금성121 그룹의 최신 APT 캠페인 - '작전명 로켓 맨(Operation Rocket Man)'

By 알약(Alyac)

Published: 2018-08-22 · Archived: 2026-04-06 00:58:50 UTC

1. 금성121, 최신 APT 캠페인 '작전명 로켓 맨(Operation Rocket Man)'

안녕하세요? 이스트시큐리티 사이버 위협 인텔리전스(CTI) 전문조직인 시큐리티대응센터 (이하 ESRC)입니다.

ESRC에서는 지난 03월 20일 미디어를 통해 대북 단체 및 국방분야를 주요 공격 대상으로 사이버 침투활동을 전개해 온 정부지원 APT 위협그룹 금성121(Geumseong121) 조직이 안드로이드 기반 모바일 스피어피싱(Spear Phishing)공격까지 수행함을 공개한 바 있습니다.

그리고 07월 04일에는 남북이산가족찾기 전수조사 내용으로 사칭한 스피어피싱 이메일 주의를 안내해 드린 바도 있습니다.

[그림 1] 금성121 그룹의 공격 벡터 사례

베일에 쌓여있는 공격자들은 CVE-2018-4878 0-Day 취약점을 카카오톡 메신저로 유포한 바 있고, 악성 HWP 문서를 활용해 은밀한 표적공격도 수차례 시도했습니다.

지난 03월에 발견된 모바일 스피어 피싱(APK)의 경우에는 '불법' 대신 '비법'이라는 표현이 포함된 상태로 악성 APK 악성앱이 유포되었습니다.

금성121 그룹은 특정 정부가 배후에서 지원할 것으로 믿고있는 국가기반 사이버 군대조직으로 한국의 대표 포털사에서 개발한 모바일 백신 앱으로 위장한 공격을 수행했었고, 이와 관련된 악성앱 (Trojan.Android.Fakeav)에 대한 상세한 분석정보를 포스팅 하기도 했었습니다.

[그림 2] 모바일 보안앱 설치로 위장한 악성앱(APK) 설치 유도 화면

추후 이 내용은 Cisco Talos, Paloalto Unit 42 보안 블로그의 포스팅을 통해 추가 위협 사례들이 자세히 공개된 바 있었습니다.

ESRC에서 다년간 조사한 결과 이 공격그룹은 2013년 전후부터 한국 등을 상대로 수년간 지속적으로 사이버 캠페인을 수행해 왔으며, 주요 위협 벡터로는 워터링 홀(Watering Hole), 스피어 피싱(Spear Phishing), 소셜 네트워크 피싱(Social Network Phishing), 토렌트 피싱(Torrent Phishing) 공격 등을 사용하고 있습니다.

이런 가운데 2018년 08월 한국의 특정 대상을 겨냥한 최신 스피어 피싱이 추가로 발견되었는데, 이 공격을 분석하던 중 몇 가지 흥미로운 사실을 발견하기도 했습니다. 또한, 공격자는 한국의 기업 인사담당자로 위장해 공격을 수행했습니다.

아래는 실제 공격에 사용된 침해지표(IoC) 자료들로 ESRC에서는 한국인터넷진흥원(KISA)에 해당 내용을 신속히 공유해 유포를 조기에 차단시킨 상태입니다.

- http://m.ssbw.co.kr/admin/form_doc/image/down/down[.]php (MD5 : af6721145079a05da53c8d0f3656c65c)

- http://m.ssbw.co.kr/admin/form_doc/image/down/worldnews[.]doc (MD5 :1213e5a0be1fbd9a7103ab08fe8ea5cb)

- http://m.ssbw.co.kr/admin/form_doc/image/img/111[.]hwp (MD5 : edc1bdb2d70e36891826fdd58682b6c4)

- http://m.ssbw.co.kr/admin/form_doc/image/img/Ant_3.5[.]exe (MD5 : b710e5a4ca00a52f6297a3cc7190393a)

- http://m.ssbw.co.kr/admin/form_doc/image/img/desktops[.]ini (MD5 : 05eef00de73498167b2d7ebdc492c429)

금성121 위협그룹이 사용하는 스피어 피싱 전략에는 나름의 고유한 특징이 존재하는데, 직접적인 감염 유도(Lure, Decoy)파일을 첨부하는 대신에 해킹한 한국의 웹 사이트 주소를 추가하고, 마치 첨부된 파일처럼 이미지로 교묘히 위장하는 수법입니다.

이들도 정교한 한글을 사용하지만, 간혹 지리적 언어 표현에 미묘한 차이가 존재하는 경우가 목격됩니다. 이러한 접근 방법론은 공격자의 언어 구사력을 기반해 지역적 특색을 분석하는데 활용되며, 해당 언어를 제대로 이해할 수 있는 분석가를 통해 보다 심층적 데이터로 접근하게 됩니다.

