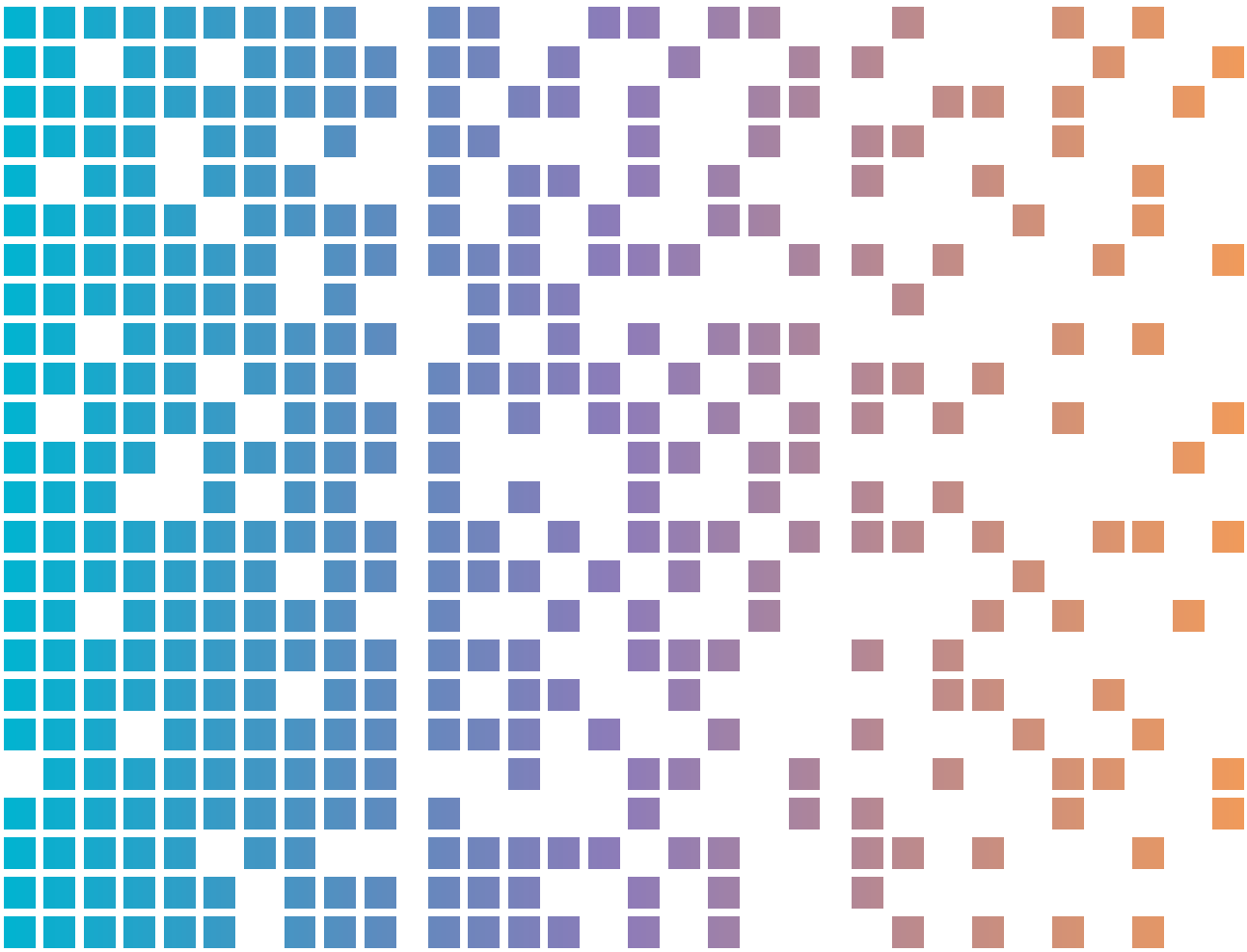
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Чимээгүй дээрэм: цахим гэмт хэрэгтнүүд мэдээлэл хулгайлагч хорт програм ашиглан байгууллагын сүлжээнд нэвтэрч байна



Агуулгын төвшин
дунд төвшний

cyber.gov.au

ГАРЧИГ

Агуулга

Мэдээлэл хулгайлагч хорт програм нь хэрэглэгчийн нэвтрэх хувийн нууц мэдээлэл болон системийн мэдээллийг хулгайлдаг бөгөөд ингэснээр цахим гэмт хэрэгтнүүд үүнийг ихэвчлэн мөнгө олох зорилгоор ашигладаг. Австрали төдийгүй дэлхий даяар олон байгууллага, салбарын эсрэг чиглэсэн цахим гэмт хэргийн халдлагуудад Мэдээлэл хулгайлагч хортой програм ашиглаж байгаа нь ажиглагдсан. Уг нийтлэлд мэдээлэл хулгайлагч хортой программ, эрсдэл учруулах үйл ажиллагаа болон үүнийг хэрхэн шийдвэрлэх тухай арга замуудыг багтаасан бөгөөд аливаа байгууллага, тэдгээрийн ажилтан албан хаагч нарт зориулсан болно.

