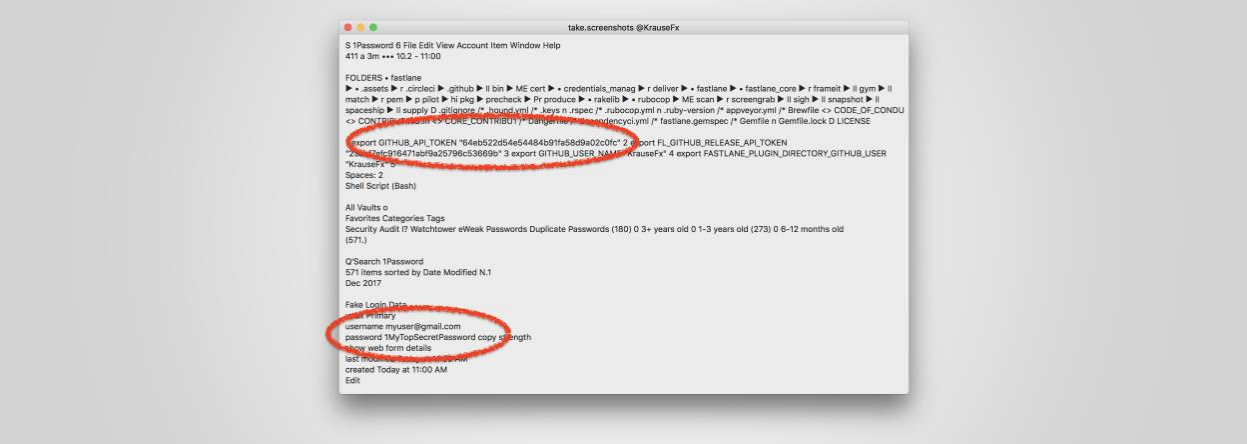
National Datacenter

DCERT

DATACENTER EMERGENCY RESPONSE TEAM

ХАЛДЛАГАД ХАРИУ ҮЙЛДЭЛ ҮЗҮҮЛЭХ БАГ

Хэрэглэгчийн Нууц үг, Нууц түлхүүр, Токенг хулгайлахад макYC (MacOS)[1] үйлдлийн системийн дэлгэцийн агшныг буулгах (Screenshot)[2] функцийг ашиглах боломжтой болохыг судлаач мэдээлжээ.



Хортой програм хөгжүүлэгчид макYC (macOS) API[3]-г нууцаар ашиглан хэрэглэгчийн дэлгэцийн агшны зургийг дарж, улмаар OCR[4] програмын тусламжтайгаар дэлгэц дээр байх текстийг унших үйлдлийг хийх боломжтой байна.

Хэрэглэгчийн компьютерын дэлгэц дээрх агшныг зураг болгох эсвэл дэлгэцийг видео хэлбэрээр бичих үйлдэл хийдэг Мак аппликэшн[5] нь ихэвчлэн CGWindowListCreateImage функцийг ашигладаг юм.

API функцийг хэрэглэгчийн эмзэг мэдээллийг унших ашиглах боломжтой

[1] Apple компанийн үйлдвэрлэсэн компьютерт ажиллах зориулалт бүхий үйлдлийн систем

[2] Screenshot буюу компьютерын дэлгэц дээр харагдаж байгаа зүйлсийг зураг болгон хадгалах функц

[3] Application Programming Interface - Аппликэшн програм зохиоход ашиглагддаг протокол, хэрэглүүр, дэд функц зэргийг хэлнэ.

[4] OCR (Optical Character Recognition) - Оптик зургаас тэмдэгт таних үйлдэл хийдэг програм

[5] Application - Програм

Фэйстлайн Түүлс[6] -ийг үүсгэн байгуулагч Пеликс Краус-ын хэлснээр, тухайн програм сэндбокс горим[7] -д ажиллаж байна уу үгүй юу гэдгээсээ үл хамааран Мак (Mac)-ийн аппликэшнүүд энэ функц рүү хандах эрхтэй ба эдгээр апплткэшн нь хэрэглэгчийн дэлгэцийн агшны зургийг нууцаар авах боломжтой байна.

Краус-ын үзэж байгаагаар халдлага үйлдэх зорилго бүхий этгээд энэхүү цоорхой дээр суурилан, CGIWindowLostCreateImage-г ашиглан хэрэглэгчийн зөвшөөрөлгүйгээр компьютерынх нь дэлгэцийн агшны зургийг дарах боломжтой байна.

Краус энэ эмзэг байдлыг туршиж үзсэн бөгөөд тэрээр CGIWindowListCreateImage-г ашиглан дэлгэцийн агшны зураг авч, улмаар OCR програм ашиглан төрөл бүрийн мэдээллийг унших боломжтой байснаа дурджээ. Түүний хэлснээр, халдлага үйлдэх зорилго бүхий этгээд дараах зүйлсийг хийж чадах гэнэ.

