ຜູ້ໃຫ້ບໍລິການ “Bulletproof” hosting ຮອຍແຕກໃນເກາะป้องกันของโครงสร้างพื้นฐานของอาดะยากอมทางไซเบิ

ອາດຊະຍາກອນທາງໄຊເບີທີ່ປະສົບຄວາມສຳເລັດແມ່ນຕ້ອງອາໄສໂຄງສ້າງພື້ນຖານທີ່ປອດໄພ, ບໍ່ສາມາດກວດພົບໄດ້ ແລະ ທົນທານ. ພາຍໃຕ້ທຸກໆກໍລະນີຂອງການບຸກລຸກເຄືອຂ່າຍ, ການລັກຂໍ້ມູນສຳຄັນ, ຊອບແວຣ໌ ຮຽກຄ່າໄຖ່ ແຣມຊຳແວຣ໌ (ransomware) ຫຼື ການລັກ ແລະ ການຂາຍຂໍ້ມູນ ໃນເວທີທີ່ ຜິດ ກົດໝາຍ, ແມ່ນໂຄງສ້າງພື້ນຖານ ທີ່ ປອດໄພ ທີ່ຊ່ວຍໃຫ້ອາດຊະຍາກອນທາງໄຊເບີ ສາມາດດຳເນີນງານ ແລະ ຍັງຊັ້ນຕ໋ວຢູ່ໄດ້.

ຢ່າງໃດກໍຕາມ, ສຳລັບອາດຊະຍາກອນທາງໄຊເບີການທີ່ຍັງບໍ່ມີໃຜສາມາດກວດຈັບໄດ້ ແລະ ຍາກທີ່ຈະຕິດຕາມກາຍເປັນສິ່ງທ້າທາຍເພີ່ມຂຶ້ນ. ການຮ່ວມມືທົ່ວໂລກລະຫວ່າງລັດຖະບານ, ການບັງຄັບໃຊ້ກົດໝາຍ, ແລະ ພາກເອກະຊົນ ແມ່ນເຮັດໃຫ້ມັນຍາກຂຶ້ນສຳລັບພວກເຂົາທີ່ຍັງບໍ່ເປີດເຜີຍຕົວຕົນທາງ ອອນລາຍ. ນອກຈາກນັ້ນ, ອາດຊະຍາກອນທາງໄຊເບີບໍ່ເທົ່າໃດຄົນທີ່ມີຄວາມສາມາດ ແລະ ຄວາມ ຊ່ຽວຊານເຊິ່ງເປັນສິ່ງຕ້ອງມີໃນການຈັດການ ແລະ ຮັກສາໂຄງສ້າງພື້ນຖານທີ່ປອດໄພ ດ້ວຍຕົນເອງ. ດັ່ງນັ້ນ, ພວກເຂົາ ຊອກຫາຜູ້ໃຫ້ບໍລິການໂຄງສ້າງພື້ນຖານທີ່ຜິດກົດໝາຍທີ່ ສາມາດໃຫ້ ບໍລິການນີ້ໃນນາມຂອງພວກເຂົາ ເຊິ່ງເຮັດໃຫ້ຜູ້ກໍ່ອາດຊະຍາກຳ ທາງໄຊເບີສຸມໃສ່ເຫຍື່ອຜູ້ ເຄາະຮ້າຍ ແລະ ສະແຫວງຫາກຳໄລໄດ້.