더불어 공격에 이용된 다양한 메타 데이터는 과거에 수행된 흔적들과 침해사고 연관성 지표에 핵심단서로 활용이 되고 있습니다.

이번 8월에 새롭게 발견된 공격은 지난 3월 공격과 마찬가지로 한국의 보안프로그램 처럼 아이콘을 위장하였는데, 이번에는 모바일 보안이 아닌 PC용 보안 프로그램으로 위장한 것이 특징입니다.

[그림 3] 보안 프로그램으로 위장한 공격 흐름도

공격 벡터에 따라 보안 프로그램으로 위장한 악성코드는 여러 단계를 거쳐 추가 파일을 설치하게 되는데, 닷넷 버전별로 선택적인 명령을 수행하게 됩니다.

닷넷 기반으로 유포된 악성파일에는 'Ant.pdb' 라는 빌드 데이터를 볼 수 있습니다. 특히, 공격자는 '로켓(Rocket)'이라는 프로젝트 폴더에서 악성파일 변종 시리즈를 지속적으로 제작하고 있는 것을 알 수 있습니다.

- E:\project\windows**Rocket**\Ant\Api\PubnubApi\obj\Debug\net35\Pubnub.pdb

- E:\project\windows**Rocket**\Ant_3.5\Ant\obj\Release\Ant.pdb

[그림 3-1] Rocket 경로에서 제작된 PDB 경로 화면

저희는 주요 키워드를 활용해 사이버 캠페인(Campaign)을 분류했으며, **'작전명 로켓 맨(Operation Rocket Man)'**으로 명명하였습니다.

또한, 이후 이들 조직에 대한 상세한 추가 분석자료 및 침해지표(IoC) 자료는 기업용 Threat Inside 서비스를 통해 지속적으로 제공할 예정입니다.

[그림 3-2] Threat Inside 인텔리전스 리포트 표지

※ ESRC-1808-TLP-White-IR002_RocketMan_English

ESRC-1808-TLP-White-IR002_RocketMan_English.pdf

ESRC는 공격에 활용된 코드를 분석하던 중 위협 인텔리전스(TI) 혼선 기법의 거짓 플래그(False Flag)를 다수 발견했습니다. 제작자는 중국어 영문식 표기로 어린아이를 의미하는 'Haizi' 영어 표현을 사용했습니다.

이 표현은 추후 설치되는 닷넷 기반의 프로그램에서도 동일하게 사용되는 것이 확인되는데, 닷넷 기반 악성코드에서는 'PAPA'라는 문자가 존재합니다. 그러나 아버지를 의미하는 중국어의 영문표기는 'BABA' 가 사용되고 있습니다.

단순히 이를 기반으로 추론했을 때 공격자는 중국어 역시 모국어가 아닐 가능성도 존재하는 중요한 단서가 될 수 있습니다.

[그림 4] 중국어 영문표기 표현이 담긴 악성코드 내부 화면

이렇게 설치된 악성코드는 암호화된 ini 설정 파일을 다운로드해 복호화 과정을 거치게 됩니다. 이 설정 파일은 'desktops.ini' 파일명을 가지고 있으며, 취약점 공격을 사용하던 명령제어(C2) 서버와 동일한 곳에서 수신하게 됩니다.

```
public void SetPubnub(string[] strArr)

{

if (strArr.Length != 7)

{

return;
```

```
}

for (int i = 0; i < strArr.Length; i++)

{

strArr[i] = this.calcXor(strArr[i], 23);

}

this.m_strChannelNameTmp = strArr[1];
```

명령어를 통해 암호화되어 있는 설정 파일은 XOR 0x17 키값으로 복호화가 진행되고, 복호화가 완료되면 서비스로서의 인프라스트럭처(Infrastructure as a Service)의 하나인 퍼브너브(PubNub) 채널로 명령제어(C2)통신을 시도하게 됩니다.

공격자는 여기서도 'LiuJin' 계정을 사용하는데, 이 부분 역시 중국근거 요소로 사용할 수 있도록 유도하는 부분 중에 하나입니다.

'LiuJin' 영문 표기는 다양한 표현이 존재하는데, 중국어로 표현하면 '刘劲'(리우진)으로 사용할 수 있고, 중국의 배우이름이나 온라인게임에서도 사용됩니다.

코드 안에는 중국과 연관되는 다양한 기록들이 의도적으로 남겨져 있는데, ESRC에서는 언어적, 지리적 코드를 고의로 노출해 위협 인텔리전스(TI)에 혼선을 유발하기 위한 교란전술 가능성이 높다고 판단하고 있습니다.

