OSINT (OPEN-SOURCE INTELLIGENCE) БУЮУ НЭЭЛТТЭЙ ЭХ СУРВАЛЖААС МЭДЭЭЛЭЛ ЦУГЛУУЛАХ

Б.Ганболд, Дотоод Хэргийн Их Сургуулийн Цагдаагийн сургуулийн Гүйцэтгэх ажлын тэнхимийн багш, цагдаагийн ахмад

B. Ganbold, lecturer of the Department of Criminal intelligence at the Police School of the University of Internal Affairs, police captain

Хураангуй: OSINT гэж юу вэ? OSINT гэдэг нь нээлттэй эх сурвалжаас мэдээлэл цуглуулах үйл ажиллагааг хэлдэг. Нээлттэй эх сурвалжууд гэдэгт засгийн газар, банк санхүүн мэдээллийн сан, хувь хүн албан байгууллагын веб сайтууд, олон нийтийн мэдээллийн платформууд болон сонин хэвлэл гэх мэт бусад мэдээллийн эх сурвалжууд орно.

Abstract: What is OSINT? OSINT refers to the collection of information from open sources. Open sources include government and banking databases, websites of individuals and organizations, social media platforms and other sources of information such as newspapers.

Түлхүүр үгс: OSINT- нээлттэй эх сурвалж, гэмт хэрэгтэй тэмцэх, кибер орчноос мэдээлэл цуглуулах

Keywords: OSINT- open source intelligence, crime fighting, intelligence gathering from the cyber environment

Оршил: OSINT-буюу нээлттэй эх сурвалжаас мэдээлэл цуглуулах аргыг хууль сахиулах байгууллагаас кибер орчинд үйлдэгдэж буй залилах гэмт хэргийг илрүүлэх, мөн кибер аюулгүй байдлын мэргэжилтнүүд итгэлцэл, аюулгүй байдал эрсдэлийн менежмент хийхэд ашигладаг. Үүнээс гадна хүний нөөцийн болон бизнесийн менежерүүд ажилчид эсвэл түншүүдээ сайтар судлахын тулд OSINT-ийн хэрэгслийг ашигладаг байна.

Кибер орчинд нээлттэй эх сурвалж \OSINT\ ашиглан мэдээлэл ямар мэдээлэл цуглуулах боломжтой талаар тоймлон харуулав. Жишээлбэл

- Хувь хүмүүсийн физик байршил
- Олон нийтийн мэдээллийн платформууд дээрх мэдээлэл
- Хувь хүн, аж ахуйн нэгж байгууллагын нэр дээр бүртгэлтэй домэйн нэр, сервер, цахим шуудангийн хаягууд
- Төрийн байгууллагын ил тод байдлын мэдээллийн сангууд, зөрчлийн бүртгэл, эзэмшиж буй лиценз гэх мэт. Эдгээр мэдээллийг албан ёсны мэдээллийн сан дээрх мэдээлэл, мэргэжлийн байгууллагаас өгсөн хувийн мэдээлэл гэж ангилдаг.
- Блог, сэтгүүлийн нийтлэл, мэдээний нийтлэл, хурлын материал
- Гар утасны мэдээллүүд болох утасны дугаар, төхөөрөмжийн төрөл, ашиглагдаж буй программууд гэх мэт.

Олон улсад хууль сахиулах байгуулга гэмт хэрэгтэй тэмцэх зорилгоор ашиглаж болох мэдээ мэдээллийг үндсэн гурван эх сурвалжаас цуглуулдаг байна. Нэгдүгээрт: нээлттэй эх сурвалжийн ашиглах (OSINT- open-source intelligence), хоёрдугаарт: кибер орчинд мэдээлэл цуглуулах (CYBINT), гуравдугаарт: хүн эх сурвалж ашиглан мэдээлэл цуглуулах (HUMINT)[1]. Үүнээс бид OSINT буюу олон нийтэд ил байдаг нээлттэй эх сурвалжаас (интернет болон бусад нээлттэй эх сурвалж) мэдээлэл цуглуулах тэр дундаа кибер орчинд нээлттэй эх сурвалжаас мэдээлэл цуглуулах үйл явцын талаар дэлгэрэнгүй авч үзье.

