2017.07.03

Analysis Report

국내 방위산업체 공격 동향 보고서

안랩 시큐리티대응센터(ASEC) 분석팀

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

개요

지난 2010 년부터 본격화된 국내외 방위산업체에 대한 공격은 현재까지 꾸준히 지속되고 있다. 방위산업체는 방위산업물자를 생산하는 업체로, 단순 산업 분야가 아니라 국가 안보와 밀접히 연관되어 있으며, 경쟁국 혹은 적대국가에서 이들 업체의 정보를 노릴 가능성도 배제할 수 없다. 최근 국내 방위산업체에 대한 공격도 지속적으로 확인되고 있으며, 일부 공격 그룹은 방위산업체뿐 아니라 국내 정치, 외교 분야에 대해서도 공격을 가하고 있다. 한편, 공격자들이 특정 국가의 지원을 받고 있는지는 확인되지 않았다.

방위산업체 공격 사례를 분석한 결과, 공격자는 주로 스피어피싱(Spear Phishing) 이메일과 워터링 홀(Watering-hole) 방식을 통해 악성코드를 유포하였다. 특히 국내 업체 공격의 경우 중앙 관리 시스템 등의 국내 유명 프로그램의 취약점을 이용해 악성코드를 유포하기도 했다.

2010년 이후 국내에서는 4개 이상의 공격 그룹이 활동한 것으로 확인된다. 또한 일부 그룹에서 사용된 악성코드와 공격에 사용된 프로그램에서 한글이 사용된 것을 미뤄보아 공격자 중에는 한국어 사용자도 존재할 것으로 추정된다.

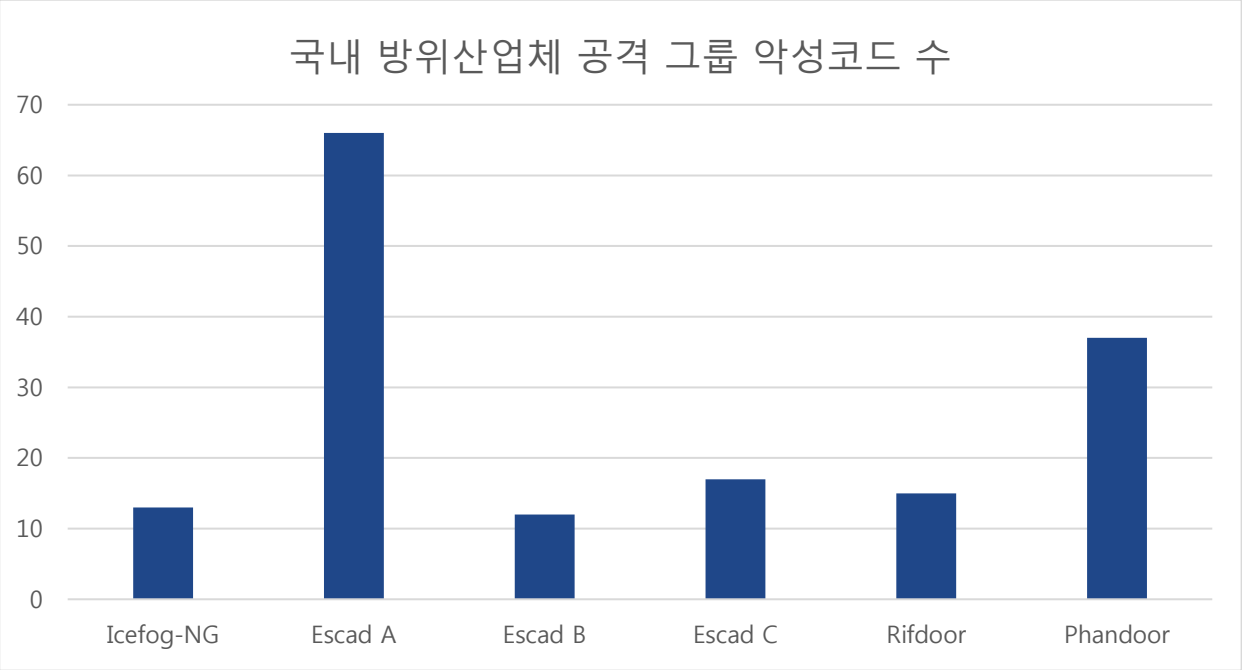
본 보고서에서는 국내 방위산업체를 대상으로 한 공격 사례를 상세히 살펴본다.

일시	공격 대상	공격 그룹	악성코드	설명
2013년 9월	주로 한국 및 일본. 한국의 방위산업체, 정치, 외교 부분 등	아이스포그(Icefog)	Icefog, Icefog-NG	한국을 노린 공격의 경우 정상 한글 (HWP) 파일을 보여줘 사용자를 속임
2015년 11월	서울 ADEX 참가 업체	레드닷 (Red Dot)과 고스트 라이플 (Ghost Rifle)	Escad, Rifdoor	문서 파일을 변조해 취약점 공격을 하는 형태와 오피스 내 매크로 기능을 이용한 형태로 나뉨
2016년 1월	국내 방위산업체	어나니머스 팬텀 (Anonymous Phantom)	Phandoor 등	정확한 감염 방식은 확인되지 않음. 2017년에는 다른 분야로도 공격을 넓히고 있음
2016년 6월	방위산업체와 연관된 대기업	고스트 라이플 (Ghost Rifle)	Ghostrat Rifdoor 등	자산관리 프로그램 취약점을 이용한 국내 방위산업체 연관 대기업 해킹. 해당 공격 그룹은 2015년 11월 ADEX 참관 업체와 2016년 초 보안 업체 해킹 사건과도 연관

[표 1] 주요 국내 방위산업체 공격 사건

공격 현황

국내 방위산업체를 공격한 그룹에서 제작한 악성코드 종류별 수는 다음과 같다. Icefog-NG는 13개, Escad A 형 66개, Escad B형 12개, Escad C형 17개, Rifdoor 15개, Phandoor 37개이다. Escad 변형에 대한 상세 구분은 국내 공격 사례 '오퍼레이션 레드닷(Operation Red Dot) 분석'에서 확인할 수 있다.

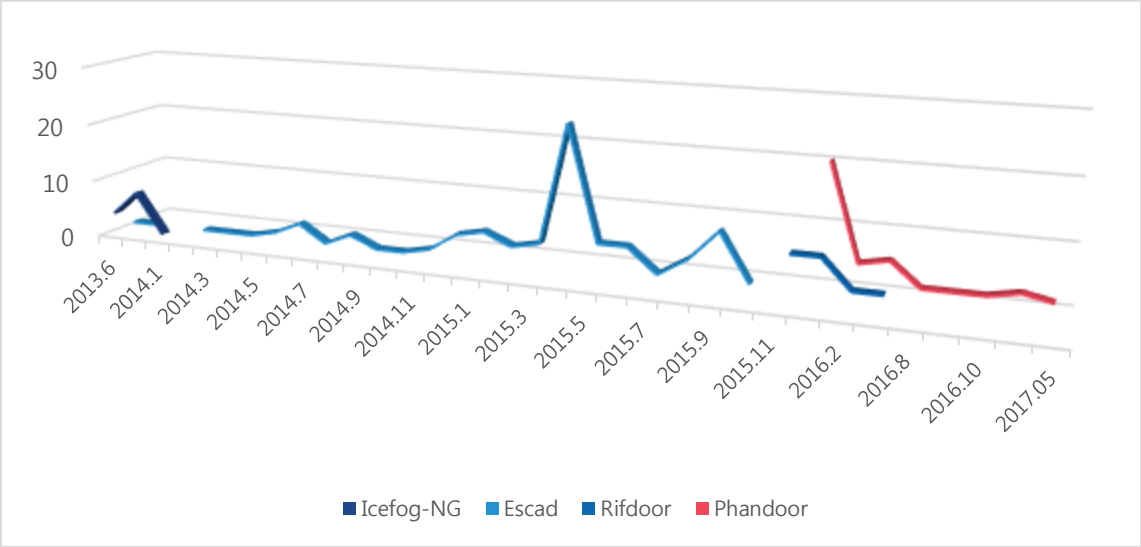


[그림 1] 국내 방위산업체 공격 그룹의 악성코드 종류별 수량

2013 년부터 2017 년 5 월까지 발견된 관련 악성코드 수는 다음과 같다.

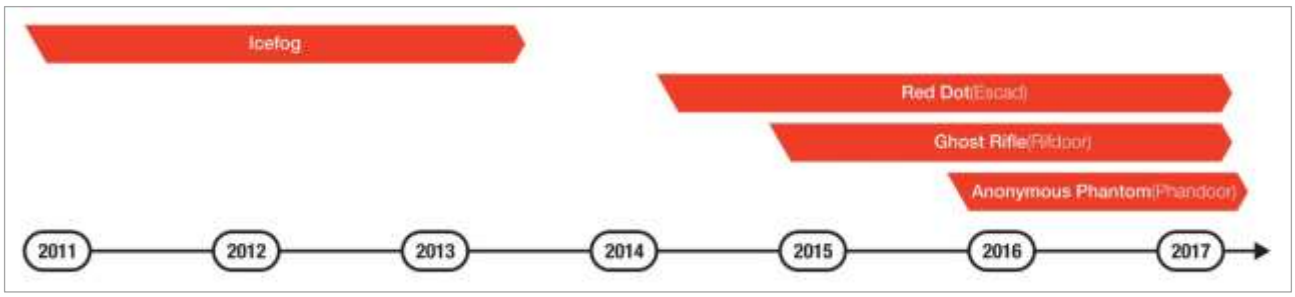
	Icefog-NG	Escad	Rifdoor	Phandoor
2013년	13	2		
2014년		22		
2015년		71	6	
2016년		5	7	32
2017년 5월까지				3

[표 2] 연도별 악성코드 발견 수



[그림 2] 기간별 악성코드 발견 수

국내 방위산업체를 공격한 주요 그룹의 활동 기간은 다음과 같다.



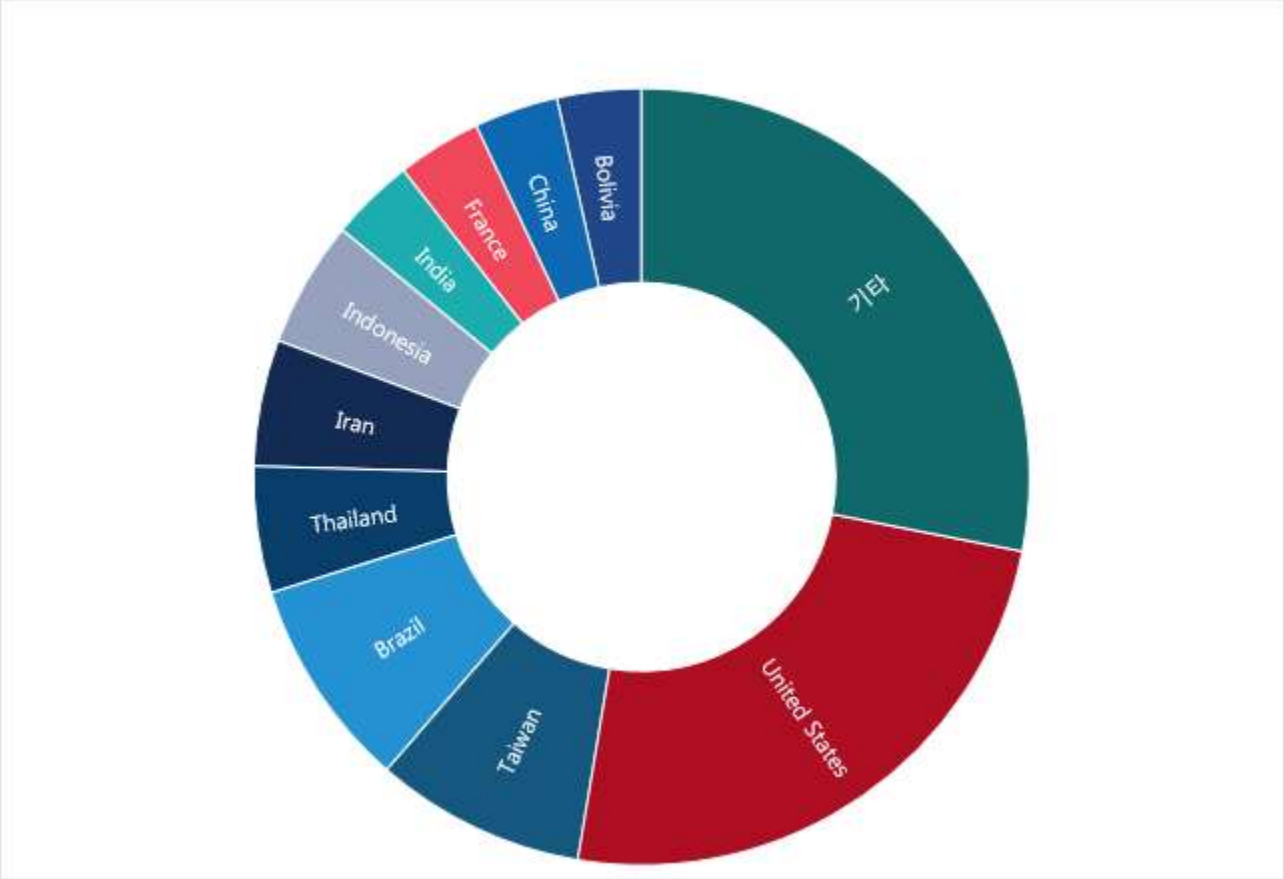
[그림 3] 주요 공격 그룹 활동 기간

주요 공격 그룹 중 하나인 아이스포그(Icefog) 그룹은 적어도 2011년부터 활동을 시작해 2013년 10월까지 활동이 확인되었다. 현재는 활동이 확인되지 않는데 악성코드를 변경해서 활동할 가능성도 있다. 이스캐드(Escad) 악성코드를 사용한 레드닷(Red Dot) 그룹은 2014년 6월부터 2016년 말까지 활동했다. 하지만, 초기 버전으로 보이는 악성코드는 2013년에도 발견되었다. 특히 이 그룹은 2014년 11월 미국 영화사 공격에도 연관된 것으로 보인다. 2016년에는 방위산업체뿐만 아니라 다른 국내 기업에 대한 공격도 진행했다.

