“Буллетпруф” хостинг үйлчилгээ үзүүлэгчид: Цахим гэмт хэргийн системийн дэд бүтцийн хамгаалалтын ан цав

Мэргэжлийн цахим гэмт хэрэгтнүүд аюулгүй, илрүүлэх боломжгүй, уян хатан дэд бүтцэд найддаг. Сүлжээг халдварлуулах, нэвтрэх мэдээлэл хулгайлах, рансомвэр хортой програм тараах, мэдээлэл хулгайлах, хууль бус форум дээрх худалдаа гэх мэт бүхий л үйлдлийн ард цахим гэмт хэрэгтнүүдийг далд байдлаар үйл ажиллагаагаа явуулахад тусалдаг системийн дэд бүтэц оршдог.

Гэсэн хэдий ч цахим гэмт хэрэгтнүүдийн хувьд илрэхгүй хэвээр байх, мөн хяналтаас бултах нь улам хүндрэлтэй болсоор байна. Дэлхийн улс орнуудын Засгийн газар, хууль сахиулах байгууллага болон хувийн хэвшил хоорондын хамтын ажиллагаа нь кибер гэмт хэрэгтнүүдийг цахим орчинд нуугдах боломжийг улам хязгаарлаж байна. Түүнчлэн, тун цөөн тооны кибер гэмт хэрэгтнүүд л системийн аюулгүй дэд бүтцийг бие даан удирдаж, ажилуулах мэдлэг, ур чадварыг эзэмшсэн байдаг. Ийм учраас, тэд тус үйлчилгээг өөрсдийнх нь өмнөөс үзүүлэх хууль бус системийн дэд бүтэц нийлүүлэгчдийг хайж, харин өөрсдөө хохирогчид болон ашиг олох ажиллагаандаа илүү төвлөрдөг.

‘Кибер гэмт хэргийн үйлчилгээ’ гэдэг нь төрөл бүрийн хортой цахим халдлага үйлдэгч этгээдүүдийг дэмжих зорилгоор бий болсон далд зах зээл юм. Энэхүү хууль бус далд зах зээл дээр гэмт хэрэгтнүүдэд цахим халдлага үйлдэхэд нь дэмжлэг болох, худалдан авч болохуйц төрөл бүрийн хэрэгсэл, үйлчилгээ, мэдээллүүд байдаг бөгөөд эдгээр нь тасралтгүй өсөн нэмэгдэж, хувьсан өөрчлөгдсөөр байна. Цахим гэмт хэрэг үйлдэхийг зорьж буй этгээдүүд сүлжээнд нэвтрэх эрх, аюулгүй байдлын системээс зайлсхийх хэрэгслээс гадна хохирогчдын эсрэг ашиглах, хувийн мэдээлэл хулгайлахад ашигладаг хорт программ худалдан авдаг. Буллетпруф хостинг (BPH) үйлчилгээ үзүүлэгчид нь энэ хууль бус экосистемийн нэг хэсэг бөгөөд цахим гэмт хэрэгтнүүдийг хамгааллын системийн дэд бүтцээр хангадаг. Нэг BPH үйлчилгээ үзүүлэгч л гэхэд хэдэн зуун гэмт хэрэгтнүүдийг дэлхийн өнцөг бүрт халдлага хийхэд нь тусалж чадна.

“Буллетпруф” хостинг үйлчилгээ үзүүлэгч гэж юу вэ?

Энгийнээр хэлбэл, BPH үйлчилгээ үзүүлэгчид кибер гэмт хэрэгтнүүдэд виртуал болон бодит дэд бүтцээ түрээслүүлдэг. BPH үйлчилгээ үзүүлэгчид нь аюултай этгээдүүдэд (үүнд кибер гэмт хэрэгтнүүд орно) интернэт орчинд хууль бус контент байршуулж, гэмт хэргийн шинжтэй үйл ажиллагаа явуулах боломжийг олгодог системийн дэд бүтцийн тусгай ангиллын үйлчилгээ юм.

“Буллетпруф” гэх нэршил нь цэвэр маркетингийн хэллэг юм. Үнэн хэрэгтээ, ийм төрлийн үйлчилгээнүүд бусад системийн дэд бүтцийн адил саатал, тасалдалд өртөх магадлалтай. Харин, BPH үйлчилгээ үзүүлэгчид нь хууль сахиулах байгууллагын шаардлага, хууль бус агуулгыг устгах хүсэлт, хохирогч болон хэрэглэгчдийн гомдлыг үл тоомсорлодог. Ингэснээр кибер гэмт хэрэгтнүүд хууль сахиулах байгууллага болон бусад этгээдүүдийн шаардлагаар системийн дэд бүтцийн ашиглалтыг цуцлах вий гэсэн айдасгүйгээр харилцаа холбоо тогтоох, хууль бус форум болон вэбсайт ажиллуулах, хорлонтой болон фишинг халдлага зохион байгуулах, мөнгө угаах зэрэг хууль бус үйл ажиллагааг явуулж чаддаг.

BPH үйлчилгээ үзүүлэгчид кибер гэмт хэргийн экосистемд зориудаар оролцож, санхүүгийн зорилготой онц ноцтой цахим гэмт хэрэг үйлдэх боломж олгодог. Австралийн байгууллагууд, тэдгээрийн хэрэглэчдийг чиглэсэн олон кибер халдлага BPH-д түшиглэж хийгдсэн. Үүний уршгаар рансомвэр хортой программын халдлага, мэдээлэл луйвардах, хувийн мэдээлэл хулгайлах зэрэг онц ноцтой хэргүүд гарсаар байна.

