2020.04.07

Analysis Report

Operation Shadow Force

안랩 시큐리티대응센터(AhnLab Security Emergency response Center)

AhnLab

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

목차

본 보고서는 현재까지 안랩 ASEC에서 확인한 사실을 바탕으로 분석가의 의견이 포함되어 있습니다. 다른 근거에 따라 분석가들 마다 의견이 다를 수 있으며 새로운 근거에 따라 본 보고서 작성자의 의견이 달라질 수 있습니다.

Operation Shadow Force 개요

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.

1) 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.exe 파일에서 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 프로그램 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 기법과 파일 이름을 사용해 비교적 쉽게 연관성을 찾을 수 있었다.

2) 피해 사례

지금까지 확인된 공격 사례는 다음과 같다.

일시	목표	내용
2014년 9월	IT 운영 관리	Htran(d014027b15e3f5099676e423131ef805), Pemodifier (9e0859b29641c9300058a2686daa1b06), Wgdrop (1fd5d459f198bda20399f0e76ce64f8e) 등을 이용한 공격
2015년 1월	의료	VAN 관리 프로그램 패치 해 Wgdrop B형 (e4b0d1942064d644e7bd65fca8508c21) 실행
2015년 5월	언론사	Shadow Force 변형(5408579f20d1dc533857cbbc114323d3) 접수
2015년 7월	운송	Shadow Force(07a390809ba4f8e4d0b213e9f9a88252), Pemodifier (e52dddabd40783032e85fe1076db2c6c) 발견
2015년 8월	외식	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 파악되었으며 2020년 3월에도 활동이 확인되었다.

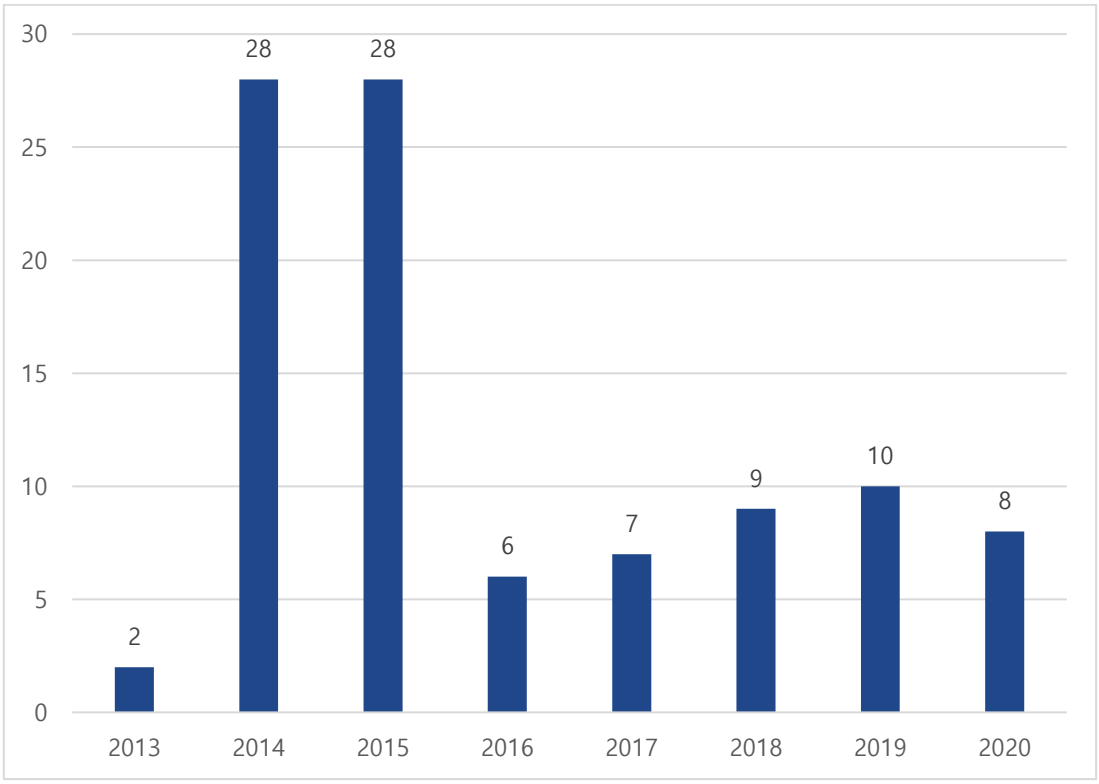
3) 공격 단계

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.

4) 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 Wg드롭 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.[1] 2013년부터 오로라 판다(Aurora Panda, APT17), 엠디비(Emdivi), 틱(Tick), 블랙테크(BlackTech)로 알려진 4개 그룹의 공격 시도가 있었다고 한다.[2] 이중 엠디비의 일본 연금기구 해킹[3]과 틱 그룹의 한국 내 활동[4]에 대해서는 안랩에서도 분석 보고서를 공개했다. 하지만, 오로라 판다(Aurora Panda), 블랙테크(BlackTech)는 한국에서는 잘 알려지지 않은 그룹이다. 안랩은 오로라 판다의 한국에 대한 공격이 확인된 바 없어 오로라 판다 그룹이 한국에서 활동 정황이 있는지 추적키로 했다. 참고로 현재까지 미쓰비시 전기 해킹에 사용된 악성코드 정보는 공개되지 않았다.

1) 4N* 인증서 서명 파일 조사

여러 보안 업체에서 오로라 판다 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 판다와 연관되었다고 알려진 Zoxpng 변형이 한국 업체의 인증서로 서명되었다는 내용을 읽고[5] 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 악성코

[1] https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html

[2] https://www.asahi.com/articles/photo/AS20200121004397.html

[3] https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?cmd=scrap&seq=23821&menu_dist=2

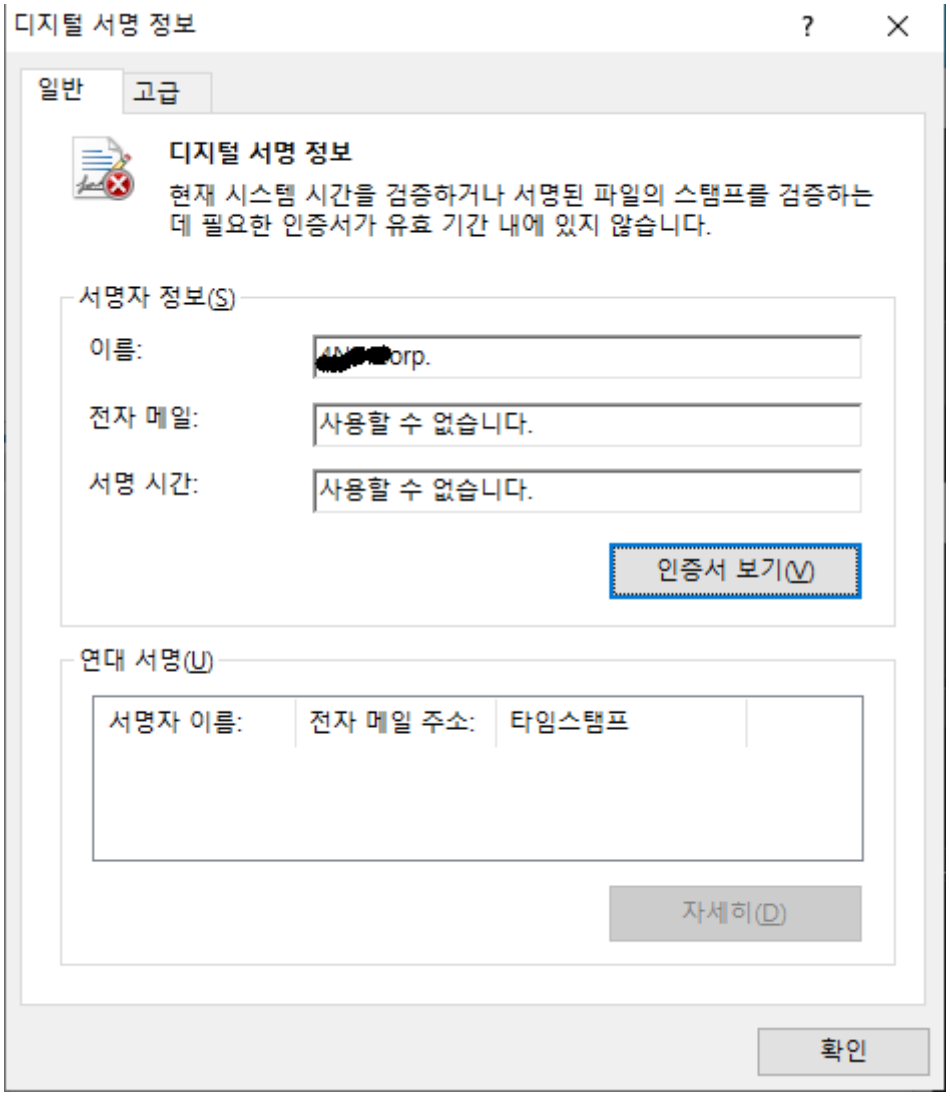
[4] https://asec.ahnlab.com/1216

[5] https://www.novetta.com/wp-content/uploads/2014/11/ZoxPNG.pdf

드 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 아니다.



[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.[6]

2) 섀도 포스(Shadow Force) 변형 헌팅

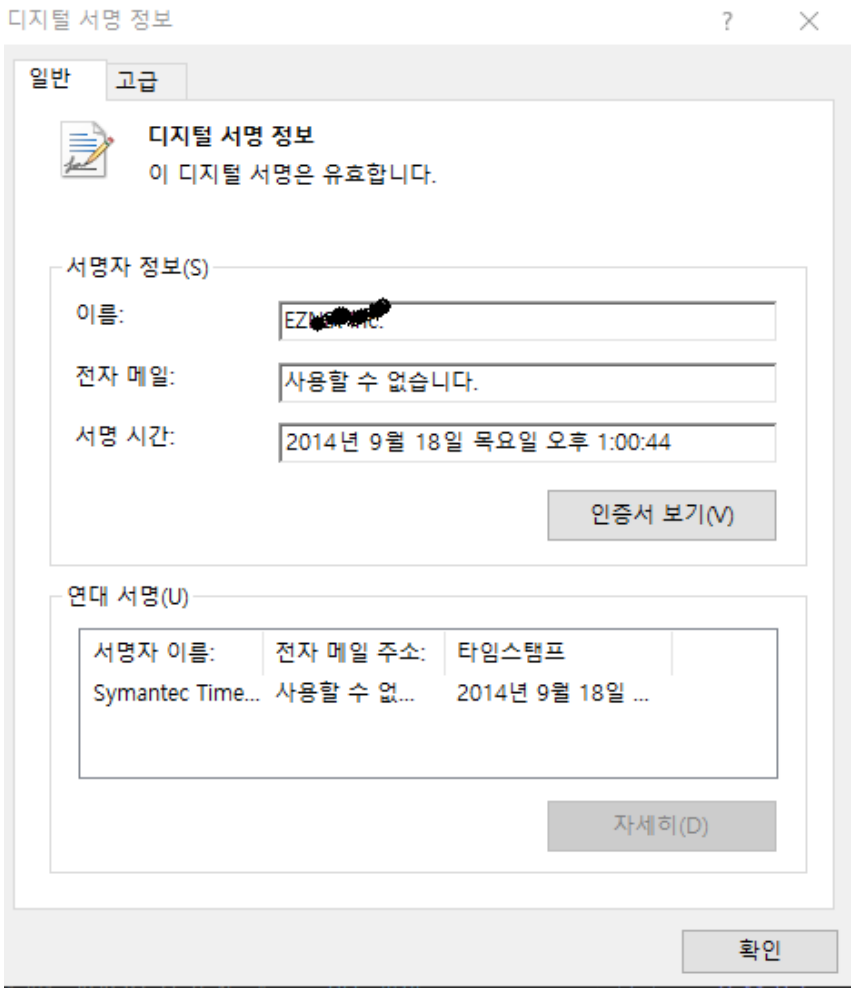
위조 4N* 인증서로 섀도 포스(Shadow Force) 변형을 하나 찾고 안랩에서 보유 중인 샘플에서 관련 변형을

[6] https://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company/

본격적으로 찾아 총 23개의 섀도 포스 변형을 찾았다. 트렌드 마이크로 보고서는 2015년 한국 기업을 공격한 변형에 대한 내용이었으나 해시 정보를 공개하지 않아 정확히 어떤 악성코드 인지는 확인할 수 없었지만 파일 이름 등을 통해 2015년에 접수된 샘플과 유사한 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 2019년 이후에도 꾸준히 활동했으며 2020년 3월 초에도 활동이 확인된 파일(md5: a952b2cd5661c94ed7f13a88f8c41ee7)도 있었다.

