|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **شماره هشدار** | W14040005 | **تاریخ** | 1404/05/11 | **تعداد صفحه** | 3 |
| **سطح هشدار** | C:\Users\SCADA\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Untitled-1.png  **بحرانی**  بحرانی  زیاد  متوسط  بحرانی  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 شیوه‌های حملات سایبری مبتنی بر مهندسی اجتماعی، ترکیبی از سایت‌های به ظاهر معتبر برای دانلود ویدیو از شبکه های اجتماعی و صفحات جعلی احراز هویت (Fake CAPTCHA Verification) برای فریب کاربران و نصب بدافزار مشاهده شده است. بررسی‌ها نشان می‌دهد که سایت qdownloader.cc در مراحل خاصی از فرآیند دانلود، کاربران را به سایت مخرب fy3.fit هدایت می‌کند. نکته ای که وجود دارد این است که سایت qdownloader.cc توسط برخی از سایت های ایرانی تبلیغ شده است. همچنین سایت qdownloader.ccاقدام به پذیرش تبلیغات از سایت های مختلف بدون بررسی محتوای آن ها می‌نماید که مجرمین از این فرصت سو استفاده نموده و به دنبال اهداف مجرمانه خود هستند.  مراحل حمله :   1. کاربر به قصد دانلود ویدیو وارد سایت qdownloader.cc می‌شود. 2. پس از وارد کردن لینک ویدیو و کلیک روی گزینه "دانلود"، سایت کاربر را به طور خودکار به دامنه‌ای ثالث با آدرس fy3.fit هدایت می‌کند. 3. 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. 4. 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. 5. کد مذکور یک اسکریپت مخرب است PowerShell میباشد که پس از اجرا فایل بدافزار را دانلود کرده و سپس فورا اجرا می کند. 6. 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 Base64، XOR 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:  1. سیستم را فوراً از شبکه جدا کنید. 2. با استفاده از آنتی ویروس سیستم را اسکن کامل کنید. | | | | | | |



