National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

BND

Bundesamt für Verfassungsschutz

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

ຄຳແນະນຳ

BADBAZAAR ແລະ MOONSHINE: ການວິເຄາະທາງເຕັກນິກ ແລະ ການບັນເທົາຜົນກະທົບ

ວັນທີ 9 ເມສາ 2025

BADBAZAAR ແລະ MOONSHINE: ການວິເຄາະທາງເຕັກນິກ ແລະ ການບັນເທົາຜົນກະທົບ

ບົດສະຫຼຸບ

ດ້ວຍການສະໜັບສະໜູນ Cyber League ໄຊເບີລີກຈາກອັງກິດ, ຄຳແນະນຳນີ້ໄດ້ຮັບການຜະລິດ ຮ່ວມກັນ ໂດຍສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດ (NCSC UK) ແລະ ຄູ່ຮ່ວມງານສາກົນ:

- **ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕາລີ, ເຊິ່ງເປັນສ່ວນໜຶ່ງຂອງສຳນັກງານສັນຍານຂອງອົດສະຕາລີ**
- **ສູນຄວາມປອດໄພທາງໄຊເບີຂອງການາດາ, ເຊິ່ງເປັນສ່ວນໜຶ່ງຂອງການສ້າງຕັ້ງຄວາມປອດໄພດ້ານການສື່ສານ**
- **ບໍລິການຂ່າວລັບຂອງລັດຖະບານກາງຂອງເຢຍລະມັນ**
- **ສຳນັກງານລັດຖະບານກາງເຢຍລະມັນເພື່ອປົກປ້ອງລັດຖະທຳມະນູນ**
- **ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດນິວຊີແລນ, ເຊິ່ງເປັນ ສ່ວນໜຶ່ງຂອງສຳນັກງານຄວາມປອດໄພດ້ານສື່ສານຂອງລັດຖະບານ**
- **ສຳນັກງານສືບສວນຂອງລັດຖະບານກາງສະຫະລັດ**
- **ອົງການຄວາມໝັ້ນຄົງແຫ່ງຊາດຂອງສະຫະລັດ**

ຄຳແນະນຳນີ້ໃຫ້ຂໍ້ມູນກ່ຽວກັບໄພຂົ່ມຂູ່ອັນໃໝ່ ແລະ ປະສົມປະສານກັນຢູ່ໃນສະປາຍແວສອງປະເພດທີ່ເອີ້ນວ່າ BADBAZAAR ແລະ MOONSHINE, ແລະ ລວມໄປເຖິງຄຳແນະນຳສຳລັບຜູ້ໃຫ້ບໍລິການຮ້ານແອັບ, ຜູ້ພັດທະນາ ແລະ ບໍລິສັດສື່ສັງຄົມ ເພື່ອຊ່ວຍຮັກສາຜູ້ໃຊ້ຂອງເຂົາເຈົ້າມີຄວາມປອດໄພ.

ຄຳແນະນຳນີ້ໄດ້ຮັບການເຜີຍແຜ່ພ້ອມກັນກັບຄຳແນະນຳສຳລັບຜູ້ເຄາະຮ້າຍຈາກມັນແວເຫຼົ່ານີ້.

ເອກະສານນີ້ໃຊ້ຄຳນິຍາມຄຳສັບຂອງ NCSC ຂອງ ສະປາຍແວ: "ມັນແວປະເພດໜຶ່ງທີ່ຕິດຕັ້ງຢູ່ໃນອຸປະກອນໂດຍ ບໍ່ໄດ້ຮັບການຍິນຍອມຈາກຜູ້ໃຊ້, ການລວບລວມຂໍ້ມູນ ແລະ ສົ່ງຂໍ້ມູນດັ່ງກ່າວໄປຫາພາກສ່ວນທີສາມ."

ກໍລະນີສຶກສາທີ່ຫນຶ່ງ: MOONSHINE

MOONSHINE ເປັນສະປາຍແວລະບົບປະຕິບັດການ Android ທີ່ ລາຍງານໃນປີ 2019 ໂດຍ ຫ້ອງທົດລອງພົນລະເມືອງ ເປັນເປົ້າໝາຍກຸ່ມຊາວທິເບດ. MOONSHINE ປອມຕົວເປັນແອັບຖືກກົດໝາຍເພື່ອລໍ້ລວງໃຫ້ຜູ້ຖືກເຄາະຮ້າຍຕິດຕັ້ງ ແອັບນີ້. ໄດ້ມີການແບ່ງປັນຜ່ານຊ່ອງທາງ Telegram ແລະ ຜ່ານລິ້ງທີ່ສົ່ງຜ່ານ WhatsApp.

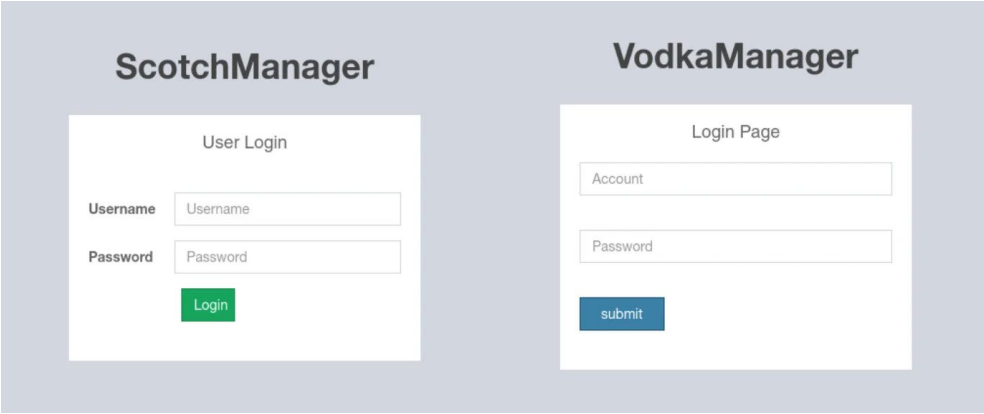
ການຄົ້ນຄວ້າ NCSC ໃນ MOONSHINE ຊີ້ໃຫ້ເຫັນດັ່ງຕໍ່ໄປນີ້:

- MOONSHINE ໃຊ້ການໂຕ້ຕອບການຈັດການທີ່ມີການປ່ຽນແປງນັບຕັ້ງແຕ່ມີການລາຍງານຄັ້ງທຳອິດ.
- ການໂຕ້ຕອບການຈັດການເປີດເຜີຍຄວາມສາມາດໃນການເຝົ້າລະວັງຢ່າງກວ້າງຂວາງ, ລວມທັງຄວາມສາມາດໃນການດຶງ ໄຟລ໌ອອກຈາກອຸປະກອນເຊັ່ນດຽວກັນກັບການບັນທຶກສຽງສົດ ແລະ ການບັນທຶກໜ້າຈໍ.
- ພົບຊຸດອິນເຕີເຟດການຈັດການ MOONSHINE ເປັນເຈົ້າພາບສະເໜີຍນຈິງ ອິນເຕີເຟດເຫຼົ່ານີ້ມີໂຄງສ້າງພື້ນຖານທີ່ທັບຊ້ອນກັບແຜງເຂົ້າສູ່ລະບົບທີ່ກ່ຽວຂ້ອງກັບ UPSEC, ເຊິ່ງອີງຕາມ Intelligence Online ໝາຍເຖິງ 'Sichuan Dianke Network Security Technology Co., Ltd.'.

ອິນເຕີເຟດຈັດການ

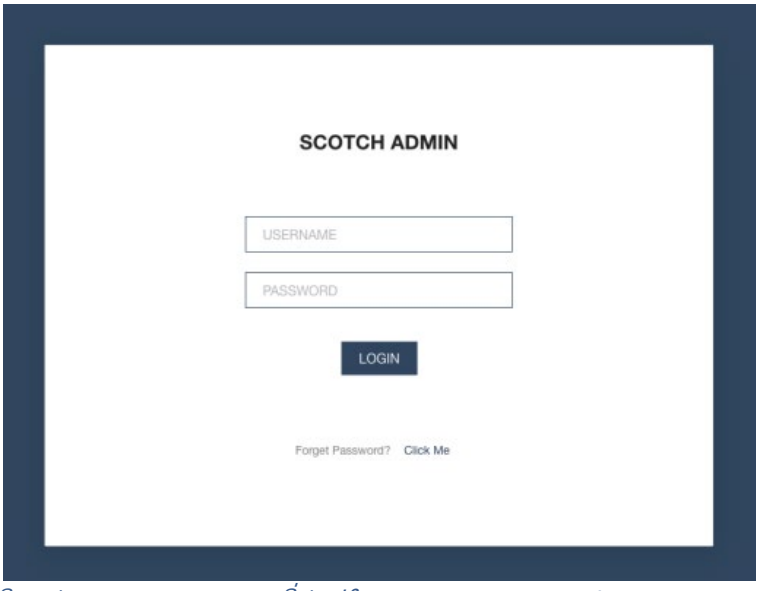
ການລາຍງານກ່ອນໜ້ານີ້ກ່ຽວກັບອິນເຕີເຟດການຈັດການ MOONSHINE ຊີ້ໃຫ້ເຫັນວ່າມີການປ່ຽນແປງ, ເຊິ່ງຊີ້ໃຫ້ເຫັນເຖິງການພັດທະນາຢ່າງຕໍ່ເນື່ອງ.

ຕົວຢ່າງທຳອິດຂອງອິນເຕີເຟດການຈັດການແມ່ນພົບເຫັນຢູ່ໃນການລາຍງານຂອງຫ້ອງທົດລອງພົນລະເມືອງໃນປີ 2019.



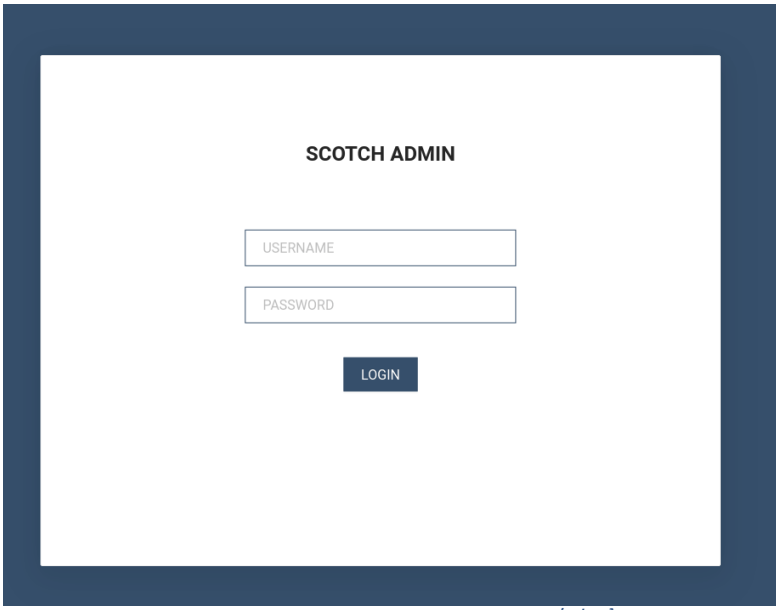
ຮູບທີ 1: ພົບອິນເຕີເຟດຈັດການ MOONSHINE ໃນບົດລາຍງານຂອງຫ້ອງທົດລອງພົນລະເມືອງໃນປີ 2019 ກຸ່ມຊາວທີເບດທີ່ຂາດການເຊື່ອມໂຍງຖືກກຳນົດເປົ້າໝາຍດ້ວຍຊ່ອງໂຫວ່ໃນມືຖືແບບ 1 ຄລິກ'.

ໃນຊ່ວງຕົ້ນປີ 2022, Lookout ໄດ້ລາຍງານອິນເຕີເຟດການຈັດການທີ່ແຕກຕ່າງກັນທີ່ໄດ້ຮັບການອອກແບບໃໝ່ໃຫ້ມີລັກສະນະດັ່ງຕໍ່ໄປນີ້ (ແທນທີ່ອິນເຕີເຟດກ່ອນໜ້າໃນຮູບ 1):



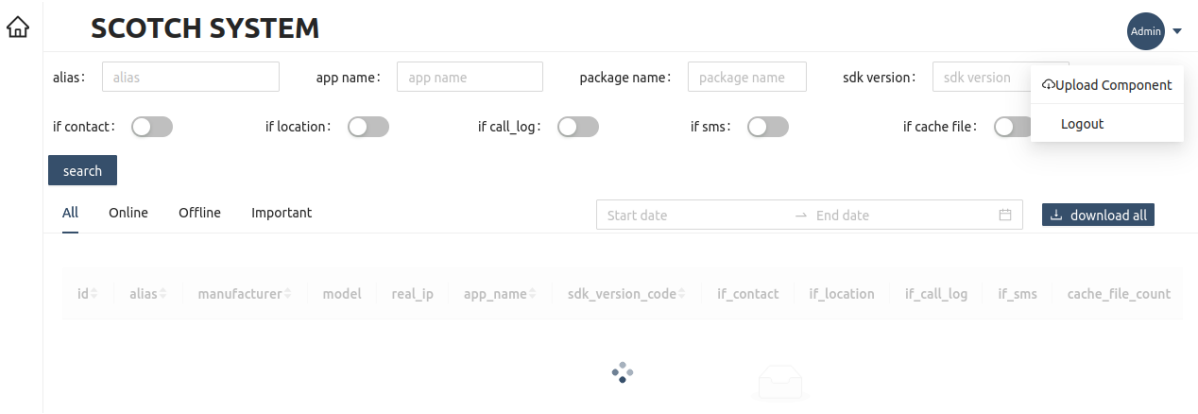
ຮູບທີ 2: ອິນເຕີເຟດຈັດການ MOONSHINE ທີ່ເຫັນຢູ່ໃນລາຍງານ 2022 ຂອງ Lookout ลายงาน 'MOONSHINE: ການພັດທະນາລະບົບເຝົ້າລະວັງແອນດອຍໂດຍ APT POISON CARP ຂອງຈີນເພື່ອກໍານົດເປົ້າໝາຍຂອງຊາວທິເບດ ແລະ ຊາວອຸຍກູ.

ໃນເດືອນສິງຫາ 2023, ການສະແກນ ຂອງຄໍາສັ່ງ ແລະ ການຄວບຄຸມ MOONSHINE (C2) ໄດ້ເປີດເຜີຍໃຫ້ເຫັນ ອິນເຕີເຟດທີ່ຄ້າຍກັບອິນເຕີເຟດປີ 2022 ທີ່ມີຟັງຊັນ **'ລືມລະຫັດຜ່ານ'** ບໍ່ມີໃຫ້ນໍາໃຊ້ອີກຕໍ່ໄປ ຕາມທີ່ສະແດງຢູ່ໃນຮູບທີ 2:



ຮູບທີ 3: ອິນເຕີເຟດການຈັດການ MOONSHINE ປະຕິບັດຕາມໃນເດືອນສິງຫາ 2023 ເຊິ່ງບໍ່ມີຂໍ້ຄວາມແຈ້ງເຕືອນ 'ລືມລະຫັດຜ່ານ' ອີກຕໍ່ໄປ.

ການສືບສວນເພີ່ມເຕີມຂອງອິນເຕີເຟດການຈັດການພົບເນື້ອຫາພາຍໃນແຜງເຊິ່ງຜີຍໃຫ້ເຫັນວ່າລາຍລະອຽດຂອງອຸປະ ກອນທີ່ຖືກທໍາລາຍຈະຖືກເກັບໄວ້ແນວໃດ .



ຮູບທີ 4: ໜ້າເວັບທີ່ຢູ່ດ້ານຫຼັງໜ້າເຂົ້າສູ່ລະບົບຂອງອິນເຕີເຟດການຈັດການ MOONSHINE.

ການຄົ້ນຄວ້າ Lookout ສະແດງໃຫ້ເຫັນການຖ່າຍທອດ **'ຄະແນນ'** ຈາກອຸປະກອນຜູ້ເຄາະຮ້າຍໄປຫາເຊີບເວີ MOONSHINE C2. ມູນຄ່າຂອງ 'ຄະແນນ'
ແມ່ນອີງໃສ່ການອະນຸຍາດຂອງຕົວຢ່າງທີ່ເປັນອັນຕະລາຍໃນອຸປະກອນຜູ້ຖືກເຄາະຮ້າຍ.

ຖັນ 'if_contact', 'if_location', 'if_call_log' ແລະ 'if_sms' ພາຍໃນເພຈນີ້ແນະນຳຕົວຢ່າງ MOONSHINE ບໍ່ສາມາດເຂົ້າເຖິງອຸປະກອນທີ່ຖືກບຸກລຸກໄດ້ທັງໝົດ. ຄວາມຮູ້ກ່ຽວກັບຄໍລຳເຫຼົ່ານີ້ ແລະ 'ຄະແນນ' ທີ່ຜ່ານຈາກອຸປະກອນໄປຫາ C2 ຊີ້ໃຫ້ເຫັນວ່າຜູ້ຂົ່ມຂູ່ກຳລັງໃຊ້ຄະແນນເພື່ອສື່ສານລະດັບການເຂົ້າເຖິງມັນແວທີ່ມີຕໍ່ອຸປະກອນທີ່ຖືກທຳລາຍກັບ ບຸກຄົນທີ່ເຂົ້າເຖິງອິນເຕີເຟດການຈັດການ.

