ຄຳແນະນຳ APT40

ງານຝຶກ ຳ MSS ຂອງ PRC ກ ຳລັງດ ຳເນີນການ

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

ສາລະບານ

ພາບລວມ

ຄວາມເປັນມາ

ຄໍາແນະນໍານີ້, ຂຽນໂດຍສູນຄວາມໝັ້ນຄົງປອດໄພທາງໄຊເບີຂອງອົດສະຕາລີ (ACSC) ຂອງສໍານັກງານສັນຍານອົດສະຕາລີ (ASD), ອົງກອນຄວາມປອດໄພທາງໄຊເບີ ແລະ ໂຄງສ້າງພື້ນຖານຂອງສະຫະລັດ (CISA), ອົງກອນຄວາມປອດໄພແຫ່ງຊາດສະຫະລັດ (NSA), ຫ້ອງການສືບສວນຂອງລັດຖະບານກາງສະຫະລັດ (FBI), ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງສະຫະລາຊະອານາຈັກ (NCSC-UK), ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງເຄນາດາ (CCCS) ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງນິວຊີແລນ (NCSC-NZ), ສູນບໍລິການຂ່າວລັບຂອງລັດຖະບານກາງເຢຍລະມັນ (BND) ແລະ ສໍານັກງານລັດຖະບານກາງເພື່ອປົກປ້ອງລັດຖະທໍາມະນູນ (BfV), ໜ່ວຍຂ່າວກອງແຫ່ງຊາດຂອງສາທາລະນະລັດເກົາຫຼີ (NIS) ແລະ ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງ NIS ແລະ ສູນຄວາມພ້ອມຮັບມືກັບເຫດການ ແລະ ຍຸດທະສາດແຫ່ງຊາດຂອງຍີ່ປຸ່ນ (NISC) ແລະ ອົງການຕໍາຫຼວດແຫ່ງຊາດ (NPA) ເຊິ່ງຕໍ່ໄປນີ້ ຈະເອີ້ນວ່າ "ໜ່ວຍງານຜູ້ຂຽນ" ໂດຍໄດ້ສະຫຼຸບກຸ່ມໄຊເບີທີ່ໄດ້ຮັບການສະໜັບສະໜູນຈາກລັດຖະບານຂອງສາທາລະນະລັດ ປະຊາຊົນຈີນ (PRC) ແລະ ໄພຄຸກຄາມຕໍ່ເຄືອຂ່າຍຂອງອົດສະຕາລີໃນປະຈຸບັນ. ຄໍາແນະນໍາດັ່ງກ່າວໄດ້ດຶງດູດຄວາມເຂົ້າໃຈຮ່ວມກັນຂອງອົງກອນຜູ້ຂຽນກ່ຽວກັບໄພຂົ່ມຂູ່ເຊັ່ນດຽວກັນກັບການສືບສວນການຕອບໂຕ້ກັບເຫດການ ACSC ຂອງ ASD.

ກຸ່ມໄຊເບີໄດ້ຮັບການສະໜັບສະໜູນຈາກລັດຂອງ PRC ເຄີຍໂຈມຕີອົງກອນຕ່າງໆ ໃນປະເທດໃນຫຼາຍໆປະເທດມາກ່ອນ, ລວມທັງອົດສະຕາລີ ແລະ ສະຫະລັດອາເມລິກາ ແລະ ເຕັກນິກທີ່ຊີ້ ໃຫ້ເຫັນຂ້າງລຸ່ມນີ້ ແມ່ນຖືກນໍາໃຊ້ເປັນປະຈໍາໂດຍອົງກອນອື່ນໆ ທີ່ໄດ້ຮັບການສະໜັບສະໜູນຈາກລັດຖະບານຂອງ PRC ທົ່ວໂລກ. ດັ່ງນັ້ນ, ອົງກອນຜູ້ຂຽນເຊື່ອວ່າກຸ່ມດັ່ງກ່າວ ແລະ ເຕັກນິກທີ່ຄ້າຍຄືກັນຍັງຄົງເປັນໄພຂົ່ມຂູ່ຕໍ່ເຄືອຂ່າຍຂອງປະເທດຂອງພວກເຂົາເຊັ່ນກັນ.

ໜ່ວຍງານຜູ້ຂຽນປະເມີນວ່າກຸ່ມນີ້ ດໍາເນີນການດໍາເນີນງານທາງໄຊເບີທີ່ເປັນອັນຕະລາຍຕໍ່ກະຊວງຄວາມປອດໄພຂອງສາທາລະນະລັດປະຊາຊົນຈີນ (MSS). ກິດຈະກໍາ ແລະ ເຕັກນິກການທັບຊ້ອນກັບກຸ່ມທີ່ຖືກຕິດຕາມເປັນໄພຄຸກຄາມຂັ້ນສູງຕໍ່ເນື່ອງ (APT) 40 (ຍັງເອີ້ນວ່າ Kryptonite Panda, GINGHAM TYPHOON, Leviathan ແລະ Bronze Mohawk ໃນການລາຍງານອຸດສາຫະກໍາ). ກ່ອນໜ້ານີ້ ມີລາຍງານວ່າກຸ່ມນີ້ ມີຖານຢູ່ທີ່ໄຮກູ, ແຂວງໄຫໜານ ສາທາລະນະລັດປະຊາຊົນຈີນ ແລະ ໄດ້ຮັບມອບໝາຍວຽກຈາກສໍານັກງານຄວາມໝັ້ນຄົງແຫ່ງລັດໄຫໜານ (MSS) ຂອງສາທາລະນະລັດປະຊາຊົນຈີນ.[2] ຄໍາແນະນໍາຕໍ່ໄປນີ້ ສະແດງຕົວຢ່າງຂອງກໍລະນີສຶກສາທີ່ສໍາຄັນກ່ຽວກັບເຕັກນິກຂອງຝ່າຍກົງກັນຂ້າມໃນການດໍາເນີນການກັບເຄືອຂ່າຍຜູ້ເຄາະຮ້າຍສອງເຄືອຂ່າຍ. ກໍລະນີສຶກສາເຫຼົ່ານີ້ ມີຄວາມສໍາຄັນຕໍ່ຝ່າຍຜູ້ປະຕິບັດງານດ້ານຄວາມປອດໄພທາງໄຊເບີໃນການລະບຸ, ປ້ອງກັນ ແລະ ແກ້ໄຂການບຸກລຸກ APT40 ຕໍ່ເຄືອຂ່າຍຂອງຕົນເອງ. ກໍລະນີສຶກສາທີ່ຖືກຄັດເລືອກແມ່ນກໍລະນີທີ່ມີການດໍາເນີນການແກ້ໄຂທີ່ເໝາະສົມ ເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງໃນການໃຊ້ປະໂຫຍດຊໍ້າຕໍ່ໄພຄຸກຄາມລາຍນີ້ ຫຼື ລາຍອື່ນໆ. ດັ່ງນັ້ນ, ກໍລະນີສຶກສາແມ່ນມີອາຍຸຕາມທໍາມະຊາດ, ເພື່ອໃຫ້ແນ່ໃຈວ່າອົງກອນຕ່າງໆ ໄດ້ຮັບເວລາທີ່ຈໍາເປັນໃນການແກ້ໄຂບັນຫາ.

ສະຫຼຸບການເຄື່ອນໄຫວ

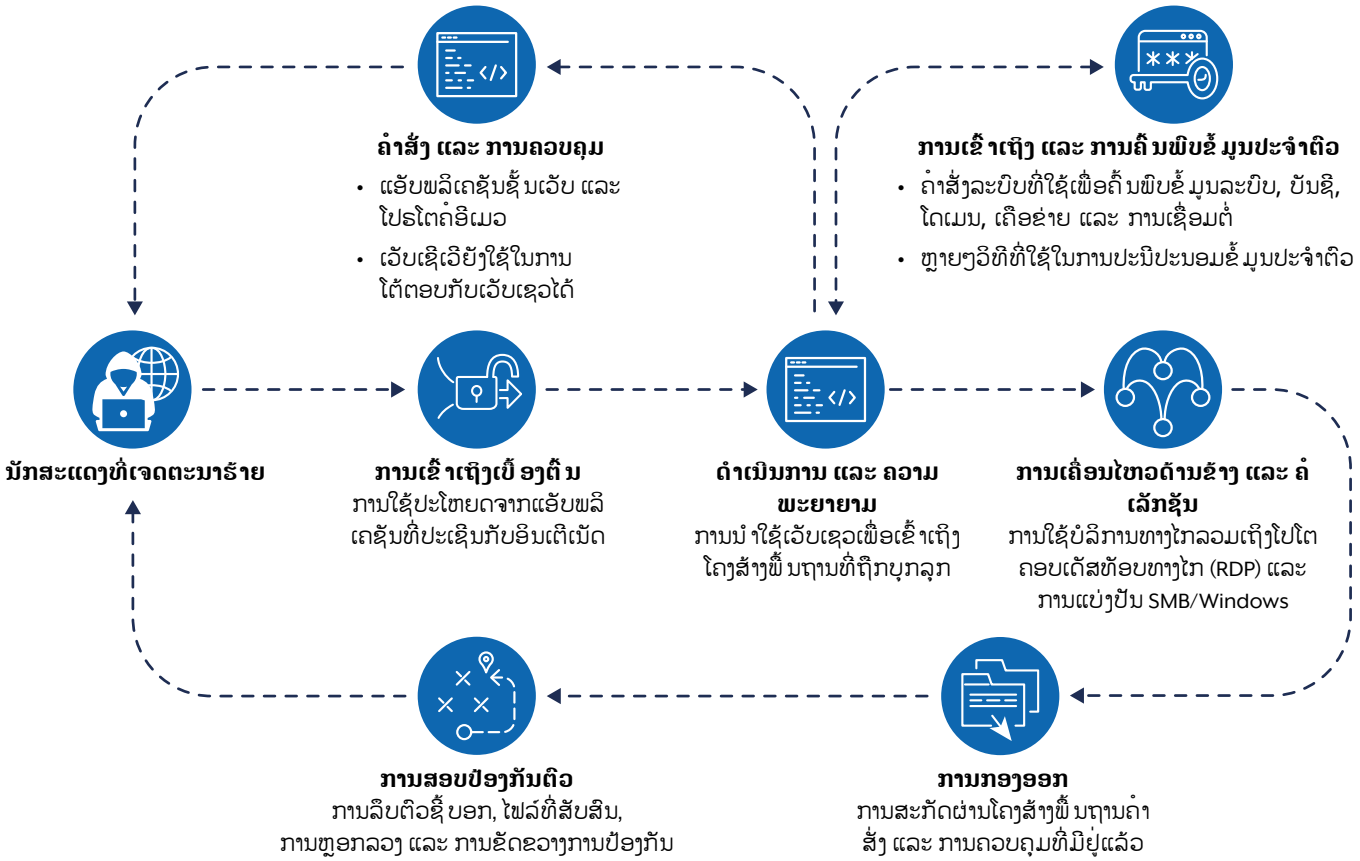
APT40 ໄດ້ໂຈມຕີເຄືອຂ່າຍຂອງອົດສະຕາລີ ລວມທັງເຄືອຂ່າຍພາກລັດ ແລະ ເອກະຊົນໃນພາກພື້ນ ແລະ ໄພຂົ່ມຂູ່ຕໍ່ເຄືອຂ່າຍຂອງພວກເຮົາແມ່ນດໍາເນີນຢູ່ຕໍ່ໄປ. ການຄ້າທີ່ອະທິບາຍໄວ້ໃນຄໍາແນະນໍານີ້ ໄດ້ຮັບການກວດສອບເປັນປະຈໍາກັບເຄືອຂ່າຍຂອງອົດສະຕາລີ.

ເປັນທີ່ໜ້າສັງເກດ, APT40 ມີຄວາມສາມາດໃນການປ່ຽນແປງ ແລະ ປັບຕົວການຂຸດຄົ້ນແນວຄວາມຄິດ (POCs) ຂອງຊ່ອງໂຫວ່ໃໝ່ໆ ແລະ ນໍາໃຊ້ກັບເຄືອຂ່າຍເປົ້າໝາຍທີ່ມີໂຄງສ້າງພື້ນຖານຂອງຊ່ອງໂຫວ່ທີ່ກ່ຽວຂ້ອງໄດ້ທັນທີ. APT40 ດໍາເນີນການລາດຕະເວນເຄືອຂ່າຍທີ່ມີຄວາມສົນໃຈເປັນປະຈໍາ, ລວມທັງເຄືອຂ່າຍໃນປະເທດຂອງອົງກອນຜູ້ຂຽນ, ເພື່ອຊອກຫາໂອກາດທີ່ຈະເຈາະເປົ້າໝາຍ. ການລາດຕະເວນປົກກະຕິນີ້ ເຮັດໃຫ້ກຸ່ມສາມາດລະບຸອຸປະກອນທີ່ມີຄວາມສ່ຽງ, ອຸປະກອນທີ່ໝົດອາຍຸການໃຊ້ງານ ຫຼື ອຸປະກອນທີ່ບໍ່ໄດ້ຮັບການດູແລອີກຕໍ່ໄປໃນເຄືອຂ່າຍທີ່ໜ້າສົນໃຈ ແລະ ປັບໃຊ້ການທົດສອບຢ່າງວ່ອງໄວ. APT40 ຍັງຄົງປະສົບຄວາມສໍາເລັດໃນການໃຊ້ປະໂຫຍດຈາກຊ່ອງຫວ່າງຕັ້ງແຕ່ປີ 2017.

APT40 ໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫວ່ສາທາລະນະໃໝ່ໆ ໃນຊອບແວທີ່ໃຊ້ກັນຢ່າງກວ້າງຂວາງ ເຊັ່ນ: Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) ແລະ Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ACSC ຂອງ ASD ແລະ ໜ່ວຍງານຜູ້ຂຽນຄາດວ່າກຸ່ມຈະຍັງຄົງນໍາໃຊ້ POCs ສໍາລັບຊ່ອງໂຫວ່ທີ່ມີຊື່ສຽງໃໝ່ໆ ຕໍ່ໄປພາຍໃນຊົ່ວໂມງ ຫຼື ສອງສາມມື້ ຫຼັງຈາກເຜີຍແຜ່ສູ່ສາທາລະນະ.

2 ກະຊວງຍຸຕິທໍາຂອງສະຫະລັດ. 2021. ຊາວຈີນສີ່ຄົນທີ່ເຮັດວຽກຮ່ວມກັບກະຊວງຄວາມໝັ້ນຄົງແຫ່ງລັດຖືກກ່າວຫາວ່າມີແຄມເປນການບຸກລຸກຄອມພິວເຕີທົ່ວໂລກໂດຍແນເປົ້າໝາຍໃສ່ຊັບສິນທາງປັນຍາ ແລະ ຂໍ້ມູນທາງທຸລະກິດທີ່ເປັນຄວາມລັບ, ລວມທັງການຄົ້ນຄວ້າພະຍາດຕິດເຊື້ອ.

ຮູບທີ 1. ຕາຕະລາງການໄຫຼວຽນຂອງ TTP ສຳລັບກິດຈະກຳ APT40



ກຸ່ມນີ້ ເບິ່ງຄືຈະມັກທີ່ຈະໃຊ້ປະໂຫຍດຈາກໂຄງສ້າງພື້ ນຖານທີ່ ສ່ຽງຕໍ່ການເຂົ້ າເຖິງສາທາລະນະຫຼາຍກວ່າເຕັກນິກທີ່ຕ້ອງການ ການໂຕ້ຕອບຂອງຜູ້ ໃຊ້, ເຊັ່ນແຄມເປນຟິດຊິ ງ ແລະ ໃຫ້ຄວາມ ສຳຄັນສູງໃນການໄດ້ຮັບຂໍ້ ມູນປະຈຳຕົວທີ່ຖືກຕ້ອງເພື່ອ ໃຫ້ສາມາດດຳເນີນກິດຈະກຳຕໍ່ເນື່ອງໄດ້. APT40 ມັກໃຊ້ເວັບ ເຊວ (T1505.003) ເພື່ອຄວາມຄົງຕົວ, ໂດຍສະເພາະໃນຕົ ນໆ ຂອງວົງຈອນຊີວິດຂອງການບຸກລຸກ. ໂດຍປົກກະຕິ, ຫຼັງຈາກ ການເຂົ້ າເຖິງເບື້ ອງຕົ ນສົບຜົນສຳເລັດ APT40 ສຸມໃສ່ການສ້າງ ຄວາມຄົງທີ່ ເພື່ອຮັກສາການເຂົ້ າເຖິງສະພາບແວດລ້ອມຂອງ ຜູ້ ຖືກເຄາະຮ້າຍ. ຢ່າງໃດກໍ່ຕາມ, ເນື່ອງຈາກຄວາມຄົງຄ້ ງ ເກີດຂຶ້ ນໃນຕອນຕົ ນຂອງການບຸກລຸກ, ຈຶ່ງມີແນວໂນ້ມທີ່ຈະ ສັງເກດເຫັນການບຸກລຸກ - ໂດຍບໍ່ຄຳນຶງເຖິງຂອບເຂດຂອງ ການປະນີປະນອມ ຫຼື ການດຳເນີນການຕໍ່ໄປ.

ງານຝີມືທີ່ໂດດເດັ່ນ

ເຖິງແມ່ນວ່າ APT40 ຜ່ານມາເຄີຍໃຊ້ເວັບໄຊທ໌ຂອງອົດສະ ຕຣາລີທີ່ຖືກບຸກລຸກເປັນຄຳສັ່ງ ແລະ ການຄວບຄຸມ (C2) ສຳ ລັບການປະຕິບັດງານມາກ່ອນ, ແຕ່ກຸ່ມດັ່ງກ່າວໄດ້ພັດທະນາ ເຕັກນິກນີ້ ຂຶ້ ນມາ (T1594).

APT40 ໄດ້ນຳແນວໂນ້ມທົ່ວໂລກມາໃຊ້ໃນການໃຊ້ອຸປະກອນ ທີ່ຖືກບຸກລຸກ, ລວມທັງອຸປະກອນສຳນັກງານຂະໜາດນ້ອຍ/ ສຳນັກງານຢູ່ບ້ານ (SOHO), ເປັນໂຄງສ້າງພື້ ນຖານດ້ານ ການປະຕິບັດງານ ແລະ ຕົວຊີ້ ທິດທາງສຸດທ້າຍ (T1584.008) ສຳລັບການປະຕິບັດງານຢູ່ໃນອົດສະຕາລີ. ສິ່ງນີ້ ໄດ້ເຮັດໃຫ້ ໜ່ວຍງານຜູ້ ຂຽນສາມາດກຳນົດລັກສະນະ ແລະ ຕິດຕາມ ການເຄື່ອນໄຫວຂອງກຸ່ມນີ້ ໄດ້ດີຍິ່ງຂຶ້ ນ.

ອຸປະກອນ SOHO ເຫຼົ່ານີ້ ຈຳນວນຫຼາຍແມ່ນອຸປະກອນທີ່ໃກ້ ໝົດອາຍຸການໃຊ້ງານ ຫຼື ບໍ່ໄດ້ຮັບການແກ້ໄຂ ແລະ ມັກຖືກ ໂຈມຕີແບບ N-day. ເມື່ອຖືກບຸກລຸກ, ອຸປະກອນ SOHO ຈະ ກາຍເປັນຈຸດເລີ່ມຕົ ນຂອງການໂຈມຕີທີ່ຖືກອອກແບບມາເພື່ອ ປະສົມກັບການຮັບສິ່ງຂໍ້ ມູນທີ່ຖືກກົດໝາຍ ແລະ ທ້າທາຍຜູ້ ປົກປ້ອງເຄືອຂ່າຍ (T1001.003).

