National Datacenter

РийлФиш[1]**: Бодит хугацааны, *хоёр хүчин*[2] зүйлийн *фишинг*[3]**

Сошиал Инженерчлэл* ба *Хоёр-Хүчин зүйлийн баталгаажуулалт

Сошиал инженерчлэл ажиллагаа нь аюулгүй байдлын бүрэлдэхүүн дундаас хамгийн сул цэг болох хүнийг өөрийн бай болгодог учраас бизнест байнга аюул заналхийлэл үзүүлсээр байдаг. Ийм төрлийн, энгийн халдлагын үед хохирогч этгээдийн хэрэглэгчийн нэр, нууц үгийг олж авч улмаар дараа нь халдлага үйлдэхэд ашиглах зорилгоор хадгалдаг. *Хоёр-Хүчин зүйлийн баталгаажуулалт /2FA/* (эсвэл *Олон хүчин зүйлийн баталгаажуулалт*[4] */MFA/*)-г энэ төрлийн халдлагаас сэргийлэх шийдэл хэмээн үздэг юм.

2FA нь энгийн хэрэглэгчийн нэр болон нууц үг гэсэн хослол хамгаалалт дээр дахин нэмэлт нэг хамгаалалтын түвшин нэмдэг юм. *2FA* -ын олон шийдлээс хамгийн түгээмэл хэрэгжсэн байдаг шийдлүүд нь *нэг удаагийн нууц үг*[5] мөн *дээр нь дарах зориулалт бүхий анхааруулга*[6] юм. *Нэг удаагийн нууц үг* нь үндсэн төхөөрөмжөөс өөр төхөөрөмж дээр үүсдэг (жишээлбэл техник хангамжид суурилсан токен) бөгөөд тухайн нэг хэрэглэгчтэй холбогдсон байдаг. Ийнхүү үүссэн нэг удаагийн нууц үг нь ихэвчлэн 30-аас 60 секунд хүртэл хүчинтэй байх бөгөөд дахин ашиглагдах боломжгүй байдаг.

Дээр нь дарах зориулалт бүхий анхааруулга нь хэрэглэгчийн гар утас руу сануулга илгээх бөгөөд тухайн сануулга нь таны хаяг руу нэвтрэх оролдлого хийгдэж буйг анхааруулахын зэрэгцээ тухайн нэвтрэх оролдлогыг зөвшөөрөх функцийг агуулдаг. Энэхүү

---

[1] ReelPhish - Аюулгүй байдлын судлаачдын гаргасан, хоёр хүчин зүйлт баталгаажуулалтыг даван гарах фишинг програм

[2] Two Factor - 2FA - Энгийн баталгаажуулалтын механизм дээр нэмэлт нэг түвшин нэмж оруулсэн баталгаажуулалтын механизм

[3] Phishing - Хэрэглэгчийг хуурч нэврэх нэр, нууц үг гэх мэт эмзэг мэдээллийг хулгайлан авах халдлагын арга

[4] Multi factor Authentication - Олон хүчин зүйлт баталгаажуулалт, баталгаажуулалт хийхдээ нэгээс олон хүчин зүйлийг шалгадаг арга

[5] One Time Password - Нэг удаагийн нууц үг. Ихэвчлэн 30-60 секундын хугацаа бүхий ганц удаа хэрэглэх зориулалт бүхий нууц үг

[6] Push notification - Хэрэглэгчийн хөдөлгөөнт төхөөрөмж рүү сануулга илгээдэг олон хоёр хүчин зүйлийн баталгаажуулалт

хоёр шийдэл нь уламжлалт *фишинг* халдлага (хэрэглэгчийн нэвтрэх нэр, нууц үгийн хослол хулгайлах)-аас хэрэглэгчийг хамгаалж чадаж байгаа юм.

Бодит хугацааны фишинг

Аюулгүй байдлын мэргэжилтнүүд өөрийн хувийн болон арилжааны зориулалтаар ашиглаж буй аппликэшн бүрдээ *2FA*-г ашиглахыг зөвлөж байгаа хэдий ч энэ шийдэл маань төгс шийдэл бас биш юм. *2FA* -г бодит хугацааны фишинг хийх техник ашиглан амжилттай давж гарсан байна. Энэ төрлийн фишингийн үед, хакер болон хохирогч хоорондоо нэг агшинд харилцдаг юм.