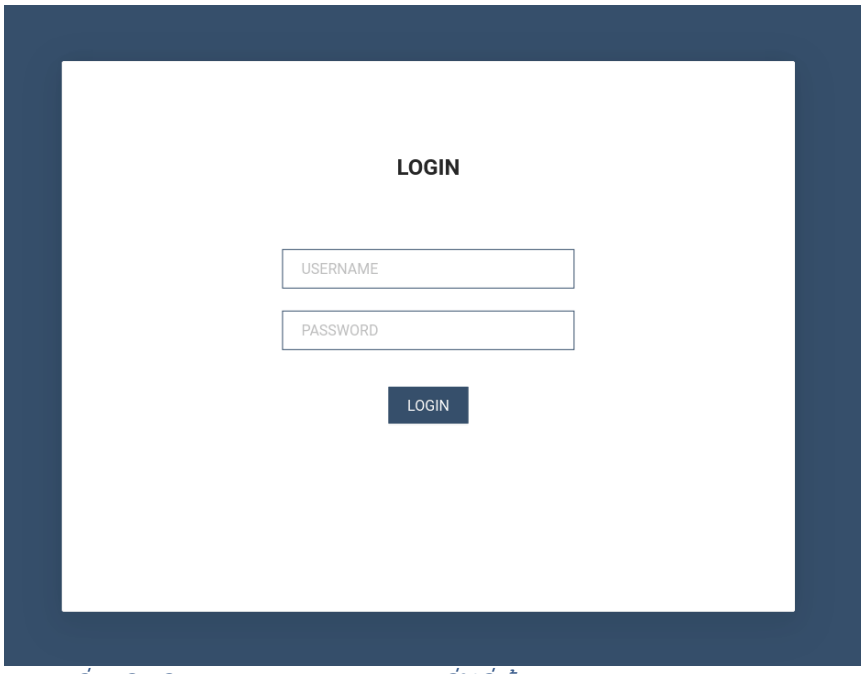
ໂດຍທົ່ວໄປແລ້ວ, ຄຳແນະນຳດ້ານການປະຕິບັດທີ່ດີທີ່ສຸດເພື່ອປ້ອງກັນບໍ່ໃຫ້ແອັບລວບລວມຂໍ້ມູນຈາກອຸປະກອນແມ່ນ ເພື່ອກວດສອບເບິ່ງການອະນຸຍາດແອັບສຳລັບສິ່ງທີ່ຜິດປົກກະຕິກ່ອນທີ່ຈະດາວໂຫຼດ. ແນວໃດກໍ່ຕາມ, ຕົວຢ່າງ MOONSHINE ຈະຂໍອະນຸຍາດທີ່ກ່ຽວຂ້ອງກັບການເຮັດວຽກຂອງແອັບ, ດັ່ງນັ້ນອາດເບິ່ງຄືວ່າບໍ່ໜ້າສົງໄສ, ແຕ່ຍັງໃຊ້ສິດ ເຫຼົ່ານີ້ເພື່ອເກັບກຳຂໍ້ມູນຈາກອຸປະກອນຕ່າງໆ.

MOONSHINE ຍັງມີອິນເຕີເຟດການຂຽນໂປລແກຼມຂອງແອັບພລິເຄຊັນ(API) ເປີດເຜີຍຄວາມສາມາດອັນກວ້າງຂວາງ ຂອງຂອງມັນ. ເອກະສານ API ເວີຊັນທຳອິດມີຊື່ API ເປັນພາສາຈີນ.

ໂຮສສະເໝືອນຈິງ

ໃນການຊອກຫາແຜງ MOONSHINE, ມີການຄົ້ນພົບຕົວຢ່າງທີ່ເປັນແມ່ຂ່າຍເກືອບທັງໝົດ. ໂຮສຕິ້ງສະເໝືອນຈິງແມ່ນ ເມື່ອທີ່ຢູ່ IP ໜຶ່ງສາມາດໂຮສເວັດໄຊຫຼາຍເວັດໄຊໄດ້ໃນເວລາດຽວກັນ. ບໍ່ພົບທີ່ຢູ່ IP ຂອງອິນສະແຕນທີ່ໂຮສສະເໝືອນຈິງ ເຫຼົ່ານີ້ ແລະ ໂດເມນທີ່ໂຮດໃນຕົວຢ່າງມັນແວທີ່ຮູ້ຈັກ.

ຕົວຢ່າງເຫຼົ່ານີ້ຂອງອິນເຕີເຟດການຈັດການເຫຼົ່ານີ້ມີຄວາມແຕກຕ່າງກັນ, ເນື່ອງຈາກຊື່ຂອງໜ້າເວັບຕ່າງໆແມ່ນ **'ເຂົ້າສູ່ລະບົບ'** ແທນທີ່ຈະເປັນ **'SCOTCH ADMIN'** ທີ່ເຫັນກ່ອນໜ້ານີ້.



ຮູບທີ 5: ອິນເຕີເຟດຈັດການ MOONSHINE ທີ່ໃຊ້ຊື່ເຂົ້າສູ່ລະບົບແທນ SCOTCH ADMIN.

ນອກຈາກນີ້, ເນື້ອຫາຢູ່ໃນແຜງຍັງແຕກຕ່າງຈາກຮູບທີ 4 ອີກດ້ວຍ, ດັ່ງທີ່ເຫັນໃນຮູບທີ 6:

ຮູບທີ 6: ໜ້າເວັບທີ່ຢູ່ເບື້ອງຫຼັງໜ້າເຂົ້າສູ່ລະບົບຂອງອິນເຕີເຟດການຈັດການ MOONSHINE ທີ່ໂຮດແບບສະເໝືອນ.

ແຜງໃນຮູບທີ 6 ເບິ່ງຄືຈະເປັນເວີຊັນທີ່ຫຼຸດຂະໜາດຂອງແຜງໃນຮູບທີ 4. ລັກສະນະການທີ່ທັບຊ້ອນກັນຂອງແຜງແມ່ນຊື່ ຖັນ 'id', 'ຜູ້ຜະລິດ' ແລະ 'ຕົວແບບ' ໃນຕາຕະລາງ.

ກໍລະນີຕົວຢ່າງ MOONSHINE ທີ່ໂຮດສະເໝີອນຈິງຄົ້ນພົບແມ່ນ:

ໂດເມນ	ທີ່ຢູ່ IP
vsa.ahamar].]com	194.71.107[.]160
gates.chatonlineapp].]com	172.67.208[.]167
www.onlineweixin].]net	103.254.108[.]108
www.weetogether].]top	103.254.108[.]108
www.onlinewxapp].]net	103.43.18[.]43
www.unusualtransaction].]com	2.58.15[.]101
m.leak-news].]com	103.56.17[.]194
www.unusualtransaction].]com	46.246.98[.]209
www.lodepot].]com	62.72.58[.]168
www.online-wechat].]com	103.254.108[.]87

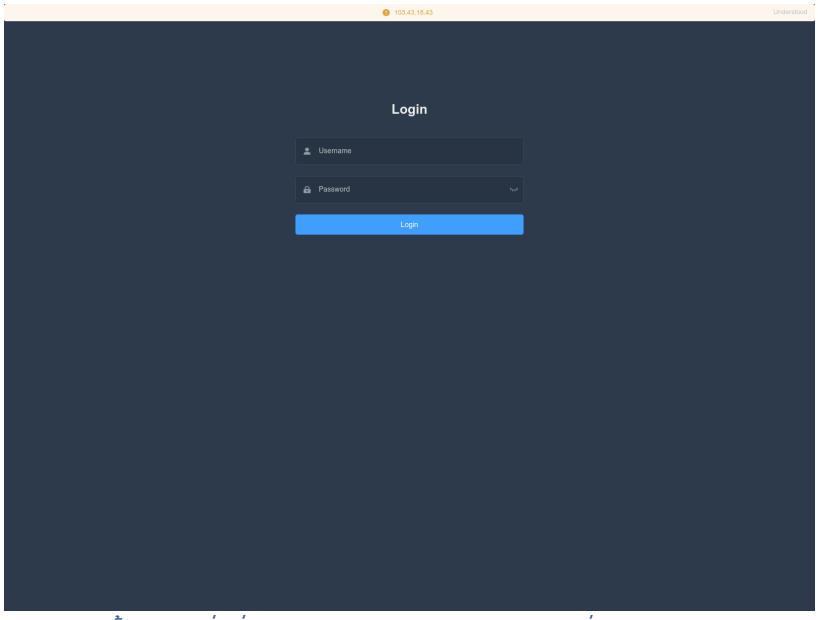
ໂດເມນເຫຼົ່ານີ້ຖືກລະບຸໄວ້ໂດຍ Trend Micro ວ່າເປັນຊຸດຊ່ອງໂຫວ່ MOONSHINE, ເຊິ່ງຮັບຜິດຊອບໃນການສະແຫ່ວງຫາຜົນປະໂຫຍດຈາກຊ່ອງໂຫວ່ຂອງຕົວທ່ອງເວັບເພື່ອຕິດຕັ້ງມັນແວໃນອຸປະກອນມືຖື. Trend Micro ຕັ້ງຊື່ມັນແວນີ້ວ່າ 'Dark Nimbus'.

ເພື່ອຄວາມກະຈ່າງແຈ້ງ, ອິນເຕີເຟດການຈັດການ MOONSHINE ແມ່ນສິ່ງທີ່ຕົວຢ່າງຂອງມັນແວ MOONSHINE ໃຊ້ຕິດຕໍ່ສື່ສານກັບ ແລະ ຂໍ້ມູນຜູ້ຖືກເຄາະຮ້າຍຈະຖືກແຍກອອກໄປ. ຊຸດຊ່ອງໂຫວ່ MOONSHINE ທີ່ລາຍງານໂດຍ Trend Micro, ແມ່ນຄວາມສາມາດແຍກຕ່າງຫາກທີ່ໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫວ່ຂອງຕົວທ່ອງເວັບເພື່ອຕິດຕັ້ງມັນແວທີ່ເອີ້ນວ່າ Dark Nimbus ໃນອຸປະກອນມືຖື. ນອກຈາກນັ້ນ, Dark Nimbus ແລະ MOONSHINE ຍັງເປັນມັນແວທີ່ແຕກຕ່າງກັນທັງໝົດ.

ທັງອິນເຕີເຟດການຈັດການ MOONSHINE ແລະ ຊຸດການໂຈມຕີ MOONSHINE ນັ້ນມີລະຫັດທີ່ທັບຊ້ອນກັນ ດັ່ງນັ້ນຈຶ່ງມີຂໍ້ຄວາມແຈ້ງໃຫ້ເຂົ້າສູ່ລະບົບທີ່ຄ້າຍຄືກັນໃນຮູບທີ່ 3 ແລະ 5 ເຊັ່ນດຽວກັນກັບເນື້ອຫາຂອງໜ້າໃນຮູບທີ່ 4 ແລະ 6. ພວກເຂົາທັງສອງຍັງມີສະຕິງ 'webpackJsonpreact-scotchui' ໃນລະຫັດຕົ້ນສະບັບດ້ວຍ.

ຜູ້ກໍ່ໃຫ້ເກີດໄພຄຸກຄາມໄດ້ສ້າງລິ້ງ URL ທີ່ເຊື່ອມຕໍ່ກັບຊຸດການໂຈມຕີ MOONSHINE ແລະ ຫຼັງຈາກນັ້ນໄດ້ໂອນໄປຫາ ວິດີໂອທີ່ກ່ຽວຂ້ອງກັບຊາວທິເບດ ແລະ ຊາວອຸຍເກີ, ເຊິ່ງທັບຊ້ອນກັນກັບການກຳນົດເປົ້າໝາຍຂອງ MOONSHINE.

ທີ່ຢູ່ IP ຈຳນວນຫຼາຍທີ່ໂຮດໂດເມນຊຸດຊ່ອງໂຫວ່ MOONSHINE, ມີໜ້າເຂົ້າສູ່ລະບົບທີ່ມີຊື່ວ່າ 'VLiteUI' ຢູ່ໃນພອດ 444. ບໍ່ຄ່ອຍມີໃຜສັງເກດເຫັນໜ້ານີ້ ແລະ ການປະກົດຕົວຂອງໜ້ານີ້ຢູ່ໃນ IPs ເຫຼົ່ານີ້ຊີ້ໃຫ້ເຫັນເຖິງການເຊື່ອມຕໍ່ທີ່ເປັນໄປໄດ້ກັບການປະຕິບັດງານຂອງຜູ້ດຳເນີນການ.



ຮູບທີ່ 7: ແຜງການເຂົ້າສູ່ລະບົບທີ່ມີຊື່ HTML 'VLiteUI' ພົບເຫັນຢູ່ໃນ IPs ທີ່ໂຮດຊຸດຊ່ອງໂຫວ່ MOONSHIN.

ການວິເຄາະ Trend Micro ຂອງ Dark Nimbus ເປີດເຜີຍໃຫ້ເຫັນວ່າ ມັນແວສາມາດເກັບກຳຂໍ້ມູນທີ່ຄວບຄຸມໃນອຸປະກອນ ແລະ ສື່ສານກັບ C2 ໂດຍໃຊ້ອະນຸສັນຍາ XMPP.

Trend Micro ຍັງລະບຸວ່າໃນ Dark Nimbus ບາງເວີຊັນ, ພວກເຂົາໄດ້ກຳນົດຄວາມແຜ່ຫຼາຍຂອງສາຍ 'DKNS'.

‘ansec[.]com’ (ສະແດງລາຍຊື່ເປັນ Dark Nimbus C2 ໂດຍ TrendMicro)
ຍັງຖືກສັງເກດເຫັນໃນການບໍລິການ XMPP ສຳລັບທີ່ຢູ່ IP ອື່ນໆທີ່ໃຫ້ບໍລິການໜ້າເວັບທີ່ມີ DKNS ໃນຫົວຂໍ້:

- DKNS Android远程取证系统 (ລະບົບຟໍເຣນຊິກໄລຍະໄກ Android DKNS)
- DKNS云网侦控平台 (ແພລດຟອມການສືບສວນ ແລະການຄວບຄຸມເຄືອຂ່າຍຄລາວ DKNS)
- DKNS 云网侦控平台 (ແພລດຟອມການສືບສວນ ແລະການຄວບຄຸມເຄືອຂ່າຍຄລາວ DKNS)
- DKNS远程控制侦查系统 (DKNS ລະບົບການສືບສວນການຄວບຄຸມໄລຍະໄກ)

ຊຸດອື່ນຂອງທີ່ຢູ່ IP ກັບ**‘ansec[.]com’** ຢູ່ໃນບໍລິການ XMPP ມີໜ້າເວັບທີ່ມີຫົວຂໍ້:

- UPSEC互联网控制指挥系统 (UPSEC ລະບົບຄຳສັ່ງຄວບຄຸມອິນເຕີເນັດ)
- UPSEC无线侦控系统 (UPSEC ລະບົບເຝົ້າລະວັງ ແລະ ຄວບຄຸມໄຮ້ສາຍ)
- UPSEC重点人数据还原系统 (UPSEC ລະບົບການຟື້ນຟູຂໍ້ມູນບຸກຄົນທີ່ສຳຄັນ)

ອີງຕາມລາຍງານຂອງ Intelligence Online, ພົບວ່າ 'UPSEC' ທີ່ສັງເກດເຫັນໃນຫົວຂໍ້ຂອງໜ້າ HTML, ໝາຍເຖິງເຖິງ 'Sichuan Dianke Network Security Technology Co., Ltd'.

ກໍລະນີສຶກສາສອງ: BADBAZAAR

BADBAZAAR ເປັນມັນແວມືຖືທີ່ມີເວີຊັນ iOS ແລະ Android ທີ່ມຸ່ງເປົ້າໄປທີ່ຊາວອຸຍກູ, ຊາວທິເບດ ແລະ ຊາວໄຕ້ຫວັນ. ສະປາຍແວນີ້ແຜ່ຂະຫຍາຍຜ່ານແພຣດຟອມສື່ມວນຊົນສັງຄົມ ແລະ ຮ້ານ app stores. ການລາຍງານຫຼ້າສຸດຈາກ Volexity ສະແດງໃຫ້ເຫັນຄວາມແຕກຕ່າງຂອງ BADBAZAAR ຫຼາຍລຸ້ນ, ເຊິ່ງແຍກອອກເປັນ BadSolar, BADBAZAAR ແລະ BadSignal. ທັງສາມຮູບແບບທີ່ເຊື່ອມຕໍ່ກັນໂດຍຟັງຊັນທີ່ທັບຊ້ອນກັນທີ່ໃຊ້ໃນການເກັບກຳຂໍ້ມູນໃນອຸປະກອນ ແລະ ຜູ້ປະຕິບັດການ.

ການຄົ້ນຄວ້າ NCSC ກ່ຽວກັບ BADBAZAAR ເປີດເຜີຍສິ່ງຕໍ່ໄປນີ້:

- ການຈັດກຸ່ມໂດເມນ C2 ເປີດເຜີຍໃຫ້ເຫັນລິ້ງເພີ່ມເຕີມໄປຍັງໂດເມນທີ່ລາຍງານໃນຂໍ້ມູນໄພຂົ່ມຂູ່ທາງປະຫວັດສາດ.
- ເຊີບເວີ C2 ແລະ ຕົວຢ່າງມັນແວເປີດເຜີຍຊື່ໂຮດທີ່ກ່ຽວຂ້ອງກັບໂຄງສ້າງພື້ນຖານຂອງຕົວກຳນົດການ.
- ໂປຼໄຟລ໌ເພີ່ມເຕີມທີ່ກໍ່ໃຫ້ເກີດໄພຄຸກຄາມໃຊ້ສຳລັບວິສະວະກຳສັງຄົມເພື່ອແຜ່ກະຈາຍມັນແວອອກໄປນອກຮ້ານຄ້າແອັບຢ່າງເປັນທາງການ.