Онцлох зүйлс

- Мэдээлэл хулгайлагч хортой программ нь хохирогчийн төхөөрөмжөөс мэдээлэл цуглуулах зориулалттай хортой програмуудын нэг төрөл юм. Үүнд хэрэглэгчийн нэвтрэх нэр, нууц үг, зээлийн картын мэдээлэл, криптовалютын түрийвч, компьютерийн файлууд болон күүки, хэрэглэгчийн түүх, автоматаар бөглөх маягтын мэдээлэл зэрэг хөтчийн өгөгдөл багтана.
- Цахим гэмт хэрэгтнүүд байгууллагын аккаунттай холбоотой хулгайд алдсан хэрэглэгчийн нэвтрэх мэдээллийг худалдан авч ашигласнаар хохирогчийн ажил олгогч, тэдний үйлчлүүлэгчид болон бусад байгууллагын цахим системд анхны нэвтрэлтийг хийхийг оролддог. Ингэснээр эдгээр байгууллагуудад дараах сөрөг үр дагаврууд учирч болно: барьцаалагч программын халдлага, сүрдүүлэлт, бизнес имэйлийг хулгайд алдах болон оюуны өмчийн хулгай.
- Австралийн Радиотехникийн Газрын харьяа Цахим Аюулгүй Байдлын Төвд (ASD-ийн ACSC) тухайн байгууллагын ажилтны халдлагад өртсөн хувийн төхөөрөмжөөр дамжин байгууллагын сүлжээнд нэвтэрсэн тохиолдлууд бүртгэгдсэн байна.. Хэд хэдэн тохиолдолд цахим гэмт хэрэгтнүүд хулгайлсан хүчин төгөлдөр хэрэглэгчийн нэвтрэх мэдээллийг ашиглан байгууллагын сүлжээнд анхны нэвтрэлтийг хийж чадсан байна. Цахим гэмт хэрэгтнүүд нэвтрэх эрх бүхий хэрэглэгчийн аккаунтад амжилттай нэвтэрсний дараа ихэвчлэн байгууллагын сүлжээнд томоохон хэмжээний дайралт хийж байгааг манай судалгаагаар тогтоосон.
- Ажилтнууд, гэрээт гүйцэтгэгчид, менежментийн үйлчилгээ үзүүлэгчид болон бусад талуудад өөрийнхөө сүлжээнд алсаас, өөрийн төхөөрөмж (BYOD) ашиглан холбогдох боломжийг олгодог албан байгууллагууд мэдээлэл хулгайлагчийн учруулж буй эрсдлийг ойлгож, энэхүү аюулаас өөрсдийгөө хамгаалах хэрэгтэй. Цахим гэмт хэрэгтнүүд мэдээлэл хулгайлагчийг хохирогчийн төхөөрөмж дээр олон төрлийн арга ашиглан байршуулдаг. Үүнд цахим шуудангийн фишинг, хууль бусаар татаж авсан програм, хайлтын системийн оновчлол (SEO)-ын техникүүд, хортой зар сурталчилгаа болон олон нийтийн сүлжээ дээр нийтлэгдсэн хортой холбоосууд орно. Ерөнхийдөө ажлын болон хувийн зориулалтаар хамтад нь ашиглагддаг төхөөрөмжүүд хэрэглэгчийн буруу зуршилт үйлдэл болон аюулгүй байдлын хяналт сулрахтай холбоотойгоор эдгээр аргуудаар халдлагад өртөх өндөр эрсдэлтэй байдаг.
- Мэдээлэл хулгайлагч нь цахим гэмт хэрэгтнүүдэд, ялангуяа туршлагагүй гэмт хэрэгтнүүд болон технологийн чадвар багатай хүмүүст цахим гэмт хэргээр мөнгө олох таатай боломжийг олгодог. Зарим цахим гэмт хэрэгтнүүд мэдээлэл хулгайлагчийг бүтээгдэхүүн болгон Malware-as-a-Service (MaaS) буюу Хортой Программ Үйлчилгээ хэлбэрээр зах зээлд сарын хураамжтайгаар нийлүүлэх нь бий.

Үндсэн мэдээлэл

Цахим гэмт хэрэгтнүүд мэдээлэл хулгайлагчийг ашиглаж байгаа нь Австралийн байгууллагуудын аюулгүй байдал болон хэвийн үйл ажиллагаанд заналхийлж байна. Мэдээлэл хулгайлагчийн халдвар нь ихэвчлэн томоохон цахим аюулгүй байдлын халдлага хийхийн өмнөх урьдчилсан үйлдэл байдлаар илэрдэг бөгөөд цахим гэмт хэрэгтнүүд хэрэглэгчдийн нэвтрэх мэдээллийг цуглуулахад ашигладаг. Эдгээр хэрэглэгчдийн нэвтрэх мэдээлэл, ялангуяа интернэтэд холбогдсон алсын үйлчилгээ эсвэл нэвтрэх эрх олгогдсон аккаунтуудад хандах боломжтой мэдээлэл нь байгууллагын сүлжээ болон өгөгдөлд анхны нэвтрэлт хийхэд ашиглагддаг.

Тэмдэглэл: Анхны нэвтрэлт гүйцэтгэгчид нь цахим гэмт хэргийн экосистемд тусгай үүргийг гүйцэтгэдэг бөгөөд тэд хулгайлсан хэрэглэгчийн нэвтрэх мэдээллийг худалдан авч шалган баталгаажуулдаг. Үүний дараа тэд эрэлттэй байгууллагын баталгаатай хэрэглэгчийн нэвтрэх мэдээллийг цахим гэмт хэрэгтнүүдэд дуудлага худалдаагаар санал болгож, улмаар байгууллагын сүлжээнд нэвтрэхэд ашиглагддаг.

Хулгайлагдсан хүчин төгөлдөр хэрэглэгчийн нэвтрэх мэдээлэл нь цахим гэмт хэрэгтнүүдэд ихээхэн үнэ цэнэтэй байдаг. Учир нь үүний тусламжтайгаар байгууллагын сүлжээ болон бизнесийн системд анх нэвтрэх үйл явцыг түргэсгэдэг. Хулгайлагдсан хүчин төгөлдөр хэрэглэгчийн нэвтрэх мэдээллийг ашигласнаар цахим гэмт хэрэгтнүүд дараах алхмуудыг хийх шаардлагагүй болдог:

- Байг тодорхойлох, судлах
- Хохирогчийн сүлжээнүүдийг олж сул талыг тодорхойлох
- Анхны нэвтрэлтийн аргыг тодорхойлох, үүнд:
  - Фишинг хийх
  - Програм хангамжийн сул талыг ашиглах
  - Алсын үйлчилгээ, тухайлбал Remote Desktop Protocol (RDP) болон виртуал хувийн сүлжээ (VPN)-г онилох
  - Нууц үг таах зэрэг хүч хэрэглэсэн халдлага (brute force) хийх

Эдгээр алхмууд нь тодорхой хэмжээний цаг хугацаа болон техникийн ур чадвар шаарддаг бөгөөд зарим цахим гэмт хэрэгтнүүдэд тодорхой хэмжээнд сорилт болдог. Ялангуяа байгууллагын сүлжээний хамгаалалтыг эвдэж чадаагүй цахим гэмт хэрэгтнүүдэд мэдээлэл хулгайлагч ихээхэн ашигтай. Учир нь үүний тусламжтайгаар онилж буй байгууллагын сүлжээнд нэвтрэх боломжтой хэрэглэгчийн нэвтрэх мэдээллийг хурдан бөгөөд хялбархан олж авах боломжтой.