[그림 5] IaaS 기반 PubNub 명령제어(C2) 사용 화면

이처럼 공격자는 정상적인 IaaS 서비스를 이용해 은밀하고 교묘하게 통신을 수행하고 있어, 유해 트래픽 식별하는데 많은 어려움이 존재하게 됩니다.

2. 유사 위협 사례 및 연관성 심층 분석

2017년 09월에는 동일한 기법의 스피어 피싱 사례가 발견된 바 있습니다. 이 공격에도 HWP 취약점이 사용되었는데, 메타 데이터가 2018년 8월 침해사고 지표와 동일하게 존재합니다.

공격자에 대한 계정명과 OLE 코드도 동일하게 사용이 되며, 참고자료 처럼 위장하고, 원본 메일에 회신하는 형태로 구성되어 있는 특징이 있습니다.

[그림 6] 공격에 사용된 이메일 화면 중 일부

공격에 사용된 악성 프로그램은 'icloud.exe' 파일명도 사용하고, 내부에는 다음과 같은 PDB(Program Data Base) 코드가 존재합니다.

- E:\))PROG\doc_exe\Release\down_doc.pdb

해당 PDB 시리즈는 변종 악성파일에 따라 매우 다양하게 존재하며, 동일 시리즈 중에 AOL 메신저(AIM)를 이용하는 2013년 초기버전과도 연결됩니다.

AOL 메신저로 통신하던 초기모델 이후 한국의 웹 사이트를 해킹해 통신하는 형태로 진화하고, 이후에는 스트림네이션(Streamnation.com)을 통한 명령제어 방식을 사용합니다.

명령제어 통신용 계정 가입에는 주로 한국, 미국, 중국, 인도, 러시아 등의 이메일 정보를 사용합니다.

그 다음에는 피클라우드(pcloud.com)나 얀덱스(yandex.com), 드롭박스(Dropbox) 등의 클라우드 서비스를 지속적으로 활용했으며, 최근에는 IaaS 방식이며, 사물인터넷(IoT) 클라우드 디바이스를 하나의 시스템으로 상호 연결할 때 사용할 수 있는 실시간 네트워크 플랫폼인 퍼브너브(PubNub) 서비스를 통신제어 방식으로 사용하고 있습니다.

- K:\))pick\ie\test.pdb

- D:\))pick\doc_exe\Release\down_doc.pdb

- E:\))PROG\doc_exe\Release\down_doc.pdb

- E:\))PROG\doc_exe\Release\drun.pdb

- E:\))PROG\ie\Release\drun.pdb

- E:\))PROG\Upload\Upload\thunder

- E:\))PROG\waoki\Release\runner.pdb

- E:\))PROG\waoki\Release\kltest.pdb

[그림 7] 악성 프로그램 내부에 존재하는 PDB 코드 분석 화면

이 공격에 사용된 명령제어(C2) 서버는 'endlesspaws.com' 도메인으로 이 호스트는 수차례 유사 공격에 이용된 바 있습니다.

위협 인텔리전스(TI) 측면에서 이 공격에 사용된 서버를 통해 공격자의 유사 위협 사례를 조사하는데 유용하게 활용할 수 있습니다.

ESRC는 이 도메인이 2015년 대북관련 한국의 워터링 홀 공격과 연관된 것도 확인하였으며, 2017년 실행파일을 첨부한 스피어 피싱 공격에도 사용된 증거를 확보했습니다.

더불어 CVE-2017-8759 취약점을 통한 공격도 존재합니다. 그 중 일부를 중국의 보안업체인 텐센트(Tencent)에서 블로그를 통해 공개한 바 있습니다.

2017년 2월에도 다수의 유사 위협 사례들이 포착되었는데, 당시 다음과 같이 탈북 인사 보호 강화를 위한 안전수칙이라는 내용으로 현혹해 악성코드를 유포하는데 'endlesspaws.com' 도메인이 이용되기도 했습니다.

[그림 8] 탈북인사 보호강화 안전수칙 위장 악성 파일 유포 화면

마치 '안전수칙.zip' 파일을 이메일에 첨부한 것처럼 보이지만, 실제로는 'endlesspaws.com' 도메인에서 압축 파일을 설치하도록 연결해 두고 있으며, HWP 문서처럼 위장한 이중확장자의 EXE 실행타입의 악성파일이 포함되어 있습니다.

공격자는 이중확장자로 위장하면서, 아이콘도 문서파일 리소스를 활용해 얼핏보기에 정상적인 HWP 파일로 보이도록 조작해 두었습니다.