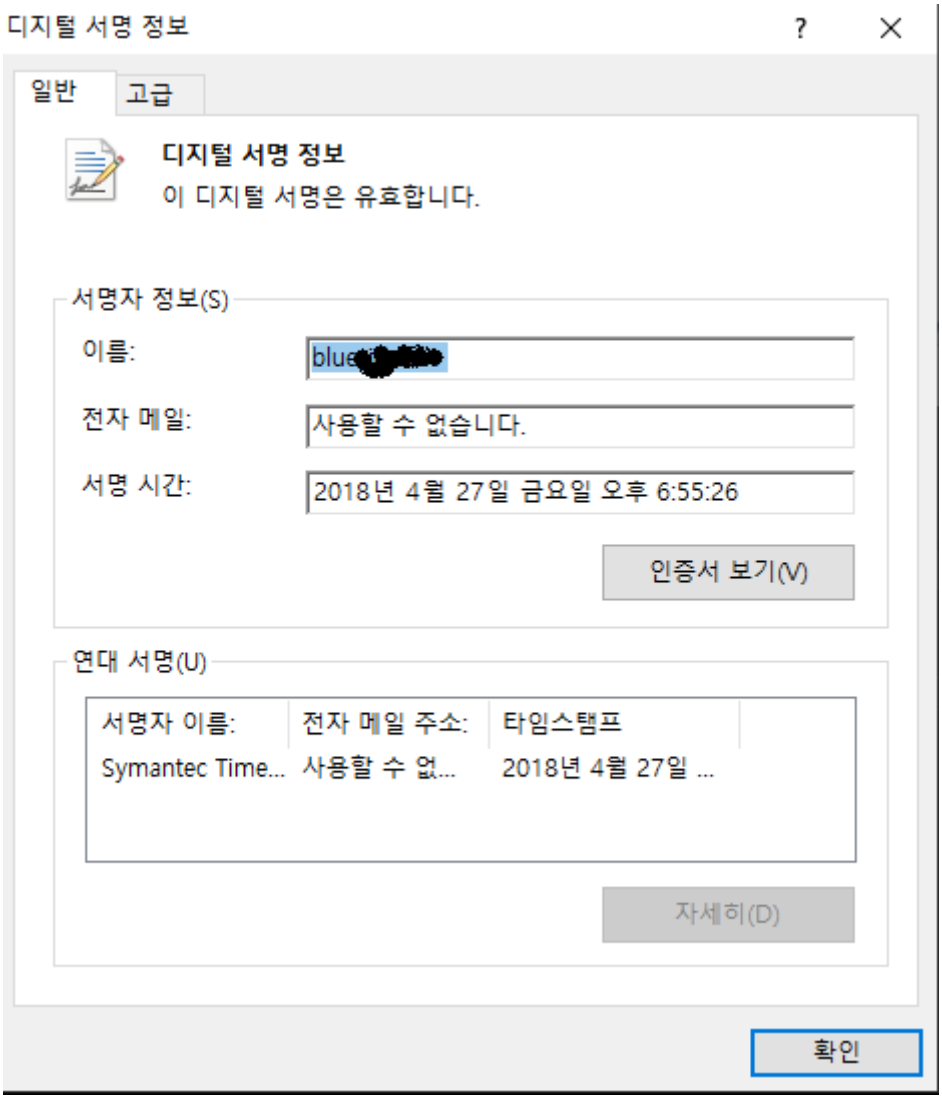
여러 개의 섀도 포스 변형 파일이 한국의 소프트웨어 개발 업체와 게임 개발 업체의 인증서로 서명되어 있었다.

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

3) 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 악

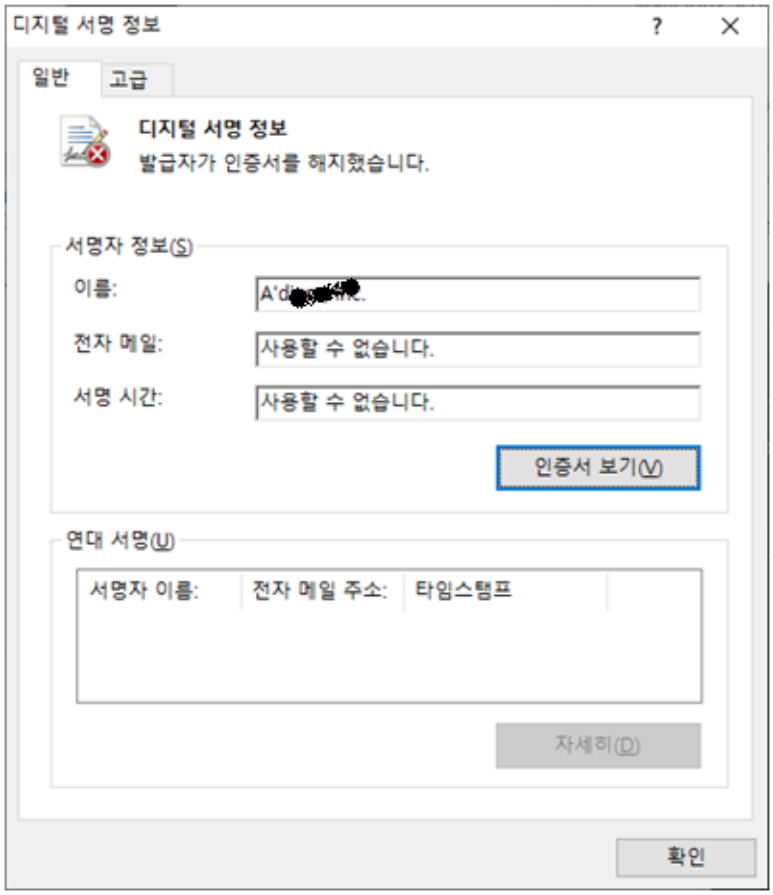
성코드는 이 인증서로 서명되었지만 실제 악성코드는 2014년에 제작된 듯하다. Wg드롭 변형을 정리하면서 한국 의류 회사로 추정되는 A'd*** 인증서로 서명된 악성코드(md5: 106ec8522b99ca3988ce28d7bfaa0be9)를 추가 확인했다.

4) 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 해킹 도구를 찾았다. 하지만, 여전히 의심스러운 파일이 더 존재해 실제 악성코드 수는 더 많을 것으로 예상된다.