Алсын зайнаас ажиллаж буй зарим ажилтнууд өөрсдийн хувийн төхөөрөмж дээрээ интернэт веб хөтчийг ажлын болон хувийн зориулалтаар ашигладаг. Ингэхдээ тухайн ажилтан өөрийн хэрэглэгчийн нэвтрэх мэдээллээ веб хөтчийн нууц үгийн хадгалах сан, өргөтгөлүүдэд хадгалах эсвэл веб хөтчийн автоматаар бөглөх функцүүдийг ашиглаж болно. Мэдээлэл хулгайлагч нь эдгээр нууц үг хадгалах санд нэвтрэх эсвэл баталгаажуулах күүки болон веб хөтчийн бусад хувийн мэдээллийг олж авах үүрэгтэй байдаг.

Байгууллагын төхөөрөмжүүдээс ялгаатай нь, хувийн төхөөрөмжийг байгууллагын аюулгүй байдлын журмын дагуу эрсдэлээс хамгаалан боломжгүй бөгөөд энэ нь эргээд байгууллагуудад өндөр эрсдэл үүсгэдэг. Жишээ нь, ажилтнууд хууль бус программ татах, эрсдэлтэй онлайн хайлт хийх гэх мэт үйлдлээс болж байгууллагын цахим занахийлэл болон хортой программд өртөх эрсдлийг нэмэгдүүлдэг.

Мэдээлэл хулгайлагч, түгээлт хийдэг этгээдүүд, анхны нэвтрэлт хийхэд зуучлагчид, мөн түүнчлэн барьцаалагч програм хангамжийн хөгжүүлэгчид нь санхүүгийн ашиг олох зорилгоороо нэгдэн цахим гэмт хэргийн экосистемийн үндсэн чухал бүрдэл хэсэг болж байна. Цахим гэмт хэрэгтнүүд халдлагын тодорхой шатнуудад мэргэшиж тухайн шатны онцлог чадваруудыг хөгжүүлэн, үүнийг бусад гэмт этгээдүүдэд үйлчилгээ хэлбэрээр худалдах үед уг экосистем илүү үр бүтээмжтэй болдог.

Аюул заналхийлэл

ASD-ийн ACSC нь дэлхий даяарх мэдээлэл хулгайлагчдын өсч буй идэвхжилтийг хянаж, Австралийн сүлжээнүүдэд өсөн нэмэгдэж буй аюул заналхийлэл болж буйг тогтоож байна. Салбарын тайланд дурдсанаар, 2023 онд мэдээлэл хулгайлагчид цахим гэмт хэргийн үйл ажиллагаанд хамгийн түгээмэл тархсан хортой программын төрөл байсан байна. Хууль бус зах зээл дээр зарагдаж буй хулгайлагдсан мэдээллийн хэмжээ нэмэгдэж, энэ мэдээллийг ашиглан анхны нэвтрэлтийн зуучлагчдын үйл ажиллагаа нэмэгдэж байгаа нь эрсдэл үүсгэж байгаа бөгөөд 2024 онд ч гэсэн өсөх хандлагатай байна.

Мэдээлэл хулгайлагчийн экосистем

1-р үе шат: Хортой програм олж авах

Мэдээлэл хулгайлагч програм хангамжийг ихэвчлэн цахим гэмт хэрэгтнүүдийн зах зээл дээр “Malware-as-a-Service (MaaS)” эсвэл “Stealer-as-a-Service" хэлбэрээр, эсвэл эх кодоор нь худалддаг. “MaaS (Malware-as-a-Service)” гэдэг нь хортой програмыг хөгжүүлэгчид өөрсдийн хортой программд зориулсан захиалгын үйлчилгээ хэлбэрээр веб платформ ашиглан хэрэглэгчдэд санал болгодог ба энэ нь хууль ёсны “Software-as-a-Service (SaaS)” үйлчилгээтэй адилхан загварчлал юм. “MaaS” загвар нь туршлагагүй кибер гэмт хэрэгтнүүдэд учрах сорилтыг багасгаж, технологийн мэдлэг дутмаг байсан ч хортой програм тарааж, хулгайлсан мэдээллийг цуглуулан цахим халдлагад ашиглах боломжийг олгодог.

“MaaS” хэлбэрээр санал болгож буй мэдээлэл хулгайлагчдыг ихэвчлэн харьцангуй хямд сарын хураамжтайгаар ашиглуулдаг бөгөөд цахим гэмт хэрэгтнүүд тус мэдээлэл хулгайлагчийн хяналтын самбарт нэвтрэх боломжтой болдог. Тус хяналтын самбар нь мэдээлэл хулгайлагч хортой програм үүсгэх, хулгайлагдсан өгөгдлийг эмхлэх, мөн халдаж орсон сүлжээний тоо хэмжээг хянах боломж олгодог. “MaaS”-г ажиллуулж буй этгээдүүд вирусны эсрэг програм хангамжийн илрүүлэлтээс зугтах, захиалагчдыг татах, захиалагчдаа хадгалахын тулд шинэлэг функцууд, хэрэгслүүд болон техникийн дэмжлэгийг санал болгодог. Олон мэдээлэл хулгайлагчууд өгөгдөл хулгайлсны дараа хохирогчийн төхөөрөмжөөс өөрийгөө устгах чадвартай байдаг.

2-р үе шат: Түгээлт

Мэдээлэл хулгайлагчийг суулган төхөөрөмжүүдэд нэвтрэн улмаар тэндээс мэдээлэл цуглуулдаг кибер гэмт хэрэгтнүүдийг “Трафферууд” (урсгал түгээгч) гэж нэрлэдэг. Трафферууд хохирогчдыг хортой холбоос руу чиглүүлэн хандуулж, ингэснээр өргөн хүрээний халдлагын нэг хэсэг болох мэдээлэл хулгайлагчийг тараах үйл ажиллагааг явуулдаг. Тэдний ихэнх халдлага нь тодорхой зорилтот байгүй бөгөөд тохиолдлоор халдварлуулахыг зорьдог. Гэсэн хэдий ч, тэдний зарим халдлагууд тусгайлсан салбарт чиглэсэн байдаг бөгөөд үүний нэг жишээ нь тодорхой хохирогчийг чиглэсэн зорилтот фишинг (spear-phishing) үйлдэл юм. Трафферүүд эдгээр тодорхой бай бүхий халдлагуудыг үйлчлүүлэгчдийн хүсэлтээр зохион байгуулдаг бөгөөд жишээ нь, үйлчлүүлэгч нь тодорхой өндөр үнэ цэнэтэй байгууллага эсвэл салбарт нэвтрэх боломжийг эрэлхийлж байгаа үед ийм үйлдэл хийдэг.