ການຈັດກຸ່ມ WHOIS / ນາຍໜ້າໂດເມນ

'UJYJYUJ'

ການວິເຄາະບັນທຶກ WHOIS ສຳລັບໂດເມນ BADBAZAAR **'signalplus[.]org'** (ລາຍງານໂດຍ ESET) ສະແດງຄ່າ **'UJYJYUJ'** ໃນຊ່ອງຂໍ້ມູນ **'State'**.

ການຄົ້ນຫາໂດເມນອື່ນໆທີ່ມີຄ່າດຽວກັນຈະເປີດເຜີຍໂດເມນທີ່ມີຄວາມສົນໃຈຕໍ່ໄປນີ້:

- thetubeplus[.]com
- tubevideoplus[.]org
- pmumail[.]com
- signalplus[.]org

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບທີ່ 1)

ໂດເມນ **signalplus[.]org, tubevideoplus[.]org** ແລະ **thetubeplus[.]com** ໄດ້ຮັບການລາຍງານວ່າເປັນໂດເມນ BADBAZAAR C2, ໃນຂະນະທີ່ ESET ລາຍງານໂດເມນຍ່ອຍ **mail.pmumail[.]com** ເປັນເຊີບເວີພຣັອກຊີ FlyGram. FlyGram ແມ່ນແອັບ BADBAZAAR ທີ່ໄດ້ຮັບການພັດທະນາໂດຍຜູ້ບໍ່ຫວັງດີທາງໄຊເບີ (ເບິ່ງລາຍຊື່ແອັບ BADBAZAAR ອື່ນໆໃນພາກບວກ).

ຄ່າການຍ່າງຂອງແປ້ນພິມ

NCSC ຍັງພົບຮູບແບບການຍ່າງແປ້ນພິມທີ່ຄ້າຍຄືກັນຢູ່ໃນໂດເມນ BADBAZAAR C2 ທີ່ລົງທະບຽນອື່ນດ້ວຍ.

ຕົວຢ່າງ, ໂດເມນຕໍ່ໄປນີ້ທັງໝົດມີມູນຄ່າ **'REWR'** ຕາມທີ່ສັງເກດເຫັນຢູ່ໃນພາກສະໜາມ **'State'** (ຕາມທີ່ໃຊ້ໃນກ່ອນໜ້ານີ້):

- yumoftion[.]com
- fvbyavgyea[.]com
- jkiohreh[.]com
- pmstwocqn[.]com

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບທີ່ 2)

ໂດເມນທີ່ມີສະຖານະ 'FSDF'

ໂດເມນ BADBAZAAR C2 ອີດຊຸດໜຶ່ງມີມູນຄ່າ **‘State’** ແມ່ນ **'FSDF':**

- tryhrwserf[.]com
- tibetone[.]org
- comeflxyr[.]com

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 3)

ການລາຍງານປະຫວັດສາດດ້ວຍຄ່າການຍ່າງແປ້ນພິມ

ການໃຊ້ຄ່າການຍ່າງແປ້ນພິມໃນບັນທຶກ WHOIS ຂອງໂດເມນ BADBAZAAR ຍັງສາມາດເຫັນໄດ້ຢູ່ໃນການກຳນົດເປົ້າໝາຍຂອງອົງກອນທິເບດທີ່ມີລາຍງານໄວ້ໃນອາດີດໂດຍ TA413. ອະນາຄົດທີ່ບັນທຶກໄວ້ ໄດ້ສັງເກດເຫັນໂດເມນທີ່ຄວບຄຸມໂດຍຜູ້ກະທຳທີ່ຫຼອກລວງອົງກອນຂອງຊາວທິເບດ ແລະ ການໃຊ້ມູນຄ່າຂອງອົງກອນທີ່ຈົດທະບຽນເປັນ **“asfasf”.**

clublogs[.]com

ຕົວຢ່າງ BADBAZAAR ທີ່ໄດ້ຮັບຈາກ Lookout ມີ **‘xle.clublogs[.]com’** ເປັນໂດເມນ C2. ໂດເມນຮາກ **‘clublogs[.]com’** ຖືກໂຮດໃນທີ່ຢູ່ IP **‘95.179.210[.]85’** ແລະ ມີໃບຢັ້ງຢືນ SSL ທີ່ມີຫົວຂໍ້ ແລະ ຄ່າຜູ້ຈັດທຳເປັນ **‘CN=WIN-50QO3EIRQVP’**. ຄ່ານີ້ກົງກັບໃບຢັ້ງຢືນ SSL ທີ່ພົບໃນຕົວຢ່າງ BADBAZAAR ເຊິ່ງໃຊ້ການປັກໝຸດ SSL ເພື່ອຫຼີກເວັ້ນການຂັດຂວາງການສື່ສານ.

ປະຫວັດການໂຮດສຳລັບທີ່ຢູ່ IP **95.179.210[.]85** ສົ່ງຄືນໂດເມນທີ່ສົນໃຈຕໍ່ໄປນີ້:

- actuallys[.]com
- bre.myloughborough[.]com
- rewrwer[.]com
- www.voiceoftibet[.]net

- clublogs[.]com

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 4)

www.voiceoftibet[.]net

ໂດເມນ **‘www.voiceoftibet[.]net’** ເບິ່ງຄືຈະແອບອ້າງເປັນສະຖານີວິທະຍຸ 'ສຽງຂອງທິເບດ', ຄ້າຍຄືກັນກັບ TTP ທີ່ໃຊ້ໂດຍ TA413.

ໂດເມນ ‘**rewrwer[.]com’** ແມ່ນຄ້າຍຄືກັນກັບຄ່າ **‘State’** ທີ່ລະບຸໄວ້ກ່ອນໜ້ານີ້ **‘REWR’** ທີ່ພົບໃນບັນທຶກ WHOIS ຂອງໂດເມນ BADBAZAAR.

ໂດເມນ ‘**clublogs[.]com’**, **‘rewrwer[.]com’**, **‘voiceoftibet[.]net’** ແລະ **‘myloughborough[.]com’** ທັງໝົດໄດ້ຮັບການລົງທະບຽນດ້ວຍທີ່ຢູ່ອີເມວ **‘tplutalova@list[.]ru’**.

actuallys[.]com

ບັນທຶກ WHOIS ສຳລັບ ‘**actuallys[.]com’** ສະແດງໃຫ້ເຫັນຕົວຢ່າງທີ່ຢູ່ອີເມວດ້ານເຕັກໂນໂລຢີ ແລະ ຜູ້ເບິ່ງແຍງລະບົບ **‘tplutalova@list[.]ru’** ແຕ່ທີ່ຢູ່ອີເມວຜູ້ລົງທະບຽນແມ່ນ **‘ivan_s81@mail[.]ru’**.

ຂໍ້ມູນ WHOIS ໃນປະຫວັດສາດສຳລັບໂດເມນ **‘actuallys[.]com’** ເປີດເຜີຍອີເມວລົງທະບຽນ **‘wangminghua6@gmail[.]com’** ທີ່ລະບຸໃນວັນທີ 24 ກຸມພາ 2016. ໃນວັນທີ 11 ມີນາ 2016, ອີເມວດັ່ງກ່າວໄດ້ຖືກປ່ຽນແປງເປັນ **‘ivan_s81@mail.ru’** ເຖິງແມ່ນວ່າວັນທີໝົດອາຍຸການລົງທະບຽນຂອງ ຜູ້ໃຫ້ບໍລິການລົງທະບຽນຈະຍັງຄົງຢູ່ຄືເກົ່າ.

wangminghua6@gmail[.]com

ທີ່ຢູ່ອີເມວ **‘wangminghua6@gmail[.]com’** ຖືກນຳໃຊ້ເພື່ອລົງທະບຽນໂດເມນທີ່ພົບເຫັນຢູ່ໃນການລາຍງານ ຂ່າວລັບໄພຂົ່ມຂູ່ໃນອາດີດ. ໃນປີ 2015, Palo Alto ໄດ້ລະບຸອີເມວທີ່ໃຊ້ເພື່ອລົງທະບຽນໂດເມນ C2 ສຳລັບມັນແວ, Cmstar. ໃນປີ 2014, ຍັງຖືກໃຊ້ເພື່ອລົງທະບຽນໂດເມນທີ່ລະບຸໂດຍ Mandiant ໃນແຄມເປນຟິດຊິງທີ່ດຳເນີນໂດຍ APT3. ໃນປີ 2013, ມີການໃຊ້ເພື່ອລົງທະບຽນໂດເມນທີ່ພົບເຫັນໂດຍ CrowdStrike ໃນຂອບມັນແວທີ່ມີເສັ້ນທາງ ຖານຂໍ້ມູນໂປຣແກຣມ (PDB) ທີ່ມີຕົວອັກສອນຈີນ. ນີ້ຊີ້ໃຫ້ເຫັນເຖິງການລວບລວມຂໍ້ມູນຢູ່ໃນລະບົບພາສາຈີນ.

taoyujun@gmail[.]com

ໂດເມນ ‘**hcjbtt[.]com’** ໄດ້ລົງທະບຽນດ້ວຍທີ່ຢູ່ອີເມວ **‘taoyujun@gmail[.]com’** ແຕ່ອີເມວຜູ້ເບິ່ງແຍງລະບົບໄດ້ລົງທະບຽນກັບ **‘wangminghua6@gmail[.]com’**.

ບໍ່ມີກິດຈະກຳທີ່ເປັນອັນຕະລາຍທີ່ເຊື່ອມຕໍ່ກັບໂດເມນ **‘hcjbtt[.]com’**, ຢ່າງໃດກໍຕາມ, ທີ່ຢູ່ອີເມວ **‘taoyujun@gmail[.]com’** ໃນບົດລາຍງານຂ່າວດ້ານໄພຂົ່ມຂູ່ໃນອາດີດ. ໃນປີ 2014, ໄດ້ມີການນຳມາໃຊ້

ເພື່ອລົງທະບຽນໂດເມນທີ່ພົບໂດຍ Mandiant ໃນຕົວຢ່າງ '**Cueisfry Trojan**' ທີ່ໃຊ້ໃນການກຳໜົດເປົ້າໝາຍ ອົງກອນຂອງຍີ່ປຸ່ນ.

ທີ່ຢູ່ອີເມວດັ່ງກ່າວຍັງໄດ້ຈົດທະບຽນໂດເມນຕ່າງໆເຊັ່ນ '**iaea-international[.]org**' ເຊິ່ງແອບອ້າງວ່າເປັນ **ສຳນັກງານພະລັງງານປະລະມານູສາກົນ** ແລະ **'idc-ctbto[.]org'** ເຊິ່ງແອບອ້າງເປັນ **ສູນຂໍ້ມູນລະຫວ່າງປະເທດ** ທີ່ **ອົງກອນສົນທິສັນຍາຫ້າມທົດລອງອາວຸດນິວເຄຣຍໂດຍສົມບູນ (CTBTO)**.

ບັນທຶກ Whois ກ່ອນໜ້ານີ້ສຳລັບໂດເມນ '**iaea-international[.]org**' ສະແດງໃຫ້ເຫັນອີເມວຜູ້ລົງທະບຽນເປັນ '**wangminghua6@gmail[.]com**'.

udtglobals[.]com

ພົບໂດເມນ '**udtglobals[.]com**' ໂດຍໃຊ້ '**wangminghua6@gmail[.]com**' ເປັນອີເມວຜູ້ເບິ່ງແຍງລະບົບ ແລະ '**ocean.nio@rediffmail[.]com**' ເປັນທີ່ຢູ່ອີເມວຂອງຜູ້ລົງທະບຽນ. ບັນທຶກ WHOIS ອື່ນໆສຳລັບໂດເມນ ນີ້, ສະແດງໃຫ້ເຫັນອີເມວຜູ້ລົງທະບຽນດຽວກັນແຕ່ກັບທີ່ຢ่ູອີເມວຂອງຜູ້ເບິ່ງແຍງລະບົບແມ່ນ '**taoyujun@gmail[.]com**'

'udtglobals[.]com' ເບິ່ງຄືຈະແອບອ້າງ '**UDT Global**' ເຊິ່ງເປັນງານລະດັບໂລກສຳລັບບໍລິສັດດ້ານການປ້ອງກັນ ແລະ ຄວາມປອດໄພໃຕ້ທະເລ. ຊື່ຜູ້ໃຊ້ '**ocean.nio**' ໃນທີ່ຢູ່ອີເມວສາມາດຮຽນແບບ**ສະຖາບັນມະຫາສະໝຸດແຫ່ງຊາດ (NIO)** ທີ່ມີຢູ່ໃນຫຼາຍປະເທດ. ເຖິງແມ່ນວ່າການໃຊ້ບໍລິການອີເມວ '**Rediff**' (ເຊິ່ງມີຖານຢູ່ໃນອິນເດຍ) ອາດເຮັດໃຫ້ການລອກແບບ ຂອງ **ສະຖາບັນມະຫາສະໝຸດແຫ່ງຊາດຂອງອິນເດຍ.**

Djibdiplomatie[.]com

ໂດເມນ '**djibdiplomatie[.]com**' ເບິ່ງຄືວ່າຈະປອມແປງບໍລິການດ້ານການທູດຂອງຈິບູຕີ, ເຊິ່ງມີບັນທຶກ WHOIS ທີ່ຄ້າຍຄືກັນກັບ '**utdglobals[.]com'.** ມີບັນທຶກໜຶ່ງທີ່ສະແດງໃຫ້ເຫັນວ່າຜູ້ລົງທະບຽນແມ່ນ '**ocean.nio@rediffmail[.]com**' ແລະ ຜູ້ເບິ່ງແຍງລະບົບ '**taoyujun@gmail[.]com**' ໃນຂະນະທີ່ບັນທຶກອື່ນໆສະແດງໃຫ້ເຫັນວ່າ '**wangminghua6@gmail[.]com**' ເປັນທີ່ຢູ່ອີເມວຂອງຜູ້ເບິ່ງແຍງລະບົບ ແລະ '**ocean.nio@rediffmail[.]com**' ເປັນອີເມວຂອງຜູ້ລົງທະບຽນ.

ໂດເມນທັງສອງເຫຼົ່ານີ້ຍັງມີຄ່າປະເພດການຍ່າງແປ້ນພິມຢູ່ໃນບັນທຶກ WHOIS ອີກດ້ວຍ. ຕົວຢ່າງ, '**udtglobals[.]com**' ມີມູນຄ່າ '**ASDF**' ເປັນເມືองທີ่ลົงทะบรม ແລะ '**djibdiplomatie[.]com**' ມີຄ່າ '**DAF DAGF**' ເປັນມູນຄ່າຊື່ການລົງທະບຽນ. ຄ່ານີ້ແມ່ນປຽບທຽບໄດ້ກັບຄ່າທີ່ສັງເກດເຫັນໃນໂດເມນ BADBAZAAR ອື່ນໆ.

ເຖິງແມ່ນວ່າຈະພົບທີ່ຢ่ູອີเมว '**wangminghua6@gmail[.]com**' ແລະ '**taoyujun@gmail[.]com**' ໃນບັນທຶກ WHOIS ສຳລັບໂດເມນທີ่แอบอ้างเป็น**ภิดจะกำป้องกันใต้น้ำละดับโลก, บໍลิการการทูดจิบูติ** ແລะ **สำนักงานพะลังงานปะละมานูสาก็น**, ແต่ที่ยู่อีเมวเฟ่านี้ยังยู่ในบันทึก WHOIS สำลับโดเมนที่บ่เป็นอันตะลาย จำนวนหลายอีกด้วย.

ການປະສົມຂອງໂດເມນທີ່ປອມຕົວ ແລະ ໂດເມນທີ່ບໍ່ເປັນອັນຕະລາຍສາມາດຊີ້ໃຫ້ເຫັນເຖິງການມີຢູ່ຂອງໜ່ວຍງານຈັດຊື້ ໂຄງສ້າງພື້ນຖານທີ່ໃຊ້ເພື່ອສະໜັບສະໜູນການດຳເນີນງານຂອງຜູ້ກະທຳທີ່ເປັນອັນຕະລາຍທາງໄຊເບີ.

ທີ່ຢູ່ອີເມວ '**ocean.nio@rediffmail[.]com**' ແມ່ນພົບເຫັນຢູ່ໃນໂດເມນ ທີ່ແອບອ້າງຕາມທີ່ອະທິບາຍຂ້າງເທິງ ເທົ່ານັ້ນ. '**ivan_s81@mail[.]ru**' ແລະ '**tplutalova@list[.]ru**' ໄດ້ລົງທະບຽນໂດເມນຈຳນວນໜ້ອຍຫຼາຍ ຕາມລຳດັບ ແລະ ບາງໂດເມນບາງສ່ວນເຫຼົ່ານີ້ຖືກໂຮດຢູ່ໃນໂຄງສ້າງພື້ນຖານຂອງ BADBAZAAR. ທີ່ຢູ່ອີເມວທັງສາມນີ້ຖືກ ເຊື່ອວ່າຈະເຊື່ອມຕໍ່ຢ່າງໃກ້ຊິດກັບການປະຕິບັດງານຂອງຜູ້ກໍ່ອາຊະຍະກຳທາງໄຊເບີ. ເນື່ອງຈາກຈຳນວນໂດເມນທີ່ເຊື່ອມໂຍງ ກັບກິດຈະກຳທີ່ເປັນອັນຕະລາຍ, ຫຼາຍກວ່າອີເມວ '**wangminghua6@gmail[.]com**' ແລະ '**taoyujun@gmail[.]com**'.