- Нууц үг болон нууц түлхүүрийн менежер програмаас мэдээллийг нь унших
- Эмзэг програмын эх код, API түлхүүрүүд эсвэл үүнтэй төстэй мэдээллийг унших
- Хэрэглэгчдийн мак (mac) компьютер дээрээ нээсэн имэйл болон мессежийг унших
- Хэрэглэгч ашиглаж буй веб үйлчилгээг мэдэх (жишээлбэл, имэйл үйлчилгээ үзүүлэгч, нууц үгийн менежер, аппликэшний жагсаалт гэх мэт)
- Хэрэглэгчийн банкны мэдээлэл, цалин, хаяг гэх мэт хувийн мэдээллийг мэдэх

Блийпинг Компьютер[8]-д илгээсэн имэйлдээ, Краус энэ эмзэг байдлын талаарх мэдэгдлийг Apple компанид өнгөрсөн оны арван нэгдүгээр сард албан ёсоор мэдэгдсэн болохоо дурдсан байна. Гэвч, энэ асуудал өнөөг хүртэл шийдэгдээгүй байгаа тул тэрээр энэ мэдээллээ олон нийтэд түгээж буйгаа өөрийн блогоороо дамжуулан хэлжээ. Ингэхдээ Apple-ийн олон нийтэд ил болсон алдаа хэсэгт энэхүү эмзэг байдлыг байрлуулсан байна.

[6] Fastlane Tools - Android болон iOS систем бүхий төхөөрөмж дээр програм хөгжүүлэх, байрлуулах үйлдлийг хялбарчлах зориулалт бүхий, нээлттэй эх код, платформ

[7] Sandboxed - Компьютер дээр ажиллаж буй програмыг тусгаарладаг аюулгүй байдлын механизм

[8] Bleeping computer - Компьютерын тусламж авдаг сайт

Судлаач энэ алдааны хор хөнөөлийг бууруулах боломжит шийдлийг санал болгожээ.

CGWindowListCreateImage функцийн энэхүү эрсдэлээс сэргийлэхэд хэрэглэж болохуйц зарим шийдлийг Краус санал болгосон байна.

Хэрэгжүүлэхэд хамгийн хялбар шийдэл нь дэлгэцийн агшинг буулгах эрх бүхий аппликэшн ашиглах үед тухайн хандах эрхийг зөвшөөрч байгаа эсэхийг хэрэглэгчээс асуудаг болгох. (Хэрэглэгчид анхааруулга өгч, зөвшөөрөл авах)

Түүний санал болгосон өөр нэг шийдэл нь аливаа аппликэшн хэрэглэгчийн дэлгэцийн агшны зургийг дарах бүрт хэрэглэгчид анхааруулга өгдөг байх, Мак (Mac) системийн аюулгүй байдлын програм дээр суурилан ийм төрлийн оролдлогыг хэрэглэгчид мэдэгдэж зөвшөөрөлгүй хандалт хийгдэж байгаа үед түүнийг блоклох.

“*Өнөөдөр Мак Аппликэшн (Mac Applications)-үүдээс дэлгэц бичих боломж бүхий олон аппликэшн байна. Жишээлбэл, 1Password 2fA дэмждэг эсвэл дэлгэцийн агшныг бичих зориулалт бүхий бүх төрлийн програмууд гэх мэт. Гэвч эдгээр програмуудад ямар нэгэн хяналт хэрэгтэй*.” хэмээн Краус хэлжээ.

Краус-ын хувьд энэ нь Apple компанийн хувь хүний нууцыг хамгаалах шийдлийг сул анхаарч үзэж буй анхных нь тохиолдол биш юм. Өнгөрсөн жил, тэрээр iOS төхөөрөмж дээрх зураг руу хандах эрх авч, тухайн зураг дээр хадгалагдсан байх хэрэглэгчийн байрлалтай холбоотой мэдээллийг задлан уншиж, хэрэглэгчийн гео-байрлалын мэдээлэл рүү хандаж байсан аппликэшнийг илрүүлж байсан юм.

Энэхүү нийтлэлд Краус-тай харилцсан имэйлийн дагуу өөрчлөлт оруулав. Краус олон нийтэд мэдэгдэхээс өмнө буюу өнгөрсөн арван нэгэн сард Apple компани руу энэхүү асуудлын талаар мэдээлэл хүргүүлсэн байна.

Эх сурвалж: https://www.bleepingcomputer.com/news/apple/researcher-uses-macos-app-screenshot-feature-to-steal-passwords-tokens-keys/

2018.2.27