# SPECIAL REPORT

## Operation Shadow Force

Operation Shadow Force 분석 보고서

# 정상 인증서에 숨은 섀도 포스, 7년간의 행적 드러나

시작은 미쓰비시 전기 해킹 사건으로부터 비롯되었다. 2020년 1월 아사히 신문은 일본의 방위 산업과 주요 사회 인프라를 관리하는 대형 전기 회사인 미쓰비시 전기(Mitsubishi Electric)가 대규모 사이버 공격을 받았다고 발표했다. 이 공격에는 오로라 판다(Aurora Panda), 엠디비(Emdivi), 틱(Tick), 블랙테크(BlackTech) 등 4개의 공격 그룹이 관련되었다고 보도했다. 안랩시큐리티대응센터(AhnLab Security Emergency response Center, 이하 ASEC)는 이 가운데 한국에서 잘 알려지지 않은 오로라 판다 그룹을 주목하고 한국에서의 활동 정황을 확인하기 위해 분석을 시작했다. 그리고 오로라 판다와 연관이 있다고 알려진 그룹의 악성코드를 분석하던 중 뜻밖에 새로운 공격 흔적을 발견했다. 그 단서를 제공한 문자열은 바로 "Welcome To Shadow Force"이다. 이 글에서는 ASEC이 오퍼레이션 섀도 포스(Operation Shadow Force)를 어떻게 발견했는지 그 추적 과정을 소개한다.

오퍼레이션 섀도 포스(Operation Shadow Force)는 2013년 이후 2020년 현재까지 섀도 포스(Shadow Force)와 Wg드롭(Wgdrop)으로 대표되는 악성코드로 한국의 기업과 기관을 공격하는 그룹의 활동이다. 이 그룹의 확인된 최초 공격은 2013년 3월이지만 악성코드 제작 일자 등을 고려했을 때 2012년 이전에도 활동했을 가능성이 높다. 이들이 주로 사용한 악성코드가 섀도 포스(Shadow Force)라는 점에서 착안해 오퍼레이션 섀도 포스로 명명했으며, 공격자가 기존에 알려진 그룹과 연관되어 있는지는 아직 확인되지 않았다.

## 공격자 특징

오퍼레이션 섀도 포스의 공격 방식은 정확히 알려지지 않았다. 메일 등을 통한 내부 침입도 추정할 수 있지만 감염 시스템의 대부분이 윈도우 서버이며 정상 SQL 서버 실행 파일인 sqlserver.exe에서 다른 악성코드를 다운로드한 경우가 있어 취약한 SQL 서버로 침투했을 가능성이 높다.

공격자가 지난 7년 동안 잘 알려지지 않은 이유는 2014년 이후 에러 처리 프로그램이나 디스크 관리 프로그램과 같은 사용자가 신뢰하는 파일을 변조해 이들 프로그램이 실행될 때 악성코드가 로딩되는 방식을 사용했기 때문이다. 이들 프로그램은 조금 수상한 행위를 해도 원래 네트워크 접속이 잦고 사용자가 신뢰하는 프로그램이라 사용자의 의심을 피할 수 있다. 또 상당수 악성코드가 유출된 정상 디지털 인증서로 서명되어 있다. 정상 디지털 인증서로 서명된 파일은 보안 프로그램에서 신뢰할 수 있는 프로그램으로 판단해 어느 정도 수상한 행위를 해도 사용자에게 경고를 하지 않는다.

2014년 9월 처음 발견된 Pemodifier(iatinfect.exe) 파일은 Wg드롭(Wgdrop) 악성코드가 DLL 형태로 변경된 시점과 비슷하다. 공격자는 EXE 파일 형태의 Wg드롭을 사용하다가 2014년 봄 이후에 공격 전략을 바꿔 정상 EXE 파일을 변조해 DLL 형태의 악성코드를 실행하는 방식으로 바꿨다.

제작된 악성코드에 제작자 이름이 표시된 경우가 많다. 멜로디(Melody), 시링크스(Syrinx), 윈에그드롭(WinEggDrop)이 이 그룹의 대표적 제작자다. 이들은 해킹에 사용하는 파일 속성 변환, 프로세스 뷰어 등의 여러 도구를 제작하기도 했다.