2015년 등장한 고스트 라이플(Ghost Rifle) 그룹은 라이프도어(Rifdoor)와 고스트랫(Ghostrat) 악성코드를 주로 사용했다. 레드닷(Red Dot) 그룹과 고스트 라이플(Ghost Rifle) 그룹은 2015년 가을 국내 방위산업체 관련 컨퍼런스인 ADEX((Seoul International Aerospace & Defense Exhibition) 참가 업체에 대한 공격을 가했다. 고스트 라이플(Ghost Rifle) 그룹은 2016년 초 보안 업체에 대한 공격과 대기업 해킹에도 연루되었다고 알려졌다. 2016년 초 등장한 어나니머스 팬텀(Anonymous Phantom) 그룹은 2016년 가을 이후 활동이 뜸하다가

2017년 봄 에너지 관련 연구소 등에 대한 공격이 확인되었다.

오퍼레이션 레드닷(Operation Red Dot)에서 사용된 Escad 악성코드의 C&C 서버 국가별 분포는 다음과 같다.



[그림 4] Escad C&C 서버 국가별 분포

총 57개의 C&C 주소 중 미국이 14곳으로 가장 많으며 그 다음은 브라질 5곳, 대만 5곳이다. 아르헨티나, 벨기에, 볼리비아, 브라질, 중국, 체코, 프랑스, 독일, 인도, 인도네시아, 이란, 일본, 쿠웨이트, 멕시코, 파키스탄, 필리핀, 사우디 아라비아, 슬로바키아, 스페인, 태국, 우크라이나 등 세계 여러 곳에 C&C 서버가 존재한다.

Escad 악성코드 변형에서 확인된 C&C 서버 주소 중 한국은 없지만 2015년부터 2016년까지 발견된 Rifdoor 악성코드와 2016년 초부터 활동을 시작한 Phandoor 악성코드의 C&C 서버 주소는 대부분 한국에 위치했으며, 국내 대학교 시스템을 주로 이용하고 있었다.

공격 방식

방위산업체에 대한 공격 방식은 다른 표적 공격과 마찬가지로 크게 스피어피싱(Spear Phishing) 이메일을 통한 악성코드 유포, 워터링 홀(Watering-hole) 공격, 중앙 관리 시스템을 이용한 공격 등 3가지로 나뉜다. 이외에도 보안 프로그램, 액티브 엑스(Active-X) 프로그램의 취약점을 이용한 공격 방식도 알려졌지만 아직 확인하지 못했다.

스피어피싱(Spear Phishing) 이메일

공격자는 이메일 수신자의 정보를 파악해 첨부 파일을 열어보거나 본문 내용에 포함된 링크(Link)를 클릭하도록 유도한다. 메일의 내용은 주로 업무나 사회적으로 관심을 끄는 내용이다.

일반적으로 워드, 엑셀, 한글, PDF 등의 문서에 악성코드를 포함시켜, 취약점이 존재하는 프로그램으로 해당 문서를 열어볼 경우 취약점을 악용해 악성코드를 감염시킨다. 하지만 이처럼 취약점을 이용한 공격 방식은 해당 취약점이 해결되면 더 이상 사용할 수 없고, 패치가 나오지 않은 제로데이(Zero-day) 취약점을 찾는 것 또한 쉽지 않다.

따라서 공격자는 취약점을 이용하지 않을 경우에는 실행 파일을 그대로 첨부하는 방식을 사용한다. 하지만 단순 실행 파일을 첨부하는 방식은 사용자와 보안 시스템으로부터 쉽게 의심받을 수 있기 때문에 실행 파일을 문서 파일로 위장하여 첨부 파일을 보내기도 한다.

문서 파일로 위장하는 파일 형식으로는 EXE, LNK 파일이 대표적이다. 예를들어 사용자가 HWP 파일로 위장한 LNK 파일을 문서 파일로 착각하여 열어보면 특정 주소로 접속을 유도해 악성코드를 다운로드 한다.

워터링 홀(Watering hole)

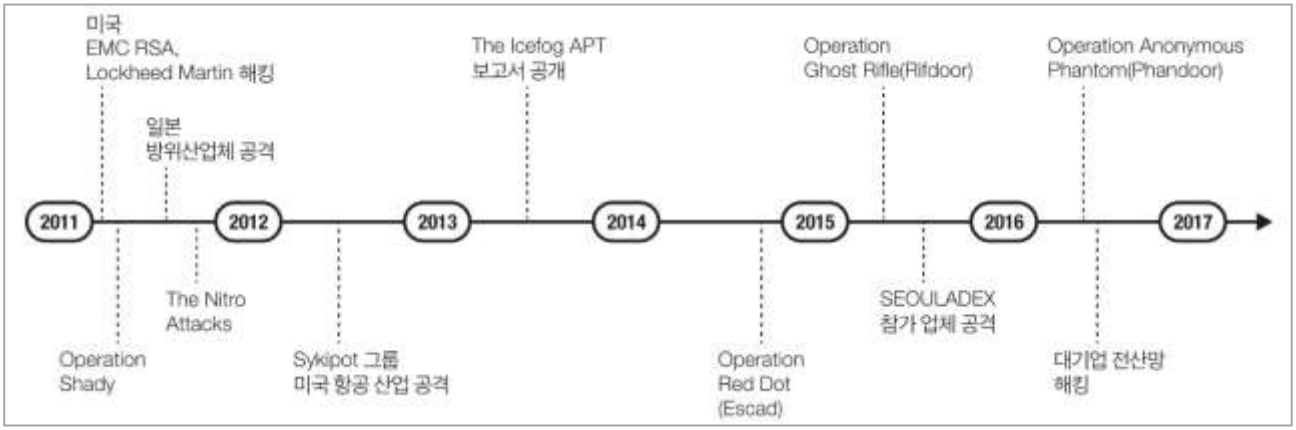
워터링 홀(Watering hole)은 공격자가 특정 웹사이트를 해킹해 취약점 공격 코드를 숨겨두고 사용자가 취약한 웹 브라우저로 접속할 경우 악성코드를 감염시키는 공격 방식이다. 공격자는 자신이 원하는 공격 대상이 자주 방문할만한 사이트를 해킹한다. 일부의 경우, 특정 아이피 주소(IP Address)에서 접속한 경우에만 악성코드에 감염되게 하는 방식으로 더욱 한정된 대상만을 노려, 공격시도를 발견하기 어렵게 한다.

중앙 관리 시스템

일반적으로 회사에서 사용하는 컴퓨터는 관리를 위해 특정 관리 시스템에 연결되어 있다. 2016년 국내 보안 업체와 대기업 해킹 건은 모두 중앙 관리 시스템을 해킹하여 시스템에 연결된 컴퓨터에 악성코드를 배포하는 방식을 사용했다. 공격자는 목표 대상 업체에서 사용하는 프로그램을 미리 분석한 후 해당 프로그램의 취약점을 노려 공격에 이용하고 있다.

국내외 주요 공격 사례

보안 업체 및 언론을 통해 알려진 방위산업체에 대한 주요 공격은 다음과 같다.



[그림 5] 주요 방위산업체 공격

일시	공격 대상	공격 그룹	악성코드	설명
2011년 3월	EMC RSA 와 록히드마틴	미상	Poisonivy	EMC RSA를 해킹 해 OTP 알고리즘을 훔친 후 미국 방산업체인 록히드마틴사를 해킹해 군사 정보 유출
2011년 8월	방산 업체를 포함한 최소 71개 조직	Operation Shady	Shady Rat	5년 동안 공격 진행. 한국 기업 포함
2011년 9월	일본 미쓰비시 중공업	미상	Hupigon	
2011년 10월	미국과 영국 방위산업체	The Nitro Attacks	Poisonivy	화학, 방산 분야 공격
2012년 1월	미국 방위산업체	Sykipot	Sykipot[1]	미국 첨단 사업 분야에 전문 공격 그룹
2013년 9월	주로 한국 및 일본. 한국의 방위산업체, 정치, 외교 부분 등	아이스포그(The Icefog APT).[2]	Icefog. Icefog-NG	한국을 노린 공격의 경우 정상 한글 (HWP) 파일을 보여줘 사용자를 속임
2015년 11월	서울 ADEX 참가업체[3][4]	레드닷 (Red Dot), 고스트 라이플(Ghost Rifle)	Escad, Rifdoor	문서 파일을 변조해 취약점 공격을 하는 형태와 오피스 내 매크로 기능을 이용한 형태로 나뉨
2016년 1월	국내 방위산업체	어나니머스 팬텀 (Anonymous Phantom).	Phandoor 등	정확한 감염 방식은 확인되지 않음. 2017년에는 다른 분야로도 공격을 넓히고 있음
2016년 6월	방위산업체와 연관된 대기업	고스트 라이플(Ghost Rifle).	Ghostrat Rifdoor 등	자산관리 프로그램 취약점을 이용한 국내 방위산업체 연관 대기업 해킹[5]. 해당 공격 그룹은 2015년 11월 ADEX 참관 업체와 2016년 초 보안 업체 해킹 사건과도 연관

[표 3] 주요 방위산업체 공격 사례

[1] http://labs.alienvault.com/labs/index.php/2012/when-the-apt-owns-your-smart-cards-and-certs

[2] http://www.securelist.com/en/blog/208214064/The_Icefog_APT_A_Tale_of_Cloak_and_Three_Daggers

[3] http://www.hankookilbo.com/v/1822cb4edb8f40fa9a778e7584e9c44e

[4] https://www.hankookilbo.com/v/2f84f7d377ec42f99c38bee8bf1e8cd4

[5] http://www.yonhapnews.co.kr/northkorea/2016/06/13/1801000000AKR20160613092851004.HTML

국내 사례

국내 방위산업체에 대한 주요 공격 사례는 다음과 같다.

Icefog-NG 변형

2013년 9월 러시아 보안 업체인 카스퍼스키랩(KasperskyLab)은 분석 보고서를 통해 아이스포그(Icefog) 공격 그룹에 대한 정보를 공개했다.[6] 이에 따르면 해당 그룹은 2011년부터 공격을 시작했으며 한국과 일본의 정부 기관, 그리고 방위 산업체가 주 공격 대상이었다. 마이크로소프트 오피스 취약점(CVE-2012-1856, CVE-2012-0158), 자바 취약점 (CVE-2013-0422, CVE-2012-1723), HLP 취약점 등이 공격에 이용되었으며 국내 공격 대상에는 한글 프로그램의 취약점도 이용되었다. 공격에 사용된 악성코드 중에는 윈도우 악성코드뿐만 아니라 맥 악성코드도 존재한다. 국내 업체의 경우 자료가 유출된 정황도 확인되었다.

안랩은 국내 방위산업체 등에서 해당 그룹의 악성코드 변형을 추가 확인했다. 분석 보고서에 따르면 마지막으로 발견된 변형은 Icefog-NG다. 또한 해당 보고서에 언급되지 않은 변형도 국내 방위산업체로부터 접수되었다. Icefog-NG는 2013년 6월 19일 최초 발견되었으며 10월까지(제작은 8월로 추정) 총 13개의 변형이 발견되었다. 국내에서 발견된 변형인 Icefog-NG의 경우 방위산업체뿐 아니라 정치, 외교 분야도 공격 대상으로 포함되었다.

Icefog-NG는 변형에 따라 다른 PDB 정보를 가지고 있다.

PDB 정보
d:₩jd₩jd(RegRun)₩release₩jd3(reg).pdb
e:₩jd4₩myServer(RegRun)₩release₩jd4(reg).pdb
x:₩jd(RegRun)₩release₩jd3(reg).pdb

[표 4] Icefog-NG PDB 정보

일부 변형은 악성코드가 실행될 때 %TMP%₩~AA.tmp의 존재 여부를 검사한다. 만일 존재하면 자기 자신을 %TMP%₩hwp.hwp로 복사한 다음 hwp.exe를 종료하고 hwp.hwp을 실행한다. 이는 사용자에게 정상 HWP 파일 내용을 보여줘 감염 사실을 알지 못하게 하기 위함으로 보인다.

[6] http://www.securelist.com/en/blog/208214064/The_Icefog_APT_A_Tale_of_Cloak_and_Three_Daggers

변형별로 접속하는 C&C 서버의 주소를 분석한 결과 nprottct.com, boanews.net, hauurri.com 등과 같이 국내 보안 사이트와 유사한 주소가 확인되는 것으로 보아 해당 샘플은 국내를 목표로 했을 가능성이 높다. 현재까지 안랩에서는 이들 변형 중 최소 3개가 국내 공격에 이용되었음을 확인했지만 확인되지 않은 공격 대상이 더 있었을 것으로 보인다.

이처럼 HWP 한글 파일을 보여주는 기능과 국내 사이트와 유사한 C&C 서버 주소를 사용한 것으로 보아 Icefog-NG는 국내를 노린 악성코드로 추정된다. Icefog-NG 변형에 따른 주요 C&C 서버 주소는 다음과 같다.

C&C 서버 주소
esdlin.com/news/upload.aspx
fruitloop.8.100911.com/news/upload.aspx
minihouse.website.iiswan.com/update/upload.aspx
starwings.net
www.***news.net
www.***urri.com
www.kreamnnd.com
www.mnndsc.com/news/upload.aspx
www.***ottct.com

[표 5] Icefog-NG 주요 C&C 서버 주소

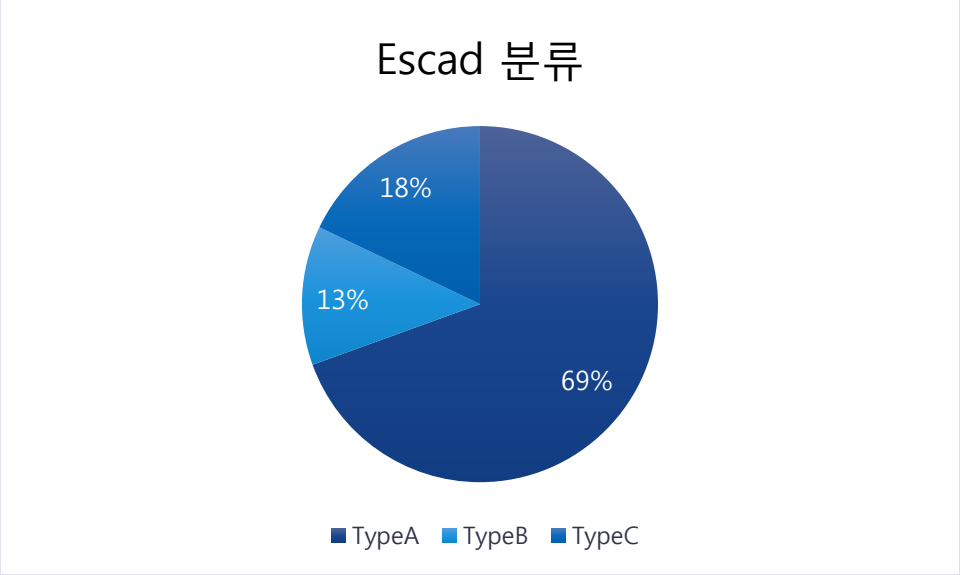
실존하는 국내 사이트 주소와 매우 유사한 www.***ottct.com, www.***news.net, www.***urri.com 사이트 이외에도 www.kreamnnd.com 사이트에 포함된 문자 또한 korea나 mnd(Ministry of National Defense)와 유사해 역시 국내 사용자를 노렸을 가능성이 있다.