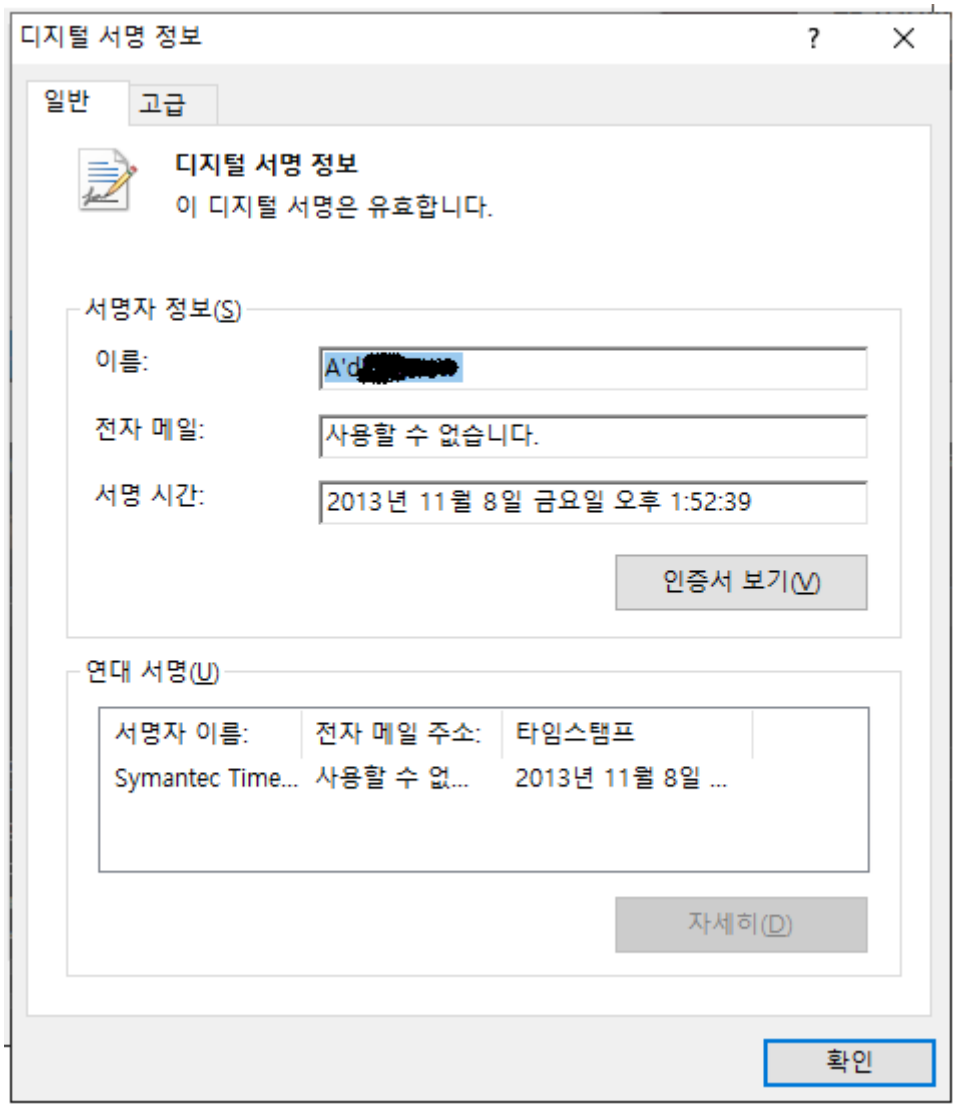
5) A'd*** 인증서 서명 파일 조사

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



[그림 6] 해지된 A'd* 인증서**

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



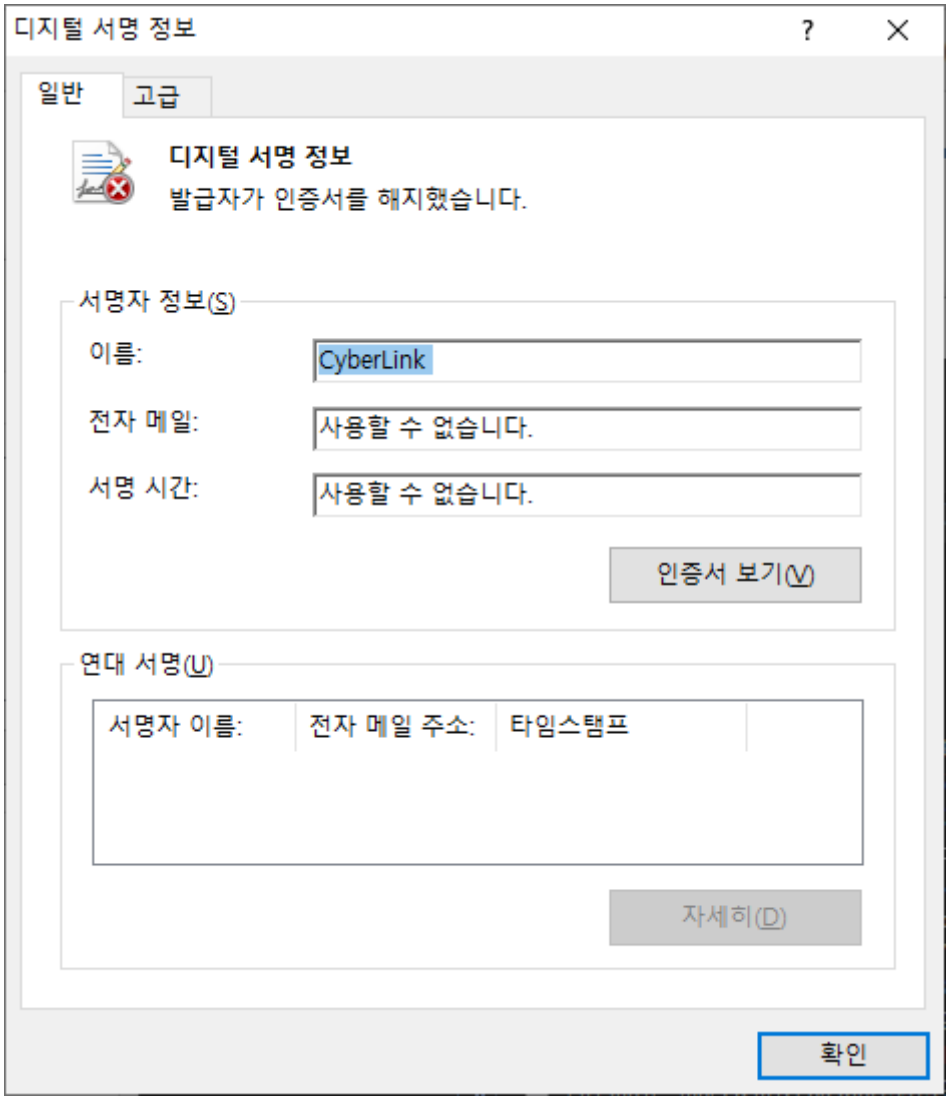
[그림 7] 유효한 A'd* 인증서**

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.

6) 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.

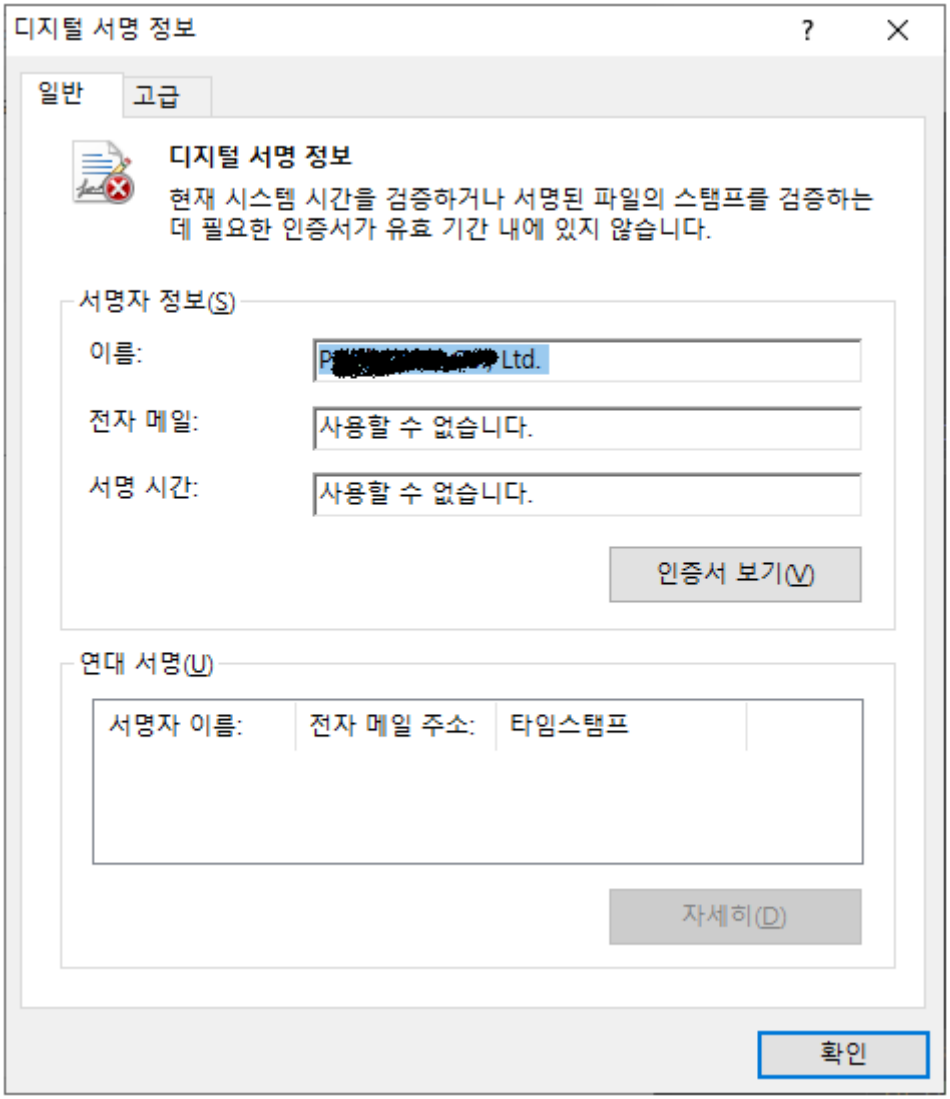


[그림8] 해지된 CyberLink 인증서

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

7) P*****a 인증서 서명 파일 조사

로더(Loader) B 형 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 2020 년 3 월 현재 총 4,969 개 이상으로 아직 이 그룹과 연관된 악성코드나 도구를 확인하지는 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 4N*, 2018년~2020년에는 blue**** 인증서를 사용했다.

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

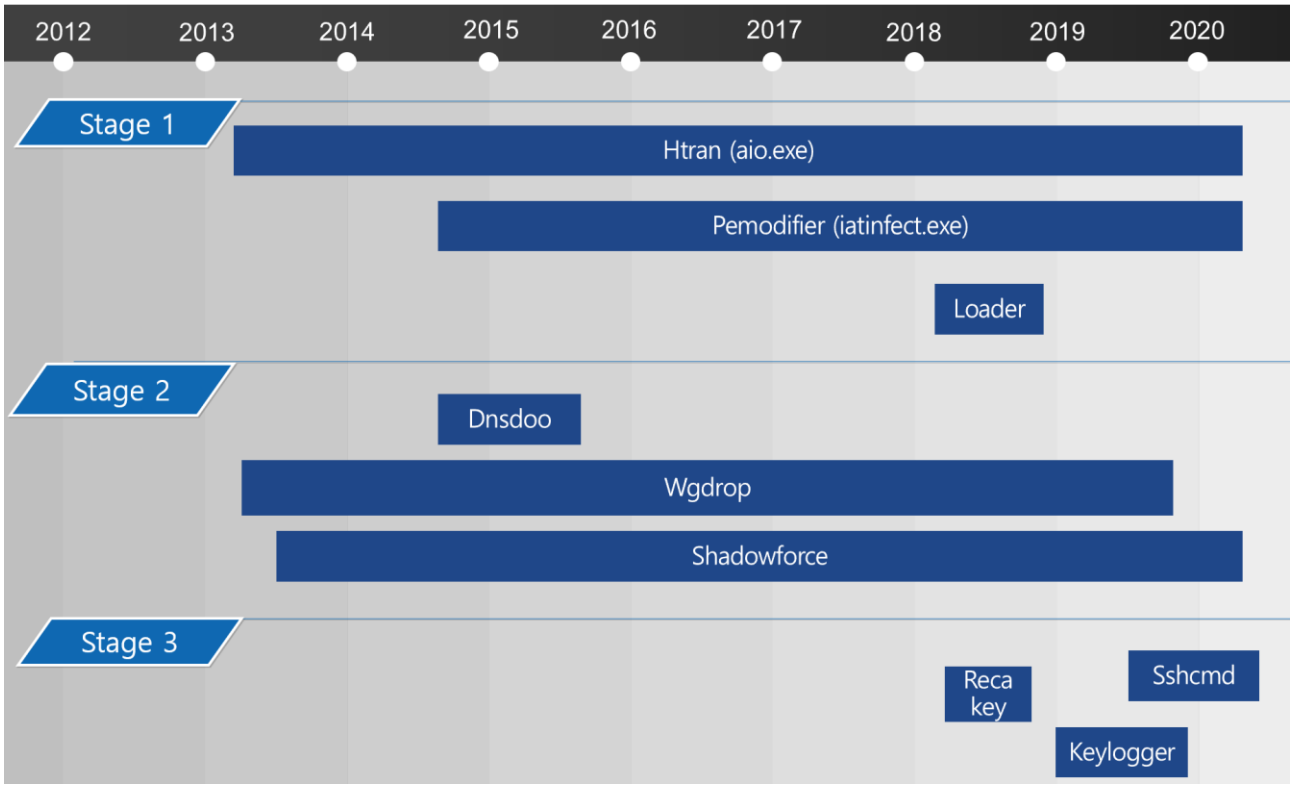
[표 2] 공격자에게 도용된 인증서

공격자는 대부분 대한민국 업체의 인증서를 도용하거나 위조했다.

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

주요 악성코드 및 도구 분석

현재까지 확인된 주요 악성코드는 다음과 같다.



