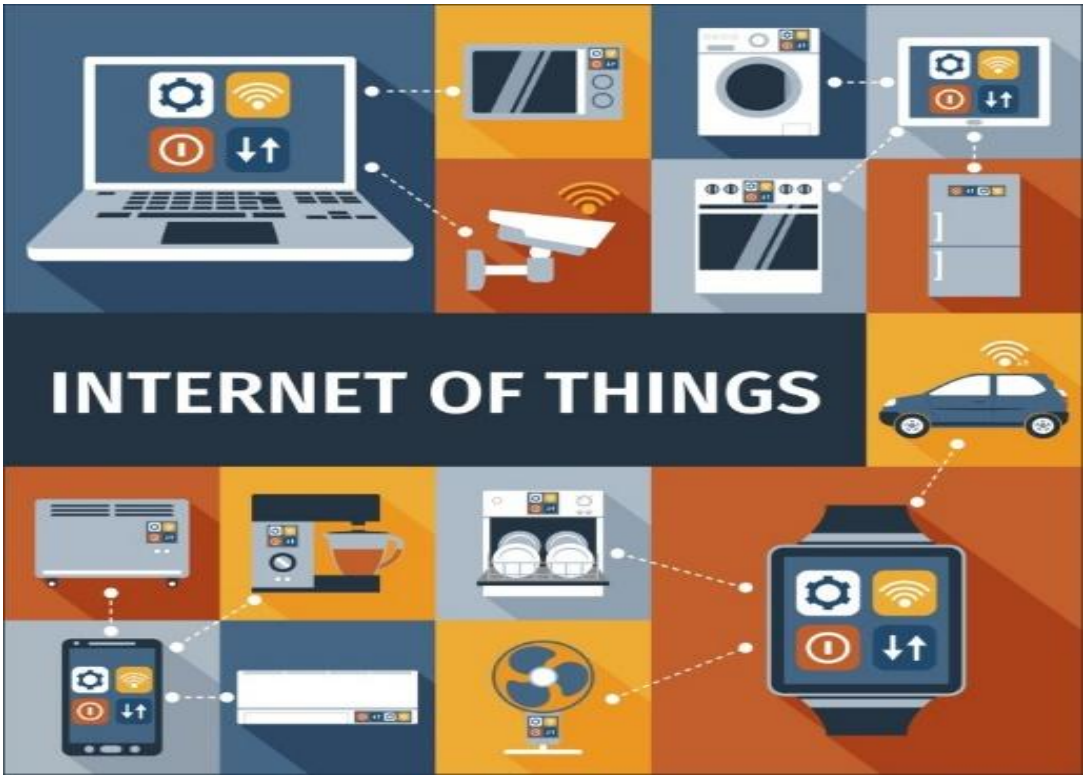
ໄພຄຸກຄາມຈາກ Internet of things ແລະ ແນວທາງໃນການຮັບມືໃນຕໍ່ໜ້າ

ປະຈຸບັນການນຳໃຊ້ອຸປະກອນທີ່ສາມາດເຊື່ອມຕໍ່ກັບອິນເຕີເນັດ (Internet of Things ຫຼື IoT) ເຊັ່ນວ່າ: ກ້ອງວົງຈອນປິດ, ໂທລະພາບຈໍສຳພັດ (smart TV) ຫຼື ເຄື່ອງໃຊ້ໄຟຟ້າທີ່ສາມາດເຊື່ອມຕໍ່ອິນເຕີເນັດໄດ້ ມີແນວໂນ້ມທີ່ຈະເພີ່ມຂຶ້ນເລື້ອຍໆ ແຕ່ເນື່ອງຈາກບັນດາອຸປະກອນເຫຼົ່ານີ້ສ່ວນໃຫຍ່ບໍ່ໄດ້ຖືກຕິດຕັ້ງ ຫຼື ອອກແບບມາໃຫ້ມີລະບົບການຮັກສາຄວາມປອດໄພທີ່ດີພໍ ເຮັດໃຫ້ຜູ້ບຸກລຸກສາມາດເຈາະລະບົບເພື່ອຄວບຄຸມອຸປະກອນດັ່ງກ່າວມາໃຊ້ເປັນເຄື່ອງມືໃນການໂຈມຕີໄດ້. ຊຶ່ງໃນໄລຍະຜ່ານມາກໍ່ມີຫຼາຍເຫດການໂຈມຕີທີ່ຜູ້ໃຊ້ບໍ່ສາມາດຈະປ້ອງກັນ ຫຼື ຫາແນວທາງການແກ້ໄຂບັນຫາດ້ວຍຕົວເອງໄດ້ ເພາະເຄື່ອງອຸປະກອນສ່ວນໃຫຍ່ແມ່ນບໍ່ໄດ້ຖືກອອກແບບມາໃຫ້ຮອງຮັບການປັບປຸງດ້ານຄວາມປອດໄພຕັ້ງແຕ່ທຳອິດ.