Трафферүүд мэдээлэл хулгайлагчийг хохирогчийн төхөөрөмж дээр олон төрлийн аргууд ашиглан суулгадаг, үүнд:

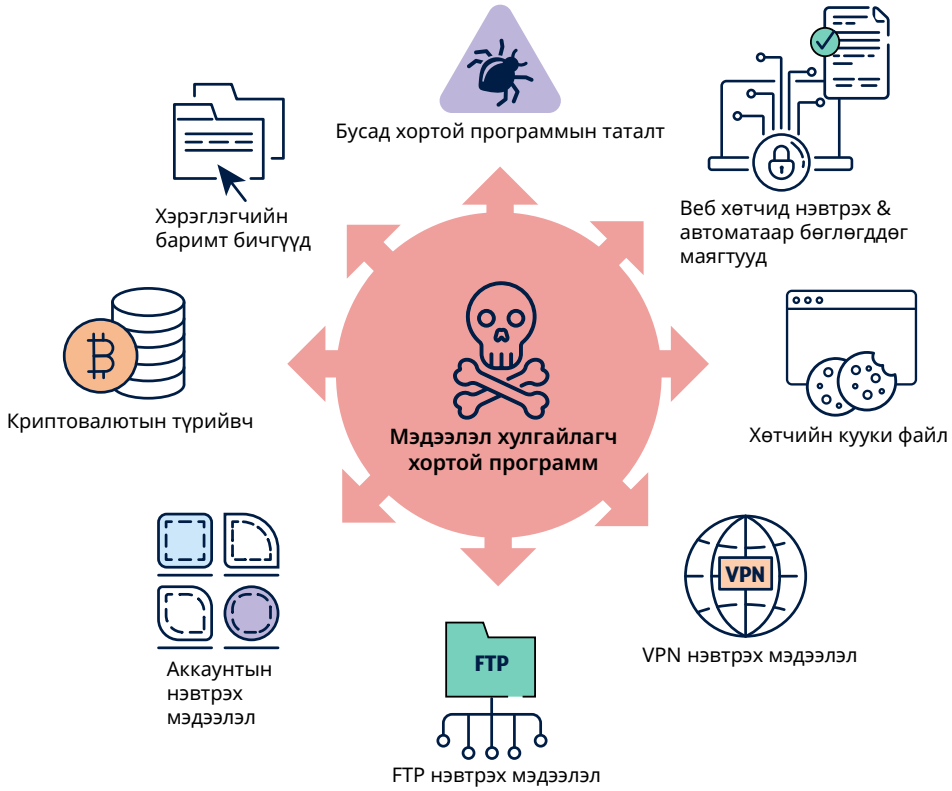
- **ботнетүүд**: цахим гэмт хэрэгтнүүдийн удирддаг, фишинг мессеж эсвэл хортой програм тараах зэрэг хууль бус үйлдлүүдийг гүйцэтгэх зорилготой халдлагад өртсөн компьютер системийн сүлжээнүүд

- **Фишинг**: цахим шуудан, олон нийтийн сүлжээ, форум, мессежийн аппликейшнүүдээр дамжуулан нууцлал бүхий мэдээлэл авах оролдлогууд. Эдгээр нь туршлагагүй цахим гэмт хэрэгтнүүдийн ихэвчлэн хэрэглэдэг түгээх арга хэлбэрүүд юм:
  - Эдгээр мессежүүд нь ихэвчлэн хортой файлын оронд хортой холбоосыг агуулсан и-мэйлүүд байдаг.
- **Хортой хайлтын үр дүн**: хайлтын системийн оновчлол (SEO) аргаар дамжуулж, хохирогчдыг хууль ёсны програм, контент мэт харагдах хортой програм тараадаг вэбсайтуудад чиглүүлдэг
- **Хортой зар сурталчилгаа (malvertising)**: хууль ёсны онлайн зар сурталчилгаанд хортой код оруулж, хортой программ тараах арга
- **Нэвтрэн орсон эсвэл хууль бус програм хангамж**: төрөл бүрийн татаж авсан файлууд. Үүнд видео тоглоомууд, шэйрлэсэн YouTube-ийн видеонууд нь хортой линк тайлбар/коммент хэсэгтээ агуулсан байх, эсвэл найдвартай бус татаж авах сайтуудаас тараах
- **Олон нийтийн сүлжээний зар сурталчилгаа ба постууд**: зорилтот бай бүхий хортой програмтай файлуудыг чиглүүлэх
- **Хортой програмын шинэчлэлтүүд**: ихэвчлэн веб хөтчийн шинэчлэлт мэтээр далдлан нуух

3-р үе шат: Мэдээлэл цуглуулалт

Мэдээлэл хулгайлагч хохирогчийн төхөөрөмжид нэвтэрсний дараа уг төхөөрөмжөөс хувийн нууцлал бүхий мэдээллүүдийг цуглуулж эхэлдэг. Мэдээлэл хулгайлагч ботнетийн нэг хэсэг болсон тохиолдолд, тэр хэрэглэгчийн нэвтрэх мэдээллийг хулгайлахаас гадна, цахим гэмт хэрэгтнүүд уг нэвтрэн орсон төхөөрөмжийг алсаас удирдаж, хэрэгцээтэй нэмэлт үйлдлүүдийг идэвхжүүлэх эсвэл бусад хортой программ тараахын тулд тохиргоог өөрчилж чаддаг. Ерөнхийдөө мэдээлэл хулгайлагчид дараах мэдээллийг хулгайлах чадвартай байдаг:

- Хэрэглэгчийн нэр, нууц үг, ялангуяа веб хөтчүүдийн давхар баталгаажуулалт (MFA), хэрэглэгчийн идэвхтэй хэрэглээ болон токенуудад хадгалагдсан мэдээлэл.
- Баталгаажуулах күүки (authentication cookies)
- Веб хөтчийн автоматаар бөглөх маягтын мэдээлэл
- И-мэйлийн нэвтрэх мэдээллүүд, агуулга, и-мэйлд хадгалсан холбогдох хаягнууд
- Интэрнет үзэлтийн түүх
- Хэрэглэгчийн баримтууд
- зээлийн картын дэлгэрэнгүй мэдээлэл
- Десктоп дээрх мессежийн аппликейшнуудад бичсэн чатийн түүх
- Системийн мэдээлэл
- Криптовалютын түрийвчүүд
- VPN эсвэл FTP нэвтрэх мэдээлэл



Зураг 1. Мэдээлэл хулгайлагчийн чадварууд

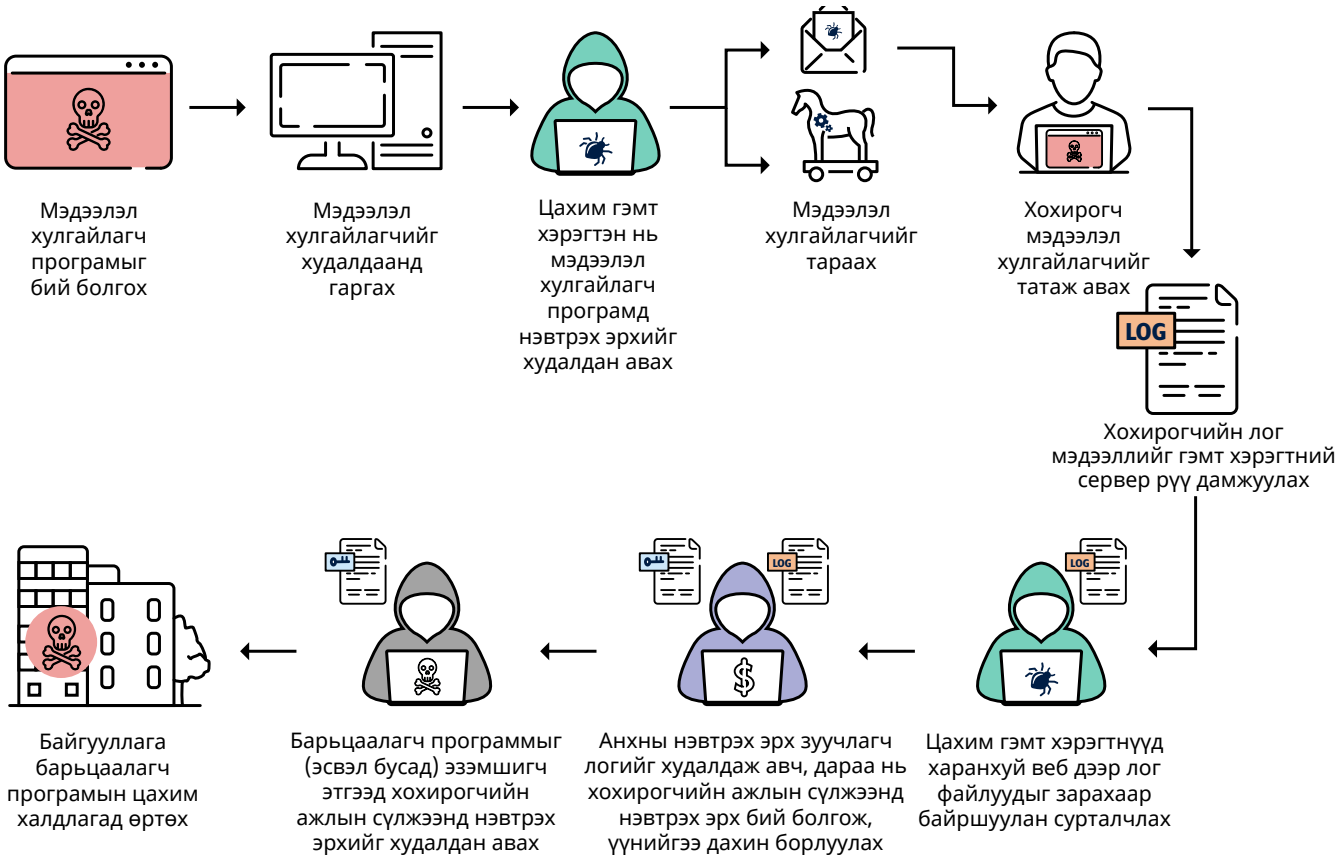
Вэб хөтчийн баталгаажуулалтын күүкинүүд нь хэрэглэгчийг олон хоногийн турш нэг аккаунт эсвэл үйлчилгээнд нэвтэрсэн хэвээр байлгах боломжтой байдаг тул хэрэглэгчид дахин нэвтрэх шаардлагагүй болдог. Хэрвээ эдгээр күүкинүүд хулгайлагдвал, тэдгээр нь давхар баталгаажуулалт (MFA)-н шалгуурыг даван гарч, цахим гэмт хэрэгтнүүдэд хохирогчийн данс, компанийн сүлжээ болон бизнесийн системүүдэд нэвтрэх боломжийг гаргаж өгч болно.

4-р үе шат: Өгөгдлийг цуглуулан нэгтгэх ба мөнгөжүүлэх

Хохирогчийн мэдээллийг, тухайлбал “лог” файлуудыг, хортой удирдлагын (C&C) серверүүд рүү нууцаар гадагш гаргах үүрэгтэйгээр мэдээлэл хулгайлагчийг бүтээсэн байдаг.” Ерөнхийдөө, мэдээлэл хулгайлагч програмууд нь Telegram, Discord зэрэг түгээмэл мессеж аппликейшнүүдийг ашиглан лог мэдээллүүдийг цахим гэмт хэрэгтнүүдэд дамжуулдаг.

