National Datacenter

ХАЛДЛАГАД ХАРИУ ҮЙЛДЭЛ ҮЗҮҮЛЭХ БАГ

2017 он

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЧИГ ХАНДЛАГА ХААШАА ЧИГЛЭНЭ ВЭ?

Мэдээллийн технологийн ертөнцөд шинэ техник технологи бий болон, хүний амьдралд хэвшихийн хирээр түүний аюулгүй байдлыг хэрхэн хангах талаар асуудал урган гардаг. Өөрөөр хэлбэл олны анхаарлыг татаж байгаа обьект руу эсрэг талынхан ч гэсэн анхаарлаа хандуулдаг байх нь. Яг л үүнтэй адил хүмүүс бидний амьдралд асар богино хугацаанд хэвшил болон заншсан сошиал медиа, андройд төрлийн гар утас, сүлжээ, үүлэн тооцооллын үйлчилгээнүүдийн аюулгүй байдлыг хангах нь өнөө цагийн чухал асуудал болжээ. Өнгөрөгч 2012 онд ч гэсэн цахим ертөнцийн аюулгүй байдалд дээрхи чиглэлийн аюулгүй байдлыг хангах нь олон улсад шинэ хандлага болсон гэхэд хилсдэхгүй болсон байна.

Олон улсын мэргэжилтнүүд дэвшилтэт технологийн чанар чансаа сайжрахын хирээр түүнд хариу халдлага үзүүлэх хортой вирусын хүчин чадал давхар чангарч, улам зохион байгуулалттай, стратегийн шинж чанартай болсон гэж үзэж байгаа юм. Үүнтэй уялдуулаад олон улсын байгууллагууд өөрийн цахим хамгаалалтаа давхар давхар хамгаалалт хийж эхэлжээ. Дэлхийн нийтийн ихэнхи бизнесийн байгууллагууд ухаалаг гар утас, андройд төрлийн утас, таблетуудын сүлжээнд давхар шинэ хаягжилт өгч, мэдээллийн аюулгүй байдлын тоног төхөөрөмж үйлдвэрлэгч байгууллагууд ч гэсэн Java, Flash технологийн тоног төхөөрөмжийн эмзэг сул цоорхой цэгүүдийг тодорхойлон, улам илүү хамгаалалт сайтайгаар дараагийн хувилбаруудаа үйлдвэрлэн гаргаж байгаа юм.

Одоо та бүхэнд нэгэн жишээ дурдъя. Кибер гэмт хэргийн хууль сахиулагч байгууллагууд ОХУ-д болсон 4,5 сая компьютерийн бодийг нь хөтөлж, тус улсын банкны системд нэвтэрч улмаар Арменд байрлах салбар банкны төлбөр тооцооны системийг доголдуулсан “Bredoloab botnet” вируснаас гаралтай хэргийг илрүүлж, зохих арга хэмжээг авсан явдал байсан юм. Бас нэг тод жишээ нь Майкрософт компанийн шинжээч нар БНХАУ-ын динамик домэйн нэрийн систем /DNS/-д суурилсан халдлага болох “Nitol botnet” төрлийн амьсгалын замын халдварт өвчин мэт тархасан цахим гэмт хэргийн гол шалтгааныг илрүүлсэн нь онц чухал байлаа.

2013 онд мэдээллийн технологийн салбар виртуалчлал буюу хийсвэр хэлбэр лүү шилжсэн бөгөөд мобайл төрлийн цахим халдлагууд нь ихэсч байгаа явдал юм. Энэ нь бүхий л төрлийн мэдээллийн технологийн байгууллагууд, түүний хэрэглэгчид, энэ төрлийн үйлчилгээ үзүүлэгч байгууллагууд өөр хоорондоо ялгаатай тоног төхөөрөмж, девайс, дэд бүтцээ улам илүү системжүүлж, аль ч төрлийн халдлагад автахааргүй дархлаа тогтоох явдал юм.

Сошиал медиатай холбоотой цахим халдлагуудын тухайд

1 тэрбум гаруй хэрэглэгчидтэй олны анхаарлын төвд байдаг Фейсбүүк саяханаас өөрийн шинэ интерфейс болох Timeline-тай болсон билээ. Эсрэг талын нөхдүүд ч гэсэн энэ боломжийг ашиглан уг сүлжээг хэрэглэгчдийн зураг, төрөл бүрийн пост, шуудан зэргийг онилон цахим дайралтууд хийсээр байна. Мөн түүнчлэн, богино хугацаанд мэдээ мэдээлэл дамжуулагч Твиттер жиргээчдийн амар тайван байдлыг алдагдуулах халдлагыг ч гэсэн хийж байна.

