MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
02 February 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 0202-40-2016

1. References:

   a. Command Guidance, and;
   b. VAPT and PANET Monitoring Result.

2. As per above references, forwarded is the Cybersecurity Bulletin Number 045 with topic regarding **Internet of Things Offers Hackers Access to your Home.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
LTC JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC) PA AC OF S FOR CEIS, G6, PA	

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

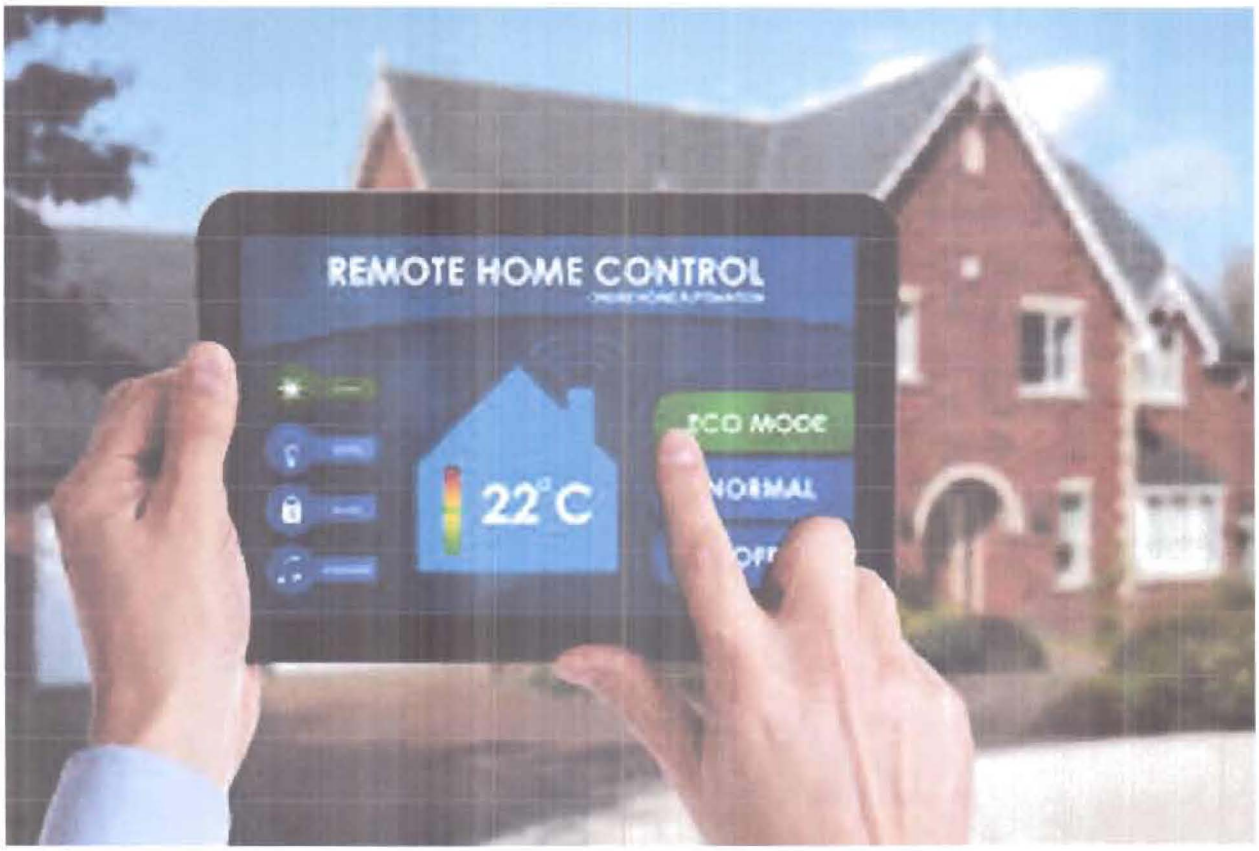
6/CMB

02 February 2016

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #45

INTERNET OF THINGS OFFERS HACKERS ACCESS TO YOUR HOME



HIJACKING "smart" toasters and refrigerators and hacking corporate ventilation systems are among the threats envisioned by cybersecurity experts as an increasing array of items are connected to the internet.

The Internet of Things, a movement that seeks to control everything from factory equipment to traffic lights and household appliances through the web, creates vast

opportunities for improved efficiency and convenience. But unless companies tackle the emerging cybersecurity risks, the Internet of Things will fail, says Stephen Pattison, the vice-president of public affairs at ARM Holdings, the UK semiconductor company.

"We ain't seen nothing yet," he says, speaking on a panel at the Security Innovation Network's US-UK Global Cybersecurity Innovation Summit in London last week.

The Internet of Things is a nascent area, and the fact that there have been relatively few cyber attacks targeting industrial control systems or equipment other than computers doesn't mean such systems are necessarily safe.

It's the risk to critical infrastructure from the internet — enabled industrial control systems, such as those that help run nuclear power plants or chemical factories — that has received the most attention from national security agencies, says Alison Vincent, chief technology officer for Cisco's UK and Ireland businesses.

As a result, many of these networks have already been fortified against possible cyber attacks. Instead, consumer devices may pose a greater risk, particularly in terms of privacy and data protection.

"Consumer technology is the Wild West," she says.

Paddy Francis, chief technology officer for Airbus Group's Defense and Space division, warns of the risks posed by increasingly internet-connect household appliances.

The sheer number of these appliances — from coffee makers to refrigerators to televisions — and the relatively weak firewalls of most household wireless networks, could make such mundane items attractive to cybercriminals for use as "botnets" in denial of service attacks, in which a hacker disables a website by flooding it with specious message traffic.

Francis also worries that "cyber-assisted burglary" might become increasingly common, with criminals hacking into household networks to extract data from routine items — such as smart-metered lighting or heating systems — to determine if the occupant was home, looking for the best time to break in.

Jeremy Watson, vice-dean of engineering sciences at University College London, says even something as simple as allowing a large office building's facilities team to control the heating and air-conditioning systems through a cellphone app — one often cited use of Internet of Things technology — poses a risk.

He says, for example, a disgruntled employee with access to the system might use it to cause temperatures in a server room to soar, resulting in computer failure.

Even if such internet-enabled devices are built with good security measures, the evolving tactics used by hackers and cyber criminals mean that security protocols need constant updating. Another concern is whether businesses and households would be able to keep on top of this process, Watson says.

"What if you have an Internet of Things fridge and it is not being updated," he says. "The real question is how do you get protection by default?"

Pattison notes that a number of car companies, such as Tesla Motors, already provide updates of their software automatically over cellphone and wireless connections.

Reference:

This was cross-posted from: http://www.bdlive.co.za/life/gadgets/2016/02/02/internet-of-things-offers-hackers-access-to-your-home.

DO YOU WANT TO KNOW MORE? TALK TO US.

POCs:

a. **LTC JOEY T FONTIVEROS (INF) PA –** Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-628-1057. Email: fontiverosjt@army.mil.ph.

b. **Sgt Mark Dave M Tacadena (SC) PA** – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-534-2877. Email: tacadenamdm@army.mil.ph.