ກ່ອນໜ້ານີ້ ຄວາມສ່ຽງຂອງການໃຊ້ອຸປະກອນ IoT ສ່ວນຫຼາຍຈະຖືກກ່າວເຖິງໃນຮູບແບບຂອງການສູນເສຍຄວາມເປັນສ່ວນຕົວເຊັ່ນ: ການເຈາະເຂົ້າລະບົບກ້ອງວົງຈອນປິດເພື່ອໃຊ້ລັກເບິ່ງ. ແຕ່ໃນປະຈຸບັນເນື່ອງຈາກມີການໃຊ້ອຸປະກອນ IoT ໃນຮູບແບບອື່ນໆ ເພີ່ມຫຼາຍຂຶ້ນ ກໍ່ເຮັດໃຫ້ຄວາມສ່ຽງໃນຮູບແບບອື່ນໆກໍ່ເພີ່ມຂຶ້ນຫຼາຍເຊັ່ນກັນ ເປັນຕົ້ນແມ່ນ ການເຈາະລະບົບອຸປະກອນທາງການແພດເພື່ອລັກເອົາຂໍ້ມູນດ້ານສຸຂະພາບ ຫຼື ເຮັດການປ່ຽນແປງການເຮັດວຽກຂອງອຸປະກອນດັ່ງກ່າວ ເຊິ່ງອາດຈະສົ່ງຜົນກະທົບຕໍ່ການປິ່ນປົວ ໄດ້ ຫຼື ຮ້າຍແຮງໄປກວ່ານັ້ນອາດຈະສົ່ງຜົນກະທົບຕໍ່ຊີວິດຂອງຄົນເຈັບໄດ້. ປະຈຸບັນ, ໜຶ່ງໃນບັນຫາທີ່ໃຫຍ່ທີ່ສຸດຂອງການໃຊ້ອຸປະກອນ IoT ແມ່ນເຈາະລະບົບເພື່ອຄວບຄຸມອຸປະກອນດັ່ງກ່າວມາໃຊ້ໃນການໂຈມຕີທາງໄຊເບີ (cyber). ຊຶ່ງໃນໄລຍະຜ່ານມາ ອຸປະກອນ IoT ເຄີຍຖືກຄວບຄຸມເພື່ອໃຊ້ໃນການໂຈມຕີທາງ cyber ຫຼາຍພໍສົມຄວນ, ສາເຫດຫຼັກແມ່ນເກີດຈາກອຸປະກອນຈຳນວນຫຼວງຫຼາຍຖືກຕິດຕັ້ງໂດຍການໃຊ້ລະຫັດຜ່ານທີ່ມາກັບໂຕອຸປະກອນເອງ (Default Password) ເຮັດໃຫ້ບຸກຄົນທີ່ມີບໍ່ຫວັງດີສາມາດເຂົ້າຫາລະບົບ (login) ເພື່ອໄປຕິດຕັ້ງ malware ໃນອຸປະກອນດັ່ງກ່າວ.



ບໍລິສັດ Gartner ຊຶ່ງເປັນບໍລິສັດທີ່ເຮັດການຄົ້ນຄວ້າ ວິໄຈ ແລະ ໃຫ້ຄຳແນະນຳດ້ານ ໄອທີ ຂອງສະຫະລັດອາເມລິກາ ໄດ້ສະຫຼຸບວ່າ ໃນປີ 2016 ມີການນຳໃຊ້ອຸປະກອນ IoT ເຖິງ 6,400 ລ້ານໜ່ວຍໃນທົ່ວໂລກ ແລະ ຄາດຄະເນວ່າຈະມີການເພີ່ມຂຶ້ນເຖິງ 3 ເທົ່າ ຫຼື ປະມານ 20,000 ລ້ານໜ່ວຍໃນປີ 2020. ສະຖິຕິດັ່ງກ່າວສະແດງໃຫ້ເຫັນເຖິງ