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 5)

ລິ້ງໄປຍັງຜູ້ກໍ່ໄພຂົ່ມຂູ່ອື່ນໆ

ລັກສະນະທົ່ວໄປອີກປະການໜຶ່ງຂອງໂດເມນທີ່ເຊື່ອມໂຍງ BADBAZAAR '**actuallys[.]com**', '**clublogs[.]com**', '**myloughborough[.]com**', '**rewrwer[.]com**', ແລະ '**voiceoftibet[.]net**' ແມ່ນວ່າພວກເຂົາທັງໝົດໄດ້ລົງທະບຽນກັບ eNom ແລະ 'ຈອດ' ຢູ່ທີ່ '**255.255.255[.]254**'.

ຫຼັງຈາກການກວດສອບຂອງ NCSC ທີ່ຜ່ານມາ, ໂດເມນທີ່ມີລັກສະນະເຫຼົ່ານີ້ໄດ້ເປີດເຜີຍກິດຈະກຳທີ່ເຊື່ອມຕໍ່ກັບ **APT5** ໃນປີ 2019, ແລະ **APT14** ລະຫວ່າງ 2009 ແລະ 2011.

ໂດເມນທີ່ເຊື່ອມຕໍ່ APT5- ມີບັນທຶກ WHOIS ມີອາດີດເຊິ່ງລະບຸວ່າ '**taoyujun@gmail[.]com**' ເປັນທີ່ຢູ່ອີເມວຂອງຜູ້ລົງທະບຽນ.

ໂດເມນທີ່ເຊື່ອມໂຍງ APT14 ມີໂດເມນຍ່ອຍສາມຕົວອັກສອນທີ່ປາກົດວ່າເປັນຕົວແທນເປົ້າໝາຍຂອງການປະຕິບັດງານ ທີ່ເປັນອັນຕະລາຍຂອງພວກເຂົາ. ຕົວຢ່າງນີ້ແມ່ນ '**bae.cisconline[.]net**', ເຊິ່ງແນະນຳການຕັ້ງເປົ້າໝາຍຂອງລະບົບ BAE ແລະພົບເຫັນຢູ່ໃນຕົວຢ່າງ '**Poison Ivy**'.

ລັກສະນະທີ່ຄ້າຍຄືກັນແມ່ນສັງເກດເຫັນຢູ່ໃນໂດເມນ BADBAZAAR ໂດເມນຍ່ອຍກ່ຽວຂ້ອງກັບຊື່ຂອງແອັບທີ່ຖືກໂຈມ:

ຫົວຂໍ້ການສະໝັກ	C2 URL
1ຊາວມຸດສະລິມ	**mpp**.pmstwocqn[.]com
Video Player ສຳລັບ Android	**vpf**.titeperformance[.]com
Batter Master	**bat**.androidupdated[.]net
ວິທະຍຸອາຟການິສຖານ	**afg**.collinformations[.]com

EN-UG Dictionary Free	**eud**.titeperformance[.]com
ການກູ້ຄືນວິດີໂອໃນດິສ	**dvr**.collinformations[.]com
ຂຽນຂໍ້ຄວາມຕອນນີ້	**ttn**.titeperformance[.]com

ມັນເປັນສິ່ງສໍາຄັນທີ່ຈະສັງເກດວ່າກິດຈະກໍາທີ່ກ່ຽວຂ້ອງກັບ APT5 ແລະ APT14 ແມ່ນປະຫວັດສາດ ແລະ ຍັງມີໂດເມນອື່ນໆທີ່ລົງທະບຽນກັບ eNom ແລະ ຖືກແກ້ໄຂເປັນ '**255.255.255.254**' ເຊິ່ງບໍ່ສາມາດເຊື່ອມໂຍງກັບກິດຈະກໍາທີ່ເປັນອັນຕະລາຍໄດ້. ສະນັ້ນມັນບໍ່ແນ່ໃຈວ່າຜູ້ດໍາເນີນການຢູ່ເບື້ອງຫຼັງແຄມເປນເຫຼົ່ານີ້ແມ່ນຄືກັນ ຫຼື ມີຄວາມກ່ຽວຂ້ອງກັບ.

ຊື່ເຄື່ອງຈັກ

ການວິເຄາະ BADBAZAAR C2s ແລະ ຕົວຢ່າງໄດ້ເປີດເຜີຍໃຫ້ເຫັນຊື່ໂຮດທີ່ໃຊ້ເປັນຄ່າ 'ຊື່ທົ່ວໄປ' ໃນໃບຢັ້ງຢືນ SSL. ການສືບສວນຂອງ NCSC ກ່ຽວກັບໃນຊື່ໂຮດທີ່ສັງເກດເຫັນຢູ່ໃນຕົວຢ່າງ ແລະ ໂຄງສ້າງພື້ນຖານຂອງ BADBAZAAR ໄດ້ສະແດງໃຫ້ເຫັນວ່າຊື່ໂຮດເຫຼົ່ານີ້ຖືກນໍາໃຊ້ໃນທີ່ຢູ່ IP ຫຼາຍລາຍການ. ທີ່ຢູ່ IP ເຫຼົ່ານີ້ແມ່ນໂຮດໂດເມນທີ່ພົບເຫັນຢູ່ໃນຕົວຢ່າງ BADBAZAAR. ມີລາຍລະອຽດເພີ່ມເຕີມໃນສ່ວນຂ້າງລຸ່ມນີ້ກ່ຽວກັບຊື່ໂຮດ ແລະທີ່ຢູ່ IP ພ້ອມດ້ວຍຊື່ໂຮດທີ່ໂຮດຢູ່ໃນໂດເມນ BADBAZAAR C2.

ໃນເກືອບທຸກກໍລະນີ, ການມີຢູ່ຂອງໃບຢັ້ງຢືນທີ່ມີຄ່າຊື່ໂຮດຈະທັບຊ້ອນກັນກັບການແກ້ໄຂ IP ສໍາລັບຊື່ໂດເມນທີ່ເປັນອັນຕະລາຍທີ່ລະບຸໄວ້, ໂດຍມີບາງກໍລະນີທີ່ບໍ່ເປັນເຊັ່ນນັ້ນ.

WIN-EU0VLBL7TUJ

ພົບຊື່ໂຮດ '**WIN-EU0VLBL7TUJ**' ໃນທີ່ຢູ່ IP ຕໍ່ໄປນີ້ທີ່ສົນໃຈ:

- '**116.203.53[.]21**' ໂຮດໂດເມນ BADBAZAAR C2 ໄດ້ແກ່ '**uyapkfinder[.]com**' ແລະ '**thewestuniverse[.]com**'.

- '**95.216.169[.]27**' ໂຮດໂດເມນ BADBAZAAR C2 '**adysfunction[.]com**' ແລະ ໂດເມນຍ່ອຍ '**download.apkbazar[.]biz**' ທີ່ສັງເກດເຫັນເປັນລິ້ງດາວໂຫຼດສໍາລັບຕົວຢ່າງ BADBAZAAR.

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບທີ່ 6)

WIN-70E59JVOB9G

ພົບຊື່ໂຮດ '**WIN-70E59JVOB9G**' ໃນທີ່ຢູ່ IP ຕໍ່ໄປນີ້ທີ່ສົນໃຈ:

- ‘**23.88.28[.]220**’ ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ໂດເມນຍ່ອຍ, **‘aua.rondwsign[.]com’, ‘nal.tokenmajorp[.]com’, ‘pep.rondwsign[.]com’ ‘doa.rondwsign[.]com’**, ແລະ **‘pls.rondwsign[.]com’.** ມີຊ່ວງເວລາສອງວັນລະຫວ່າງເວລາທີ່ກວດພົບໃບຢັ້ງຢືນຈາກເຄື່ອງຄັ້ງຫຼ້າສຸດ ແລະ ເມື່ອພົບໂດເມນທີ່ເປັນອັນຕະລາຍ ແລະ ແກ້ໄຂເປັນ IP ຄັ້ງທຳອິດ.

- ‘**23.88.28[.]221’** ໂຮດ BADBAZAAR ທີ່ເຊື່ອມຕໍ່ໂດເມນຍ່ອຍ ‘**bt.bhvghg[.]com**’.

- **‘23.88.28[.]222’** ໂຮດໂດເມນ BADBAZAAR C2 ‘**tubevideoplus[.]org’** ແລະ ‘**cde.mpoxcases[.]com**’.

- ‘**65.21.92[.]67’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 sub-domain **'bat.androidupdated[.]net'**. ນອກຈາກນີ້ຍັງໂຮດໂດເມນຍ່ອຍ ‘**bat.androidupdated[.]net’** ເຊິ່ງເປັນມັນແວ DoubleAgent C2.

- ‘**65.21.92[.]77’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ໂດເມນຍ່ອຍ ‘**wyo.titeperformance[.]com’, ‘big.collinformations[.]com’ ‘vpf.titeperformance[.]com’, ‘eud.titeperformance[.]com’** ແລະ **‘afg.collinformations[.]com’**

- ‘**65.108.192[.]134’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ແມ່ນ ‘**upd.whoscaller.net’**. ແລະ ‘**ggl.whoscaller[.]net’**.

- ‘**142.132.131[.]15’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ແມ່ນ ‘**bvn.lookincategory[.]com’** ແລະ ‘**edr.lookincategory[.]com’.** ມີຊ່ວງເວລາສິບເອັດວັນລະຫວ່າງເວລາທີ່ພົບໃບຢັ້ງຢືນທີ່ມີຊື່ເຄື່ອງຄັ້ງຫຼ້າສຸດ ແລະ ພົບໂດເມນທີ່ເປັນອັນຕະລາຍທີ່ຈະແກ້ໄຂ IP ຄັ້ງທຳອິດ.

- **‘142.132.131[.]20’** ໂຮດໂດເມນຍ່ອຍ ‘**son.onlinegamersgroup[.]com’** ແລະ ‘**system.onlinegamersgroup[.]com’**, ເຊື່ອວ່າເປັນ BADBAZAAR C2s ເນື່ອງຈາກຖືກໂຮດໃນຂະນະທີ່ກວດພົບໃບຢັ້ງຢືນ SSL ທີ່ກ່ຽວຂ້ອງຂອງ BADBAZAAR ຢູ່ໃນ IP.

- ‘**142.132.131[.]28’** ໂຮດໂດເມນ BADBAZAAR C2 ໂດເມນ ‘**goldplusapp[.]net’** ແລະ ໂດເມນຍ່ອຍ ‘**who.goldplusapp[.]net’** ແລະ ‘**cgf.goldplusapp[.]net’.**

- ‘**162.55.103[.]211’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ໄດ້ແກ່ ‘**oha.alpinemap[.]net’, ‘aru.alpinemap[.]net’, ‘aso.alpinemap[.]net’, ‘afr.alpinemap[.]net’**, ແລະ ‘**aar.alpinemap[.]net’**.

- ‘**162.55.103[.]212’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ໂດເມນຍ່ອຍ **‘pep.rondwsign[.]com’, ‘ckp.jkiohreh[.]com’, ‘aar.tokenmajorp[.]com’, ‘nal.tokenmajorp[.]com’, ‘pls.rondwsign[.]com’** ແລະ **‘aua.rondwsign[.]com’.**

- **‘195.154.47[.]99’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ແມ່ນ ‘**ggl.whoscaller[.]net’** ແລະ **‘upd.whoscaller.net’**. ມີຊ່ວງເວລາສາມວັນລະຫວ່າງເວລາທີ່ພົບໃບໃບຢັ້ງຢືນທີ່ມີຊື່ເຄື່ອງ ຄັ້ງທຳອິດ ແລະ ພົບໂດເມນທີ່ເປັນອັນຕະລາຍຄັ້ງສຸດທ້າຍທີ່ຈະແກ້ໄຂເປັນ IP.

- ‘**195.154.60[.]3’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ‘**upd.whoscaller[.]net’ ‘ggl.whoscaller[.]net’.**

- ‘**212.83.189[.]89’** ໂຮດໂດເມນຍ່ອຍ BADBAZAAR C2 ໄດ້ແກ່ ‘**wyo.titeperformance[.]com’, ‘eud.titeperformance[.]com’, ‘vpf.titeperformance[.]com**’ ແລະ ‘**afg.collinformations[.]com’.**

- ‘**212.129.21[.]168’** ໂຮດໂດເມນ BADBAZAAR C2, **‘fre.lookincategory[.]com’, ‘tgr.lookincategory[.]com’, ‘fgt.lookincategory[.]com’ ‘luj.lookincategory[.]com’** ແລະ **‘bvn.lookincategory[.]com’**

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 7)

WIN-50QO3EIRQVP

ພົບໂຮດ ‘**WIN-50QO3EIRQVP’** ໃນທີ່ຢູ່ IP ຕໍ່ໄປນີ້ທີ່ສົນໃຈ:

- ໂດເມນໂຮດ ‘**45.76.132[.]91’**, ‘**yumoftion[.]com’, ‘androidupdated[.]net’**. ໂດເມນທັງສອງເຊື່ອມໂຍງກັບ BADBAZAAR ເນື່ອງຈາກໂດເມນຍ່ອຍ **‘fow.yumoftion[.]com’** ແລະ ‘**bat.androidupdated[.]net’** ແມ່ນໂດເມນ BADBAZAAR C2. ນອກຈາກນັ້ນ, ໂດເມນຍ່ອຍ

‘**apps.androidupdated[.]net’** ยังเป็นโดเมน DoubleAgent C2. นอกจากนี้ยังโรดโดเมน ‘**pmstwocqn[.]com’**, ที่เชื่อมต่กับ BADBAZAAR ผ่านทางบันทึก WHOIS.

- ‘**95.179.210[.]85’** โรด ‘**clublogs[.]com**’, ในนั้น ‘**xle.clublogs[.]com’** เชิ่งเป็นโดเมน BADBAZAAR C2 และ ยังเป็นโรด BADBAZAAR โดเมนที่เชื่อมโยง **‘bre.myloughborough[.]com’, ‘img.rewrwer[.]com’, ‘www.voiceoftibet[.]net’** และ ‘**actuallys[.]com’**. อีกด้วย.

- ‘**199.247.21[.]34’** โรด ‘**titeperformance[.]com’**, และ ‘**collinformations[.]com’** เชิ่งโดเมนย่อยแม่นโดเมน BADBAZAAR C2.

- ‘**217.69.10[.]128’** โรดโดเมน BADBAZAAR C2 ‘**uyghurdict[.]com**’.

(เบิ่งเอกะสามช้อมท้าย ก, รูบ 8)

WMSvc-WIN-50QO3EIRQVP

พับชื่โรด ‘**WMSvc-WIN-50QO3EIRQVP’** ในที่ยู่ IP ต่ไปนี้ที่สัมใจ:

- ‘**78.46.185[.]251’** โรดโดเมน BADBAZAAR C2 โดเมน ‘**groupgram[.]org’**, ลายงามโดย Volexity ที่จะใช้พอด 4432 สำลับภามเชื่อมต่ที่เป็นอันตะลาย.

- ‘**65.21.92[.]69’** และ ‘**163.172.205[.]207**’ โรดโดเมน ‘**widelygram[.]org’** เชิ่งเชื่อว่าเป็นโดเมน BADBAZAAR C2, เมื่องจากในขะนะที่โรสยู่ใน IP ทังสอง, พอด 4432 ยังถ์งเปิดยู่.

- ‘**163.172.198[.]206’** โรดโดเมน ‘**maxgram[.]org’** เชิ่งเชื่อว่าเป็นโดเมน BADBAZAAR C2, ในขะนะที่มันถืกโรดพอด 4432 จะเปิดยู่.

(เบิ่งเอกะสามช้อมท้าย ก, รูบ 9)

WMSvc-WIN-50QO3EIRQVP & WIN-7LSBB9R0F1L

ພົບຊື່ໂຮດ '**WMSvc-WIN-50QO3EIRQVP'** ແລະ '**WIN-7LSBB9R0F1L**' ໃນທີ່ຢູ່ IP ຕໍ່ໄປນີ້ພ້ອມໆກັນ:

- '**148.251.87[.]245'** ໂຮດໂດເມນ BADBAZAAR C2 '**flygram[.]org'** ແລະ '**groupgram[.]org**'.

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 10)

WIN-N8H8S9BG2P0
ພົບຊື່ໂຮດ '**WIN-N8H8S9BG2P0'** ໃນທີ່ຢູ່ IP ຕໍ່ໄປນີ້:

- '**148.251.87[.]247'** ໂຮດໂດເມນ BADBAZAAR C2 '**omarwhatsapp[.]org'** ແລະ '**flygram[.]org**'.

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 11)

WIN-I6VBN8MR92A
ພົບຊື່ໂຮດ '**WIN-I6VBN8MR92A'** ໃນທີ່ຢູ່ IP ຕໍ່ໄປນີ້:

- '**148.251.87[.]197'** ໂຮດໂດເມນ BADBAZAAR C2 '**tryhrwserf[.]com**'.