Icefog 공격 그룹은 2013년 10월 이후 현재까지 활동이 확인되지 않고 있다. 활동이 중단된 시기는 보고서 발표 시기와 비슷하며 이들이 활동을 중단했는지 악성코드를 변경해 새롭게 활동하고 있는지는 확인되지 않고 있다.

오퍼레이션 레드닷(Operation Red Dot)

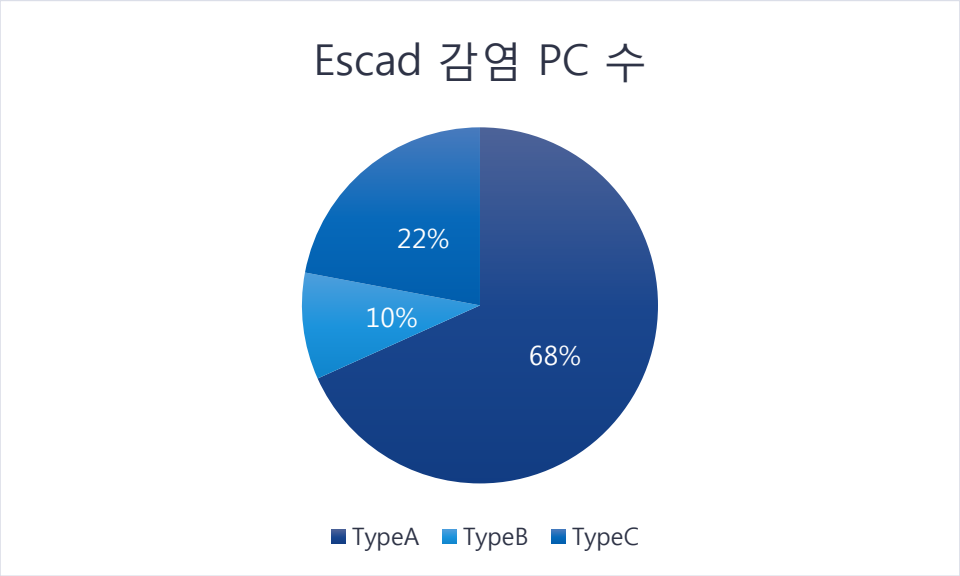
오퍼레이션 레드닷은 2014년 봄부터 2017년 2월까지 계속된 공격으로 2014년 말 미국 영화사 해킹과 연계된 것으로 보인다. 안랩은 100여 개의 관련 Escad 악성코드 변형을 발견했으며 초기 버전으로 추정되는 변형은 2013년부터 발견되었다. 2014년부터는 미국 영화사뿐만 아니라 대북 사이트, 방위 산업체 등에 대한 공격도 확인되었다. 발견된 변형 사이에는 코드 유사성을 포함해 AbodeArm.exe, msnconf.exe 등과 같은 파일명에도 상당한 공통점이 존재했다.

Escad 악성코드는 크게 A형, B형, C형으로 나뉘며 A형이 69%로 가장 많고 그 다음으로는 B형이 18%, 그리고 C형이 13%로 가장 적었다.



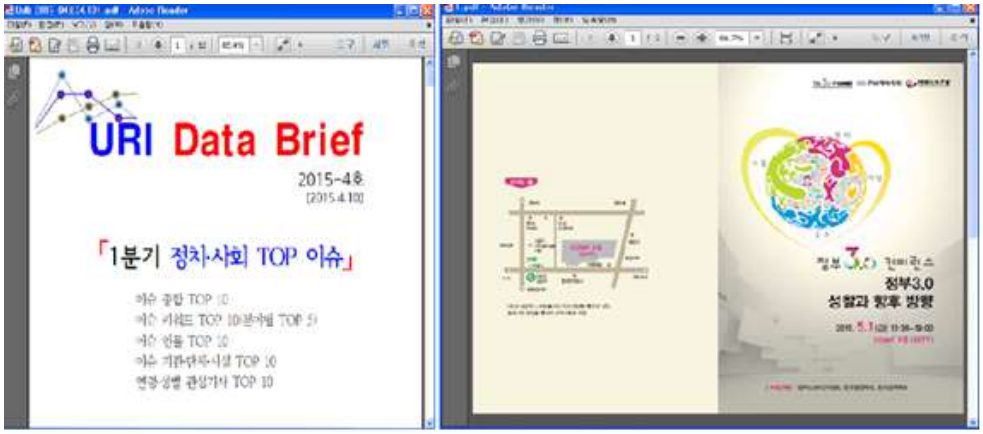
[그림 6] Escad 분류

Escad 악성코드 변형에 감염된 PC의 비율은 A형이 68%, B형은 10%, C형은 22%이다.



[그림 7] Escad 감염 PC 비율

국내 기관에 대한 공격은 2014년 11월 미국 영화사 해킹 이후 2015년 봄부터 확인되었다.

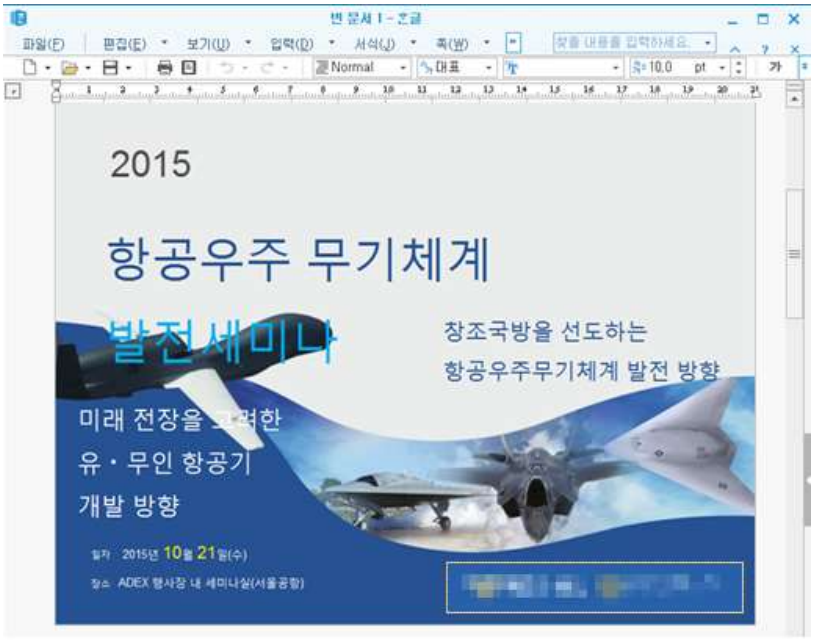


[그림 8] 2015년 공격 메일 첨부 파일 내용

또한 국내 방위산업체에 대한 공격은 2015년 가을부터 본격화됐다. 2015년 10월 국내 방위산업체를 목표로 한 공격은 특정 학회를 사칭한 스피어 피싱 공격이었다.

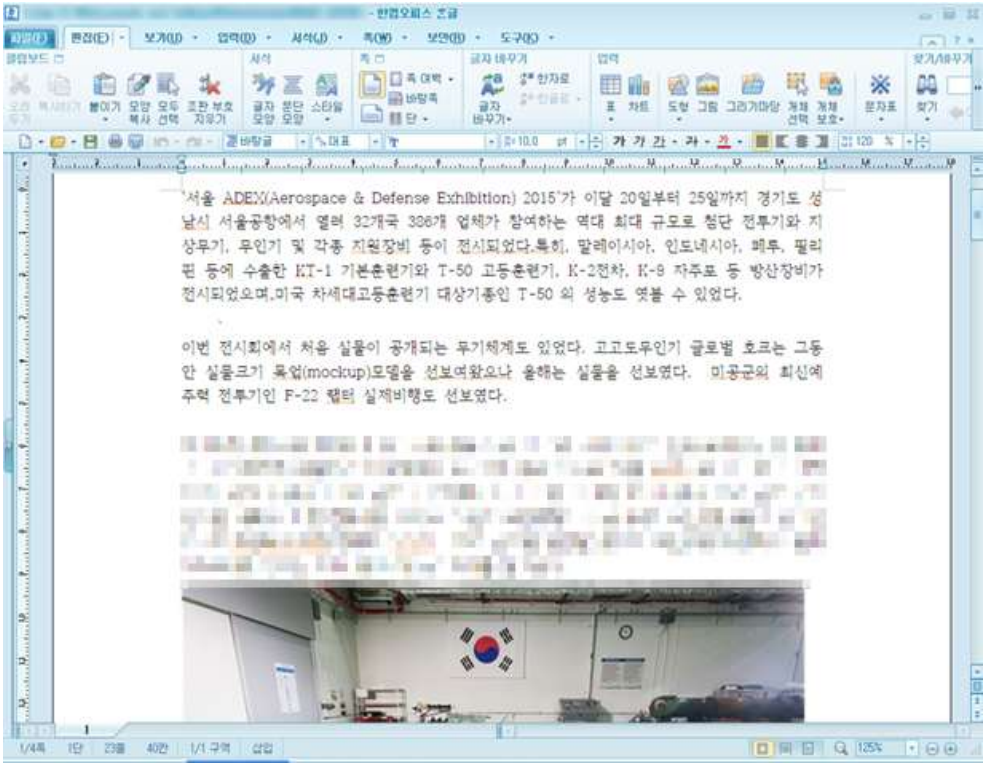
[그림 9] 스피어 피싱 메일

메일에 첨부된 초청장.hwp 파일을 열면 한글 워드프로세스 취약점을 이용한 백도어(Backdoor)가 사용자 컴퓨터에 설치된다.



[그림 10] 초대장 내용

2015년 11월에는 '서울 에어쇼에서 전시된 10대 명품무기입니다'라는 제목으로 전시회 참가 업체들에게 한글 문서를 첨부한 메일을 발송했다. 첨부된 한글 문서를 실행하면 마찬가지로 한글 워드프로세스 취약점을 공격해 사용자 PC를 Escad 악성코드에 감염시킨다.



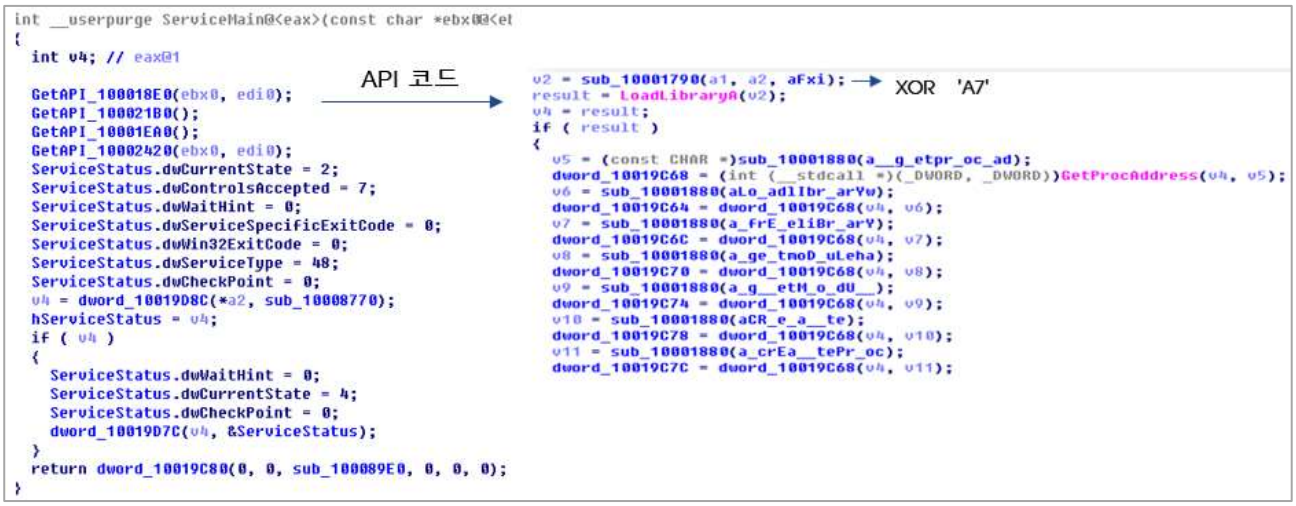
[그림 11] 행사 관련 메일로 가장한 한글 파일

2016년부터는 공격 대상이 확대되어 호스팅 업체, 대기업, 언론사 등에 대해서도 공격을 수행하였으며 악성코드도 좀 더 다양화되었으며 윈도우 제로데이 취약점을 이용한 공격도 진행했다. 최종적으로 2017년 2월까지 공격이 확인되었지만 현재까지도 공격을 지속하고 있을 가능성이 높다.