ເຕັກນິກນີ້ ຍັງຖືກນຳໃຊ້ເປັນປົກກະຕິໂດຍໜ່ວຍງານອື່ນໆ ທີ່ໄດ້ຮັບການສະໜັບສະໜຸນຈາກລັດຂອງສາທາລະນະລັດ ປະຊາຊົນຈີນທົ່ວໂລກ ແລະ ໜ່ວຍງານຜູ້ ຂຽນຖືວ່ານີ້ ຖືວ່າ ເປັນໄພຂົ່ມຂູ່ຮ່ວມກັນ. ສຳລັບຂໍ້ ມູນເພີ່ມເຕີມ, ເບິ່ງຄຳ ແນະນຳຮ່ວມກັນ ຜູ້ ກະທຳຄວາມຜິດທາງໄຊເບີທີ່ໄດ້ຮັບ ການສະໜັບສະໜຸນຈາກສາທາລະນະລັດປະຊາຊົນຈີນໃຊ້ ປະໂຫຍດຈາກຜູ້ ໃຫ້ບໍລິການເຄືອຂ່າຍ ແລະ ອຸປະກອນ ແລະ ຜູ້ ກະທຳຄວາມຜິດທີ່ໄດ້ຮັບການສະໜັບສະໜຸນຈາກ ລັດຖະບານສາທາລະນະລັດປະຊາຊົນຈີນລະເມີດ ແລະ ຮັກສາການເຂົ້ າເຖິງໂຄງສ້າງພື້ ນຖານທີ່ສຳຄັນຂອງສະຫະລັດ ຢ່າງຕໍ່ເນື່ອງ.

APT40 ບາງຄັ້ງກໍ່ໃຊ້ໂຄງສ້າງພື້ ນຖານທີ່ຊື້ ຫຼື ເຊົ່າເປັນພື້ ນຖານ ໂຄງລ່າງ C2 ທີ່ປະເຊີນກັບຜູ້ ເຄາະຮ້າຍໃນການດຳເນີນງານຂອງ ຕົນ; ແນວໃດກໍດີ, ການຄ້ າປະເພດນີ້ ເບິ່ງຄືຈະຢູ່ໃນຊ່ວງກົດ ຖອຍເມື່ອທຽບກັບຕະຫຼາດອື່ນໆ.

ເຄື່ອງມື

ACSC ຂອງ ASD ກຳລັງແບ່ງປັນບາງໄຟລ໌ທີ່ເປັນອັນຕະລາຍ ທີ່ໄດ້ລະບຸໄວ້ໃນລະຫວ່າງການສືບສວນທີ່ລະບຸໄວ້ຂ້າງລຸ່ມນີ້. ໄຟລ໌ເຫຼົ່ານີ້ ໄດ້ຮັບການອັບໂຫຼດໄປຍັງ VirusTotal ເພື່ອເຮັດໃຫ້ ການປ້ອງກັນເຄືອຂ່າຍ ແລະ ຊຸມຊົນຄວາມປອດໄພທາງໄຊເບີ ທີ່ກວ້າງຂຶ້ ນ ເພື່ອເຂົ້ າໃຈການຂົ່ມຂູ່ທີ່ຈຳເປັນຕ້ອງປ້ອງກັນໄດ້ ດີຍິ່ງຂຶ້ ນ.

ກໍລະນີສຶກສາ

ACSC ຂອງ ASD ກຳລັງແບ່ງປັນສອງບົດລາຍງານການ ສືບສວນທີ່ບໍ່ເປີດເຜີຍຊື່ເພື່ອໃຫ້ຄວາມຮູ້ ກ່ຽວກັບວິທີການທີ່ ຜູ້ ກ່ຽວຂ້ອງນຳໃຊ້ເຄື່ອງມື ແລະ ອາຊີບຂອງຕົນ.

MD5	ຊື່ໄຟລ໌	ຂໍ້ ມູນເພີ່ມເຕີມ
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_ jsp$TomcatListenerMemShellFromThread. class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

ກໍລະນີສຶກສາ 1

ບົດລາຍງານນີ້ ຖືກເຮັດໃຫ້ບໍ່ລະບຸຊື່ ເພື່ອໃຫ້ສາມາດເຜີຍແຜ່ ໄດ້ກວ້າງຂວາງຍິ່ງຂຶ້ ນ. ຕໍ່ໄປນີ້ ອົງກອນທີ່ໄດ້ຮັບຜົນກະທົບຈະ ເອີ້ ນວ່າ 'ອົງກອນ'. ລາຍລະອຽດສະເພາະບາງສ່ວນໄດ້ຖືກລຶບ ອອກ ເພື່ອປົກປ້ອງຕົວຕົນຂອງຜູ້ ເຄາະຮ້າຍ ແລະ ວິທີການຕອບ ໂຕ້ເຫດການຂອງ ACSC ຂອງ ASD.

ສະຫຼຸບສັງລວມ

ບົດລາຍງານນີ້ ໃຫ້ລາຍລະອຽດກ່ຽວກັບຜົນການສືບສວນ ACSC ຂອງ ASD ໃນການປະນີປະນອມສົບຜົນສຳເລັດຂອງ ເຄືອຂ່າຍອົງກອນລະຫວ່າງເດືອນກໍລະກົດຫາເດືອນກັນຍາ 2022. ບົດລາຍງານການສືບສວນນີ້ ໄດ້ຖືກສະໜອງໃຫ້ອົງກອນ ເພື່ອສະຫຼຸບກິດຈະກຳທີ່ເປັນອັນຕະລາຍ ແລະ ການກຳນົດ ຄຳແນະນຳໃນການແກ້ໄຂ. ຜົນການວິໄຈພົບວ່າ APT40 ເປັນ ຜູ້ ດຳເນີນການປະນີປະນອມ.

ໃນສ່ວນກາງເດືອນສິງຫາ, ACSC ຂອງ ASD ໄດ້ແຈ້ງໃຫ້ ອົງກອນຊາບເຖິງການໂຕ້ຕອບທີ່ເປັນອັນຕະລາຍກັບເຄືອຂ່າຍ ຂອງພວກເຂົາຈາກອຸປະກອນທີ່ອາດຈະຖືກບຸກລຸກເຊິ່ງກຸ່ ມ ດັ່ງກ່າວໃຊ້ໃນທ້າຍເດືອນສິງຫາ ແລະ ດ້ວຍການຍິນຍອມຂອງ ອົງກອນ, ACSC ຂອງ ASD ໄດ້ນຳໃຊ້ເຊັນເຊີໄປໃຊ້ກັບໂຮດທີ່ ອາດຈະໄດ້ຮັບຜົນກະທົບໃນເຄືອຂ່າຍຂອງອົງກອນ. ເຊັນເຊີ ເຫຼົ່ານີ້ ອະນຸຍາດໃຫ້ນັກວິເຄາະການຕອບສະໜອງຕໍ່ເຫດການ ຂອງ ASD ຂອງ ACSC ສາມາດດຳເນີນການສືບສວນທາງດ້ານ ນິຕິສາດທາງດິຈິຕອນຢ່າງລະອຽດ. ນັກວິເຄາະ ACSC ຂອງ ASD ປະສົບຜົນສຳເລັດໃນການວາງແຜນທີ່ກິດຈະກຳຂອງກຸ່ ມ ແລະ ສ້າງເສັ້ ນເວລາລາຍລະອຽດຂອງເຫດການທີ່ສັງເກດເຫັນ ໄດ້ໂດຍໃຊ້ຂໍ້ ມູນຊັບສິນທີ່ມີຢູ່.

ຕັ້ ງແຕ່ເດືອນກໍລະກົດຫາເດືອນສິງຫາ, ກິດຈະກຳຜູ້ ມີ ສ່ວນຮ່ວມທີ່ສຳຄັນທີ່ ACSC ຂອງ ASD ສັງເກດໄດ້ມີ:

- ການນັບໂຮດ, ເຊິ່ງເຮັດໃຫ້ຜູ້ ສະແດງສາມາດສ້າງແຜນທີ່ ເຄືອຂ່າຍຂອງຕົນເອງຂອງໄດ້;
- ການໃຊ້ເວັບເຊວ, ໃຫ້ຜູ້ ສະແດງມີຖານທີ່ໝັ້ ນເລີ່ມຕົ້ ນ ໃນເຄືອຂ່າຍ ແລະ ມີຄວາມສາມາດໃນການດຳເນີນການ ຄຳສັ່ງ ແລະ
- ການໃຊ້ງານເຄື່ອງມືອື່ນໆທີ່ຜູ້ ກະທຳນ ຳໃຊ້ປະໂຫຍດ ເພື່ອຈຸດປະສົງທີ່ເປັນອັນຕະລາຍ.

ການສືບສວນໄດ້ເປີດເຜີຍຫຼັກຖານຂອງຂໍ້ ມູນທີ່ລະອຽດ ອ່ອນຈຳນວນຫຼວງຫຼາຍທີ່ກຳລັງເຂົ້ າເຖິງ ແລະ ຫຼັກຖານທີ່ ສະແດງວ່າຜູ້ ກະທຳໄດ້ເຄື່ອນຍ້າຍໄປໃນແນວນອນຜ່ານເຄືອ ຂ່າຍ (T1021.002). ການປະນີປະນອມສ່ວນໃຫຍ່ເກີດຂຶ້ ນ ຈາກການກຸ່ ມຈັດຕັ້ ງເວັກເຕີ ການເຂົ້ າເຖິງຫຼາຍລາຍການໃນ ເຄືອຂ່າຍ, ເຄືອຂ່າຍທີ່ມີໂຄງສ້າງຮາບພຽງ ແລະ ການນຳໃຊ້ ຊອບແວທີ່ພັດທະນາພາຍໃນທີ່ບໍ່ປອດໄພທີ່ສາມາດຖືກນຳ ໃຊ້ໃນການອັບໂຫຼດໄຟລ໌ຕາມຕົນເອງມັກ. ຂໍ້ ມູນທີ່ຖືກລັດ ໄປປະກອບດ້ວຍຂໍ້ ມູນປະຈຳຕົວການກວດສອບສິດທິ ມີ ສິດພິເສດເຊິ່ງເຮັດໃຫ້ກຸ່ ມສາມາດເຂົ້ າສູ່ລະບົບໄດ້, ລວມທັ ງ ຂໍ້ ມູນເຄືອຂ່າຍທີ່ຊ່ວຍໃຫ້ຜູ້ ສະແດງສາມາດເຂົ້ າເຖິງ ໂດຍບໍ່ໄດ້ ຮັບການອະນຸຍາດໄດ້ອີກຄັ ງຖ້າເວັດເຕີເຂົ້ າເຖິງຕົ້ ນສະບັບຖືກ ບລັອກ. ບໍ່ພົບເຄື່ອງມືທີ່ເປັນອັນຕະລາຍເພີ່ມເຕີມນອກເໜືອ ໄປຈາກເຄື່ອງມືໃນເຄື່ອງທີ່ຖືກໃຊ້; ແນວໃດກໍ່ຕາມ, ການເຂົ້ າ ເຖິງຂໍ້ ມູນປະຈ ຳຕົວທີ່ຖືກຕ້ອງ ແລະ ມີສິດທິພິເສດຂອງກຸ່ ມ ໃດໜຶ່ງຈະປະຕິເສດຄວາມຕ້ອງການເຄື່ອງມືເພີ່ມເຕີມ. ຜົນ ການສອບສວນຊີ້ ໃຫ້ເຫັນວ່າອົງກອນດັ່ງກ່າວມີແນວໂນ້ມທີ່ ຈະຕົກເປັນເປົ້ າໝາຍຂອງ APT40 ໂດຍເຈດຕະນາ, ບໍ່ແມ່ນຕົກ ເປັນເຫຍື່ອຂອງຊ່ອງໂຫວ່ທີ່ເປີດເຜີຍຕໍ່ສາທາລະນະ.

ຜົນການສຶບສວນ

ໃນສ່ວນກາງເດືອນສິງຫາ 2022, ACSC ຂອງ ASD ແຈ້ງໃຫ້ອົງກອນດັ່ງກ່າວຮູ້ ວ່າ IP ທີ່ເປັນອັນຕະລາຍທີ່ໄດ້ຮັບການຢືນຢັນວ່າມີສ່ວນພົວພັນກັບກຸ່ມໄຊເບີທີ່ໄດ້ຮັບການສະໜັບສະໜູນຈາກລັດ ໄດ້ໂຕ້ຕອບກັບເຄືອຂ່າຍຄອມພິວເຕີຂອງອົງກອນລະຫວ່າງຢ່າງຫນ້ອຍເດືອນກໍລະກົດຫາເດືອນສິງຫາ. ອຸປະກອນທີ່ຖືກບຸກລຸກອາດຈະເປັນຂອງທຸລະກິດຂະໜາດນ້ອຍ ຫຼື ຜູ້ ໃຊ້ຢູ່ເຮືອນ.

ໃນຊ່ວງທ້າຍເດືອນສິງຫາ, ACSC ຂອງ ASD ໄດ້ປະຕິບັດຕົວແທນທີ່ໃຊ້ໂຮດໄປໃຊ້ກັບໂຮດໃນເຄືອຂ່າຍຂອງອົງກອນ ເຊິ່ງສະແດງໃຫ້ເຫັນຫຼັກຖານວ່າໄດ້ຮັບຜົນກະທົບຈາກການປະນີປະນອມດັ່ງກ່າວ.

ວັດຖຸປອມບາງຢ່າງທີ່ສາມາດສະໜັບສະໜູນຄວາມພະຍາຍາມໃນການສືບສວນບໍ່ສາມາດໃຊ້ງານໄດ້ເນື່ອງຈາກການກໍານົດຄ່າການບັນທຶກ ຫຼື ການອອກແບບເຄືອຂ່າຍ. ເຖິງວ່າຈະເປັນສິ່ງນີ້, ຄວາມພ້ອມຂອງອົງກອນໃນການຈັດກຽມຂໍ້ ມູນທີ່ມີຢູ່ທັງໝົດ ເຮັດໃຫ້ຜູ້ ຕອບສະໜອງຕໍ່ເຫດການ ACSC ຂອງ ASD ສາມາດດໍາເນີນການວິເຄາະທີ່ສົມບູນແບບ ແລະ ສ້າງຄວາມເຂົ້ າໃຈກ່ຽວກັບກິດຈະກໍາ APT40 ທີ່ເປັນໄປໄດ້ໃນເຄືອຂ່າຍ.

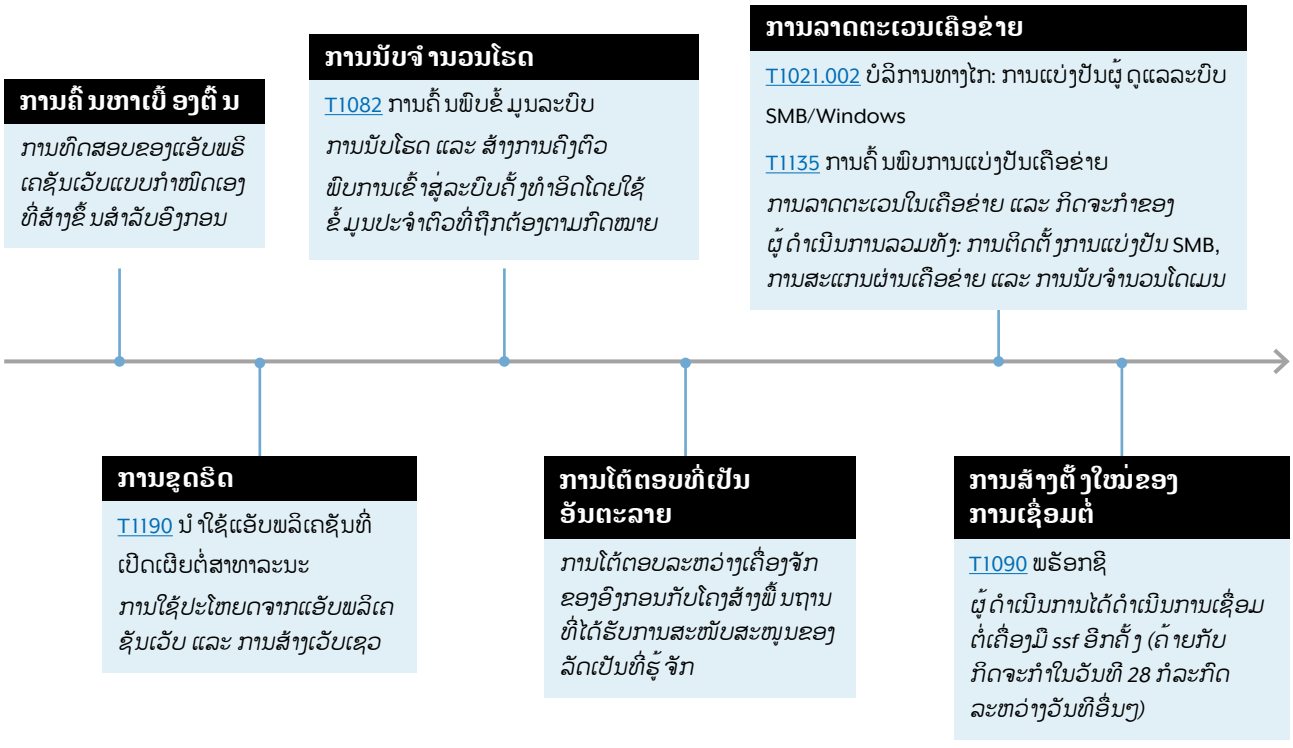
ໃນເດືອນກັນຍາ, ຫຼັງຈາກການປຶກສາຫາລືກັບ ACSC ຂອງ ASD, ອົງກອນໄດ້ຕັດສິນໃຈທີ່ຈະນໍາ IP ທີ່ລະບຸໄວ້ໃນແຈ້ງເຕືອນເບື້ ອງຕົ້ ນໄປໄວ້ໃນລາຍຊື່. ໃນເດືອນຕຸລາ, ອົງກອນໄດ້ເລີ່ມຕົ້ ນການແກ້ໄຂ.

ລາຍລະອຽດ

ເລີ່ມຕົ້ ນໃນເດືອນກໍລະກົດ, ຜູ້ ມີສ່ວນກ່ຽວຂ້ອງສາມາດທົດສອບ ແລະ ນໍ າໃຊ້ປະໂຫຍດຈາກແອັບພລິເຄຊັນເວັບແບບກໍ ານົດເອງ (T1190) ທີ່ເຮັດວຽກໃນ `<webapp>2-ext`, ເຊິ່ງເຮັດໃຫ້ກຸ່ມສາມາດຕັ້ ງຖານທັບຢູ່ໃນເຂດປອດທະຫານເຄືອຂ່າຍໄດ້ (DMZ). ສິ່ງນີ້ ຖືກນໍ າມາໃຊ້ເພື່ອລະບຸທັງເຄືອຂ່າຍ ແລະ ໂດເມນທີ່ເຫັນໄດ້ທັງໝົດ. ຂໍ້ ມູນປະຈໍ າຕົວທີ່ຖືກບຸກລຸກ (T1078.002) ຖືກໃຊ້ເພື່ອສອບຖາມ Active Directory (T1018) ແລະ ດຶງຂໍ້ ມູນອອກໂດຍການຕິດຕັ້ ງການແບ່ງປັນໄຟລ໌(T1039) ຈາກຫຼາຍເຄື່ອງພາຍໃນ DMZ. ຜູ້ ສະແດງໄດ້ດໍາເນີນການໂຈມຕີ Kerberoasting ເພື່ອໃຫ້ໄດ້ຮັບຂໍ້ ມູນປະຈໍາເຄືອຂ່າຍທີ່ຖືກຕ້ອງຈາກເຄື່ອງແມ່ຂ່າຍ (T1558.003). ບໍ່ ພົບວ່າກຸ່ມດັ່ງກ່າວໄດ້ຮັບຄະແນນເພີ່ມເຕີມໃນເຂດ DMZ ຫຼື ເຄືອຂ່າຍພາຍໃນແຕ່ຢ່າງໃດ.

ພາບເສັ້ ນເວລາ

ເສັ້ ນເວລາລຸ່ມນີ້ ໃຫ້ພາບລວມຢ່າງກວ້າງຂວາງຂອງໄລຍະທີ່ສໍາຄັນຂອງກິດຈະກໍາຂອງຜູ້ ບໍ່ປະສົງດີທີ່ສັງເກດເຫັນໃນເຄືອຂ່າຍຂອງອົງກອນ.



ເສັ ນເວລາທີ່ລະອຽດ

ເດືອນກໍລະກົດ: ຜູ້ ສະແດງໄດ້ສ້າງການເຊື່ອມຕໍ່ເບື້ ອງຕົ້ ນກັບ ໜ້ າເວັບຂອງແອັບພລິເຄຊັນເວັບແບບກໍ ານົດເອງ (T1190) ທີ່ ສ້າງຂຶ້ ນສໍ າລັບອົງກອນ (ຕໍ່ໄປນີ້ ເອີ້ ນວ່ າ 'ແອັບພລິເຄຊັນເວັບ' ຫຼື 'webapp') ຜ່ານການເຊື່ອມຕໍ່ການຮັກສາຄວາມປອດໄພ ຊັ້ ນການຂົນສົ່ ງ (TLS) (T1102). ບໍ່ພົບກິດຈະກໍາອື່ນໆ ທີ່ໜ້ າ ສັງເກດ.