ຄວາມເປັນໄປໄດ້ທີ່ບັນຫາທີ່ກ່າວມານີ້ຈະມີແນວໂນ້ມເພີ່ມຂຶ້ນ ແລະ ເພີ່ມທະວີຄວາມຮຸນແຮງຂຶ້ນໄປເລື້ອຍໆ ເຊິ່ງເຮັດໃຫ້ຜູ້ໃຫ້ບໍລິການອິນເຕີເນັດ ແລະ ຜູ້ໃຫ້ບໍລິການຮັບມືກັບ DDos ຕ້ອງພະຍາຍາມຊອກຫາວິທີທາງໃນການຮັບມືຈາກການໂຈມຕີທີ່ມີຂະໜາດໃຫຍ່ຂຶ້ນໄປເລື້ອຍໆ ໃນຂະນະທີ່ໜ່ວຍງານລະດັບປະເທດ ແລະ ອົງການຈັດຕັ້ງຫຼາຍພາກສ່ວນເລີ່ມເບິ່ງບັນຫາ ແລະ ກະກຽມອອກນະໂຍບາຍ ຫລື ແນວທາງໃນການຮັບມືແລ້ວ.

ເນື່ອງຈາກອຸປະກອນ IoT ທີ່ຈໍາໜ່າຍໃນປະຈຸບັນ ສ່ວນໃຫຍ່ຖືກອອກແບບມາໃຫ້ມີລາຄາຖືກ ແລະ ສາມາດຕິດຕັ້ງ ແລະ ນໍາໃຊ້ໄດ້ງ່າຍ. ຜູ້ຜະລິດເຄື່ອງອຸປະກອນສ່ວນໃຫຍ່ຈຶ່ງບໍ່ໄດ້ໃຫ້ຄວາມສໍາຄັນ ແລະ ລົງທຶນດ້ານຄວາມໝັ້ນຄົງ ແລະ ຄວາມປອດໄພຂອງຜະລິດຕະພັນເຫຼົ່ານີ້ຫຼາຍ ເຮັດໃຫ້ເກີດບັນຫາພາຍຫຼັງເຊັ່ນ:

- ອຸປະກອນຖືກເປີດຊ່ອງທາງສໍາລັບໃຊ້ບໍລິຫານຈັດການ ການເຮັດວຽກຜ່ານລະບົບອິນເຕີເນັດ ໂດຍໃຊ້ລະຫັດຜ່ານທີ່ຖືກຕັ້ງຄ່າມາກັບໂຕເຄື່ອງເອງ ຫຼື ໃຊ້ ຊ່ອງທາງການເຊື່ອມຕໍ່ທີ່ບໍ່ມີການເຂົ້າລະຫັດລັບຂໍ້ມູນທີ່ຮັບສົ່ງ ເຮັດໃຫ້ຖືກບຸກຄົນບໍ່ຫວັງດີ ດັກຈັບລະຫັດຜ່ານໄດ້.
- ມີການຝັງ (hard-coded) ບັນຊີ ແລະ ລະຫັດຜ່ານສໍາລັບໃຊ້ຕັ້ງຄ່າການເຮັດວຽກໄວ້ໃນໂຕເຄື່ອງອຸປະກອນ ເຊິ່ງບັນຊີຜູ້ໃຊ້ບໍ່ສາມສາດປິດ ຫຼື ປ່ຽນລະຫັດຜ່ານໄດ້.
- ບໍລິສັດບໍ່ມີການພັດທະນາ ຫຼື ປັບປຸງຊ້ອບແວເພື່ອແກ້ໄຂຊ່ອງຫວ່າງຂອງບັນຫາທີ່ເກີດຂຶ້ນຂອງໂຕເຄື່ອງອຸປະກອນທີ່ໄດ້ຖືກວາງຂາຍໄປແລ້ວ ແລະ ບໍ່ມີຄວາມສາມາດໃນການປັບປຸງແກ້ໄຂຊ່ອງຫວ່າງຂອງບັນຫາໂດຍອັດຕະໂນມັດ ແລະ ບໍ່ມີຊ່ອງທາງໃຫ້ຜູ້ໃຊ້ສາມາດປັບປຸງແກ້ໄຂຊ່ອງຫວ່າງຂອງບັນຫາຂອງໂຕເຄື່ອງອຸປະກອນໄດ້.