악성파일은 내부에 암호화 함수 루틴으로 구성된 코드를 로드하고, 특정 16진수 코드들을 로직 XOR 0x55 키값으로 디코딩하게 됩니다.

ZIP 압축파일을 유포하는데 사용된 C2 도메인과 마찬가지로 EXE 실행형 악성파일은 다음과 같은 주소로 접속을 시도하게 됩니다.

- http://endlesspaws.com/vog/tan[.]php?fuck=x

- http://endlesspaws.com/vog/denk[.]zip

[그림 9] 암호화된 C2 데이터를 변환하는 코드 화면

추가로 다운로드되는 'denk.zip' 파일은 겉으로 보기에 ZIP 형식의 압축파일로 보이지만, 실제로는 HWP 형식의 문서파일입니다.

보통 EXE 형식으로 유포되는 악성코드는 내부에 정상적인 HWP 문서를 포함한 후 감염될 때 보여주거나, 명령제어 서버에서 정상적인 HWP 문서를 다운로드해 보여줍니다. 하지만, 이번 사례는 추가로 악성 HWP 문서를 다운로드해 설치하는 독특한 절차를 수행하게 됩니다.

이미 감염된 시스템에 문서기반 악성 파일을 추가로 설치하는 특이한 경우라 볼 수 있습니다. 해당 문서파일에는 공격에 사용된 이메일 내용과 일치하는 내용이 포함되어 있어, 다른 사이버 작전과 혼동하여 잘못된 파일이 링크된 것은 아닌 것으로 보입니다.

'denk.zip' 파일에는 DefaultJScript 영역에 악성 스크립트 코드를 삽입하였고, BASE64 코드로 인코딩된 악성 DLL 파일을 임베디드 형식으로 포함하고 있다가 스크립트 작동시 디코딩하여 로딩하게 됩니다.

[그림 10] 문서파일 내부에 포함되어 있는 악성 스크립트 코드 화면

BASE64 코드가 디코딩되어 작동하는 악성 DLL 파일에는 다음과 같은 PDB 경로가 포함되어 있으며, 총 6개의 한국 명령제어(C2) 서버와 통신을 시도하게 됩니다.

통신시에는 'srvrlyscss' 코드를 사용하는데, 이 코드는 한국내 다수의 침해사고 지표에서 포착된 바 있습니다.

[그림 11] 통신에 사용하는 'srvrlyscss' 스트링을 가진 코드 화면

- seline.co.kr/datafiles/CNOOC[.]php

- www.causwc.or.kr/board_community01/board_community01/index2[.]php

- www.kumdo.org/admin/noti/files/iindex[.]php

- www.icare.or.kr/upload/board/index1[.]php

- cnjob.co.kr/data/blog/iindex[.]php

- notac.co.kr/admin/case/iindex[.]php

그리고 중복실행 방지를 위해 사용한 뮤텍스(Mutex) 코드로 'taihaole9366' 이라는 스트링이 사용되었는데, 'taihaole'는 중국어(太好了) 영문표기와 일치하며 의미는 '매우 좋다' 입니다.

공격자는 과거부터 중국어 영문표기 방식을 매우 자주 사용하였으며, 이외에도 다양한 표현이 존재합니다.

[그림 12] 인코딩되어 있는 C2와 중국식 영문표기 뮤텍스 화면

2018년 01월에는 기존 한국 보안 프로그램으로 위장한 사례와 다르게, 중국의 유명 보안 프로그램으로 위장해 유포되는 경우가 확인됩니다.

공격자는 한국의 웹 사이트 'ebsmpi.com' 사이트에 마치 중국의 360 TOTAL SECURITY 보안 프로그램 웹 페이지처럼 위장한 가짜 화면을 추가하였습니다.

당시 실제 중국에서 운영되고 있던 웹 사이트의 소스코드를 복사해 사용하였으며, 다운로드되는 파일만 악성으로 변경해 사용하였습니다.

다운로드로 연결된 주소는 다음과 같고, 'Free Download' 링크를 클릭할 경우 '360TS_Setup_Mini.exe' 파일이 다운로드 됩니다.

- http://ebsmpi.com/ipin/360/down[.]php

[그림 13] 한국의 'ebsmpi.com' 웹 사이트를 해킹해 화면을 추가한 모습

중국의 보안 프로그램처럼 파일명(360TS_Setup_Mini.exe)을 위장하고 있으며, 아이콘 리소스 역시 실제 정상 프로그램 것을 그대로 도용해 사용하였습니다. 그리고 추가적인 닷넷 기반 악성파일이 환경조건에 따라 설치시도 됩니다.

또한, 2018년 8월 한국의 포털사 보안 프로그램 위장 공격 벡터 기법과 100% 일치하고, 암호화 알고리즘도 동일한 것을 확인했습니다.