-

-

OSINT ХЭРЭГСЛҮҮД

Нээлттэй эх сурвалжаас \OSINT\ мэдээлэл цуглуулах зорилгоор дараах хэрэгслүүдийг ашиглах боломжтой. Эдгээр хэрэгслүүд ямар чиглэлээр мэргэшсэн, юугаараа өвөрмөц, ялгаатай болохыг доор харуулав.

Maltego: Малтего нь хүмүүс, компаниуд, домэйн болон интернэт дэх олон нийтэд нээлттэй мэдээлэл хоорондын харилцааг илрүүлэх чиглэлээр мэргэшсэн мэдээллийн сайт юм. Дэлгэрэнгүй мэдээллийг https://www.maltego.com/ хаягаар нэвтэрч судлаарай.

Mitaka: Та өөрийн ашиглаж байгаа интернэт хөтөч болох Chrome эсвэл Firefox дээр нэмэлтээр Mitaka-г үнэгүй суулгаснаар олон төрлийн хайлтын системээс IP хаяг, домэйн нэрийн бүртгэл, URL, хэш, биткойн түрийвчний хаяг гэх мэт төрөл бүрийн мэдээллийг өөрийн вэб хөтчөөсөө хайх боломжийг олгоно.
Хэрэгслийг https://github.com/ninoseki/mitaka хаягаар нэвтэрч суулгаарай.

Spiderfoot: нь IP хаяг, домэйн болон дэд домайн, имэйл хаяг, утасны дугаар, хэрэглэгчийн нэр, BTC хаяг мэт мэдээллийг цуглуулж, дүн шинжилгээ хийх боломжтой олон төрлийн мэдээллийн эх сурвалжтай нэгтгэсэн үнэгүй OSINT хайгуулын хэрэгсэл юм. Та Spiderfoot программыг GitHub дээрээс татаж суулгах боломжтой.
Хэрэгслийг https://github.com/smicallef/spiderfoot хаягаар нэвтэрч суулгаарай.

BuiltWith: BuiltWith сан нь таны сонирхсон вэбсайтууд юугаар бүтээгдсэнийг олох боломжийг танд олгоно. Вэбсайтууд нь янз бүрийн технологийн арга, платформууд өөр өөр сайтуудыг ажиллуулж байдаг.
https://builtwith.com/ хаягаар орж туршиж үзээрэй.

Intelligence X: программ нь вэб хуудаснуудын түүхэн хувилбаруудыг төдийгүй агуулгын үл нийцэх шинж чанар эсвэл хууль эрх зүйн шалтгааны улмаас вэбээс устгагдсан мэдээллийн багцыг бүхэлд нь хадгалж байдаг архивын үйлчилгээг агуулсан хайлтын систем юм.
https://intelx.io/ хаягаар орж туршиж үзээрэй.