다행히 공격자는 2014년 이후 동일한 기법을 사용해 비교적 쉽게 연관성을 찾을 수 있었다.

| 일시 | 목표 | 내용 |
|---|---|---|
| 2014년 9월 | IT 운영 관리 업체 | Htran(d014027b15e3f5099676e423131ef805), Pemodifier(9e0859b29641c9300058a2686daa1b06), Wgdrop (1fd5d459f198bda20399f0e76ce64f8e) 등을 이용한 공격 |
| 2015년 1월 | 의료 기관 | VAN 관리 프로그램 패치 해 Wgdrop B형(e4b0d1942064d644e7bd65fca8508c21) 실행 |
| 2015년 5월 | 언론사 | Shadow Force 변형(5408579f20d1dc533857cbbc114323d3) 접수 |
| 2015년 7월 | 운송 업체 | Shadow Force(07a390809ba4f8e4d0b213e9f9a88252), Pemodifier(e52dddabd40783032e85fe1076db2c6c) 발견 |
| 2015년 8월 | 외식 업체 | Wgdrop A형(f57e577822b6aaac5b9dfd9e464d4694)과 시스템 관리 프로그램 변조해 Wgdrop B형 실행(9fe571b36f14e232690951643981011c) 실행 |
| 2019년 3월 | 정치기구 | Shadow Force 변형 신고 |

[표 1] 오퍼레이션 섀도 포스에 의한 피해 사례

2013년부터 7년 동안 활동했지만 이 그룹에 의한 피해 신고는 많지 않았다. 하지만, 고객 신고 외에 감염되어도 모르고 있는 경우도 20곳 이상으로 파악되었다.

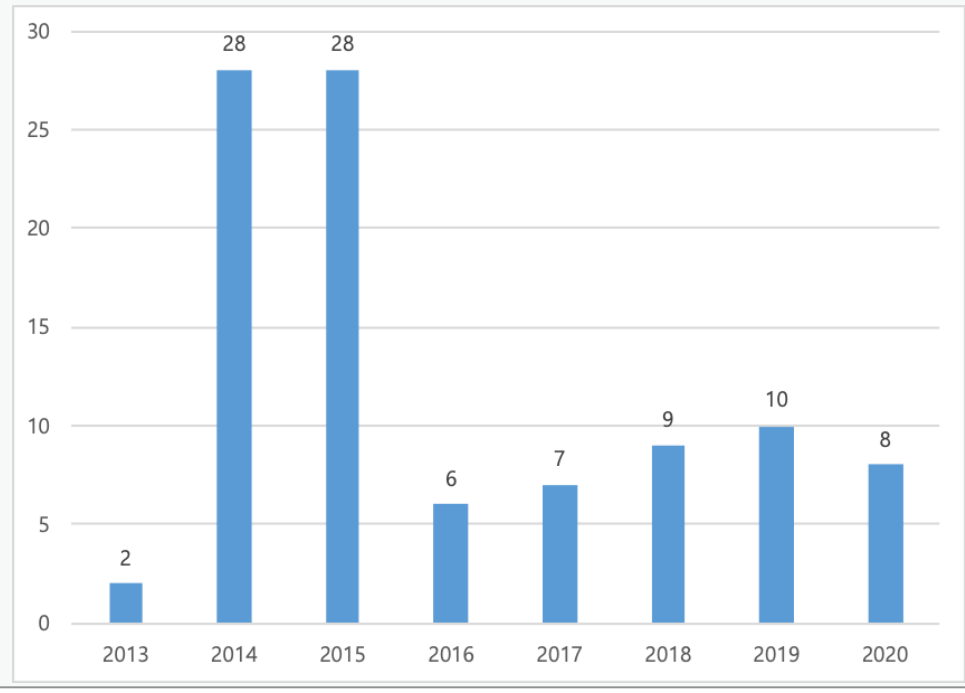
### 공격 단계

피해 시스템은 보통 윈도우 서버이며 공격자는 아직 확인되지 않은 방법으로 시스템에 침입한다. 많은 관련 악성코드는 aio.exe 파일을 통해 다운로드 되었다. SQL 관련 파일인 sqlservr.exe 파일에서 aio.exe 파일을 다운로드 한 기록이 있어 공격자는 SQL 서버를 장악 후에 aio.exe 파일을 다운로드 했다고 생각된다.

Htran(aio.exe) 파일을 통해 관련 악성코드를 다운로드 하고 윈도우 실행 파일을 패치시키는 Pemodifier (iatinfect.exe)로 정상 프로그램을 변조해 특정 DLL 파일이 함께 실행되도록 한다. 변조된 EXE 파일이 실행되고 섀도 포스(Shadow Force) 등의 악성 DLL이 함께 실행된다. 일부 시스템은 키로거, 화면 녹화 등의 추가 프로그램을 설치한다. 현재까지 자료를 유출하는 방식은 확인되지 않았다.

### 통계

2013년부터 2020년 3월 현재까지 오퍼레이션 섀도 포스와 연관되어 사용된 악성코드는 98 개 이상이다.
각 연도별 발견된 악성코드는 [그림 1]과 같다. 단, 공격 시점과 발견 시점이 일치하지 않을 수 있다.




[그림 1] 오퍼레이션 섀도 포스 관련된 악성코드의 연도별 발견 수

악성코드 종류는 Wg드롭 변형이 32개로 가장 많으며, 섀도 포스 변형은 23개이다. 공격자는 2014년 이후 Wg 드롭 대신 섀도 포스를 사용하고 있어 섀도 포스 변형의 비중 증가가 예상된다. 공격자가 해킹을 위해 사용한 도구들은 총 34개이다.

