

**МЕТА ӨГӨГДЛИЙГ АШИГЛАН ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ, ӨӨРИЙН
АЮУЛГҮЙ БАЙДЛАА КИБЕР ОРЧИНД ХЭРХЭН ХАМГААЛАХ
ТАЛААРХ ОЙЛГОЛТ**
**UNDERSTANDING HOW TO FIGHT CRIME AND PROTECT YOURSELF
IN CYBER ENVIRONMENT USING META DATA**

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

Товч агуулга: Хэн нэгэнд илгээсэн энгийн файл эсвэл зураг таны бусадтай хуваалцахыг хүсээгүй мэдээллийг дотроо агуулж байдаг гэдгийг мэдэх үү. Бусад илгээсэн гэрэл зураг нь тухайн зурагт байгаа мэдээллээс гадна зураг дарсан газар орны байршил, огноо, ямар төхөөрөмжөөс авсан зэрэг мэдээллийг танд мэдэгдэлгүй бусад дэлгэж байдаг. Эдгээр мэдээлэл нь файлын мета өгөгдөл дотор хадгалагдаж байдаг. Файлын мета өгөгдөл гэж юу болохыг хүн бүр мэддэггүй. Хэн нэгэнд илгээх гэж байгаа зураг болон бусад файлд агуулагдаж байгаа мета өгөгдлөө хамгаалснаар болзошгүй гэмт хэргийн хохирогч болохоос урьдчилан сэргийлж чадах юм.

Abstract: Did you know that a simple file or photo that you send to someone can contain information you don't want to share with others? In addition to the information contained in the photo, the photos sent to others reveal information such as the location of the photo taken, the photo date, and the device from which it was taken without your knowledge. This information is stored in the file's metadata. Not everyone knows what file metadata is. By protecting the metadata contained in the images and other files you are sending to others, you can prevent yourself from becoming a potential victim of crime.

Түлхүүр үгс: Нийгмийн инженерчэл, Фишинг халдлага, мета өгөгдөл.

Keywords: Social engineering, Phishing attack, meta data.

Удиртгал

Мета өгөгдлийн аюулын талаар: Юуны өмнө мета өгөгдөл нь өгөгдлийн талаарх өгөгдөл гэдгийг ойлгох хэрэгтэй. Жишээлбэл, танд олон нийтийн сүлжээнд байршуулсан зураг байна. Тэр зургийн файл дараах мета өгөгдлийг дотроо агуулж байдаг - зургийг хаана, хэзээ, хэдэн цагт, ямар төхөөрөмж ашиглан авсан гэх мэт мэдээллийг дотроо агуулж байдаг. Тэхээр та зарим мэдээллийг бусад илгээх үед бусадтай огт хуваалцахаар төлөвлөөгүй мэдээллээ хамт илгээж болох нь харагдаж байна.

Хүний онлайн орчинд хийж буй бүх үйлдлүүд болох гэрэл зураг авах, файл илгээх, пост нийтлэх, хөгжим сонсох, онлайн худалдан авалт хийх зэрэг бүх зүйлд бидний өөрийн оруулсан мэдээллээс гадна тоон ул мөр давхар үлдэж байдаг. Энэ тоон ул мөр нь мета

өгөгдлийн улмаас үүсдэг. Ихэнхдээ хүмүүс энэ талаар мэдэхгүйн улмаас аль эсвэл мэдсэн ч энэ баримтыг үл тоомсорлох нь араасаа аюул заналхийллийн эрсдэл дагуулж байдаг.

Жишээлбэл, нийгмийн сүлжээн дэх гэрэл зургуудыг гэмт хэрэгтэн судалснаар ирээдүйд хохирогч болох хүний тогтмол явдаг маршрутыг тогтоохоос гадна түүний очих дуртай газар зэргийг олж мэдэх боломжтой. Энэ өгөгдөл дээр үндэслэн гэмт этгээд фишинг халдлага хийхэд бэлтгэх эсвэл нийгмийн инженерчлэлийн арга ашиглан залилан мэхлэх замаар гэмт хэрэг үйлдэх боломжтой юм.

Нийгмийн инженерчлэл гэдэг нь бусдаас мэдээлэл авах эсвэл ямар нэг үйлдэл хийлгэх зорилгоор тухайн нөхцөлд тааруулж зохиомол нөхцөл байдал үүсгэн, бусад нөлөөлөх замаар бусдыг удирдах сэтгэлзүйн заль мэх юм.