---

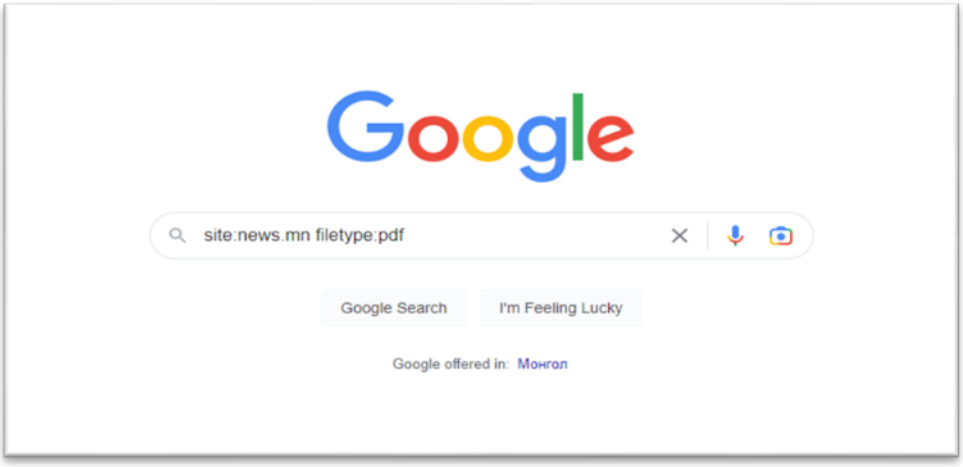
[1] https://www.crowdstrike.com

Grep.app: Та интернэтээр өөрт хэрэгтэй программчлалын эх кодыг хэрхэн хайх вэ? Мэдээжийн хэрэг GitHub, GitLab эсвэл BitBucket-ийн санал болгож буй хайлтын талбаруудыг та ашиглаж болно.
https://grep.app/ хаягаар орж туршиж үзээрэй.

Вэбсайтаас мэдээлэл цуглуулах: Албан байгууллага хувь хүний талаарх мэдээллүүдийг вэбсайтаас олох боломжтой байдаг. Дараах мэдээллийг цуглуулах боломжтой:
-Тэд юу хийдэг;
-Тэдний үзүүлж буй бүтээгдэхүүн, үйлчилгээ;
-Хаяг байршил;
-Нээлттэй ажлын байрууд;
-Холбоо барих утасны дугаарууд;
-Захирлууд эсвэл ажилчдын талаарх мэдээлэл, намтар;
-Хамтран ажилдаг албан байгуулга;
-И-мэйл хаяг;
-Холбоо барих утасны дугаар гэх мэт.

Цагдаагийн байгууллагын мөрдөгч гэмт этгээдийн талаар олон нийтийн мэдээллийн сайтуудаас /нээлттэй эх сурвалж/ төрөл бүрийн мэдээлэл цуглуулах боломжтой, тэд өөрсдийн зураг, байшин, тээврийн хэрэгсэл, ажил гэх мэт амьдралынхаа бараг бүх нарийн ширийн зүйлийг кибер орчинд нийтлэх тохиолдол их байдаг. Ихэнх тохиолдолд нэг газар хамт ажилладаг хүмүүс олон нийтийн мэдээллийн сайтууд дээр нэг бүлэг болж холбогдсон байдаг. Хэрэв мөрдөгч LinkedIn эсвэл Facebook дээр нэг ажилтан олсон бол түүгээр дамжуулан бусад бүх ажилчдыг тодорхойлох боломжтой. Ихэнх хүмүүс өөрсдийн ажил албан тушаалын талаар олон нийтийн мэдээллийг хэрэгсэлд оруулсан байдаг. Энэ мэдээллүүд нь мөрдөгчид тухай албан байгууллагын талаарх мэдээлэл, дотоод бүтэц, хэлтэст хэдэн хүн ажилладаг болох гэх мэт мэдээллүүдийг тодорхойлоход тусална.