### 추적기

오퍼레이션 섀도 포스, 이 그룹은 특이하게 다른 사건에 흥미를 가졌다가 꼬리가 밟혔다. 2020년 1월 일본 언론은 미쓰비시 전기 해킹을 보도한다. 2013년부터 오로라 판다(Aurora Panda, APT17), 엠디비(Emdivi), 틱(Tick), 블랙테크(BlackTech)로 알려진 4개 그룹의 공격 시도가 있었다고 한다.  이중 엠디비(Emdivi)의 일본 연금기구 해킹과 틱(Tick) 그룹의 한국 내 활동에 대해서는 안랩에서도 분석 보고서를 공개했다. 하지만, 오로라 판다(Aurora Panda), 블랙테크(BlackTech)는 한국에서는 잘 알려지지 않은 그룹이다. 안랩은 오로라 판다(Aurora Panda)의 한국에 대한 공격이 확인된 바 없어 오로라 판다(Aurora Panda) 그룹이 한국에서 활동 정황이 있는지 추적키로 했다. 참고로 현재까지 미쓰비시 전기 해킹에 사용된 악성코드 정보는 공개되지 않았다.

### 4N* 인증서 서명 파일 조사

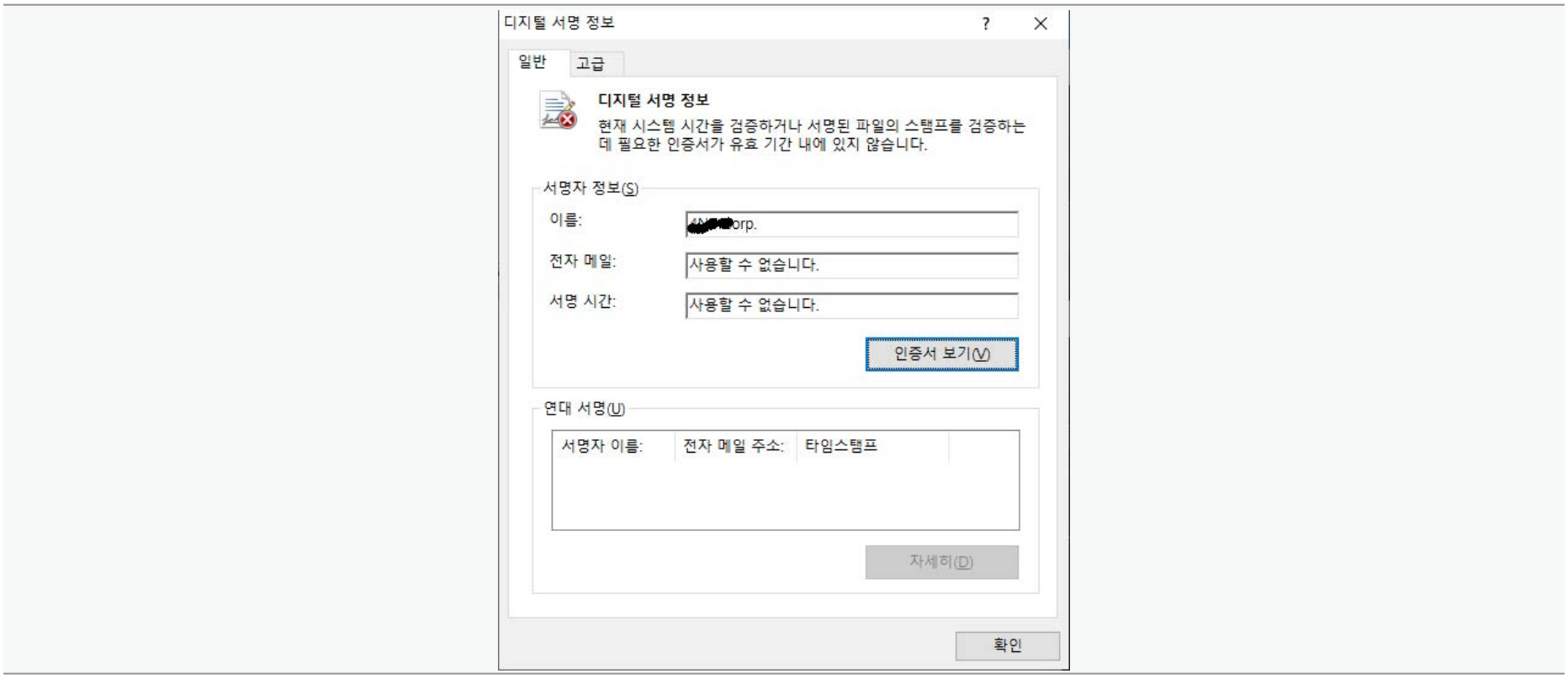
여러 보안 업체에서 오로라 판다(Aurora Panda) 그룹과 관련된 분석 보고서를 공개하고 있어 쉽게 침해사고 지표(Indicator of Compromise, 이하 IOC)를 확인할 수 있었다. 하지만, 이미 알려진 IOC로는 이 그룹의 한국내 활동은 확인할 수 없었다. 여기서 추적을 끝낼까 했지만 오로라 판다(Aurora Panda)와 연관되었다고 알려진 Zoxpng 변형이 한국 업체의 인증서로 서명되었다는 내용을 읽고  4N* 인증서로 서명된 다른 악성코드가 존재할 수도 있어 4N* 인증서로 서명된 파일에서 의심스러운 파일을 찾아봤다.