[그림 14] 중국 보안프로그램으로 위장한 악성파일과 정상파일 비교

- http://ebsmpi.com/ipin/360/Ant_3.5[.]exe (MD5 : ff32383f207b6cdd8ab6cbcba26b1430)

- http://ebsmpi.com/ipin/360/Ant_4.5[.]exe (MD5 : 84cbbb8cdad90fba8b964297dd5c648a)

- http://ebsmpi.com/ipin/360/desktops[.]ini (MD5 : ab2a4537c9d6761b36ae8935d1e5ed8a)

- http://**cgalim.com**/admin/hr/temp[.]set (MD5 : fa39b3b422dc4232ef24e3f27fa8d69e)

정상적인 '360TS_Setup_Mini.exe' 파일은 'cgalim.com' 도메인에서 'temp.set' 파일명으로 설치하게 되는데, 이 경로는 하기 유사한 침해사고에도 동일하게 사용됩니다.

[그림 14-1] '360TS_Setup_Mini.exe' 정상 파일 설치 시도 화면

닷넷 기반의 초기 악성파일에는 다음과 같은 PDB 경로들이 포함되어 있고, 최신 변종들에서는 일부 생략되어 있습니다.

- E:\project\windows\Rocket\Ant\Api\PubnubApi\obj\Debug\net35\Pubnub.pdb

- E:\project\windows\Rocket\Sys-Guard\Servlet-standalone_Guard\Release\Servlet.pdb

- E:\project\windows\Rocket\Sys-Guard\Chutty_Guard\Release\Chutty.pdb

- E:\project\windows\Rocket\Servlet\Release\Servlet.pdb

- E:\project\windows\Rocket\Ant_4.5\Ant\obj\Release\Ant.pdb

ESRC는 분석을 통해 악성파일 실행시 정상 프로그램을 또 다른 해킹서버에서 다운로드해 이용자로 하여금 정상적인 프로그램처럼 인식하도록 만들고 있다는 것을 검증했습니다.

이때 사용하는 C2 서버가 기존 안드로이드 악성앱(1.apk) 유포와 비트코인 관련 'bitcoin-trans.doc' (MD5 : 8ab2819e42a1556ba81be914d6c3021f) 악성파일에서 확인된 호스트와 오버랩됩니다.

- http://cgalim.com/admin/hr/hr[.]doc (MD5 : 24fe3fb56a61aad6d28ccc58f283017c)

- http://cgalim.com/admin/hr/1[.]apk (MD5 : 9525c314ecbee7818ba9a819edb4a885)

- http://**cgalim.com**/admin/hr/temp[.]set (MD5 : fa39b3b422dc4232ef24e3f27fa8d69e)

'cgalim.com' 도메인의 경우는 하위 주소 /hr/ 경로외에도 /1211me/ 주소에서도 변종 파일이 유포된 이력이 존재합니다.

동일 조직은 2015년과 2016년에는 대북 유관단체 등을 상대로 한 워터링 홀 공격이 수행되었습니다. 당시에 공격자들은 플래시 플레이어 취약점을 적극적으로 활용했습니다.

북한관련 뉴스 사이트나 대북관련 웹 사이트들이 집중적으로 해킹되었으며, 이 공격은 수개월간 지속됩니다.

다음 화면은 실제 해킹된 웹 사이트에 추가된 악성 오브젝트입니다.

[그림 15] 워터링 홀 공격에 사용된 플래시 플레이어 취약점 코드 화면

공격 조직은 2015년 당시 CVE-2015-5119, CVE-2015-0313 최신 플래시 플레이어 취약점 뿐만 아니라, 이탈리아 Hacking Team 서버 해킹으로 유출된 플래시 플레이어 취약점인 CVE-2015-5119 취약점 등을 사용한 바 있습니다.

그리고 이들은 2017년 하반기부터 카카오톡 메신저 등을 활용해 공격 대상자를 선별하고 CVE-2018-4878 플래시 플레이어 Zero-day 취약점 공격을 수행하기도 하였습니다.

- G:\FlashDeveloping\mstest\src (CVE-2014-8439)

- G:\FlashDeveloping\20148439\src (CVE-2014-8439)

- G:\FlashDeveloping\Main\src\ (CVE-2015-0313)

- G:\FlashDeveloping\2015-3090\src (CVE-2015-3090)

- G:\FlashDeveloping\20153105\src (CVE-2015-3105)

- G:\FlashDeveloping\20155119\src (CVE-2015-5119)

- G:\FlashDeveloping\chrome_ie\src (CVE-2015-5119)

공격자는 여러 워터링 홀 공격 중에 플래시 플레이어 취약점(SWF)에 의해 다운로드된 추가 악성코드가 사용자 계정 컨트롤 (User Account Control)을 통한 관리자권한 실행에 실패할 경우 약 5분 후 가짜 하드디스크 문제 오류창을 출력합니다.