■ Escad 악성코드 변형

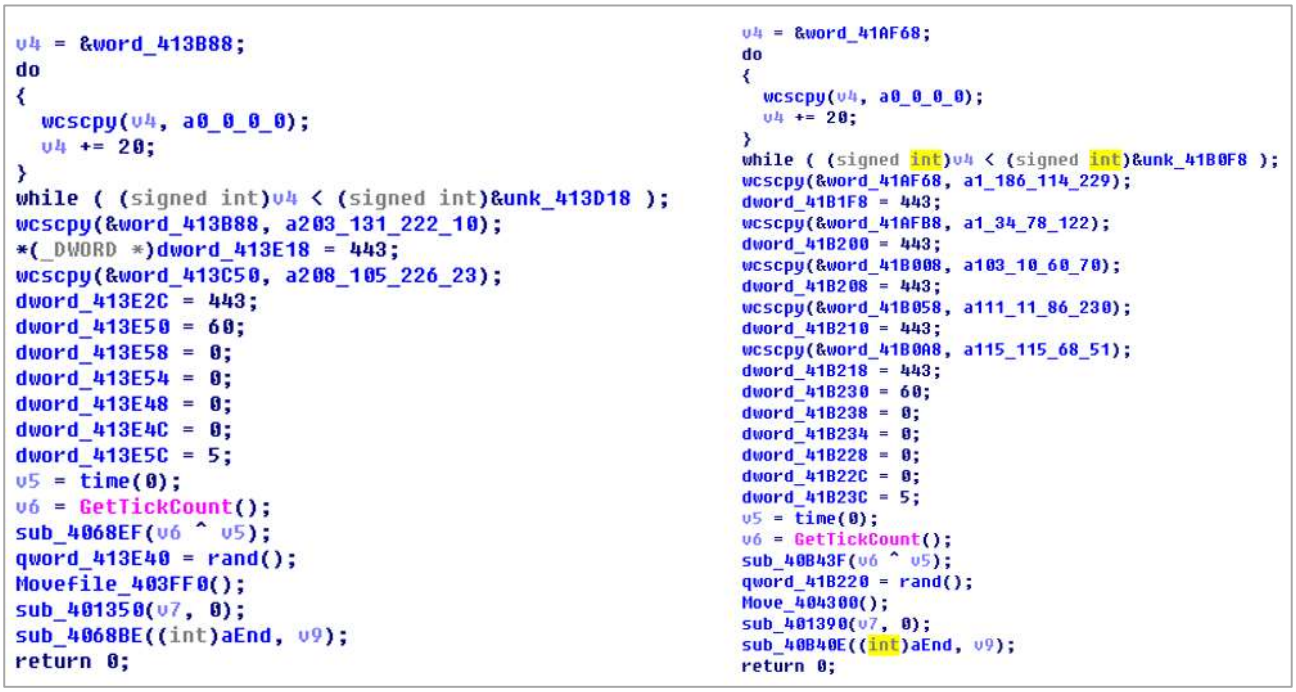
Escad 악성코드는 다수의 변형이 존재하며 2014년 미국 영화사 미국 영화사 공격에 사용된 악성코드는 Escad A형과 연관된 것으로 보인다. 2013년에도 문자열 처리에 비슷한 코드를 사용하는 악성코드가 발견되었지만 연관 가능성이 있는지 판단하기는 힘들다.

2014년 5월에 발견된 초기 버전은 2014년 11월 미국 영화사 공격에 사용된 파일과 동일한 방식으로 API를 구한다. 차이점은 초기 버전의 파일은 상위 드롭퍼에 의해 서비스로 등록되어 동작한다는 점이다.



[그림 12] 2014년 5월 발견된 초기 버전

미국 영화사 공격에 사용된 악성코드와 유사한 형태의 변형은 2014년 7월 이후부터 발견된다.

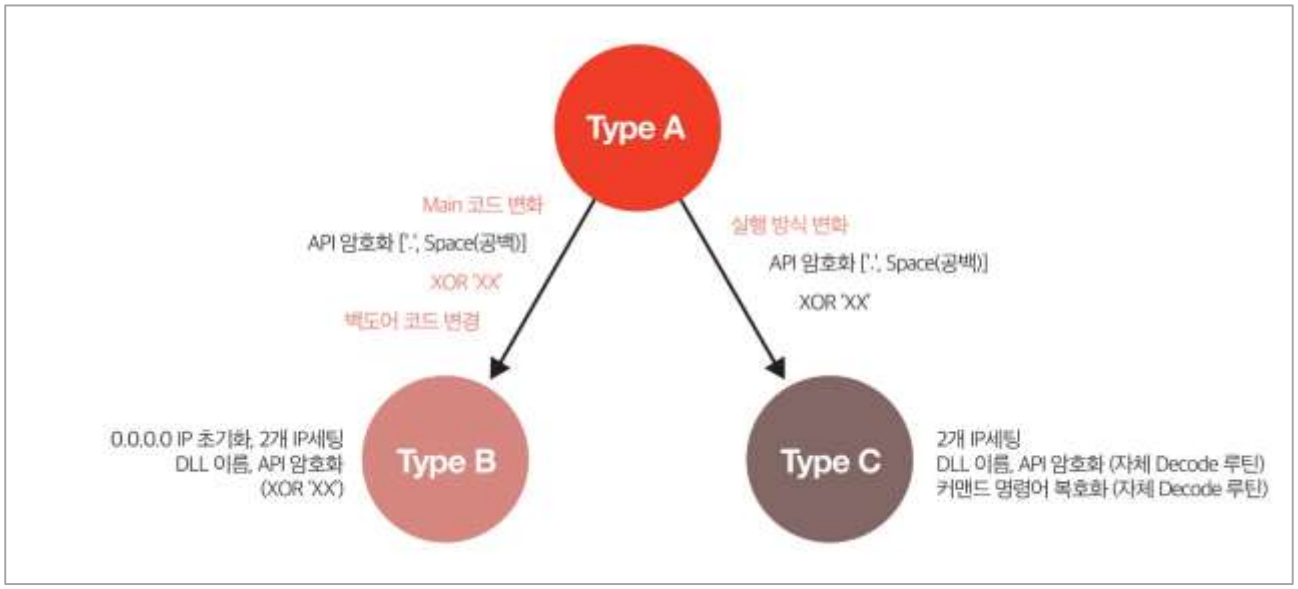


[그림 13] 국내 발견 변형과 미국 영화사 공격 샘플 비교

앞서 언급된 바와 같이 Escad 악성코드 변형은 크게 A형, B형, C형으로 나뉜다. 최초 기준이 된 A형의 주요 특징은 메인 코드에서 2개의 IP를 설정하는 것, 'XOR 0xA7'을 이용하여 DLL 파일의 이름을 구하는 것, 그리고 사용할 API의 실제 사용을 위해서는 모두 ' '(space)와 '.'(dot)을 제거해야 한다는 점 등이 있다. 그 후 백도어 명령을 받을 때는 자체 디코드 루틴을 사용하였다.

B형은 메인 코드에서 2개의 IP를 설정하는 것은 동일하나 코드 형태가 변화하였다. DLL 파일의 이름과 사용할 API를 구할 때 ' '(space)와 '.'(dot)을 제거하는 것이 아닌 XOR 연산을 통해 구하는 것으로 변경되었다. C형은 서비스로 동작하며 A형, B형과 마찬가지로 2개의 IP가 설정된다. DLL 파일의 이름과 사용할 API, 백도어 명령어까지 자체 디코드 루틴을 사용하여 구한다. 백도어 코드는 A형과 동일하다.

2016년 발견된 변형은 파일 길이가 50 메가바이트(MB)가 넘는 경우도 있다. 또한 암호화된 파일이나 리소스 영역의 메모리에서만 동작하는 새로운 형태의 백도어도 발견되었다.



[그림 14] Escad 악성코드 변형 관계도

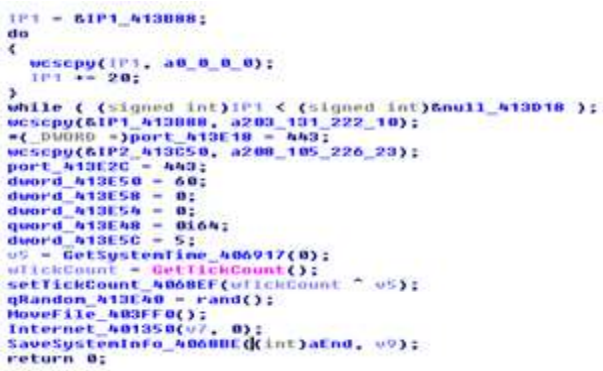
[그림 14]의 관계도에서 붉은색 글씨는 변경된 부분을 의미하고, 회색 글씨는 사라진 방식을 의미한다.

```
*(_DWORD *)(a4 + 4 * *a2) = *a3 * *(_DWORD *)(a4 + 4 * *a2) + 1;
v4 = *(_DWORD *)(a4 + 4 * *a2);
v5 = ((v4 >> 0x10) & 0x7FFF) + *a1;
LOBYTE(v4) = ((v4 >> 0x10) + *(_BYTE *)a1) & 0xF;
v6 = v5 >> (0x10 - v4);
result = v5 << v4;
*a1 = result | v6;
return result;
}
```

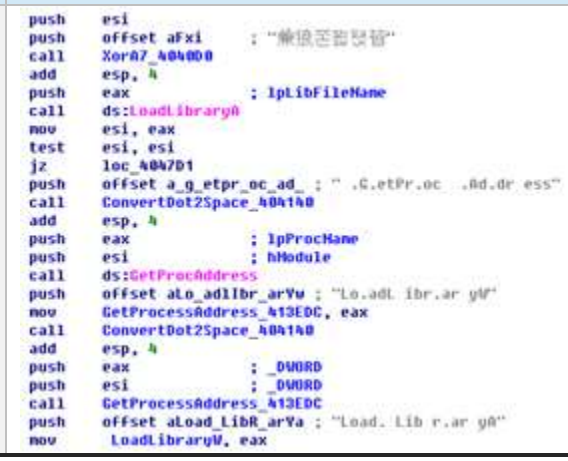
[그림 15] 자체 디코드 루틴

Type	악성코드	API 구하는 방법
A형	미국 영화사 공격	API 주소에 .이 존재
B형	한글 취약점을 통해 유포	API 주소에서 .가 사라지고 XORING으로 변경 (XOR 키는 변형 마다 다름)
C형	국내 정치권 공격	자체 Decode 루틴 사용

[표 6] 변형 해시 및 API 특징

A형 메인 코드	B형 메인 코드
	

[표 7] A형과 B형의 메인 코드 비교

Type	API 구하는 코드
A형	

B형

```
do
{
  LibFileName[v0] ^= 0x89u;
  ++v0;
}
while ( v0 < 0x110 );
v1 = LoadLibraryA(LibFileName);
v2 = v1;
if ( !v1 )
  return 245;
dword_4318BC = (int)GetProcAddress(v1, &ProcName[2]);
if ( !dword_4318BC )
  return 245;
dword_4318B0 = (int)GetProcAddress(v2, &v19[2]);
if ( !dword_4318B0 )
  return 245;
v4 = LoadLibraryA(&v18[3]);
v5 = v4;
if ( !v4 )
  return 245;
dword_4318B4 = (int (__stdcall *)(_DWORD))GetProcAddress(v4, &v23[2]);
if ( !dword_4318B4 )
  return 245;
dword_4318CC = (int)GetProcAddress(v5, &v27[3]);
```

C형

```
Kernel32.dll = (const CHAR *)DecRoutine_10005070((const char *)&unk_10018278);
result = LoadLibraryA(Kernel32.dll);
v2 = result;
if ( result )
{
  v3 = (const CHAR *)DecRoutine_10005070((const char *)&unk_10018D18);
  GetProcAddress_1001FCF4 = (int (__stdcall *)(_DWORD, _DWORD))GetProcAddress(v2, v3);
  v4 = (const CHAR *)DecRoutine_10005070((const char *)&unk_10018D08);
  LoadLibraryW_1001FCEC = (int (__stdcall *)(_DWORD))GetProcAddress(v2, v4);
  v5 = DecRoutine_10005070((const char *)&unk_10018CF8);
  LoadLibraryA_1001FCF0 = GetProcAddress_1001FCF4(v2, v5);
  v6 = DecRoutine_10005070((const char *)&unk_10018CE8);
  FreeLibrary_1001FCF8 = (int (__stdcall *)(_DWORD))GetProcAddress_1001FCF4(v2, v6);
```

[표 8] 변형별 API 구하는 코드

Escad 악성코드 변형이 감염 시스템에서 사용한 파일 이름은 다음과 같다. 공격 대상이 해당 파일을 실행할 수 있도록 주소록, 송금증, 초대장 등의 문서 파일로 파일 이름을 위장하고 있다.

파일 이름
adobe.exe
AdobeArm.exe
AdobeARM.exe
adobearm.exe
AdobeFlash.exe
msdtc.exe
msnconf.exe

[표 9] Escad 변형 파일 이름

Escad 변형에서 확인된 주요 C&C 서버 주소는 다음과 같다.

203.113.122.164:443	122.224.214.108:443	66.45.231.125:443
196.202.33.106:8443	183.82.97.201:443	87.197.125.51:110

[표 20] Escad 변형 주요 C&C 서버 주소

오퍼레이션 고스트 라이플(Operation Ghost Rifle)

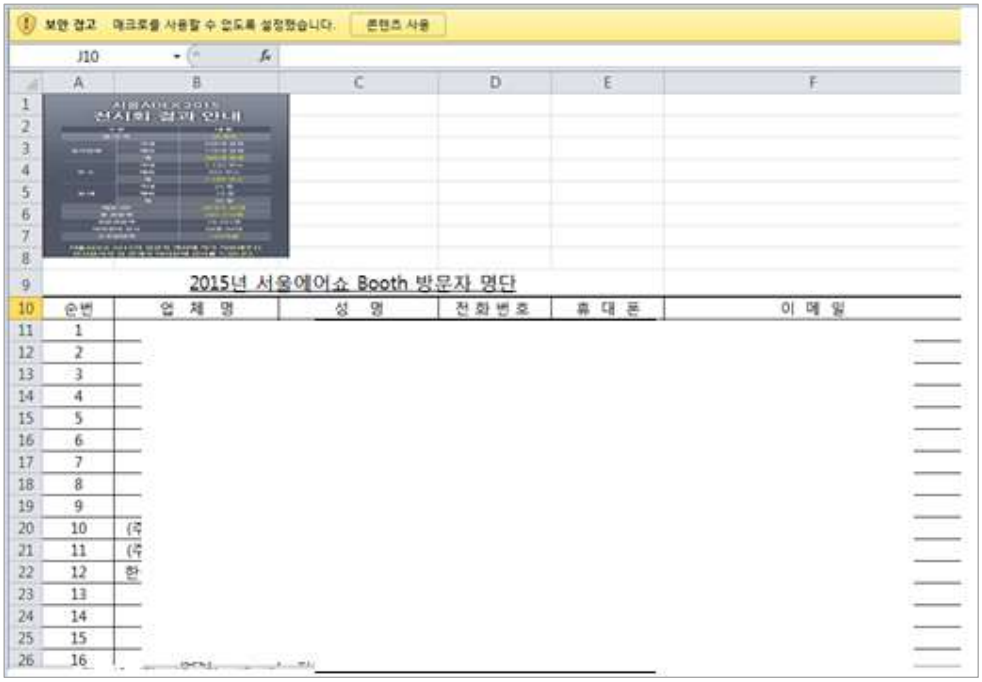
오퍼레이션 고스트 라이플을 진행한 공격 그룹은 주로 방위산업체를 노렸다. 해당 그룹은 2016년 초 국내 보안 업체, 2016년 6월 대기업 전산망 해킹 등에도 연관된 것으로 알려져 있다. 방위산업체에 대한 공격은 지속적으로 발생하고 있으며 특히 국내 업체에는 국내 환경에 맞춘 공격이 이뤄졌다.

2015년 가을, 서울 국제 항공우주 및 방위산업 전시회(Seoul International Aerospace & Defence Exibition, ADEX) 참가 업체에 대한 공격이 있었다. ADEX는 1996년부터 격년으로 열리는 국제 방위산업 전시회다.