[그림 10] 오퍼레이션 섀도 포스(Operation Shadow Force) 주요 악성코드

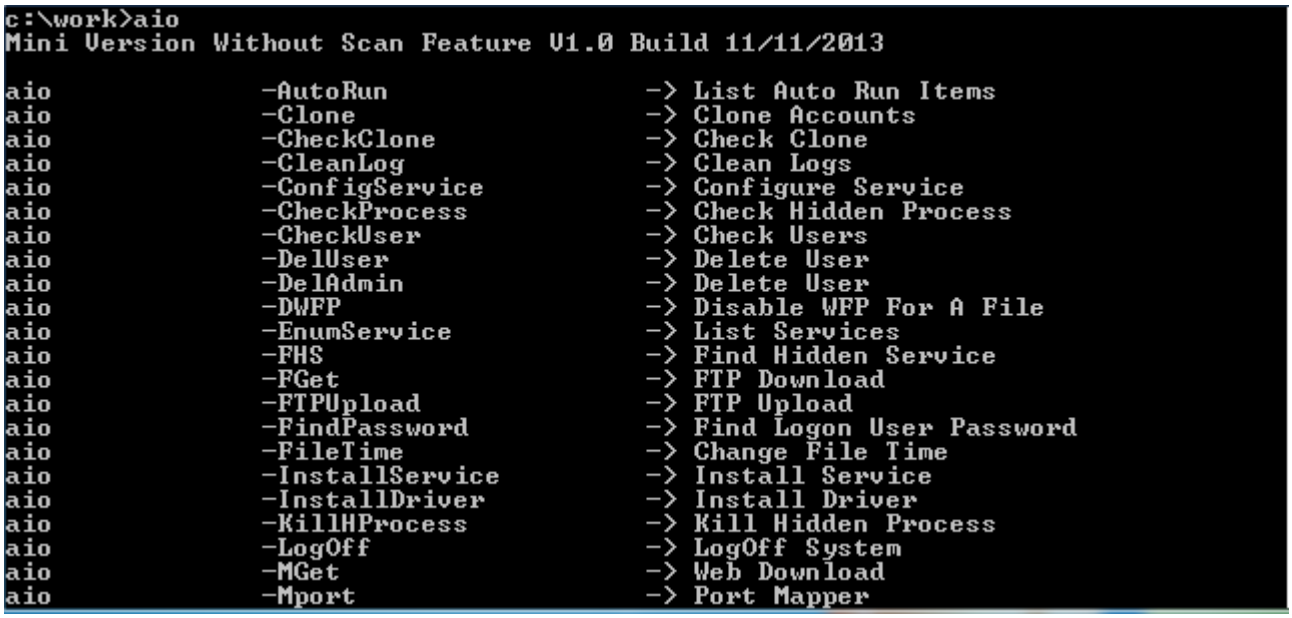
여기서는 공격자의 공격 단계 순서로 정리했다.

1) Tool - Htran(aio.exe)

Htran은 해킹 도구로 해킹에 필요한 여러가지 기능을 제공한다. 여기서는 공격자가 다른 악성코드를 다운로드 하기 위해 사용했다. 관련 변형은 2013년 3월에 처음 확인되었다. 파일 이름은 모두 aio.exe 이며 파일 길이는 90,112바이트에서 95,048바이트이다. 단, 2020년 3월 공격에 사용된 파일(md5: c22b29fcaac4b583a27693d0f72f617a)은 기존 파일을 UPX(Ultimate Packer for eXecutables)로 패킹해 파일 길이가 36,864바이트이다.

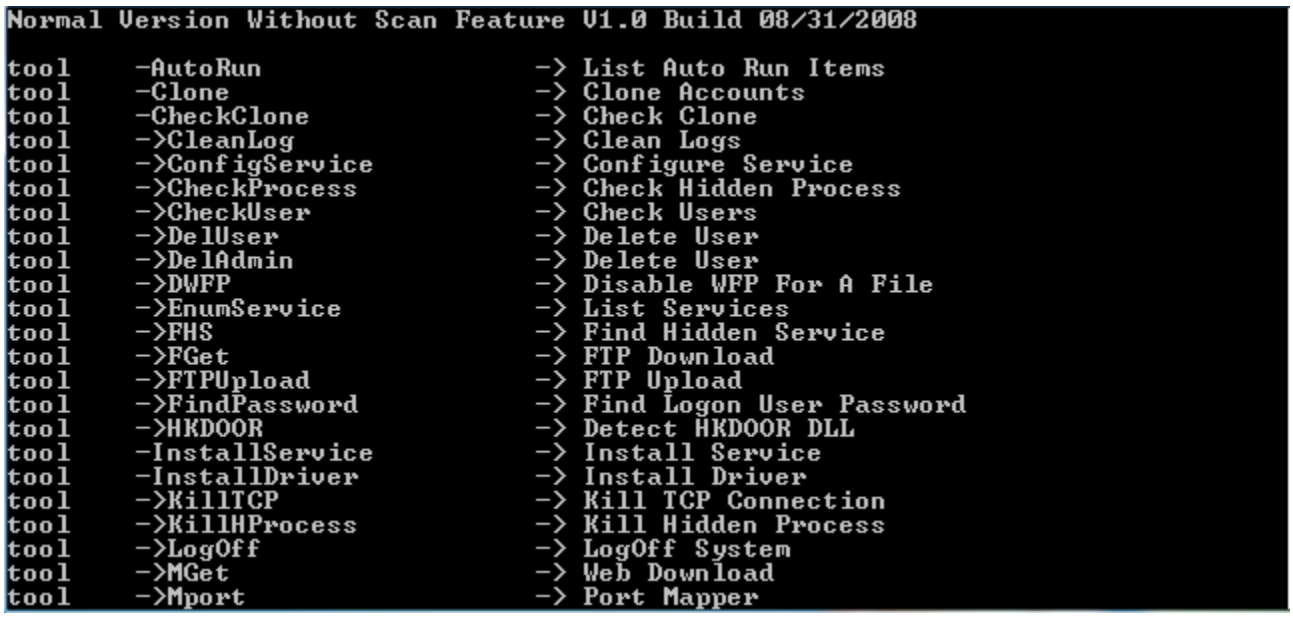
2014년에 발견된 aio.exe 파일을 실행하면 [그림 11]에서 확인할 수 있듯이 'Mini Version Without Scan

Feature V1.0 Build 11/11/2013'이 출력되며 로그 삭제, FTP 기능, 사용자 암호 찾기, 서비스 및 드라이버 실행 등의 기능을 제공한다.



[그림 11] aio.exe 실행 화면

2014년 침해 사고가 발생한 시스템에서 발견된 aio.exe는 2008년 제작된 해킹 도구를 수정했다. 2008년에 제작된 해킹 도구(md5: 07e5fbe4bf98da12af167fd8962339a1)는 [그림 12]와 같이 'Normal Version Without Scan Feature V1.0 Build 08/31/2008'을 출력한다.



[그림 12] 2008년 초기 버전 실행 화면

동일한 제작자가 제작한 도구인지 소스코드가 공개된 도구를 수정했는지는 확인되지 않았다. 또, 2018년 발

생한 국내 해킹 사건에 이 도구와 유사한 프로그램이 사용되었는데 해당 해킹 사건과 이 그룹의 연관성이 아직 확인되지 않아 여기서는 언급하지 않았다.

2) Tool - Pemodifier(iatinfect.exe)

공격자는 aio.exe 파일을 이용해 iatinfect.exe 등의 파일을 다운로드 했다. Pemodifier는 EXE 파일을 실행 될 때 특정 DLL 파일을 로드 하게 변조한다. 2014년 9월부터 2020년 3월 현재까지 꾸준히 사용하고 있으며 파일 이름은 모두 iatinfect.exe이다. 파일 길이는 39,424 바이트에서 103,424 바이트이다. 시스템에서 iatinfect.exe 파일이 발견된다면 이 그룹의 공격을 받았을 가능성이 높다.

Iatinfect.exe 파일은 32 비트 버전과 64 비트 버전이 존재한다.

32비트 버전(md5: 8a3a6faf42201033ae0c0c57d47a58f9)이 실행되면 [그림 13]과 같이 'PE File Infector V1.0 Built 2014/10/31 By WinEggDrop'이 출력된다. 변형에 따라 날짜는 바뀔 수 있다.

```
c:\work>iatinfect.exe
PE File Infector V1.0 Built 2014/10/31 By WinEggDrop
```

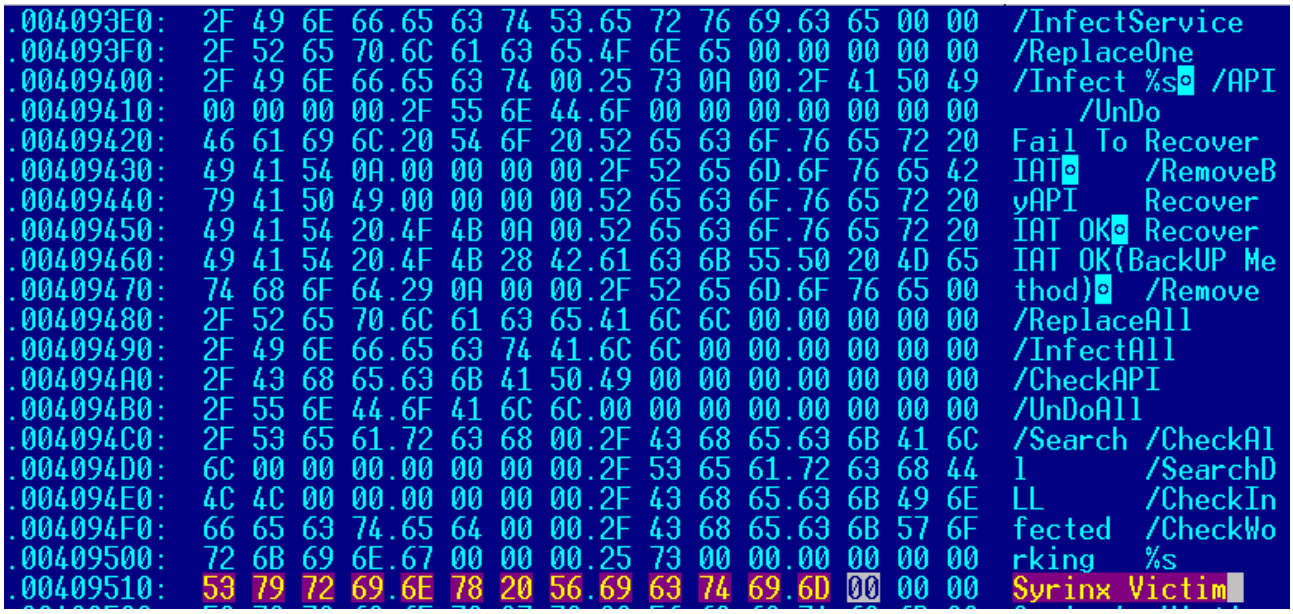
[그림 13] 32 비트 iatinfect.exe 실행

64비트 버전(md5: 9e0859b29641c9300058a2686daa1b06)이 실행되면 [그림 14]에서 볼 수 있듯이 'PE File Infector X64 V1.0 Built 2014/09/24 By WinEggDrop'이 출력된다.

```
c:\work>iatinfect.exe
PE File Infector X64 V1.0 Built 2014/09/24 By WinEggDrop
```

[그림 14] 64 비트 iatinfect.exe 실행

제작자 이름은 다른 악성코드도 제작한 윈에그드롭(WinEggDrop)이지만 파일 내부에는 다른 제작자의 별명인 시링크스(Syrinx)도 포함되어 있다. 전체 도구는 윈에그드롭이 제작하고 PE 파일 감염 부분은 시링크스가 제작했을 가능성이 높다.