(ເບິ່ງເອກະສານຊ້ອນທ້າຍ ກ, ຮູບ 12)

ອີງຕາມຂໍ້ມູນທາງການຄ້າທີ່ມີຢູ່, ອັດຕາສ່ວນຂອງຊື່ເຄື່ອງຈັກເຫຼົ່ານີ້ໃນທົ່ວອິນເຕີເນັດແຕກຕ່າງກັນ. ມີການສັງເກດບາງສ່ວນພ້ອມໆກັນໃນຫຼາຍໆຢູ່ IP ຫຼາຍອັນທີ່ຊີ້ໃຫ້ເຫັນ VMs ກຳລັງຖືກສ້າງຂຶ້ນຈາກແມ່ແບບດຽວກັນ. ມັນເປັນສິ່ງສຳຄັນທີ່ຈະສັງເກດວ່າສຳລັບບາງຊື່ນັ້ນ, ບໍ່ແມ່ນທຸກ IP ທີ່ກວດພົບຈະເຊື່ອມຕໍ່ກັບກິດຈະກຳທີ່ເປັນອັນຕະລາຍ. ນີ້ອາດຈະໝາຍຄວາມວ່າການໃຊ້ຊື່ ບໍ່ໄດ້ຈຳກັດຢູ່ສະເພາະກັບຜູ້ກໍ່ໃຫ້ເກີດໄພຂົ່ມຂູ່ເຫຼົ່ານີ້.

ຢ່າງໃດກໍຕາມ, ການແຜ່ກະຈາຍຂອງຊື່ເຄື່ອງຈັກເຫຼົ່ານີ້ບາງຊື່ໃນ IPs ທີ່ມີການໂຮດໂດເມນ BADBAZAAR C2, ອາດບົ່ງບອກວ່າມີການໃຊ້ໂຄງສ້າງພື້ນຖານເພື່ອກຳນົດເຄື່ອງຈັກເພື່ອສະໜັບສະໜູນການດຳເນີນງານທາງໄຊເບີຂອງຜູ້ຖືກເຄາະຮ້າຍ.

ການປະກົດຕົວຂອງສື່ມວນຊົນສັງຄົມ

ການລາຍງານກ່ອນໜ້ານີ້ໂດຍ Volexity ສະແດງໃຫ້ເຫັນວ່າວິດີໂອ YouTube (ສົ່ງເສີມການນຳໃຊ້ແອັບພລິເຄຊັນທີ່ເປັນອັນຕະລາຍ) ໄດ້ຖືກສ້າງຂຶ້ນໂດຍຜູ້ກະທຳຄວາມຜິດທາງໄຊເບີ. ວິດີໂອເຫຼົ່ານີ້ປະກອບດ້ວຍບົດຊ່ວຍສອນກ່ຽວກັບວິທີການນຳໃຊ້ແອັບພລິເຄຊັ່ນທີ່ພັດທະນາຂຶ້ນ.

NCSC ໄດ້ຄົ້ນພົບຊ່ອງ YouTube ເພີ່ມເຕີມອີກສອງຊ່ອງທີ່ກ່ຽວຂ້ອງກັບການປະຕິບັດງານຂອງຜູ້ກໍ່ໄພຂົ່ມຂູ່. ຊ່ອງ YouTube ທີ່ມີ URL ວ່າ '**@josephjoey3499**' ເບິ່ງຄືວ່າຈະສົ່ງເສີມການໃຊ້ '**Maxgram**' ແລະ ຍັງມີ ຊ່ອງ ເພີ່ມເຕີມທີ່ລົງທະບຽນກັບ '**@uyghurapks3096**' ສົ່ງເສີມ '**Uyghur APK Finder**'.

ນອກຈາກນີ້, ວິດີໂອ YouTube ທີ່ສົ່ງເສີມ '**Flygram**' ແລະ '**Signal Plus**', ຍັງສະແດງໃຫ້ເຫັນຜູ້ຂົ່ມຂູ່ໂດຍໃຊ້ໝາຍເລກໂທລະສັບທີ່ເບິ່ງເຫັນໄດ້. ໃນວິດີໂອ '**Flygram**' ວິດີໂອ, ທີ່ເວລາ 0:36 ຈະເຫັນໝາຍເລກໂທລະສັບ '**+1 (570) 378-7250**' ແລະ ໃນລະຫວ່າງວິດີໂອ **'Signal Plus'** ວິດີໂອ, ຈະເຫັນໝາຍເລກໂທລະສັບ '**+1 (267) 298 4259**'.

Volexity ລາຍງານເວັບໄຊທ໌ຂ່າວປອມກ່ຽວກັບທິເບດ '**ignitetibet[.]net**', ເຊິ່ງພວກເຂົາຄົ້ນພົບໃນຊ່ອງ Telegram ທີ່ເຊື່ອວ່າເວັດໄຊດັ່ງກ່າວຖືກດຳເນີນການໂດຍຜູ້ກໍ່ໄພຂົ່ມຂູ່. ທີ່ຢູ່ອີເມວ **'choekyi.wangmo@ignitetibet[.]net'** ສະແດງຄວາມຄິດເຫັນໃນເພຈ **'tibetone.org'** ເຊິ່ງ Lookout ລາຍງານຕໍ່ສາທາລະນະວ່າເປັນເພຈ C2 ທີ່ໃຊ້ສຳລັບ ເວີຊັນ iOS BADBAZAAR.

ເຊື່ອກັນວ່າທີ່ຢູ່ອີເມວນີ້ຖືກຄວບຄຸມໂດຍນັກສະແດງ, ໂດຍໃຊ້ຕົວຕົນຂອງ '**Choekyi Wangmo**'.

ການປະເມີນ

BADBAZAAR ແລະ MOONSHINE ໃຊ້ວິທີການວິສະວະກຳສັງຄົມຈຳນວນໜຶ່ງເພື່ອກຳນົດເປົ້າໝາຍໄປທີ່ຊຸ່ມຊົນອຸຍກູ, ທິເບດ ແລະ ໄຕ້ຫວັນໂດຍສະເພາະ, ດັ່ງຕໍ່ໄປນີ້:

- ການໃຊ້ໂທຈັນໃນແອັບຕ່າງໆທີ່ມີຄວາມສົນໃຈກັບຊຸມຊົນເຫຼົ່ານີ້, ເຊັ່ນ ແອັບຄູຣານພາສາອຸຍກູ, ມີແນວໂນ້ມສູງວ່າຈະຖືກປັບແຕ່ງໃຫ້ເໝາະສົມກັບຖານຜູ້ເຄາະຮ້າຍເປົ້າໝາຍ.
- ການເພີ່ມແອັບໂທຈັນເຫຼົ່ານີ້ໄປຍັງຮ້ານຄ້າແອັບຢ່າງເປັນທາງການນັ້ນເປັນໄປໄດ້ສູງທີ່ຈະເຮັດໃຫ້ເກີດຄວາມສອບທຳ ແລະ ການແບ່ງປັນໃນກຸ່ມສົນທະນາແມ່ນມີຄວາມຕັ້ງໃຈສູງທີ່ຈະມີຈຸດປະສົງເພື່ອໃຊ້ປະໂຫຍດຈາກຄວາມສຳພັນທີ່ໄວ້ວາງໃຈໄດ້ພາຍໃນຊຸມຊົນເຫຼົ່ານີ້.

BADBAZAAR ແລະ MOONSHINE ເກັບກຳຂໍ້ມູນນີ້ເກືອບຈະແນ່ນອນວ່າຈະມີຄຸນຄ່າຕໍ່ລັດຖະບານຈີນ. ເຖິງແມ່ນວ່າ BADBAZAAR ແລະ MOONSHINE ຈະພົບ ກຳນົດເປົ້າໝາຍເປັນຊາວອຸຍເກີ, ທິເບດ ແລະ ໄຕ້ຫວັນ, ແຕ່ຍັງມີມັນແວ ອື່ນໆ ທີ່ກຳນົດເປົ້າໝາຍໃສ່ກຸ່ມຊົນເຜົ່າສ່ວນນ້ອຍອື່ນໆໃນປະເທດຈີນດ້ວຍ. ພົນລະເມືອງຈາກບັນດາປະເທດພັນທະມິດ, ທັງໃນຈີນ ແລະ ຕ່າງປະເທດ, ເຊິ່ງຖືກເບິ່ງວ່າສະໜັບສະໜູນສາເຫດທີ່ເປັນໄພຂົ່ມຂູ່ຕໍ່ຄວາມໝັ້ນຄົງຂອງລະບອບການປົກຄອງ, ເກືອບຈະແນ່ນອນວ່າຕົກຢູ່ພາຍໃຕ້ໄພຂົ່ມຂູ່ຈາກມັນແວມືຖືເຊັ່ນ BADBAZAAR ແລະ MOONSHINE. ຄວາມສາມາດໃນການເກັບກຳຂໍ້ມູນສະຖານທີ່, ສຽງ ແລະ ຮູບພາບຊ່ວຍໃຫ້ສາມາດແຈ້ງການດຳເນີນການເຝົ້າລະວັງ ແລະ ໄພຂົ່ມຂູ່ໃນອະນາຄົດໄດ້ຢ່າງແນ່ນອນໂດຍໃຫ້ຂໍ້ມູນໃນເວລາທີ່ແທ້ຈິງກ່ຽວກັບກິດຈະກຳຂອງເປົ້າໝາຍ.

MITRE ATT&CK®

ບົດລາຍງານນີ້ໄດ້ຖືກລວບລວມກ່ຽວກັບກອບຂອງ MITER ATT&CK®, ເຊິ່ງເປັນພື້ນຖານຄວາມຮູ້ທີ່ສາມາດເຂົ້າເຖິງໄດ້ທົ່ວໂລກກ່ຽວກັບກົນລະຍຸດ ແລະ ເຕັກນິກຂອງຝ່າຍກົງກັນຂ້າມທີ່ເຂົ້າເຖິງໄດ້ທົ່ວໂລກໂດຍອີງຈາກການສັງເກດການໃນໂລກແຫ່ງຄວາມເປັນຈິງ.

ຍຸດທະວິທີ	ບັດປະຈຳຕົວ	ເຕັກນິກ	ຂັ້ນຕອນ
ການລາດຕະເວນ	T1593.001	ຄົ້ນຫາເປີດເວັບໄຊທ໌/ໂດເມນທີ່ເປີດ: ສື່ມວນຊົນສັງຄົມ	ນັກສະແດງຊອກຫາກຸ່ມອອນລາຍ ແລະ ເວທີສົນທະນາທີ່ກົງກັບຜູ້ຖືກເຄາະຮ້າຍຂອງພວກເຂົາເພື່ອແບ່ງປັນມັນແວ
ການພັດທະນາຊັບພະຍາກອນ	T1583.001	ໄດ້ຮັບພື້ນຖານໂຄງລ່າງ: ໂດເມນ	ນັກສະແດງລົງທະບຽນໂດເມນສຳລັບຄຳສັ່ງ ແລະ ເຄື່ອງແມ່ຂ່າຍຄວບຄຸມຂອງພວກເຂົາ
ການພັດທະນາຊັບພະຍາກອນ	T1587.001	ພັດທະນາຄວາມສາມາດ: ມັນແວ	ລະຫັດທີ່ເປັນອັນຕະລາຍຖືກຂຽນໄວ້ເພື່ອແຊກເຂົ້າໃນແອັບທີ່ມີໂທຈັນ
ການພັດທະນາຊັບພະຍາກອນ	T1608.001	ຄວາມສາມາດໃນຂັ້ນຕອນ: ອັບໂຫຼດມັນແວ	ແອັບໂທຈັນຖືກອັບໂຫຼດໄປຍັງເວທີອອນລາຍ ລວມທັງຮ້ານຄ້າແອັບ
ການພັດທະນາຊັບພະຍາກອນ	T1585.001	ສ້າງຕັ້ງບັນຊີ: ບັນຊີສື່ມວນຊົນສັງຄົມ	ນັກສະແດງສ້າງບັນຊີຢູ່ໃນເວັບໄຊທ໌ ແລະ ສື່ສັງຄົມເພື່ອແບ່ງປັນ ແລະ ໂຄສະນາມັນແວ
ການພັດທະນາຊັບພະຍາກອນ	T1585.002	ສ້າງຕັ້ງບັນຊີ: ບັນຊີອີເມວ	ນັກສະແດງໃຊ້ບັນຊີອີເມວທີ່ເປັນໂຮດສ່ວນຕົວ ແລະ ການຄ້າສຳລັບການໂຮດ ແລະ ການແບ່ງປັນມັນແວ
ການເຂົ້າເຖິງເບື້ອງຕົ້ນ	T1189	ການປະນີປະນອມລະຫວ່າງຂັບລົດ	ສະຄຣິບທີ່ເປັນອັນຕະລາຍຖືກເຊື່ອງໄວ້ໃນແອັບທີ່ຖືກຕ້ອງຕາມກົດໝາຍ ແລະ ອັບໂຫຼດໄປຍັງຮ້ານຄ້າແອັບ
ການເຂົ້າເຖິງເບື້ອງຕົ້ນ	T1566.003	ຟິດຊິງ: ສະເປຍຟິດຊິງຜ່ານການບໍລິການ	ນັກສະແດງສົ່ງແອັບໂທຈັນໄປຍັງ ກັບກຸ່ມເປົ້າໝາຍໂດຍຜ່ານສື່ມວນຊົນສັງຄົມ ລວມທັງ Telegram
ການດຳເນີນການ	T1204.002	ການດຳເນີນການຜູ້ໃຊ້: ໄຟລ໌ທີ່ເປັນອັນຕະລາຍ	ຜູ້ຖືກເຄາະຮ້າຍຕ້ອງຕິດຕັ້ງແອັບທີ່ມີໂທຈັນ ເພື່ອດຳເນີນການໂຫຼດ
ການຫຼີກລ່ຽງການປ້ອງກັນ	T1027.009	ໄຟລ໌ ຫຼື ຂໍ້ມູນທີ່ສັບສົນ: ການໂຫຼດທີ່ຝັງຕົວ	ເພຍໂຫຼດທີ່ເປັນອັນຕະລາຍຖືກເຊື່ອງໄວ້ພາຍໃນແອັບທີ່ຖືກຕ້ອງຕາມກົດໝາຍ
ການຫຼີກລ່ຽງການປ້ອງກັນ	T1036.005	ການປອມແປງ: ກົງກັບຊື່ ຫຼື ສະຖານທີ່ທີ່ຖືກຕ້ອງ	ໄຟລ໌ໂທຈັນຈະກົງກັບຊື່, ຮູບລັກສະນະ ແລະ ຟັງຊັນຂອງແອັບທີ່ຖືກຕ້ອງຕາມກົດໝາຍ.
ການຫຼີກລ່ຽງການປ້ອງກັນ	T1656	ການປອມຕົວ	ນັກສະແດງປອມຕົວເປັນບຸກຄົນທີ່ເຊື່ອຖືໄດ້ ໂດຍການສ້າງເວັບໄຊທ໌ປົກປິດ ແລະ ນຳໃຊ້ຊື່ຜູ້ໃຊ້ທີ່ກ່ຽວຂ້ອງກັບກຸ່ມເປົ້າໝາຍ

ການລວບລວມ	T1123	ການຈັດສຽງ	ແອັບໂທຈັນອາດຈະຮ້ອງຂໍການອະນຸຍາດທີ່ບໍ່ຈຳເປັນລວມທັງການເຂົ້າເຖິງໄມໂຄຣໂຟນ
ການລວບລວມ	T1125	ການຈັບພາບວິດີໂອ	ແອັບທີ່ຖືກໂທຈັນອາດຈະຮ້ອງຂໍການອະນຸຍາດທີ່ບໍ່ຈຳເປັນລວມທັງການເຂົ້າເຖິງກ້ອງຖ່າຍຮູບ
ການລວບລວມ	T1005	ຂໍ້ມູນຈາກລະບົບທ້ອງຖິ່ນ	ແອັບທີ່ຖືກໂທຈັນອາດຈະຮ້ອງຂໍການອະນຸຍາດທີ່ບໍ່ຈຳເປັນລວມທັງໄຟລ໌ໃນເຄື່ອງດ້ວຍ.
ຄຳສັ່ງ ແລະ ການຄວບຄຸມ	T1071.001	ໂປຣໂຕຄອນຊັ້ນຂໍ້ມູນແອັບພລິເຄຊັນ: ໂປໂຕຄອນເວັບ	ມັນແວເຊື່ອມຕໍ່ກັບ C2 ໂດຍໃຊ້ HTTPS ແລະ WebSocket.
ຄຳສັ່ງ ແລະ ການຄວບຄຸມ	T1509	ພອດທີ່ບໍ່ໄດ້ມາດຕະຖານ	ໃຊ້ພອດທີ່ບໍ່ໄດ້ມາດຕະຖານເຊັ່ນ: ພອດ 4432 ແລະ 2333
ການກອງອອກ	T1041	ການກອງຜ່ານຊ່ອງ C2	ມັນແວລັກຂໍ້ມູນໂດຍໃຊ້ການເຊື່ອມຕໍ່ HTTPS ແລະ WebSocket.
ຜົນກະທົບ	T1565.002	ການຈັດການຂໍ້ມູນ: ການຈັດການຂໍ້ມູນທີ່ສົ່ງຜ່ານ	ຜູ້ດູແລຮັບຂໍ້ມູນຈາກຜູ້ຖືກເຄາະຮ້າຍໂດຍເປີດໃຊ້ງານການຮັບສົ່ງຂໍ້ມູນທາງເວັບຂອງແອັບທີ່ບໍ່ຈຳເປັນຕ້ອງການເຮັດວຽກຂອງແອັບ