Фишинг халдлага гэдэг нь кибер орчинд хамгийн түгээмэл тархсан нийгмийн инженерчлэлийн халдлагын нэг төрөл юм¹. Үндсэндээ фишинг гэдэг нь иргэдийн нэвтрэх нэр нууц үгийг олж авахад чиглэсэн байдаг. Хуурамч цахим шуудан ашиглах, эсвэл хууль ёсны мэт харагдах веб хуудас ашиглан бусдын нууц үгийг хулгайлдаг. Заримдаа гэмт этгээд хохирогчийг зээлийн картын мэдээлэл эсвэл бусад хувийн мэдээллээ өгөхийг албадах оролдлого хийдэг. Мөн илүү дэвшилтэт халдлагууд мөн ransomware² гэх мэт илүү аюултай халдлагууд ихэвчлэн фишинг халдлагаас эхэлдэг.

Мета өгөгдөл нь хэрэглэгчийн оролцоогүйгээр автоматаар үүсэх бөгөөд тэдгээр нь ихэвчлэн файл үүсгэсэн огноо, газар, ашигласан техник, файлд нэмсэн тохиолдолд зохиогчийн өгсөн тайлбар, түүнийг үүсгэсэн программын хувилбарын талаарх мэдээллийг агуулдаг. Зарим тохиолдолд мета өгөгдөл нь хэрэглэгч хооронд шилжүүлэн дамжсан түүх, файлын өөрчлөлтийн талаарх мэдээллүүдийг хэлж чаддаг тул нэлээд эмзэг бөгөөд хувийн шинж чанартай мэдээллүүдийг агуулж байдаг.

Яагаад мета өгөгдөл хэрэгтэй байдаг вэ?

Мета өгөгдлийн гол зорилго бол тухайн файлын албан ёсны лицензийн хязгаарлалтыг тогтоох, мөн зохиогчийг тодорхойлоход оршиж байдаг. Мөн сайтууд болон аппликешнүүдэд байрлуулсан файлуудын агуулгыг цэгцлэх, тодорхойлоход тусалдаг. Жишээлбэл, харилцаа холбооны операторууд мета өгөгдөл дээр тулгуурлан хэрэглэгчдийн үйл ажиллагааг хянах боломжтой байдаг.

Нийгмийн сүлжээ, интернэтэд үлдээсэн тоон ул мөр буюу мета өгөгдөлд дүн шинжилгээ хийснээр зорилтот хэрэглэгчдийн сонирхол, сонголт, байршил, дадал зуршил, үйл ажиллагааны талбарын талаарх мэдээллүүдийг ангилах боломжтой болдог.

Мета өгөгдлөө хэрхэн хамгаалах, эсвэл устгах вэ?

Мета өгөгдөл нь ердийн өгөгдлийн нэгэн адил хамгаалагдсан байдаг, ялангуяа энэ нь энгийн хэрэглэгч гэхээсээ илүү байгууллагатай холбоотой байдаг. Энгийн хэрэглэгчийн хувьд хувийн мэдээллээ бусадтай хуваалцахыг хүсэхгүй байгаа бол өөрийн дижитал ул мөр буюу мета өгөгдлийг илгээх гэж байгаа файлаасаа устгаж байх хэрэгтэй.

iPhone гар утас ашиглан зурган файлаас мета өгөгдлийг устгах амархан:

1. Photos программыг нээгээд мета өгөгдлийг устгахыг хүссэн зургаа сонгоно уу.

¹ Руководство по защите от хакеров/ Коул Эрик. Пер. с англ. – М. Издательский дом «Вильямс», 2002.

² Ransomware гэдэг нь хохирогчийн төхөөрөмж дээрх файлуудыг шифрлэн түгжиж барьцаалдаг хортой вирус бөгөөд түгжээтэй файлуудыг тайлахын тулд хохирогчоос мөнгө нэхдэг.

2. Дэлгэцийн баруун доод буланд байрлах Хуваалцах дүрс дээр товшоод мета өгөгдлийг бүү хадгалах сонголтыг сонгоно.
3. "Дууссан" товчийг дарна.

Андройд дээрх файлын мета өгөгдлийг үзэхийн тулд та Google Photo-г татаж авах шаардлагатай бөгөөд устгахын тулд гуравдагч талын програмыг ашиглах шаардлагатай болно.

Төхөөрөмжийн тохиргоо руу орох, эсвэл ямар нэг программ татаж авахгүйгээр мета өгөгдлийг устгаж болох бас нэг арга бол файлаа илгээхээсээ өмнө мет өгөгдөл устгах зорилгоор бүтээсэн сайтуудыг ашиглах боломжтой. Үнэгүй ашиглах хувилбаруудад файлын хэмжээ хязгаарлагдмал байдаг бөгөөд ихэвчлэн 5 МБ хүртэлх хэмжээтэй файлын мета өгөгдлийг устгах боломжтой байдаг.