‘ອາດຊະຍາກຳທາງໄຊເບີໃນຮູບແບບບໍລິການ’('Cybercrime-as-a-service') ໝາຍເຖິງ ຕະຫຼາດໃຕ້ດິນທີ່ພັດທະນາຂຶ້ນເພື່ອ ສະໜັບສະໜູນກຸ່ມຜູ້ກະທຳຜິດທາງໄຊເບີທີ່ເປັນ ອັນຕະລາຍ. ຕະຫຼາດໃຕ້ດິນນີ້ປະກອບດ້ວຍເຄື່ອງມື, ບໍລິການ, ແລະ ຂໍ້ມູນທີ່ຊື້ ໄດ້ເຊິ່ງເພີ່ມຂຶ້ນ ແລະ ພັດທະນາຢ່າງຕໍ່ເນື່ອງທີ່ຊ່ວຍ ພວກກໍ່ອາດຊະຍາກຳທາງໄຊເບີໃນການ ຫຼອກເປົ້າໝາຍ ທາງອອນລາຍໃຫ້ຕົກ ເປັນເຫຍື່ອໄດ້. ຜູ້ທີ່ຢາກເປັນອາດຊະຍາກອນທາງໄຊເບີສາມາດຊື້ການເຂົ້າເຖິງເຄືອຂ່າຍ, ຊື້ເຄື່ອງມືເພື່ອ ຊ່ວຍໃນການຫຼີກລ່ຽງມາດ ຕະການຮັກສາຄວາມປອດໄພ, ພ້ອມທັງຊື້ມາລແວ ເພື່ອນຳໃຊ້ ກັບຜູ້ເຄາະຮ້າຍ ແລະ ລັກຂໍ້ມູນສ່ວນຕົວ. ຜູ້ໃຫ້ບໍລິການ Bulletproof hosting (BPH) ແມ່ນສ່ວນໜຶ່ງຂອງລະບົບນິເວດນີ້ ແລະ ສະເໜີໂຄງສ້າງພື້ນຖານທີ່ປອດໄພສຳລັບອາດຊະຍາກອນທາງໄຊເບີ. ສິ່ງສຳ ຄັນ, ຜູ້ໃຫ້ບໍລິການ BPH ພຽງຄົນດຽວສາມາດເຮັດໃຫ້ຜູ້ກໍ່ອາດຊະຍາກຳທາງໄຊເບີ ຫຼາຍຮ້ອຍຄົນກຳນົດເປົ້າໝາຍເຫຍື່ອໃນທົ່ວໂລກ ໄດ້ໂດຍກົງ.

ผู้ให้บริการ "Bulletproof" hosting แม่นหยัง?

ເວົ້າງ່າຍໆກໍຄື ຜູ້ໃຫ້ບໍລິການ BPH ຈະໃຫ້ຜູ້ກໍ່ອາດຊະຍາກຳທາງໄຊເບີເຊົ່າໂຄງສ້າງພື້ນຖານ ທີ່ຄືແທ້ ແລະ/ຫຼື ທາງກາຍຍະພາບເພື່ອ ດຳເນີນການ. ຜູ້ໃຫ້ບໍລິການ BPH ເປັນປະເພດສະເພາະຂອງການບໍລິການໂຄງສ້າງພື້ນຖານອິນເຕີເນັດທີ່ ຊ່ວຍໃຫ້ຜູ້ກະທຳທີ່ເປັນ ອັນຕະລາຍ (ລວມທັງຜູ້ກໍ່ອາດຊະຍາກຳທາງໄຊເບີ) ສາມາດຈັດ ການເນື້ອຫາທີ່ຜິດກົດໝາຍ ແລະ ດຳເນີນງານໃນທາງອິນເຕີເນັດໄດ້.

ຄຳວ່າ "bulletproof" ແມ່ນການຕະຫຼາດຢ່າງແທ້ຈິງ. ໃນຄວາມເປັນຈິງ, ການບໍລິການເຫຼົ່ານີ້ແມ່ນມີຄວາມສ່ຽງຕໍ່ການຂັດຂວາງ ເຊັ່ນດຽວກັນກັບ ຜູ້ໃຫ້ບໍລິການດ້ານໂຄງສ້າງພື້ນຖານອື່ນໆ. ໃນທາງກັບກັນ, ຜູ້ໃຫ້ບໍລິການ BPH ປະຕິເສດທີ່ຈະປະຕິບັດຕາມ ການບັງຄັບໃຊ້ກົດໝາຍ ແລະ ການຮ້ອງຂໍໃຫ້ລຶບເນື້ອຫາອື່ນໆ ແລະ ເພີ່ກເສີຍຕໍ່ຄຳຮ້ອງຮຽນກ່ຽວກັບການລະເມີດ ຈາກຜູ້ຖືກເຄາະ ຮ້າຍ ແລະ ການແຈ້ງເຕືອນຄຳຮ້ອງຂໍຂອງສະມາຊິກ. ນີ້ໝາຍຄວາມວ່າຜູ້ກໍ່ອາດຊະຍາກຳທາງໄຊເບີສາມາດຕິດຕໍ່ສື່ສານ, ເປີດເວທີ ສົນທະນາ ແລະ ເວັບໄຊທ໌ທີ່ຜິດກົດໝາຍ, ນຳໃຊ້ ມາລແວ ແລະ ການໂຄສະນາຫຼອກເອົາຂໍ້ມູນ ຟິຊຊິ່ງ (phishing)ແລະ ຟອກເງິນ ໂດຍບໍ່ມີຄວາມຢ້ານກົວວ່າຜູ້ໃຫ້ບໍລິການ ຈະຍົກເລີກ ການເຊົ່າຂອງພວກ ເຂົາຕາມການບັງຄັບໃຊ້ກົດໝາຍ ຫຼື ຕາມຄຳຮ້ອງຂໍອື່ນໆ.