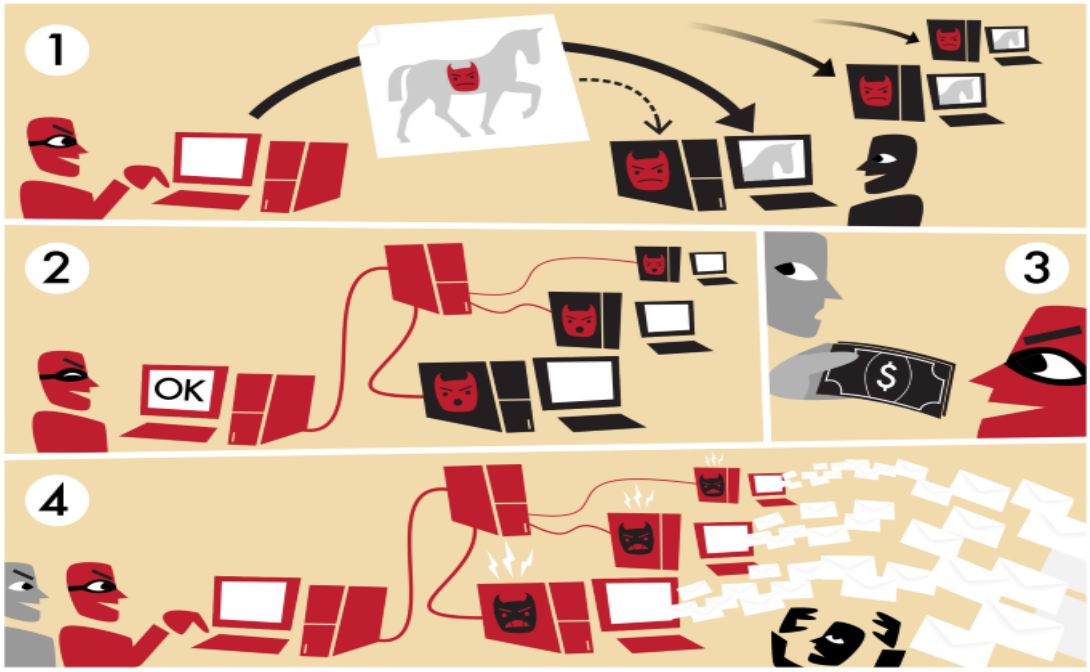
  ບັນຫາເຫຼົ່ານີ້ ເຮັດໃຫ້ເກີດຄວາມສ່ຽງທີ່ຜູ້ໃຊ້ອຸປະກອນ IoT ຈະຕົກເປັນເຫຍື່ອຈາກການຖືກໂຈມຕີ ຕັ້ງແຕ່ການສູນເສຍຄວາມເປັນສ່ວນຕົວ ຫຼື ຖືກໃຊ້ງານອຸປະກອນ IoT ເປັນຊ່ອງທາງໃນການໂຈມຕີບຸກຄົນຫຼື ໜ່ວຍງານອື່ນ.

Botnet ແລະ ການໂຈມຕີແບບ DDos .

Denial of Service (DoS) ແມ່ນການພະຍາຍາມໂຈມຕີລະບົບຄອມພິວເຕີເພື່ອເຮັດໃຫ້ບໍ່ສາມາດໃຊ້ບໍລິການໄດ້ ເຊິ່ງອາດເຮັດໄດ້ຫຼາຍວິທີເຊັ່ນວ່າ: ອັບໂຫຼດຟາຍທີ່ມີຂະໜາດໃຫຍ່ເຂົ້າໄປເພື່ອເຮັດໃຫ້ຮາດດິສເຕັມ, ພະຍາຍາມສັ່ງງານໃຫ້ເຄື່ອງເປີດໃຊ້ງານຫຼາຍໂປຣແກຣມເຮັດວຽກພ້ອມກັນເພື່ອໃຫ້ໜ່ວຍຄວາມຈໍາເຕັມ, ພະຍາຍາມສົ່ງຄໍາຮ້ອງຂໍເຂົ້າໄປຫາໜ່ວຍເຊີເວີຫຼາຍເທື່ອໃນຊ່ວງເວລາດຽວເພື່ອໃຫ້ແບນວິດເຄືອຂ່າຍເຕັມ ຫຼື ອາດໃຊ້ວິທີພື້ນຖານເຊັ່ນການຕັດລະບົບໄຟຟ້າເປັນຕົ້ນ.