Мөн Explorer ашиглан Windows үйлдлын систем дээр ийм өгөгдлийг устгахад маш хялбар байдаг.

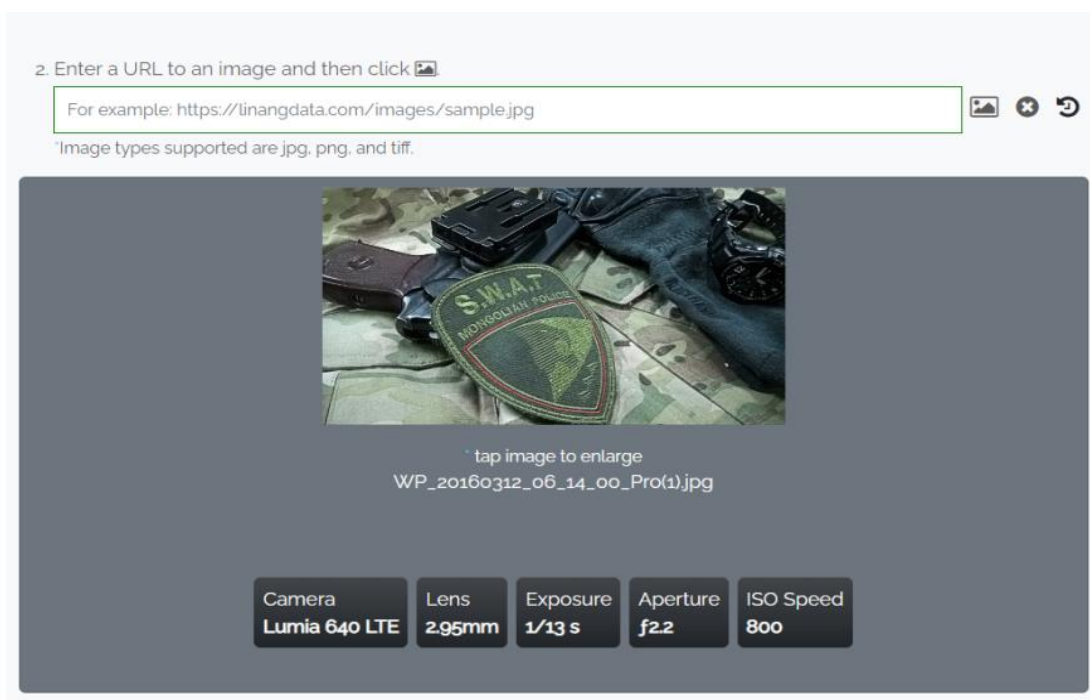
Та Windows Explorer программыг нээж, хүссэн зураг руугаа очоод хулганы баруун товчийг дараад "Properties" -ийг сонгоод, "Details" табыг сонгоод Remove properties and personal information сонголтыг дарж хялбархан устгах боломжтой.

Мета өгөгдлийг хамгаалах хамгийн сайн стратеги бол баримт бичгийг илгээхээс өмнө нууц мэдээллийг илчлэх мета өгөгдлийг устгах явдал юм. Үүнээс гадна шаардлагатай бол мета өгөгдлийг файлд хадгалахгүй байх тохиргоог программ хангамжид урьдчилан тохируулж болно.

1. <https://www.adarsus.com/en/remove-metadata-online-document-image-video/>
2. <https://www.metacleaner.com/>
3. <https://www.imgonline.com.ua/eng/delete-exif.php> зэрэг холбоосоор орж мета өгөгдлын мэдээллийг устгах боломжтой.

EXIF өгөгдлүүд нь зургийн техникийн чухал мэдээллийг агуулдаг. Тэд таны камер, утасны марк, загвар, зургийг хэзээ авсан, зураг авсан байршил тэр ч байтугай камер, зураг авахад асдаг флаш гэрлийн тохиргоог хэлж чадна.

Жишээлбэл: Ухаалаг гар утас нь GPS-ийн (Global Positioning System - Дэлхийн байршил тогтоох систем) байршлын мэдээллийг авсан зураг дээрээ суулгаж 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, хаяг байршил (зураг дарах үед GPS асаалттай байсан тохиолдолд) зэрэг мэдээллийг харах боломжтой.