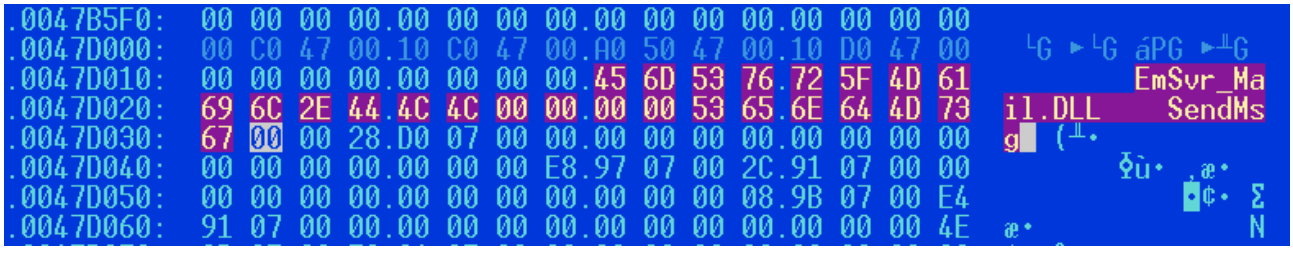


[그림 15] iatinfect.exe 파일 내 특징적 문자열

iatinfect.exe로 패치된 파일은 파일 헤더 내에 '시링크스의 희생자(Syrinx's Victim)'라는 문자열이 추가된다.

[그림 16] iatinfect.exe에 패치 된 파일

변조된 EXE 파일이 실행되면 지정된 악성코드 DLL 파일과 실행 함수(보통 NTPacket, SendMsg, Shadow Force 등)로 악성코드를 실행한다.



[그림 17] 패치 된 파일 내 로딩할 DLL 파일

변조된 EXE 파일이 실행될 때만 악성코드가 실행되므로 공격자는 사용자가 신뢰하는 프로그램을 주로

패치한다. 공격자의 변조가 확인된 파일은 EmSvr_Mail.exe(오류 발생시 메일 전송 프로그램), NCleanService.exe, UBiz5.exe, vivaldiframework.exe(Megaraid Storage Manager) 등으로 관리 프로그램이나 메신저 프로그램 등이 주요 목표이다.

3) Loader

공격자는 iatinfect.exe를 이용해 기존 실행 파일을 변조해 로더 역할을 하게 하는 방법 외에도 2018년에는 악성코드를 로딩하는 로더를 사용했다. 단, 관련 변형은 2017년 말에도 발견(md5: a1cd7d68d4f52d987db8ee8f1ce8c38c) 되었지만 이 그룹과의 연관성을 아직 찾지 못했다.

2018년 4월 공격에 사용된 로더 A형(md5: 7b329a6bcdc15cff1eb3c5bd31176b2c)은 _XblAuthManagerProxy.xml에서 실행에 필요한 코드를 읽어 실행한다. _XblAuthManagerProxy.xml 파일이 확인되지 않아 어떤 코드가 실행되는지는 확인하지 못했다.

```
v2 = CreateFileW(L"_XblAuthManagerProxy.xml", 0x80000000, 1u, 0i64, 3u, 0, 0i64);
v3 = v2;
if ( v2 != (HANDLE)-1i64 )
{
  v4 = GetFileSize(v2, 0i64);
  v5 = v4;
  v2 = VirtualAlloc(0i64, v4, 0x3000u, 0x40u);
  v1 = (DWORD (__stdcall *)(LPVOID))v2;
  if ( v2 )
  {
    NumberOfBytesRead = 0;
    LODWORD(v2) = ReadFile(v3, v2, v5, &NumberOfBytesRead, 0i64);
    if ( NumberOfBytesRead == v5 )
    {
      v2 = CreateThread(0i64, 0i64, v1, 0i64, 0, 0i64);
      if ( v2 )
      {
        LODWORD(v2) = CloseHandle(v2);
        v0 = 1;
      }
```

[그림 18] Loader A 형

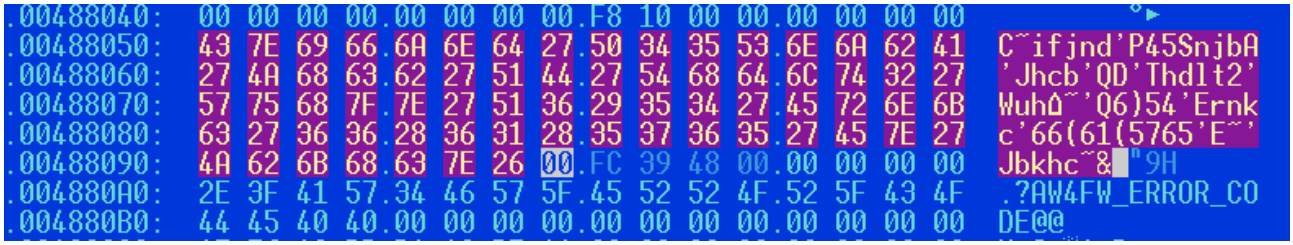
로더(Loader) B 형은 2018년 4월에 발견(md5: 442d63fba7f549d416e624d67ddc03c9)되었으며, C:₩ProgramData₩Microsoft₩Crypto₩DSS₩MachineKeys₩f686aace6942fb7f7ceb231212eef4b4.dat 파일에서 데이터를 읽어 메모리에서 실행한다. 역시 이 파일을 확보하지 못해 어떤 코드가 실행되는지 확인할 수가 없었다.

4) Backdoor - Wgdrop

Wg드롭(Wgdrop)의 변형은 2013년 3월부터 2015년 12월까지 32개가 발견되었다.

초기 버전은 EXE 형태로 2013년에 발견되었지만, 2012년 11월에 제작된 것으로 보이는 파일(9552c356950daf907f30da1ca2dcb755)도 있어 2012년부터 제작되었을 가능성이 높다. 파일 이름은 Sqlserver.exe, wmipsrv.exe, inetinfo.exe, w32timef.exe 등이며 파일 길이는 591,192 바이트 ~ 646,656 바이트로 총 17개 변형이 발견되었다.

Wg드롭의 변형은 특징적으로 문자열이 0x0F 키 값으로 XOR 연산된 후 암호화 되었다.



[그림 19] XOR로 암호화 된 문자열

암호를 풀어보면 [그림 20]과 같이 'Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 11/16/2012 By Melody!'와 유사한 문자열을 확인할 수 있다.

[그림 20] 암호화 되어 있는 문자열

현재까지 확인된 악성코드 정보 문자열은 [표 3]과 같다.

암호 해제 후 문자열
Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 10/14/2012 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 04/19/2014 By Melody!

Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 09/16/2014 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 10/22/2014 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 11/16/2012 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 12/05/2014 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 12/16/2013 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy X64 V1.23 Build 04/19/2014 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy X64 V1.23 Build 10/22/2014 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy X64 V1.23 Build 11/01/2013 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy X64 V1.23 Build 12/05/2014 By Melody!
Dynamic W32TimeF Mode VC Socks5 Proxy X64 V1.23 Build 12/16/2013 By Melody!

[표 3] Wg드롭(Wgdrop)의 암호화 문자열

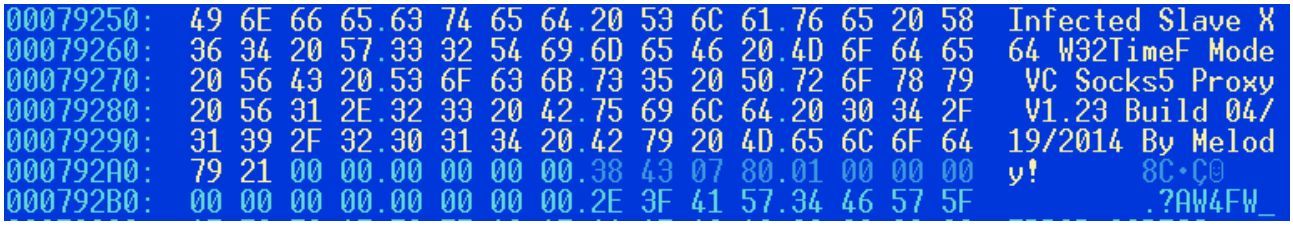
2014년에 제작된 초기 버전 (md5: 954122ca75a556f3059b14fe11002f71)에는 제작자의 존재를 유추할 수 있는 문자열('Programmed By Syrinx', 'Syrinx Software Solutions' 등)이 존재한다.

```
BLOCK "040904b0"
{
        VALUE "Comments", "Programmed By Syrinx"
        VALUE "CompanyName", "Syrinx Software Solutions"
        VALUE "FileDescription", "Networking Application"
        VALUE "FileVersion", "1, 2, 3, 0"
        VALUE "InternalName", "NetworkServer"
        VALUE "LegalCopyright", "Copyright (C) 2005"
        VALUE "LegalTrademarks", "www.SyrinxInc.com"
        VALUE "OriginalFilename", "NetworkServer.EXE"
        VALUE "PrivateBuild", "Version 1.23"
        VALUE "ProductName", "Network Application"
        VALUE "ProductVersion", "1, 2, 3, 0"
        VALUE "SpecialBuild", ""
}
```

[그림 21] 버전 정보에 존재하는 제작자

Wg드롭은 2014년 봄부터는 DLL 형태(md5: 7e746a804afc65cf95b8c346c2ee0ca3)로 변경되었으며, 15개의 변형이 발견되었다.

역시 XOR 0x07로 암호화 된 악성코드 버전과 제작 날짜 등의 문자열이 저장되어 있다. 암호를 풀면 'Infected Slave X64 W32TimeF Mode VC Socks5 Proxy V1.23 Build 04/19/2014 By Melody!' 와 유사한 문자열을 볼 수 있다.



[그림 22] Wg드롭(Wgdrop) DLL형의 숨겨진 문자열

현재까지 확인된 Wg드롭(Wgdrop) DLL형의 악성코드 정보 문자열은 [표 4]와 같다.

암호 해제 후 문자열
Infected Slave W32TimeF Mode VC Socks5 Proxy V1.23 Build 02/20/2014 By Melody!
Infected Slave W32TimeF Mode VC Socks5 Proxy V1.23 Build 04/19/2014 By Melody!
Infected Slave W32TimeF Mode VC Socks5 Proxy V1.23 Build 09/16/2014 By Melody!
Infected Slave W32TimeF Mode VC Socks5 Proxy V1.23 Build 12/05/2014 By Melody!
Infected Slave X64 W32TimeF Mode VC Socks5 Proxy V1.23 Build 04/19/2014 By Melody!
Infected Slave X64 W32TimeF Mode VC Socks5 Proxy V1.23 Build 09/16/2014 By Melody!
Infected Slave X64 W32TimeF Mode VC Socks5 Proxy V1.23 Build 09/23/2014 By Melody!
Infected Slave X64 W32TimeF Mode VC Socks5 Proxy V1.23 Build 12/05/2014 By Melody!

[표 4] Wgdrop DLL 버전의 암호화 문자열

공격자는 2015년 이후에는 Wg드롭 변형을 사용하지 않는다.

5) Backdoor - Shadow Force

공격자는 2014년부터 Wg드롭을 대신해 섀도 포스(Shadow Force) 악성코드를 사용한다. 섀도 포스는 트렌드마이크로가 2015년에 관련 정보를 공개하면서 처음 알려졌다. 2014년 9월에 최초 버전이 제작된 것으로 보이며 2020년 3월에도 변형이 발견되었다.

섀도 포스는 Wg드롭(Wgdrop)과는 다르게 문자열이 암호화 되어 있지 않아 [그림 23]과 같이 특징적인 문자열(예; Welcome To Shadow Force)을 볼 수 있다.

[그림 23] 샤도 포스 특징적 문자열

샤도 포스는 23개 이상의 변형이 확인되었으며 현재까지 확인된 특징적 문자열은 [표 5]와 같다.