Лог мэдээллийг худалдах, арилжаалах тусгайлсан зах зээлүүд Telegram болон харанхуй веб (dark web)-д оршдог. Цахим гэмт хэрэгтнүүд лог мэдээллийг дараах аргаар мөнгөжүүлдэг:

- Лог мэдээллийг хууль бус зах зээл дээр худалдаалах, үүнд анхны нэвтрэх эрхийг зуучлагчдад ч зардаг.
- Таних мэдээлллиг нь хулгайлах болон сүрдүүлэх замаар хохирогчийг өөрин эрхэнд байлгаж ашиглах
- Лог мэдээллийг ашиглан байгууллагын сүлжээнд анхны нэвтрэлт хийх эрхтэй болох, ингэснээр барьцаалагч програмаар халдлага хийх



Зураг 2. Мэдээлэл хулгайлагчийн экосистем ба байгууллагад үзүүлэх боломжит нөлөө

Үр дагавар

Мэдээлэл хулгайлагч нь хувь хүн болон байгууллагад ноцтой үр дагавар учруулах боломжтой. Мэдээлэл хулгайлагч нь хэрэглэгчийн нэвтрэх мэдээллийг цуглуулж, цахим гэмт хэрэгтнүүд уг мэдээллийг ашиглан хүчинтэй хэрэглэгчийн бүртгэлээр байгууллагын сүлжээ эсвэл бизнесийн системд нэвтрэх боломжтой болдог. Ихэнхдээ байгууллагууд үүнийг илрүүлэхэд удаашралтай байдаг.

Мэдээлэл хулгайлагчдад өртсөн **байгууллагуудын** хувьд дараах үр дагаврууд үүсч болзошгүй:

- Барьцаалагч программын халдлагад өртөх
- мэдээлэл алдах
- бизнесийн и-мэйлийн нууцлал алдагдах
- оюуны өмчийн хулгай
- Нууцлал бүхий эмзэг мэдээлэл алдагдах

Мэдээлэл хулгайлагчдад өртсөн **хувь хүмүүст** хувьд дараах үр дагаврууд үүсч болзошгүй:

- Хувийн и-мэйл эсвэл олон нийтийн сүлжээний аккаунтад зөвшөөрөлгүй нэвтрэх
- Хувийн мэдээллийг ашиглан залилан хийх эрсдэл нэмэгдэх
- Фишинг халдлагад өртөх эрсдэл нэмэгдэх
- Санхүүгийн хохирол амсах эсвэл банкны дансанд зөвшөөрөлгүй нэвтрэх
- Хувийн нууцлал алдагдах

Жишиг судалгаа:

Энэхүү жишиг судалгааг олон нийтэд түгээх зорилгоор байгууллагын нэрийг нууцалсан болно. Энэ нь Австралийн байгууллагуудад томоохон нөлөө үзүүлсэн, ASD-ийн ACSC-д мэдээлэгдсэн хэд хэдэн цахим аюулгүй байдлын зөрчлүүд дээр үндэслэсэн мэдээлэл юм. Хохирогч байгууллагыг цаашид “Байгууллага” гэж нэрлэнэ. Энэхүү жишиг судалгаанд дурдсан хувь хүмүүсийн нэрсийг өөрчилсөн бөгөөд хохирогчдын нэр төрийг хамгаалахын тулд нарийн мэдээллийг оруулаагүй болно.

Энэ бол Австралийн байгууллага бөгөөд өөрийн ажилчдад хувийн төхөөрөмжөөсөө байгууллагын сүлжээнд нэвтрэн ажиллах боломж олгодог байсан. Алис нь тус байгууллагад алсаас ажилладаг ажилтан юм.

Гэрээсээ ажиллахдаа Алис хувийн зөөврийн компьютер ашиглан байгууллагынхаа сүлжээнд нэвтэрдэг. Алис нь **өөрийн зөөврийн компьютерт** итгэлтэй гэж үзсэн вебсайтаас тэмдэглэл хөтлөх зориулалттай Notepad++ програмын нэг хувилбарыг **татаж авсан** байна. Notepad++ програмын суулгагч дотор **мэдээлэл хулгайлагч** нуугдсан байв.

Алис тус програмыг суулгах гэж оролдох үед мэдээлэл хулгайлагч идэвхжиж, зөөврийн компьютерээс нь **хэрэглэгчийн нэвтрэх эрхийн мэдээллийг хулгайлах** үйл ажиллагаагаа эхлүүлсэн. Үүнд түүний веб хөтчийн бэлэн хадгалах нэвтрэх мэдээллийн хэсэг дэх ажлын сүлжээнд нэвтрэн орох хэрэглэгчийн нэр ба нууц үг орсон байв. Дараа нь мэдээлэл хулгайлагч уг хэрэглэгчийн нэвтрэх мэдээллийг цахим гэмт хэргийн бүлэглэлийн хяналттай алсын команд-удирдлагын сервер рүү илгээсэн.

Хулгайлагдсан лог файлуудыг бусад ижил мэдээллүүдтэй хамт багцалж, дараа нь харанхуй веб дээр **цахим гэмт хэрэгтнүүдэд борлуулсан**.

Боб хэмээх цахим гэмт хэрэгтэн Алисийн хэрэглэгчийн нэвтрэх мэдээллийг худалдан авч, түүний байгууллагын сүлжээнд ашиглагддаг мэдээллийг олж тодорхойлсон. Алисийн ажилладаг байгууллага өөрийн сүлжээндээ **давхар баталгаажуулалт (MFA)-ыг тохируулаагүй** байсан тул Боб зөвхөн хулгайлсан хэрэглэгчийн мэдээллийг ашиглаж амжилттайгаар **баталгаажилт хийлгэн байгууллагын сүлжээнд нэвтрэх** боломжтой болсон.

Боб хулгайлсан **хүчинтэй хэрэглэгчийн нэвтрэх мэдээллийг** ашиглан Алисийн ажилладаг байгууллагын сүлжээнд мэдэгдэхгүйгээр нэвтэрсэн. Боб байгууллагын сүлжээнд нэвтрэн түүний бусад төхөөрөмж системд шилжиж, байгууллагад хамаарах эмзэг нууцлал бүхий мэдээллийг илрүүлж сүрдүүлэх зорилгоор уг мэдээллүүдийг гартаа оруулжээ.

Уг мэдээллийг хулгайлсны дараа Боб байгууллагын **өгөгдлийн сан болон файлын системүүдийг шифрлэж**, бусад ажилтнууд үүнд нэвтрэх боломжгүй болгосон.