그리고 마치 백업 프로세스로 조작해 관리자 권한 CMD 명령으로 악성코드를 재실행 하도록 유도하는데 이때 사용한 한글표기 중 일부가 북한에서 사용하는 영문식 컴퓨터 용어표현(프로쎄스, 프로그람)과 동일한 것을 알 수 있습니다.

[그림 16] 북한식 컴퓨터 용어 표현이 포함된 가짜 메시지 창 화면

명령제어(C2) 통신방식에도 나날이 진화를 거듭하고 있습니다. 가장 초기에는 AOL(America Online) 메신저인

AIM(America Online Instant Messenger) Oscar 프로토콜을 이용해 명령제어를 수행했습니다.

AIM 메신저의 계정과 암호를 통해 암호화된 명령을 주고 받는데, 로그인 암호가 한글식 영문 타이핑이라는 것을 알 수 있습니다. 또한, 초기에 사용한 PDB 경로에는 AOL 폴더에서 개발된 것을 알 수 있습니다.

- fastcameron13 / powercooper00 / dPfWls&Rkapfns19 (옐찐&까메룬19)

- F:\Program\svr_install\Release\svr_install.pdb

- F:\Program**Aol**\Release\ServiceDll1.pdb

[그림 17] AIM 메신저를 C2로 사용하고 있는 화면

AIM 메신저로 통신을 시도할 때 공격자는 로그인 계정과 암호를 통해 접속한 후 암호화된 메시지를 또 다른 계정 사용자에게 발송하게 됩니다.

실제 감염된 경우 컴퓨터 정보, 추가 명령 등 암호화된 메시지가 전송되게 되며, 다양한 계정들을 사용한 바 있습니다.

공격자들은 대표적으로 다음과 같은 aol.com, hotmail.com, yahoo.com, India.com, inbox.com, gmail.com, zmail.ru 계정들이 존재하며, 이외에도 다양한 변종들을 제작해 사용하였습니다.

- allmothersorg11@hotmail.com

- allmothersorg@hotmail.com

- bluelove@india.com

- cmostenda01@yahoo.com

- cmostenda102@yahoo.com

- cmostenda103@yahoo.com
- daum14401@zmail.ru
- dapplecom2013@yahoo.com
- eatleopard00@inbox.com
- fastcameron00
- fastcameron11
- fastcameron13
- fatpigfarms@hotmail.com
- fatpigs9009@hotmail.com
- friendleopard00@aol.com
- ganxiangu04@hotmail.com
- ganxiangu07@hotmail.com
- greatvictoria84
- greatvictoria85
- greatvictoria86
- greatvictoria87
- hatmainman@hotmail.com
- hatwoman40@hotmail.com
- jinmeng288@gmail.com
- minliu231@gmail.com
- Okokei@india.com
- pghlsn333@gmail.com
- prettysophia00
- prettysophia47
- prettysophia48
- prettysophia49

- prettysophia50

- prettysophia51

- prettysophia52

- prettysophia53

- prettysophia54

- prettysophia55

- prettysophia56

- prettysophia57

- tosarang87@gmail.com

- winpos1000@zmail.ru

- winpos1001@zmail.ru

- winpos1002@zmail.ru

- winpos1003@zmail.ru

- winpos1004@zmail.ru

- xiangangxu88@hotmail.com

- zum36084@gmail.com

- zum36084@zmail.ru

- zum36085@zmail.ru

2016년 초 공격자는 'zum36084@gmail.com', 'zum36084@zmail.ru', 'daum14401@zmail.ru' 등의 이메일을 생성한 후 테스트용 이메일을 발송하는 것이 확인됩니다.

IoA(Indicators of Attack) 기반으로 조사를 하면 공격자는 마치 'Google 계정팀' 처럼 'zum36084@gmail.com' 이메일을 설정한 것을 알 수 있으며, 처음부터 한글을 사용하고 있다는 것도 확인할 수 있습니다.

[그림 18] 공격용 이메일을 생성 후 테스트한 화면

2016년 03월 03일 테스트한 이메일에서는 '0303_zmail.gif' 파일을 첨부해 발송하는데, XOR 0x69 키 등으로 2단계 암호화된 EXE 형식의 악성파일입니다.

복호화된 악성파일은 특정 컴퓨터 이름만 감염되도록 설정한 특징이 존재하는데, 이곳에는 한글 이름과 특정 언론사의 기자도 포함되어 있습니다.

