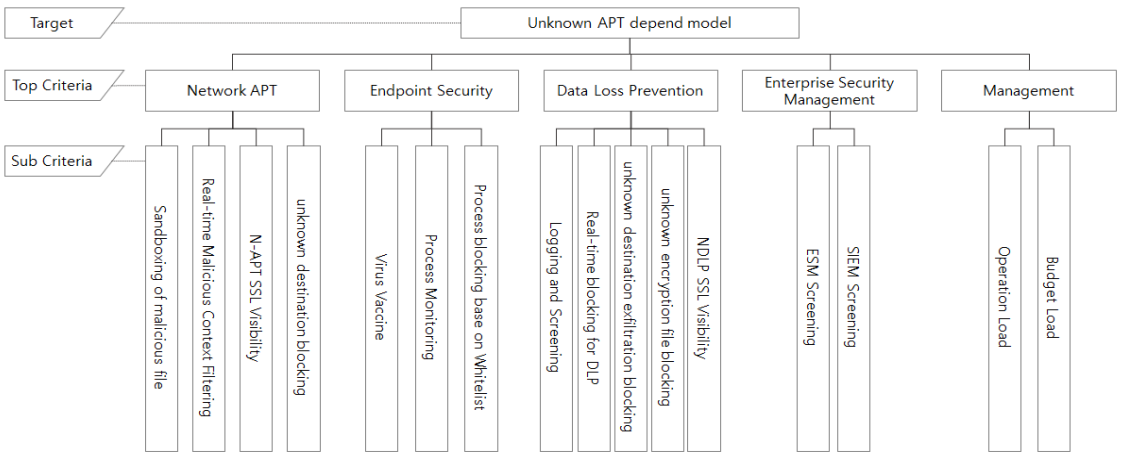

Fig. 6. Defense Model for Unknown APT

Table 13. Ranking of APT Defense Criteria

Top Criteria	Weight	Sub Criteria	Weight	Final Weight	Priority
Network APT	0.434	Sandboxing of malicious file	0.043	0.019	13
		Real-time Malicious Context Filtering	0.329	0.143	2
		N-APT SSL Visibility	0.433	0.188	1
		unknown destination blocking	0.195	0.085	4
Endpoint Security	0.092	Virus Vaccine	0.081	0.007	16
		Process Monitoring	0.188	0.017	14
		Process blocking base on Whitelist	0.731	0.067	7
Data Loss Prevention	0.265	Logging and Screening	0.037	0.01	15
		Real-time blocking for DLP	0.322	0.085	5
		unknown destination exfiltration blocking	0.152	0.04	10
		unknown encryption file blocking	0.152	0.04	11
		NDLP SSL Visibility	0.337	0.089	3
Enterprise Security Management	0.128	ESM Screening	0.345	0.044	9
		SIEM Screening	0.655	0.084	6
Management	0.081	Operation Load	0.750	0.061	8
		Budget Load	0.250	0.02	12

Table 14. APT Defense Countermeasure Operation Model by Cyber Kill Chain

Phase	N-APT / DLP			White list Process Blocking
	SSL Visibility	Real-time Blocking	Unknown Blocking	
Reconnaissance	-	-	-	-
Weaponization	-	-	-	-
Delivery	O(APT)	O(APT)	O(APT)	O
Exploitation	O(APT)	O(APT)	O(APT)	O
Installation	-	-	-	O
Command and Control	O(APT)	O(APT)	O(APT)	-
Actions on Objectives	O(DLP)	O(DLP)	O(DLP)	-

쌍대비교 수행과 CR에 대한 검증을 계산하기 위해 AHP 분석 전문 프로그램인 Export Choice 2000을 이용하였다.

4.6.3 평가 항목 가중치 도출 및 효율적인 APT 대응 시스템 운영 모델 수립

상위 계층(Top Criteria) 5개의 항목과 하위 계층(Sub Criteria) 16개의 평가 항목에 대해 쌍대비교를 수행하고 2개 계층의 평가 결과에 각 항목의 가중치를 반영하면 〔표 13〕의 최종결과가 도출 된다.