공격자는 주최측으로 위장하여 취약점이 포함된 한글 파일이나 악성 매크로를 포함한 엑셀, 워드 문서를 메일에 첨부하는 공격 방식을 사용했다.

[그림 15] ADEX 참가 업체 공격 메일

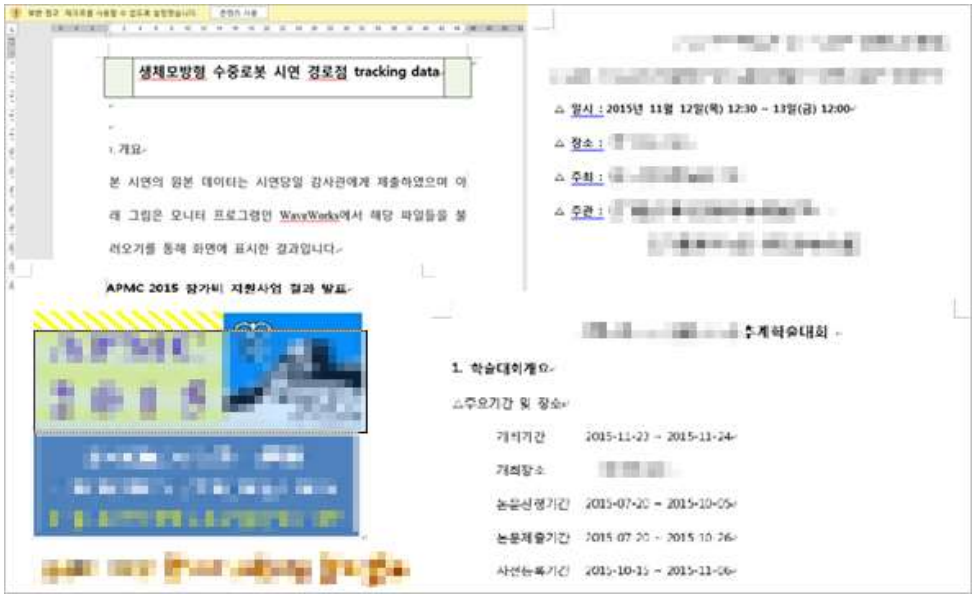
메일에 첨부된 문서는 행사 관련 내용이며 첨부 파일 실행 시 사용자가 '콘텐츠 사용'을 선택하면 악성코드를 다운로드한다.



[그림 16] ADEX 참가 관련 문서 내용

2015년 ADEX 참관 업체에 대한 공격에 최소 2개 이상의 공격 그룹이 참여했으며 한글 프로그램 취약점 파일의 경우 Escad 악성코드 변형도 포함되어 있었다. 워드나 엑셀 파일의 경우에는 사용자가 매크로를 실행하면 Rifdoor 악성코드 변형에 감염된다.

이후에 발견된 문서 파일의 내용을 확인한 결과, 이 공격자는 주로 방위산업체에 대한 공격을 지속적으로 수행한 것으로 추정된다.



[그림 17] 국내 방위산업체 공격에 사용된 문서 내용

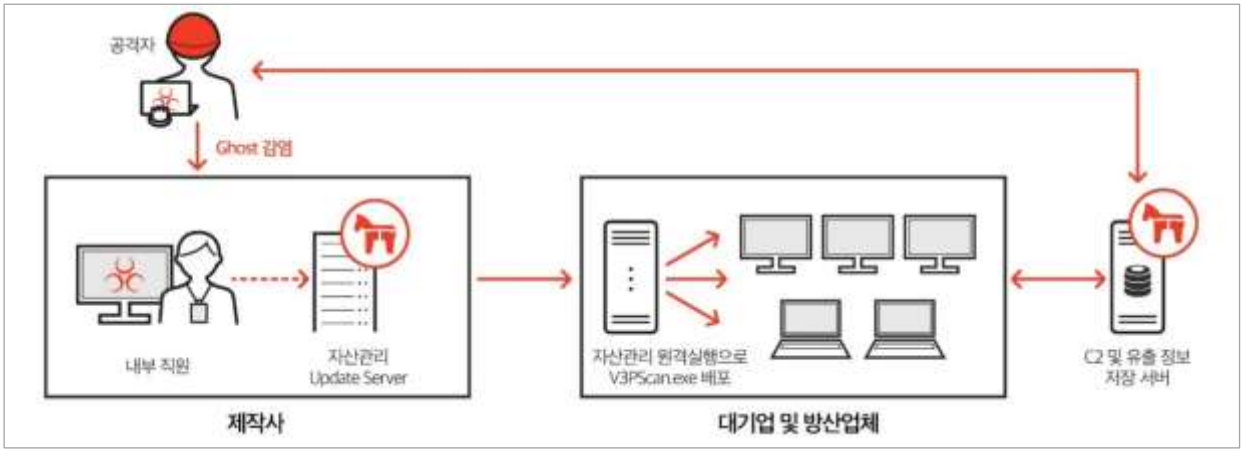
또한 동일 공격 그룹이 국내 보안 업체의 DRM 프로그램으로 위장한 악성코드를 배포한 정황도 포착되었다.

2016년 1월 국내 보안 업체 공격에 사용된 변형은 주요 문자열이 암호화되어 있다.

```
.0040F240:  58 4E 5D 4A.53 42 66 6C.7D 60 7C 60.69 7B 53 58  XN]JSBfl}`|`i{SX
.0040F250:  66 61 6B 60.78 7C 2F 41.5B 53 4C 7A.7D 7D 6A 61  fak`x|/A[SLz}}ja
.0040F260:  7B 59 6A 7D.7C 66 60 61.53 00 00 00.5F 7D 60 6B  {Yj}|f`aS   _}`k
.0040F270:  7A 6C 7B 41.6E 62 6A 00.4C 5C 4B 59.6A 7D 7C 66  zl{Anbj L\KYj}|f
.0040F280:  60 61 00 00.20 2F 20 00.25 64 2E 25.64 00 00 00  `a   /  %d.%d
.0040F290:  25 32 2E 32.58 00 00 00.25 73 00 00.25 73 2F 25  %2.2X   %s  %s/%
.0040F2A0:  73 00 00 00.73 65 63 2E.65 78 65 00.4C 35 53 78  s   sec.exe L5Sx
.0040F2B0:  66 61 6B 60.78 7C 53 7C.76 7C 7B 6A.62 3C 3D 53  fak`x|S|v|{jb<=S
.0040F2C0:  6C 62 6B 21.6A 77 6A 00.25 73 20 2F.63 20 25 73  lbk!jwj %s /c %s
.0040F2D0:  00 00 00 00.5F 5D 40 4C.4A 5C 5C 4A.4B 2F 4E 5B      _]@LJ\\JK/N[
.0040F2E0:  00 00 00 00.0D 0A 43 4D.44 3A 25 73.20 25 73 20      ♪◙CMD:%s %s
.0040F2F0:  25 64 2F 25.64 2F 25 64.20 25 64 3A.25 64 3A 25  %d/%d/%d %d:%d:%
.0040F300:  64 0D 0A 00.2B 66 61 7B.6A 7D 79 6E.63 00 00 00  d♪◙ +fa{j}ync
.0040F310:  46 61 7B 6A.7D 79 6E 63.2F 66 7C 2F.7C 6A 7B 2F  Fa{j}ync/f|/|j{/
.0040F320:  7B 60 00 00.25 73 20 25.64 20 6D 69.6E 0D 0A 00  {`  %s %d min♪◙
.0040F330:  2B 6B 60 78.61 63 60 6E.6B 6A 77 6A.6C 00 00 00  +k`xac`nkjwjl
.0040F340:  4B 60 78 61.63 60 6E 6B.2F 69 6E 66.63 7A 7D 6A  K`xac`nk/infcz}j
.0040F350:  00 00 00 00.0D 0A 00 00.4B 60 78 61.63 60 6E 6B      ♪◙  K`xac`nk
.0040F360:  2F 7C 7A 6C.6C 6A 7C 7C.00 00 00 00.4A 77 6A 6C  /|zllj||    Jwjl
.0040F370:  7A 7B 66 60.61 2F 69 6E.66 63 7A 7D.6A 00 00 00  z{f`a/infcz}j
.0040F380:  4A 77 6A 6C.7A 7B 66 60.61 2F 7C 7A.6C 6C 6A 7C  Jwjlz{f`a/|zllj|
```

[그림 18] 0x0F 로 암호화된 문자열

2016년 6월에는 자산관리 솔루션을 이용한 방위산업체 관련 대기업 해킹 사건이 경찰청에 접수되었다.[7] 자산관리 솔루션의 취약점을 이용한 것으로 파일 배포 기능을 통해 악성코드를 배포하여 대기업 해킹을 시도한 사건이다. 해당 공격으로 인해 설치된 고스트랫(GhostRat) 악성코드로 약 4만여 건의 문서가 유출된 것으로 확인되었다.



[그림 19] 중앙 관리 시스템 취약점을 이용한 악성코드 관계도

[7] http://www.yonhapnews.co.kr/northkorea/2016/06/13/1801000000AKR20160613092851004.HTML

사건 개요를 정리하면 다음과 같다. 특히 사건이 발생하기 4년 전인 2012년, 자산관리 프로그램 취약점 테스트 정황이 확인되고 2014년 7월부터 해킹을 시도한 것으로 보아 공격자는 해당 대기업에 대한 공격을 장기간 준비했음을 예상할 수 있다.

2012년 7월	자산관리 프로그램 취약점 테스트 정황
2014년 7월	자산관리 프로그램 취약점 이용한 대기업 해킹 시도 시작
2015년 3월	자산관리 프로그램을 통해 백도어 프로그램을 담은 V3PScan.exe 배포
2015년 11월	모 보안 프로그램 가장 악성코드 배포
2016년 2월	경찰청 사이버안전국 관련 첩보 입수해 수사
2016년 3월	자산관리 프로그램 보안 패치 발표
2016년 4월	관련 정보 관계사, 관련 당국에 공유

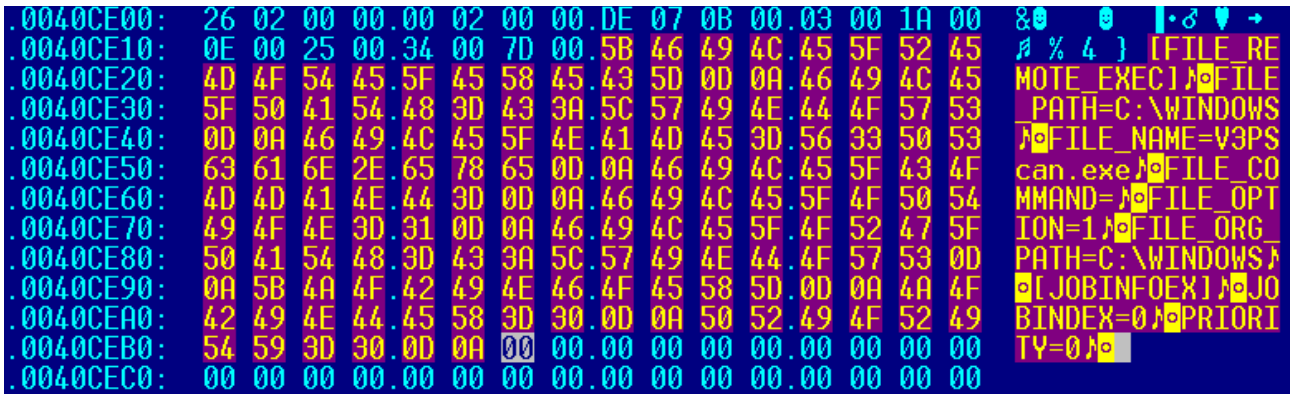
[표 11] 대기업 해킹 사건 타임라인

2012년 7월 취약점 테스트로 추정되는 코드에서 발견된 PDB 정보는 다음과 같다.

c:₩new folder₩connecttest₩release₩ConnectTest.pdb

[표 32] 취약점 테스트 추정 코드에서 발견된 PDB 정보

2015년 3월 자산관리 프로그램을 통해 실행 파일인 V3PScan.exe를 배포할 때 사용한 코드의 내용은 다음과 같다.



[그림 20] 자산관리 프로그램을 이용한 실행 파일 배포

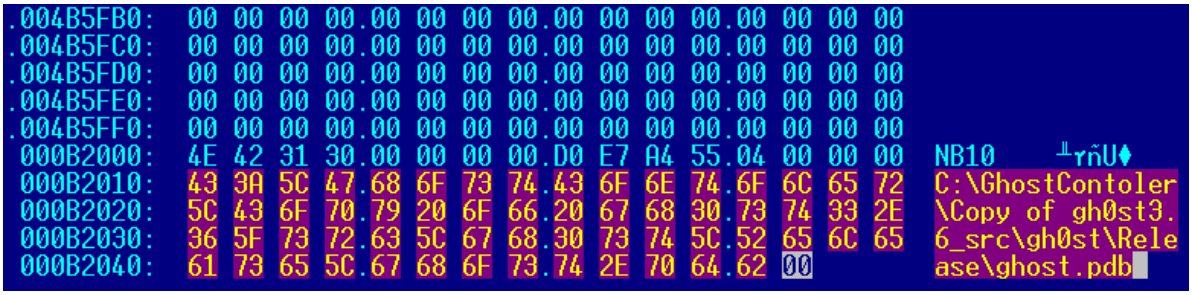
Rifdoor 악성코드 변형에 따른 PDB 정보는 다음과 같다.

PDB 정보
C:₩Users₩C8₩Desktop₩rifle₩Release₩rifle.pdb
E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩rifle₩Release₩rifle.pdb

[표 4] Rifdoor 악성코드 변형에 따른 PDB 정보

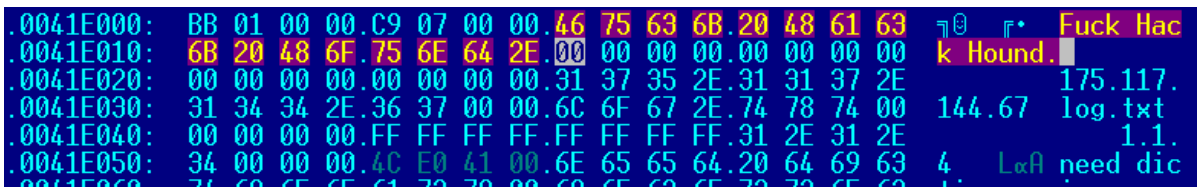
■ 추가 악성코드

오퍼레이션 고스트 라이플을 수행한 해당 공격 그룹은 자체 제작한 Rifdoor 악성코드 이외에도 Ghostrat, Aryan 등 이미 알려진 다른 악성코드도 이용하고 있다.