ໃນເວລາຕໍ່ມາໄດ້ມີການພັດທະນາວິທີການໂຈມຕີມາໃຊ້ເຄື່ອງຄອມພິວເຕີຈໍານວນຫຼາຍ (ຕັ້ງແຕ່ຫຼັກພັນຫາ ຫຼັກແສນໜ່ວຍ) ເຂົ້າໂຈມຕີພ້ອມກັນວິທີນີ້ເອີ້ນວ່າ: Distributed Denial of Service (DDoS) ສ່ວນຫຼາຍການໂຈມຕີດ້ວຍວິທີນີ້ຈະໃຊ້ຊ້ອບແວເຂົ້າໄປຕິດຕັ້ງໃນໜ່ວຍຄອມພິວເຕີຂອງເຫຍື່ອເພື່ອລໍຖ້າຮັບຄໍາສັ່ງຈາກໜ່ວຍສັ່ງການ ໜ່ວຍທີ່

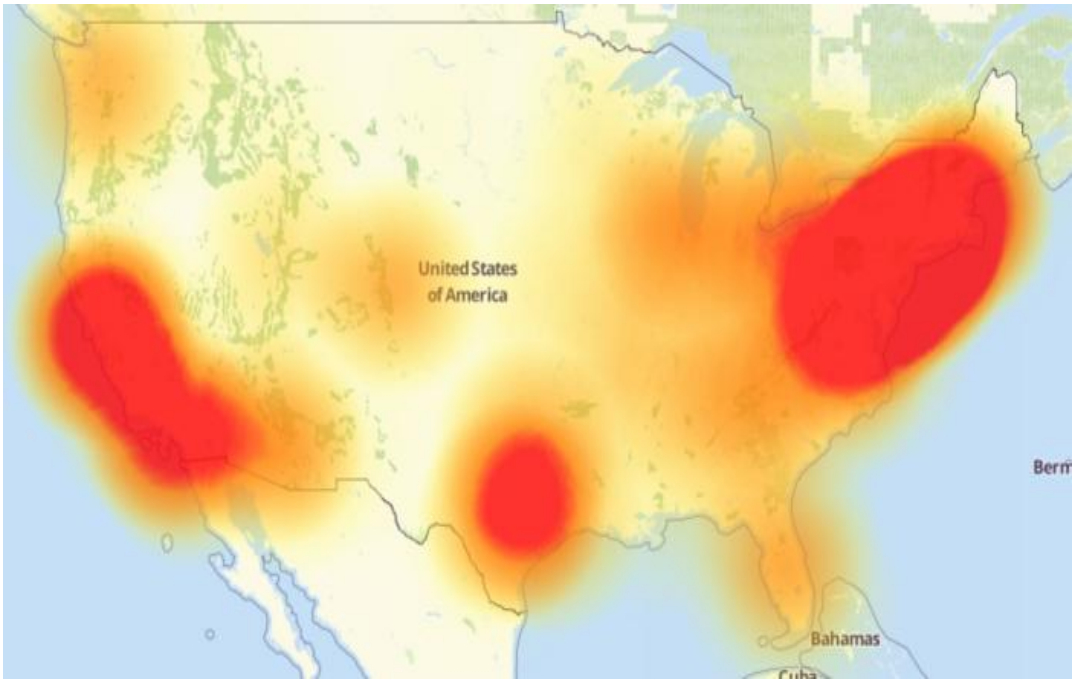
ຖືກຕິກເປັນເຫຍື່ອຈະຖືກເອີ້ນວ່າ robot ຫຼື zombie ເຄື່ອງທີ່ໃຊ້ຄວບຄຸມ ແລະ ສັ່ງການເອີ້ນວ່າ command & control ຫຼື C2 ຖ້າເຄື່ອງທີ່ເປັນເຫຍື່ອມີຈານວນຫຼາຍຈະເອີ້ນວ່າເປັນ botnet ເຊິ່ງຫຍໍ້ມາຈາກ Robot Network ຕົວຢ່າງການເຮັດວຽກຂອງ Botnet ສະແດງດັ່ງຮູບທີ່ 2



ຮູບທີ2: ຕົວຢ່າງການເຮັດວຽກຂອງ Botnet (ທີ່ມາ http://www.huffingtonpost.com)

ການໂຈມຕີແບບ DDoS ດ້ວຍ Mirai Malware

Mari ເປັນ malware ທີ່ຖືກພັດທະນາໃຫ້ມີຄວາມສາມາດໃນການເຈາะລະບົບເຂົ້າຄວບຄຸມອຸປະກອນ IoT ແລະ ໃຊ້ອຸປະກອນດັ່ງກ່າວໂຈມຕີເປົ້າໝາຍໃນຮູບແບບ DDoS. Malware ຊະນິດນີ້ຖືກຄົ້ນພົບໃນ ເດືອນ ສິງຫາ 2016 ຈາກການກວດສອບຊ່ວງ ເດືອນ ຕຸລາ 2016 ພົບເຄື່ອງອຸປະກອນທີ່ຕິດ malware ຊະນິດນີ້ສູງເຖິງ 493,000 ເຄື່ອງໃນທົ່ວໂລກ. ຈາກນັ້ນບໍ່ດົນ ທ້າຍເດືອນ ຕຸລາ ປີ 2016 ກໍ່ພົບເຫັນການໃຊ້ Mari Malware (ແລະ malware ທີ່ມີລັກສະນະຄ້າຍຄືກັນ) ໃນການຄວບຄຸມອຸປະກອນ IoT ເພື່ອໂຈມຕີ ບໍລິສັດ Dyn ຊຶ່ງເປັນບໍລິສັດຜູ້ໃຫ້ບໍລິການ DNS ສົ່ງຜົນກະທົບໃຫ້ເວັບໄຊຈໍານວນຫຼວງຫຼາຍບໍ່ສາມາດເຮັດວຽກໄດ້ຫຼາຍຊົ່ວໂມງ.