ຕົວຊີ້ວັດ

MOONSHINE:

- ໃນວັນທີ 1 ເມສາ 2025, ການຄົ້ນຫາສໍາລັບແຜງ VLiteUI ສະແດງຜົນດັ່ງຕໍ່ໄປນີ້:

ທີ່ຢູ່ IP	ພອດ	ເຫັນຄັ້ງທໍາອິດ	ເຫັນຄັ້ງສຸດທ້າຍ
103.254.108[.]87	888	2024-10-17	2025-02-14
43.159.192[.]7	444	2024-11-21	2025-02-13
103.27.109[.]109	444	2024-07-11	2025-02-07
45.119.99[.]83	444	2024-12-26	2025-01-24
103.254.108[.]76	444	2024-09-12	2024-12-05
194.71.107[.]160	444	2023-12-10	2024-11-01
103.254.108[.]108	444	2023-11-12	2024-09-25
103.56.17[.]194	444	2024-04-03	2024-08-23
103.254.108[.]87	444	2023-11-14	2024-08-15
62.72.58[.]168	444	2024-01-29	2024-08-07
103.43.18[.]43	444	2024-02-12	2024-07-19
77.91.123[.]208	444	2024-02-04	2024-04-09
46.246.98[.]229	444	2024-03-07	2024-03-26
2.58.15[.]101	444	2024-02-23	2024-02-27
46.246.98[.]209	444	2024-01-08	2024-02-14
103.254.108[.]87	8000	2023-10-17	2023-10-17
103.254.108[.]87	8080	2023-04-15	2023-10-16
103.254.108[.]108	9090	2023-04-13	2023-10-16
103.45.66[.]123	9090	2023-03-02	2023-04-08
103.45.66[.]32	8080	2022-07-29	2023-04-06
27.124.20[.]23	9090	2022-05-28	2023-03-24
27.124.20[.]22	9090	2022-05-28	2023-03-23
27.124.20[.]24	9090	2022-05-27	2023-03-17
69.176.94[.]148	9090	2023-03-04	2023-03-10
69.176.94[.]228	9090	2022-12-24	2023-02-25
103.253.40[.]137	8000	2022-06-24	2022-09-02
27.124.4[.]80	8080	2022-02-25	2022-06-23
27.124.4[.]81	8080	2022-02-25	2022-06-23
47.242.46[.]79	8080	2021-05-03	2022-06-17
27.124.4[.]82	8080	2022-02-24	2022-06-15

27.124.4[.]165	9090	2022-05-14	2022-05-28
27.124.4[.]184	9090	2022-05-14	2022-05-27
27.124.4[.]178	9090	2022-05-13	2022-05-26
103.15.28[.]165	8080	2022-03-05	2022-05-25
69.176.94[.]226	8080	2022-03-05	2022-04-22
27.124.4[.]3	8080	2022-03-11	2022-04-02
103.140.238[.]235	8080	2022-03-04	2022-04-01
27.124.4[.]2	8080	2022-03-12	2022-04-01
165.84.180[.]107	8000	2022-02-25	2022-03-19
69.176.94[.]156	8000	2022-02-25	2022-03-05
141.98.212[.]70	9090	2021-10-05	2022-03-04
5.188.33[.]50	8000	2022-02-15	2022-03-04
5.188.70[.]193	8000	2022-02-15	2022-03-04
69.176.94[.]140	8080	2022-02-24	2022-02-24
27.124.20[.]83	8000	2022-02-14	2022-02-18
208.87.200[.]106	8000	2022-01-02	2022-01-02
121.127.241[.]37	8000	2021-12-08	2021-12-08
156.255.2[.]211	443	2021-10-05	2021-10-05
156.255.2[.]211	8000	2021-10-04	2021-10-04
156.255.2[.]203	8000	2021-10-03	2021-10-03
47.243.43[.]248	8000	2021-07-05	2021-07-05
45.115.236[.]6	8080	2021-05-03	2021-06-01
43.251.118[.]97	8000	2021-01-03	2021-03-01
185.243.43[.]138	8000	2021-01-04	2021-02-02
47.245.59[.]33	8000	2021-01-05	2021-01-05

- ໃນວັນທີ 1 ເດືອນເມສາປີ 2025, ການຊອກຫາແຜງ SCOTCH ADMIN ສະແດງຜົນດັ່ງຕໍ່ໄປນີ້:

ທີ່ຢູ່ IP	ພອດ	ເຫັນຄັ້ງທຳອິດ	ເຫັນຄັ້ງສຸດທ້າຍ
104.194.152[.]24	2333	2025-02-06	2025-02-27
172.86.80[.]126	2333	2025-02-07	2025-02-27
154.90.59[.]62	2333	2024-06-20	2024-09-20
154.90.59[.]88	2333	2024-06-21	2024-09-20
154.90.58[.]210	2333	2024-05-16	2024-06-14
154.90.59[.]225	2333	2024-05-17	2024-06-13
38.60.199[.]208	2333	2023-11-26	2024-01-09
38.60.199[.]254	2333	2023-11-28	2024-01-09

38.60.199[.]99	2333	2023-08-26	2023-11-21
38.60.199[.]44	2333	2023-07-20	2023-09-11
194.163.34[.]23	443	2022-09-30	2023-04-14
45.32.125[.]112	10443	2022-10-01	2023-03-17

- ໃນວັນທີ 14 ມີນາ 2024, ການຊອກຫາແຜງ SCOTCH ADMIN ສະເໝີອນໄດ້ສົ່ງຄືນສິ່ງຕໍ່ໄປນີ້:

ໂດເມນ	ທີ່ຢູ່ IP
vsa.ahamar[.]com	194.71.107[.]160
gates.chatonlineapp[.]com	172.67.208[.]167
www.onlineweixin[.]net	103.254.108[.]108
www.weetogether[.]top	103.254.108[.]108
www.onlinewxapp[.]net	103.43.18[.]43
www.unusualtransaction[.]com	2.58.15[.]101
m.leak-news[.]com	103.56.17[.]194
www.unusualtransaction[.]com	46.246.98[.]209
www.lodepot[.]com	62.72.58[.]168
www.online-wechat[.]com	103.254.108[.]87

BADBAZAAR:

ຄຳອະທິບາຍ	ພົບໃບຮັບຮອງ SSL ຢູ່ໃນ BADBAZAAR C2s.
MD5	ee6e0fc26e94e5b2e52d57ac035b36ff
SHA-1	10f8806c72bf5d56efa41c430e8692d55dd49674
SHA-256	1e72d5a908c6fcb4b59b65973ec8d4cf4c57b31e2b4973e72b8b85b4a6a0b9f7

- ໃນວັນທີ 1 ເດືອນເມສາປີ 2025, ການຄົ້ນຫາໃບຮັບຮອງ BADBAZAAR ຂ້າງເທິງສົ່ງຄືນດັ່ງຕໍ່ໄປນີ້:

ທີ່ຢູ່ IP	ພອດ	ເຫັນຄັ້ງທຳອິດ	ເຫັນຄັ້ງສຸດທ້າຍ
65.108.192[.]173	31237	2025-03-14	2025-03-28
65.108.192[.]173	31236	2025-03-14	2025-03-28
65.108.192[.]173	31235	2025-03-14	2025-03-28
157.90.129[.]73	31236	2025-03-27	2025-03-27
142.132.131[.]15	31236	2024-07-24	2025-03-27

142.132.131[.]15	31235	2024-07-26	2025-03-27
142.132.131[.]20	31237	2023-08-11	2025-03-27
142.132.131[.]15	31237	2024-07-24	2025-03-27
142.132.131[.]20	31236	2023-09-27	2025-03-26
142.132.131[.]20	31235	2023-10-18	2025-03-26
65.108.192[.]155	31236	2024-12-05	2025-02-20
65.108.192[.]155	31237	2024-12-05	2025-02-20
65.108.192[.]155	31235	2024-12-05	2025-02-19
23.88.28[.]222	31237	2024-04-25	2024-11-29
23.88.28[.]222	31235	2024-05-02	2024-11-28
23.88.28[.]222	31236	2024-05-01	2024-11-28
212.129.21[.]168	31235	2023-10-16	2024-03-17
212.129.21[.]168	31237	2023-08-24	2024-03-17
212.129.21[.]168	31236	2023-09-26	2024-03-14

ຄຳອະທິບາຍ	ພົບໃບຮັບຮອງ SSL ຢູ່ໃນ BADBAZAAR C2s
MD5	46923e10db90bde295960851245f199a
SHA-1	87a3d3f9bb6c78a5e71cfdf9975ca6a083dd5ebc
SHA-256	72e321bca1437eaf4a40b677cae5e09c5971fc3b972b11494712e62db3db1baa

- ໃນວັນທີ 1 ເດືອນເມສາປີ 2025, ການຄົ້ນຫາໃບຮັບຮອງ BADBAZAAR ຂ້າງເທິງສົ່ງຄືນດັ່ງຕໍ່ໄປນີ້:

ທີ່ຢູ່ IP	ພອດ	ເຫັນຄັ້ງທຳອິດ	ເຫັນຄັ້ງສຸດທ້າຍ
162.55.103[.]211	20122	2023-01-12	2025-03-28
162.55.103[.]212	20121	2022-06-30	2025-03-28
162.55.103[.]212	20122	2023-07-14	2025-03-28
162.55.103[.]211	20121	2022-06-03	2025-03-28
162.55.103[.]211	20123	2023-07-22	2025-03-27
162.55.103[.]212	20123	2023-07-22	2025-03-27
212.83.162[.]152	9090	2022-10-13	2025-03-27
23.88.28[.]221	20422	2023-07-28	2023-09-30
23.88.28[.]221	20421	2023-05-18	2023-09-28
23.88.28[.]221	20423	2023-07-28	2023-09-28
162.55.103[.]210	20121	2022-09-30	2023-02-23

65.21.92[.]67	20121	2021-11-02	2022-10-13
65.21.92[.]67	20122	2022-08-10	2022-10-13
23.88.28[.]220	20121	2021-12-08	2022-05-13
94.130.92[.]230	20121	2021-01-04	2021-10-05
88.99.150[.]246	20121	2021-04-06	2021-09-08
45.76.132[.]91	20121	2021-02-02	2021-03-01

- ໂດເມນ WHOIS

ຂ້າງລຸ່ມນີ້ແມ່ນຕາຕະລາງຂອງໂດເມນທີ່ບັນທຶກ WHOIS ໃນປັດຈະບັນ ຫຼື ໃນອາດີດທີ່ມີຄ່າທີ່ກົງກັບຄ່າທີ່ພົບໃນໂດເມນ BADBAZAAR C2.

ຄ່າ WHOIS	ໂດເມນ
ລັດຜູ້ລົງທະບຽນ: UJYJYUJ **ປະເທດທີ່ລົງທະບຽນ**: **Bolivia** **ຜູ້ຈົດທະບຽນ**: **eNom**	• ntc-mobile[.]com • microtik[.]net • ntc-ftth[.]net • axisupdating[.]com • axisupdate[.]com • telegramrouter[.]org • telegramtor[.]com • fufijxgkg[.]com • jindjjdtc[.]com • tubevideoplus[.]org • thetubeplus[.]com • tbgram[.]org • signalplus[.]org • pmumail[.]com
ລັດຜູ້ລົງທະບຽນ: **REWR** **ປະເທດທີ່ລົງທະບຽນ**: **CF** **ຜູ້ຈົດທະບຽນ**: **eNom**	• yumoftion[.]com • fvbyavgyea[.]com • jkiohreh[.]com • pmstwocqn[.]com • ofsggcccreq[.]com • verifyss[.]com • tooenabled[.]com • suguestions[.]com • searching2[.]com

ລັດຜູ້ລົງທະບຽນ: FSDF **ປະເທດທີ່ລົງທະບຽນ: AL** **ຜູ້ຈົດທະບຽນ: eNom**	• tryhrwserf[.]com • tibetone[.]org • comeflxyr[.]com • adoptewer[.]com • bhvghg[.]com • fgttgvh[.]com • in7n[.]com • o21q[.]com • ophgfhfgt7[.]com

ທີ່ຢູ່ອີເມວ
taoyujun@gmail.com
tplutalova@list.ru
wangminghua6@gmail.com
choekyi.wangmo@ignitetibet.net
ivan_s81@mail.ru
ocean.nio@rediffmail.com

ຊ່ອງ YouTube
https://www.youtube.com/@flygram1665
https://www.youtube.com/@bradshannon334
https://www.youtube.com/@uyghurapks3096
https://www.youtube.com/@josephjoey3499

ຕໍ່ໄປນີ້ແມ່ນເປັນລິ້ງໄປຍັງຕົວຊີ້ວັດອື່ນໆຂອງການປະນີປະນອມ (IoCs) ທີ່ກ່ຽວຂ້ອງກັບ BADBAZAAR ແລະ MOONSHINE. NCSCບໍ່ສາມາດຢືນຢັນຄວາມຖືກຕ້ອງຂອງຂໍ້ມູນທັງໝົດໃນລິ້ງເຫຼົ່ານີ້ໄດ້ ແລະ ຂໍແນະນຳໃຫ້ຜູ້ອ່ານກວດສອບຄວາມຖືກຕ້ອງ ແລະ ຄວາມກ່ຽວຂ້ອງດ້ວຍຕົນເອງ:

- ESET
- Trend Micro
- Lookout
- Lookout
- Volexity
- Citizen Lab

ການບັນເທົາຜົນກະທົບ

NCSC ຂໍແນະນຳໃຫ້ນຳຄຳແນະນຳຂ້າງລຸ່ມນີ້ມາໃຊ້ເພື່ອປ້ອງກັນໄພຂົ່ມຂູ່ຕາມທີ່ອະທິບາຍໄວ້ໃນກໍລະນີສຶກສາ.

- **ຜູ້ປະກອບການ App Store, ລວມທັງ App Store ບຸກຄົນທີສາມ ແລະ ຜູ້ພັດທະນາຄວນກວດສອບໃຫ້ແນ່ໃຈວ່າແອັບໃນແພລດຟອມນັ້ນປອດໄພ ແລະ ສອດຄ່ອງກັບຈັນຍາບັນປະຕິບັດຂອງລັດຖະບານ.**
  ບິ່ງຄຳແນະນຳ: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version

- **ຮອງຮັບຫຼາຍພາສາ:**
  ຜູ້ພັດທະນາແອັບຄວນລົງທຶນໃນຄວາມພະຍາຍາມເພື່ອຕັ້ງແອັບຍອດນິຍົມໃຫ້ເໝາະສົມກັບຜູ້ໃຊ້ທີ່ເວົ້າພາສາຊົນເຜົ່າກຸ່ມນ້ອຍໃນບັນດາກຸ່ມເປົ້າໝາຍເຊັ່ນ: ຊາວອຸຍກູ, ຊາວທິເບດ, ໄຕ້ຫວັນຮົກກຽ ແລະ ກວາງຕຸ້ງ.
  ຄຳແນະນຳຂອງ Apple ສຳລັບການແປເປັນພາສາຕັ້ງທ້ອງຖິ່ນໃນແອັບ: https://developer.apple.com/documentation/xcode/supporting-multiple-languages-in-your-app. ຄຳແນະນຳຂອງ Google ກ່ຽວກັບແອັບແປ: https://support.google.com/l10n/answer/6227218?hl=en&ref_topic=6307483&sjid=5961568056509626593-EU

- **ການຮັກສາຄວາມປອດໄພແພລະຕະຟອມສື່ສັງຄົມຂອງທ່ານ:**
  ບໍລິສັດສື່ມວນຊົນສັງຄົມສາມາດເຮັດໃຫ້ຜູ້ບໍ່ຫວັງດີທາງໄຊເບີສ້າງບັນຊີປອມ ແລະ ແບ່ງປັນໄຟລ໌ທີ່ເປັນ ຫຼື ລິ້ງທີ່ເປັນອັນຕະລາຍຢູ່ໃນເວທີຂອງຕົນໃນຊຸມຊົນອອນລາຍທີ່ຖືກຕ້ອງຕາມກົດໝາຍໄດ້ຢ່າງຍິ່ງຂຶ້ນ.
  ຖ້າເປັນໄປໄດ້, ບໍລິສັດຄວນແບ່ງປັນຕົວຊີ້ວັດອັນຕະລາຍກັບອຸດສາຫະກຳທີ່ກວ້າງຂວາງ ເພື່ອປັບປຸງຄວາມເຂົ້າໃຈຮ່ວມກັນກ່ຽວກັບໄພຂົ່ມຂູ່ ແລະ ເພື່ອຊ່ວຍເຫຼືອໃນມາດຕະການປ້ອງກັນ.