ເດືອນກໍລະກົດ: ຜູ້ ສະແດງເລີ່ ມຕົ້ ນການນັບຈໍ ານວນເວັບ ໄຊທ໌ຂອງແອັບພລິເຄຊັນຊອກຫາຈຸດສິ້ ນສຸດ[2] ເພື່ອສືບສວນ ຕື່ ມອີກ.

ເດືອນກໍລະກົດ: ຜູ້ ມີສ່ ວນຮ່ ວມມຸ່ ງເນັ້ ນໄປທີ່ຄວາມ ພະຍາຍາມໃນການໃຊ້ປະໂຫຍດຈາກຈຸດສິ້ ນສຸດສະເພາະ ເຈາະຈົ ງ.

ເດືອນກໍລະກົດ: ຜູ້ ສະແດງສາມາດ ໂພສ ໄປຍັງເວັບເຊັ ລທີ່ ເວ ໄດ້ສໍ າເລັດ, ອາດຈະຜ່ ານທາງເວັບເຊລທີ່ ອາຢູ່ ໃນໜ້ າອື່ ນ. IP ທີ ສອງ, ເຊິ່ ງອາດຈະໃຊ້ ງານໂດຍນັກສະແດງດຽວກັ ນ, ຍັ ງເລີ່ ມຕົ້ ນ ໂພສໄປຫາ URL ດຽວກັ ນ. ນັກສະແດງໄດ້ສ້ າ ແລະ ທົ ດສອບ ເວັບເຊລທີ່ໜ້ າຈະເປັ ນໄປໄດ້ ຈໍ ານວນໜຶ່ ງ.

ບໍ່ຮູ້ ວິ ທີການໂຈມຕີທີ່ ແນ່ ນອນ, ແຕ່ ຊັ ດເຈນວ່ າຈຸດສິ້ ນສຸດ ສະເພາະເຈາະຈົ ງນັ້ ນຖືກກໍ ານົ ດເປົ້ າໝາຍເພື່ ອສ້ າງໄຟລ໌ ໃນ `<webapp>2-ext`.

ACSC ຂອງ ASD ເຊື່ ອວ່ າການເຊື່ ອມຕໍ່ ທີ່ ຢູ່ IP ທັ ງສອງນັ້ ນເປັ ນ ສ່ ວນໜຶ່ ງຂອງການບຸ ກລຸ ກອັ ນດຽວກັ ນເນື່ ອງຈາກຄວາມສົ ນໃຈ ຮ່ ວມກັ ນ ແລະ ການເຊື່ ອມຕໍ່ ເບື ອງຕົ້ ນທີ່ ເກີ ດຂຶ້ ນໃນນາທີ ຫ່ າງ ກັ ນ.

ເດືອນກໍລະກົດ: ກຸ່ ມຍັ ງຄົ ງດໍ າເນີ ນການນັ ບໂຮດ, ຊອກຫາ ໂອກາດການຂະຫຍາຍສິ ດທິ ພິ ເສດ ແລະ ນໍ າໃຊ້ ແຜ່ ນເວັ ບ ທີ່ ແຕກຕ່ າງກັ ນ. ຜູ້ ສະແດງເຂົ້ າສູ່ ແອັ ບພລິ ເຄຊັ ນເວັ ບໂດຍ ໃຊ້ ຂໍ້ ມູ ນປະຈໍ າຕົ ວທີ່ ຖືກ ບຸ ກລຸ ກ ສໍ າ ລັ ບ `<firstname.surname>@<organisation domain>`.

ເບິ່ ງຄື ວ່ າ ການ ເຄື່ ອນ ໄຫ ວ ຂອງ ຜູ້ ສະ ແດງ ຈະ ບໍ່ ປະ ສົ ບ ຄວາມ ສໍ າ ເລັ ດ ໃນ ການ ຍົ ກ ລະ ດັ ບ ສິ ດ ທິ ພິ ເສ ດ ຢູ່ ໃນ `<webapp>2-ext`. ໃນ ທາງ ກັ ບ ກັ ນ, ນັ ກ ສະ ແດງ ໄດ້ ປ ່ ຽນ ສູ່ ກິ ດ ຈະ ກໍ າ ໃນ ເຄືອ ຂ ່ າ ຍ ແທ ນ.

ເດືອນກໍລະກົດ: ຜູ້ ສະແດງໄດ້ ທົ ດສອບຂໍ້ ມູ ນປະຈໍ າຕົ ວທີ່ ຖືກ ບຸ ກລຸ ກ ສໍ າ ລັ ບ ບັ ນ ຊີ ການ ບໍ ລິ ການ[3] ເຊິ່ ງ ມີ ແນ ວ ໂນ້ ມ ທີ່ ຈ ະ ພົ ບ ວ ່ າ ຖືກ ເຂົ້ າ ລ ະ ຫັ ດ ແບ ບ ຮ າ ດ ໂຄ ດ ໃນ ໄຟ ລ ຖ ານ ສ ອ ງ ທີ່ ສ າ ມ າ ດ ເຂົ້ າ ເ ຖ ິ ງ ໄ ດ ້ ພ າ ຍ ໃ ນ .

ເດືອນກໍລະກົດ: ຜູ້ ສະແດງນໍ າໃຊ້ ເຄື່ ອງມື open-source Secure Socket Funnelling, ເຊິ່ ງໃຊ້ ເພື່ ອເຊື່ ອມຕໍ່ ກັ ບໂຄງ ສ້ າງພື້ ນຖານທີ່ ເປັ ນອັ ນຕະລາຍ. ການເຊື່ ອມຕໍ່ ນີ້ ແມ່ ນໃຊ້ ເຂົ້ າໃນການສ້ າງອຸ ໂມງຮັ ບສົ່ ງຂໍ້ ມູ ນຈາກເຄື່ ອງໂຈມຕີ ຂອງ ຜູ້ ກະທໍ າຄວາມຜິ ດໄປຍັ ງເຄືອ ຂ ່ າ ຍ ພາຍ ໃ ນ ຂ ອ ງ ອ ົ ງ ກ ອ ນ, ໂ ດ ຍ ຊ ື່ ເຄື່ ອງຂອງອົ ງກອນຈະຖືກ ເປີ ດ ເຜີ ຍ ຢູ່ ໃ ນ ບັ ນ ທ ຶ ກ ເ ຫ ດ ການ ເ ມ ື ່ ອ ພະຍາຍາມໃຊ້ ຂໍ້ ມູ ນຮັ ບຮ ອ ງ ສ ໍ າ ລ ັ ບ ບ ັ ນ ຊ ີ ບ ໍ ລ ິ ການ.

ເດືອນສິ ງຫ າ: ນັ ກ ສ ະ ແ ດ ງ ໄ ດ ້ ດ ໍ າ ເ ນ ີ ນ ການ ກ ິ ດ ຈ ະ ກ ໍ າ , ລ ວ ມ ທ ັ ງ ການ ລ ື້ ມ ເ ຫ ຼ ອ ໃ ນ ການ ສ ້ າ ງ ການ ເ ຊ ື ່ ອ ມ ຕ ໍ ່ ທ ີ ່ ກ ່ ຽ ວ ຂ ້ ອ ງ ກ ັ ບ ບ ັ ນ ຊ ີ ການ ບ ໍ ລ ິ ການ.

ເດືອນສິ ງຫ າ: ຜູ້ ສະແດງດໍ າເນີ ນການນັ ບເຄືອ ຂ ່ າ ຍ ແລະ Active Directory ທີ່ ສໍ າ ຄັ ນ. ບັ ນ ຊ ີ ທ ີ ່ ຖ ືກ ບ ຸ ກ ລ ຸ ກ ອ ື ່ ນ ຈ ະ ຖ ືກ ນ ໍ າ ໃ ຊ ້ ເ ພ ື ່ ອ ຕ ິ ດ ຕ ັ ້ ງ ການ ແ ບ ່ ງ ປ ັ ນ[4] ຢ ູ ່ ໃ ນ ເ ຄ ື ່ ອ ງ Windows ພ າ ຍ ໃ ນ DMZ, ເ ຊ ິ ່ ງ ເ ຮ ັ ດ ໃ ຫ ້ ສ າ ມ າ ດ ດ ຶ ງ ຂ ໍ ້ ມ ູ ນ ອ ອ ກ ໄ ດ ້ ສ ໍ າ ເ ລ ັ ດ ຜ ົ ນ .

ນີ້ ເບິ່ ງຄື ວ່ າ ຈະ ເປັ ນ ການ ສອ ຍ ໃ ຊ ້ ຂ ໍ ້ ມ ູ ນ ປ ະ ຈ ໍ າ ຕ ົ ວ ທ ີ ່ ຖ ືກ ລ ັ ກ ຢ ູ ່ ໃ ນ ເ ຄ ື ່ ອ ງ ທ ີ ່ ຕ ິ ດ ຕ ັ ້ ງ ຢ ູ ່ ໃ ນ ເ ຂ ດ DMZ. ໄ ຟ ລ ໌ ບ ລ ັ ອ ກ ຜ ູ ້ ກ ະ ທ ໍ າ ຈ າ ກ ການ ກ ໍ າ ໜ ົ ດ ເ ປ ົ ້ າ ໝ າ ຍ ເ ຄ ື ອ ຂ ່ າ ຍ ພ າ ຍ ໃ ນ ທ ີ ່ ມ ີ ກ ິ ດ ຈ ະ ກ ໍ າ ທ ີ ່ ຄ ້ າ ຍ ຄ ື ກ ັ ນ .

ເດືອນສິ ງຫ າ – ເດືອນກັ ນຍ າ: ເຄື່ ອງມື SSF ໄດ້ ຕັ້ ງ ການເຊື່ ອມ ຕໍ່ ກັ ບ IP ທີ່ ເປັ ນອັ ນຕະລາຍອີ ກຄັ້ ງ. ກຸ່ ມດັ ່ ງກ ່ າ ວ ບ ໍ ່ ໄ ດ ້ ຖ ືກ ສັ ງ ເ ກ ດ ເ ຫ ັ ນ ວ ່ າ ດ ໍ າ ເ ນ ີ ນ ການ ກ ິ ດ ຈ ະ ກ ໍ າ ເ ພ ີ ່ ມ ເ ຕ ິ ມ ໃ ດ ໆ ຈ ົ ນ ກ ່ ອ ນ ການ ເ ຂ ົ ້ າ ເ ຖ ິ ງ ຂ ອ ງ ພ ວ ກ ເ ຂ ົ າ ຖ ືກ ບ ລ ັ ອ ກ .

ເດືອນກັ ນຍ າ: ອົ ງ ກ ອ ນ ປ ິ ດ IP ທ ີ ່ ເ ປ ັ ນ ອ ັ ນ ຕ ະ ລ າ ຍ ໂ ດ ຍ ການ ປ ະ ຕ ິ ເ ສ ດ ບ ໍ ່ ໃ ຫ ້ ສ ະ ແ ດ ງ ຢ ູ ່ ໃ ນ ໄ ຟ ລ ໌ .

2 ໃນ ບໍ ລິ ບົ ດ ນີ້ , ຈຸ ດ ສິ້ ນ ສຸ ດ ແມ່ ນ ໜ ້ າ ທີ ່ ຂ ອ ງ ແ ອ ັ ບ ພ ລ ິ ເ ຄ ຊ ັ ນ ເ ວ ັ ບ

3 ບັ ນ ຊ ີ ການ ບ ໍ ລ ິ ການ ບ ໍ ່ ໄ ດ ້ ຜ ູ ກ ມ ັ ດ ກ ັ ບ ຜ ູ ້ ໃ ຊ ້ ສ ່ ວ ນ ບ ຸ ກ ຄ ົ ນ , ແ ຕ ່ ແ ທ ນ ທ ີ ່ ຈ ະ ເ ປ ັ ນ ການ ບ ໍ ລ ິ ການ . ໃ ນ ໂ ດ ເ ມ ນ ຂ ອ ງ ອ ົ ງ ກ ອ ນ Microsoft, ມ ີ ບ ັ ນ ຊ ີ ຫ ຼ າ ຍ ປ ະ ເ ພ ດ .

4 ການ ຕ ິ ດ ຕ ັ ້ ງ ການ ແ ບ ່ ງ ປ ັ ນ ແ ມ ່ ນ ຂ ະ ບ ວ ນ ການ ເ ຮ ັ ດ ໃ ຫ ້ ໄ ຟ ລ ໌ ໃ ນ ໂ ຄ ງ ສ ້ າ ງ ລ ະ ບ ົ ບ ໄ ຟ ລ ໌ ສ າ ມ າ ດ ເ ຂ ົ ້ າ ເ ຖ ິ ງ ຜ ູ ້ ໃ ຊ ້ ຫ ຼ ື ກ ຸ ່ ມ ຜ ູ ້ ໃ ຊ ້ ໄ ດ ້ .

ยุดທະວິທີ ແລະ ເຕັກນິກຂອງນັກສະແດງ

ໂຄງຮ່ຳ MITER ATT&CK ແມ່ນຊຸດເອກະສານການເກັບກຳ ຳ ຍຸດທະວິທີ ແລະ ເຕັກນິກທີ່ນຳ ໃຊ້ໂດຍຜູ້ ກ່ຳໄພຄຸກຄາມໃນໂລກ ໄຊເບີ. ໂຄງຮ່ຳດັ່ງກ່ າວຖືກສ້ ຳງຂຶ້ ນໂດຍບໍລິສັດ MITER ເຊ ່ ຳງ ເປັນອົງກອນບໍ່ ຫວັ ງຜົນກຳ ໄລຂອງສະຫະລັດ ແລະ ເຮັດໜ ້ ຳທີ ່ ເປັນພາສາສາກົນທີ ່ ໃຊ້ສ ື ່ ສານກ ່ ຽວກັບພຶດຕິກຳ ຳ ຂອງຜູ ້ ກ ່ ຳໄພຄຸກ ຄາມ.

ACSC ຂອງ ASD ປະເມີນເຕັກນິກ ແລະ ຍຸດທະວິທີຕ ່ ຳໄປນ ີ ້ ອ ່ ານີ ້ ຄວາມກ ່ ຽວຂ ້ ອງກັບກິດຈະກຳ ຳ ທີ ່ ເປັນອັນຕະລາຍຂອງຜູ ້ ກະທຳ ຳ :

ການລາດຕະເວນ

T1594 – ຄົ ້ ນຫາເວັບໄຊທ ์ ທີ ่ ຜູ ้ ຖືກເຈາະຮ ้ ายເປັນເຈ ้ ຳ ຂອງ

ນັກສະແດງລະບຸ ວັ ບໄຊທ ์ ຂອງແອັ ບພລິເຄຊັ ນເວັ ບແບບກຳ ນົ ດ ເອງ ເພ ື ່ ອລະບຸ ໂອກາດໃນການເຂ ้ ຳ ເຖ ິ ງເຄ ື ອຂ ่ າຍ.

ການເຂ ้ ຳ ເຖ ິ ງເບ ื ้ ອງຕ ้ ົ ນ

T1190 – ໃຊ ้ ປະໂຫຍດຈາກແອັ ບພລິເຄຊັ ນທ ี ่ ເຜ ີ ຍແຜ ่ ສາທາລະນະ (ກ ่ ຽວກັບການໃຊ ้ ປະໂຫຍດຈາກແອັ ບພລິເຄຊັ ນ ເວັ ດທ ี ่ ກຳ ນົ ດເອງ)

T1078.002 – ບັ ນຊ ີ ທ ี ่ ຖືກຕ ้ ອງ: ບັ ນຊ ີ ໂດເມນ (ກ ่ ຽວກັບ ການເຂ ้ ຳ ສ ่ ູ ລະບົ ບດ ้ ວຍຂ ้ ໍ ມູ ນປະຈ ຳ ຕ ົ ວທ ี ่ ປະກອບຂ ึ ้ ນ)

ການໃຊ ้ ປະໂຫຍດຈາກແອັ ບພລິເຄຊັ ນເວັ ບແບບກຳ ນົ ດເອງທ ี ่ ເປ ิ ດເຜ ີ ຍທາງອິ ນເຕ ิ ເນັ ດເຮັ ດໃຫ ้ ຜູ ้ ກະທຳ ຳ ຜ ิ ດສາມາດເຂ ้ ຳ ເຖ ิ ງ ຈ ุ ດເລ ิ ่ ມຕ ้ ົ ນໄດ ้ . ຕ ่ ຳ ມານ ักสะแดงสามาดใช ้ ข ้ ้ มูนปะจ ำ ตอที ่ ถูกละเมิดเพ ื ่ อเข ้ ำ เถ ิ งเคือข ่ ายเพ ิ ่ มเต ิ มได ้ .

ການດ ຳ ເນ ิ ນການ

T1059 – ຕ ็ ອແປຄ ่ ຳ ສ ั ่ ງ ແລະ ການຂຽນສະຄຣ ิ ບ (ກ ่ ຽວກັບ ການດ ຳ ເນ ิ ນການຄ ่ ຳ ສ ั ่ ງຜ ่ ານເວັ ບເຊ ็ ອ)

T1072 – ເຄ ื ่ ອງມ ื ອການປັ ບໃຊ ้ ຊ ็ ອບແອ (ກ ่ ຽວກັບຜ ู ้ ດ ຳ ເນ ิ ນ ການທ ี ่ ໃຊ ้ ເຄ ื ่ ອງມ ื อ open-source tool Secure Socket Funnelling (SSF) ເພ ื ่ ອເຊ ื ่ อມຕ ่ ຳ ກັบ IP)

ຄວາມຄ ิ ງທ ึ ม

T1505.003 – ສ ่ ວນປະກອບຂອງຊ ็ ອບແອເຊ ิ ບເວ ิ : ເວັ ບເຊ ็ ອ (ກ ่ ຽວກັບການໃຊ ้ ເວັ ບເຊ ็ ອ ແລະ SSF ເພ ื ่ ອສ ้ ຳ ງການເຂ ้ ຳ ເຖ ิ ງ)

ການເຂ ้ ຳ ເຖ ิ ງຂ ้ ้ ມູ ນປະຈ ຳ ຕ ົ ວ

T1552.001 – ຂ ้ ้ ມູ ນປະຈ ຳ ຕ ົ ວຈາກຮ ้ ານຄ ้ ຳ ລະຫັ ດຜ ่ ານ (ກ ่ ຽວ ກັບໄຟລ ์ ລະຫັ ດຜ ่ ານທ ี ่ ກ ่ ຽວຂ ้ ອງກັບລະບົ ບການຈັ ดการ ອາຄານ (BMS))

T1558.003 – ລັ ກ ຫ ื ປອມແປງ Kerberos: Kerberoasting (ກ ่ ຽວກັບການໂຈມຕ ิ ເພ ื ่ ອໃຫ ้ ໄດ ้ ຮັ ບຂ ้ ้ ມູ ນປະຈ ຳ ເຄ ื ອຂ ่ າຍ)

ການເຄ ื ่ ອນໄຫວດ ้ ານຂ ้ ำ ງ

T1021.002 – ການບໍ ລິ ການທ ำ ງໄກ: SMB Shares (ກ ่ ຽວກັບ ผู ้ ดำ เนินการติดตั ้ ง SMB shares จากหลายอุ ปะกอบหลาย เคื ่ อง)

ການລວບລວມ

T1213 – ຂ ้ ้ ມູ ນຈາກບ ่ ອນເກັ ບຂ ้ ้ ມູ ນ (ກ ่ ຽວກັບຄ ู ่ ม ื ือเอกะสาน ท ี ่ พ ิ บเห ็ นย ู ่ ในเช ิ บเว ิ BMS)

ການກ ็ ອງອອກ

T1041 – ການລັ ກຂ ้ ้ ມູ ນຜ ่ ານຊ ่ ອງ C2 (ກ ่ ຽວກັບການລັ ກຂ ้ ้ ມູ ນ ของผู ้ กะทำ คามผ ิ ดจาก Active Directory และ การ ติดตั ้ งการแบ ่ งป ั น)

ກໍລະນີສຶກສາ 2

ບົດລາຍງານນີ້ ຖືກເຮັດໃຫ້ບໍ່ລະບຸຊື່ ເພື່ອໃຫ້ສາມາດເຜີຍແຜ່ໄດ້ກວ້າງຂວາງຍິ່ງຂຶ້ ນ. ຕໍ່ໄປນີ້ ອົງກອນທີ່ໄດ້ຮັບຜົນກະທົບຈະເອີ້ ນວ່າ 'ອົງກອນ'. ລາຍລະອຽດສະເພາະບາງສ່ວນໄດ້ຖືກລຶບອອກ ເພື່ອປົກປ້ອງຕົວຕົນຂອງຜູ້ ເຄາະຮ້າຍ ແລະ ວິທີການຕອບໂຕ້ເຫດການຂອງ ACSC ຂອງ ASD.