Энгийн жишээ дурдвал, Хэрэглэгчээс нэр нууц үг болон нэг удаагийн нууц үгийг нь асуудаг фишинг веб сайт юм. Хэрэглэгч баталгаажуулалтын механизмыг амжилттай дуусгамагц, эдгээр сайтууд нь хэрэглэгчид “Хандалт амжилттай болсон[7]” гэсэн мессеж бүхий ерөнхий хуудсыг харуулах ба улмаар нэг удаагийн түлхүүрийг ашиглалгүйгээр хадгалж авдаг. Энэ хүртэл амжилттай халдлага үйлдсэн этгээдэд хэрэглэгчийн *нэг удаагийн нууц үг*-ийн хүчинтэй хугацаа дуусахаас өмнө ашиглан нэвтэрч орох богинохон хугацаа гарч ирнэ.

Сошиал инженерчлэл -д ийм арга хэрэглэх нь цоо шинэ ойлголт биш юм. 2010 оны эхээр, *бодит хугацааны фишинг* буюу ийм техник ашиглан халдлага үйлдэж байсан тайлан байдаг юм. Гэвч энэ техникийг ашиглан халдлага хийх нь төвөгтэй, хүндрэлтэй байдаг учраас олон нийт анхааралгүй өнгөрөөсөн юм. Энэ нийтлэл нь хуучны хандлагыг өөрчилж, бодит тулгараад буй асуудалд анхаарал хандуулах, шинэ шийдлийн эрэлхийлэхийг дэмжих зорилготой юм.

***Бодит хугацааны фишинг* програм хэрхэн ажилладаг вэ?**

Сошиал инженерчлэл-ийн үнэлгээг сайжруулахын тулд бид РийлФиш гэгдэг програмыг хөгжүүлсэн юм. Энэхүү програм нь *бодит хугацааны фишинг* -ийг хялбарчлах

[7] Login successful - Амжилттай нэвтэрч орсон гэдгийг илтгэх веб хуудас

юм. Энэ програмын хамгийн чухал бүрэлдэхүүн хэсэг нь хакерын компьютер дээр ажиллах юм. Энгийнээр бол энэ нь хакерын тохируулсан фишинг сайтаас өгөгдөл ирэхийг хүлээх ба ирмэгц нь түүнийгээ *Селениум фрэймворк*[8]

ашиглан локал веб хөтөч рүү чиглүүлэх үйлдэл хийдэг *Пайтон*[9] скрипт програм юм.

Энэ програм нь хакерын веб хөтчийг тухайлан зааж өгсөн веб хуудаснууд руу чиглүүлэх, түүний HTML объектуудтай[10] нь харилцан ажиллаж, мэдээллийг нь ялгаж авах зэргээр техник ашиглан хакерын компьютерын веб хөтчийг удирдах чадвартай юм.

РийлФиш -ийн хоёр дахь үндсэн бүрэлдэхүүн хэсэг нь фишинг сайт юм. Фишинг сайтад шигтгэгдсэн код нь хохирогч этгээдийн нэвтрэх нэр, нууц үг гэх мэт мэдээллээ фишинг програмын үндсэн бүрэлдэхүүн хэсэг ажиллаж буй хакерын компьютер луу илгээдэг. Фишинг програм нь мэдээллийг хүлээн авмагцаа, *Селениум*-ыг ашиглан веб хөтчийг ачаалж, хууль ёсны жинхэнэ сайт руу нь хэрэглэгчийн өмнөөс баталгаажуулалт хийн нэвтэрдэг. Хакерын компьютер болон Фишинг веб серверийн хооронд илгээгдэж буй бүх мэдээлэл нууцлагдсан SSH туннелиэр дамждаг.

Хохирогч этгээдийг Фишинг сайт болон *РийлФиш*-ийн холболтод байх сешин токен ашиглан мөшгөдөг. Олон хуудас рүү баталгаажуулалт хийх үед энэ токен нь фишинг програмаас баталгаажуулалтын төлөвийг хадгалж байх боломжийг олгодог. Энэ фишинг програм нь төлөв хадгалдаг учраас, хохирогч этгээдээс хууль ёсны веб баталгаажуулалтын портал руу эсвэл эсрэг чиглэлтэй мэдээлэл илгээх боломжтой.

Жишээ нь:

Бид *РийдФиш* болон энэ технологийг *Мэндиэнт Ред баг*[11]ийн олон ажиллагаанд амжилттай ашигласан. Хамгийн түгээмэл тохиолдол нь *Хоёр-Хүчин зүйлийн баталгаажуулалт* бүхий VPN портал байсан юм. Сошиал инженерчлэлийн даалгавар гүйцэтгэхийн тулд, бид бодит VPN порталын HTML, JavaScript, CSS-г хуулбарлан авсан.