### 섀도 포스(Shadow Force) 발견

2020년 1월 첫 분석 시점에 4N* 인증서로 서명된 파일은 총 672개였으며, 의심스러운 파일 몇 개를 조사했다. 대부분 정상이었고 2017년 11월 수집된 파일(md5: 6f0e62b15efd2b2468ef37c138eb189a)에서 악성코드 느낌이 물씬 풍기는 'Welcome To Shadow Force'란 문자열을 발견했다.


[그림 2] 섀도 포스(Shadow Force) 주요 문자열

이 파일은 기존 4N* 인증서(일련 번호: 483f0bf7a6d84c6cf429d4eb4988e686)로 서명된 악성코드와는 인증서 일련 번호가 다르고 인증서 정보도 불명확해 정상 인증서는 아니었다.




[그림 3] 위조된 4N* 인증서

하지만, 결과적으로 섀도 포스(Shadow Force)의 발견은 중요한 실마리였다. 이미 공개된 정보가 있는지 확인하기 위해 2015년 트렌드 마이크로에서 공개한 분석 내용을 확인했다.

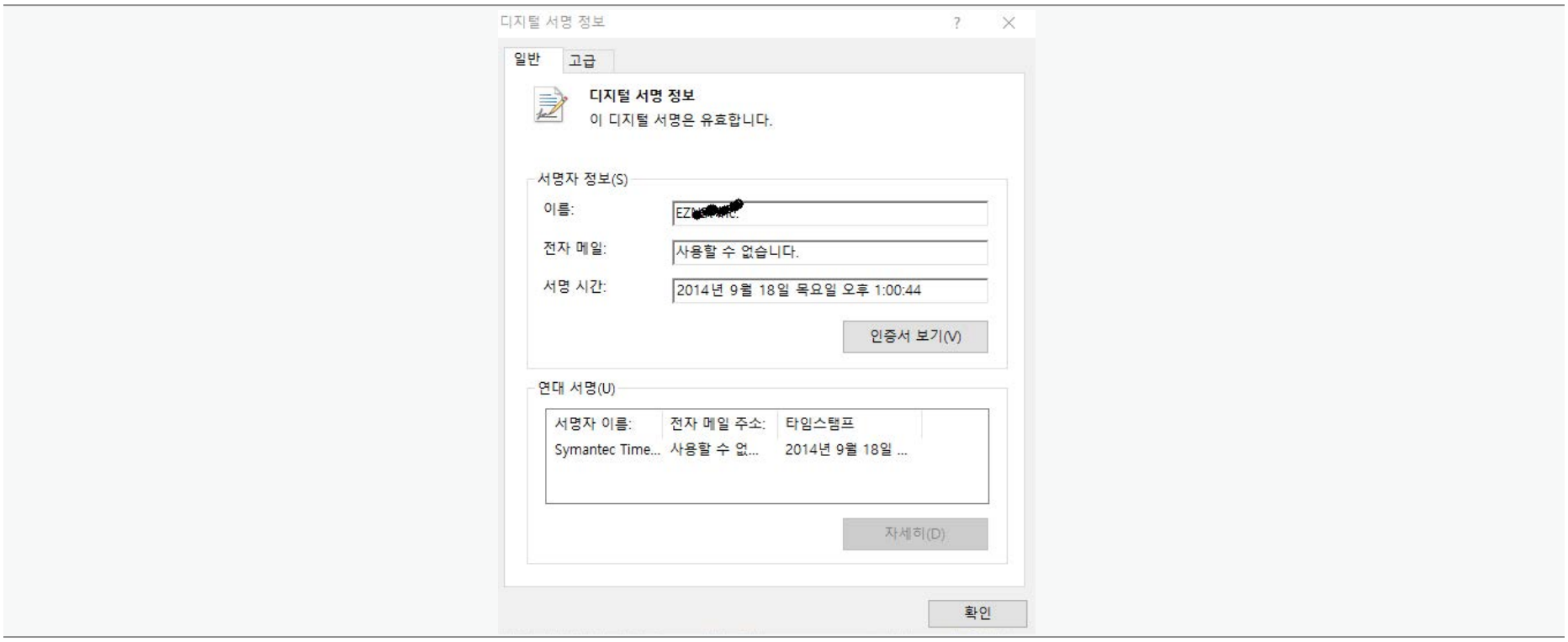
### 섀도 포스(Shadow Force) 변형 헌팅

위조 4N* 인증서로 섀도 포스(Shadow Force) 변형을 하나 찾고 안랩에서 보유 중인 샘플에서 관련 변형을 본격적으로 찾아 총 23개의 섀도 포스 변형을 찾았다. 