Эрсдэлийг бууруулах арга хэмжээ

Байгууллагууд өөрсдийн систем, сүлжээнд холбогддог төхөөрөмжүүд, ялангуяа алсаас ажиллаж буй ажилтнуудын хувийн төхөөрөмжүүдэд хяналт тавих боломжгүй байж болдог. Байгууллагуудад хэрэглэгчийн нэвтрэх мэдээллийг хулгайлах эрсдэлээс хамгаалах зорилгоор хяналт тавьж байхыг ASD-ийн ACSC зөвлөж байна. Эрсдэлийг бууруулах арга хэмжээнд дараах алхмууд багтана:

Ажилтнуудад цахим аюулгүй байдлын сургалт зохион байгуулах

- Зориулалтын нийгмийн инженерчлэл болон хортой файл таталтыг амжилттай таслан зогсоох зорилгоор үр дүнтэй сургалт явуулах
- Мэдээлэл хулгайлагчид, тэдгээрийн халдлага хийх арга хэлбэрүүд болон фишингийн эрсдэлүүдийн талаарх мэдлэгийг нэмэгдүүлэх

Байгууллагын аккаунтыг аюулгүй болгох

- Давхар баталгаажуулалт (MFA)-ыг хэрэгжүүлэх:
- Гадаад болон дотоод үйлчилгээ, сүлжээ болон эмзэг мэдээллийн сангууд, ялангуяа веб имэйл, VPN, системд нэвтрэх эрхтэй давуу эрхтэй хэрэглэгчийн бүртгэлд Давхар баталгаажуулалт (MFA)-ыг хэрэгжүүлэх. Бүх онлайн хэрэглэгчдийн аккаунт дээр фишингт тэсвэртэй Давхар баталгаажуулалтыг хэрэгжүүлэх нь хамгийн сайн арга юм.
- Хэрэглэгчийн аккаунтыг шаардлагагүй болсон үед нь идэвхгүй болгох.
- Админы эрхийг хязгаарлах:
- Сүлжээний удирдлага болон бусад давуу эрхтэй үүргүүдийг зөвхөн тусгайлан хамгаалагдсан, түгжигдсэн төхөөрөмжөөс (жишээ нь, аюулгүй администраторын төхөөрөмж) гүйцэтгэх.
- Администраторуудад системийг удирдахад нь давуу эрхтэй хэрэглэгчийн аккаунтийг ашиглуулах, бусад энгийн үүрэгт ердийн хэрэглэгчийн аккаунтийг ашиглах замаар хамгийн бага эрхийг хамгийн түрүүнд гэсэн зарчмыг мөрдөх
- Давуу эрхтэй хэрэглэгчийн аккаунтуудыг (онлайн үйлчилгээ ашиглах тусгай зөвшөөрөлтэй аккаунтаас бусад) интернет, имэйл болон веб үйлчилгээнд хандахыг хязгаарлах
- Систем, аппликейшнүүдэд шаардлагатай үед л тохиргоо хийх (just-in-time administration) арга хэмжээг хэрэгжүүлэх
- Давуу эрхтэй хэрэглэгчийн аккаунтуудад менежмент, аудитын үйл ажиллагааг чанд мөрдөх
- Нууц үгийг тогтмол шинэчлэх, ялангуяа гадаад сүлжээгээр алсаас нэвтэрдэг аккаунтуудын хувьд
- Баталгаажуулалтын токен, күүкийн хугацаа дуусах болон ахин баталгаажуулах бодлогыг чанд мөрдөх

Байгууллагын сүлжээний орчны аюулгүй байдлыг бэхжүүлэх

- Байгууллагын сүлжээний орчны эрсдэлд үнэлгээг хийж, байгууллагын сүлжээний орчны бэхжүүлэлтийн журмыг хэрэгжүүлэх
- Албан хаагчдад хувийн төхөөрөмжийг ашиглахыг зөвшөөрсөн тохиолдолд “Өөрийн Төхөөрөмжийг Авчир” буюу “Bring Your Own Device” (BYOD) бодлогыг хэрэгжүүлэх, учир нь байгууллагаас удирддаг төхөөрөмжүүд нь хувийн хяналтгүй төхөөрөмжөөс илүү аюулгүй байдаг.

Танай сүлжээнд нэвтэрдэг гаднын нийлүүлэгчдэд сүлжээний эрсдлийн үнэлгээ хийх, үүнд “Software-as-a-Service (SaaS)” нийлүүлэгчид болон удирдлагын менежменттэй үйлчилгээ үзүүлэгчид орно. Удирдлагын менежменттэй үйлчилгээ үзүүлэгчдийг ашиглах үед Аюулгүй Байдлыг Хэрхэн Удирдах аргачлалыг мөрдөх.

Байгууллагын сүлжээгээ хамгаалах

- Аппликейшн болон үйлдлийн системийг үргэлж шинэчилж байх
- Аппликейшний хяналтыг хэрэгжүүлэхийн тулд хатуу зөвшөөрөгдсөн жагсаалт бүхий дотоод сүлжээний аюулгүй байдлын бодлогыг хэрэгжүүлэх.
- Сүлжээг гүйцэтгэдэг үүрэг, үйл ажиллагаагаар нь ангилж сүлжээний сегментчиллийг хэрэгжүүлэх.
- Хэрэглэгчийн үйл ажиллагааг, ялангуяа алсаас ажиллаж буй ажилтнуудын үйлдэлд аудит хийх, хянах.
- Давуу эрхтэй бүртгэлүүдийг хянаснаар эмзэг нууцлал бүхий мэдээлэлд зөвшөөрөлгүй хандах эсвэл хэвийн бус өгөгдөл дамжуулах үйлдлүүдийг илрүүлэх боломжтой. Тухайлбал их хэмжээний өгөгдлийг гадаад сүлжээнд илгээх гэх мэт үйлдлийг илрүүлэх боломжтой.
- Өгөгдөл алдагдахаас сэргийлэх бодлого, зөвшөөрөлгүй өгөгдөл дамжуулахыг таслан зогсоох зорилгоор зохих хэрэгслүүдийг ашиглах

ASD-ийн Цахим аюулгүй байдлын сүлжээнд нэгдэх. Мөн түүнчлэн ASD-ийн Цахим аюул заналхийллийн мэдээлэл солилцох (CTIS) үйлчилгээнд бүртгүүлэх.