- 하지나

- WOOSEONG-PC

- T-PC

변종 중에는 다음과 같은 계정을 체크하는 종류도 존재하는데, 'SEIKO' 컴퓨터명의 경우에는 다양한 침해 지표에서 발견이 되고 있습니다. 특히, HWP 문서파일 취약점을 사용할 때 마지막 작성자의 계정과 일치

하며, '175.45.178.133' 아이피의 감염 로그에서도 확인된 바 있습니다.

- 홍채연[하율]

- KIM[Administrator]

- JAMIE[Jamie Kim]

- DONGMIN[MinSk]

- T-PC[T]

- YONGJA-PC

- USER

- sec

- CRACKER-PC

- SEIKO

'SEIKO' 계정으로 감염된 로그 기록에는 다음과 같이 해당 사용자가 다음과 같은 사이트를 즐겨찾기 해 둔 것을 확인할 수 있습니다.

특히, 여기서 북한 평양 아이피 주소가 식별되기도 했습니다.

Windows IP Configuration

Host Name . . . . . : **SEIKO-PC**

Primary Dns Suffix . . . . . :

Node Type . . . . . : Hybrid

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Description . . . . . : Realtek PCIe FE Family Controller

DHCP Enabled. . . . . : No

Autoconfiguration Enabled . . . . : Yes

IPv4 Address. . . . . : **175.45.178.133**(Preferred)

Subnet Mask . . . . . : 255.255.255.240

Directory of c:\users**SEIKO**\Favorites\Links\mail

150 126?易.url

213 163?易.url

808 **AOL Mail.url**

265 Gmail.url

837 Hotmail.url

152 Inbox.url

183 **India.url**

466 Yahoo mail.url

218 **zmail.url**

Directory of c:\users**SEIKO**\Favorites\Links\뉴스

112 FN지니아이.URL

115 Sputnik.URL

110 네이트.URL

109 다음사전.URL

114 러.URL

113 **로동신문.URL**

151 한경.URL

Directory of f:\2_Program**Orbis_zmail**\Debug

아울러 조건이 맞는 컴퓨터의 경우에는 내부에 암호화된 코드를 XOR 0x55 키로 복호화한 후 'conhost.exe' 파일명으로 생성해 실행하게 됩니다.

'conhost.exe' 파일의 경우가 바로 AOL 메신저로 통신을 하는 기능을 수행하게 됩니다.

[그림 19] AOL 메신저로 통신을 시도하는 코드 화면

특히 주목해야 할 점은 AOL 메신저로 로그인하기 위해 사용된 암호코드(dPQms&Thvldk1987) 알파벳을 한글 키보드에서 변환하게 되면 한국어로 '예쁜&쏘피아1987' 표현으로 완벽히 변환이 된다는 것입니다.

공격자는 AOL 메신저 통신기법에서도 다수의 중국식 표현을 복합적으로 사용하기도 합니다. 또 다른 변종에서는 'Dajiahao' 코드를 Mutex 키로 사용하는데, 중국어로 '여러분 안녕하세요.' 라는 의미를 가지고 있으며, AOL 로그인 계정 암호로는 (dPfWls&Rkapfns19) 알파벳을 쓰는데, 이것도 한글 키보드 상태에서 입력하면, 한국어로 '옐찐&까메룬19' 표현으로 변경되는 것을 알 수 있습니다.

[그림 20] 중국식 인사말과 한글 변환 가능 암호가 사용된 화면

이러한 종류의 변종은 매우 다양한 형태가 발견되었는데, 'SEIKO' 컴퓨터명을 감염대상으로 하고 있는 경우에는 내부에 다음과 같은 PDB 경로가 존재합니다. 공격자는 'zum36085@zmail.ru', 'pghlsn333@gmail.com' 이메일을 사용합니다.

- F:\2_Program**Orbis_zmail**\Release\RecvTest_zmail.pdb

유사한 시리즈로는 다음과 같은 PDB 자료를 포함하고 있습니다.

- F:\2_Program**Orbis_academia**\Release\RecvTest_zmail.pdb

- F:\2_Program\Orbis_academia\Release\Recv_Pwd_2_India.pdb

[그림 21] Zmail 테스트 정보가 포함되어 있는 PDB 코드 화면

ESRC는 이들이 APT 표적공격 외에도 불특정다수를 겨냥한 다양한 공격 기법을 활용하는 정황도 포착한 바 있는데, 바로 한국의 토렌트 웹 사이트에 가입해 불법 소프트웨어 속에 은밀하게 악성코드를 삽입해 유포하는 기법입니다.

내부에 악성코드를 삽입한 후, 유명 상용 소프트웨어를 불법적으로 사용할 수 있도록 배포를 하는 방식입니다.