가중치가 반영된 최종 〔표 13〕의 결과를 정리하면 APT 방어를 위해 필요한 16개의 세부 대응 요소들 중에 AHP 방법론으로 도출한 주요 7개의 우선순위 항목과 unknown 목적지에대한 통신 및 unknown 암호화 정보유출차단 항목을 사이버킬체인의 7단계에 적용하면 〔표 14〕과 같이 3단계에서 7단계까지의 사이버킬체인의 5단계 영역에 대한 보안대책을 수립할 수 있게 된다. 도입비용 및 운영비용 측면에서 가장 고비용이 필요한 SIEM 영역을 제외하더라도 3단계에서 7단계까지의 5단계의 사이버킬체인 영역에 대한 보안대책 수립이 가능하게 된다.

V. 결 론

사이버킬체인 모델에서는 APT공격이 어느 한 부분에 대한 방어로 이루어지는 것이 아니라 처음의 정찰 단계부터 마지막 단계인 정보유출차단에 대해서까지 전체 영역에 대해서 방어 체계를 준비해야 한다고 명시하고 있다. 이러한 전 방위적 대응 체계로 APT 대한 피해를 최소화 할 수 있다.

APT에 있어서 가장 최대의 위험은 암호화된 통신의 가시성을 확보하지 못하는 블라인드(BLIND) 영역이고 공격자는 점차적으로 이러한 취약점을 악용해 갈 것이다. 이를 위해 암호화된 트래픽인 SSL에 대한 가시성을 확보하는 문제는 가장 최우선적이며 확보된 SSL가시성은 사이버킬체인의 각 단계에서 최대한 활용해야하며 최종 목적달성 단계에서 가능한 정보유출의 DLP 영역까지 충분히 활용 되어져야 한다.

현재 국내의 보안 현황은 극도로 위험한 APT 대응을 탐지 모드 방식으로 운영하며 운영인력에 의한 수동으로 대응하고 있는 한계점에 머물러 있다. 정보유출차단을 위한 DLP분야도 마찬가지로 탐지와 로깅을 우선으로 하고 있다. 이러한 탐지에 국한된 대응을 향후 점차적으로 In-Line 방식으로 구성하여 Real-time 통제 방향으로 발전해야 한다.

사용자가 접속되는 목적지에 대한 검증을 통하여 Unknown 목적지에 대한 통신과 정보전송을 차단하는 정책은 우선적으로 적용되어져야 하며 실행되는 모든 프로세스에 대한 검증과 Whitelist 기반의 통제 방식도 알려지지 않은 APT 공격 방어 대응에 큰 역할을 할 수 있는 부분으로 반드시 고려해야 할 중요한 부분이다.

본 연구에서 제시하는 효율적인 APT 대응 시스템 운영 모델은 사이버킬체인 대응 모델의 3단계부터 7단계까지 대응을 포함하는 효과적인 운영 모델로 금융기관과 대규모의 기업뿐만 아니라 운영인력이 적은 소규모의 기업까지 모두 활용할 수 있는 방법이다. 이러한 보안 방법을 적극적으로 구현하면, 더욱 진보하는 APT 공격에 대한 취약 부분을 개선할 수 있으며, 보다 안전하고 효율적인 보안 체계를 유지할 수 있을 것으로 기대된다.

References

〔1〕 Sung-Baek HAN, Sung-Kwon Hong, "Measures against the APT attack in the financial sector", Journal of The Korea Institute of Information Security & Cryptology, VOL.23, NO.1, pp. 44-53, Feb. 2013

〔2〕 Eric Hutchins, Michael Cloppert and Rohan Amin "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," The Proceedings of the 6th International Conference on Information Warfare and Security, 6, pp. 113-125, March 17-18, 2011.

〔3〕 NTT Security, The NTT Group 2016 Global Threat Intelligence Report

〔4〕 Defense Strategies for Advanced Threats - White Paper: Mapping the SANS 20 Critical Security Controls to the Cyber Kill Chain, NTT Security https://www.solutionary.com/resource-center/white-papers/advanced-threat-protection/

〔5〕 The Center for Internet Security, Critical Security Controls for Effective Cyber Defense Version 6.1, Aug 31,2016

〔6〕 Jeff Jarmoc, "SSL/TLS Interception Proxies and Transitive Trust," Dell SecureWorks Counter Threat Unit Threat Intelligence, Black Hat Europe , March 14, 2012.