트렌드 마이크로 보고서는 2015년 한국 기업을 공격한 변형에 대한 내용이었으나 해시 정보를 공개하지 않아 어떤 악성코드인지는 확인할 수 없었지만 파일 이름 등을 통해 2015년에 접수된 샘플로 추정할 수 있었다. 2014년 9월 처음 변형이 발견되었으며 찾은 파일은 고객 접수 유무를 확인해 2019년 3월 한국 정치기구에서 신고한 파일(md5: fcd695fa1cd04b23697b2e4fdd2d557b)임을 확인했다. 고객 신고는 없었지만 문서를 한참 작성하고 있던 3월 중순에도 2020년 3월 초 활동이 확인된 파일(md5: a952b2cd5661c94ed7f13a88f8c41ee7)도 있었다.

여러 개의 섀도 포스 변형 파일이 한국의 소프트웨어 개발 업체와 게임 개발 업체의 인증서로 서명되어 있었다.

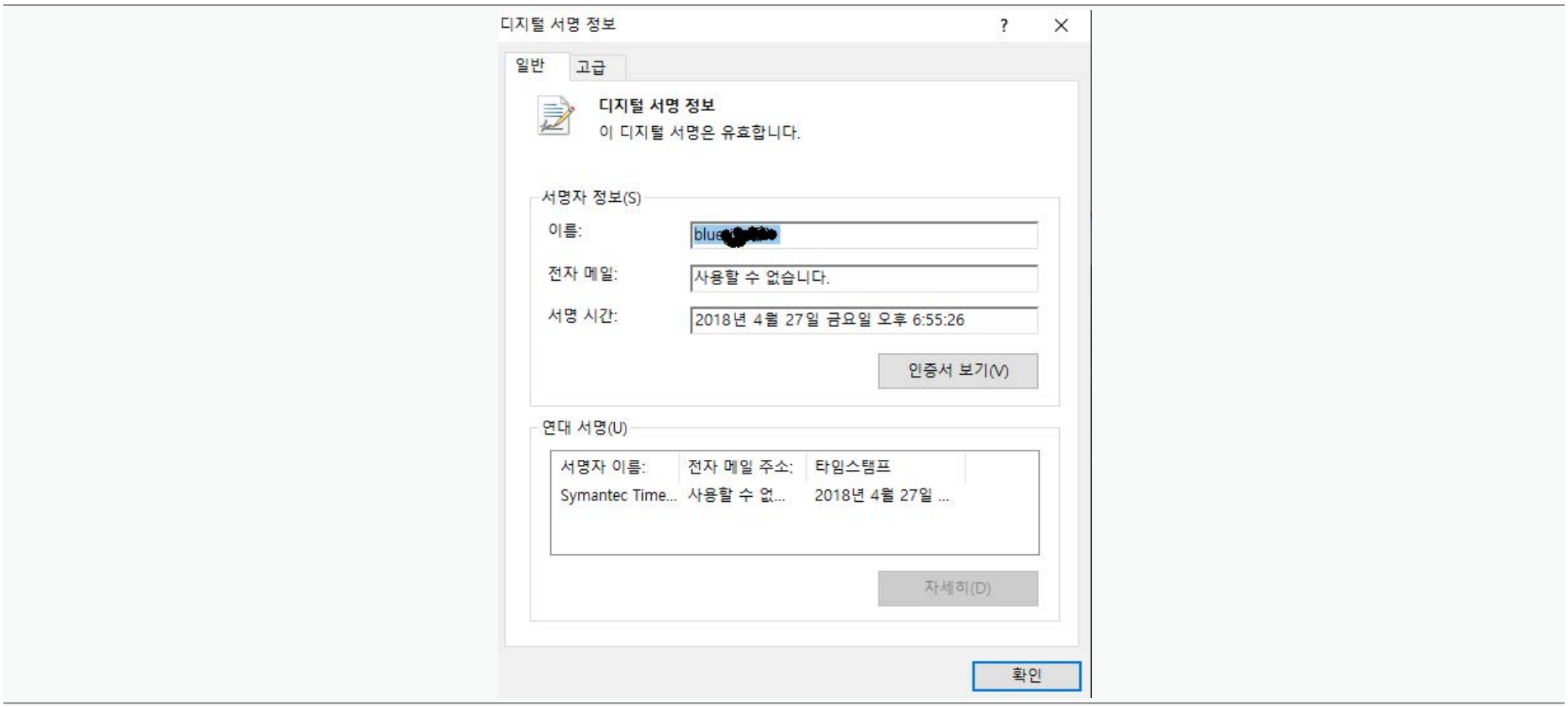
섀도 포스 변형을 조사하던 중 EZ*** 인증서(일련 번호: 73e78017a7bf71b6762a603dc41fb6b5)로 서명된 파

일(md5: f23bf5c35273927979ea47413a141a05)을 발견했다. EZ*** 인증서는 2020년 3월 현재도 유효하다.