실제 공격자가 한국의 특정 토렌트에서 활동하면서 얻은 포인트 이력은 다음과 같고, 업로드와 댓글 등의 활발한 움직임을 보이기도 했습니다.

[그림 22] 한국의 토렌트 사이트에서 활동한 이력 화면

3. 금성121 그룹의 시계열 흐름 정리

2013년 상반기 AOL 메신저를 통한 통신 기법이후에 공격자는 잠시 한국의 웹 사이트를 해킹해 C2로 활용을 하기도 합니다. 그러나 해당 웹 사이트들이 노출되고, 신속하게 차단되자 지속적 효용성이 떨어진다는 것을 의식한 것으로 추정됩니다.

그래서인지 얼마 후에 다시 AOL 메신저를 통한 통신 기법으로 회귀해 지속적인 변종을 제작하였고, 그러다가 워드프레스(WordPress) 기반 웹 사이트를 집중적으로 해킹해 워터링 홀 공격 거점으로 활용하게 됩니다.

워드프레스 웹 사이트를 이용한 공격에서는 주로 플래시 플레이어 취약점 파일을 이용하게 되며, 개인용 미디어 허브 서비스인 'Streamnation' 클라우드 계정을 본격적으로 쓰게 됩니다.

공격자는 그 과정에서도 꾸준히 AOL 메신저를 이용한 통신 방식을 유지하였고, 스피어 피싱이나 워터링 홀 공격의 중개 서버로는 워드프레스 웹 사이트를 C2로 활용하게 됩니다.

그러던 중 'Streamnation' 서비스가 2016년 2월경 서비스를 종료한다고 알려지면서, 공격자는 2016년 1월 말부터 'zmail.ru' 서비스를 본격적으로 테스트하기 시작합니다. 물론, 공격자는 그 전부터 'zmail.ru' 서비스를 이용하고 있었습니다.

그렇게 'zmail.ru' 서비스 등을 통해 공격자는 새로운 C2 서버 체계로 변경을 시도하고, AOL 메신저 통신과 함께 'pCloud' 서비스를 도입하기 시작합니다. 클라우드 서비스 계정을 생성할 때는 한국 뿐만 아니라 미국, 중국, 인도, 러시아 등 다양한 국가의 무료 이메일 서비스를 활용하기도 합니다.

공격 전술의 변화는 시간이 갈수록 변화를 거듭하며, 친구 추가가 되어 있지 않은 특정 대상을 상대로 카카오톡 메시지로 CVE-2018-4878 취약점 파일을 전송하거나, 스마트폰 이용자를 겨냥한 안드로이드 악성앱 유포도 발견되었습니다.

2017년 말 암호화폐 관련 내용의 DOC 문서 취약점 공격은 해외에서 먼저 보고되기도 했습니다. 그외 한국, 중국 등의 보안프로그램 위장 유포, 토렌트를 통한 악성코드 무차별 배포 등 공격 기술을 꾸준히 업그레이드 하고 있다는 것을 알 수 있었습니다.

[시계열에 따라 일부 C2 기법의 변화]

2013년 03월 26일 : AOL 메신저 서비스 방식 지속

2013년 04월 20일 : 한국내 특정 웹 사이트 통신

2015년 07월 10일 : 워드프레스 웹 사이트 통신

2015년 07월 14일 : Streamnation 개인용 클라우드 서비스

2015년 08월 09일 : Streamnation 개인용 클라우드 서비스

2016년 02월 09일 : Streamnation 개인용 클라우드 서비스 공식종료

2016년 04월 11일 : Pcloud 개인용 클라우드 서비스

2017년 12월 15일 : AOL 메신저 서비스 공식종료

2017년 12월 12일 : PubNub IaaS 서비스

2018년 01월 16일 : PubNub laaS 서비스

2018년 02월 23일 :PubNub IaaS 서비스

2018년 08월 14일 : PubNub IaaS 서비스

[그림 23] 시간에 따라 변화하는 C2 통신 화면

지금까지의 사례외에도 동일한 IoC 코드나 메타 데이터를 사용하는 유사한 침해사고가 한국에서는 수년간 계속 이어지고 있으며, ESRC는 그 변화 과정을 지속적으로 추적 연구하고 있습니다.

보다 추가적인 내용들은 하반기부터 서비스가 예정인 '쓰렛 인사이드(Threat Inside)'를 통해 보다 체계적인 위협정보(IoC)와 전문화된 인텔리전스 리포트 서비스를 기업대상으로 제공할 예정입니다.

▶ **https://www.estsecurity.com/product/threatinside**

Source: http://blog.alyac.co.kr/1853