شماره هشدار	W14040005	تاریخ	۱۴۰۴/۰۵/۱۱	تعداد صفحه	۳
سطح هشدار	بحرانی	بحرانی	زیاد	متوسط	کم
مخاطبین	کاربران شبکه های اجتماعی (یوتیوب، تیک تاک، توییتر، اینستاگرام، فیسبوک و ...)				
عنوان	نصب بدافزار در قالب دانلود فیلم از بستر شبکه های اجتماعی				

متن هشدار

در جدیدترین شـیوه‌های حملات سـایبری مبتنی بر مهندسـی اجتماعی، ترکیبی از سـایت‌های به ظاهر معتبر برای دانلود ویدیو از شـبکه های اجتماعی و صـفحات جعلی احراز هویت (Fake CAPTCHA Verification)برای فریب کاربران و نصب بدافزار مشاهده شده است. بررسی‌ها نشان می‌دهد که سـایت qdownloader.cc در مراحل خاصـی از فرآیند دانلود، کاربران را به سـایت مخرب fy3.fit هدایت می‌کند. نکته ای که وجود دارد این است که سایت qdownloader.cc توسط برخی از سایت های ایرانی تبلیغ شـده اسـت. همچنین سـایت qdownloader.cc اقدام به پذیرش تبلیغات از سـایت های مختلف بدون بررسـی محتوای آن ها می‌نماید که مجرمین از این فرصـت سـو اسـتفاده نموده و به دنبال اهداف مجرمانه خود هستند.

مراحل حمله :

۱. کاربر به قصد دانلود ویدیو وارد سایت qdownloader.cc می‌شود.
۲. پس از وارد کردن لینک ویدیو و کلیک روی گزینه "دانلود"، سـایت کاربر را به طور خودکار به دامنه‌ای ثالث با آدرس fy3.fit هدایت می‌کند.
۳. در fy3.fit، کاربر با صفحه‌ای مواجه می‌شود که در ظاهر مربوط به احراز هویت CAPTCHA است اما در واقعیت، یک صفحه جعلی و فریبنده است.
۴. این صفحه از کاربر می‌خواهد برای تأیید ربات نبودن اقدامات زیر را انجام دهد:
   - ترمینال ویندوز را باز کند (Windows + X سپس I)
   - کدی را که در کلیپ‌بورد قرار گرفته است، Paste (Ctrl + V) کرده و اجرا (Enter) نماید.

وب سایت: mirghazab.ir
شبکه‌های اجتماعی: @mirghazab_ir
شماره تماس : ۰۹۳۸۸۸۲۱۵۸۳
آی دی ادمین: @mirghazab_ir_admin

۵. کد مذکور یک اسکریپت مخرب است PowerShell میباشد که پس از اجرا فایل بدافزار را دانلود کرده و سپس فورا اجرا می کند.
۶. بر اساس بررسی های اولیه انجام شده بر روی فایل بدافزار مشخص گردید این فایل شامل تکه کد رمز گذاری شده ای است که با استفاده از سه مرحله رمزگشایی با استفاده از الگوریتم های رمزنگاری XOR،Base64 و AES به کد باینری تبدیل شده و در نهایت این کد باینری برای اجرا وارد رم میشود. (بررسی های فنی در خصوص ماهیت واقعی این بدافزار در حال انجام می‌باشد.)

از اینرو در استفاده از سایت های دانلود ویدیو از بستر یوتیوب نهایت دقت را به عمل آورید.

توصیه ها

- اجرای این فایل در سیستم واقعی اکیداً ممنوع است.
- از مراجعه به سایت qdownloader.cc و سایت‌هایی با عملکرد مشابه اکیداً خودداری نمایید.
- به هیچ عنوان هیچ دستوری را طبق درخواست وب‌سایت‌ها در ترمینال یا CMD وارد نکنید، حتی اگر ظاهر آن‌ها قانونی به نظر برسد.
- در محیط‌های دانشگاهی و سازمانی، دسترسی به دامنه‌های qdownloader.cc و fy3.fit را مسدود نمایید.
- اگر این فایل اجرا شده یا باز شده است:

۱. سیستم را فوراً از شبکه جدا کنید.
۲. با استفاده از آنتی ویروس سیستم را اسکن کامل کنید.

دانلود از یوتیوب با سایت qdownloader

QDownloader، که به عنوان یک ابزار دیگر برای دانلود از youtube معرفی شده است، به کاربران امکان دانلود ویدیوها را در کیفیت‌های مختلف می‌دهد. نحوه استفاده از این سرویس مشابه سایر سرویس‌ها است. کاربران باید لینک ویدیوی مورد نظر را وارد کنند و سپس فرمت و کیفیت دلخواه خود را برای دانلود انتخاب نمایند.

لینک مستقیم سایت QDownloader