[그림 4] EZ*** 인증서 서명 샘플

다른 섀도 포스 변형(md5: a3440c605ceecfba560e33f167530d9b)은 한국 게임 개발 업체인 blue**** 사의 인증서(일련 번호: 706ac96953034b9d9926d4cc1d3248b3)로 서명되었다. Blue**** 인증서도 2020년 3월 현재 유효하다.




[그림 5] Blue*** 인증서 서명

EZ***와 Blue**** 인증서로 서명된 파일을 조사하기로 결정했다.

### EZ*** 인증서 서명 파일 조사

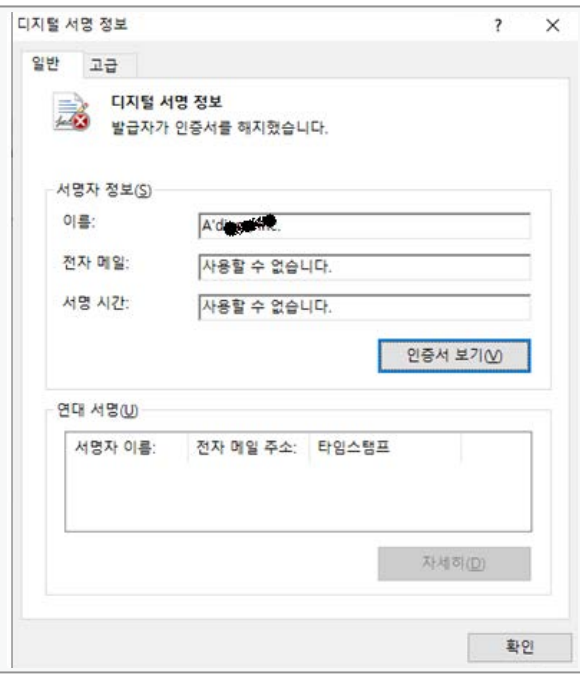
EZ*** 인증서로 서명된 파일은 4,859개이며 이 중 의심스러운 파일을 선택적으로 분석해 32개의 악성코드를 발견했다. 공격자는 2014년부터 해당 인증서를 도용하고 있어 2014년 공격자에 의해 해당 업체의 인증서 키가 유출된 것으로 보인다. 공격자는 탈취한 EZ*** 인증서 키를 통해 2014년 악성 섀도 포스와 Wg드롭(md5: 954122ca75a556f3059b14fe11002f71) 변형 파일에 서명했다. 2014년에서 2019년 사이에 발견된 악성코드는 이 인증서로 서명되었지만 실제 악성코드는 2014년에 제작된 듯 하다. Wg드롭 변형을 정리하면서 한국 의류 회사로 추정되는 A'd*** 인증서로 서명된 악성코드(md5: 106ec8522b99ca3988ce28d7bfaa0be9)를 추가 확인했다.

### Blue**** 인증서 서명 파일 조사

섀도 포스 변형에서 한국 게임 업체의 인증서를 발견하고 해당 인증서로 서명된 파일 목록에서 의심스러운 파일을 찾아 분석했다. Blue**** 인증서로 서명된 파일은 116개이며 이 인증서로 서명된 악성코드는 총 9개로 2018년 4월 첫 발견된 이후 2020년 3월까지 발견되었다. Blue**** 인증서로 서명된 파일을 조사해 로더(Loader), 섀도 포스(Shadow Force), 로그온스틸러(LogonStealer), 키로거(Keylogger), 로그인 정보 탈취 등의 추가 해킹도구를 찾았다. 하지만, 여전히 의심스러운 파일이 더 존재해 실제 악성코드 수는 더 많을 것으로 예상된다.

### A'd*** 인증서 서명 파일 조사

한국 의류 회사로 추정되는 A'd*** 인증서(일련 번호: 456e967a815aa5cbb99fb86aca8f7f69)로 서명된 파일에서 Wg드롭(md5: 9552c356950daf907f30da1ca2dcb755) 변형이 발견되었다.




[그림 6] 해지된 A'd*** 인증서

하지만, 동일 인증서로 서명된 일부 파일(md5: 106ec8522b99ca3988ce28d7bfaa0be9)의 디지털 서명은 현재도 유효 상태이다.