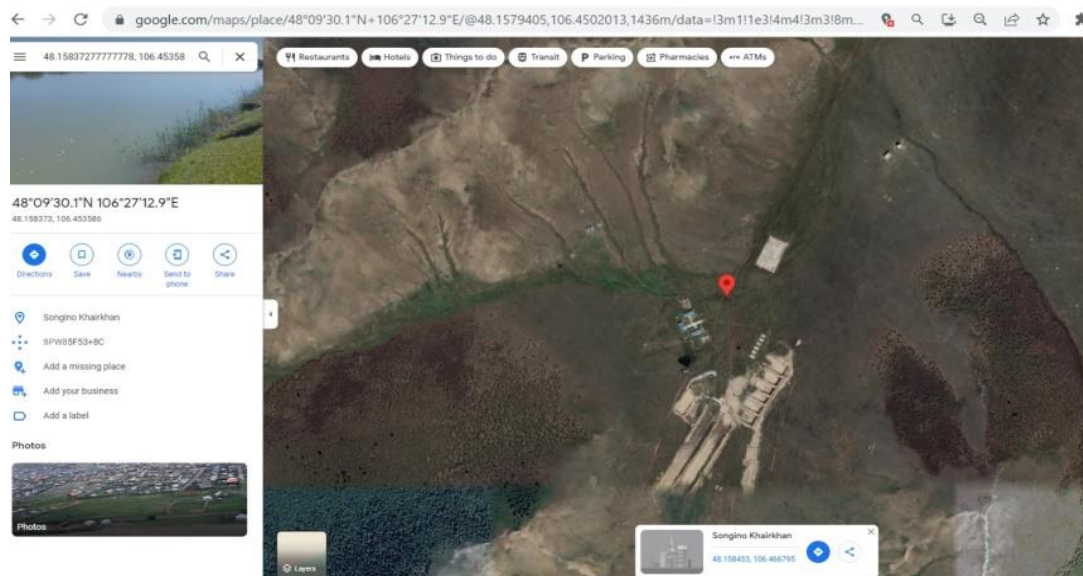


Зураг: Дээрх зургийг жишээ болгон ашиглав.

Flashpix Version	1.0
Color Space	sRGB
Image Size	3071x1728
Exposure Mode	Auto
White Balance	Auto
Focal Length (35mm Film Equivalent)	30mm
Scene Capture Type	Standard
GPS Version ID	2.2.0.0
GPS Latitude Ref	N
GPS Latitude	48.15837277777778
GPS Longitude Ref	E
GPS Longitude	106.45358555555556
GPS Altitude Ref	0
GPS Altitude	1461
GPSTimeMeasure Mode	3
GPSDOP	71744
latitude	48.15837277777778
longitude	106.45358555555556

Тухайн зургийг 2016 оны 03 дугаар сарын 12-ны өдрийн 06 цаг 14 минутад Lumia 640 LTE загварын утсаар авсан байна.

Latitude Longitude хэсэг дээр байрлах уртраг өргөргийн мэдээллийг авч www.google.com/maps дээр оруулан шалгахад Төв аймгийн Нарстайн аманд байрлах ЦЕГ-ын сургалт дадлагын төвийн байршлыг харуулж байна.



<https://linangdata.com/exif-reader/> гэх холбоосоор нэвтэрч зураг дээрх мета өгөгдлийг шалгаж үзээрэй.

Дүгнэлт

Та ямар нэг зураг файл илгээхдээ өөрийн ашиглаж буй төхөөрөмжийн программ хангамж, үндсэн тохиргоо, эсвэл бэлэн онлайн хэрэгсэл ашиглан мета өгөгдлийг устгах боломжтой талаар мэдэж авлаа. Гэхдээ мета өгөгдөл нь ялангуяа албан хэрэгцээнд маш хэрэгтэй гэдгийг бүү мартаарай. Учир нь мета өгөгдөл нь файлыг аль хэрэглэгч, ямар программ хангамж дээр үүсгэсэн, түүний ажлын нэр, үүсгэсэн огноог тодорхойлоход тусалдаг. Энэ нь файлыг хөрвүүлэх эсвэл шинэ системд ашиглах боломжийг олгож байдаг. Мөн энгийн хэрэглэгч ч гэсэн заримдаа хаана, хэзээ ямар файл үүсгэсэн эсвэл хэзээ зураг авснаа санах хэрэгтэй болдог шүүдээ. Гэхдээ нөгөө талаас авч үзвэл мета өгөгдлийн хамгаалалт байхгүй тохиолдолд гэмт этгээд таны мета өгөгдлийн мэдээллийг авч, таны эсрэг ашиглах боломжтой юм.

Жишээлбэл, гэмт этгээд кибер халдлага хийх хэрэгслээ сонгохдоо хохирогчийн ашиглаж байгаа программ хангамжийн нэр, хувилбар болон ашигладаг төхөөрөмжүүдийн талаарх бусад мэдээллийг олж авах шаардлагатай болдог. Таны нийгмийн сүлжээнд тавьсан жирийн нэг зураг гэмт этгээдэд дээрх мэдээллүүдийг өгч энэ хорт санаа бодлоо амжилттай хэрэгжүүлэхэд нь тусалж байж болох 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>