ຮູບທີ3 : ສະແດງການໂຈມຕີແບບ DDoS ບໍລິສັດ Dyn ເມື່ອທ້າຍເດືອນ ຕຸລາ 2016 (ທີ່ມາ-http://www.dailydot.com/layer8/dyn-ddos-twitter-reddit-east-coast)

ຈາກການວິເຄາະ Mirai Malware ເຮັດການໂຈມຕີແບບ DDoS ດ້ວຍການເຊື່ອມຕໍ່ຈາກອຸປະກອນໂດຍກົງ ຊຶ່ງບໍ່ໄດ້ໃຊ້ເຕັກນິກ amplification attack ຫຼື reflection attack ເພື່ອເພີ່ມປະສິດທິພາບໃນການໂຈມຕີຫຼືມີການປອມໝາຍເລກ IP (IP spoofing) ເພື່ອເຊື່ອງແຫຼ່ງທີ່ມາຂອງການໂຈມຕີ ແຕ່ຢ່າງໃດ, ຊຶ່ງການໂຈມຕີລັກສະນະນີ້ແມ່ນຍາກໃນການປ້ອງກັນ ເນື່ອງຈາກທາຟຟິກທີ່ເຂົ້າມາຈາກອຸປະກອນທີ່ຕິດ malware ກັບທາຟຟິກທີ່ມາຈາກການເຊື່ອມຕໍ່ຕາມປົກກະຕິນັ້ນເປັນແບບດຽວກັນ. Mirai malware ໄດ້ແຜ່ຂະຫຍາຍດ້ວຍການພະຍາຍາມເຂົ້າລະບົບອຸປະກອນ IoT ທີ່ເປີດພອດ Telonet ໂດຍໃຊ້ລະຫັດທີ່ມາກັບຕົວຂອງອຸປະກອນ ໃນໂຄ້ດຂອງ malware ມີລະຫັດຂອງອຸປະກອນທີ່ສາມາດເຂົ້າລະບົບໄດ້ຈຳນວນ 68 ລາຍການ. ຫຼັງຈາກເຂົ້າລະບົບສຳເລັດ malware ຈະຕິດຕັ້ງຕົວເອງໃນເຄື່ອງ ຈາກນັ້ນຈະປິດການເຮັດວຽກຂອງພອດ 22,23,80 ເຊິ່ງເປັນພອດທີ່ໃຊ້ສຳລັບການບໍລິຫານຈັດການເຄື່ອງອຸປະກອນຈາກໄລຍະໄກ ໂດຍຈຸດປະສົງໃນການປິດການເຮັດວຽກເຫຼົ່ານັ້ນເພື່ອປ້ອງກັນບໍ່ໃຫ້ຜູ້ໃຊ້ ເຂົ້າເຖິງການຕັ້ງຄ່າອຸປະກອນ ແລະ ປ້ອງກັນ malware ອື່ນບໍ່ໃຫ້ມາແຜ່ກະຈາຍລົງໃນອຸປະກອນຜ່ານພອດດັ່ງກ່າວ.
(ຜູ້ທີ່ສົນໃຈສາມາດເບິ່ງແຜນທີ່ການສະແດງການກວດສອບອຸປະກອນທີ່ຕິດ mirai Malware ໃນແຕ່ລະປະເທດໄດ້ທີ່ https://intel.malwaretech.com/botnet/mirai)

