화웨이 관련 보안이슈

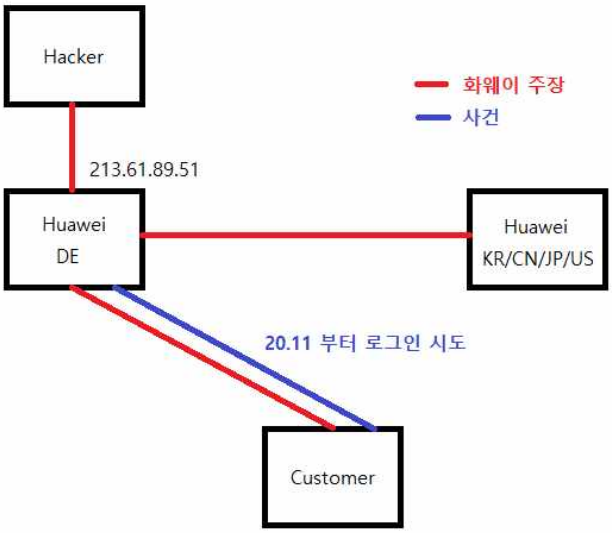
분석가: 박수곤 D 대학교 정보보호학과
홍세웅 I 대학교 컴퓨터공학과
이정훈 I 대학교 컴퓨터공학과

용의자: 화웨이, 화웨이 독일지사, 제3자

기간: 2020.11. - 2021.05.

소스: Facebook - 코딩이랑 무관합니다만
게시자: 채하람 (부산출신, 경상대)

모식도



침해 내용

불법적인 로그인 시도 (10회 이상)

침해 발생 경위

1. 피해자의 화웨이 공유기 사용
2. 화웨이 독일 지사(이후 HWDE) 컴퓨터에서 불법적인 로그인 시도
3. 패스워드 불일치 이벤트 로그 발생
4. 지속적인 접근으로 인해 운용 중인 Synology NAS에서 해당 접속 감지 및 차단
5. 로그 확인, 20년도 11월부터 접근 시도가 있었음을 인지
6. 논의 및 국가 기관에 정보제공
7. 화웨이와 연락

화웨이 측 주장

a. 접근 시도한 IP는 HWDE가 맞으나 HWDE는 경유지
a-근거1. 화웨이에서도 피해
a-근거2. 화웨이 공유기가 해당 접속 차단
a-피드백. 현재 조사 중이며 가능한 신속히 로그 제공
a-근거2-반박. 피해자의 NAS가 접속 차단

예상 가능한 시나리오

a-1. 화웨이 보안 취약
a-2. HWDE의 사적인 이익 등을 위한 VPN 서버 운용
b. 화웨이의 침해시도

관련 자료


범주: 자동 차단
이벤트: FTP을(를) 통해 CHTUNNAS에서 IP 주소 [213.61.89.51]이(가) 차단됨
시간: 2021-05-20 14:06
설명: 5분 이내에 CHTUNNAS에서 실행 중인 FTP에 로그인 시도 시 IP 주소 [213.61.89.51]이(가) 시도를 10회 실패하여 Thu May 20 14:06:49 2021에서 차단되었습니다.

inetnum: 213.61.89.48 - 213.61.89.55
netname: NET-DE-Huawei-Technologies-Dusseldorf-GmbH
descr: Huawei Technologies Dusseldorf GmbH
country: DE
admin-c: VR829-RIPE
tech-c: VR829-RIPE
status: ASSIGNED PA
mnt-by: DE-COLT-MNT
created: 2019-06-20T15:19:42Z
last-modified: 2019-06-20T15:19:42Z
source: RIPE

https://threats.autohost.ai/ip/213.61.89.51 - 해당사건 관련 해외 리포트

정리 및 이슈 체크

화웨이 공유기 설치이후 화웨이 독일지사 부정접속(FTP 로그인 10회 시도) 건('21.05.20. 14:06) 관련입니다.

(화웨이측주장)'21.05.27 금일 화웨이 한국지사 담당자와 통화를 했으며, 화웨이의 주장은 다음과 같습니다.

가. 해당 IP는 화웨이 독일지사 IP가 맞으며, 독일지사가 경유지로 사용되었다.
화웨이가 직접 시도한 것은 아니며, 화웨이도 피해를 봤다.

나. 위 내용에 대해서는 지금 조사 중이며, 조사되는대로 로그를 제공하겠다.
다. 어쨌든 차단은 화웨이 공유기가 차단했다.

- 해당 내용은 통화 시 Synology NAS가 차단했다고 반박함

라. 우리회사에서도 난리났다.
(이전기록확인)통화 이후, 해당 IP에 대해 구글링을 했으며,
해당 IP에 대한 부정접속 Report는 '20.11.23. 부터 있었음을 확인했습니다.
출처 : https://www.abuseipdb.com/check/213.61.89.51?page=4#report

(결론) 화웨이가 벌인 일인지 아닌지는 아직 알 수 없으나,
설령 화웨이의 서버가 경유지로 이용되었다고 하더라도,
작년 11월부터 약 6개월간 방치하였다는 것이고,
항상 보안을 부르짖었던 화웨이 자체의 보안관리에 큰 문제가 있었음을 자백하는 꼴이 될 것입니다.
중국의 네트워크 회사인 화웨이 관련 보안이슈입니다.