Уг сэжимтэй холбогдуулаад 2012 оны 9 сард сошиал медиа сүлжээг ашиглаж буй онлайн хэрэглэгчдийн хувийн профайл хуудас нь руу нэвтрэн тухайн хэрэглэгчийн найзууд руу нь өөрийн хуудас дээр нь пост хийхийг хүссэн илгээмж явуулж, улмаар үүнийг хүлээн авсан хэрэглэгч идэвхижүүлсэнээр Youtube player-ээр төрөл бүрийн видео бичлэг үзэх боломж бий болж түүгээр дамжин Troj/Mdrop-EML Trojan төрлийн вирус тархадаг байна.

1 тэрбум гаруй хэрэглэгчидтэй олны анхаарлын төвд байдаг Фейсбүүк саяханаас өөрийн шинэ интерфейс болох Timeline-тай болсон билээ. Эсрэг талын нөхдүүд ч гэсэн энэ боломжийг ашиглан уг сүлжээг хэрэглэгчдийн зураг, төрөл бүрийн пост, шуудан зэргийг онилон цахим дайралтууд хийсээр байна. Мөн түүнчлэн, богино хугацаанд мэдээ мэдээлэл дамжуулагч Твиттер жиргээчдийн амар тайван байдлыг алдагдуулах халдлагыг ч гэсэн хийж байна.

Уг сэжимтэй холбогдуулаад 2012 оны 9 сард сошиал медиа сүлжээг ашиглаж буй онлайн хэрэглэгчдийн хувийн профайл хуудас нь руу нэвтрэн тухайн хэрэглэгчийн найзууд руу нь өөрийн хуудас дээр нь пост хийхийг хүссэн илгээмж явуулж, улмаар үүнийг хүлээн авсан хэрэглэгч идэвхижүүлсэнээр Youtube player-ээр төрөл бүрийн видео бичлэг үзэх боломж бий болж түүгээр дамжин Troj/Mdrop-EML Trojan төрлийн вирус тархадаг байна.

Үүлэн тооцооллын үйлчилгээтэй холбоотойгоор үүсч буй эрсдэлүүд

Манай Монгол улсад сүүлийн үед үүлэн тооцоолол гээч шинэ технологи олны сонорыг нь мялаагаад багагүй хугацаа өнгөрч байна. Дотоодын зах зээлд ч гэсэн энэ чиглэлээр дагнан үйлчилгээ үзүүлэгч байгууллагууд шил шилээ даган нэмэгдэж байна гэхэд хилсдэхгүй биз ээ. Тэгвэл олон улсад уг технологи аль хэдийн өөрийн байр суурыа олж, сэдэв нь хуучирч үүний аюулгүй байдлыг хэрхэн хангах талаар шинжээч, мэргэжилтнүүд оюун ухаанаа зарцуулж байна.

Төрөл бүрийн компани, аж ахуйн нэгжүүд өөрийн мэдээллийн технологио улам боловсронгуй болгож, хийсвэр хэлбэр лүү шилжүүлж, private cloud-ийн шийдэлтэй болсон байна. Төрөл бүрийн мэдээ мэдээлэл, файл, видео бичлэг дамжуулах чадвартай Dropbox-руу халдлага

хийн, тухайн хэрэглэгчийн нэр, нууц үгийг ашигладаг бөгөөд халдлага хийгч этгээдүүдэд ихэвчлэн хүмүүс бүх төрлийн бүртгэлүүд дээрээ өөр хоорондоо ижил төрлийн нууц үг, хэрэглэгчийн нэр ашигладаг нь өгөөш болж, үүнийг ашиглан Dropbox-ийн эсрэг төрөл бүрийн халдлага хийдэг ажээ.

Мөн түүнчлэн, Dropbox болон зарим төрлийн цахим хуудсууд нь өгөгдөл хадгалах, түүнийг дамжуулах үйлдэлд өгөгдөл шифрлэх боломжтой байдаг бөгөөд энэ нь хэрэглэгчийн нэвтрэх эрхийг хамгаалж чадна гэсэн үг биш юм аа.

Андройд утасны эргэн тойронд

Өнгөрөгч оны байдлаар дэлхий дээр 100 сая гаруй хүмүүс андройд, ухаалаг гар утас хэрэглэж байна гэсэн судалгаа гарсан бөгөөд уг төрлийн утасны зах зээлийн 52,2 хувь нь хэрхэн өөрийн дархан цаазат байдлаа хамгаалж үлдэх вэ? гэсэн асуулттай тулгараад байгаа юм. Андройд вирусны нэг төрөл болох Андр/ Боксер нь халдлагуудын бүртгэлээс хамгийн дээгүүр байрыг эзэлжээ.