ຜູ້ໃຫ້ບໍລິການ BPH ມີສ່ວນຮ່ວມໃນລະບົບນິເວດຂອງອາດຊະຍາກຳທາງໄຊເບີຢ່າງຮູ້ເຫັນ ແລະ ເຮັດໃຫ້ເກີດອາດຊະຍາກຳທາງໄຊເບີ ທີ່ ກໍ່ໃຫ້ເກີດແຮງຈູງໃຈທາງດ້ານ ການເງິນ ທີ່ຮ້າຍແຮງ. ເຫດການຄວາມປອດໄພທາງໄຊເບີທີ່ສຳຄັນທີ່ສົ່ງຜົນກະທົບຕໍ່ອົງການຈັດຕັ້ງ ຂອງອົດສະ ຕຣາລີ ແລະ ລູກຄ້າຂອງພວກເຂົາໄດ້ເກີດຂຶ້ນຍ້ອນອາດຊະຍາກອນທີ່ໃຊ້ປະໂຫຍດ ຈາກ ຜູ້ໃຫ້ບໍລິການ BPH. ຜົນທີ່ຕາມ ມາຂອງເຫດການເຫຼົ່ານີ້ລວມມີການໂຈມຕີດ້ວຍ ແຣມຊຳແວຣ໌ ການຂົ່ມຂູ່ເອົາ ຂໍ້ມູນ ແລະ ການລັກຂໍ້ມູນທີ່ລະອຽດອ່ອນ.