ສະຫຼຸບສັງລວມ

ບົດລາຍງານນີ້ ໃຫ້ລາຍລະອຽດກ່ຽວກັບຜົນການສືບສວນ ACSC ຂອງ ASD ໃນການປະນີປະນອມເຄືອຂ່າຍຂອງອົງກອນທີ່ປະສົບຜົນສໍາເລັດໃນເດືອນເມສາ 2022. ບົດລາຍງານການສືບສວນນີ້ ໄດ້ຖືກສະໜອງໃຫ້ອົງກອນເພື່ອສະຫຼຸບກິດຈະກໍາທີ່ເປັນອັນຕະລາຍ ແລະ ຄໍາແນະນໍາໃນການແກ້ໄຂ. ຜົນການວິໄຈພົບວ່າ APT40 ເປັນຜູ້ ດໍາເນີນການປະນີປະນອມ.

ໃນເດືອນພຶດສະພາ 2022, ACSC ຂອງ ASD ໄດ້ແຈ້ງໃຫ້ອົງກອນຊາບເຖິງກິດຈະກໍາທີ່ສົງໃສວ່າເປັນອັນຕະລາຍທີ່ສົ່ງຜົນກະທົບຕໍ່ເຄືອຂ່າຍຂອງອົງກອນຕັ້ ງແຕ່ເດືອນເມສາ 2022. ຫຼັງຈາກນັ້ ນ, ອົງກອນໄດ້ແຈ້ງໃຫ້ ACSC ຂອງ ASD ວ່າ ພວກເຂົາໄດ້ຄົ້ ນພົບຊອບແວທີ່ເປັນອັນຕະລາຍຢູ່ໃນເຄື່ອງແມ່ຂ່າຍທີ່ປະເຊີນກັບອິນເຕີເນັດເຊິ່ງສະໜອງການເຂົ້ າສູ່ລະບົບສໍາລັບການແກ້ໄຂການເຂົ້ າເຖິງທາງໄກຂອງອົງກອນ. ເຊີບເວີນີ້ ໄດ້ໃຊ້ການເຂົ້ າສູ່ລະບົບ ແລະ ການລະບຸຕົວຕົນແບບໄລຍະໄກ ແລະ ຈະຖືກເອີ້ ນໃນລາຍງານນີ້ ວ່າ 'ອຸປະກອນທີ່ຖືກບຸກລຸກ'. ບົດລາຍງານນີ້ ໃຫ້ລາຍລະອຽດຜົນການສືບສວນ ແລະ ຄໍາແນະນໍາການແກ້ໄຂທີ່ສ້ າງຂຶ້ ນສໍາລັບອົງກອນເພື່ອຕອບສະໜອງຕໍ່ການສືບສວນທີ່ດໍາເນີນການໂດຍ ACSC ຂອງ ASD.

ຫຼັກຖານຊີ້ ໃຫ້ເຫັນວ່າສ່ວນໜຶ່ງຂອງເຄືອຂ່າຍຂອງອົງກອນໄດ້ຖືກບຸກລຸກໂດຍຜູ້ ບໍ່ຫວັງດີທາງໄຊເບີຜ່ານປະຕູເຂົ້ າລະບົບການເຂົ້ າເຖິງທາງໄກຂອງອົງກອນຕັ້ ງນັບຕັ້ ງແຕ່ເດືອນເມສາ 2022 ເປັນຢ່າງໜ້ ອຍ. ເຊີບເວີນີ້ ອາດຈະຖືກບຸກລຸກໂດຍຜູ້ ບໍ່ຫວັງດີຫຼາຍຄົນ ແລະ ອາດຈະໄດ້ຮັບຜົນກະທົບຈາກຊ່ອງໂຫວ່ຂອງການປະຕິບັດລະຫັດທາງໄກ (RCE) ທີ່ຖືກເຜີຍແຜ່ຢ່າງກວ້າງຂວາງໃນຊ່ວງເວລາຂອງການບຸກລຸກ.

ກິດຈະກໍາທີ່ສໍາຄັນທີ່ສັງເກດເຫັນໂດຍ ACSC ຂອງ ASD ປະກອບມີ:

- ການນັບໂຮດ, ເຊິ່ງເຮັດໃຫ້ຜູ້ ສະແດງສາມາດສ້ າງແຜນທີ່ເຄືອຂ່າຍຂອງຕົນເອງຂອງໄດ້;
- ການໃຊ້ປະໂຫຍດຈາກແອັບພລິເຄຊັ່ນທີ່ປະເຊີນກັບອິນເຕີເນັດ ແລະ ການນໍາໃຊ້ເວັບເຊວ, ຊ່ວຍໃຫ້ຜູ້ ດໍາເນີນການມີພື້ ນຖານເບື້ ອງຕົ້ ນໃນເຄືອຂ່າຍ ແລະ ມີຄວາມສາມາດໃນການປະຕິບັດຄໍາສັ່ ງ;
- ການໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫ່ວຂອງຊອບແວເພື່ອຍົກລະດັບສິດທິ ແລະ
- ການເກັບກໍາຂໍ້ ມູນປະຈໍາຕົວເພື່ອເຮັດໃຫ້ສາມາດເຄື່ອນໄປດ້ານຂ້ າງ

ACSC ຂອງ ASD ຄົ້ ນພົບວ່າຜູ້ ບໍ່ປະສົງດີໄດ້ລັກຊື່ ຜູ້ ໃຊ້ ແລະ ລະຫັດຜ່ານທີ່ບໍ່ຊ້ ໍາກັນຫຼາຍຮ້ ອຍຊຸດຈາກອຸປະກອນທີ່ຖືກບຸກລຸກໃນເດືອນເມສາ 2022, ເຊັ່ນດຽວກັນກັບລະຫັດການພິສູດຢືນຢັນຫຼາຍປັດໃຈ ແລະ ສິ່ງປອມແປງທາງເຕັກນິກຈໍ ານວນໜຶ່ງທີ່ກ່ຽວຂ້ ອງກັບເຊດຊັນການເຂົ້ າເຖິງທາງໄກ. ເມື່ອອົງກອນກວດສອບແລ້ວພົບວ່າລະຫັດຜ່ານເປັນລະຫັດທີ່ຖືກຕ້ ອງ. ACSC ຂອງ ASD ປະເມີນວ່າຜູ້ ກະທໍ ່ າຄວາມຜິດໄດ້ລວບລວມຂໍ້ ມູນທາງເຕັກນິກເຫຼົ ່ ານີ້ ເພື່ອໂຈມຕີ ຫຼື ສ້ າງເຊດຊັນການເຂົ້ າສູ່ລະບົບທາງໄກໃນຖານະຜູ້ ໃຊ້ຖືກຕ້ ອງຕາມກົດໝາຍ ແລະ ເຂົ້ າເຖິງເຄືອຂ່າຍພາຍອົງກອນໂດຍໃຊ້ບັນຊີຜູ້ ໃຊ້ທີ່ຖືກຕ້ ອງຕາມກົດໝາຍ.

ຜົນການສືບສວນ

ສະຫຼຸບຜົນການສືບສວນ

ACSC ຂອງ ASD ໄດ້ກຳນົດວ່າຜູ້ກະທຳຄວາມຜິດໄດ້ບຸກລຸກອຸປະກອນທີ່ໃຫ້ເຊດຊັນການເຂົ້າສູ່ລະບົບທາງໄກສຳລັບເຈົ້າໜ້າທີ່ອົງກອນ ແລະ ນຳໃຊ້ອຸປະກອນບຸກລຸກນີ້ ເພື່ອພະຍາຍາມດຳເນີນກິດຈະກຳຕໍ່ໄປ. ເຄື່ອງໃຊ້ເຫຼົ່ານີ້ ປະກອບດ້ວຍໂຮດທີ່ໂຫຼດສົມດຸນສາມຕົວເຊິ່ງກວດພົບຫຼັກຖານການບຸກລຸກໃນໄລຍະທຳອິດ. ອົງກອນໄດ້ປິດໂຮດທີ່ສົມດຸນສອງໃນສາມເຄື່ອບໍ່ດົນຫຼັງຈາກການປະນີປະນອມເບື້ອງຕົ້ນ. ດັ່ງນັ້ນ, ກິດຈະກຳຕໍ່ໄປທັງໝົດເກີດຂຶ້ນຢູ່ໃນໂຮດດຽວ. ເຊີບເວີອື່ນທີ່ເຊື່ອມໂຍງກັບອຸປະກອນທີ່ຖືກບຸກລຸກກໍ່ໄດ້ຮັບການໂຫຼດສົມດຸນໃນລັກສະນະທີ່ຄ້າຍຄືກັນ. ເພື່ອຄວາມຊັດເຈນ, ເຄື່ອງໃຊ້ໄຟຟ້າທີ່ໄດ້ຮັບຜົນກະທົບທັງໝົດຈະຖືກອ້າງເຖິງໃນລາຍງານນີ້ ວ່າເປັນ 'ເຄື່ອງໃຊ້ໄຟຟ້າພຽງຄັ້ງດຽວ'.

ເຊື່ອກັນວ່ານັກສະແດງດັ່ງກ່າວໄດ້ໃຊ້ຊ່ອງໂຫວ່ທີ່ເປີດເຜີຍຕໍ່ສາທາລະນະເພື່ອປັບໃຊ້ເວັດເຊວກັບອຸປະກອນທີ່ບຸກລຸກຕັ້ງແຕ່ເດືອນເມສາ 2022 ເປັນຕົ້ນໄປ. ຜູ້ກໍ່ໄພຄຸກຄາມຈາກກຸ່ມໄດ້ຮັບການປະເມີນວ່າໄດ້ຮັບສິດທິພິເສດທີ່ເພີ່ມຂຶ້ນໃນອຸປະກອນ. ACSC ຂອງ ASD ບໍ່ສາມາດກຳນົດຂອບເຂດທັງໝົດຂອງກິດຈະກຳໄດ້ເນື່ອງຈາກຂາດຄວາມສາມາດໃນການບັນທຶກຂໍ້ມູນ. ຢ່າງໃດກໍຕາມ, ຫຼັກຖານໃນອຸປະກອນຊີ້ໃຫ້ເຫັນວ່າຜູ້ສະແດງປະສົບຄວາມສຳເລັດດັ່ງຕໍ່ໄປນີ້:

- ການເກັບກຳຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານທີ່ແທ້ຈິງຫຼາຍຮ້ອຍຄູ່ ແລະ
- ການເກັບກຳຂໍ້ມູນປອມທາງເທັກນິກທີ່ອາດເຮັດໃຫ້ຜູ້ບໍ່ຫວັງດີສາມາດເຂົ້າເຖິງເຊດຊັນໂຄງສ້າງພື້ນຖານເດັສທັອບສະເໝືອນ (VDI) ໃນຖານະຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຕາມກົດໝາຍໄດ້.

ACSC ຂອງ ASD ປະເມີນວ່າຜູ້ກະທຳຄວາມຜິດຈະພະຍາຍາມປະນີປະນອມຂອງເຄືອຂ່າຍອົງກອນໃຫ້ຫຼາຍຂຶ້ນ. ສິ່ງປະດິດທີ່ຖືກລັກໄປໂດຍຜູ້ກະທຳອາດຈະອະນຸຍາດໃຫ້ພວກເຂົາ ສາມາດເຂົ້າຄວບຄຸມ ຫຼື ເລີ່ມຕົ້ນເຊດຊັນເດັສທັອບສະເໝືອນໃນຖານະຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຕາມກົດໝາຍ, ໂດຍອາດຈະເປັນຜູ້ໃຊ້ທາງເລືອກຂອງເຂົາເຈົ້າ, ລວມທັງຜູ້ດູແລລະບົບ. ນັກສະແດງອາດຈະໄດ້ນຳໃຊ້ເວັກເຕີການເຂົ້າເຖິງນີ້ ເພື່ອປະນີປະນອມການບໍລິການອົງກອນເພື່ອໃຫ້ບັນລຸຄວາມຄົງຢູ່ ແລະ ເປົ້າໝາຍອື່ນໆ.

ອຸປະກອນອົງກອນອື່ນໆ ພາຍໃນສະພາບແວດລ້ອມທີ່ຄຸ້ມຄອງໂດຍຜູ້ໃຫ້ບໍລິການໂຮດຕິ້ງບໍ່ໄດ້ສະແດງຫຼັກຖານຂອງການປະນີປະນອມ.

ການເຂົ້າເຖິງ

ໂຮດທີ່ມີອຸປະກອນທີ່ຖືກບຸກລຸກໄດ້ໃຫ້ການກວດສອບສິດພິສູດຢືນຢັນຜ່ານ Active Directory ແລະ ເວັດເຊີເວີ, ສຳລັບຜູ້ໃຊ້ທີ່ເຊື່ອມຕໍ່ກັບເຊດຊັນ VDI (T1021.001).

ສະຖານທີ່	ຊື່ໂຮສຂອງອຸປະກອນທີ່ຖືກບຸກລຸກ (ໂຫຼດໄດ້ສົມດຸນ)
ສູນຂໍ້ມູນ 1	ໂຮດ1, ໂຮດ2, ໂຮດ3

ໂຄງສ້າງພື້ນຖານຂອງອຸປະກອນຍັງລວມເຖິງໂຮດເກດການເຂົ້າເຖິງທີ່ໃຫ້ຊ່ອງທາງໄປຍັງ VDI ສຳລັບຜູ້ໃຊ້, ເມື່ອພວກເຂົາມີໂທເຄັນການກວດສອບຄວາມຖືກຕ້ອງທີ່ສ້າງຂຶ້ນ ແລະ ດາວໂຫຼດຈາກອຸປະກອນ.

ບໍ່ມີຫຼັກຖານຂອງການປະນີປະນອມໃດໆຂອງໂຮດເຫຼົ່ານີ້. ຢ່າງໃດກໍຕາມ, ບັນທຶກການເຂົ້າເປັນເຈົ້າພາບໄດ້ສະແດງໃຫ້ເຫັນຫຼັກຖານຂອງການໂຕ້ຕອບທີ່ສຳຄັນກັບທີ່ຢູ່ IP ທີ່ເປັນອັນຕະລາຍທີ່ຮູ້ຈັກ. ມີແນວໂນ້ມວ່າກິດຈະກຳນີ້ສະທ້ອນເຖິງສິ່ງທີ່ເກີດຂຶ້ນໃນໂຮດນີ້ ຫຼື ການເຊື່ອມຕໍ່ເຄືອຂ່າຍທີ່ມີໂຄງສ້າງພື້ນຖານຂອງຜູ້ຄຸກຄາມທີ່ເຂົ້າເຖິງໂຮດ. ບໍ່ສາມາດລະບຸລັກສະນະຂອງກິດຈະກຳນີ້ໄດ້ໂດຍໃຊ້ຫຼັກຖານທີ່ມີຢູ່ແຕ່ຊີ້ໃຫ້ເຫັນວ່າກຸ່ມນີ້ໄດ້ພະຍາຍາມທີ່ຈະເຄື່ອນໄຫວໃນແນວຂວາງໃນເຄືອຂ່າຍຂອງອົງກອນ (TA0008).

ໂຮດພາຍໃນ

ACSC ຂອງ ASD ກວດສອບຂໍ້ມູນຈຳກັດຈາກກຸ່ມເຄືອຂ່າຍພາຍໃນອົງກອນ. ຄວາມພະຍາຍາມ ຫຼື ການເຄື່ອນໄຫວທີ່ເປັນອັນຕະລາຍທີ່ປະສົບຜົນສຳເລັດທີ່ຮູ້ວ່າໄດ້ສົ່ງຜົນກະທົບຕໍ່ພາກສ່ວນເຄືອຂ່າຍຂອງອົງກອນພາຍໃນ ຮວມເຖິງການເຂົ້າເຖິງຂອງຜູ້ກະທຳຕໍ່ກັບສິ່ງປະດິດທີ່ກ່ຽວຂ້ອງກັບ VDI, ການຂູດຂໍ້ມູນຈາກເຊີບເວີ SQL ພາຍໃນ (T1505.001) ແລະ ການຈັດສິ່ງທີ່ບໍ່ສາມາດອະທິບາຍໄດ້ສັງເກດເຫັນວ່າມາຈາກທີ່ຢູ່ IP ທີ່ເປັນອັນຕະລາຍທີ່ຮູ້ຈັກຜ່ານອຸປະກອນເກດເວການເຂົ້າເຖິງ. (TA0011).

ກຸ່ມດັ່ງກ່າວໄດ້ສິດເຂົ້າເຖິງອຸປະກອນທີ່ຖືກບຸກລຸກ, ເພື່ອລວບລວມຊື່ຜູ້ໃຊ້, ລະຫັດຜ່ານ (T1003) ແລະ ຄ່າໂທເຄັນ MFA (T1111). ກຸ່ມດັ່ງກ່າວຍັງໄດ້ເກັບກຳຂໍ້ມູນ JSON Web Tokens (JWTs) (T1528), ເຊິ່ງເປັນສິ່ງປະດິດຂອງການກວດສອບຄວາມຖືກຕ້ອງທີ່ໃຊ້ໃນການສ້າງເຊດຊັນການເຂົ້າສູ່ລະບົບເດັສທັອບສະເໝືອນ. ຜູ້ສະແດງອາດຈະສາມາດໃຊ້ສິ່ງເຫຼົ່ານີ້ ເພື່ອສ້າງ ຫຼື ແຍກຊິງເຊດຊັນເດັສທັອບສະເໝືອນ (T1563.002) ແລະ ເຂົ້າເຖິງສ່ວນເຄືອຂ່າຍຂອງອົງກອນພາຍໃນເປັນຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຕາມກົດໝາຍ (T1078).

ນັກສະແດງຍັງໄດ້ໃຊ້ການເຂົ້າເຖິງອຸປະກອນທີ່ຖືກບຸກລຸກ ເພື່ອຂຸດຂໍ້ ມູນເຊີເວີ SQL (T1505.001), ເຊິ່ງຢູ່ໃນເຄືອຂ່າຍ ພາຍໃນຂອງອົງກອນ. ເປັນໄປໄດ້ວ່ານັກສະແດງມີສິດການເຂົ້າ ເຖິງຂໍ້ ມູນນີ້.

ຫຼັກຖານທີ່ມີຢູ່ໃນອຸປະກອນເກດເວການເຂົ້າເຖິງເປີດເຜີຍ ວ່າການຮັບສົ່ງຂໍ້ ມູນໃນເຄືອຂ່າຍເກີດຂຶ້ ນຜ່ານ ຫຼື ໄປຫາ ອຸປະກອນນີ້ ຈາກທີ່ຢູ່ IP ທີ່ຮູ້ ວ່າເປັນອັນຕະລາຍ. ດັ່ງທີ່ ອະທິບາຍໄວ້ຂ້າງເທິງ, ນີ້ ອາດຈະຊີ້ ບອກວ່າຜູ້ ກ່ຽວຂ້ອງທາງ ໄຊເບີສົ່ງຜົນກະທົບ ຫຼື ນ ໍ ໃຊ້ອຸປະກອນນີ້ , ເຊິ່ງອາດນ ໍ າໄປສູ ການປ່ຽນຜ່ານໄປຍັງເຄືອຂ່າຍພາຍໃນໄດ້.

ກ ໍ ານົດເວລາຂອງການສືບສວນ

ລາຍການຂ້າງລຸ່ມນີ້ ສະແດງໄລຍະເວລາຂອງກິດຈະກ ໍ າທີ່ສ ໍ າຄັນ ທີ່ຄົ ນພົບໃນລະຫວ່າງການສືບສວນ.