ບາງຂໍ້ແນະນຳໃນການເບິ່ງແຍງຄວາມໝັ້ນຄົງຄວາມປອດໄພຂອງອຸປະກອນ IoT

ບັນຫາຄວາມໝັ້ນຄົງຄວາມປອດໄພຂອງການໃຊ້ອຸປະກອນ IoT ນັ້ນໄດ້ຖືກຮັບຮູ້ມາໄດ້ໄລຍະໜຶ່ງ ແຕ່ເນື່ອງຈາກອຸປະກອນ IoT ໃນປະຈຸບັນຍັງຖືວ່າເປັນເລື່ອງທີ່ຍັງໃໝ່ພໍສົມຄວນ ມາດຕະການປ້ອງກັນໃນຮູບແບບນະໂຍບາຍອາດຈະຕ້ອງໃຊ້ເວລາອີກໄລຍະໃດໜຶ່ງ ແຕ່ໃນສ່ວນການປ້ອງກັນທາງດ້ານເຕັກນິກສາມາດເຮັດໄດ້ດັ່ງນີ້:

1) ຂໍ້ແນະນຳສຳລັບຜູ້ທີ່ໃຊ້ງານອຸປະກອນ IoT

- ບໍ່ໃຊ້ລະຫັດຜ່ານທີ່ມາກັບໂຕເຄື່ອງ (Default Password) ເນື່ອງຈາກລະຫັດຜ່ານເຫຼົ່ານັ້ນສາມາດຄົ້ນຫາໄດ້ທົ່ວໄປຈາກອິນເຕີເນັດ ແລະ malware ທີ່ໂຈມຕີອຸປະກອນ IoT ມີລະຫັດຜ່ານຂອງອຸປະກອນ IoT ສ່ວນໃຫຍ່ມີລະຫັດດັ່ງກ່າວໃນຖານຂໍ້ມູນ ເຮັດໃຫ້ສາມາດເຊື່ອມຕໍ່ເຂົ້າມາຄວບຄຸມເຄື່ອງໄດ້ທັນທີ.
- ບໍ່ຕ້ອງເຊື່ອມຕໍ່ອິນເຕີເນັດຫາກບໍ່ມີຄວາມຈຳເປັນ ເພາະອຸປະກອນ IoT ບາງຢ່າງເຊັ່ນ: ຕູ້ຊັກເຄື່ອງ, ເຄື່ອງຊົງກາເຟ ຜູ້ໃຊ້ມັກຈະມີຄວາມຈຳເປັນຕ້ອງໃຊ້ງານອຸປະກອນເຫຼົ່ານີ້ເມື່ອຢູ່ເຮືອນເທົ່ານັ້ນ ການເປີດໃຫ້ອຸປະກອນເຫຼົ່ານີ້ສາມາດເຂົ້າເຖິງໄດ້ໂດຍຜ່ານເຄືອຂ່າຍອິນເຕີເນັດອາດເປັນສິ່ງທີ່ບໍ່ຈຳເປັນ ແລະເພີ່ມຄວາມສ່ຽງດ້ານຄວາມປອດໄພ.
- ປິດການເຂົ້າຫາການຕັ້ງຄ່າຂອງເຄື່ອງອຸປະກອນໄດ້ຈາກອິນເຕີເນັດ ອຸປະກອນຫຼາຍລຸ້ນສາມາດຕັ້ງຄ່າໃຫ້ປິດການເຂົ້າເຖິງສ່ວນທີ່ຄວບຄຸມການເຮັດວຽກຂອງອຸປະກອນຈາກພາຍນອກໄດ້ ເພື່ອຊ່ວຍຫຼຸດຄວາມເສຍຫາຍຈາກຜູ້ທີ່ບໍ່ຫວັງດີເຊື່ອມຕໍ່ເຂົ້າຄວບຄຸມເຄື່ອງ
- ຕິດຕາມຂ່າວສານ ແລະ ອັບເດດ firmware ເປັນປະຈຳ ຜູ້ຜະລິດຈະມີການອັບເດດ firmware ຂອງອຸປະກອນແຕ່ລະໄລຍະ ແລະ ຫຼາຍເທື່ອມັກມີການແກ້ໄຂຊ່ອງຫວ່າງຂອງບັນຫາດ້ານຄວາມປອດໄພລວມຢູ່ນຳ. ຜູ້ໃຊ້ຄວນກວດສອບ ແລະ ອັບເດດ firmware ໃຫ້ເປັນເວີເຊິນລ່າສຸດຢູ່ເລື້ອຍໆເພື່ອຄວາມປອດໄພ.
- ຖ້າພົບຄວາມຜິດປົກກະຕິອາດຈະລອງ reboot ເນື່ອງຈາກ malware ໃນ IoT ສ່ວນໃຫຍ່ຈະເຮັດວຽກຢູ່ໃນໜ່ວຍຄວາມຈຳຂອງເຄື່ອງເທົ່ານັ້ນ ການ reboot ອາດຊ່ວຍໃຫ້ສາມາດລຶບ malware ໄດ້ (ເມື່ອ reboot ສຳເລັດແລ້ວ ຄວນປ່ຽນລະຫັດຜ່ານເພື່ອປ້ອງກັນບໍ່ໃຫ້ກັບມາອີກເທື່ອໜຶ່ງ)