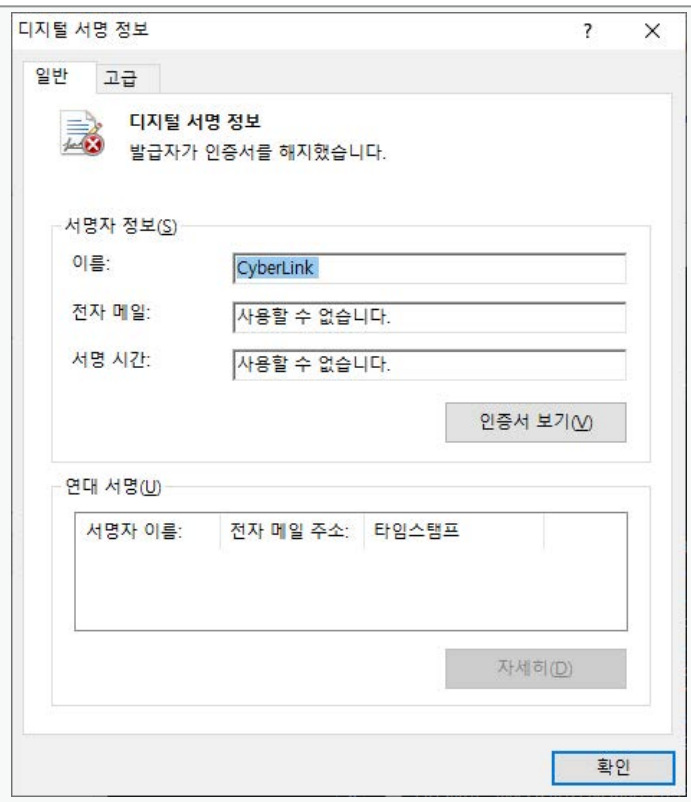

[그림 7] 유효한 A'd*** 인증서

A'd*** 인증서로 서명된 파일은 30개 이상이며 총 5개의 서명 파일이 확인되었다. 2013년 3월부터 이 인증서로 서명된 악성코드가 발견되었다. 2019년 11월에도 인증서로 서명된 변형이 발견되었지만 여러 정황상 2013년까지만 사용되었다.  보통 Wg드롭 변형이지만 다른 악성코드도 존재하며 이들 악성코드가 이 그룹과 연관되었는지는 추가 조사가 필요하다.

## CyberLink 인증서 서명 파일 조사

타이완 CyberLink로 서명된 악성 Wg드롭(md5: f5eb4f51f0e8a96d39ba2ab3e4890b4f)이 2015년에 수집되었다. 하지만, 파일 빌드 시간은 2012년 10월로 초기에 제작된 Wg드롭 변형으로 보인다.

CyberLink 인증서는 현재 해지 상태이다.

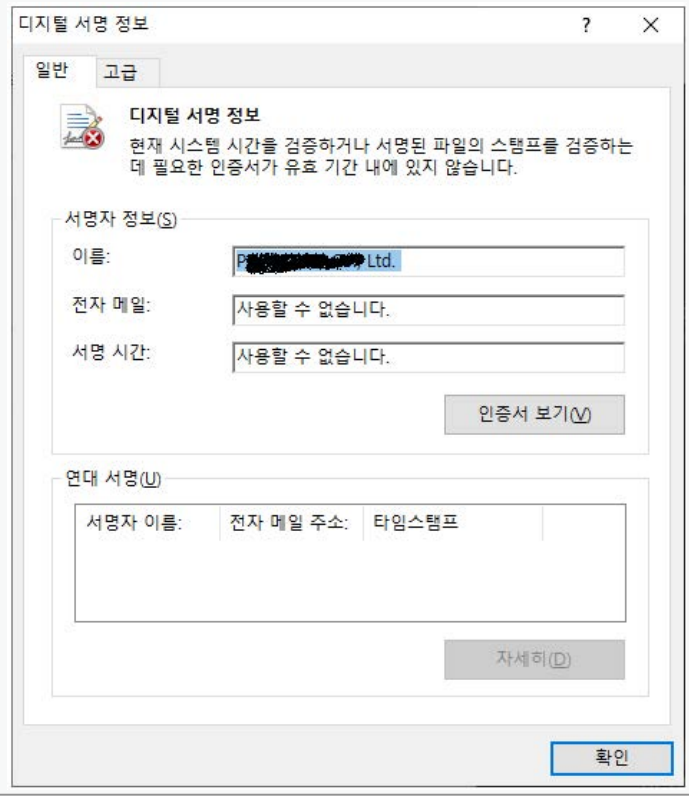



[그림8] 해지된 CyberLink 인증서

CyberLink로 서명된 파일은 6만 5천개가 넘어 조사에 어려움이 있어 추가 연관 악성코드를 확인하지 못했다.

## P*****a 인증서 서명 파일 조사

로더(Loader) B형 변형을 조사하다 한국 UCC 미디어 회사의 인증서(일련 번호: 39880be01fe37120ad98698509663f92)를 위조한 악성코드(md5: b070f96f08e4947dbf725b80f5c51af3)를 발견했다. 비정상 인증서로 인증서 키 유출이 아닌 단순 위조로 보인다.




[그림 9] 위조된 P*****a 인증서

이 업체의 인증서로 서명된 파일은 2020년 3월 현재 총 4,969개 이상으로 아직 이 그룹과 연관된 악성코드나 도구를 확인하지 못했다.