화웨이의 특징 : 가성비와 안전성을 마케팅으로 높은 성장력과 시장 장악을 보여줌,
하지만 보안 관련 사항으로 퇴출 등과 다양한 문제사항에 직시하였으며,
21.05.20일 해당 보안 문제사항이 발생함.

시나리오 : 하웨이가 주체일 경우,
공격 경유지로 활용 되었을 경우,
보안에 문제가 발생했을 경우,
사적 이익과 이윤 창출의 목적이였을 경우
요주의 IP/국가 탐지 정보 탐지내용
유형 탐지
대응 방안

타임라인

1. 화웨이 공유기 구매 및 설치,
   자기 NAS에 FTP 접속 시도 하다가 차단당한 IP를 확인 해보니 독일 지사 ip

2. 화웨이 사용
   화웨이 AX3, 공유기 기종을 사용

3. 화웨이 독일지사 부정 접속
   FTP 로그인 10회시도 [21.05.20.14:06] 차단당함

4. 운용중인 NAS에서 화웨이 독일지사발 공격시도임을 확인
   패스워드 불일치로 차단 / CTHUNNAS에서 차단

5. 이벤트로그 발생
   ISP : Huawei 테크놀로지 뒤셀도르프 (독일지사)
   데이터 센터 / 웹 호스팅
   도메인 : huawei.com
   위치 : 뒤셀도르프 노르드헤인 서부
   호스트 : h-213.61.89.51.host.de.colt.net

6. 인지후 관련 그룹에 논의
   21.05.27 화웨이 한국지사 담당자 통화

7. 국가기관, 유관기관 실무 부처에 해당 사항과 관련된 정보보고
   국가정보원에 제보

8. 화웨이측의 연락
   화웨이의 주장
   해당 IP는 독일지사 일치 및 경유지로 사용되어 피해를 봤다
   조사중이며 조사되는데로 로그를 제공하겠다
   차단은 화웨이 공유기가 차단했다고 하지만 Synology NAS가 차단
   화웨이는 우리회사도 난리 났다

9. 상세사항은 보고서와 별첨 부분 참고 요함

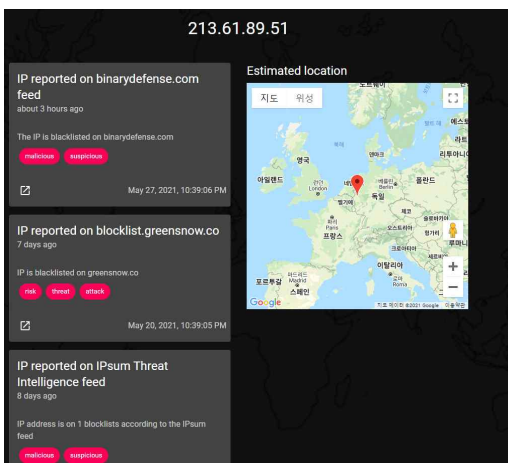
별첨 부록

https://www.facebook.com/groups/System.out.Coding/permalink/4104441316282199/

https://www.facebook.com/groups/System.out.Coding/permalink/4109498779109786/

https://www.facebook.com/groups/System.out.Coding/permalink/4119687744757556/

(좌 : 화웨이 AX3, 우 : iptime AX2004M)



213.61.89.51 SEARCH

조회한 인터넷주소는 한국인터넷진흥원(KISA)이 아닌 다른 해외 기관에서 관리하고 있습니다.
더 자세한 내용은 해당 인터넷주소를 관리하는 Whois 조회 사이트를 이용해 주시기 바랍니다.

(한국인터넷진흥원 후이즈 서버를 경유하여 해외 IP주소를 반복 질의하는 경우 해당
대륙별 인터넷주소관리기구 정책에 의해 차단될 수 있음을 알려드립니다.)