[8] Selenium Framework - Селениум Фрэймворк, Веб аппликэшн тест хийх зориулалт бүхий фрэймворк

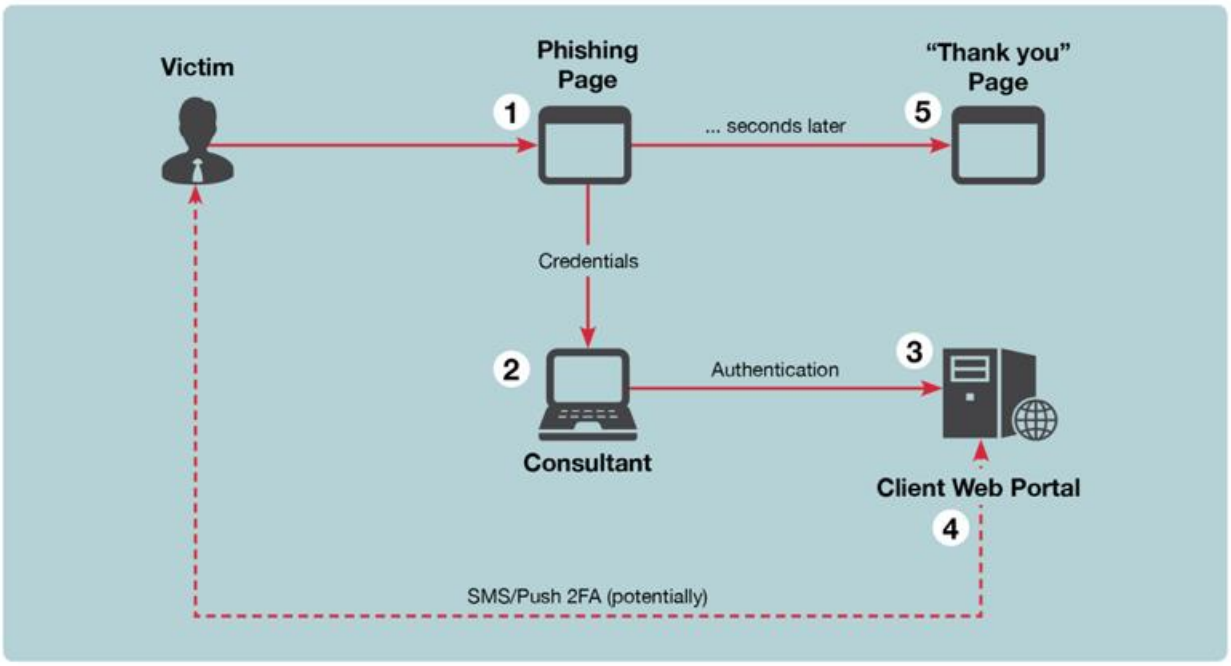
[9] Python - Програмчлалын хэл

[10] HTML objects - Hypertext Markup Language буюу веб хуудас харуулах хэлний обьектууд

[11] Mandiant Red Team - Сошиал инженеринг хийж байгууллагын аюулгүй байдлыг шалгадаг баг

Энэхүү хуулбарлан авсан эх кодоо бид фишинг сайтыг жинхэнэ сайттай нь ижилхэн функц хийж буй мэт харагдуулахад ашигласан юм.

Бодит хугацааны фишингийг хялбархан болгохын тулд, бид хакерын компьютертой холбогдох фишинг сайт дээр сервер талын кодыг шигтэж өгсөн. Түүнээс гадна, бид фишинг сервер дээр SSH туннель тохируулж өгсөн. Фишинг сайт дээрх баталгаажуулалтын форм бөглөгдөх үед хэрэглэгчийн оруулсан баталгаажуулалтын мэдээлэл (нэвтрэх нэр, нууц үг, нэг удаагийн нууц үг гэх мэт бүх мэдээлэл) хакерын компьютер руу SSH туннелиэр дамжуулагдана. Улмаар хакерын талд ажиллаж буй фишинг програм нь веб хөтчийн шинэ процессыг ачаалалж жинхэнэ VPN портал руу хэрэглэгчийн баталгаажуулалтын мэдээллийг ашиглан нэвтэрнэ. Зураг 1-т энэ процессыг тайлбарлан харуулав.



Зураг 1: РийлФиш -ийн ажиллагааны бүдүүвч зураг

Бид VPN портал сайтууд дээр *Хоёр-Хүчин зүйлийн баталгаажуулалт*-ын олон төрлийн шийдлийг харж байсан. Зарим тохиолдолд токен нь баталгаажуулалтын формынхоо талбарт (Field) “Хоёр дахь нууц үг” байдлаар дамжуулагддаг. Бусад тохиолдолд, хэрэглэгч нь гар утаснаасаа ирсэн сануулга дээр дарах тохиолдол ч гэсэн байдаг. Хэрвээ фишинг сайт нь жинхэнэ сайтаасаа ялгагдахгүй байгаа тохиолдолд, хэрэглэгч өөрийн гар утсанд ирсэн нэвтрэх сануулгыг зөвшөөрөх магадлал өндөр юм.