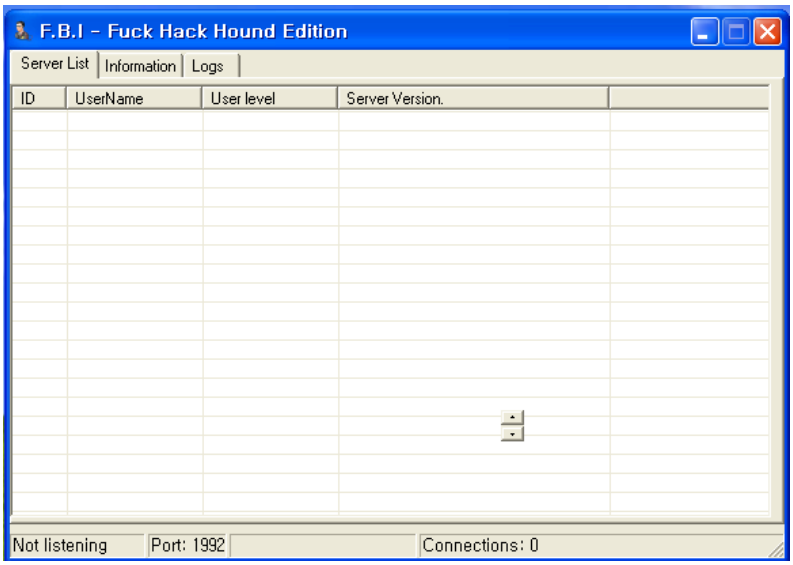
[그림 21] 추가 악성코드

Aryan 악성코드는 'Fuck Hack Hound.'와 같은 특징적 문자열을 포함하고 있다.



[그림 22] 특징적 문자열

Aryan 악성코드 해킹 툴 관리 프로그램도 존재한다.



[그림 23] 해킹 툴 관리 프로그램

또한 해당 그룹은 Crash.exe, Test.exe라는 이름으로 매년 8월 이후 PC의 하드 디스크 내용을 파괴하도록 설계된 악성코드를 제작했다. 하지만, 실제 공격에 사용되었는지는 확인할 수 없다.

오퍼레이션 어나니머스 팬텀(Operation Anonymous Phantom)

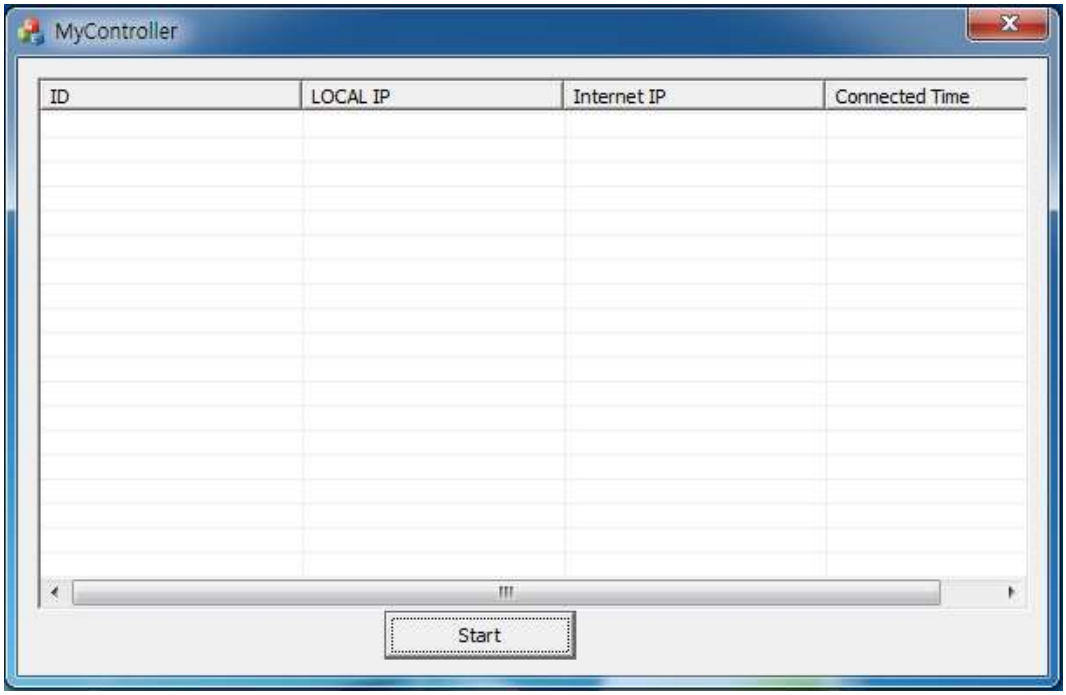
2016년 1월부터 10월까지 유사 악성코드를 이용한 국내 방위산업체에 대한 공격이 확인되었다. 초기 공격에 사용된 파일 이름은 Phantom.exe 이며, 악성코드 진단명은 'Phandoor'이다. 또한 통신을 할 때 익명을 의미하는 'Anonymous' 문자열을 사용하는 것이 확인되었다. 안랩은 공격에 사용된 파일 이름과 통신 시 사용하는 문자열을 토대로 해당 공격을 '어나니머스 팬텀(Operation Anonymous Phantom)'으로 명명했다.

해당 악성코드는 2016년 1월 최초 발견되었지만 2015년 10월 처음 제작된 것으로 추정된다. 국내 방위산업체 몇 곳이 공격 대상으로 확인된 것으로 미뤄보아 방위산업체를 노린 공격으로 추정된다. 정확한 공격 방식은 확인되지 않았다. 현재까지 총 37개의 변형이 발견되었으며 파일의 크기는 76,800 바이트에서 95,232 바이트 사이다. Phantom.exe 외 F_lps.exe, ahnV3.exe, 12teimong12.exe, Tiemong.exe, v3scan.exe, otuser.exe, v3log.exe 등의 파일 이름으로도 발견되었다.

최근에는 2017년 4월 더미다(Themida) 패커로 패킹된 변형이 국내 에너지 관련 연구소에서 발견되었으며 2017년 5월에는 특징적인 Anonymous 문자열이 제거된 변형도 발견되는 등 현재까지 꾸준히 활동 중이다.

■ 추가 악성코드

어나니머스 팬텀 공격 그룹에서 사용한 Phandoor 컨트롤 프로그램 화면은 다음과 같다.



[그림 24] Phandoor 컨트롤 프로그램

중계 서버 역할을 하는 것으로 보이는 Transponder.exe도 발견되었으며, 변형에 따라 443번, 6000번, 10666번 포트를 LISTENING 상태로 열어둔다.

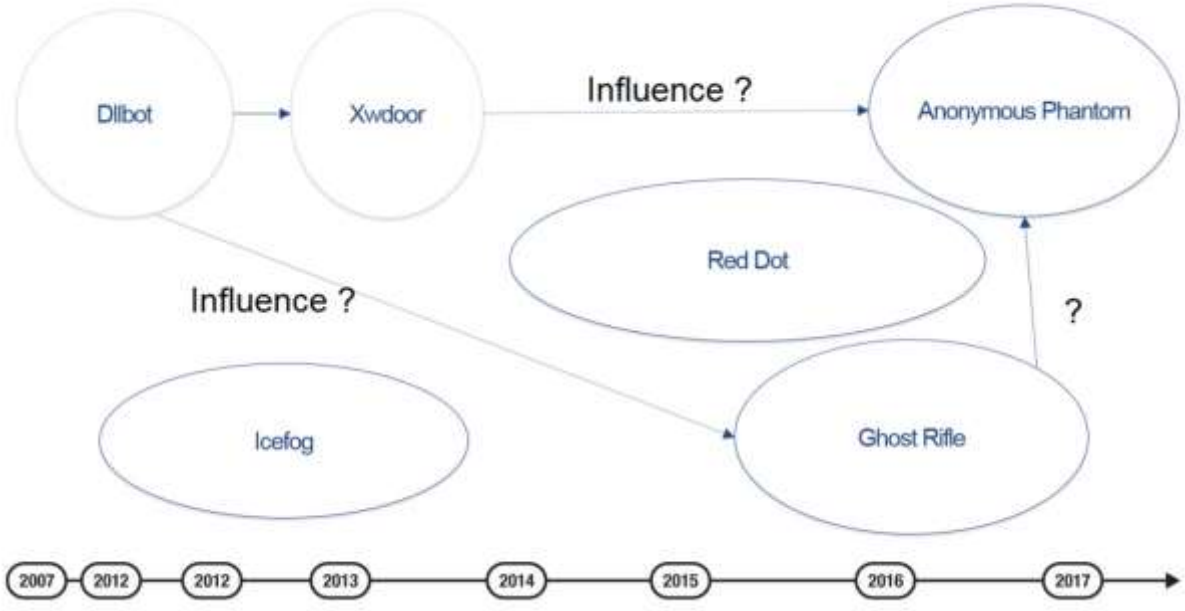
국내 공격 사례의 특징

국내 방위산업체에 대한 공격은 여러 그룹에 의해 이뤄졌다. 국내 방위산업체를 공격 대상으로 한 레드닷(Red Dot) 그룹, 고스트 라이플(Ghost Rifle) 그룹, 어나니머스 팬텀(Anonymous Phantom) 그룹에서 사용한 코드와 암호화 방식의 유사성으로 미루어볼 때 이들 그룹이 동일 그룹 혹은 협력 그룹일 가능성이 있다. 한편 국내 공격에 사용된 악성코드를 추적해보면 다른 악성코드도 연관되어 발견되고 있다.

공격 그룹 연관성

국내 방위산업체에 대한 공격을 시도한 그룹은 다수 존재한다. 2013년 알려진 아이스포그(Icefog) 그룹은 중국 그룹으로 추정되고 있다. 2014년 국내 방위산업체를 공격한 레드닷(Red Dot) 그룹은 2014년 미국 영화사를 공격한 그룹과 동일 그룹으로 보인다. 레드닷(Red Dot) 그룹과 함께 2015년 ADEX 참가 업체 공격을 시작으로 국내 방위산업체를 공격한 고스트 라이플(Ghost Rifle) 그룹은 2016년 국내 대기업 해킹으로 유명해졌다. 어나니머스 팬텀(Anonymous Phantom) 그룹은 2016년 초부터 활동을 시작하는데 기존 악성코드와 코드에서 유사점이 있다.

Dllbot은 2007년부터 국내 군 관련 해킹에 이용된 악성코드다. Dllbot은 여러 변형이 발견되는데 2012년에 발견된 변형에서는 문자열에서 S^를 제거하는 코드를 포함하는 특징이 발견되었다. 같은 해 Dllbot의 변형인 Xwdoor에서도 동일 코드가 발견되었다. 2015년 발견된 Phandoor는 Dllbot와 Xwdoor와는 전반적인 코드는 다르지만 S^를 처리하는 코드는 유사하다.



[그림 25] 공격 그룹 관계도

Phandoor 변형에서 발견된 문자열 앞에 붙어 있는 'S^'의 경우 2012년에 발견된 국내 표적 공격 악성코드에서도 발견되었다.

```
.10015650:  73 65 72 00.53 5E 4C 61.6E 67 75 61.67 65 00 00  ser S^Language
.10015660:  53 5E 53 74.75 62 49 6E.66 6F 00 00.0D 0A 00 00  S^StubInfo  ♪◙
.10015670:  FF FF FF FF.5E 25 00 10.64 25 00 10.00 00 00 00      ^% ►d% ►
.10015680:  FF FF FF FF.E0 25 00 10.21 26 00 10.25 73 00 00      α% ►!& ►%s
.10015690:  53 5E 4F 4C.4C 59 44 42.47 00 00 00.53 5E 50 61  S^OLLYDBG   S^Pa
.100156A0:  74 68 46 69.6C 65 45 78.69 73 74 73.41 00 00 00  thFileExistsA
.100156B0:  53 5E 73 68.6C 77 61 70.69 2E 64 6C.6C 00 00 00  S^shlwapi.dll
.100156C0:  53 5E 49 6E.74 65 72 6E.65 74 47 65.74 43 6F 6E  S^InternetGetCon
.100156D0:  6E 65 63 74.65 64 53 74.61 74 65 00.53 5E 44 65  nectedState S^De
.100156E0:  6C 65 74 65.55 72 6C 43.61 63 68 65.45 6E 74 72  leteUrlCacheEntr
.100156F0:  79 00 00 00.53 5E 48 74.74 70 45 6E.64 52 65 71  y   S^HttpEndReq
.10015700:  75 65 73 74.41 00 00 00.53 5E 49 6E.74 65 72 6E  uestA   S^Intern
.10015710:  65 74 57 72.69 74 65 46.69 6C 65 00.53 5E 48 74  etWriteFile S^Ht
.10015720:  74 70 53 65.6E 64 52 65.71 75 65 73.74 45 78 41  tpSendRequestExA
.10015730:  00 00 00 00.53 5E 48 74.74 70 41 64.64 52 65 71      S^HttpAddReq
.10015740:  75 65 73 74.48 65 61 64.65 72 73 41.00 00 00 00  uestHeadersA
.10015750:  53 5E 48 74.74 70 51 75.65 72 79 49.6E 66 6F 41  S^HttpQueryInfoA
.10015760:  00 00 00 00.53 5E 48 74.74 70 53 65.6E 64 52 65      S^HttpSendRe
```