### 인증서 도용 및 위조

공격자는 정상 인증서를 도용 및 위조해 악성코드에 서명했다. 즉 공격자가 해킹을 통해 얻은 인증서 키를 악성코드에 사용한 것으로 추정된다.

공격자는 2012년 CyberLink 인증서, 2012년~2013년 A'd*** 인증서, 2014년 EZ***, 2017년 4NB, 2018년~2020년에는 blue**** 인증서를 사용했다.

| 인증서 | 일련 번호 | 국가 | 기간 | 방식 | 상태 |
|---|---|---|---|---|---|
| 4N* | 483f0bf7a6d84c6cf429d4eb4988e686 관리 업체 | 대한민국 | 2017년 | 위조 추정 | ? |
| A'd*** | 456e967a815aa5cbb99fb86aca8f7f69 | 대한민국 | 2012년 ~ 2013년 | 도용(키 유출 추정) | 해지 |
| Blue**** | 706ac96953034b9d9926d4cc1d3248b3 | 대한민국 | 2018년 ~ 2020년 | 도용(키 유출 추정) | 유효 |
| CyberLink | 1d226108cbb0eb7b504697bdfec66a8b | 타이완 | 2012년 | 위조 추정 | 해지 |
| EZ*** | 73e78017a7bf71b6762a603dc41fb6b5 | 대한민국 | 2014 년 | 도용(키 유출 추정) | 유효 |
| P*****a | 39880be01fe37120ad98698509663f92 | 대한민국 | 2018년 | 위조 추정 | ? |

[표 2] 공격자에게 도용된 인증서

공격자는 대부분 대한민국 업체의 인증서를 도용하거나 위조했다.

단, 인증서만으로 이 그룹과의 연관성을 단정 지을 수는 없다. 누군가 유출한 인증서 키를 다른 공격자들과 공유할 수 있기 때문이다. 이 그룹과 연관성을 확인하기 위해서는 단순히 동일 인증서 서명뿐만 아니라 공격 방식 등을 함께 고려해야 한다.

### 왜 오퍼레이션 섀도 포스를 주목해야 하는가

처음에는 일본 미쓰비시 해킹을 시도했던 그룹의 한국 활동을 추적하는 것이 목적이었다. 이 과정 중에 7년 동안 한국에서 은밀히 활동한 그룹의 흔적을 찾을 수 있었다. 이렇게 오랜 기간 동안 잘 알려지지 않고 활동했다

는 점에서도 그들의 은밀함에 놀랍기도 하지만 알려지지 않은 다른 그룹이 분명 존재 한다고 생각하니 걱정스러운 생각도 들었다. 다행히 이번 공격자는 비슷한 공격 방식을 사용하고 동일한 파일 이름의 도구를 몇 년 째 사용하는 등 습관을 크게 바꾸지는 않았다. 여기서 분명히 해둘 점은 이 공격 그룹이 은밀하게 활동하였다고 해도 일부의 악성코드는 탐지되었다. 지금까지 탐지되었던 악성코드와 공격 수법의 연관성을 파악해 오퍼레이션 섀도 포스라는 공격 그룹으로 그룹화 할 수 있었으며 추적 과정 중 지금까지 미진단 악성코드도 추가로 확인 대응 할 수 있었다. 그리고 이 공격 그룹이 즐겨 사용하는 도구가 다른 국내 해킹 사건에서도 발견되기도 해 이들과의 관련성도 계속 파악할 필요가 있다.

여전히 이 그룹은 여러가지 측면에서 의문스러운 점 있다. 이 그룹의 공격 수법이나 악성코드는 확인되었지만 이들이 다른 그룹과 연관 관계가 있는지 혹은 독자 그룹인지는 아직 알 수 없다. 오퍼레이션 섀도 포스(Operation Shadow Force)를 수행한 그룹과 오로라 판다(APT17)와 연관되었다는 명백한 근거는 없다. 또한 ZoxPNG 악성코드와 오퍼레이션 섀도 포스와는 일련 번호가 다른 동일한 인증서 1개 뿐이라 아직까지 연관되었다고 하기는 어렵다.

아직 초기 침입 방법, 정보 유출 방법 등은 여전히 확인되지 않았다. 그럼에도 불구하고 안랩이 오퍼레이션섀도포스를 소개한 이유는 여기에 공개된 IOC 정보를 바탕으로 의심스러운 침해 행위를 조기에 탐지하고 관련 업계와 협력해 남은 의문점을 함께 풀어가고자 함이다.

오퍼레이션 섀도 포스의 10가지 주요 악성코드 및 도구 분석, 연관 관계 분석, 의심 증상, 대응 현황 등의 상세한 내용은 ASEC이 발표한 분석보고서에서 확인할 수 있다.

▶'오퍼레이션 섀도 포스 분석 보고서' 전문보기