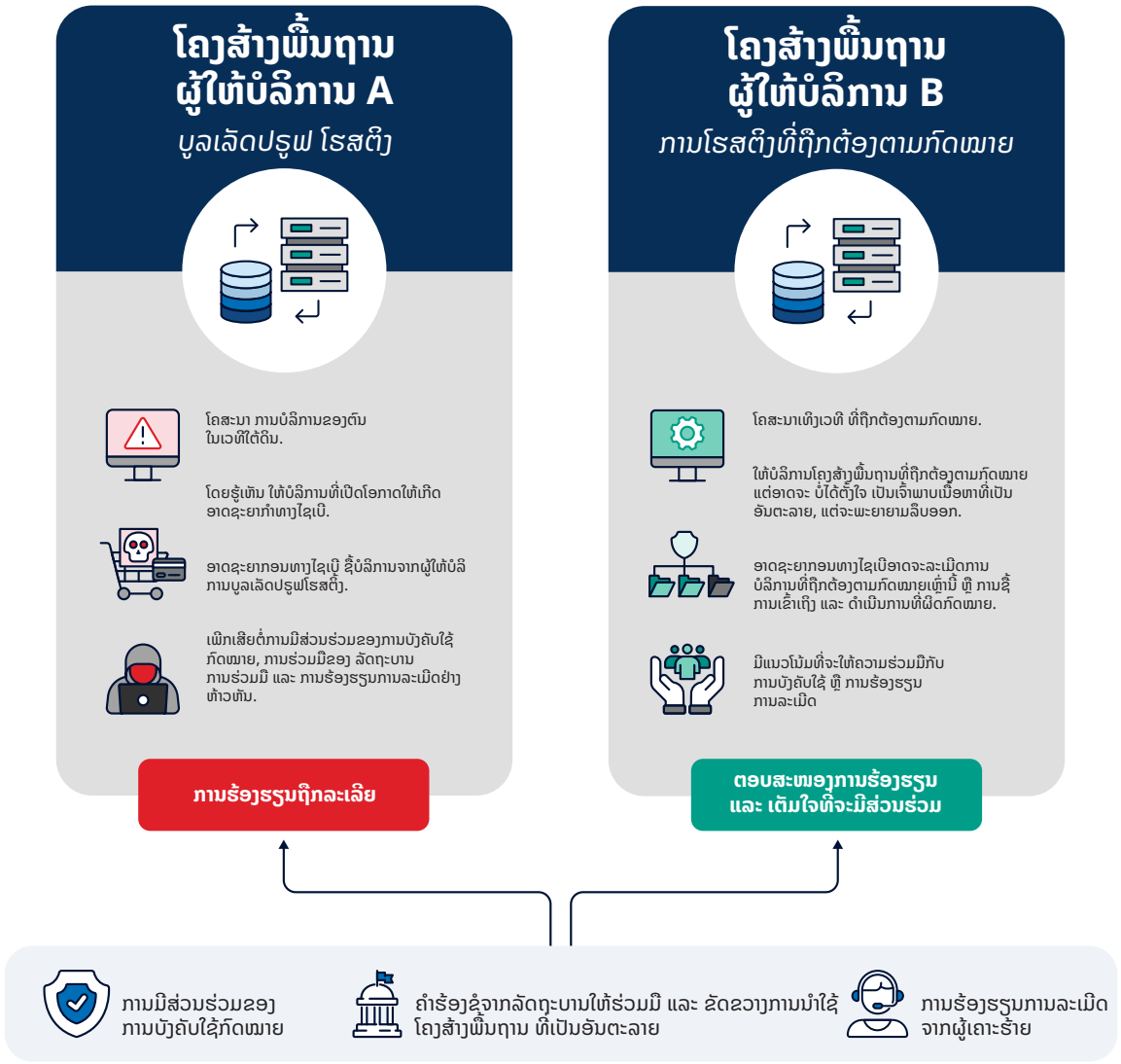
ภานนำสะเพิ ผู้ให้บริภาน bulletproof hosting [1] ภานโถสะมาผู้ให้บริภานใน เวทีใต้ดิน:

ผู้ให้บริภาน BPH เธิดวยกแมวใด?

รูบแบบทุละกิดแตกต่างกันไปละหว่างผู้ให้บริภาน BPH. วิทีภานที่พับเห้นเลื้อยๆที่สุดก่ยวข้องกับภานเช่าที่ยู่ IP ให้กับลูกค้าที่เป้น อาดชะยากอมทางไซเบิ และ ใช้วิทีภานป่ยนเถือข่ายที่ซับซ้อนเพื่อช่วยปิดบัง สะถานที่, ต์วต์น และ กิดจะกำของพวกเข้า. ในพ้ายๆกำละมิ, ผู้ให้บริภาน BPH จะขายต่ ซือ เช่าที่ยู่ IP และ เธ็บเวิจาก ผู้ให้บริภานโธสติ้ง, สูมข้อมูน ซือ ผู้ให้บริภานอิมเติเม้ด (ISPs) ที่ถืกต้องตาม กัดพมายอื่นๆ. ผู้ให้บริภาน 'ต้นทาง' เห้านี้อาดจะบ่รู้ต์วว่า พวกเข้ากำลังสะพองโครงสร้างพื้นถาน ให้แก่ผู้ให้บริภาน BPH เธิ่งต่มาป้นผู้ที่ให้บริภาน 'ปายทาง' ให้แก่ผู้ก่อาดชะยากำทาง ไซเบิ.