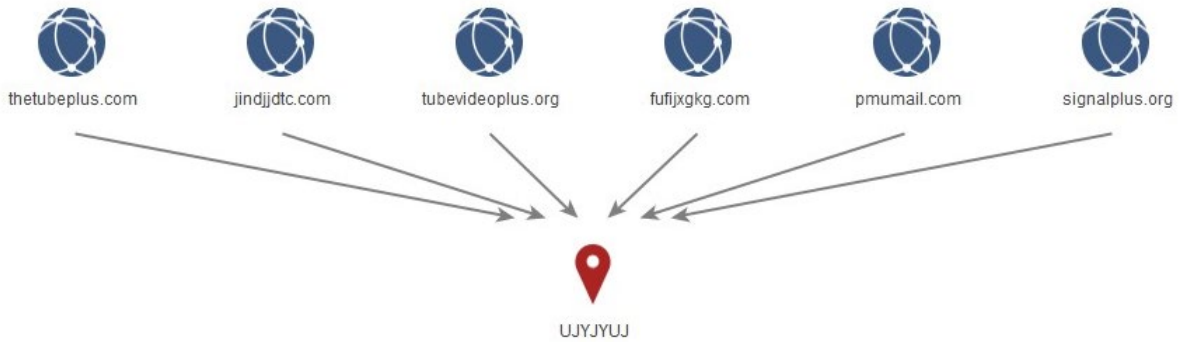
- **ແຜນການແກ້ໄຂສຳລັບລູກຄ້າ:**
  ອົງກອນຕ່າງໆຄວນມີຂັ້ນຕອນເພື່ອແຈ້ງໃຫ້ລູກຄ້າທີ່ຕິດຕັ້ງແອັບທີ່ເປັນອັນຕະລາຍໂດຍໃຊ້ບໍລິການຂອງຕົນ. ການແຈ້ງເຕືອນເຫຼົ່ານີ້ຄວນຈະເປັນການດຶງດູດຄວາມສົນໃຈ ແລະ ໃຫ້ຂໍ້ມູນ. ເມື່ອເໝາະສົມ, ກັບອົງກອນຕ່າງໆ ຄວນໃຫ້ຄຳແນະນຳກ່ຽວກັບວິທີການລຶບຊອບແວອອກ ແລະ ສະໜັບສະໜູນໃຫ້ຜູ້ເຄາະຮ້າຍລາຍງານຕໍ່ເຈົ້າໜ້າທີ່, ເຊັ່ນ: NCSC ໃນອັງກິດ.
  ເບິ່ງຈັນຍາບັນການປະຕິບັດຂອງ App Store ເພື່ອເບິ່ງຂໍ້ມູນເພີ່ມເຕີມ: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

- **ກຸ່ມເຮັດວຽກສຳລັບການຮ່ວມມື:** ບໍລິສັດສື່ມວນຊົນສັງຄົມສາມາດປະກອບເປັນກຸ່ມເຮັດວຽກ, ອະນຸຍາດໃຫ້ທີມງານຄວາມປອດໄພຂອງພວກເຂົາແບ່ງປັນຕົວຊີ້ວັດທີ່ເປັນອັນຕະລາຍ, TTPs ແລະ ການສັງເກດການ, ເຮັດໃຫ້ຜູ້ບໍ່ຫວັງດີໃຊ້ເວທີຂອງຕົນເພື່ອສະໜັບສະໜູນການໂຄສະນາທີ່ເປັນອັນຕະລາຍ ໄດ້ຍາກຂຶ້ນ.

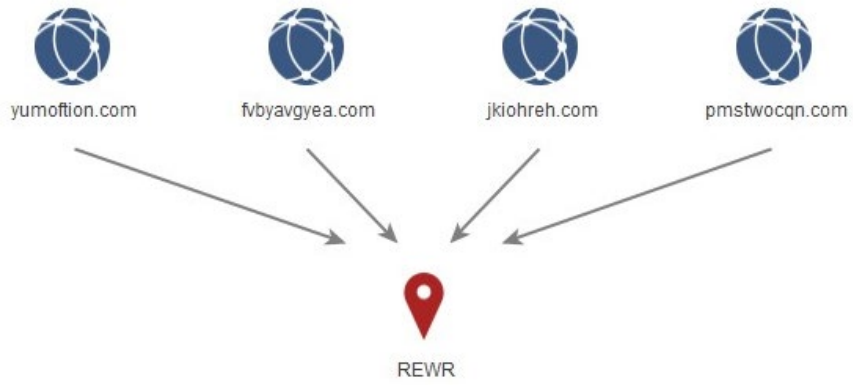
- **ການກວດຈັບແອັບທີ່ຖືກປ່ຽນແປງ:** ຖ້າເປັນໄປໄດ້, ຜູ້ພັດທະນາແອັບຄວນເພີ່ມຟັງຊັນທີ່ແຈ້ງໃຫ້ຜູ້ໃຊ້ຊາບ ຖ້າເຂົາເຈົ້າໄດ້ດາວໂຫຼດແອັບເວີຊັນ 'ບໍ່ເປັນທາງການ', ເພື່ອຊ່ວຍປົກປ້ອງການສຳເນົາທີ່ເປັນອັນຕະລາຍ.

ເອກະສານຊ້ອນທ້າຍ ກ: ກຣາບຂອງຂໍ້ມູນການຈັດກຸ່ມ WHOIS ຂອງ BADBAZAAR / ຂໍ້ມູນນາຍໜ້າໂດເມນ

ຮູບພາບ 1 - 'UKYJYUJ'