문자열
Shadow Force(DLL Free Version) X64 V1.0 Build 2014/09/16 By WinEggDrop
Shadow Force(DLL Free Version) X64 V1.0 Build 2014/09/17 By WinEggDrop
Shadow Force(DLL Free Version) X64 V1.0 Build 2014/09/23 By WinEggDrop
Shadow Force(DLL Free Version) X64 V1.0 Build 2014/10/22 By WinEggDrop
Shadow Force(DLL Free Version) X64 V1.0 Build 2016/12/30
Welcome To Shadow Force DLL X32 V1.0 Build 2014/09/18
Welcome To Shadow Force DLL X32 V1.0 Build 2014/10/22
Welcome To Shadow Force DLL X32 V1.0 Build 2015/06/11
Welcome To Shadow Force DLL X64 V1.0 Build 2014/09/18
Welcome To Shadow Force DLL X64 V1.0 Build 2014/10/22
Welcome To Shadow Force DLL X64 V1.0 Build 2015/06/10
Welcome To Shadow Force DLL X64 V1.0 Build 2020/02/29

[표 5] 샤도 포스 변형에서 발견된 문자열

제작자는 자신을 윈에그드롭(WinEggDrop)으로 부르며 일부 변형에는 제작자 이름이 없다.

6) Backdoor - Dnsdoo

Dnsdoo는 2014년~2015년 수집된 악성코드로 3개의 변형만 확인되었으며 파일 이름은 dns.exe이다. 특

징적으로 'DNS Door X64 V1.0 Built 2013/11/10 By WinEggDrop' 와 같은 문자열을 포함하고 있다([그림 24] 참고).

[그림 24] Dnsdoo의 특징적 문자열

문자열
DNS Door X64 V1.0 Built 2013/11/10 By WinEggDrop
DNS Door X64 V1.0 Built 2014/01/09 By WinEggDrop

[표 6] Dnsdoo에서 발견된 문자열

Dnsdoo가 실행되면 IP 주소 208.67.222.220 (미국)로 접속해 명령을 받고 명령 프롬프트 (CMD.exe)를 통해 원격에서 시스템을 관리 할 수 있다.

7) Stealer - Recakey

2018년 침해를 당한 시스템에서 화면 녹화 및 키로깅 기능을 가진 도구(md5: (e94d2ac3dd6f315e32960583be42d2ce)가 발견되었다. 파일 이름은 Linkinfo.dll이며 399,984바이트이다. Linkinfo.dll의 리소스 영역에 RAR 3.80 콘솔 파일이 저장되어 있다.

공격자는 녹화된 동영상이나 유출할 정보의 파일 길이를 줄이기 위해 압축 프로그램인 RAR 콘솔 3.80 버전을 시스템에 생성한다.

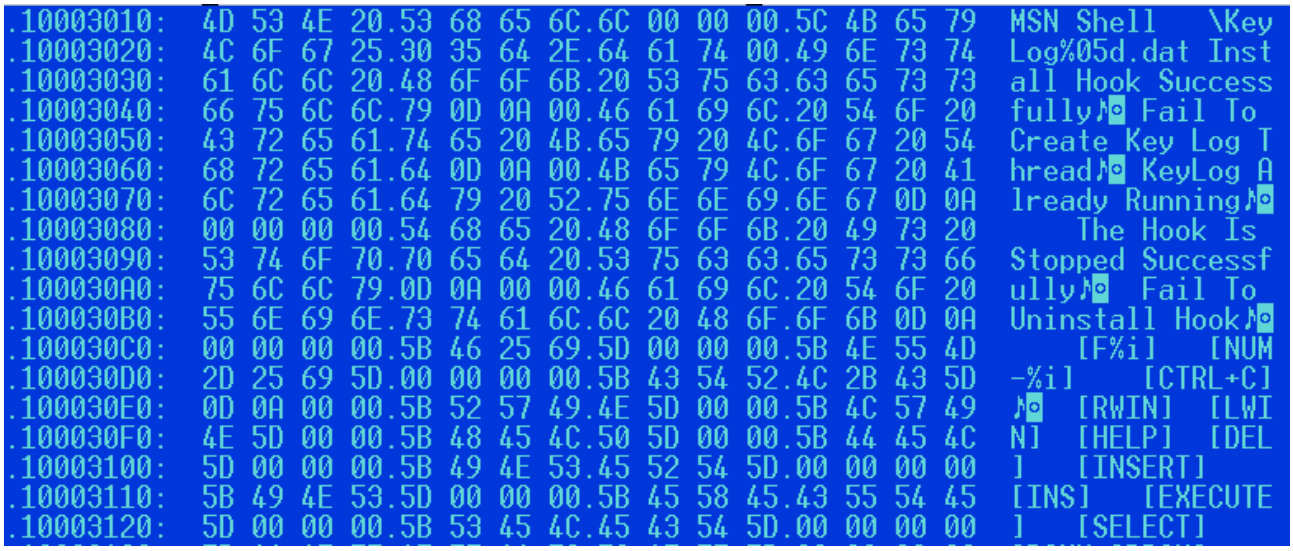
[그림 25] Recakey 악성코드 리소스 영역에 포함된 RAR 3.80 버전

Recakey 초기 버전은 2011년 3월부터 발견(md5: 5d3419c5a08e830b0be854540ac12e61)되었다. 초기 버전은 RAR 콘솔 파일 생성과 화면 동영상 저장 기능만 있었지만 이 그룹에서 사용한 2018년 버전은 64 비트이며 키로깅 기능도 추가되었다.

8) Tool - Keylogger

2019년에 피해를 입은 시스템에서는 여러 개의 키로거가 발견되었다.

이 가운데 RDPClient.dll (md5 : 359f09a1313e79aebf93bf3109e7afd9)은 9,728 바이트 길이를 가진다.



[그림 26] 키로거 문자열

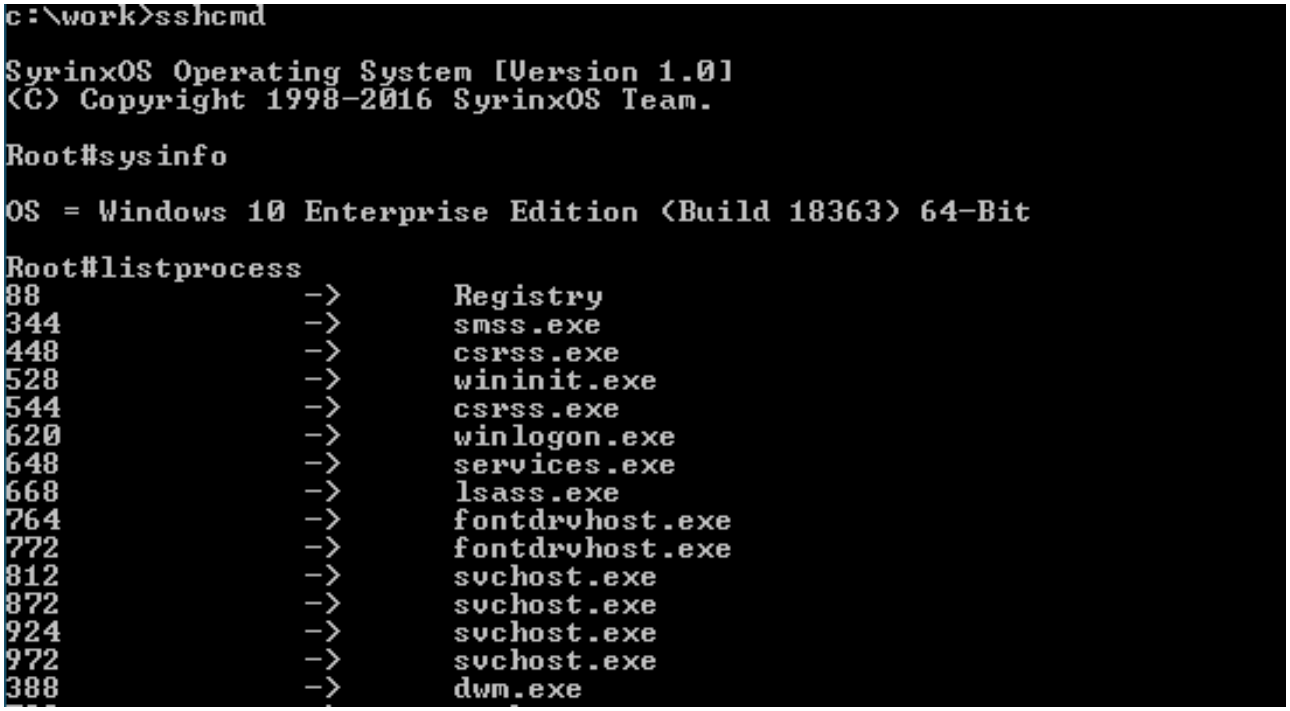
KeyLog.dll (md5: 06961fa526d26403f1d894fdf45346a5)은 62,464 바이트 길이이며, [그림 26]과 같이 PDB 정보'F:₩Source₩KeyLogInfect₩Release₩KeyLog.pdb'를 포함하고 있다.

[그림 27] 키로거에 포함된 특징적 PDB 정보

9) Tools - SSHCMD

sshcmd.exe 파일은 2019년 11월 처음 발견된 이후 2020년 3월에도 발견되었으며, 29,696바이트 ~ 42,160바이트의 길이를 가진다. UPX로 패킹되어 있고 이 파일은 SSHService.dll (b3473d03ad4b17aba64fd5894707bb88) 파일 내 리소스 영역에 존재해 SSHService.dll가 sshcmd.exe 파일을 생성할 것으로 예상된다.

SSHCMD는 시스템 정보, 프로세스 리스트 얻기, 파일 실행 등의 기능을 지원한다. 실행되면 [그림 28]과 같은 문자열(SyrinxOS Operating System [Version 1.0] (C) Copyright 1998-2016 SyrinxOS Team.)이 출력된다.

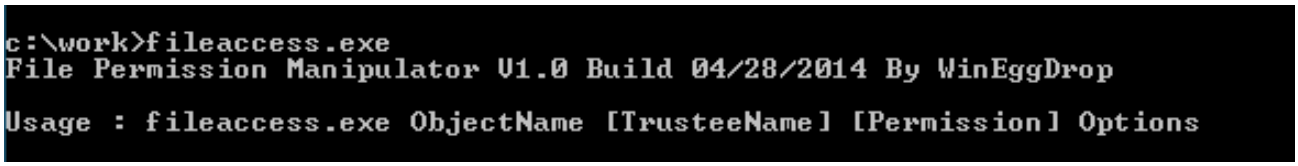


[그림 28] SSHCMD 실행 화면

10) 기타 도구

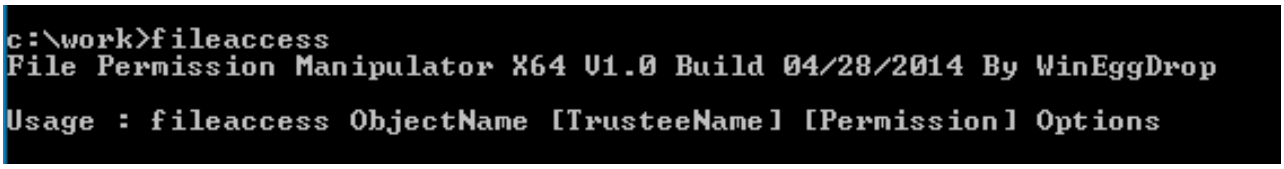
침해 당한 시스템에서 수집된 파일을 분석하면서 공격자가 사용한 여러 도구를 확인할 수 있었다. 많은 공격자는 이미 알려진 도구를 사용하지만 이 그룹은 파일, 프로세스, 서비스, 스캐너 등 해킹에 도움이 되는 여러 도구를 제작해 사용하고 있다. 도구 중 상당수는 제작자 중 한명인 윈에그드롭(WinEggDrop)의 문자열을 포함하고 있다.