ผู้ให้บริภาน BPH กำนัดถ่าเถือข่าย และ สะถาปัดตะยะกำละบับของต์น เพื่อ เธิดให้มันยากที่จะละบุลูกค้าของเข้าเจ้าได้. ต์วย่างเช่น เข้าเจ้ามักจะป่รุนต์วละบุต์วต์นที่เธื่อมต่กับอิมเติเม้ดที่ก่ยวข้องกับ กิดจะกำของลูกค้าเลื้อยๆ- เช่น: ที่ยู่ IP ที่ได้รับมอบพมาย และ ซื่โดเมน. เต้กนิกดั่งก่าวท้าทายผู้ถืกก่าวฟ้อง และ ผู้สืบสวนโดยภานเธิดให้มันยาก ที่จะ เธื่อมโยงเทดภานและที่ยู่ IP ที่ถืกนำใช้โดยผู้กะทำ ซือ ลูกค้าในเวลาใดก่ตาม. นอกจากนั้น, ผู้ให้บริภาน BPH มักจะใช้โครงสร้างพื้นถานในปะเทดที่มีละบับ ไซเบิ ที่ได้รับอะนุยาด, เธิ่งมาดตะภานย่างเป้นทางภานเพื่อสืบสวน และ ป้องกัน กิดจะกำไซเบิที่เป้นอันตะลายนั้นแม่นบ่มียู่แท้ ซือ ที่บ่เค้งถัด.

ผู้ให้บริการ บูลเล็ดปรูฟ โรสติ้ง มีความแตกต่างกันแนวใด กับผู้ให้บริการโครงสร้างพื้นฐานที่ถูกกฎหมาย?



การกำหนดเป้าหมายผู้ให้บริการ BPH มีผลกระทบ ต่อไซเบอร์ต่ออาชญากรทางไซเบอร์ แนวใด

ผู้ให้บริการ BPH ถือเป็นโอกาสอันมีค่าที่จะยุติยั้งอาชญากรทางไซเบอร์ หลาย ร้อยหาหลายพันคนในเวลาเดียวกัน. อาชญากรทางไซเบอร์หลายกลุ่ม และ ผู้กระทำผิดทางไซเบอร์ที่เป็นอันตรายอื่นๆ ใช้บริการเหล่านี้เพื่อเริ่ม และ ดำเนินการต่อไปได้ถึงแม้ว่าจะมีการ ร้องขอ การลบล้าง หรือ การร้องเรียนเกี่ยวกับการละเมิด.

อย่างไรก็ตาม, การบังคับใช้กฎหมาย, หน่วยงานของรัฐบาล และ ภาคเอกชน กำลังร่วมมือกันเพื่อกำหนดเป้าหมาย และ ยุติยั้งผู้ให้บริการโครงสร้างพื้นฐานที่ ผิดกฎหมายเหล่านี้, รวมทั้งผ่านมาตรการป้องกันเช่น สะกัดกั้นการรับส่งข้อมูลทางอินเตอร์เน็ตจากผู้ให้บริการ BPH ที่รู้จัก. กิจกรรมเหล่านี้ช่วยลดผลกระทบจำนวนอาชญากรทางไซเบอร์ที่พัวพันกับเครือข่ายอาชญากรรมสากล และ เครือข่ายพันธมิตร, และ รวมถึงผู้ให้บริการโครงสร้างพื้นฐาน และ ISP ‘ต้นทาง’ ที่ถูกต้องตามกฎหมาย ซึ่งอาจจะเริ่มให้ผู้ให้บริการ BPH เข้าถึง อินเตอร์เน็ตได้ และ สนับสนุนโครงสร้างพื้นฐานที่ปลอดภัยให้กับอาชญากรทางไซเบอร์ โดยไม่รู้ตัว.

BPH ไม่ใช่ผู้ให้บริการโครงสร้างพื้นฐานประเภทเดียวในระบบนิเวศ ของอาชญากรทางไซเบอร์ ในรูปแบบบริการ (cybercrime-as-a-service). การบริการเหล่านี้เริ่มให้มีการยืดเยื้อและเกิดภัยคุกคามทางไซเบอร์ต่ออาชญากรรม โดยการสนับสนุนการโจมตีด้านอาชญากรทางไซเบอร์ อย่างทันท่วงที และ เจตนา ขัดขวางการสืบสวน และ การตอบโต้ที่ถูกต้องตามกฎหมาย. การดำเนินการกับผู้ให้บริการ BPH ชี้ให้เห็นถึงช่องโหว่ของการบริการเหล่านี้ และ ของผู้กระทำผิดทางไซเบอร์ที่เป็นอันตรายที่นำใช้บริการเหล่านี้