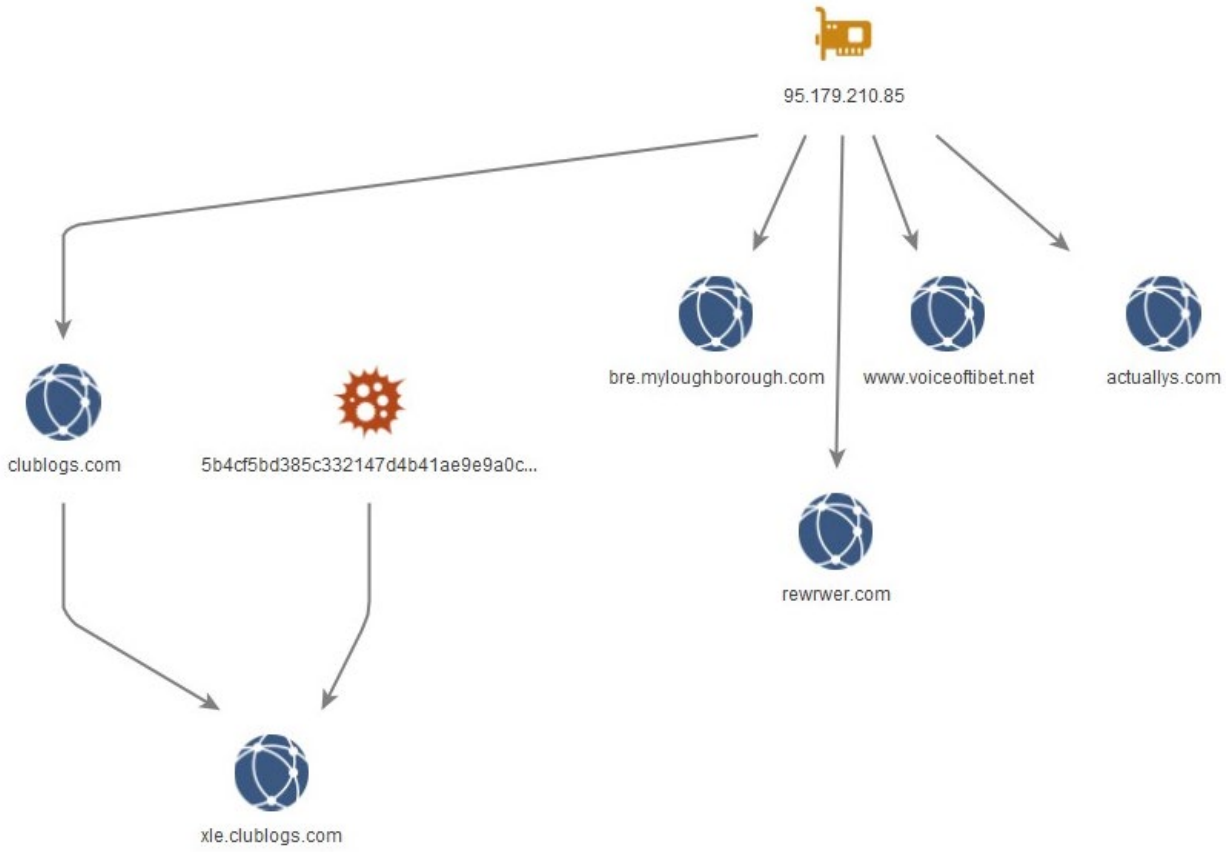


ຮູບພາບ 2 – ຄ່າການຍ່າງແປ້ນພິມ

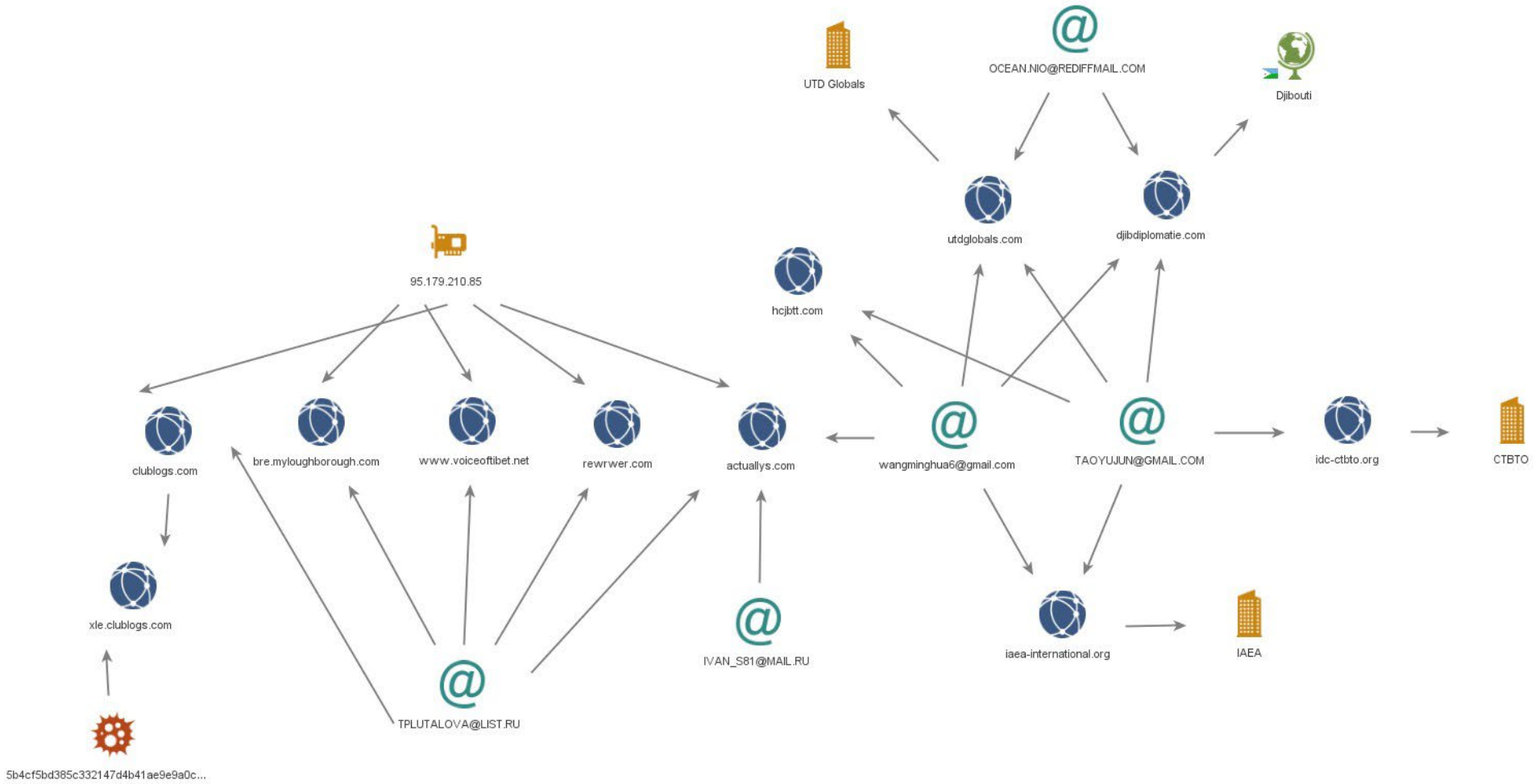


ຮູບພາບ 3 - ໂດເມນເພີ່ມເຕີມທີ່ມີ 'FSDF' ຄ່າຊ່ອງຂໍ້ມູນຂອງລັດ

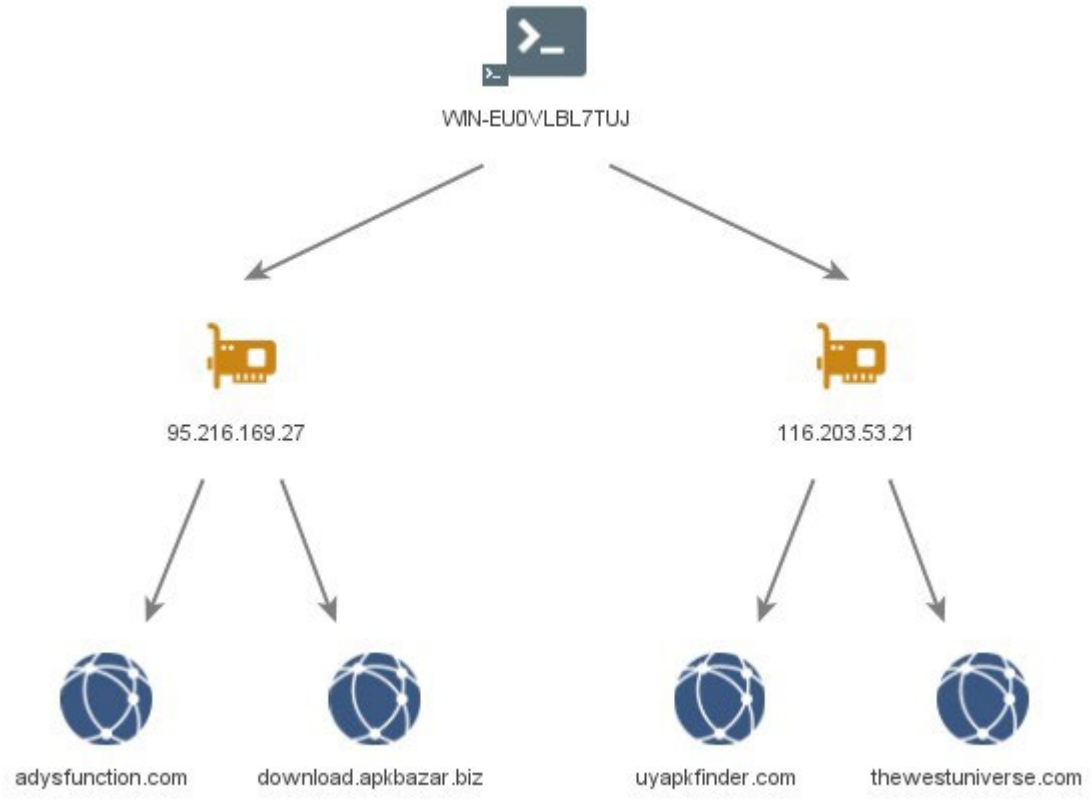
รูปพาบ 4 – **95.179.210[.]85**



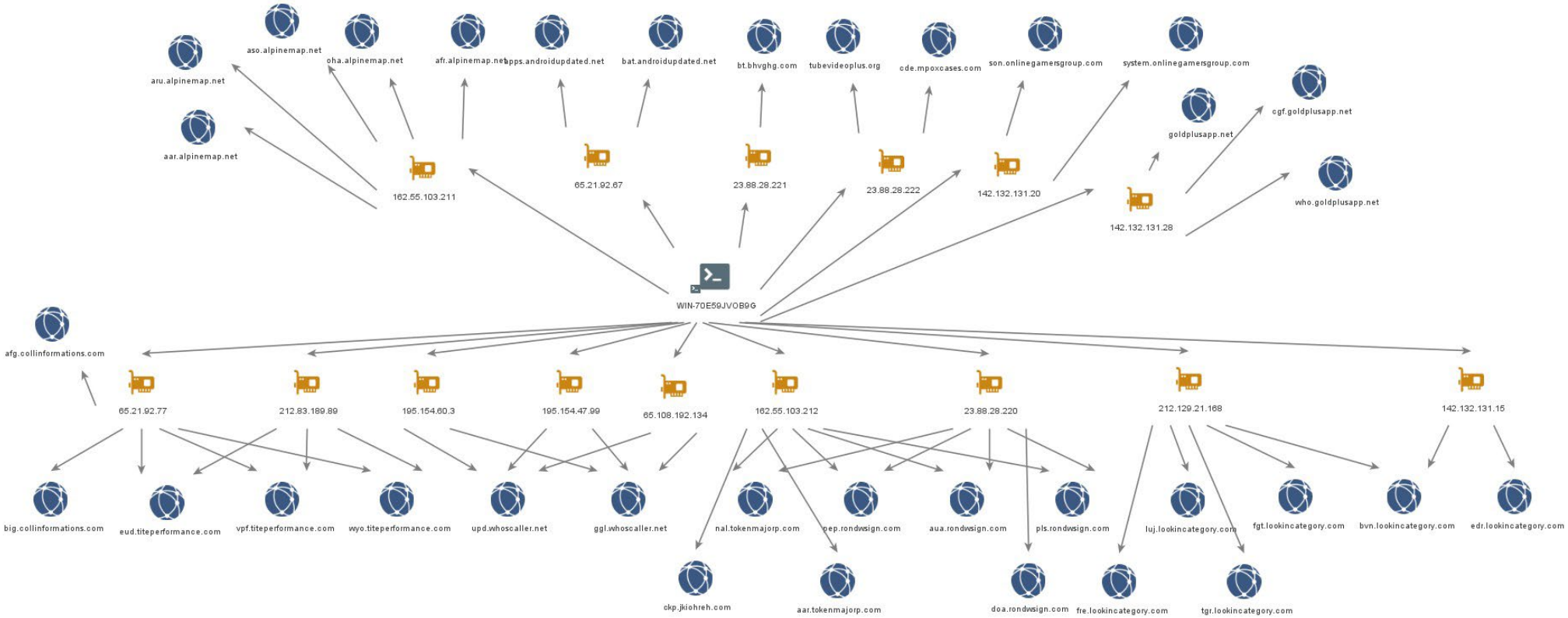
ຮູບພາບ 5 – ລິ້ງ WHOIS



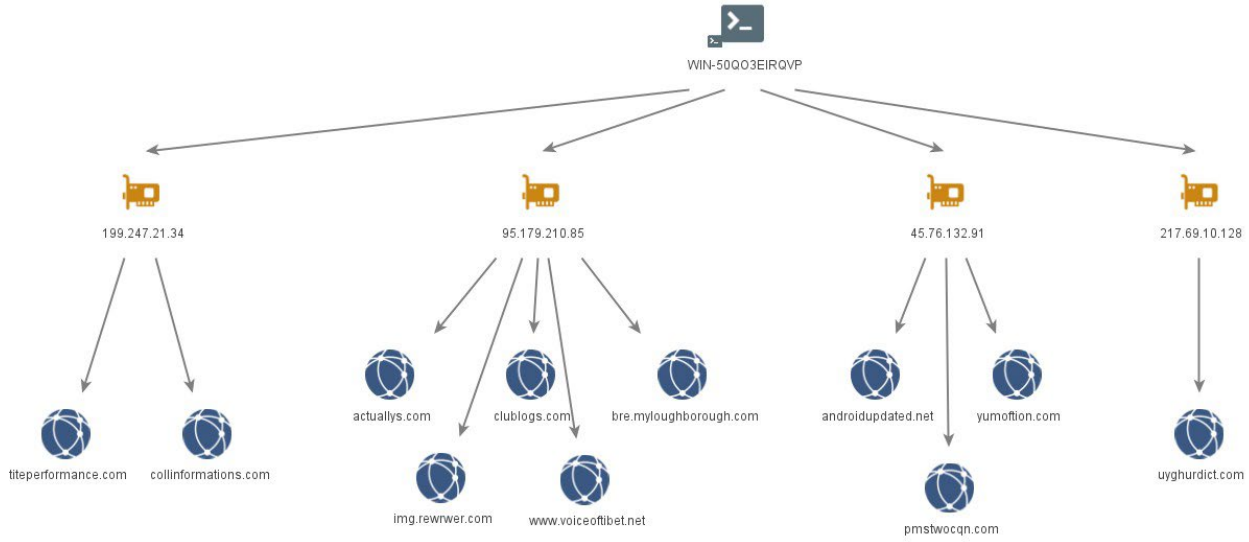
รูปภาพ 6 – **WIN-EU0VLBL7TUJ**



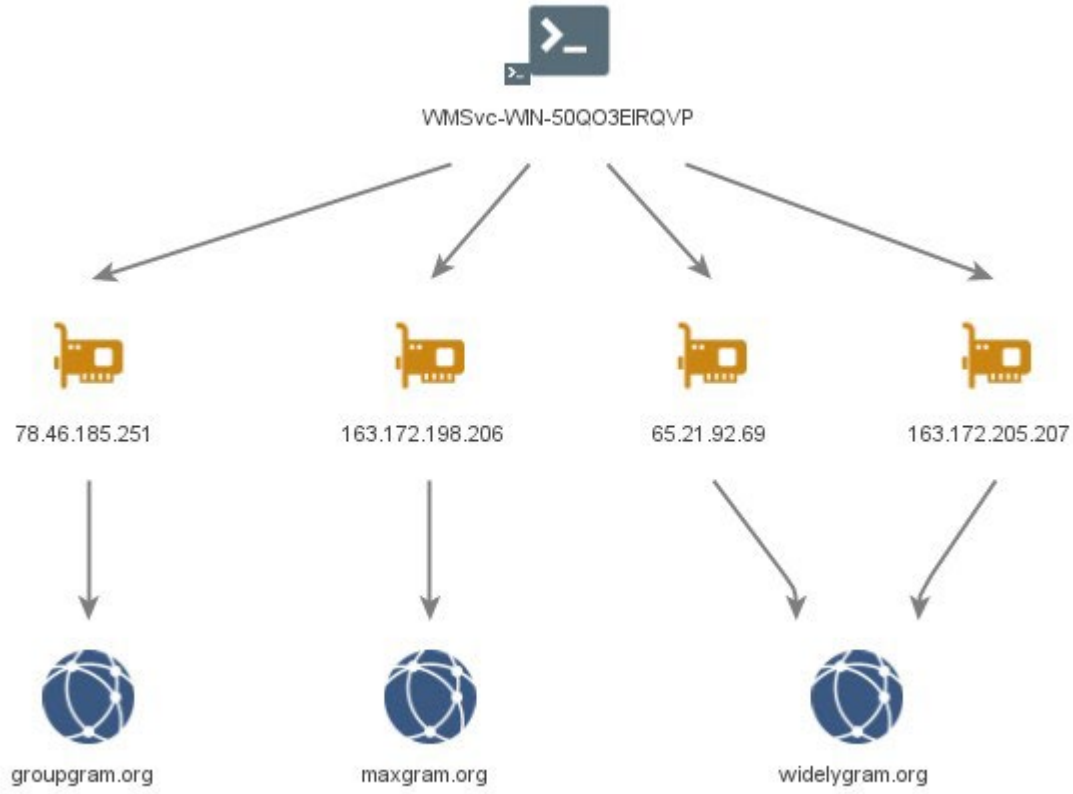
ธูบพาบ 7 – **WIN-70E59JVOB9G**



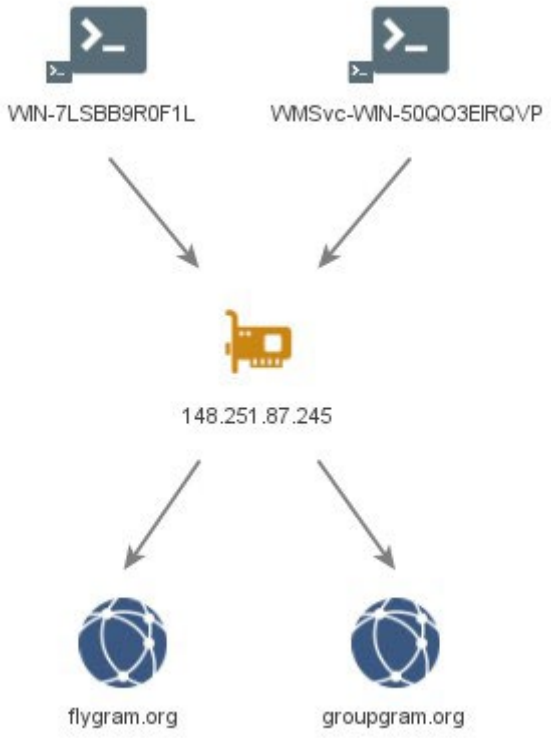
รูปพาบ 8 - **WIN-50QO3EIRQVP**



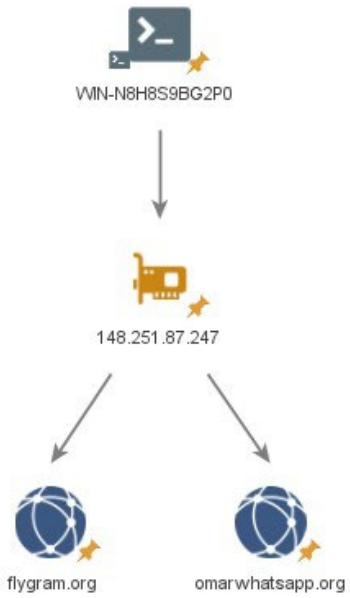
รูปพาบ 9 - **VMSvc-WIN-50QO3EIRQVP**



ธูบพาบ 10 – **VMSvc-WIN-50QO3EIRQVP** และ **WIN-7LSBB9R0F1L**



ธูบพาบ 11 - **WIN-N8H8S9BG2P0**



ธูบพาบ 12 – **WIN-I6VBN8MR92A**

ເອກະສານຊ້ອນທ້າຍ ຂ: ພົບຕົວຢ່າງ MOONSHINE ແລະ BADBAZAAR

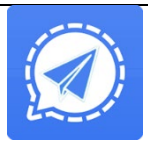
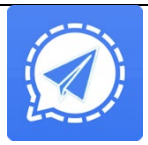
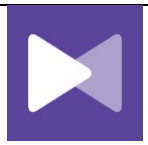
ຕາຕະລາງຂ້າງລຸ່ມນີ້ສະແດງລາຍການແອັບທີ່ໃຊ້ໃນແຄມເປນ MOONSHINE ແລະ BADBAZAAR ໃນຊ່ວງສອງປີທີ່ຜ່ານມາ.

ຫຼາຍໆແອັບເຫຼົ່ານີ້ສະແດງໃຫ້ເຫັນຄວາມຄ້າຍຄືກັນຢ່າງຈະແຈ້ງຕໍ່ກັບແອັບທີ່ສ້າງຂຶ້ນ. ນີ້ແມ່ນແນວໂນ້ມທີ່ຈະເປັນເຕັກນິກ ນັກສະແດງໂດຍເຈດຕະນາເພື່ອ 'ຫຼອກລວງ' ຍີ່ຫໍ້ທີ່ມີຊື່ສຽງ.

ມັນເປັນສິ່ງສໍາຄັນທີ່ຕ້ອງຮູ້ແມ່ນ, ຊື່ແອັບ, ຊື່ແພັກເກັດ ແລະ ໄອຄອນແອັບສາມາດຮຽນແບບ ຫຼື ກົງກັບແອັບພລິເຄຊັນ ທີ່ແທ້ຈິງໄດ້ ແລະ ດັ່ງນັ້ນຈຶ່ງບໍ່ຄວນໃຊ້ສະເພາະເພື່ອກໍານົດວ່າອຸປະກອນຕິດໄວຣັດ ຫຼື ບໍ່ເທົ່ານັ້ນ.

ຊື່ແອັບ	ຊື່ແພັກເກດ	ໄອຄອນແອັບ
99 Names of ALLAH	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(پښتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer (Lite)	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1)	com.bigkidsapps.buddhistsongs1	
Calculator	com.android2.calculator3	
Compass 360 Pro	com.pro.app.compass	
EN-UG Dictionary Free	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	
FAST	com.netflix.Speedtest	

FMWhatsApp	com.fmwhatsapp	
File Manager +	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	
KMPlayer	com.kmplayer	

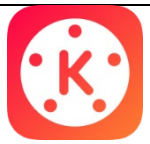
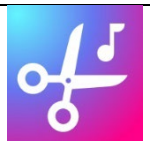
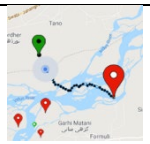
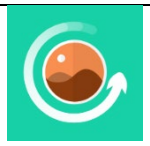
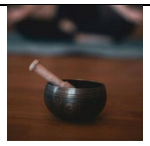
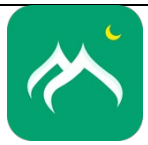
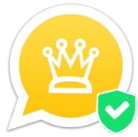
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator	com.routemap.mapdownload.gpsroute planner	
Media Recovery	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra	com.mobisystems.mobiscanner	
PDF Reader	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	

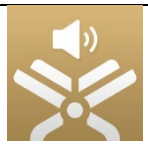
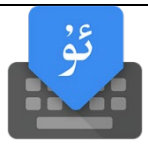
Photo Editor	com.iudesk.android.photo.editor	
Photo Recovery	recover.restore.undelete.photo.video.file	
Photo Studio	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran	com.tos.quranuighore	
QuranKerim	com.ewlat.qurankerim	
Restore Deleted Pics	com.restore.deleted.pictures.video	
Signal	org.thoughtcrime.securesms	
Signal Plus	org.thoughtcrime.securesmsplus	

SignalPlus	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD	com.soundjabber.tibetansingingbowls.candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	
Telegram X	org.thunderdog.challegram	
Tibetan Divination System MO	net.rhombapp.mo	

Tibetan Prayer	com.chorig.tibetanprayer	
Translator AR-TR	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch	com.ziipin.softkeyboard	
Video Converter	com.inverseai.video_converter	
Video Cutter	com.naing.cutter	
Video Downloader	downloader.video.download.free	
Video Maker	com.bstech.slideshow.videomaker	

Video Player for Android	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Voice Recorder	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast	com.graph.weather.forecast.channel	
WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	

WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
WiFi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	
YouTube Downloader	dentex.youtube.downloader	
Zom	im.zom.messenger	
iQuran Lite	com.guidedways.iQuran	

ئەسەرلەر ئاۋازلىق	com.ewlat.eserler	
قۇرئان ئاۋازلىق	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
قۇرئان ئۇيغۇرچە	com.c9.uyghurquran	
الكريم القرآن	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
كەرىم قۇرئان	ru.omdevelopment.ref.quranuyghur.free	
كۇھىقاپ لۇغىتى	com.kuhiqap.lughitim	
كىرگۈزگۈچ نۇر	com.nur.ime	
《心灵法门》念佛机	com.guanyincitta.chant	

汉藏英辞典	com.dacd.dictionary	
藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate	

ອ່ານເພີ່ມເຕີມ

ຄຳແນະນຳຈາກສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕຣາລີ

- ລາຍງານອາດຊະຍາກຳທາງໄຊເບີ, ເຫດການ ຫຼື ຊ່ອງໂຫວ່
- ວິທີຮັກສາອຸປະກອນຂອງທ່ານໃຫ້ປອດໄພ
- ຮັກສາຄວາມປອດໄພໂທລະສັບມືຖືຂອງທ່ານ
- ຟິດຊິງ
- ການຫຼອກລວງ
- ຮັກສາຄວາມປອດໄພສື່ສັງຄົມຂອງທ່ານ
- ເຄັດລັບຄວາມປອດໄພສຳລັບສື່ສັງຄົມ ແລະ ແອັບຮັບສົ່ງຂໍ້ຄວາມ

ຄຳແນະນຳຈາກ NCSC ແລະ NPSA ຂອງອັງກິດ

- ການປົກປ້ອງປະຊາທິປະໄຕ
- ສື່ສັງຄົມ: ວິທີໃຊ້ໃຫ້ປອດໄພ
- ຄຳແນະນຳດ້ານຄວາມປອດໄພອຸປະກອນສຳລັບອົງກອນລວມທັງມືຖື
- ລາຍງານໄພຂົ່ມຂູ່ໃນຮ້ານຄ້າແອັບພລິເຄຊັນ.
- ຄວາມປອດໄພສ່ວນຕົວ ແລະ ຄວາມໝັ້ນຄົງສຳລັບບຸກຄົນທີ່ມີຄວາມສ່ຽງສູງ

ຄຳແນະນຳຈາກ NSA ຈາກສະຫະລັດ

- ແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດຂອງອຸປະກອນມືຖື

ການປະຕິເສດຄວາມຮັບຜິດຊອບ

ກະລຸນາຮັບຊາບວ່າຄຳແນະນຳນີ້ໃຫ້ຂໍ້ມູນທີ່ໄດ້ຮັບການກວດສອບແລ້ວໃນເວລາທີ່ເຜີຍແຜ່.

ບົດລາຍງານນີ້ດຶງຂໍ້ມູນມາຈາກອົງກອນໜ່ວຍງານຜູ້ຈັດທຳ ແລະ ແຫຼ່ງທີ່ມາຈາກອຸດສາຫະກຳ. ຜົນການຄົ້ນພົບ ແລະ ຂໍ້ສະເໜີແນະໃດໆ ທີ່ເກີດຂຶ້ນບໍ່ໄດ້ຈັດທຳຂຶ້ນດ້ວຍຄວາມຕັ້ງໃຈທີ່ຈະຫຼີກເວັ້ນຄວາມສ່ຽງທັງໝົດ ແລະ ປະຕິບັດຕາມຄຳແນະນຳຈະບໍ່ສາມາດຈັດຄວາມສ່ຽງທັງໝົດດັ່ງກ່າວໄດ້. ຄວາມເປັນເຈົ້າຂອງຄວາມສ່ຽງດ້ານຂໍ້ມູນຍັງຄົງຢູ່ກັບເຈົ້າຂອງລະບົບທີ່ກ່ຽວຂ້ອງຕະຫຼອດເວລາ.

ໃນປະເທດອັງກິດ, ຂໍ້ມູນນີ້ຖືກຍົກເວັ້ນພາຍໃຕ້ກົດໝາຍວ່າດ້ວຍເສລີພາບຂອງຂໍ້ມູນຂ່າວສານ 2000 (FOIA) ແລະ ອາດໄດ້ຮັບການຍົກເວັ້ນພາຍໃຕ້ກົດໝາຍຂໍ້ມູນຂ່າວສານອື່ນໆຂອງອັງກິດ.

ອ້າງອີງຄຳຖາມ FOIA ໃດໆກໍຕາມໄປທີ່ ncscinfoleg@ncsc.gov.uk.