[그림 26] 2012년 발견된 S^를 포함한 악성코드 Dllbot

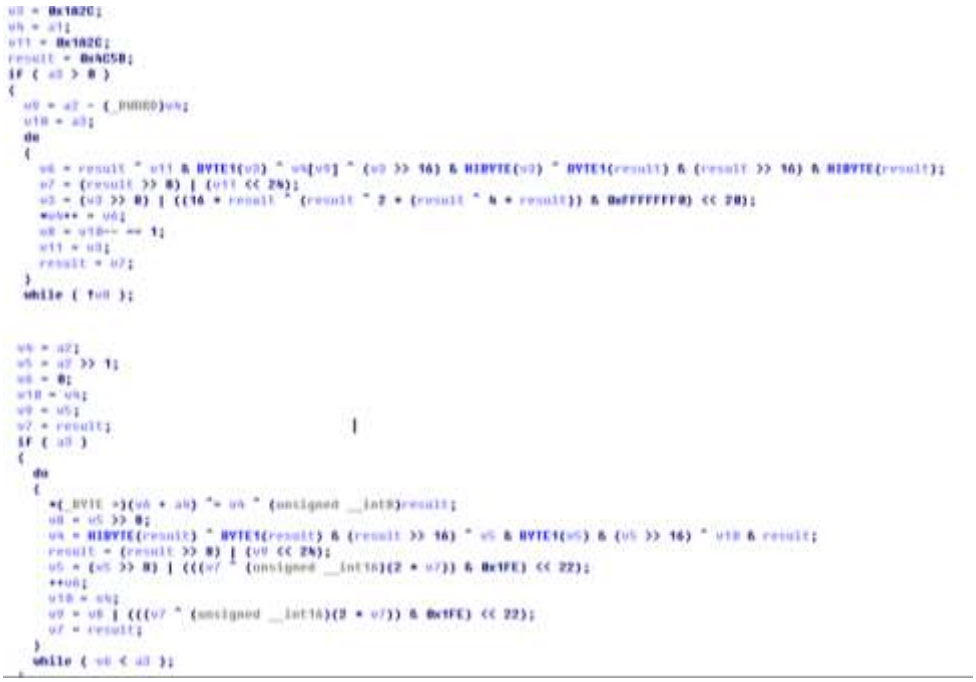
주요 문자열 앞에 붙은 S^ 뿐 아니라 문자열에서 S^를 제거하는 코드 또한 유사하다. 즉, 동일 공격자나 관련 소스코드를 이용해서 악성코드를 만들고 있는 것으로 추정된다.

```
v1 = this;
v9 = 0;
v10 = 0;
sprintf(&v9, "%s", "K^A");
memset(byte_4460D8, 0, 2999u);
if ( *v1 != 'S' || v1[1] != '^' )
{
  v4 = *(_WORD *)v1;
  if ( *(_WORD *)v1 > 2999u )
    v4 = 2999;
  if ( v4 > 0u )
  {
    v5 = v1 + 2;
    v6 = v4;
    v7 = BYTE1(v10);
    v8 = byte_4460D8;
    do
    {
      *v8++ = v7 ^ *v5++;
      --v6;
    }
    while ( v6 );
  }
  result = byte_4460D8;
}
else
```

```
v1 = this;
WaitForSingleObject(hMutex, 0xFFFFFFFF);
v9 = 0;
v10 = 0;
sprintf(&v9, "%s", &unk_10034C68);
memset(byte_1003AC98, 0, 2999u);
if ( *v1 != 'S' || v1[1] != '^' )
{
  v3 = *(_WORD *)v1;
  if ( *(_WORD *)v1 > 2999u )
    v3 = 2999;
  if ( v3 > 0u )
  {
    v4 = v1 + 2;
    v5 = v3;
    v6 = BYTE1(v10);
    v7 = byte_1003AC98;
    do
    {
      *v7++ = v6 ^ *v4++;
      --v5;
    }
    while ( v5 );
  }
}
else
{
```

[그림 27] S^를 처리하는 유사 변환 코드

Phandoor와 Rifdoor 악성코드는 유사한 암호화 방식을 사용하고 있다.



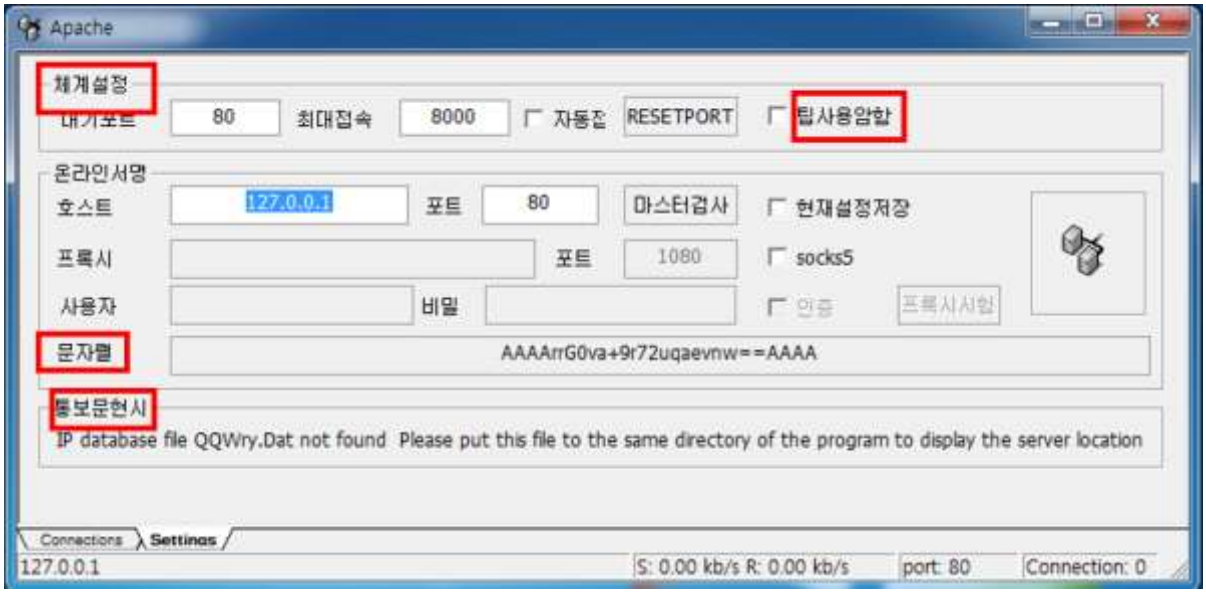
[그림 28] Rifdoor와 Phandoor의 암호화 코드

결론적으로 국내 방위산업체를 공격 대상으로 한 레드닷(Red Dot) 그룹, 고스트 라이플(Ghost Rifle) 그룹, 어나니머스 팬텀(Anonymous Phantom) 그룹의 연관성은 명백하지 않지만, 코드와 암호화 방식의 유사성으로 미루어볼 때 이들 그룹이 동일 그룹 혹은 협력 그룹일 가능성이 있다.

한국어 사용자 가능성

일부 그룹에서 공격에 사용한 프로그램 중에는 한국어로 된 프로그램도 확인되어 국내 공격자가 한국인일 가능성도 있다.

고스트 라이플 그룹에서 사용한 악성코드 제어 프로그램은 '체계설정', '문자렬', '통보문현시' 등과 같은 어색한 한글이 사용되고 있는 것이 확인됐다.

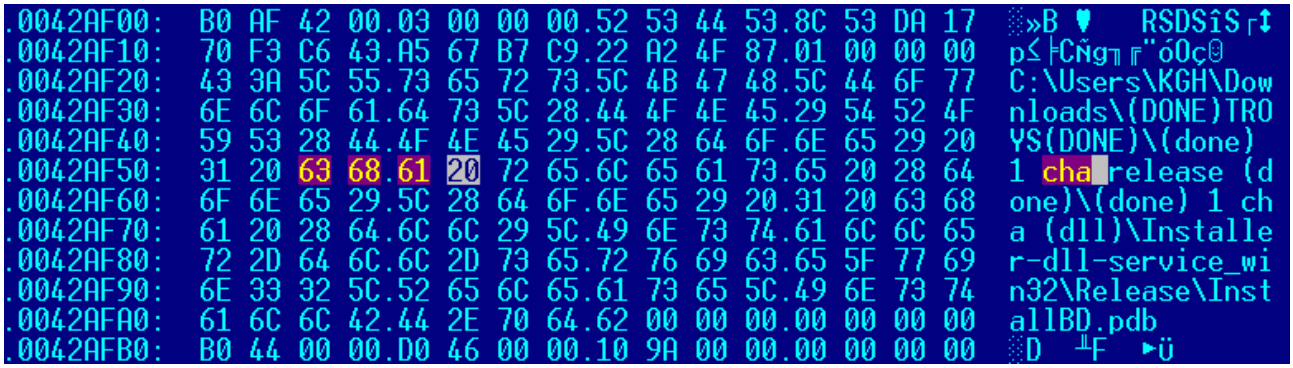


[그림 30] 오퍼레이션 고스트 라이플에서 사용된 제어 프로그램

또한 어나니머스 팬텀 그룹에서 제작한 것으로 보이는 다른 악성코드의 PDB 정보를 보면 사용자 이름에 'KGH'와 같이 한국인으로 추정할 수 있는 이니셜과 횟수를 의미하는 1 차(cha) 문자열을 포함하고 있기도 한다.

C:₩Users₩**KGH**₩Downloads₩(DONE)TROYS(DONE)₩(done) 1 **cha** release (done)₩(done) 1 cha (dll)₩Installer-dll-service_win32₩Release₩InstallBD.pdb

[표 14] PDB 정보



[그림 29] 한국인 제작자로 추정되는 정보

악성코드 상세 분석

2010년부터 2016년까지 방위산업체에 대한 공격에 이용된 주요 악성코드인 Escad, Rifdoor, Phandoor 악성코드에 대한 분석을 살펴본다.

주요 국내 방위산업체 공격에 사용된 악성코드 샘플은 다음과 같다.

	대표 파일명	주요 기능	MDS 진단명	V3 진단명
1	Rifle.exe	원격 제어를 통한 백도어	Trojan/Win32.Rifdoor	Win-Trojan/Rifdoor
2	Phantom.exe	원격 제어를 통한 백도어	Trojan/Win32.Phandoor	Trojan/Win32.Phandoor
3	AdobeArm.exe	원격 제어를 통한 백도어	Backdoor/Win32.Escad	Trojan/Win32.Escad

[표 15] 국내 방위산업체 공격 악성코드

Escad

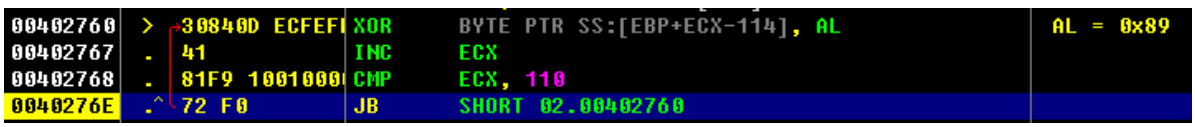
■ 기본 정보

파일 이름	AdobeArm.exe
파일 길이	179,200
파일 생성 시간	2015년 10월 19일 월요일, 오전 10시 49분 58초 (UTC 기준)
주요 기능	사용자 정보 탈취
MDS 진단명	Backdoor/Win32.Escad
V3 진단명	Backdoor/Win32.Escad

[표 56] Escad 기본 정보

■ 동작 방식

'오퍼레이션 레드닷'에서 사용된 Escad 악성코드의 특징은 API를 암호화 해둔 방식이다. 해당 파일은 사용할 DLL이름과 API 이름을 0x89로 XOR하여 가져온다.



[그림 32] XOR 89 코드


```
0012E50C 55 53 45 72 33 32 2E 64 6C 6C 00 00 00 00 49 73 USEr32.dll....Is
0012E51C 57 69 6E 64 6F 77 56 69 73 69 62 6C 65 00 47 65 WindowVisible.Ge
0012E52C 74 53 79 73 74 65 6D 4D 65 74 72 69 63 73 00 00 tSystemMetrics..
0012E53C 00 00 00 41 64 76 61 50 69 33 32 2E 64 4C 6C 00 ...AdvaPi32.dLl.
0012E54C 00 00 00 00 00 00 52 65 67 43 6C 6F 73 65 4B 65 ......RegCloseKe
0012E55C 79 00 00 00 00 00 00 4F 70 65 6E 50 72 6F 63 65 y......OpenProce
0012E56C 73 73 54 6F 6B 65 6E 00 00 00 00 00 00 46 72 65 ssToken......Fre
0012E57C 65 53 69 64 00 00 00 00 41 6C 6C 6F 63 61 74 65 eSid....Allocate
0012E58C 41 6E 64 49 6E 69 74 69 61 6C 69 7A 65 53 69 64 AndInitializeSid
0012E59C 00 00 00 00 43 68 65 63 6B 54 6F 6B 65 6E 4D 65 ....CheckTokenMe
0012E5AC 6D 62 65 72 73 68 69 70 00 00 00 00 00 00 00 00 mbership........
0012E5BC 4F 70 65 6E 53 43 4D 61 6E 61 67 65 72 57 00 00 OpenSCManagerW..
0012E5CC 00 00 44 75 70 6C 69 63 61 74 65 54 6F 6B 65 6E ..DuplicateToken
```

[그림 30] 복호화된 문자열

또한 AdobeArm.exe 파일을 시작 프로그램에 바로가기 파일로(*.lnk) 생성하여 시스템이 재부팅되어도 자동으로 다시 실행되게 한다.

```
if ( !SHGetSpecialFolderPathW(0, &pszPath, 7, 0) && !SHGetSpecialFolderPathW(0, &pszPath, 24, 0) )
  v0 = 0;
GetModuleFileNameW(0, &Filename, 0x400u);
v1 = wcsrchr(&Filename, 0x5Cu);
v2 = v1;
v25 = v1;
SHGetSpecialFolderPathW(0, &NewFileName, 40, 0);

qmemcpy(v18, &v33, v17);
if ( v0 == 1 )                                  // C:₩Documents and Settings₩Administrator₩
                                                // 시작 메뉴₩프로그램₩시작프로그램₩실행파일명.exe.lnk
  CreateInstance_404070((int)&NewFileName, v14 + 2, &pszPath);
SetFileAttributesW(&NewFileName, 0x86u);        // HIDDEN|SYSTEM|NORMAL
```

[그림 31] 시작 프로그램 등록

```
00405161  .  6A 10          PUSH    10                                  ┌AddrLen = 10 (16.)
00405163  .  99             CDQ                                         │
00405164  .  F7FE           IDIV    ESI                                 │
00405166  .  893D DC23430(  MOV     DWORD PTR DS:[4323DC], EDI          │
0040516C  .  C1E2 04        SHL     EDX, 4                              │
0040516F  .  81C2 ECFA420(  ADD     EDX, 02.0042FAEC                    │
00405175  .  52             PUSH    EDX                                 pSockAddr
00405176  .  53             PUSH    EBX                                 Socket
00405177  .  FF15 3822420(  CALL    DWORD PTR DS:[<&WS2_32.#4>]         └connect
```

0012B10C	0000011C	|Socket = 11C
0012B110	0042FB1C	|pSockAddr = 02.0042FB1C
0012B114	00000010	₩AddrLen = 10 (16.)

```
0042FAEC 02 00 01 BB CB 71 7A A3 00 00 00 00 00 00 00 00 ?.....qz?.......
0042FAFC 02 00 20 FB C4 CA 21 6A 00 00 00 00 00 00 00 00 ?. 늚?j........
```

[그림 32] C&C 서버 연결

203.113.122.163:443, 196.202.33.106:8443 두 개의 C&C 서버 주소가 있고, 실제로는 203.113.122.163:443으로 연결한다. 연결에 성공하면 컴퓨터 이름, 사용자 계정 이름, 시스템 정보 등을 전송한다. 명령어별 기능은 다음과 같다.