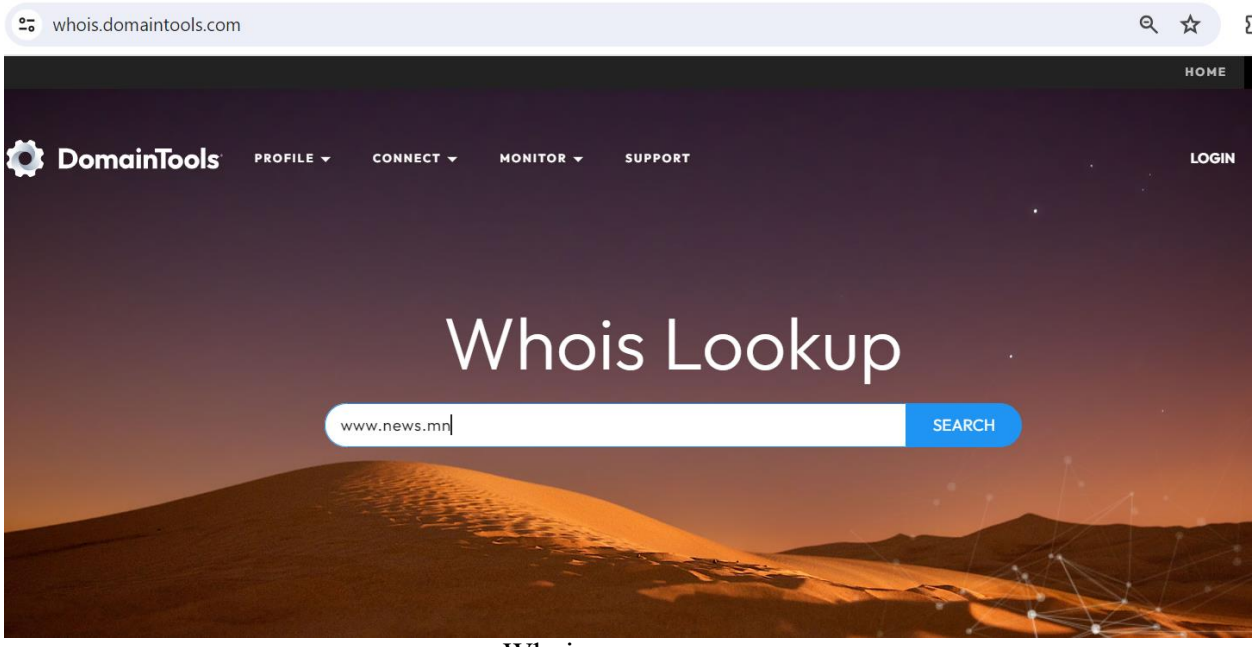
Хайлтын систем ашиглан мэдээлэл цуглуулах: Веб сайт дээр нийтлэгдээгүй мэдээллийг олохын тулд дэвшилтэт хайлтын операторуудыг ашиглан хайлтын системээс мэдээлэл олох боломжтой. Энэ аргыг Google dork буюу dork гэж нэрлэдэг. Өөрөөр хэлбэл google dorking буюу Google-ийг хакердах арга нь энгийн хайлтын асуултаар олоход хэцүү мэдээллийг тусгай компьютерын хэл \query\ ашиглан олох юм. Жишээлбэл: site:news.mn filetype:pdf гэж бичин хайлт хийвэл www.news.mn домэйн дээрх PDF өргөтгөлтэй нийтийн хүртээл болгоход зориулаагүй файлуудын жагсаалтыг гаргаж ирдэг.



Зураг дээр google dorking ашиглах аргыг харуулав

Өөрт хэрэгтэй мэдээллийг цуглуулахын тулд хайлтын нэр томьёог мэддэг байх хэрэгтэй. Ямар нэг мэдээллийг хайхдаа filetype:pdf, filetype:doc, filetype:xls, filetype:txt гэж хайдаг зуршилтай болох. Энэ нь бидэнд DAT, CFG эсвэл бусад мэдээллийн сан эсвэл сервер дээрээ тухайн байгууллагын ажилчдын нээлттэй орхисон, хуулаад мартсан файлуудыг авах боломжийг өгдөг. www.googleguide.com/advanced_operators.html гэх холбоосоор илүү дэлгэрэнгүй мэдээллийг авч бие даан суралцах боломжтой.