Fileaccess.exe는 파일 권한 관리 프로그램이다. 32비트 파일(md5: 98f16c758c32be9e4a84c4d28e86d2ca)을 실행하면 [그림 29]와 같은 문자열(File Permission Manipulator V1.0 Build 04/28/2014 By WinEggDrop)이 출력된다.



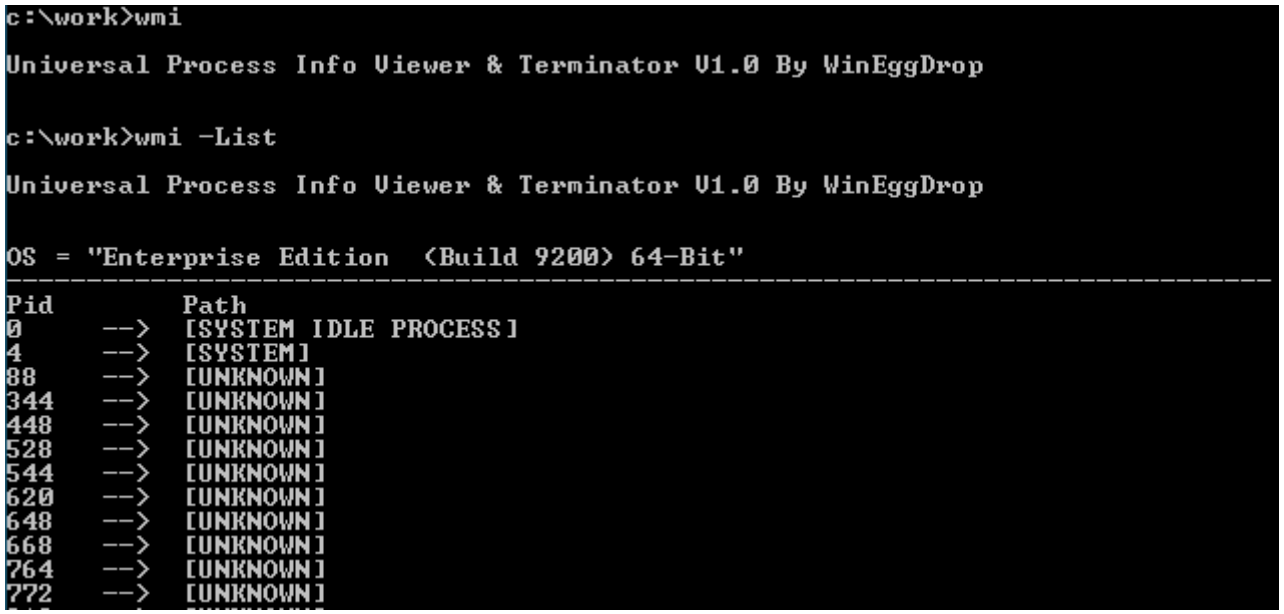
[그림 29] 32비트 fileaccess.exe 실행

64 비트 파일(md5: de2e9e0f0cffa180a3d7f5480e6b32c1)을 실행하면 [그림 30]과 같은 문자열(File Permission Manipulator X64 V1.0 Build 04/28/2014 By WinEggDrop)을 출력한다.



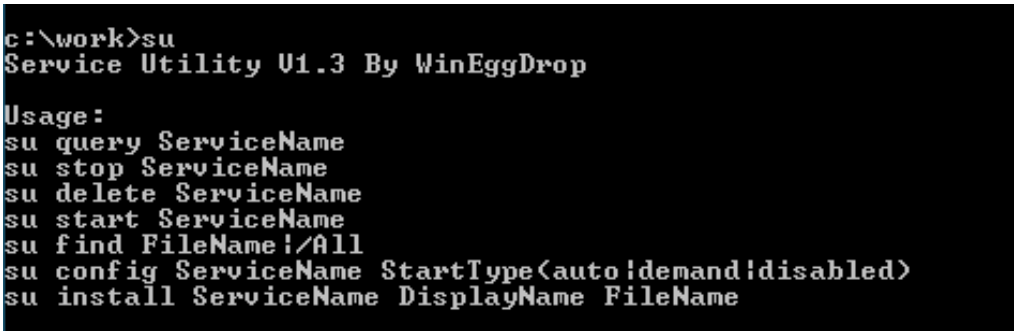
[그림 30] 64 비트 fileaccess.exe 실행

wmi.exe(md5: d9e5adb8d6364503d9f2b699fadee76e)는 프로세스 도구이며 2014년에 처음 발견되었다. 파일을 실행하면 [그림 31]과 같은 문자열(Universal Process Info Viewer & Terminator V1.0 By WinEggDrop)을 출력한다.



[그림 31] Wmi.exe 실행

su.exe(md5: 3628dd6edb9fd82bbc6ca26784e8cc70)는 서비스 관리 도구로 2014년 해킹에 사용되었다. 파일을 실행하면 [그림 32]와 같은 문자열(Service Utility V1.3 By WinEggDrop)을 출력한다.



[그림 32] Su.exe 실행

해당 도구의 초기 버전은 2008년에도 발견(md5: 2aa042c7ecb547a6e24e9a3842dae0b9)되었다.

scanipc.exe(md5: 9593a18550786fbcc281469ebfb23966)는 IPC(Inter-Process Communication) 스캐너로 실행하면 [그림 33]과 같은 문자열(IPC Scanner V1.0 Build 08/10/2005 By WinEggDrop)을 출력한다.

[그림 33] scanipc.exe 실행

el.exe (md5: 9252efea5e5d6d1c8bd0474b80c81ead)은 2018년에 제작되었으며 이벤트 로그 삭제 프로그램으로 실행되면 [그림 34]와 같은 문자열(EventLog Eraser V1.0 Build 04/27/2018)을 출력한다. 유출된 한국 게임 개발 업체 인증서로 서명되어 있다.

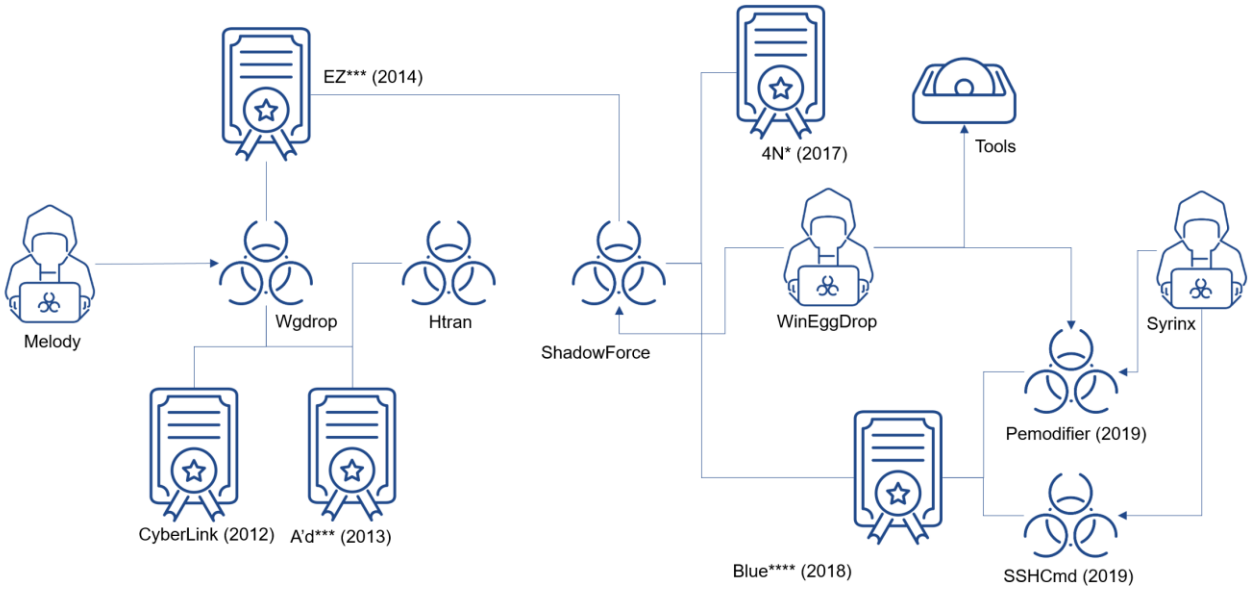
[그림 34] el.exe 실행

이외에도 아직 확인되지 않은 다수의 해킹 도구가 존재할 것으로 예상된다.

연관 관계 분석

관련 악성코드를 분석하면 제작자인 멜로디(Melody), 시링크스(Syrinx), 윈에그드롭(WinEggDrop)을 계속 볼 수 있다. 트렌드 마이크로 보고서에 따르면 윈에그드롭은 1982년에 태어난 중국인이라고 한다. 이들 제작자들이 한 명인지 여러 명인지 악성코드만 제작하는지 해킹에도 가담하는 지에 대한 정보를 확인 할 수 없다. 특히 윈에그드롭이 제작한 도구 중 일부는 인터넷에 공개되어 있어 누구나 사용할 수 있다.

악성코드, 인증서, 제작자 정보를 통한 연관성을 정리하면 다음과 같다.



[그림 35] 오퍼레이션 섀도 포스의 악성코드, 인증서, 제작자 연관 관계

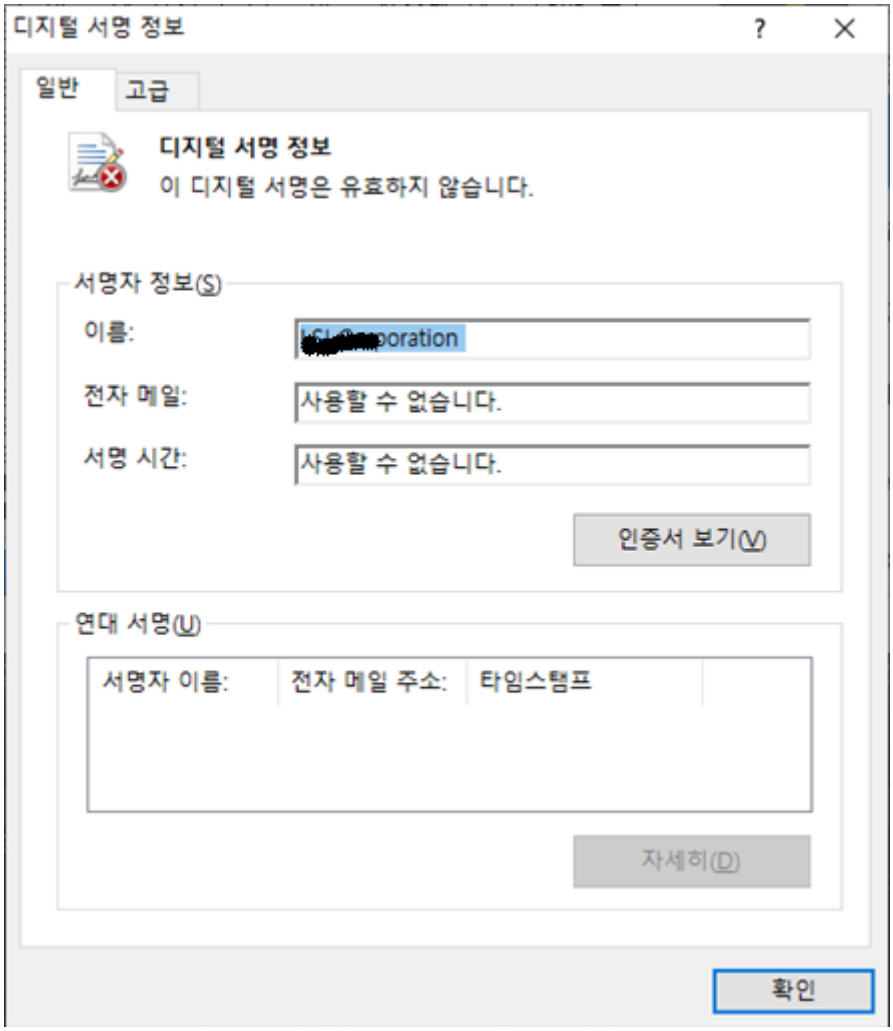
여러 악성코드가 동일한 디지털 인증서로 서명되어 있다. 하지만, 단순히 동일한 인증서로 서명되어 있어도 동일 그룹의 소행으로 단정하기 어렵다. 하지만, 이 공격자는 aio.exe 파일을 이용해 파일을 다운로드하고 iatinfect.exe 파일을 이용해 시스템의 파일을 패치해 DLL을 로딩하고 하고 유사한 백도어를 사용한다. 감염된 시스템에서 이들 파일의 흔적이 중요한 단서이다.