ເວລາ	ເຫດການ
ເດືອນເມສາ 2022	ທີ່ຢູ່ IP ທີ່ເປັນອັນຕະລາຍທີ່ຮູ້ ຈັກຈະຕອບໂຕ້ກັບໂຮດເກດເວການເຂົ້າເຖິງ HOST7. ບ ໍ່ສາມາດລະບຸລັກສະນະຂອງການໂຕ້ຕອບໄດ້.
ເດືອນເມສາ 2022	ໂຮດທັງໝົດ, HOST1, HOST2 ແລະ HOST3, ຖືກບຸກລຸກໂດຍຜູ້ ກ ະ ທ ໍ າ ທີ່ ອັ ນ ຕ ະ ລ າ ຍ ແ ລ ະ ເ ວັ ບ ເ ຊ ອ ຖ ື ກ ວ າ ງ ໄ ວ ້ ໃ ນ ໂ ຮ ດ . ໄຟລ ์ ບ ันທ ึ ก ถ ู ก ส ้ า ง ห ร ื อ แ ก ้ ไ ข ใ น HOST2. ไ ฟ ล ์ น ี ้ ม ี ข ้ อ ม ู ล ก า ร ร ั บ ร อ ง ท ี ่ อ า จ จ ะ ถ ู ก จ ั บ โ ด ย ผ ู ้ บ ่ ป ร ะ ส ง ค ์ ด ี . ไฟล์ /etc/security/opasswd ແລະ /etc/shadow ໄດ້ຮັບການແກ້ໄຂໃນ HOST1 ແລະ HOST3, ເຊິ່ງລະບຸວ່າລະຫັດຜ່ານ ໄດ້ຮັບການປ່ຽນແປງ. ຫຼັກຖານທີ່ມີຢູ່ໃນ HOST1 ຊີ້ ໃຫ້ເຫັນວ່າລະຫັດຜ່ານສ ໍ າ ລ ັ ບ ຜ ู ้ ใ ช ้ 'sshuser' ม ี ก า ร ป ่ ย น แ ป ง .
ເດືອນເມສາ 2022	HOST2 ถ ู ก ป ิ ด โ ด ย อ ง ค ์ ก อ น . เ ว ็ บ เ ช ล เ พ ิ ่ ม เ ต ิ ม (T1505.003) ถ ู ก ส ้ า ง ข ึ ้ น ใ น HOST1 แ ล ะ HOST3. HOST1 ป ะ ส บ ป ั ญ ห า ค ว า ม พ ย า ย า ม โ จ ม ต ี แ บ บ SSH brute force จาก HOST3. ไ ฟ ล ์ บ ันท ึ ก ถ ู ก ป ั บ ป ่ ย น (T1070) ใ น HOST3. ไ ฟ ล ์ น ี ้ ป ะ ก อ บ ด ้ อ ย ข ้ อ ม ู ล ป ะ จ ำ ต ิ อ (T1078) อ า จ จ ะ ถ ู ก จ ั บ โ ด ย ผ ู ้ บ ่ ป ร ะ ส ง ค ์ ด ี . JWTs ไ ด ้ ถ ู ก จ ั บ (T1528) แ ล ะ ส ่ ง อ อ ก ไ ป ย ั ง ไ ฟ ล ์ ใ น HOST3. HOST3 ถ ู ก ป ิ ด โ ด ย อ ง ค ์ ก อ น . ก ิ ด จ ะ ก ำ ท ั ง ห ม ด ห ล ั ง จ า ก เ อ ล า น ี ้ เ ก ิ ด ข ึ ้ น ใ น HOST1.
ເດືອນເມສາ 2022	ມ ີ ການ ສ ้ า ง เ ว ็ บ เ ช ล เ พ ิ ่ ม เ ต ิ ม ใ น HOST1 (T1505.003). JWTs ถ ู ก จ ั บ แ ล ะ ส ่ ง อ อ ก ไ ป ห า ไ ฟ ล ์ ใ น HOST1.
ເດືອນເມສາ 2022	ມ ีการสร ้ างเว ็ บเช ล เพ ิ ่ มเต ิ มใน HOST1 (T1505.003), แ ล ะ ท ี ่ อ ย ่ IP ท ี ่ เ ป ็ น อ ั น ต ะ ล า ย ท ี ่ ร ู ้ จ ั ก โ ต ้ ต อ บ ก ั บ โ ห ด (TA0011). ท ี ่ อ ย ่ IP ท ี ่ เ ป ็ น อ ั น ต ะ ล า ย ท ี ่ ร ู ้ จ ั ก โ ต ้ ต อ บ ก ั บ โ ฮ ด เ ก ด เ อ ก า ร เ ข ้ า เ ถ ิ ง HOST7.
ເດືອນພຶດສະພາ 2022	ท ี ่ อ ย ่ IP ท ี ่ เ ป ็ น อ ั น ต ะ ล า ย ท ี ่ ร ู ้ จ ั ก โ ต ้ ต อ บ ก ั บ โ ฮ ด เ ก ด เ อ ก า ร เ ข ้ า เ ถ ิ ง HOST7 (TA0011). เ ห ด ก า ร ก า ร ก อ ด ส อ บ ถ า ม ถ ู ก ต ้ อ ง ส ำ ล ั บ ผ ู ้ ใ ช ้ แ ม ่ น เ ช ื ่ อ ม ต ่ ำ ก ั บ ท ี ่ อ ย ่ IP ท ี ่ เ ป ็ น อ ั น ต ะ ล า ย ท ี ่ ร ู ้ จ ั ก ใ น บ ั น ท ึ ก ใ น HOST1. ม ี ก า ร ส ้ า ง เ ว ็ บ เ ช ล เ พ ิ ่ ม เ ต ิ ม ใ น โ ฮ ด น ี ้ (T1505.003).
ເດືອນພຶດສະພາ 2022	ส ะ ค ร ี บ ใ น HOST1 ไ ด ้ ร ั บ ก า ร แ ก ้ ไ ข โ ด ย ผ ู ้ ส ะ แ ด ง (T1543). ส ะ ค ร ี บ น ี ้ ป ะ ก อ บ ด ้ อ ย ก า ร เ ร ั ด อ ว ง ก ท ี ่ ส า ม า ร ถ ล อ บ ล อ ม ข ้ อ ม ู ล จ า ก เ ซ ิ เ ว ี SQL พ า ย ใ น .
ເດືອນພຶດສະພາ 2022	ไ ฟ ล ์ บ ันท ึ ก เ พ ิ ่ ม เ ต ิ ม ใ น HOST1 ไ ด ้ ร ั บ ก า ร แ ก ้ ห ล ้ า ส ุ ด (T1070). ไ ฟ ล ์ น ี ้ ป ะ ก อ บ ด ้ อ ย ช ื ่ อ ผ ู ้ ใ ช ้ แ ล ะ ล ะ ห ั ด ผ ่ า น ถ ู ก ส ำ ล ั บ เ ค ื อ ข ่ า ย อ ง ค ์ ก อ น , เ ช ื ่ อ เ ช ื ่ อ ว ่ า ถ ู ก ต ้ อ ง ต า ม ก ิ ด ห ม า ย (T1078).
ເດືອນພຶດສະພາ 2022	ไ ฟ ล ์ บ ันท ึ ก เ พ ิ ่ ม เ ต ิ ม ไ ด ้ ร ั บ ก า ร แ ก ้ ห ล ้ า ส ุ ด (T1070). ไ ฟ ล ์ น ี ้ ป ะ ก อ บ ด ้ อ ย JWTs ท ี ่ เ ก ็ บ ม า จ า ก HOST1.
ເດືອນພຶດສະພາ 2022	ม ี ก า ร ส ้ า ง เ ว ็ บ เ ช ล เ พ ิ ่ ม เ ต ิ ม ใ น HOST1 (T1505.003). ใ น อ ั น น ี ้ , อ ง ค ์ ก อ น ไ ด ้ ล า ย ง า น ก า ร ค ้ น พ บ ข อ ง เ ว ็ บ เ ช ล ท ี ่ ม ี อ ั น ท ิ ส ร ้ า ง ใ น เ ด ื อ น เ ม ส า 2022 ก ั บ ACSC ข อ ง ASD.
ເດືອນພຶດສະພາ 2022	ม ี ก า ร ส ้ า ง ส ะ ค ร ี บ จ ำ น ว น ห น ึ ่ ง ใ น HOST1, ล ว ม ท ั ง ส ะ ค ร ี บ ช ื ่ อ ว ่ า Log4jHotPatch.jar.
ເດືອນພຶດສະພາ 2022	ค ำ ส ั ่ ง iptables-save ใ ช ้ เ พ ื ่ อ เ พ ิ ่ ม พ อ ด ท ี ่ เ ป ิ ด อ ย ู ่ ส อ ง พ อ ด ใ ห ้ ก ั บ โ ฮ ด เ ก เ อ ย ก า ร เ ข ้ า เ ถ ิ ง . พ อ ด แ ม ่ น 9998 แ ล ะ 9999 (T1572).

ຍຸດທະວິທີ ແລະ ເຕັກນິກຂອງນັກສະແດງ

ຈຸດເດັ່ນຂ້າງລຸ່ມນີ້ ແມ່ນຍຸດທະວິທີ ແລະ ເຕັກນິກຫຼາຍ ປະການທີ່ລະບຸໃນລະຫວ່າງການສືບສວນ.

ການເຂົ້າເຖິງເບື້ອງຕົ້ນ

T1190 ນຳໃຊ້ປະໂຫຍດຈາກແອັບພລິເຄຊັນທີ່ເຜີຍແຜ່ສູ່ສາທາລະນະ

ກຸ່ມດັ່ງກ່າວອາດຈະໃຊ້ປະໂຫຍດຈາກ RCE, ການຍົກລະດັບສິດທິພິເສດ ແລະ ການພິສູດຢືນຢັນຜ່ານຊ່ອງໂຫວ່ໃນການເຂົ້າສູ່ລະບົບການເຂົ້າເຖິງທາງໄກ ແລະ ການຈັດການຂໍ້ມູນປະຈຳຕົວເພື່ອເຂົ້າເຖິງເຄືອຂ່າຍໃນເບື້ອງຕົ້ນ.

ວິທີການເຂົ້າເຖິງເບື້ອງຕົ້ນນີ້ ແມ່ນຖືວ່າເປັນໄປໄດ້ຫຼາຍທີ່ສຸດ ເນື່ອງຈາກສາເຫດຕໍ່ໄປນີ້:

- ເຊີບເວີມີຄວາມສ່ຽງຕໍ່ CVEs ເຫຼົ່ານີ້ ໃນເວລານັ້ນ;
- ຄວາມພະຍາຍາມທີ່ຈະໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫ່ວ ເຫຼົ່ານີ້ ຈາກໂຄງສ້າງພື້ນຖານຂອງຜູ້ກະທຳທີ່ຮູ້ ຈັກ ແລະ
- ກິດຈະກຳທີ່ເປັນອັນຕະລາຍພາຍໃນທີ່ຮູ້ ຈັກຄັ້ງທຳອິດ ເກີດຂຶ້ນບໍ່ດົນຫຼັງຈາກມີຄວາມພະຍາຍາມສະແຫວງຫາ ຜົນປະໂຫຍດ.

ການດຳເນີນການ

T1059.004 ຕົວແປຄຳສັ່ງ ແລະ ສະຄຣິບ: Unix Shell

ກຸ່ມດັ່ງກ່າວສາມາດໃຊ້ປະໂຫຍດຈາກຈາກຊ່ອງໂຫ່ວໄດ້ສຳເລັດ ແລະ ອາດສາມາດຮັບຄຳສັ່ງໃນເຊວ Unix ທີ່ມີຢູ່ໃນອຸປະກອນ ທີ່ໄດ້ຮັບຜົນກະທົບ. ບໍ່ສາມາດໃຫ້ລາຍລະອຽດຄົບຖ້ວນ ສົມບູນຂອງຄຳສັ່ງທີ່ດຳເນີນການໂດຍ ຕົວດຳເນີນການໄດ້ເນື່ອງ ຈາກຄຳສັ່ງເຫຼົ່ານັ້ນບໍ່ໄດ້ຖືກບັນທຶກໂດຍອຸປະກອນ.

ຄວາມຄົງທົນ

T1505.003 ອົງປະກອບຊອບແວເຊີບເວີ: ເວັບເຊວ

ນັກສະແດງໄດ້ນຳໃຊ້ເວັບເຊວຫຼາຍຕົວໄປໃຊ້ກັບອຸປະກອນທີ່ ໄດ້ຮັບຜົນກະທົບ. ມັນເປັນໄປໄດ້ວ່າຜູ້ ສະແດງທີ່ແຕກຕ່າງກັນ ຫຼາຍໄດ້ນຳໃຊ້ເວັບເຊວ, ແຕ່ມີພຽງຜູ້ ສະແດງຈຳນວນນ້ອຍກວ່າ ເທົ່ານັ້ນ ທີ່ດຳເນີນກິດຈະກຳໂດຍໃຊ້ເວັບເຊວເຫຼົ່ານີ້. ເວັບ ເຊວຈະອະນຸຍາດໃຫ້ຜູ້ ດຳເນີນການປະຕິບັດຄຳສັ່ງຕາມໃຈໃນ ອຸປະກອນທີ່ຖືກບຸກລຸກ.

ການເພີ່ມສິດທິພິເສດ

T1068 ການສະແຫວງຜົນປະໂຫຍດເພື່ອການຍົກລະດັບສິດທິ ພິເສດ

ຫຼັກຖານທີ່ມີຢູ່ບໍ່ໄດ້ອະທິບາຍເຖິງລະດັບສິດທິພິເສດທີ່ຜູ້ ສະແດງໄດ້ຮັບ. ຢ່າງໃດກໍຕາມ, ຖ້າໃຊ້ເວັບເຊວ, ຜູ້ ສະແດງຈະ ໄດ້ຮັບສິດທິພິເສດໃນລະດັບທຽບກັບເວັບເຊີເວີໃນອຸປະກອນ ທີ່ຖືກບຸກລຸກ. ເຊື່ອວ່າຊ່ອງໂຫວ່ມີຢູ່ໃນອຸປະກອນທີ່ຖືກ ບຸກລຸກເຊິ່ງຈະເຮັດໃຫ້ຜູ້ ກະທຳສາມາດເຂົ້າເຖິງສິດທິພິເສດໄດ້.

ການເຂົ້າເຖິງຂໍ້ ມູນປະຈຳຕົວ

T1056.003 ການຈັບຂໍ້ ມູນອິນພຸດ: ການຈັບພາບສູນເວັບ

ຫຼັກຖານກ່ຽວກັບອຸປະກອນທີ່ຖືກບຸກລຸກໄດ້ສະແດງໃຫ້ເຫັນ ວ່າຜູ້ ກະທຳຄວາມຜິດໄດ້ບັນທຶກຊື່ຜູ ໃຊ້ ແລະ ລະຫັດຜ່ານໄວ້ ຫຼາຍຮ້ອຍຄູ່ໃນຮູບແບບຂໍ້ ຄວາມທຳມະດາ, ເຊິ່ງເຊື່ອວ່າເປັນ ຂໍ້ ມູນທີ່ຖືກຕ້ອງຕາມກົດໝາຍ. ມີແນວໂນ້ມວ່າຂໍ້ ມູນເຫຼົ່ານີ້ ຖືກຈັບພາບໂດຍໃຊ້ການປັບປ່ຽນບາງຢ່າງກັບຂະບວນການ ກວດສອບຄວາມຖືກຕ້ອງຂອງແທ້ເຊິ່ງສົ່ງຂໍ້ ມູນການຢືນຢັນ ໃຫ້ກັບໄຟລ໌.

T1111 ການສະກັດກັ້ນການກວດສອບສິດແບບຫຼາຍປັດໃຈ

ນັກສະແດງຍັງໄດ້ຈັບຄ່າຂອງໂທເຄັນ MFA ທີ່ສອດຄ່ອງກັບ ການເຂົ້າສູ່ລະບົບທີ່ຖືກຕ້ອງຕາມກົດໝາຍ. ຂໍ້ ມູນເຫຼົ່ານີ້ ອາດຖືກບັນທຶກໂດຍການແກ້ໄຂຂະບວນການກວດສອບ ສິດທິ່ແທ້ຈິງເພື່ອສົ່ງຄ່າເຫຼົ່ານີ້ ໄປສູ່ໄຟລ໌. ບໍ່ມີຫຼັກຖານ ຂອງການບຸກລຸກ'ເຊີບເວີລັບ' ທີ່ຈັດເກັບຄ່າສະເພາະທີ່ໃຫ້ ຄວາມປອດໄພຂອງໂທເຄັນ MFA.

T1040 ການດັກຟັງເຄືອຂ່າຍ

ເຊື່ອກັນວ່ານັກສະແດງໄດ້ຈັບ JWTs ໂດຍການຈັບພາບການຮັບ ສົ່ງຂໍ້ ມູນ HTTP ໃນອຸປະກອນທີ່ຖືກບຸກລຸກ. ມີຫຼັກຖານ ວ່າ tcpdump utility ໄດ້ຖືກດຳເນີນການໃນອຸປະກອນທີ່ ຖືກບຸກລຸກ, ເຊິ່ງອາດຈະເປັນວິທີທີ່ນັກສະແດງໄດ້ຈັບ JWTs ເຫຼົ່ານີ້.

T1539 ລັກຄຸກກີເຊດຊັນເວັບ

ດັ່ງທີ່ໄດ້ອະທິບາຍໄວ້ຂ້າງເທິງ, ນັກສະແດງໄດ້ຈັບ JWTs, ເຊິ່ງ ຄ້າຍຄືກັນກັບຄຸກກີເຊດຊັນ. ສິ່ງເຫຼົ່ານີ້ ອາດນຳມາໃຊ້ຄືນໃໝ່ ໂດຍນັກສະແດງເພື່ອສ້າງການເຂົ້າເຖິງເພີ່ມເຕີມ.

ການຄົ້ ນຫາ

T1046 ການຄົ້ ນຫາການບໍລິການເຄືອຂ່າຍ

ມີຫຼັກຖານວ່າອຸປະກອນການສະແກນເຄືອຂ່າຍ nmap ຖືກ ດຳເນີນການຢູ່ໃນອຸປະກອນທີ່ຖືກບຸກລຸກເພື່ອສະແກນອຸປະ ກອນອື່ນໆໃນສ່ວນເຄືອຂ່າຍດຽວກັນ. ສິ່ງນີ້ ມີແນວໂນ້ມວ່າ ນັກສະແດງເພື່ອຄົ້ ນຫາການບໍລິການເຄືອຂ່າຍອື່ນໆ ທີ່ສາມາດ ເຂົ້ າເຖິງໄດ້ເຊິ່ງອາດຈະນຳສະເໜີໂອກາດສຳລັບການເຄື່ອນທີ່ ຂ້າງຄຽງ.

ການລອບລອມ

ຫຼັກຖານທີ່ມີຢູ່ບໍ່ໄດ້ເປີດເຜີຍວ່ານັກສະແດງເກັບກຳຂໍ້ ມູນແນວ ໃດ ຫຼື ສິ່ງທີ່ຖືກລວບລວມຈາກອຸປະກອນທີ່ຖືກບຸກລຸກ ຫຼື ຈາກ ລະບົບອື່ນໆ. ແນວໃດກໍ່ຕາມ, ມີແນວໂນ້ມວ່ານັກສະແດງມີການ ເຂົ້ າເຖິງໄຟລ໌ທັງໝົດໃນອຸປະກອນທີ່ຖືກບຸກລຸກ, ລວມທັງຂໍ້ ມູນ ປະຈຳຕົວທີ່ຖືກຈັບໄດ້ (T1003), ຄ່າໂທເຄັນ MFA (T1111), ແລະ JWT ທີ່ອະທິບາຍຂ້າງເທິງ.

ຄຳສັ່ງ ແລະ ການຄວບຄຸມ

T1071.001 ໂປໂຕຄອນຊັ້ ນຂໍ້ ມູນແອັບພລິເຄຊັນ: ໂປໂຕຄອນ ເວັບ

ນັກສະແດງໄດ້ໃຊ້ເວັບເຊວເພື່ອການສັ່ງການ ແລະ ຄວບຄຸມ. ຄຳສັ່ງຂອງເວັບເຊວຈະຖືກສົ່ງຜ່ານ HTTPS ໂດຍໃຊ້ເວັບເຊີບເວີ ທີ່ມີຢູ່ໃນອຸປະກອນ(T1572).