Зарим нөхцөлд тохируулан, бид илүү ахисан түвшний фишинг сайтыг хөгжүүлсэн бөгөөд энэ нь баталгаажуулалтын олон хуудсыг хүлээн авах боломжтой бөгөөд фишинг веб сервер болон хакерын компьютерын хооронд мэдээлэл дамжуулан удирдах чадвартай юм.

Бидний скрипт нь ийм нөхцөл байдлыг удирдахдаа, фишинг сайт дээр байх хохирогч этгээдийн сешинийг мөшгөж, түүнийгээ хакерын компьютер дээр ажиллах веб хөтчийн процесстой холбож өгснөөр хийж байгаа юм.

Зураг 1-т бидний бүтээсэн халдлага үйлдэх програм хэрхэн ажиллах ерөнхий схемийг харуулсан.

Бид энэхүү програмаа FireEye GitHub Repository-д нийтэд нээлттэйгээр байршуулж байна. Git Repository дээр өгөх таны санал хүсэлт, эх кодыг өөрчлөх хүсэлт (pull request)-г Github дээр оруулах боломжтой.

Дүгнэлт

2FA баталгаажуулалтын механизмыг ашиглахаа болих гэж яарах хэрэггүй. Хэдийгээр энэ баталгаажуулалтын механизм нь төгс биш боловч аюулгүй байдлын нэг түвшинг нэмж өгч байгаа юм. *2FA* баталгаажуулалтын механизм нь бусад баталгаажуулалтын механизмтай ижил шалтгаанаар халдлагад өртөх боломжтой юм. Тиймээс байгууллагуудын хувьд энэ төрлийн халдлагаас хамаарах хор хөнөөлийг бууруулах бэлтгэлтэй байх хэрэгтэй. *2FA* -г хакер амжилттай тойрон гарч чадах боломжтой байна хэмээн үзэж, *2FA* баталгаажуулалтын механизмаар хамгаалагдсан бүх сервисийн тохиргоог чангатгах хэрэгтэй. Сешинийн хугацааг бууруулах замаар, хакер системийг рүү халдах хугацааг бууруулах боломжтой. Нэг хэрэглэгчийн нэвтрэх эрхээр, хамгийн ихдээ нэг л сешин (concurrent session) үүсгэх тохиргоог хийж өгснөөр, хакер болон хохирогч этгээдүүд нэгэн зэрэг хоёул идэвхтэй холболттой байх нөхцөлийг хязгаарлаж өгөх боломжтой. Хэрвээ таны хамгаалах гэж буй сервис VPN бол сүлжээний сегментчилэлийг маш хатуу болгох хэрэгтэй. VPN хэрэглэгчид нь зөвхөн өөрсдийн зайлшгүй хандах хэрэгцээтэй нөөц рүү хандах эрхтэй байх нь зүйтэй. Эцэст нь өөрийн хэрэглэгчдээ халдлагыг таньдаг болгох, сошиал инженеринг хийх оролдлогоос зайлсхийх, тайлагнадаг болох хэмжээнд мэдлэгтэй, чадвартай болгож хөгжүүлэх хэрэгтэй.

РийлФиш-г нийтэд ил болгосноороо, *Мэндиэнт*-ийн багийнхан олон түвшин бүхий хамгаалалтын механизмыг чухал болохыг тодотгон харуулах, зөвхөн ганцхан баталгаажуулалтын механизмд найдах нь таны аюулгүй байдлыг хангаж чадахгүй болохыг харуулахыг хүссэн болно. Энэ програм нь аюулгүй байдлын мэргэжилтнүүдэд нэвтрэх эрхийн тестийг эхнээс нь дуустал нь өөрөө хийж үзэх боломжийг нь дэмжих зорилготой юм.

Мэндиэнт дээрх Улаан багийн үйл ажиллагааны үед, байгууллагын дотоод сүлжээ рүү нэвтрэн орох нь зөвхөн эхний алхам л юм. Энд танилцуулсан програм нь зөвхөн эхний алхмыг л дэмжих зориулалттай гэсэн үг. Гэвч ийм төрлийн үйл ажиллагааг тэр чигтээ амжилттай болох эсэх нь тухайн компаний хэрэгжүүлж буй аюулгүй байдлын шийдэл, хэрэгжилтээс хамааралтай. Өөрийн аюулгүй байдлыг бүхлээр нь авч үзэж, байнга сайжруулж байхын тулд ажиллах хэрэгтэй. *Мэндиэнт* нь бүх төрлийн байгууллагад аюулгүй байдлаа сайжруулахад нь дэмжлэг үзүүлэх олон төрлийн үйлчилгээг үзүүлдэг.