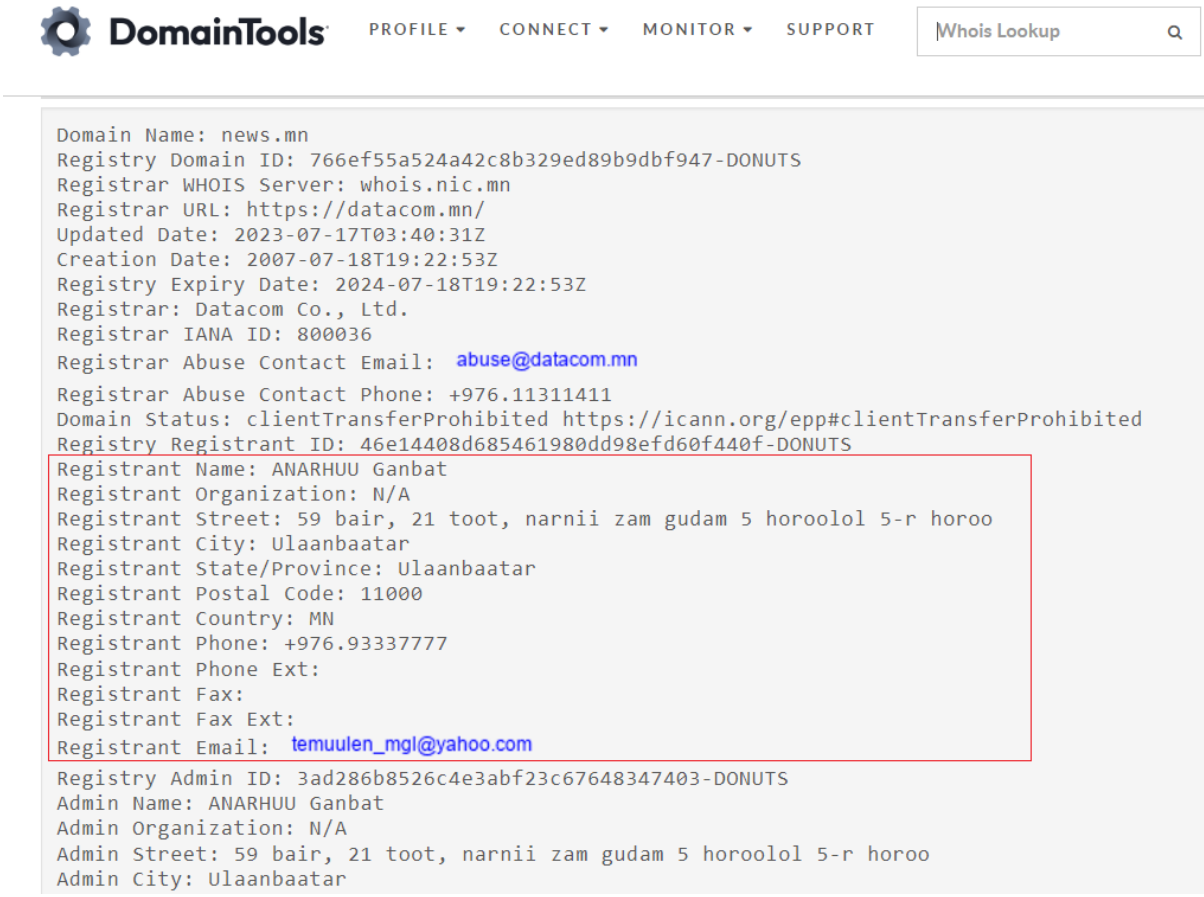
Whois сангаас мэдээлэл цуглуулах: Whois гэдэг нь интернет үйлчилгээ үзүүлэгч компани, домэйн нэр эзэмшигчдийн талаарх мэдээллийг агуулсан мэдээллийн сангийн юм. Whois мэдээллийн сан нь зарим тохиолдолд веб сайтын администраторуудын талаарх бүрэн мэдээллийг агуулж байдаг асар том мэдээллийн сан.



Whois санг харуулав.

Мөн Whois мэдээллийн сан нь тодорхой IP хаягуудын мэдээллийг агуулж байдаг. Мөрдөгч Whois мэдээллийн санг ашиглан тухайн IP хаяг бүртгэлтэй интернэтийн үйлчилгээ үзүүлэгч компанийг тогтоож, тус компанид хандсанаар тухай IP хаягийг ямар байгууллага, компани, хувь хүн ашиглаж байсан талаарх мэдээллийг тогтоох боломжтой.