Буллетпрүф хостинг үйлчилгээ үзүүлэгчийн сурталчилгаа доод түвшний форумууд дээр харагдах байдал:

BPH үйлчилгээ үзүүлэгчид яаж ажилладаг вэ?

BPH үйлчилгээ үзүүлэгчдийн үйл ажиллагааны загвар харилцан адилгүй. Хамгийн түгээмэл арга нь кибер гэмт хэрэгтнүүдэд IP хаяг түрээслүүлж, тэдний байршил, таних тэмдэг болон үйл ажиллагааг нуухын тулд сүлжээ солих нарийн аргуудыг ашигладаг. Ихэнх тохиолдолд, BPH үйлчилгээ үзүүлэгчид хууль ёсны хостинг үйлчилгээ үзүүлэгч, дата төв эсвэл интернэт үйлчилгээ үзүүлэгч (ISP) байгууллагуудаас түрээслэн авсан IP хаяг болон серверийг дамлан зарж эсвэл дахин түрээслүүлдэг. Эдгээр 'дээд түвшний' (upstream) үйлчилгээ үзүүлэгчид нь тэдний нийлүүлсэн дэд бүтцээр дамжуулан BPH үйлчилгээ үзүүлэгчид цааш нь 'доод түвшний' (downstream) буюу кибер гэмт хэрэгтнүүдэд үйлчилгээ үзүүлж байгааг мэдээгүй байх тохиолдол олон.

ВРН үйлчилгээ үзүүлэгчид үйлчлүүлэгчдийнхээ нууцлалыг хангах зорилгоор өөрсдийн сүлжээ, системийн хийцлэлдээ тохиргоо хийдэг. Жишээлбэл, тэд үйлчлүүлэгчиддээ хуваарилсан IP хаяг, домэйн нэр зэрэг үйлчлүүлэгчдийн үйл ажиллагаатай холбоотой, интернэтэд ил харагдах танигч мэдээллийг тогтмол өөрчилдөг. Эдгээр арга техник нь халдлага үйлдсэн этгээдийг тухайн үед ашигласан IP хаягтай нь холбоход хүндрэл учруулдаг тул хамгаалалт болон, мөрдөн байцаалтад саад болдог. Түүнчлэн ВРН үйлчилгээ үзүүлэгчид кибер үйл ажиллагааг мөрдөн шалгах, урьдчилан сэргийлэх албан ёсны арга хэмжээ байдаггүй эсвэл хангалтгүй кибер аюулгүй байдлын хяналт сул, эсвэл огт байхгүй улс орнуудад байрлах системийн дэд бүтцийг ашигладаг.

ВРН үйлчилгээ үзүүлэгчид хууль ёсны дэд бүтцийн үйлчилгээ үзүүлэгчдээс юугаараа ялгаатай вэ?

ВРН үйлчилгээ үзүүлэгчдэд чиглэсэн арга хэмжээ нь кибер гэмт хэргийн аюулгүй заналд хэрхэн нөлөөлдөг вэ

ВРН үйлчилгээ үзүүлэгчид нэгэн удаадаа хэдэн зуугаас хэдэн мянга хүртэлх кибер гэмт хэрэгтний үйл ажиллагааг тасалдуулах боломжтой. Кибер гэмт хэрэгтнүүд болон бусад аюултай цахим этгээдүүд эдгээр үйлчилгээг ашигласнаар хууль бус үйлдлээ илүү хялбар хэрэгжүүлэх боломжтой болдог бөгөөд тэдний үйл ажиллагаа гомдол, шаардлагыг үл харгалзан үргэлжилсээр байх болно гэсэн итгэлтэйгээр ажилладаг.

Гэвч, хууль сахиулах байгууллагууд, Засгийн газрын агентлагууд, хувийн хэвшлүүд хамтран ажиллаж, энэ төрлийн хууль бус дэд бүтцийн үйлчилгээ үзүүлэгчдийг илрүүлэх, үйл ажиллагааг нь тасалдуулах чиглэлээр арга хэмжээ авч байна. Үүнд, одоогоор ил байгаа BPH үйлчилгээ үзүүлэгчдийн интернэт урсгалыг хаах зэрэг хамгаалалтын арга хэмжээ орно. Эдгээр үйл ажиллагаа нь Австрали болон түншүүдийн сүлжээнд чиглэж буй кибер гэмт хэргийн тоог бууруулахад хувь нэмэр оруулдаг түүний бөгөөд BPH үйлчилгээ үзүүлэгчдэд интернетэд нэвтрэх болон кибер гэмт хэрэгтнүүдэд дэд бүтэц ашиглуулах боломжийг нь мэдэлгүйгээр олгож байгаа хууль ёсны ‘дээд түвшний’ (upstream) дэд бүтцийн үйлчилгээ үзүүлэгчид болон интернет үйлчилгээ үзүүлэгч байгууллагуудыг хамардаг.

BPH үйлчилгээ үзүүлэгчид нь кибер гэмт хэрэгт зориулсан үйлчилгээний экосистем дэх цорын ганц төрлийн дэд бүтцийн үйлчилгээ үзүүлэгч биш юм. Эдгээр үйлчилгээ нь кибер гэмт хэрэгтнүүдийн үйл ажиллагааг идэвхтэй дэмжиж, хууль ёсны мөрдөн шалгалт болон хариу арга хэмжээг зориудаар саад учруулах замаар Австрали улсын кибер аюулгүй байдалд заналхийлж байна. BPH үйлчилгээ үзүүлэгчдийн эсрэг арга хэмжээ авснаар эдгээр үйлчилгээ болон тэдгээрийг ашигладаг кибер гэмт этгээдүүдийн сул талыг онцлон харуулж байгаа юм.