2) ບົດບາດຂອງໜ່ວຍງານພາກລັດ ໃນດ້ານຄວາມປອດໄພຂອງການໃຊ້ງານ IoT

ສາເຫດອີກອັນໜຶ່ງຂອງບັນຫາຄວາມປອດໄພໃນການໃຊ້ງານອຸປະກອນ IoT ແມ່ນ ຍັງບໍ່ມີການກຳນົດມາດຕະຖານແນວທາງການພັດທະນາອຸປະກອນໃຫ້ມີຄວາມປອດໄພທີ່ດີພໍ, ຍັງບໍ່ມີການກຳນົດແນວທາງຄວາມຮັບຜິດຊອບຖ້າເກີດບັນຫາຈາກການໃຊ້ງານອຸປະກອນຈຳພວກນີ້ ເຊິ່ງໃນກໍລະນີນີ້ ທາງໜ່ວຍງານລັດຈຳເປັນຕ້ອງເຂົ້າມາເຮັດໜ້າທີ່ ຄວບຄຸມ ແລະ ເບິ່ງແຍງ.

ເຖິງແນວໃດກໍ່ຕາມ ບັນຫານີ້ຈຳເປັນຕ້ອງໄດ້ຮັບຄວາມຮ່ວມມືຈາກຫຼາຍໆ ພາກສ່ວນໃນການກຳນົດແນວທາງຕັ້ງແຕ່ການເລີ່ມຜະລິດ, ການຕິດຕັ້ງ ແລະ ການໃຊ້ງານຂອງອຸປະກອນ IoT ພ້ອມທັງຫາມາດຕະການປ້ອງກັນ ແລະ ແກ້ໄຂບັນຫານີ້. ປະຈຸບັນ ໜ່ວຍງານພາກລັດໃນຫຼາຍໆ ປະເທດໄດ້ເລີ່ມໃຫ້ມີຄວາມສຳຄັນກັບບັນຫາການຄວບຄຸມ ຫຼື ກຳນົດແນວທາງການໃຊ້ງານອຸປະກອນ IoT ຫຼາຍຂຶ້ນ ແລະ ໄດ້ອອກເອກະສານ ເຜີຍແຜ່ ແລະ ຂໍ້ແນະນຳໃນການພັດທະນາ ແລະ ໃຊ້ງານອຸປະກອນ IoT ຈາກໜ່ວຍງານຕ່າງໆເຊັ່ນ:

- ສະຫະພາບຢູໂຣບ ຫຼື EU ຕຽມຮ່າງຂໍ້ກຳນົດດ້ານຄວາມປອດໄພເພື່ອການຄວບຄຸມ ຕິດຕັ້ງ ແລະ ໃຊ້ງານອຸປະກອນ IoT https://krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/
- ໜ່ວຍງານ NITA ສະຫະລັດອາເມລິກາ ກະກຽມຮ່າງຂໍ້ແນະນຳໃນການອອກແບບຊ່ອງທາງການອັບເດດຂອງປະກອນ IoT https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security
- ກຸ່ມ Cloud Security Alliance (CSA) ເຜີຍແຜ່ເອກະສານຂໍ້ແນະນຳໃນການອອກແບບແລະພັດທະນາອຸປະກອນ IoT ຢ່າງໝັ້ນຄົງ https://www.thaicert.or.th/newsbite/2016-10-10-02.html
- ເອກະສານ NIST Special Publication 800-160: System Security Engineering http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
- Homeland Security ເຜີຍແຜ່ຂໍ້ແນະນຳດ້ານຄວາມໝັ້ນຄົງປອດໄພໃນການນຳໃຊ້ອຸປະກອນ IoT https://www.dhs.gov/securingtheIoT

ປະຈຸບັນແນວທາງການປະຕິບັດເຫຼົ່ານີ້ ຍັງຕ້ອງອາໄສໜ່ວຍງານກາງໃນການຄວບຄຸມ ແລະ ອາໄສຄວາມຮ່ວມມືຈາກຜູ້ຜະລິດ ແລະ ຜູ້ໃຊ້ອຸປະກອນໃນການປະຕິບັດຕາມ.

(ໂດຍ: ຈິດຕະພອນ ຈັນສີລິລາດ)