Мөн whois санг ашиглан домейн нэрийн бүртгэлийн мэдээллийг олох боломжтой. Жишээ нь www.news.mn веб хуудасны домэйн нэрийг шалгаж үзэхэд:



- Серверийн IP хаяг нь 43.231.115.241, Монгол улс, Улаанбаатар хот, Itools ХХК-дээр байршилтай ба эзэмшигчийн нэр, холбогдох утасны дугаар, имэйл хаяг гарч ирж байна.

Иймд www.whois.com, www.who.is, www.whois.domaintools.com гэх мэт санг ашиглан эзэмшигчийн мэйл хаяг, утасны дугаар, DNS серверийн IP хаягийн талаарх мэдээллийг олох боломжтой юм.

Практикт веб сайт эрхлэгчдийн мэдээлэл, гэмт хэрэг үйлдэхэд ашигласан IP хаяаг бүртгэлтэй интернэтийн үйлчилгээ үзүүлэгч компанийн мэдээлэл зэргийг авахын тулд мөрдөгч албан бичиг төлөвлөн холбогдох байгууллага руу илгээж цаг алдах тохиолдол их байдаг. Үүний оронд мөрдөгч өөрийн интернэт холболттой гар утас, нотебүүк эсвэл компьютерыг ашиглан Whios мэдээллийн санд нэвтэрч дээрх мэдээллийг түргэн хугацаанд олж авах боломжтой юм. Мөн Whois мэдээллийн сан нь сонирхож буй компанийн танилцуулга, серверийнх нь талаарх дэлгэрэнгүй мэдээллийг авахад их тустай байдаг. Энэ аргыг ашиглан нэмэлт бусад мэдээллийг цуглуулах боломжтой.

Олон нийтийн сүлжээ сайт ашиглан мэдээлэл цуглуулах: Иргэд албан байгууллагууд олон нийтийн сүлжээг өргөн ашиглах болсон. Энэ бол олон тооны боломжит худалдан авагчдыг нэг дор хамруулсан маркетингийн үр дүнтэй хямд арга юм. Нөгөө талаас хувь хүн албан байгууллын талаарх мэдээллийг агуулсан маш том мэдээллийн урсгал юм. Албан байгууллага нь өөрийн үйл ажиллагаа, байгууллагын талаарх мэдээ, шинэ бүтээгдэхүүн, хэвлэлийн мэдээ, гэх мэт одоогийн үйл ажиллагаатай холбоотой мэдээллийг нийтлэн, түүх үүсгэн хадгалагдсан байдаг. Сүүлийн үед Twitter, Instagram, Facebook, LinkedIn, Tiktok, Youtube болон бусад сайтуудын тусламжтайгаар хангалттай их мэдээллийг олж авах боломжтой.

Дүгнэлт: Дээрх жишээнүүд дээр хэлэх гэсэн гол нь санаа бол мэдээллийг хэрхэн ашиглах биш харин нээлттэй эх сурвалжаас мэдээллийг яаж цуглуулахад гол учир нь байгаа юм. Мэдээлэл цуглуулахад ашиглаж болох эх сурвалжууд, ашиглах арга тус бүр харилцан адилгүй. Мэдээлэл цуглуулах олон төрлийн эх сурвалжууд байдаг гэж өмнө дурдсан. Цагдаагийн эрүүгийн мөрдөгч бүх төрлийн эх сурвалжийг чадварлагаар ашиглан, тэдгээрийн давуу болон сул талуудыг судлан гэмт хэрэгтэй тэмцэхэд дэмжлэг үзүүлэх боломжтой мэдээллийг бие даан цуглуулах боломжтой юм.

Ашигласан материал:

Эрүүгийн мөрдөгч: гарын авлага төсөл 2023 он
https://www.kaspersky.com
https://www.cisco.com
https://www.crowdstrike.com
https://www.csoonline.com