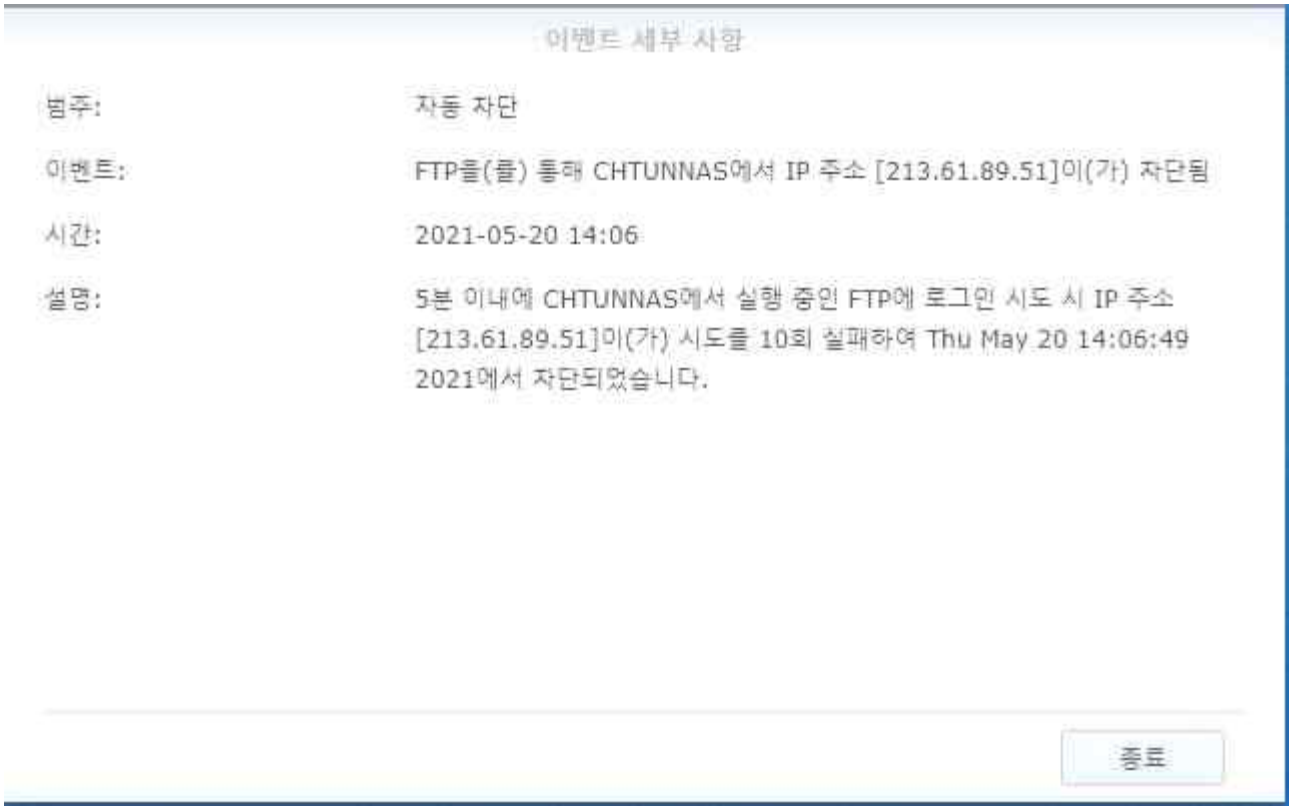
아시아태평양지역 후이즈 서비스 : http://wq.apnic.net/apnic-bin/whois.pl
북미지역 인터넷주소관리기구 : https://www.arin.net
유럽지역 후이즈 서비스 : https://apps.db.ripe.net/search/query.html
남미지역 후이즈 서비스 : http://lacnic.net/cgi-bin/lacnic/whois?lg=EN
아프리카지역 인터넷주소관리기구 : http://afrinic.net

```
%kwhois % This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '213.61.89.48 - 213.61.89.55'

% Abuse contact for '213.61.89.48 - 213.61.89.55' is 'abuse@colt.net'

inetnum:        213.61.89.48 - 213.61.89.55
netname:        NET-DE-Huawei-Technologies-Dusseldorf-GmbH
descr:          Huawei Technologies Dusseldorf GmbH
country:        DE
admin-c:        VR829-RIPE
tech-c:         VR829-RIPE
status:         ASSIGNED PA
mnt-by:         DE-COLT-MNT
created:        2019-06-20T15:19:42Z
last-modified:  2019-06-20T15:19:42Z
source:         RIPE

% Information related to '213.61.0.0/16AS8220'

route:          213.61.0.0/16
descr:          COLT TECHNOLOGIES
origin:         AS8220
mnt-by:         DE-COLT-MNT
mnt-by:         MNT-COLT-SB
created:        2002-06-25T14:35:40Z
last-modified:  2014-06-16T07:14:30Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.100 (WAGYU)
```

신고내용

* 표시는 필수 입력 항목 입니다.

분야	사이버공격
제목 *	화웨이 AX3 공유기 사용 이후 FTP 접속시도 사례 발생
첨부파일	부정접속1.PNG 파일찾기 + 부정접속2.PNG 파일찾기 − ※ 파일 용량은 10MB 이내로 첨부해 주세요.
내용 *	화웨이 공유기 사용 이후, 캡처와 같이 제가 운용중인 NAS에서 화웨이 독일 지사발 IP로 FTP 접속시도가 있었고, 패스워드 불일치로 차단되었던 이벤트 로그가 발생되었습니다. 보안에 문제가 있다고 판단되어, 해당 공유기를 폐기할 예정이나, 혹시 연구 목적으로 필요하시다면 제공해드리려고 합니다.
URL	+


이벤트 세부 사항
범주:
자동 차단
이벤트:
FTP을(를) 통해 CHTUNNAS에서 IP 주소 [213.61.89.51]이(가) 차단됨
시간:
2021-05-20 14:06
설명:
5분 이내에 CHTUNNAS에서 실행 중인 FTP에 로그인 시도 시 IP 주소 [213.61.89.51]이(가) 시도를 10회 실패하여 Thu May 20 14:06:49 2021에서 차단되었습니다.
종료