- CTIS нь засгийн газар, бизнесийн түншүүдэд хортой цахим үйл ажиллагааны талаарх мэдээллийг хүлээн авч, солилцох хоёр талт платформ юм.
- ASD-ийн ACSC нь мэдээлэл хулгайлагчийн үйл ажиллагааг хянаж, идэвхтэй команд ба удирдлагын дэд бүтцийн дэлгэрэнгүй мэдээллийг CTIS платформоор дамжуулан хуваалцдаг.
- ACSC-ийн түнш болж, байгууллага болон үйлчлүүлэгчдийнхээ мэдээллийг цахим гэмт хэрэгтнүүдээс хамгаалахыг уриалж байна.

Халдлагад өртөхөөс урьдчилан сэргийлэх

- Мэдээлэл хулгайлагдсан тохиолдолд хэрэгжүүлэх цахим аюулгүй байдлын тохиолдлын хариу арга хэмжээний төлөвлөгөөг боловсруулах Сэжигтэй файлыг татаж авсан тохиолдолд ажилтнууд ямар алхам хийх, хэнд хандах талаар мэдлэгтэй байх журмыг хэрэглүүлэх

ASD-ийн ACSC-ийн Essential Eight-г хэрэгжүүл

- Өмнө дурдсан хамгаалах арга хэмжээнүүдээс гадна ASD-ийн ACSC-ийн Essential Eight-ийн үлдсэн хэсгийг хэрэгжүүлэхийг ACSC чухалчлан зөвлөж байна.

Зайнаас ажиллах үед ажилтанг мэдээллээр хангах

- Хувийн төхөөрөмж дэх байгууллагын мэдээллээ хамгаалах
  - Цахим эрүүл ахуйг сайтар төлөвшүүлж, сэжигтэй холбоос, үсэрдэг цонхон дээр дарахгүй байх, мэдэгдэхгүй эсвэл итгэмжлэгдээгүй эх сурвалжаас файл, программ татаж авахгүй байх
  - Ажлын болон хувийн хэрэгцээнд ялгаа бүхий өөр өөр нууц үг хэрэглэх Боломжтой бол хувийн аккаунтдаа давхар баталгаажуулалт (MFA)-г ашиглах
  - Ажлын сүлжээнд нэвтрэх мэдээллээ хувийн нууц үгийн санд хадгалахгүй байх, үүнийг ажил олгогчоос зөвшөөрсөн тохиолдолд л ашиглах. Үүнд таны вэб хөтчийн нууц үгийн сан ч багтана. **Хэрэв эргэлзэж байвал, ажил олгогчоосоо байгууллагын хэрэгцээнд ашигладаг нууц үгийн санг ашиглах хүсэлт гаргах.**
  - Ажлын аккаунтдаа олон хүн хуваажашигладаг эсвэл олон нийтийн төхөөрөмжөөс нэвтрэхгүй байх.
  - Өөрийн веб хөтчийн автоматаар бөглөх (autofill) функцэд ямар мэдээлэл хадгалагдаж байгааг анхааралтай хянах. Мэдээлэл хулгайлагч нь цахим хөтчийн автоматаар бөглөх маягтад хадгалагдсан мэдээллийг олж авахыг оролддог. Цахим маягт бөглөж байхдаа, зээлийн картын дугаар зэрэг эмзэг мэдээллийг автоматаар бөглөх функцэд хадгалахын оронд гараар шивж оруулахыг зөвлөж байна.
  - Интернэт ашигласныхаа дараа цахим хөтчийн, күүкиг цэвэрлэх, идэвхтэй аккаунтуудаас бүрэн гарах замаар мэдээлэл хулгайлагдахаас сэргийлэх.
  - Үйлдлийн системийнхээ вирусны эсрэг үндсэн програмыг идэвхжүүлсэн байх. Гуравдагч этгээдийн вирусны эсрэг програм ашигладаг бол шинэчилж, нэр хүндтэй найдвартай компанийн програмыг сонгох.

Туслалцаа

Мэдээлэл хулгайлагдсан эсвэл тусламж шаардлагатай Австралийн байгууллагууд ASD-ийн ACSC-т **1300 CYBER1 (1300 292 371)** дугаар болон cyber.gov.au/report сайтаар холбогдох боломжтой.

ASD-ийн ACSC нь байгууллагуудыг мэдээлэл хулгайлагч программтай холбоотой сэжиг бүхий үйл явц болон халдлагын шинж тэмдгүүдийг хохирол учруулсан эсэхээс үл хамаарч байнга мэдээлж байх хэрэгтэй. Таны өгсөн мэдээлэл дээр үндэслэн цахим аюул заналхийлэгчдийн арга тактик, техникүүдийг илүү сайн ойлгож, ижил төрлийн халдлагад өртсөн бусад Австралийн байгууллагуудыг сэрэмжлүүлэх боломжтой болдог.

Хариуцлагаас татгалзах мэдэгдэл

Энэхүү гарын авлагын материал нь ерөнхий агуулгатай бөгөөд хууль зүйн зөвлөгөө гэж үзэхгүй бөгөөд тодорхой нөхцөл байдал эсвэл яаралтай үед тусламж авахад түшиглэх ёсгүй болно. Ямар нэгэн ноцтой асуудал үүссэн бол өөрийн нөхцөл байдалд тохирсон, бие даасан мэргэжлийн зөвлөгөөг авахыг зөвлөж байна.

Энэхүү гарын авлагад агуулагдсан мэдээлэлд үндэслэн хийсэн аливаа үйлдлээс улбаалсан аливаа хохирол, алдагдал, зардлыг Холбооны улс хариуцахгүй.

Зохиогчийн эрх

Төрийн сүлдийг ашиглах эрх

Төрийн сүлдийг ашиглах нөхцөлийн талаарх дэлгэрэнгүй мэдээлэл болон зааврыг Ерөнхий сайд ба Засгийн газрын Тамгын газрын вебсайт Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au дээрээс авна уу.

Дэлгэрэнгүй мэдээлэл авах эсвэл цахим аюулгүй байдлын тохиолдлыг мэдээлэх бол бидэнтэй холбогдоно уу:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Энэ дугаарыг зөвхөн Австралийн дотор ашиглах боломжтой.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre