КИБЕР ОРЧИНД НЭЭЛТТЭЙ ЭХ СУРВАЛЖААС МЭДЭЭЛЭЛ ЦУГЛУУЛАХ НЬ

Б.Ганболд
ДХИС-ийн Цагдаагийн сургуулийн Гүйцэтгэх ажлын тэнхимийн багш, цагдаагийн ахмад

Товч агуулга. OSINT гэж нээлттэй эх сурвалжаас мэдээлэл цуглуулах үйл ажиллагааг хэлдэг. Нээлттэй эх сурвалжууд гэдэгт Засгийн газар, банк, санхүүгийн мэдээллийн сан, хувь хүн албан байгууллагын цахим хуудас, олон нийтийн мэдээллийн платформууд болон хэвлэл мэдээллийн хэрэгсэл нийтлэгдсэн мэдээлэл хамаарна.

Abstract. 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

Удиртгал

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)[176]. 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-буюу нээлттэй эх сурвалжаас мэдээлэл цуглуулах арыг хууль сахиулах байгууллагаас гадна кибер орчинд залилан илрүүлэх, итгэлцэл, аюулгүй байдал зэрэг эрсдэлийн менежмент хийхэд кибер аюулгүй байдлын мэргэжилтнүүд мөн 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 цуглуулах боломжтой зарим төрлийг тоймлон харуулав.

- Хувь хүмүүсийн физик байршил
- Олон нийтийн мэдээллийн платформууд
- 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 сангаас олгосон нийтийн 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.

OSINT ХЭРЭГСЛҮҮД

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

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

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.

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.

Хайлтын систем ашиглан мэдээлэл цуглуулах: Веб сайт дээр нийтлэгдээгүй мэдээллийг олохын тулд дэвшилтэт хайлтын операторуудыг ашиглах боломжтой. Энэ аргыг **Google dork** буюу **dork** гэж нэрлэдэг[177]. 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:ikon.mn filetype:pdf** гэж бичин хайлт хийвэл www.ikon.mn домэйн дээрх PDF өргөтгөлтэй нийтийн хүртээл болгоход зориулаагүй файлуудын жагсаалтыг гаргаж ирдэг.

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

Whois мэдээллийн 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.

Линукс командын мөрийг ашиглах эсвэл **www.whois.com**, **www.who.is** гэх вэбсайтыг ашиглан хүний имэйл хаяг, утасны дугаар, тэр ч байтугай DNS серверийн IP хаягийн талаарх мэдээллийг олох боломжтой.

Практикт веб сайт эрхлэгчдийн мэдээлэл, гэмт хэрэг үйлдэхэд ашигласан IP хаяаг бүртгэлтэй интернэтийн үйлчилгээ үзүүлэгч компанийн мэдээлэл зэргийг авахын

[177] https://www.csoonline.com

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 1 минут магадгүй үүнээс бага хугацаанд олж авах боломжтой юм.

Олон нийтийн сүлжээ сайт ашиглан мэдээлэл цуглуулах: Сүүлийн үед 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.

Зурган файл дээрх мета өгөгдөл ашиглан мэдээлэл цуглуулах: Ухаалаг гар утас нь GPS-ийн (Global Positioning System - Дэлхийн байршил тогтоох систем) байршлын мэдээллийг авсан зураг дээрээ суулгадаг гэдгийг ихэнх хүмүүс мэддэггүй. Өөрөөр хэлбэл танд мэдэгдэлгүйгээр таны байршлыг бусдад дэлгэж байдаг гэсэн үг. Хэрэглэгч ийм өгөгдөлтэй зургийг бусдад илгээснээр өөрийн байгаа байршил руу нь хөтлөх боломжийг олгож байдаг.

www.linangdata.com веб хуудсанд байрлах EXIF data viewer хэсэгт сонирхол татсан зургийг оруулж тухайн зургийг авсан төхөөрөмжийн нэр марк дугаар, он сар өдөр цаг минут, байршил (зураг дарах үед GPS асаалттай байсан тохиолдолд) зэрэг мэдээллийг харах 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.

Ашигласан материал

- https://www.kaspersky.com
- https://www.cisco.com
- https://www.crowdstrike.com
- https://www.csoonline.com