〔7〕 Gartner, "Security Leaders Must Address Threats from Rising SSL Traffic," December 2013, refreshed in January 2015

〔8〕 LightCyber Cyber Weapons 2016 Report

〔9〕 Chan-Ku Kang, A Study on Context-aware Algorithm for responding to APT attack. December, 2013.

〔10〕 INFOSEC Institute - The Seven Steps of a Successful Cyber Attack-July 11, 2015

〔11〕 Joshua C. Douglas, CTO, Raytheon|Websense, WHITE PAPER - Cyber Dwell Time and Lateral Movement, 2015.

〔12〕 Kaspersky Security Bulletin. Predictions for 2017 "Indicators of Compromise' are dead' By Juan

〔13〕 Andrés Guerrero-Saade, GReAT, Costin Raiu on November 16, 2016

〔14〕 5 Advanced Persistent Threat Trends to Expect in 2016 By Jason F-Secure January 01. 2016 https://business.f-secure.com/5-advanced-persistent-threat-trends-to-expect-in-2016/

〔15〕 Dong-hee Han, Study of Snort Intrusion Detection Rules for Recognition of Intelligent Threats and Response of Active Detection, Journal of The Korea Institute of Information Security & Cryptology, VOL.25, NO.5, Oct. 2015

〔16〕 Ministry of Science, ICT and Future Planning, Press Release, September 2, 2016 http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1310104

〔17〕 Blue Coat Korea, DATANET, May 26, 2016

〔18〕 Saaty, T. L. "The Analytic Hierarchy Process, McGraw-Hill, New York, 1980."

〔19〕 2015 Miercom Web Security Effectiveness Test Results, DR150303P, Mirecom, April 2015

〔20〕 Committee on Commerce, Science, and Transportation, A "Kill Chain" Analysis of the 2013 Target Data Breach, Majority Staff Report for Chairman Rockefeller March 26, 2014

〔21〕 SSL Performance Problems, Significant SSL Performance Loss Leaves Much Room For Improvement. NSS Labs, Inc 2013

〔22〕 Mustafa, Tarique. "Malicious data leak prevention and purposeful evasion attacks: An approach to Advanced Persistent Threat (APT) management." Electronics, Communications and Photonics Conference (SIECPC), 2013

Saudi International. IEEE, 2013.
〔23〕 Yamamoto, Takumi, Kiyoto Kawauchi, and Shoji Sakurai. "Proposal of a method detecting malicious processes." Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on. IEEE, 2014
〔24〕 Lee, Suk-Won, and Kyung-Ho Lee. "Decision Making Model for Selecting Financial Company Server Privilege Account Operations." Journal of the Korea Institute of Information Security and Cryptology 25.6 (2015): 1607-1620.
〔25〕 Gilboy, Matthew Ryan. Fighting Evasive Malware with DVasion. Diss. 2016.
〔26〕 Joo, Jung-Uk, et al. "The User Action Event Generator Design for Leading Malicious Behaviors from Malware in Sandbox." International Journal of Security and Its Applications 9.10 (2015): 165-176.
〔27〕 Roman Jasek, Martin Kolarik and Tomas Vymola. "Apt detection system using honeypots." Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13), WSEAS Press. 2013.
〔28〕 Beuhring, Aaron, and Kyle Salous. "Beyond blacklisting: Cyberdefense in the era of advanced persistent threats." IEEE Security & Privacy 12.5 (2014): 90-93.
〔29〕 Mustafa, Tarique. "Malicious data leak prevention and purposeful evasion attacks: an approach to advanced persistent threat (APT) management." Electronics, Communications and Photonics Conference (SIECPC), 2013 Saudi International. IEEE, 2013.

〈저자소개〉

한 은 혜 (Eun-hye Han) 정회원
2017년 2월: 고려대학교 정보보호대학원 금융보안학과 석사
2001년 5월~현재: 솔루피아(주) 전무
〈관심분야〉 APT, 정보유출방지, 개인정보보호, 문서보안

김 인 석 (Sang-jin Lee) 정회원
1980년 5월~1998년 12월: 한국은행 과장
1999년 1월~2011년 3월: 금융감독원 부국장
2011년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 금융보안, 전자금융 정책, 전자금융 법규