명령어(주소로 대체)	기능
&unk_427070	디스크 용량확인
&unk_4270XX	사용자 정보
&unk_4270A0	프로세스 실행
&unk_4270B8	프로세스 목록
&unk_4270D0	프로세스 종료
&unk_4270E8	파일전송
&unk_42703C	특정 파일 찾기
&unk_427100	%temp% 파일생성
&unk_4271XX	파일생성(다운로드)
&unk_427118	파일 속성
&unk_427130	파일 생성 및 삭제
&unk_427160	소켓 연결
&unk_427190	RECV
&unk_4271A8	파일속성 변경
&unk_4271C0	파일명 변경
&unk_4271XX	배치 파일 생성 및 실행

[표 17] 명령어별 기능

Rifdoor

■ 기본 정보

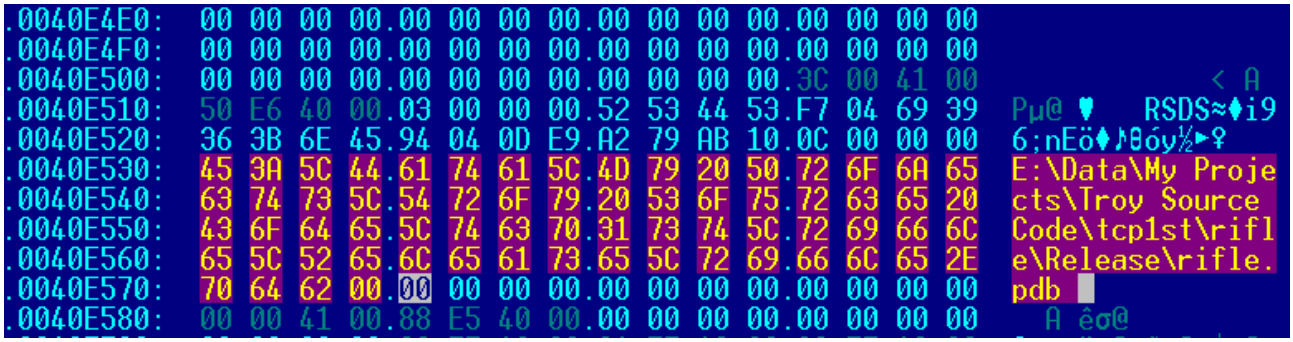
파일 이름	rfile.exe
파일 길이	95,232
파일 생성 시간	2015년 11월 18일 00x시 24분 28초 (UTC 기준)
주요 기능	원격 제어
MDS 진단명	Trojan/Win32.Rifdoor
V3 진단명	Win-Trojan/Rifdoor.Gen

[표 68] Rifdoor 기본 정보

사용자의 의심을 피하기 위해 악성코드 파일은 아이콘은 윈도우 업데이트 관련 이미지로 위장했다.

[그림 33] 악성코드 파일 아이콘

Rifdoor 악성코드의 PDB 정보는 'E:₩Data₩My Projects₩Troy Source Code₩tcp1st₩rifle₩Release₩rifle.pdb'다.



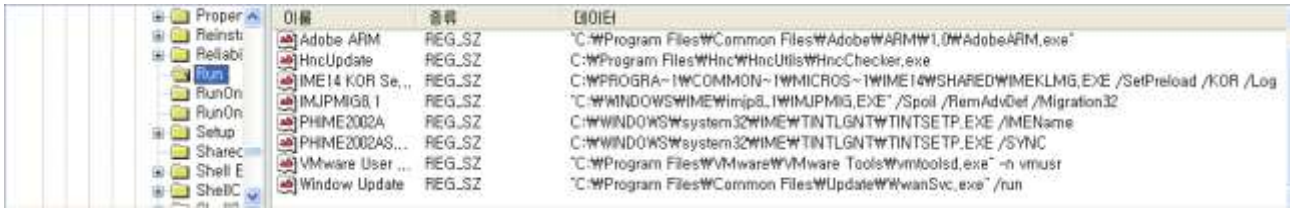
[그림 34] Rifdoor PDB 정보

■ 동작 방식

악성코드가 실행되면 C:₩Program Files₩Common Files₩Update 경로를 생성하고 악성코드를 WwanSvc.exe 로 복사한다. 또한 시스템이 재부팅될 때 자동으로 실행될 수 있도록 레지스트리에 등록한다.

Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run 키 Windows Update

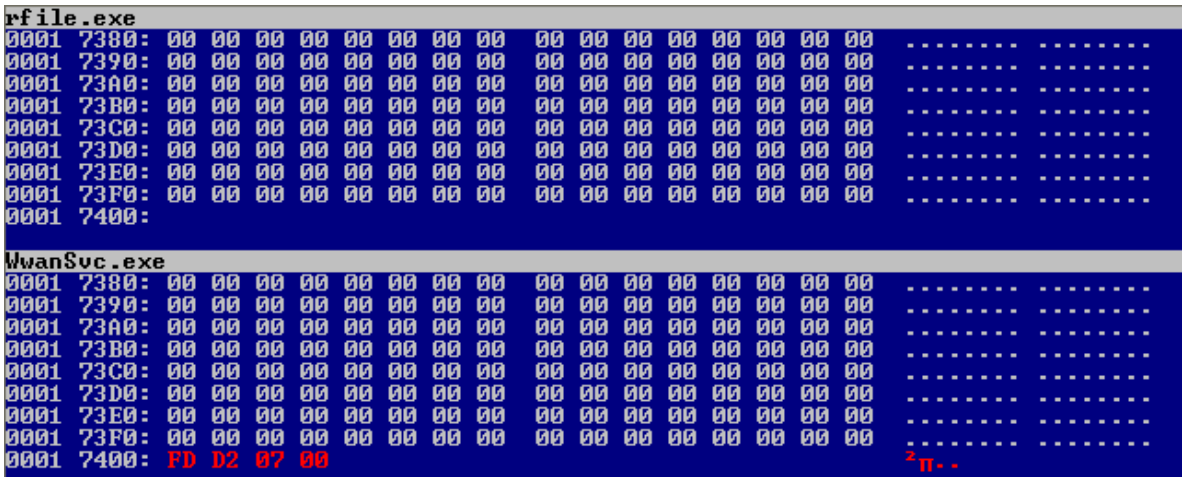
[표 19] 레지스트리 등록 내용



[그림 35] 레지스트리 등록 내용

시스템을 감염시킬 때 해당 악성코드는 파일 끝 4 바이트에 쓰레기 값을 추가하여 파일을 생성한다. 따라

서 감염될 때 마다 해시 값이 달라지기 때문에 단순 해시 값만으로는 시스템에서 악성코드를 찾을 수 없다.



[그림 36] 원본 파일과 생성 파일 비교

또한 'MUTEX394039_4930023' 뮤텍스(Mutex)를 생성하고 C&C 서버로 접속하여 탈취한 사용자 정보를 보낸 다음 통신에 성공하면 명령을 수행한다.

```
if ( !strcmp(*v7, "$interval") )            // $interval
{
  dwMilliseconds = 60000 * atoi(v7[1]);
  sprintf(v22, "Interval is set to %d min₩r₩n", (signed int)dwMilliseconds / 60 / 1000);
  Send_401280(dword_411D10, 0xA021u, s, a4, strlen(v22), (int)v22);
}
else
{
  if ( !strcmp(*v7, "$downloadexec") )      // $downloadexec
  {
    if ( Create_sec_401B80(v7[1], v7[2]) )  // download sec.exe
    {
      strcpy(v22, "Download success₩r₩n");
      if ( CreateProcess_401CD0(v7[2]) )
      {
        v10 = &v21;
        do
          v11 = (v10++)[1];
        while ( v11 );
        *(_DWORD *)v10 = 'cexE';            // Execution success
        *((_DWORD *)v10 + 1) = 'oitu';
        *((_DWORD *)v10 + 2) = 'us n';
        *((_DWORD *)v10 + 3) = 'secc';
        *((_DWORD *)v10 + 4) = '₩n₩rs';
      }
```

[그림 37] 명령어 처리 부분

Rifdoor 악성코드의 주요 명령과 그 기능은 다음과 같다.

명령	기능
$interval	대기
$downloadexec	파일 다운로드 후 실행

$download	파일 다운로드
(기본)	Cmd.exe 실행

[표 20] Rifdoor 명령

Phandoor

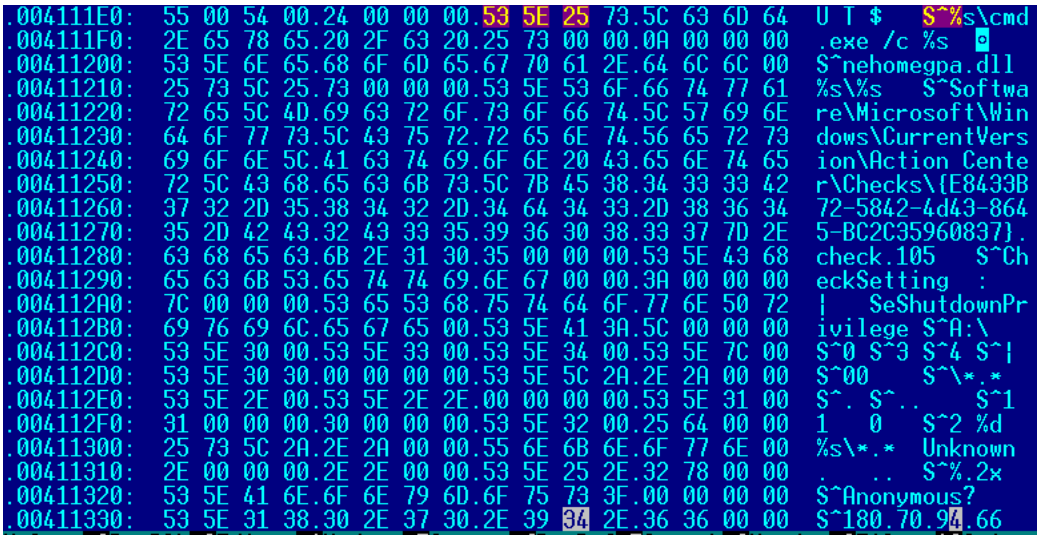
■ 기본 정보

파일 이름	Phantom.exe
파일 길이	86,016 bytes
파일 생성 시간	2015년 10월 22일 23시 59분 03초 (UTC 기준)
주요 기능	원격 제어. 통신 할 때 Anonymous? 문자열을 보냄
MDS 진단명	Trojan/Win32.Phandoor
V3 진단명	Trojan/Win32.Phandoor

[표 21] Phantom 기본 정보

■ 동작 방식

Phandoor 악성코드는 S^%s₩cmd.exe, S^nehomegpa.dll과 같이 특징적으로 주요 문자열 앞에 'S^%'가 붙는다.



[그림 38] Phandoor의 특징적 문자열 S^

악성코드가 실행되면 초기화를 거쳐 C&C 서버에 접속을 시도한다. 이때 'Anonymous?' 검사 코드를 보내 정상 서버 유무를 확인한다.

```
v1 = Convert_403820("S^Anonymous?");
strcpy_s(&Dst, 0x1Bu, v1);
strcat_s(&Dst, 0x1Bu, dword_4450C0);
if ( send_403070(0x1Au, 0, 1, 0, &Dst) == -1 || select_4031A0(fd) == -1 )
  return 0;
v3 = dword_4250A8;
decode_402EF0(dword_4250A0, dword_42509C, dword_4250A8, (int)buf);
if ( !(_BYTE)wCommand_4250A4 && v3 == 10 )
{
  v4 = Convert_403820("S^Anonymous?");
  v5 = buf;
```

[그림 39] Anonymous 검사 코드

또한 명령을 받아 cmd.exe를 실행하거나 추가 명령을 수행한다.

명령	기능
0x9	드라이브 정보
0xA	파일 검색
0xB	인터넷에서 데이터 받아 파일 생성
0x10	일정 시간 후 메인 기능 재실행
0x12	nehomegpa.dll 파일 옮김
0x19	프로세스 리스트 얻기
0x1A	프로세스 종료
0x1B	권한 상승

[표22] 주요 명령

악성코드 실행 과정 내용을 출력하는 제작 중인 버전도 발견되었다. .

안랩 대응 및 보안 권고

안랩 제품군에서는 국내 방위산업체 공격에 사용된 Escad, Rifdoor, Phandoor 악성코드를 다음과 같은 진단명으로 탐지한다.

Backdoor/Win32.Icefog
Backdoor/Win32.Escad
Trojan/Win32.Escad
Win-Trojan/Rifdoor.Gen
Trojan/Win32.Phandoor

악성코드 피해를 100% 예방하기는 어렵다. 하지만 다음 기본 보안 수칙을 잘 지키면 대부분의 악성코드 감염 피해를 예방할 수 있다.

1. 백신 프로그램의 엔진 버전을 최신으로 유지하고 주기적으로 시스템 검사를 실시한다.
2. 윈도우, 맥, 리눅스 등 운영체제를 포함하여 마이크로소프트 오피스, 어도비 플래시(Adobe Flash), 자바(JAVA) 등 주요 프로그램을 최신 버전으로 유지한다.
3. 메일 첨부 파일 또는 다운로드한 파일이 실행 파일인 경우 의도한 파일이 맞는지 확인한 후 실행한다. 특히 문서나 동영상 파일로 위장한 실행 파일을 주의해야 한다.
4. 출처가 불분명한 메일의 첨부파일은 실행을 자제한다.

결론

안랩을 비롯한 국내외 보안 업체들이 분석한 바와 같이 2011년 이후 세계적으로 방위산업체에 대한 공격은 더욱 고도화되고 있다. 방위산업체는 국가 안보와도 밀접하게 연관되어 있기 때문에 앞으로도 경쟁국, 적대국의 공격자들이 방위산업체에 대한 공격을 더욱 확대할 것으로 보인다.

국내 방위산업체에 대한 공격 또한 지속적으로 보고되고 있다. 특히 일부 공격 그룹은 국내 방위산업체뿐 아니라 정치, 외교 분야에 대한 공격도 함께 진행하고 있는 것으로 보아 산업 스파이가 아닌 경쟁국, 적대국의 첩보 가능성이 높다. 이와 같은 국내 방위산업체에 대한 공격은 단순 산업 기밀 유출을 넘어 국가 안보에 대한 위협이 야기되는 만큼 더욱 강력한 보안 대책과 관리를 통한 예방이 필수적이다.