공격자는 주기적으로 악성코드를 변경하고 있지만 현재까지 aio.exe 파일로 악성코드를 다운로드하고 iatinfect.exe 파일을 이용해 정상 파일을 변조하는 공격 방식은 유지하고 있다.

의심 증상

공격자가 시스템에 존재하는 파일을 다운로드 할 때 aio.exe를 사용하고 변조할 때 사용한 도구는 iatinfect.exe 파일 이름이다. 따라서, aio.exe나 iatinfect.exe 파일이 발견된다면 이 그룹의 공격을 받았을 가능성이 높다.

공격자들은 정상 프로그램을 패치해서 악성코드를 로드하는 기법을 사용하고 있다. 따라서 인증서로 서명된 파일은 파일이 변조되어 인증서가 유효하지 않게 된다([그림 36] 참고). 지금까지 잘 사용하던 프로그램의 디지털 서명 정보가 유효하지 않을 때는 파일 변조를 의심해 볼 수 있다.



[그림 36] 파일이 패치되어 유효하지 않은 인증서

특히 EXE 파일에 '시링크스의 피해자(Syrinx's Victim)'라는 문자열이 존재한다면 변조된 파일일 가능성이 높다. 또한 멜로디((Melody), 시링크스(Syrinx), 윈에그드롭(WinEggDrop)이 제작한 커맨드라인 프로그램이 존재하거나 RAR 3.80 콘솔 프로그램이 존재해도 오페레이션 섀도 포스를 수행한 위협 그룹임을 의심해 볼 수 있다.

안랩 대응 현황

안랩 제품군의 진단명과 엔진 날짜 정보는 다음과 같다.

Dropper/Win32.Sshcmd (2020.03.25.06)
Dropper/Win64.Shadowforce (2020.02.25.00)
HackTool/Win32.Hackhelper (2020.03.24.00)
HackTool/Win32.Htran (2020.03.22.01)
HackTool/Win32.Pemodifier (2020.03.24.00)
HackTool/Win32.Scanner (2020.03.25.06)
HackTool/Win32.Sshcmd (2020.03.24.08)
Trojan/Win32.Dnsdoo (2020.02.25.00)
Trojan/Win32.Keylogger (2020.02.05.00)
Trojan/Win32.LogEraser (2020.02.04.00)
Trojan/Win32.Shadowforce (2020.03.19.08)
Trojan/Win32.Wgdrop (2020.03.19.07)
Trojan/Win64.Loader (2020.02.12.07)
Trojan/Win64.Recakey (2020.03.23.08)
Trojan/Win64.Shadowforce (2020.02.24.07)
Trojan/Win64.Wgdrop (2020.03.19.08)

결론

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 활동했다는 점에서도 그들의 은밀함에 놀랍기도 하지만 알려지지 않은 다른 그룹이 분명 존재한다고 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 오퍼레이션 섀도 포스를 소개한 이유는 여기에 공개된 IOC 정보를 바탕으로 의심스러운 침해 행위를 조기에 탐지하고 관련 업계와 협력해 남은 의문점을 함께 풀어가고자 함이다.

IoC (Indicators of Compromise)

주요 샘플 파일명

공격자가 즐겨 사용하는 파일이름은 다음과 같다.

aio.exe

iatinfect.exe

oci.dll

Shadow Force.dll

Shadow Forcex64.dll

Shadow Forcex64.exe

sqlserver.exe

sqlwriter.dll

SSHCMD.exe

SSHService.dll

wmipsrv.exe

Hashes (md5)

관련 악성코드와 도구의 MD5는 다음과 같다.

06961fa526d26403f1d894fdf45346a5

07a390809ba4f8e4d0b213e9f9a88252

106ec8522b99ca3988ce28d7bfaa0be9

14be4db47ce4df850a73b2288bcebb42

16ee57322ba3665190f3e2ebd279f388

1a61e13d0a3bc1be5fbbc9355720fce8

1a6f757077149a565a6c97774f845e31

1dc845c8e471c3268a978b96ebcd7ff3

1fd5d459f198bda20399f0e76ce64f8e

206dab5720739ee0672a126008849077

21a7c711b29f2a3c8ac56414b0806a09

265e050268d764290bda44eb5c19305d
27f9d07af5674e6454fb2f0072847d4c
2d3f7f8efc41f4228f58b60e560173fb
3104658447dda998f7b8763bea13a2c3
359f09a1313e79aebf93bf3109e7afd9
3628dd6edb9fd82bbc6ca26784e8cc70
377bc414954e497f375ed5ce28afc0e7
3c6d671ea39665ae39b9736e73a6c761
3cea83681d97f96c9af684b1240c05a1
442d63fba7f549d416e624d67ddc03c9
44aaa2ec4ab02bb86a39dc72394471a4
4682cd461e28a5b8f7337395b9415148
4b1c711492765dec050228249225cd1d
4b85e5f3de90c6fad664a7c6f422933b
4e32573490486c43494a5eb1be0b2f0b
5408579f20d1dc533857cbbc114323d3
56b741d2ba4c92c8d60ab741db87347a
5c87878df4a39edf6a4a0e5aa03a7dd0
6aaa1d3f8c136f47a35137c663c759b7
6b59d85a86c5e85aa5c4cab36be0d6e2
6c2ce4e256b8f94f09937395de17df49
6d82306d4e101a04166156fa5b8b82cc
6f0e62b15efd2b2468ef37c138eb189a
786a8e3cbaa3c024c8dfd72d48379b83
7b329a6bcdc15cff1eb3c5bd31176b2c
7ca25a11789653befdaa9c3b9cfb8c8d
7d01fa33c33454e69bebf65a8313149c
7e746a804afc65cf95b8c346c2ee0ca3
856288812c8bba908d775a8f2ccafc5c
85b07042480a6d65f530ec4a2b93448b
8a3a6faf42201033ae0c0c57d47a58f9
8c446777ea3a31ac9b5cf27388b86275
8e7fc200d31947d49568a99edb8fbcfb
91be8058844fc0bb5af8d8b5fef5990e
9218312612eb448f089daa888f924796

9252efea5e5d6d1c8bd0474b80c81ead
934de0ba37da38d01ce3b957f04d96e4
94cdd87eba7302f875d0d16486608f20
954122ca75a556f3059b14fe11002f71
9552c356950daf907f30da1ca2dcb755
9593a18550786fbcc281469ebfb23966
96a3032a30eda25d3cd223a61ee8cfc2
970f58c2ddcf5f2cf789ba4288bd3e40
98f16c758c32be9e4a84c4d28e86d2ca
9e0859b29641c9300058a2686daa1b06
9fe571b36f14e232690951643981011c
a0aa1ae65d415db9a57f1ee965909184
a1cd7d68d4f52d987db8ee8f1ce8c38c
a3440c605ceecfba560e33f167530d9b
a952b2cd5661c94ed7f13a88f8c41ee7
afbb63cb341948fb6d7c57fb7c9993e2
b070f96f08e4947dbf725b80f5c51af3
b0a834a822b0d3b581a25e48f5ca49d3
b285fbc36a8fcb0122346a0d17327015
b3473d03ad4b17aba64fd5894707bb88
b60313da17608261071ef8d4b18db478
b78d4156bfe66a3ceecb2621c7f53145
b930b3c37623946cb06127c1ed0826ce
c22b29fcaac4b583a27693d0f72f617a
c41297dc4459759f0c008366497b3eab
c412a98126491231e7475982e749ee7d
c9af6c6c231bed20ef972e78dd7ee7cc
cb3d14b0b720fa583ebdbe7b090f4adc
cf241076fa7d20ded95935db6572aff2
cf336c998bc7c162c2b5fbb1cf98678d
cfb177aa024dfd1ab85a331a8eabca95
d014027b15e3f5099676e423131ef805
d4b055e92cc9b576655a3eccd1643da7
d5116ee172fc2b7919f9d32fe5b66b87
d9e5adb8d6364503d9f2b699fadee76e

dbfc63ea67e3d70bfe3d3036b59f4048
dd3232e2924ae6a11c393c27713d5873
de2e9e0f0cffa180a3d7f5480e6b32c1
e41bf0f72e6e1dfb4bd86a2770a590ad
e4b0d1942064d644e7bd65fca8508c21
e52dddabd40783032e85fe1076db2c6c
e679553339a07ee65c1b46e573dae6ec
e8ba1ca369f06c286cee88c9ebc22af9
e94d2ac3dd6f315e32960583be42d2ce
ebf60f405feb83e41e6324eac5e41b33
ece7bd4a77ee66ce0b7cd5437dcb1185
f23bf5c35273927979ea47413a141a05
f57e577822b6aaac5b9dfd9e464d4694
f5eb4f51f0e8a96d39ba2ab3e4890b4f
f940d717a32ee34db39283deda9453f5
fcd695fa1cd04b23697b2e4fdd2d557b
fd21014271160555e3b4b79f2670b8d5

관련 도메인, URL 및 IP 주소

다운로드 및 C&C 주소 (http를 hxxp로 변경)
208.67.222.220
hxxp://112.222.131.21/aio.exe
hxxp://112.222.131.21/iatinfect.exe
hxxp://112.222.131.21/iatinfect2008.exe
hxxp://112.222.131.21/iatinfect64.exe
hxxp://112.222.131.21/iland.dat
hxxp://112.222.131.21/infectsocks.dll
hxxp://112.222.131.21/infectsocks2010.dll
hxxp://112.222.131.21/JuicyPotato64.exe
hxxp://112.222.131.21/ndisinstaller.exe
hxxp://112.222.131.21/readpwd32.exe
hxxp://112.222.131.21/Shadow Force.dll
hxxp://112.222.131.21/Shadow Forcex64.dll

hxxp://112.222.131.21/sshd.dat

hxxp://112.222.131.21/sshservice.dll

hxxp://112.222.131.21/su.exe

hxxp://112.222.131.21/su.vmp.exe

※ 참고 문헌 (References)

[1] Shadow Force Uses DLL Hijacking, Targets South Korean Company (https://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company/)