T1001.003 ການປົກປິດຂໍ້ ມູນ: ການປອມຕົວເປັນໂປໂຕຄອນ

ນັກສະແດງໄດ້ໃຊ້ອຸປະກອນທີ່ຖືກບຸກລຸກເປັນຈຸດເລີ່ມຕົ້ ນຂອງ ການໂຈມຕີທີ່ຖືກອອກແບບມາເພື່ອປະສົມປະສານກັບການສັ່ງ ຂໍ້ ມູນທີ່ຖືກຕ້ອງ.

ຄຳແນະນຳກ່ຽວກັບການຄົ້ນຫາ ແລະ ບັນເທົາຜົນກະທົບ

ACSC ຂອງ ASD ຂໍແນະນຳໃຫ້ໃຊ້ການຄວບຄຸມ ASD ທີ່ສຳຄັນທັງແປດ ແລະ ທີ່ກ່ຽວຂ້ອງ ກັບຍຸດທະສາດ ເພື່ອຫຼຸດຜ່ອນເຫດການຄວາມປອດໄພທາງໄຊເບີ. ຂ້າງລຸ່ມນີ້ ແມ່ນຄຳແນະນຳສຳລັບການປະຕິບັດຄວາມປອດໄພຂອງເຄືອຂ່າຍທີ່ຄວນຈະຖືກປະຕິບັດເພື່ອກວດພົບ ແລະ ປ້ອງກັນການບຸກລຸກໂດຍ APT40, ຕິດຕາມດ້ວຍການບັນເທົາຜົນກະທົບສະເພາະສຳລັບ TTP ທີ່ສຳຄັນສີ່ປະການທີ່ໄດ້ສະຫຼຸບໄວ້ໃນຕາຕະລາງທີ 1.

ການກວດຈັບ

ໄຟລ໌ບາງໄຟລ໌ທີ່ລະບຸຂ້າງເທິງນັ້ນຖືກຖິ້ມໄວ້ໃນຕຳແໜ່ງ ເຊັ່ນ C:\Users\Public* ແລະ C:\Windows\Temp*. ສະຖານທີ່ເຫຼົ່ານີ້ ອາດເປັນຈຸດທີ່ສະດວກສຳລັບການຂຽນ ຂໍ້ ມູນເນື່ອງຈາກໂດຍປົກກະຕິແລ້ວສາມາດຂຽນໄດ້ທົ່ວໂລກ, ເຊິ່ງໝາຍຄວາມວ່າບັນຊີຜູ້ ໃຊ້ທັງໝົດທີ່ລົງທະບຽນຢູ່ໃນ Windows ຈະສາມາດເຂົ້ າເຖິງບັນຊີລາຍຊື່ເຫຼົ່ານີ້ ແລະ ບັນຊີ ລາຍຊື່ຍ່ອຍຂອງບັນຊີຜູ້ ໃຊ້ເຫຼົ່ານັ້ ນໄດ້. ຫຼາຍຄັ້ ງ, ທີ່ຜູ້ ໃຊ້ ໃດສາມາດເຂົ້ າເຖິງໄຟລ໌ເຫຼົ່ານີ້ ໄດ້ໃນພາຍຫຼັ ງ, ເຮັດໃຫ້ເກີດ ໂອກາດໃນການເຄື່ອນໄຫວຂ້ າງຄຽງ, ການຫຼີກລ້ ຽງການປ້ ອງກັ ນ, ການດຳເນີ ນການສິດທິພິ ເສດ ແລະ ຂັ້ ນຕອນກຽມສຳ ລັ ບການ ແອບແຝງ.

ກົດລະບຽບຊິ ກມາຕໍ່ ໄປນີ້ ຈະຊອກຫາການດຳ ເນີ ນການ ຈາກສະຖານທີ່ ທີ່ ໜ້ າສົ ງໄສເປັ ນຕົ ວຊີ້ ວັ ດຂອງກິ ດຈະກຳ ຜິ ດປົ ກກະຕິ. ໃນທຸ ກໆກໍ ລະນີ, ຈຳ ເປັ ນຕ້ ອງມີ ການສືບ ສວນ ເພີ ່ ມເຕີ ມເພື ່ ອຢືນຢັ ນກິ ດຈະກຳ ທີ ່ ເປັ ນອັ ນຕະລາຍ ແລະ ການ ບຸ ກລຸ ກແຫຼ ່ ງທີ ່ ມາ.

ຊື່ ເລື ່ ອງ: ດຳ ເນີ ນການຂຽນໄດ້ ທົ ່ ວໂລກ-ຊ ່ ອຄາວ

ລະຫັ ດ: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

ຄຳ ອະທິ ບາຍ: ກວດຈັ ບການດຳ ເນີ ນການຂະບວນການຈາກ C:\Windows\Temp.

ຄວາມເປັ ນມາ:

ກົ ດລະບຽບນີ ້ ເບິ ່ ງຫາການດຳ ເນີ ນການອອກຈາກ C:\Windows\Temp*ໂດຍສະເພາະ. ອຸ ນຫະພູ ມຖືກ ໃຊ້ ຢ ່ າງ ກວ ້ າງຂວາງໂດຍແອັ ບພລິ ເຄ ຊັ ນທີ ່ ບ ່ ເປັ ນອັ ນຕະລາຍ ດັ ່ ງນັ ້ ນ ຈຶ ່ ງມີ ຄວາມເຊື ່ ອໝັ ້ ນໃນຕົ ວຊີ ້ ວັ ດທີ ່ ເປັ ນອັ ນຕະລາຍຕ ່ ຳກວ ່ າ ການດຳ ເນີ ນການຈາກໄດເລກະທໍ ລີ ຍ ່ ອຍທີ ່ ສາມາດຂຽນໄດ ້ ຈາກ ທີ ່ ອື ່ ນໃນ C:\Windows.

ການລົ ບແອັ ບພລິ ເຄ ຊັ ນທີ ່ ປະຕິ ບັ ດໂດຍຜູ ້ ໃຊ ້ SYSTEM ຫຼ ື NETWORK SERVICE ຈະຊ ່ ວຍຫຼຸ ດປະລິ ມານກິ ດຈະກຳ ທີ ່ ບ ່ ເປັ ນອັ ນຕະລາຍທີ ່ ເລືອກໂດຍກົ ດລະບຽບນີ ້ ໄດ ້ ຢ ່ າງຫຼວ ງ ຫຼ າຍ. ເຊິ ່ ງໝາຍຄວາມວ ່ າກົ ດລະບຽບອາດຈະພາດການປະຕິ ບັ ດທີ ່ ເປັ ນອັ ນຕະລາຍໃນລະດັ ບສິ ດທິ ພິ ເສດທີ ່ ສູ ງກວ ່ າ ແຕ ່ ແນະນຳ ໃຫ ້ ໃຊ ້ ກົ ດລະບຽບອື ່ ນ ເພື ່ ອກຳ ນົ ດວ ່ າຜູ ້ ໃຊ ້ ກຳ ລັ ງພະຍາຍາມ ຍົ ກລະດັ ບສິ ດທິ ພິ ເສດໃຫ ້ ເປັ ນ SYSTEM ຫຼ ື ບ ่ .

ການສືບສວນ:

1. ກວດສອບຂໍ ້ ມູ ນທີ ່ ກ ່ ຽວຂ ້ ອງໂດຍກົ ງກັ ບການປະຕິ ບັ ດ ໄຟລ ์ ນີ ้ , ເຊ ่ ັ ນ: ບໍ ລິ ບົ ດຂອງຜູ ้ ໃຊ ้ , ລະດັ ບຄວາມສົ ມບູ ນ ຂອງການປະຕິ ບັ ດ, ກິ ດຈະກຳ ການຕິ ດຕາມທັ ນທີ ແລະ ຮູ ບພາບທີ ่ ໂຫຼ ດໂດຍໄຟລ ์ .
2. ການສືບສວນຂະບວນການຕາມບໍ ລິ ບົ ດ, ເຄືອຂ ่ າຍ, ໄຟລ ์ ແລະ ຂ ้ ມູ ນສະໜັ ບສະໜູ ນອື ่ ນໆ ໃນໂຮດເພື ่ ອຊ ่ ວຍ ເຮັ ດການປະເມີ ນວ ่ າກິ ດຈະກຳ ດັ ່ ງກ ่ າວເປັ ນອັ ນຕະລາຍ ຫຼ ื ບ ่ .
3. ຖ ้ າຈຳ ເປັ ນ ໃຫ ้ ພະຍາຍາມເກັ ບກຳ ສຳ ເນົ າຂອງໄຟລ ์ ເພື ่ ອ ຍ ้ ອນກັ ບວິ ສະວະກຳ ເພື ่ ອກວດສອບວ ่ າຖືກ ຕ ้ ອງຫຼ ื ບ ่ .

ເອກະສານອ ้ າງອິ ง

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ผู้ ขยง: ACSC ของ ASD

อันที่ : 2024/06/19

สะถานะ: การทดลอง

แท็ก:

- tlp.green
- classification.au.official
- attack.execution

แหล่งที่มาของบันทึก:

ผลิตภัณฑ์: ระบบการสร้าง
ผลิตภัณฑ์: windows

การกวดหา:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
ผู้ใช้ละบบ:
    ผู้ใช้:
    - 'ละบบ'
    - 'บริการเครือข่าย'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

ເງື່ອນໄຂ: temp and not (common_temp_path or system_user or dismhost or known_parent)

ຜົນບວກທີ່ບໍ່ຖືກຕ້ອງ:

- ພົບວ່າແອັບພລິເຄຊັ່ນກວດສອບລາຍການອະນຸຍາດກຳລັງແລ່ນດຳເນີນການໄຟລຈາກ Temp.
- Temp ຈະປະກອບດ້ວຍແອັບພລິເຄຊັ່ນ ແລະ ຕ້ອເປີດໃຊ້ງານຢ່າງຖືກຕ້ອງ, ສະນັ້ນ ຄວນພິຈາລະນາວ່າພຶດຕິກຳນີ້ ແຜ່ຫຼາຍຢູ່ໃນເຄືອຂ່າຍທີ່ຕິດຕາມກວດສອບ (ແລະ ສາມາດອະນຸຍາດໄດ້ ຫຼື ບໍ່) ກ່ອນທີ່ຈະນຳໃຊ້ກົດລະບຽບນີ້.

ລະດັບ: ຕ່ຳ

ຊື່ເລື່ອງ: ການດຳເນີນການທີ່ຂຽນໄດ້ທົ່ວໂລກ - ໄດເລກະທໍລີຍ່ອຍລະບົບທີ່ບໍ່ແມ່ນ-Temp

ຂັດປະຈຳຕົວ: 5b187157-e892-4fc9-84fc-aa48aff9f997

ຄຳອະທິບາຍ: ກວດສອບການດຳເນີນການຂະບວນການຈາກຕຳແໜ່ງທີ່ສາມາດຂຽນໄດ້ໃນບັນຊີລາຍຊື່ຍ່ອຍຂອງຕຳແໜ່ງການຕິດຕັ້ງລະບົບປະຕິບັດການ Windows.

ຄວາມເປັນມາ:

ກົດລະບຽບນີ້ຈະເບິ່ງຫາການດຳເນີນການຈາກບັນຊີລາຍຊື່ທີ່ສາມາດຂຽນໄດ້ທົ່ວໂລກໃນ C:\ ແລະ ໂດຍສະເພາະ C:\Windows*, ຍົກເວັ້ນ C:\Windows\Temp (ເຊິ່ງໃຊ້ແອັບພລິເຄຊັ່ນທີ່ບໍ່ເປັນອັນຕະລາຍຢ່າງກວ້າງຂວາງ ແລະ ດ້ວຍເຫດນີ້ຈຶ່ງເປັນຕົວຊີ້ວັດອັນຕະລາຍທີ່ມີຄວາມເຊື່ອໝັ້ນຕ່ຳກວ່າ).

ໂຟນເດີ AppData ຈະຖືກຍົກເວັ້ນຖ້າມີການແຍກໃຊ້ໄຟລ໌ເປັນລະບົບ - ນີ້ແມ່ນວິທີການທີ່ບໍ່ອັນຕະລາຍເຊິ່ງໃຊ້ໃນການຮຽກໃຊ້ໄຟລ໌ແອັບພລິເຄຊັ່ນຊ້ຳຄາວຈຳນວນຫຼາຍ.

ຫຼັງຈາກສຳເລັດການຕັ້ງຄ່າເຄືອຂ່າຍເບື້ອງຕົ້ນ ແລະ ລະບຸການດຳເນີນການທີ່ບໍ່ເປັນອັນຕະລາຍທີ່ຮູ້ຈັກຈາກຕຳແໜ່ງເຫຼົ່ານີ້ແລ້ວ, ກົດລະບຽບນີ້ຈະເລີ່ມເຮັດວຽກໜ້ອຍລົງ.

ການສືບສວນ:

1. ກວດສອບຂໍ້ ມູນທີ່ກ່ຽວຂ້ອງໂດຍກົງກັບການປະຕິບັດໄຟລ໌ນີ້, ເຊັ່ນ: ບໍລິບົດຂອງຜູ້ ໃຊ້, ລະດັບຄວາມສົມບູນຂອງການປະຕິບັດ, ກົດຈະກຳການຕິດຕາມທັນທີ ແລະ ຮູບພາບທີ່ໂຫຼດໂດຍໄຟລ໌.
2. ການສືບສວນຂະບວນການຕາມບໍລິບົດ, ເຄືອຂ່າຍ, ໄຟລ໌ ແລະ ຂໍ້ ມູນສະໜັບສະໜູນອື່ນໆ ໃນໂຮດເພື່ອຊ່ວຍເຮັດການປະເມີນວ່າກິດຈະກຳດັ່ງກ່າວເປັນອັນຕະລາຍຫຼືບໍ່.
3. ຖ້າຈຳເປັນໃຫ້ພະຍາຍາມເກັບກຳສຳເນົາຂອງໄຟລ໌ ເພື່ອຍ້ອນກັບວິສະວະກຳເພື່ອກວດສອບວ່າຖືກຕ້ອງຫຼືບໍ່.

ເອກະສານອ້າງອີງ

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ຜູ້ຂຽນ: ACSC ຂອງ ASD

ວັນທີ: 2024/06/19

ສະຖານະ: ການທົດລອງ

ແທັກ:

- tlp.green
- classification.au.official
- attack.execution

ແຫຼ່ງທີ່ມາຂອງບັນທຶກ:

ໝວດໝູ່: ຂະບວນການສ້າງ
ຜະລິດຕະພັນ: windows

ການກວດຫາ:

writable_path:

ຮູບພາບ|ປະກອບດ້ວຍ:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

ຮູບພາບ|ປະກອບດ້ວຍ: '\\AppData\\'
ຜູ້ໃຊ້: 'ລະບົບ'

ເງື່ອນໄຂ: writable_path ແລະ ບໍ່ແມ່ນ appdata

ຜົນບວກທີ່ບໍ່ຖືກຕ້ອງ:

ພົບວ່າແອັບພລິເຄຊັ່ນກວດສອບລາຍການອະນຸຍາດກຳລັງແລ່ນໄຟລຈາກບັນຊີລາຍຊື່ເຫຼົ່ານີ້.

ມັນເປັນໄປໄດ້ວ່າສະຄຣິບ ແລະ ເຄື່ອງມືການດູແລລະບົບທີ່ໃຊ້ໃນສະພາບແວດລ້ອມທີ່ມີການກວດສອບອາດຈະຢູ່ໃນບັນຊີລາຍລື່ເຫຼົ່ານີ້ ແລະ ຄວນໄດ້ຮັບການແກ້ໄຂເປັນກໍລະນີຕໍ່ໄປ.

ລະດັບ: ສູງ

ຊື່ເລື່ອງ: ການດຳເນີນການຂຽນໄດ້ທົ່ວໂລກ - ຜູ້ ໃຊ້

ບັດປະຈຳຕົວ: 6dda3843-182a-4214-9263-925a80b4c634

ຄຳອະທິບາຍ: ກວດຈັບການດຳເນີນການຂະບວນການຈາກ C:\Users\Public* ແລະໂຟເດີອື່ນໆທີ່ສາມາດຂຽນໄດ້ພາຍໃນຜູ້ໃຊ້.

ຄວາມເປັນມາ:

ໂຟນເດີ AppData ຈະຖືກຍົກເວັ້ນຖ້າມີການແຍກໃຊ້ໄຟລ໌ເປັນລະບົບ - ນີ້ແມ່ນວິທີການທີ່ບໍ່ອັນຕະລາຍເຊິ່ງໃຊ້ໃນການຮຽກໃຊ້ໄຟລ໌ແອັບພລິເຄຊັ່ນຊ້ຳຄາວຈຳນວນຫຼາຍ.

ການສືບສວນ:

1. ກວດສອບຂໍ້ ມູນທີ່ກ່ຽວຂ້ອງໂດຍກົງກັບການປະຕິບັດໄຟລ໌ນີ້ , ເຊັ່ນ: ບໍລິບົດຂອງຜູ້ ໃຊ້, ລະດັບຄວາມສົມບູນຂອງການປະຕິບັດ, ກິດຈະກຳການຕິດຕາມທັນທີ ແລະ ຮູບພາບທີ່ໂຫຼດໂດຍໄຟລ໌.
2. ການສືບສວນຂະບວນການຕາມບໍລິບົດ, ເຄືອຂ່າຍ, ໄຟລ໌ ແລະ ຂໍ້ ມູນສະໜັບສະໜູນອື່ນໆ ໃນໂຮດເພື່ອຊ່ວຍເຮັດການປະເມີນວ່າກິດຈະກຳດັ່ງກ່າວເປັນອັນຕະລາຍຫຼືບໍ່.
3. ຖ້າຈຳເປັນໃຫ້ພະຍາຍາມເກັບກຳສຳເນົາຂອງໄຟລ໌ ເພື່ອຍ້ອນກັບວິສະວະກຳເພື່ອກວດສອບວ່າຖືກຕ້ອງຫຼືບໍ່.

ເອກະສານອ້າງອີງ

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ຜູ້ຂຽນ: ACSC ຂອງ ASD

ວັນທີ: 2024/06/19

ສະຖານະ: ການທົດລອງ

ແທັກ:

- tlp.green
- classification.au.official
- attack.execution

ແຫຼ່ງທີ່ມາຂອງບັນທຶກ:

ໝວດໝູ່: ຂະບວນການສ້າງ
ຜະລິດຕະພັນ: windows

ການກວດຫາ:

ຜູ້ໃຊ້:

ຮູບພາບ|ປະກອບດ້ວຍ:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

ຮູບພາບ|ປະກອບດ້ວຍ: '\\AppData\\'
ຜູ້ໃຊ້: 'ລະບົບ'

ເງື່ອນໄຂ: ຜູ້ໃຊ້ ແລະ ບໍ່ແມ່ນ appdata

ຜົນບວກທີ່ບໍ່ຖືກຕ້ອງ:

- ມັນເປັນໄປໄດ້ວ່າສະຄຣິບ ແລະ ເຄື່ອງມືການດູແລລະບົບທີ່ໃຊ້ໃນສະພາບແວດລ້ອມທີ່ໄດ້ຮັບການກວດສອບອາດຈະຢູ່ໃນສາທາລະນະ ຫຼື ບັນຊີລາຍຊື່ຍ່ອຍ ແລະ ຄວນໄດ້ຮັບການຈັດການເປັນກໍລະນີຕໍ່ໄປ.

ລະດັບ: ປານກາງ

ການບັນເທົາ

ການບັນທຶກຂໍ້ ມູນ

ໃນລະຫວ່າງການສືບສວນຂອງ ACSC ຂອງ ASD, ບັນຫາທົ່ວໄປທີ່ຫຼຸດຜ່ອນປະສິດທິພາບ ແລະ ຄວາມໄວໃນການສືບສວນແມ່ນການຂາດຂໍ້ ມູນການບັນທຶກທີ່ຄົບຖ້ວນ ແລະ ມີປະຫວັດໃນຫຼາຍໆດ້ານ ລວມທັງບັນທຶກການຮ້ອງຂໍຂອງເຊີບເວີເວັບ, ບັນທຶກເຫດການຂອງ Windows ແລະ ບັນທຶກຕົວແທນອິນເຕີເນັດ.