Тухайлбал .ru өргөтгөлтэй домэйн нэрийн хост нь Украйнд байршдаг бөгөөд ОХУ-ас Андр/ Боксер төрлийн вирустай мессежийг Баруун Европын орнуудын андройд утас хэрэглэгчид рүү сайхан бүсгүйчүүдийн зурагтай сайт руу хандах холбоосыг илгээжээ. Улмаар уг холбоосыг идэвхижүүлсэнээр тухайн андройд утас вирустай аппликейшнүүд суулган авч, тухайн утсыг эзэмшигч этгээдийн бүхий л мэдээллийг мэдэж болох аюул нүүрлэдэг ажээ. Хэрэв тухайн хэрэглэгч нь Опера, Скайп төрлийн хуурамч аппликейшн суулгавал шууд Орос улсаас хандсан байна гэдэг нь тодорхой болох магадлалтай байдаг.

Зарим тохиолдолд хуурамч антивирусны програм идэвхижиж, жинхэнэ вируснуудыг илрүүлдэггүй тохиолдол ч бий аж. Саяханаас хуурамч програм хангамж суулгах үйлдлээс үүдсэн халдлагууд Андройд гар утсан дээр илрээд байгаа нь энгийн үзэгдэл болсон байна. Тухайлбал маш олон хэмжээгээр гэнэт дүрс зураг бий болгож хамгаалалтын системийг төөрөгдүүлэн олон төрлийн хорт вирусыг бий болгодог байна.

Мөн түүнчлэн уг утсанд төрөл бүрийн тоглоомын аппликейшн сууснаар халдлагад өртөх боломжийг бас бий болгодог. Мөн “Ginger Break” мэтийн хуурамч програм хангамж нь нэмэлт хортой кодуудыг суулгах, алсын хандалтаар цахим хуудсанд холбогдож янз бүрийн хортой вирус татах зэргээр үндсэн гол хандалтыг эвдэлдэг. Дээрхи байдал үүссэнээр Трожан мэтийн хортой вирусыг идэвхижүүлж, олон улсын ботнет төрлийн халдлагад өртүүлэх боломжийг олгодог.

Андройд төрлийн гар утсанд ирж буй мессежүүдийг өөр төрлийн серверүүд чих тавин ажиглаж байдаг ч тал бий. Уг төрлийн мэдээлэл хулгайлах үйлдэл нь байгууллага, пүүс компаниудад маш

их хэмжээний хохирол учруулдаг. Өнөө үед ажил албаа богино хугацаанд амжуулахын тулд онлайн, интернэт банкны системийг ихээхэн ашиглах болсонтой холбогдуулан хэрэглэгчид рүү банкны системээс ирүүлж буй данс руу нэвтрэх эрх, нууц үг зэргийг *Andr/Zitmo /Blackberry төрлийн гар утсанд байдаг аппликейшн/* вирусаар дамжуулан мэдэх боломжтой байдаг байна. Ийнхүү тухайн данс эзэмшигчийн бүхий л мэдээллүүдийг мэдсэнээр өөр этгээд мөнгөн гүйлгээ хийх боломж бүрддэг байна.

Дүгнэлт

Орчин цагийн мэдээллийн аюулгүй байдал дээрхи хэдэн чиглэлийн халдлагуудаар хязгаарлагдахгүй бөгөөд бид зөвхөн цөөн хэдийг нь л хөндлөө. Энэ бүхнээс өмнөх технологийн эринд механик ажиллагаа шаарддаг техник технологийн үед мэдээ мэдээллийг хулгайгаар олж авах нь болхи байсан юм шиг санагдана. Цаг хугацаа өнгөрч эргэн тойрны эдэлж хэрэглэдэг зүйлсүүд маань автомат, бүр цаашлаад хийсвэр буюу интернэт сүлжээнд холбогдон улам боловсронгуй болсоноор нийгэмд нөгөө л байсаар л байсан гэмт хэргүүд маань хүний нүднээс далд, хийсвэр орчинд шилжиж байгаа нь бас л ухаалаг болсоны шинж биз ээ.

Тиймээс бид сүлжээнд л холбогдож л байгаа бол тэдгээр тоног төхөөрөмж, харилцах данс, андройд утсаар ирж буй төрөл бүрийн аппликейшний хүсэлт, бусад системд хандах эрхийнхээ хэрэглэгчийн нууц үгээ хүүхдийнхээ төрсөн өдөр, өөрийн овог нэр, дараалсан цифр, гэр бүлийн гишүүний нэрийг өгч залхууралгүйгээр олон тэмдэгт, ямар нэгэн утга агууламжгүй үг, олон үсгийн цуглуулга, дунд нь том жижиг үсэг хийн аль болох урт нууц үг хийх хэрэгтэй.