ACSC ຂອງ ASD ແນະນຳໃຫ້ກວດສອບ ແລະ ປະຕິບັດຄຳແນະນຳກ່ຽວກັບ ການບັນທຶກ ແລະ ການສົ່ງຕໍ່ເຫດການຂອງ Windows ໄປໃຊ້ ລວມທັງໄຟລ໌ການກຳນົດ ແລະ ສະຄຣິບໃນ ທີ່ເກັບການບັນທຶກເຫດການຂອງ Windows ແລະ ແນວທາງສຳລັບການກວດສອບລະບົບຂອງຄູ່ມືຄວາມປອດໄພຂໍ້ ມູນ ເຊິ່ງລວມເຖິງຂໍ້ ມູນການລວມບັນທຶກ ແລະ ການເກັບຮັກສາບັນທຶກໄວ້ເປັນໄລຍະເວລາທີ່ເໝາະສົມ.

ການຈັດການແຜ່ນຕິດ

ຮັບແກ້ໄຂອຸປະກອນ ແລະ ການບໍລິການທີ່ເປີດເຜີຍອິນເຕີເນັດທັງໝົດໂດຍທັນທີ, ລວມທັງເວັບເຊີບເວີ, ແອັບພລິເຄຊັ່ນເວັບ ແລະ ເກດເວການເຂົ້າເຖິງທາງໄກ. ພິຈາລະນາການປະຕິບັດລະບົບການຈັດການແຜ່ນຕິດແບບລວມສູນມາໃຊ້ ເພື່ອເຮັດໃຫ້ຂະບວນການເປັນອັດຕະໂນມັດ ແລະ ໄວຂຶ້ ນ. ACSC ຂອງ ASD ແນະນ ໍ າໃຫ້ຈັດຕັ້ ງປະຕິບັດ ຂໍ້ ແນະນ ໍ າ ສ ໍ າລັບການຈັດການລະບົບ ຂອງ ISM ມາໃຊ້, ໂດຍສະເພາະ, ການຄວບຄຸມລະບົບການແກ້ໄຂລະບົບເມື ອໃຊ້ໄດ້.

ການໂຈມຕີສ່ວນໃຫຍ່ທີ່ຜູ ້ ກະທ ໍ າໃຊ້ເປັນທີ່ຮູ ້ ຈັກຕ ໍ່ ສາທາລະນະ ແລະ ມີການແກ້ໄຂ ຫຼື ການບັນເທົ າຜົນກະທົບໃຫ ້ ໃຊ ້ ໄດ ້ . ອົ ງກອນຕ ່ າ ງ ໆ ຄວນກວດສອບໃຫ ້ ແນ ່ ໃຈວ ່ າ ໄດ ້ ຕິ ດຕັ ້ ງ ແຜ ່ ນຄວາມປອດໄພ ຫຼື ການບັນເທົ າຜົນກະທົບກັ ບໂຄງສ ້ າ ງ ພື ້ ນຖານໂຄງລ ່ າ ງທີ ່ ເຊື ່ ອຕ ໍ ່ ກັ ບອິ ນເຕີ ເນັ ດພາຍໃນ 48 ຊົ ່ ວໂມ ງ , ແລະ ຖ ້ າ ເປັ ນໄປໄດ ້ , ຄວນໃຊ ້ ຊອບແວ ແລະ ລະບົ ບປະຕິ ບັ ດ ການເວີ ຊັ ນຫຼ ້ າ ສຸ ດ.

ການແບ ່ ງສ ່ ວນເຄືອຂ ່ າຍ

ການແບ ່ ງສ ່ ວນເຄືອຂ ່ າຍສາມາດເຮັ ດໃຫ ້ ຝ ່ າຍກົ ງກັ ນຂ ້ າ ມ ຄົ ້ ນຫ າ ແລະ ເຂ ້ າ ເຖິ ງຂ ້ ມູ ນສ ໍ າ ຄັ ນຂອງອົ ງກອນໄດ ້ ຍາ ກ ຍິ ່ ງຂຶ ້ ນ. ແບ ່ ງສ ່ ວນເຄືອຂ ່ າຍເພື ່ ອຈ ໍ າ ກັ ດ ຫຼື ບລັ ອ ກ ການເຄື ່ ອນໄຫວດ ້ ານຂ ້ າ ງໂດຍການປະຕິ ເສດການຮັ ບສົ ່ ງຂ ້ ມູ ນ ລະຫ ່ າ ງຄອມພິ ວ ເຕີ ເວັ ້ ນເສຍແຕ ່ ຈ ໍ າ ເປັ ນ. ເຊີ ບເວີ ທີ ່ ສ ໍ າ ຄັ ນ ເຊັ ່ ນ Active Directory ແລະ ເຊີ ບເວີ ການກວດສອບຄວາ ມ ຖືກຕ ້ ອງອື ່ ນ ໆ ຄວນຈະສາມາດບໍ ລິ ການໄດ ້ ຈ າ ກເຊີ ບເວີ ຕ ໍ ່ ກາ ງ ຈ ໍ ານວນຈ ໍ ากัด ຫຼື 'ເຊີ ບເວີ ໂດດ' ເທົ ່ ານັ ້ ນ. ຄວນກວດສອບເຊີ ບເວີ ກເຫຼ ່ ານີ ້ ຢ ່ າ ງໃກ ້ ສິ ດ, ປອດໄພດີ ແລະ ຈ ໍ າ ກັ ດວ ່ າ ຜູ ້ ໃຊ ້ ແລະ ອຸ ປະກອນໃດທີ ່ ສາມາດເຊື ່ ອມຕ ໍ ່ ກັ ບເຊີ ບເວີ ໄດ ້ .

ໂດຍບໍ ່ ຄ ໍ ານຶ ງເຖິ ງກໍ ລະນີ ທີ ່ ຖືກກ ໍ ານົ ດໄວ ້ ເຊິ ່ ງສາມາດປ ້ ອ ງ ກັ ນ ການເຄື ່ ອນໄຫວດ ້ ານຂ ້ າ ງ, ການແບ ່ ງສ ່ ວນເຄືອຂ ່ າຍເພີ ່ ມ ເຕີ ມ ສາມາດຈ ໍ າ ກັ ດຈ ໍ ານວນຂ ້ ມູ ນທີ ່ ຜູ ້ ສະແດງສາມາດເຂ ້ າ ເຖິ ງ ແລະ ດຶ ງ ອ ອ ກ ມ າ ໄດ ້ ຫຼ າ ຍ ຂຶ ້ ນ.

ການບັນເທົ າ ເພີ ່ ມ ເຕີ ມ

ອົ ງກອນຜູ ້ ຂຽນຍັ ງ ແນ ະ ນ ໍ າ ການບັ ນ ເທົ າ ຜົ ນ ກ ະ ທ ົ ບ ຕ ່ ໍ ໄ ປ ນ ີ ້ ເ ພ ື ່ ອ ສ ູ ້ ກ ັ ບ ການໃຊ ້ APT40 ແລະ TTP ຂອງຄົ ນ ອື ່ ນ ຂ ້ າ ງ ລຸ ່ ມ ນ ີ ້ .

- ປິ ດໃຊ ້ ງ ານການບໍ ລິ ການເຄືອຂ ່ າ ຍ, ພອດ ແລະ ໂປຣໂ ຕ ຄ ອ ນ ທ ີ ່ ບ ໍ ່ ໄ ດ ້ ໃ ຊ ້ ຫຼ ື ບ ໍ ່ ຈ ໍ າ ເ ປ ັ ນ.
- ໃຊ ້ ໄ ຟ ວ ໍ ແ ອ ັ ບ ພ ລ ິ ເ ຄ ຊ ັ ນ ເ ວ ັ ບ (WAF) ທ ີ ່ ປ ັ ບ ແ ຕ ່ ງ ຢ ່ າ ງ ດ ີ ເ ພ ື ່ ອ ປ ົ ກ ປ ້ ອ ງ ເ ຊ ີ ບ ເ ວ ີ ແ ລ ະ ແ ອ ັ ບ ພ ລ ິ ເ ຄ ຊ ັ ນ ເ ວ ັ ບ.
- ບັ ງ ຄ ັ ບ ໃ ຊ ້ ສ ິ ດ ທ ິ ພ ິ ເ ສ ດ ຂ ັ ້ ນ ຕ ່ ໍ ເ ພ ື ່ ອ ຈ ໍ າ ກ ັ ດ ກ ານ ເ ຂ ້ າ ເ ຖ ິ ງ ເ ຊ ີ ບ ເ ວ ີ , ກ ານ ແ ບ ່ ງ ປ ັ ນ ໄ ຟ ລ ์ ແ ລ ะ ແ ຫ ຼ ່ ງ ຂ ้ ມ ู ນ ອ ื ่ ນ ๆ .
- ใ ช ้ ก า ร พ ิ ส ู จ น ์ ย ื น ย ั น ห ล า ย ป ั จ จ ั ย (MFA) แ ล ะ บ ั น ช ี บ ร ิ ห า ร ท ี ่ ม ี ก า ร จ ั ด ก า ร เ พ ื ่ อ เ ร ั ด ใ ห ้ ข ้ ม ู น ป ะ จ ำ ต ่ อ ย า ก ต ่ ำ ก า ร ถ อ น ล ะ ห ั ด แ ล ะ น ำ ก ั บ ม า ใ ช ้ ใ ห ่ . ค ว น ใ ช ้ MFA ก ั บ บ ร ิ ห า ร เ ข ้ า เ ถ ิ ง ไ ล ย ะ ไ ก ท ี ่ ส า ม า ด เ ข ้ า เ ถ ิ ง อ ิ น เ ต ิ เ น ั ด ท ั ง ห ม ด , ล ว ม ท ั ง :
  - ▫ อ ี เ ม อ ใ น เ ว ั บ แ ล ะ ค ล า ว
  - ▫ แ พ ร ถ พ อ ม ก า ร ช ่ อ ม ม ื
  - ▫ ก า ร เ ช ื ่ อ ม ต ่ เ ค ื อ ข ่ า ย ส ่ อ ม ต ื อ ส ะ เ ม ื อ น
  - ▫ บ ร ิ ห า ร เ ด ั ส ท ั อ บ ไ ล ย ะ ไ ก
- ป ่ ร ุ น อ ุ ป ะ ก อ น ท ี ่ ห ม ด อ า ย ุ ก า น ใ ช ้ ง า น

ຕາຕະລາງ 1: ຍຸດທະສາດ/ເຕັກນິກໃນການບັນເທົາຜົນກະທົບ

TTP	ຍຸດທະສາດການບັນເທົາຜົນກະທົບທີ່ສຳຄັນແຕ່ປະການ	ການຄວບຄຸມ ISM
ການເຂົ້າເຖິງເບື້ອງຕົ້ນ T1190 ການໃຊ້ປະໂຫຍດຈາກແອັບພລິເຄຊັນທີ່ເຜີຍແຜ່ສູ່ສາທາລະນະ	ແອັບພລິເຄຊັ່ນແຜ່ນແພ ລະບົບປະຕິບັດການ Patch ການພິສູດຢືນຢັນຫຼາຍປັດໃຈ ການຄວບຄຸມແອັບພລິເຄຊັນ	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
ການດຳເນີນການ T1059 ຕ໊ອແປ່ຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ	ການຄວບຄຸມແອັບພລິເຄຊັນ ຈຳກັດມາໂຄຣ Microsoft Office ຈຳກັດສິດທິການດູແລລະບົບ	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
ຄວາມຄົງທົນ T1505.003 ອົງປະກອບຊອບແວເຊີບເວີ: ເວັບເຊວ	ການຄວບຄຸມແອັບພລິເຄຊັນ ຈຳກັດສິດທິການດູແລລະບົບ	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
ການເຂົ້າເຖິງເບື້ອງຕົ້ນ / ການຍົກລະດັບສິດທິພິເສດ / ການຄົງຢູ່ T1078 ບັນຊີທີ່ຖືກຕ້ອງ	ລະບົບປະຕິບັດການ Patch ການພິສູດຢືນຢັນຫຼາຍປັດໃຈ ຈຳກັດສິດທິການດູແລລະບົບ ການຄວບຄຸມແອັບພລິເຄຊັນ ການປັບປຸງການໃຊ້ງານຂອງຜູ້ໃຊ້	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

ສຳລັບຄຳແນະນຳທົ່ວເພີ່ມເຕີມກ່ຽວກັບການກວດຈັບ ແລະ ການບັນເທົາ, ກະລຸນາເບິ່ງພາກ ການບັນເທົາ ແລະ ການກວດຈັບ ໃນໜ້າເວັບເຕັກນິກ MITER ATT&CK ສຳລັບແຕ່ລະເຕັກນິກທີ່ໄດ້ລະບຸໄວ້ໃນບົດສະຫຼຸບຂອງ MITER ATT&CK ໃນຕອນທ້າຍຂອງຄຳແນະນຳນີ້.

ການປະຕິເສດຄວາມຮັບຜິດຊອບ

ຂໍ້ມູນໃນບົດລາຍງານນີ້ ແມ່ນໄດ້ຖືກຈັດທຳຂຶ້ນ ຕາມສະພາບ ເພື່ອຈຸດປະສົງໃນການໃຫ້ຂໍ້ມູນຂ່າວສານເທົ່ານັ້ນ. ໜ່ວຍງານຜູ້ຈັດທຳບໍ່ໄດ້ຮັບຮອງນິຕິບຸກຄົນທາງການຄ້າ, ຜະລິດຕະພັນ, ບໍລິສັດ ຫຼື ການບໍລິການ, ລວມທັງຫ້ອໜ່ວຍ, ຜະລິດຕະພັນ ຫຼື ການບໍລິການໃດໆ ທີ່ເຊື່ອມໂຍງຢູ່ໃນເອກະສານນີ້. ການອ້າງອີງເຖິງຫ້ອໜ່ວຍການຄ້າສະເພາະ, ຜະລິດຕະພັນ, ຂະບວນການ ຫຼື ການບໍລິການໂດຍເຄື່ອງໝາຍການບໍລິການ, ເຄື່ອງໝາຍການຄ້າ, ຜູ້ ຜະລິດ ຫຼື ອື່ນໆ, ບໍ່ໄດ້ປະກອບ ຫຼື ໝາຍເຖິງການຮັບຮອງ, ຄຳແນະນຳ ຫຼື ການສະໜັບສະໜຸນຈາກໜ່ວຍງານຜູ້ ຂຽນ.

ເອກະສານນີ້ ຖືກລະບຸວ່າ TLP:CLEAR. ການເປີດເຜີຍຂໍ້ມູນບໍ່ຈຳກັດ. ແຫຼ່ງຕ່າງໆອາດຈະໃຊ້ TLP:CLEAR ເມື່ອຂໍ້ມູນມີຄວາມສ່ຽງໜ້ອຍທີ່ສຸດ ຫຼື ບໍ່ມີຄວາມເປັນໄປໄດ້ໃນການນຳໃຊ້ໃນທາງທີ່ຜິດ, ຕາມກົດລະບຽບ ແລະ ຂັ້ນຕອນທີ່ໃຊ້ບັງຄັບສຳລັບການເປີດເຜີຍຕໍ່ສາທາລະນະ. ພາຍໃຕ້ລິຂະສິດມາດຕະຖານ ຂໍ້ມູນ, TLP:CLEAR ສາມາດເຜີຍແຜ່ໄດ້ໂດຍບໍ່ມີຂໍ້ຈຳກັດ. ສຳລັບຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບໂປຣໂຕຄອນໄຟຈາລາຈອນ, ໃຫ້ເບິ່ງທີ່ cisa.gov/tlp

MITER ATT&CK –ງານຝີມື APT40 ທາງປະຫວັດສາດທີ່ໜ້ າສົນໃຈ

ການລາດຕະເວນ (TA0043)	
ຄົ້ ນຫາເວັບໄຊທ໌ຂອງຜູ້ ຖືກເຄາະຮ້າຍເປັນເຈົ້ າຂອງ (T1594)	ເກັບກໍ າຂໍ້ ມູນຕົວຕົນຂອງຜູ້ ເຄາະຮ້າຍ: ຂໍ້ ມູນປະຈໍ າຕົວ (T1589.001)
ກໍ າລັງສະແກນຢູ່: ການສະແກນຊ່ອງໂຫວ່ (T1595.002)	ຮອບຮອມຂໍ້ ມູນຜູ້ ຖືກເຄາະຮ້າຍ (T1592)
ຄົ້ ນຫາເປີດເວັບໄຊທ໌/ໂດເມນທີ່ເປີດ: ເຄື່ອງມືຊອກຫາ (T1593.002)	ເກັບກໍ າຂໍ້ ມູນເຄືອຂ່າຍຜູ້ ຖືກເຄາະຮ້າຍ: ຄຸນສົມບັດໂດເມນ (T1590.001)
ເກັບກໍ າຂໍ້ ມູນຕົວຕົນຂອງຜູ້ ເຄາະຮ້າຍ: ທີ່ຢູ່ອີເມວ (T1589.002)	

ການພັດທະນາຊັບພະຍາກອນ (TA0042)	
ໄດ້ຮັບພື້ ນຖານໂຄງລ່າງ: ໂດເມນ (T1583.001)	ໄດ້ຮັບໂຄງສ້າງພື້ ນຖານ (T1583)
ໄດ້ຮັບພື້ ນຖານໂຄງລ່າງ: ເຊີບເວີ DNS (T1583.002)	ບັນຊີທີ່ຖືກບຸກລຸກ (T1586)
ພັດທະນາຄວາມສາມາດ: ໃບຢັ້ ງຢືນການເຊັນລະຫັດ (T1587.002)	ໂຄງສ້າງພື້ ນຖານທີ່ມີຄວາມສ່ຽງ (T1584)
ພັດທະນາຄວາມສາມາດ: ໃບຢັ້ ງຢືນດິຈິຕອນ (T1587.003)	ພັດທະນາຄວາມສາມາດ: ມັນແວ (T1587.001)
ໄດ້ຮັບຄວາມສາມາດ: ໃບຢັ້ ງຢືນການເຊັນລະຫັດ (T1588.003)	ສ້າງຕັ້ ງບັນຊີ: ບັນຊີຄລາວ (T1585.003)
ໂຄງສ້າງພື້ ນຖານທີ່ຖືກບຸກລຸກ: ອຸປະກອນເຄືອຂ່າຍ (T1584.008)	ໄດ້ຮັບຄວາມສາມາດ: ໃບຢັ້ ງຢືນດິຈິຕອນ (T1588.004)

ການເຂົ້ າເຖິງເບື້ ອງຕົ້ ນ (TA0001)	
ບັນຊີທີ່ຖືກຕ້ອງ (T1078)	ຟິດຊິງ (T1566)
ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີເລີ່ມຕົ້ ນ (T1078.001)	ຟິດຊິງ: ໄຟລ໌ແນບສະເປີຍຟິດຊິງ (T1566.001)
ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີໂດເມນ (T1078.002)	ຟິດຊິງ: ລິ້ ງສະເປີຍຟິດຊິງ (T1566.002)
ບໍລິການທາງໄກພາຍນອກ (T1133)	ໃຊ້ປະໂຫຍດແອັບພລິເຄຊັນທີ່ເຜີຍແຜ່ສູ່ສາທາລະນະ (T1190)
ຂໍ້ ຕົກລົງປະນີປະນອມລະຫວ່າງຂັບລົດຜ່ານ (T1189)	

ການດຳເນີນການ (TA0002)	
ເຄື່ອງມືການຈັດການ Windows (T1047)	ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: Python (T1059.006)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: ທີ່ (T1053.002)	ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: JavaScript (T1059.007)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: ໜ້າວຽກທີ່ກຳນົດເວລາໄວ້ (T1053.005)	API ດັ້ງເດີມ (T1106)
ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ (T1059)	ການສື່ສານລະຫວ່າງຂະບວນການ (T1559)
ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: ເຊວຄຳສັ່ງ Windows (T1059.003)	ບໍລິການລະບົບ: ການດຳເນີນການບໍລິການ (T1569.002)
ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: PowerShell (T1059.001)	ການໃຊ້ປະໂຫຍດສຳລັບການດຳເນີນການຂອງລູກຄ້າ (T1203)
ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: Visual Basic (T1059.005)	ການດຳເນີນການຜູ້ໃຊ້: ໄຟລ໌ທີ່ເປັນອັນຕະລາຍ (T1204.002)
ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: ເຊວ Unix (T1059.004)	ຕົວແປຄຳສັ່ງ ແລະ ການຂຽນສະຄຣິບ: ສະຄຣິບ Apple (T1059.002)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: Cron (T1053.003)	ເຄື່ອງມືການນຳໃຊ້ຊອບແວ (T1072)

ຄວາມຄົງຢູ່ (TA0003)	
ບັນຊີທີ່ຖືກຕ້ອງ (T1078)	ອົງປະກອບຊອບແວເຊີບເວີ: ເວັບເຊວ (T1505.003)
ການເລີ່ມຕົ້ນແອັບພລິເຄຊັນສຳນັກງານ: Office Template Macros (T1137.001)	ສ້າງ ຫຼື ແກ້ໄຂຂະບວນການລະບົບ: ບໍລິການ Windows (T1543.003)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: ທີ່ (T1053.002)	ການດຳເນີນການບູດ ຫຼື ເຂົ້າສູ່ລະບົບອັດຕະໂນມັດ: Registry Run Keys / ໂຟເດີເລີ່ມຕົ້ນ (T1547.001)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: ໜ້າວຽກທີ່ກຳນົດເວລາໄວ້ (T1053.005)	ການດຳເນີນການບູດ ຫຼື ເຂົ້າສູ່ລະບົບອັດຕະໂນມັດ: ການແກ້ໄຂທາງລັດ (T1547.009)
ບໍລິການທາງໄກພາຍນອກ (T1133)	ຂັ້ນຕອນການດຳເນີນການໄຮແຈັກ: ການແຮັກຄຳສັ່ງຄົ້ນຫາ DLL (T1574.001)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: Cron (T1053.003)	ຂັ້ນຕອນການດຳເນີນການໄຮແຈັກ: ດາວໂຫຼດ DLL ຈາກດ້ານຂ້າງ (T1574.002)
ການຈັດການບັນຊີ (T1098)	ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີຄລາວ (T1078.004)
ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີໂດເມນ (T1078.002)	

ການຍົກລະດັບສິດທິພິເສດ (TA0004)	
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: ທີ່ (T1053.002)	ສ້າງ ຫຼື ແກ້ໄຂຂະບວນການລະບົບ: ບໍລິການ Windows (T1543.003)
ໜ້າວຽກ/ວຽກທີ່ກຳນົດໄວ້: ໜ້າວຽກທີ່ກຳນົດເວລາໄວ້ (T1053.005)	ການດຳເນີນການບູດ ຫຼື ເຂົ້າສູ່ລະບົບອັດຕະໂນມັດ: Registry Run Keys / ໂຟເດີເລີ່ມຕົ້ນ (T1547.001)
ຂະບວນການສີດ: ການແຮັກການດຳເນີນການ (T1055.003)	ການດຳເນີນການບູດ ຫຼື ເຂົ້າສູ່ລະບົບອັດຕະໂນມັດ: ການແກ້ໄຂທາງລັດ (T1547.009)
ຂະບວນການສີດ: ຂະບວນການເຈາະລ່ອງ (T1055.012)	ຂັ້ນຕອນການດຳເນີນການໄຮແຈັກ: ການແຮັກຄຳສັ່ງຄົ້ນຫາ DLL (T1574.001)

ການຍົກລະດັບສິດທິພິເສດ (TA0004)	
ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີໂດເມນ (T1078.002)	ການໃຊ້ປະໂຫຍດສຳລັບການຍົກລະດັບສິດທິພິເສດ (T1068)
ການຈັດການໂທເຄັນການເຂົ້າເຖິງ: ການປອມແປງ/ລັກໂທເຄັນ (T1134.001)	ດຳເນີນການຕາມກິດຈະກຳ: ການປັບປ່ຽນການກຳນົດຄ່າເຊວ Unix (T1546.004)
ຂະບວນການສິດ: ການໃສ່ຫ້ອງສະໝຸດແບບໄດນາມິກລິ້ງ (T1055.001)	ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີໂດເມນ (T1078.002)
ບັນຊີທີ່ຖືກຕ້ອງ: ບັນຊີທ້ອງຖິ່ນ (T1078.003)	

ການຫຼີກລ່ຽງປ້ອງກັນ (TA0005)	
Rootkit (T1014)	ການດຳເນີນການຄຳສັ່ງທາງອ້ອມ (T1202)
ໄຟລ໌ ຫຼື ຂໍ້ ມູນທີ່ສັບສົນ (T1027)	ການດຳເນີນການພຣັອກຊີໄບນາຣີຂອງລະບົບ: Mshta (T1218.005)
ໄຟລ໌ ຫຼື ຂໍ້ ມູນທີ່ສັບສົນ: ການບັນຈຸຊອບແວ (T1027.002)	ການດຳເນີນການພຣັອກຊີໄບນາຣີຂອງລະບົບ: Regsvr32 (T1218.010)
ໄຟລ໌ ຫຼື ຂໍ້ ມູນທີ່ສັບສົນ: ການເຊື່ອມຂໍ້ ມູນ (T1027.003)	ບ່ອນທຳລາຍການຄວບຄຸມຄວາມໄວ້ວາງໃຈ ການເຊັນລະຫັດ (T1553.002)
ໄຟລ໌ ຫຼື ຂໍ້ ມູນທີ່ສັບສົນ: ລວບລວມຫຼັງຈາກການຈັດສົ່ງ (T1027.004)	ການແກ້ໄຂສິດທິຂອງໄຟລ໌ ແລະ ບັນຊີລາຍຊື່: ການແກ້ໄຂສິດໄຟລ໌ ແລະ ບັນຊີລາຍຊື່ Linux ແລະ Mac (T1222.002)
ການປອມແປງ: ກົງກັບຊື່ ຫຼື ສະຖານທີ່ທີ່ຖືກຕ້ອງ (T1036.005)	ການຈຳລອງສະເໝືອນ/ການຫຼົບຫຼີກກ່ອງຊາຍ: ການກວດສອບລະບົບ (T1497.001)
ຂະບວນການສິດ: ການແຮັກການດຳເນີນການ (T1055.003)	ການປິດບັງ (T1036)
ການໂຫຼດລະຫັດສະທ້ອນແສງ (T1620)	ຫຼຸດປະສິດທິພາບການປ້ອງກັນ: ປິດໃຊ້ງານ ຫຼື ແກ້ໄຂໄຟວໍລະບົບ (T1562.004)
ຂະບວນການສິດ: ຂະບວນການເຈາະລ່ວງ (T1055.012)	ເຊື່ອງສິ່ງປະດິດ: ໄຟລ໌ ແລະ ບັນຊີລາຍຊື່ທີ່ເຊື່ອງໄວ້ (T1564.001)
ການກຳຈັດຕົວຊີ້ ວັດ: ການລຶບໄຟລ໌ (T1070.004)	ເຊື່ອງສິ່ງປະດິດ: ປ່ອງທີ່ເຊື່ອງໄວ້ (T1564.003)
ການກຳຈັດຕົວຊີ້ ວັດ: Timestomp (T1070.006)	ຂັ້ ນຕອນການດຳເນີນການໄຮແຈັກ: ການແຮັກຄຳສັ່ງຄົ້ ນຫາ DLL (T1574.001)
ການກຳຈັດຕົວຊີ້ ວັດ: ລຶບບັນທຶກເຫດການ Windows (T1070.001)	ຂັ້ ນຕອນການດຳເນີນການໄຮແຈັກ: ດາວໂຫຼດ DLL ຈາກດ້ານຂ້າງ (T1574.002)
ແກ້ໄຂການລົງທະບຽນ (T1112)	ບໍລິການເວັບ (T1102)
ຖອດລະຫັດ/ຖອດລະຫັດໄຟລ໌ ຫຼື ຂໍ້ ມູນ (T1140)	ການປອມແປງ: ໜ້ າວຽກ ຫຼື ບໍລິການໃສ່ໜ້ າກາກ (T1036.004)
ການປ້ອງກັນຄວາມເສຍຫາຍ (T1562)	

ການເຂົ້ າເຖິງຂໍ້ ມູນປະຈຳຕົວ (TA0006)	
ການຖ່າຍໂອນຂໍ້ ມູນປະຈຳຕົວລະບົບປະຕິບັດການ: ໜ່ວຍຄວາມຈຳ LSASS (T1003.001)	ຂໍ້ ມູນປະຈຳຕົວທີ່ບໍ່ປອດໄພ: ຂໍ້ ມູນປະຈຳຕົວໃນໄຟລ໌ (T1552.001)
ການຖ່າຍໂອນຂໍ້ ມູນປະຈຳຕົວລະບົບປະຕິບັດການ: NTDS (T1003.003)	Brute Force: ການຄາດເດົາລະຫັດຜ່ານ (T1110.001)
ການດັກຈັບຂໍ້ ມູນເຄືອຂ່າຍ (T1040)	ການພິສູດຢືນຢັນຕົວຕົນແບບບັງຄັບ (T1187)

ການເຂົ້າເຖິງຂໍ້ ມູນປະຈຳຕົວ (TA0006)	
ຂໍ້ ມູນປະຈຳຕົວຈາກທີ່ເກັບລະຫັດຜ່ານ: ພວງກະແຈ (T1555.001)	ລັກ ຫຼື ປອມແປງ Kerberos: Kerberoasting (T1558.003)
ການບັນທຶກຂໍ້ ມູນອິນພຸດ: ການລັອກຂໍ້ ມູນ (T1056.001)	ການສະກັດກັ້ ນການກວດສອບສິດຫຼາຍປັດໃຈ (T1111)
ລັກຄຸກກີເຊດຊັນເວັບ (T1539)	ລັກໂທເຄັນການເຂົ້ າເຖິງຂອງແອັບພລິເຄຊັນ (T1528)
ການໃຊ້ປະໂຫຍດເພື່ອເຂົ້ າເຖິງຂໍ້ ມູນປະຈຳຕົວ (T1212)	Brute Force: ການຖອດລະຫັດຜ່ານ (T1110.002)
ການບັນທຶກຂໍ້ ມູນອິນພຸດ: ການຈັບພາບສູນເວັບ (T1056.003)	ການຖ່າຍໂອນຂໍ້ ມູນປະຈຳຕົວລະບົບປະຕິບັດການ: DCSync (T1003.006)
ຂໍ້ ມູນປະຈຳຕົວຈາກຮ້ານຄ້ າລະຫັດຜ່ານ (T1555)	ຂໍ້ ມູນປະຈຳຕົວຈາກທີ່ເກັບລະຫັດຜ່ານ: ຂໍ້ ມູນປະຈຳຕົວຈາກເວັບບຣາວເຊີ (T1555.003)

ການຄົ້ ນຫາ (TA0007)	
ການຄົ້ ນຫາບໍລິການລະບົບ (T1007)	ການຄົ້ ນຫາຂໍ້ ມູນລະບົບ (T1082)
ການຄົ້ ນພົບປ່ອງແອັບພລິເຄຊັນ (T1010)	ການຄົ້ ນຫາບັນຊີ: ບັນຊີທ້ອງຖິ່ ນ (T1087.001)
ການລົງທະບຽນແບບສອບຖາມ (T1012)	ການຄົ້ ນພົບຂໍ້ ມູນລະບົບ, ເຕັກນິກ T1082 - ອົງກອນ | MITER ATT&CK®
ການຄົ້ ນພົບໄຟລ໌ ແລະ ບັນຊີລາຍຊື່ (T1083)	ການຄົ້ ນຫາເວລາຂອງລະບົບ (T1124)
ການຄົ້ ນຫາບໍລິການເຄືອຂ່າຍ (T1046)	ການຄົ້ ນຫາເຈົ້ າຂອງລະບົບ/ຜູ້ ໃຊ້ (T1033)
ການຄົ້ ນຫາລະບົບທາງໄກ (T1018)	ການຄົ້ ນຫາຄວາມໄວ້ວາງໃຈຂອງໂດເມນ (T1482)
ການຄົ້ ນຫາບັນຊີ: ບັນຊີອີເມວ (T1087.003)	ການຄົ້ ນຫາບັນຊີ: ບັນຊີໂດເມນ (T1087.002)
ການຄົ້ ນຫາການເຊື່ອມຕໍ່ເຄືອຂ່າຍລະບົບ (T1049)	ການຈຳລອງສະເໝືອນ/ການຫຼົບຫຼີກກ່ອງຊາຍ: ການກວດສອບລະບົບ (T1497.001)
ການຄົ້ ນພົບຂະບວນການ (T1057)	ການຄົ້ ນພົບຊອບແວ (T1518)
ການຄົ້ ນພົບກຸ່ມການອະນຸຍາດ: ກຸ່ມໂດເມນ (T1069.002)	ການຄົ້ ນພົບການແບ່ງປັນເຄືອຂ່າຍ ເຕັກນິກ T1135 - ອົງກອນ | MITRE ATT&CK®
ການຄົ້ ນຫາການກຳນົດຄ່າເຄືອຂ່າຍລະບົບ: ການຄົ້ ນຫາການເຊື່ອມຕໍ່ອິນເຕີເນັດ (T1016.001)	

ການເຄື່ອນໄຫວດ້ານຂ້າງ (TA0008)	
ບໍລິການທາງໄກ: ໂປໂຕຄອນເດັສທ໊ອບທາງໄກ (T1021.001)	ບໍລິການທາງໄກ (T1021)
ບໍລິການທາງໄກ: ການແບ່ງປັນຜູ້ ເບິ່ງແຍງລະບົບ SMB/Windows (T1021.002)	ໃຊ້ເອກະສານຢືນຢັນຕົວຕົນອື່ ນ: ສິ່ງຕົວ (T1550.003)
ບໍລິການທາງໄກ: ການຄຸ້ ມຄອງໄລຍະໄກຂອງ Windows (T1021.006)	ການຖ່າຍໂອນເຄື່ ອງມືດ້ານຂ້າງ (T1570)

ຂອງສະສົມ (TA0009)	
ຂໍ້ ມູນຈາກລະບົບທ້ອງຖິ່ ນ (T1005)	ຂໍ້ ມູນທີ່ຮວບຮວມໃນຄັ ງ: ຈັດເກັບຜ່ານຫ້ ອງສະໝຸ ດ (T1560.002)
ຂໍ້ ມູນຈາກເຄືອຂ່າຍທີ່ແບ່ງປັນ Drive (T1039)	ການເກັບກຳອີເມວ: ການເກັບກຳອີເມວທາງໄກ (T1114.002)

ຂອງສະສົມ (TA0009)	
ການບັນທຶກຂໍ້ ມູນອິນພຸດ: ການລັອກຂໍ້ ມູນ (T1056.001)	ຂໍ້ ມູນຄລິບບອດ (T1115)
ການເກັບກຳຂໍ້ ມູນອັດໂນມັດ (T1119)	ຂໍ້ ມູນຈາກຄັງຂໍ້ ມູນ (T1213)
ການບັນທຶກຂໍ້ ມູນອິນພຸດ: ການຈັບພາບສູນເວັບ (T1056.003)	ການຈັດກຽມຂໍ້ ມູນ: ການຈັດກຽມຂໍ້ ມູນໄລຍະໄກ (T1074.002)
ການຈັດກຽມຂໍ້ ມູນ: ການຈັດກຽມຂໍ້ ມູນທ້ອງຖິ່ນ (T1074.001)	ເກັບກຳ ຂໍ້ ມູນໃນແຟ້ມຈັດເກັບ (T1560)
ການເກັບກຳຂໍ້ ມູນອີເມວ (T1114)	

ການກັ່ນຕອງ (TA0010)	
ການກັ່ນຕອງຜ່ານ C2 Channel (T1041)	ການກອງຂໍ້ ມູນຜ່ານໂປຣໂຕຄອນທາງເລືອກ ການກອງຂໍ້ ມູນ ຜ່ານໂປຣໂຕຄອນທີ່ບໍ່ແມ່ນ C2 ທີ່ເຂົ້ າລະຫັດແບບບໍ່ສົມມາດ (T1048.002)
ການກອງຜ່ານໂປຣໂຕຄອນທາງເລືອກ (T1048)	ການກອງຜ່ານບໍລິການເວັບ: ການສົ່ງຂໍ້ ມູນໄປຍັງລະບົບຈັດເກັບ ຂໍ້ ມູນໃນຄລາວ (T1567.002)

ການສັ່ງການ ແລະ ຄວບຄຸມ (TA0011)	
ການປົກປິດຂໍ້ ມູນ: ການປອມຕົວເປັນໂປຣໂຕຄອນ (T1001.003)	ບໍລິການເວັບ: ຕົວແກ້ໄຂບັນຫາ Dead Drop (T1102.001)
ພອດທີ່ໃຊ້ທົ່ວໄປ (T1043)	ບໍລິການເວັບ: ການສື່ສານທາງດຽວ (T1102.003)
ໂປຣໂຕຄອນຊັ້ ນຂໍ້ ມູນແອັບພລິເຄຊັນ: ໂປໂຕຄອນເວັບ (T1071.001)	ການໂອນເຄື່ອງມືຂາເຂົ້ າ (T1105)
ໂປຣໂຕຄອນຊັ້ ນຂໍ້ ມູນແອັບພລິເຄຊັນ: ໂປຣໂຕຄອນການຖ່າຍໂອນ ໄຟລ໌ (T1071.002)	ພຣັອກຊີ: ພຣັອກຊີພາຍໃນ (T1090.001)
ພຣັອກຊີ: ພຣັອກຊີພາຍນອກ (T1090.002).	ພອດທີ່ບໍ່ໄດ້ມາດຕະຖານ (T1571)
ພຣັອກຊີ: ພຣັອກຊີຫຼາຍຮ້ອບ (T1090.003)	ການສ້າງອຸໂມງໂປຣໂຕຄອນ (T1572)
ບໍລິການເວັບ: ການສື່ສານແບບສອງທິດທາງ (T1102.002)	ຊ່ອງສັນຍານເຂົ້ າລະຫັດ (T1573)
ຊ່ອງສັນຍານທີ່ເຂົ້ າລະຫັດ: ການເຂົ້ າລະຫັດແບບບໍ່ສົມມາດ (T1573.002)	ການໂອນເຄື່ອງມືຂາເຂົ້ າ (T1105)
ພຣັອກຊີ, ເຕັກນິກ T1090 - ອົງກອນ | MITER ATT&CK®	

ຜົນກະທົບ (TA0040)	
ການຢຸດເຊົາການບໍລິການ (T1489)	ການລ້າງຮາດດິສ (T1561)
ການປິດລະບົບ/ຣີບູດ (T1529)	ການລັກລອບແຫ່ ງຂໍ້ ມູນ (T1496)

ໝາຍເຫດ

ການປະຕິເສດຄວາມຮັບຜິດຊອບ

ເນື້ອຫາໃນຄູ່ມືນີ້ແມ່ນມີລັກສະນະທົ່ວໄປ ແລະ ບໍ່ຄວນຖືເປັນຄຳແນະນຳທາງດ້ານກົດໝາຍ ຫຼື ໃຊ້ເປັນຂໍ້ມູນຊ່ວຍເຫຼືອໃນສະຖານະການສະເພາະໃດໜຶ່ງ ຫຼື ສະຖານະການສຸກເສີນ. ໃນເລື່ອງທີ່ສຳຄັນໃດໆ, ທ່ານຄວນຊອກຫາຄຳແນະນຳຈາກຜູ້ຊ່ຽວຊານອິດສະຫຼະທີ່ເໝາະສົມກັບສະຖານະການຂອງທ່ານເອງ.

ເຄື່ອງຈັກພາບຈະບໍ່ຮັບຜິດຊອບໃດໆ ຕໍ່ຄວາມເສຍຫາຍ, ການສູນເສຍ ຫຼື ຄ່າໃຊ້ຈ່າຍໃດໆທີ່ເກີດຂຶ້ນອັນເປັນຜົນມາຈາກເພິ່ງພາຂໍ້ມູນທີ່ມີຢູ່ໃນຄູ່ມືນີ້.

ລິຂະສິດ

ການນຳໃຊ້ການເຄື່ອງໝາຍ

ເງື່ອນການໃຊ້ການເຄື່ອງໝາຍນັ້ນມີລາຍລະອຽດຢູ່ໃນເວັບໄຊທ໌ຂອງກົມນາຍົກລັດຖະມົນຕີ ແລະ ຄະນະລັດຖະມົນຕີ ຂໍ້ມູນ ແລະ ແນວທາງກ່ຽວກັບການເຄື່ອງໝາຍເຄື່ອງຈັກພາບ | pmc.gov.au.

ຖ້າຕ້ອງການຂໍ້ມູນເພີ່ມເຕີມ ຫຼື ລາຍງານເຫດການຄວາມປອດໄພທາງໄຊເບີ, ໃຫ້ຕິດຕໍ່ພວກເຮົາ:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ເບີໂທນີ້ສາມາດໃຊ້ໄດ້ພາຍໃນອອສເຕຣເລັຍເທົ່ານັ້ນ.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre