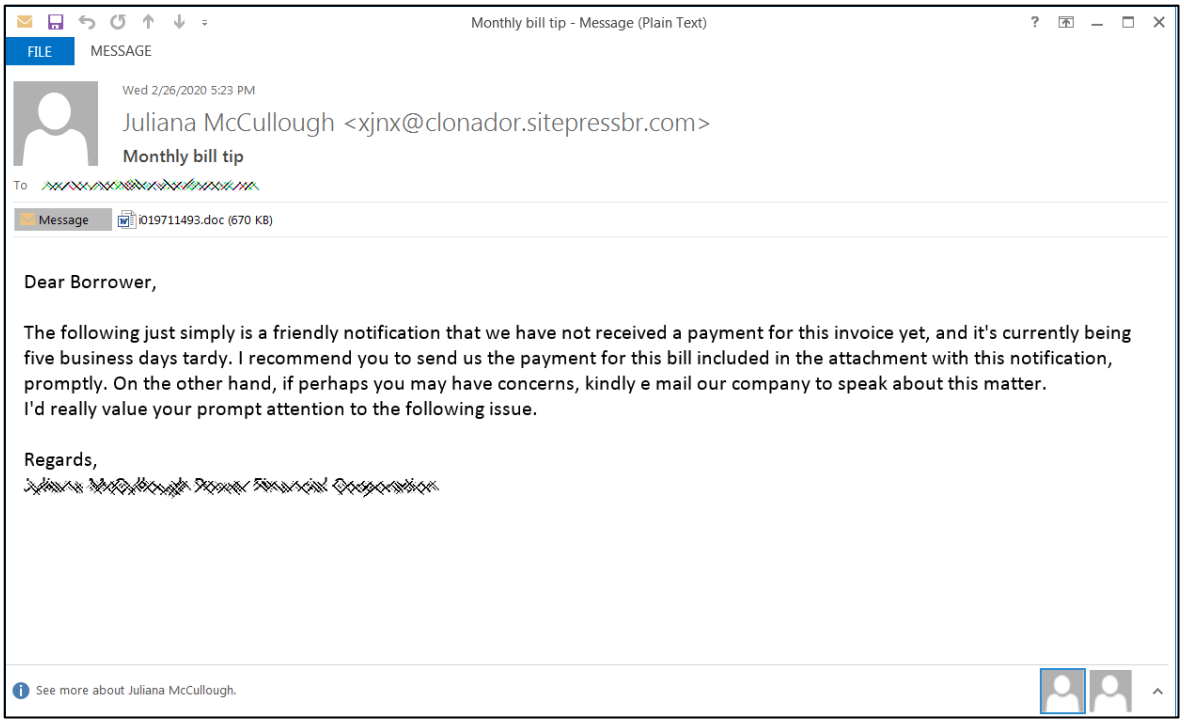
بسمه تعالی

استفاده از RDP ActiveX Control در ویندوز ۱۰ توسط بدافزار Trickbot

اخیراً مهاجمان برای اجرای خودکار یک بدافزار دانلود کننده به نام Ostap که پیش‌تر به‌کارگیری آن توسط بدافزار Trickbot مشاهده شده بود، از Remote Desktop ActiveX Control در ویندوز ۱۰ و مستندات ورد استفاده می‌کنند. ویژگی Remote Desktop ActiveX Control به مایکروسافت اجازه می‌دهد تا مرتباً سیستم عامل را برای محافظت هر چه بیشتر از سیستم به‌روزرسانی کند؛ اما در این حمله از این ویژگی برای اجرا ماکروهای مخرب که حاوی بدافزار دانلودکننده‌ی Ostap هستند، استفاده شده است. در این گزارش به بررسی عملکرد این بدافزار می‌پردازیم.

۱ آغاز کار با فیشینگ

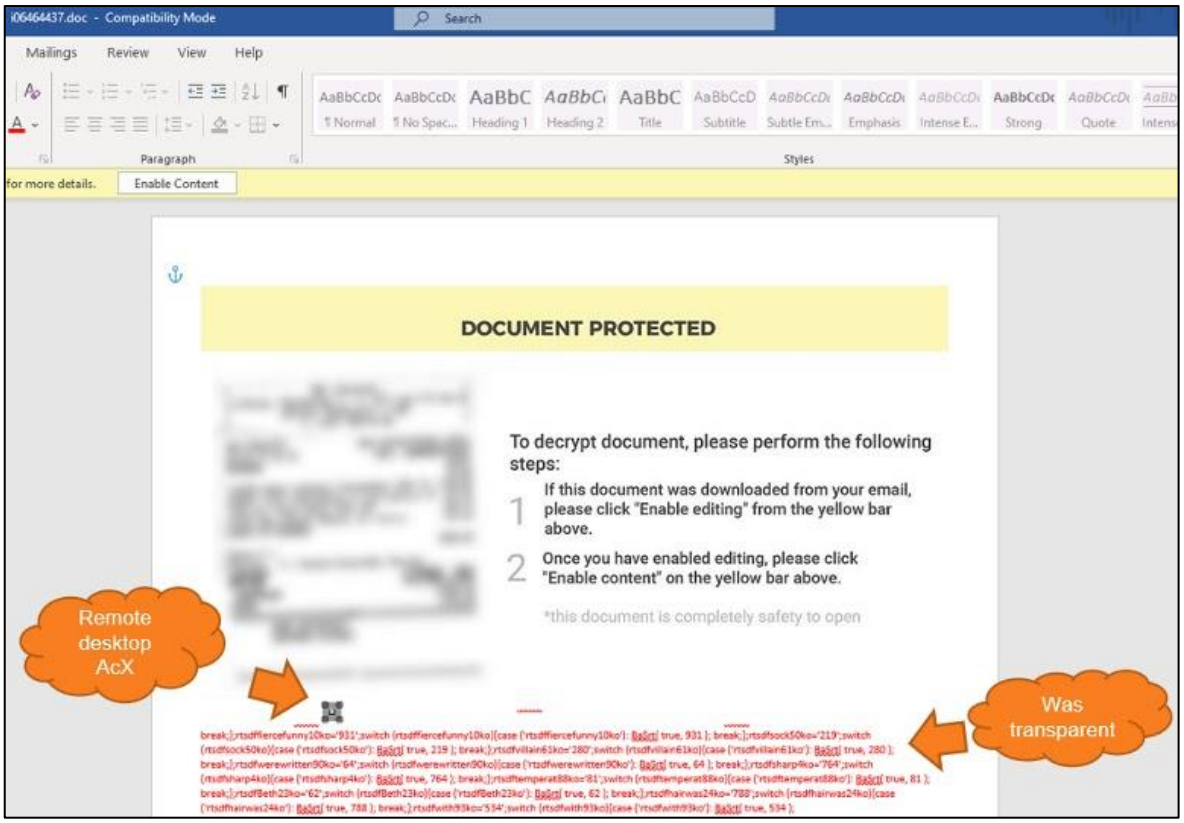
بدافزار دانلود کننده Ostap، از طریق مستند word آلوده به کد ماکرو و حاوی تصویری که رمزنگاری شده است، کاربران را به سمت فعال کردن ماکرو در مستند ورد سوق می‌دهند. فایل ورد مخرب از طریق ایمیل‌های فیشینگ به دست قربانی می‌رسد. شکل زیر نمونه ایمیل فیشینگ به همراه فایل ورد مخرب پیوست شده به آن را نشان می‌دهد.



شکل شماره ۱: نمونه ایمیل فیشینگ دریافت شده

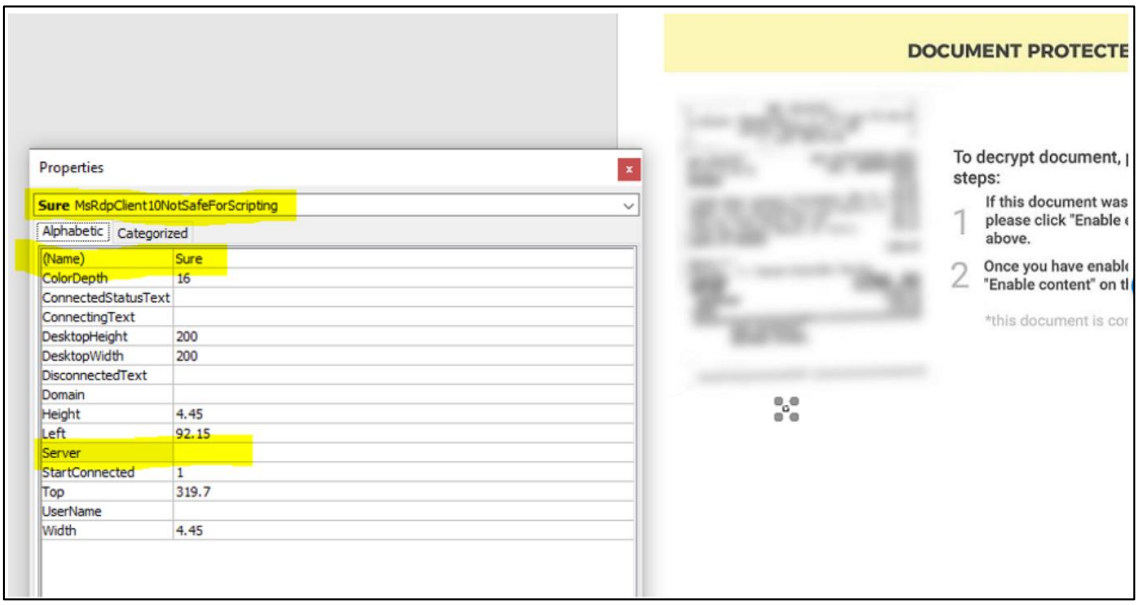
اغب فایل‌های ورد مخرب از قالب «*i<7-9 random digits>.doc*» در نامگذاری پیروی می‌کنند. در ادامه به بررسی نمونه فایل ورد دانلود شده از یکی از ایمیل‌های فیشینگ می‌پردازیم.

مهاجمان از نوعی تکنیک مهندسی اجتماعی و با استفاده از تصویری که در شکل شماره ۲ مشاهده می‌شود، برای متقاعد کردن کاربر برای فعال کردن گزینه‌ای که منجر به اجرای کد ماکرو مخرب می‌شود، استفاده می‌کنند؛ در همین حین یک ActiveX control واقع در زیر تصویر مذکور که در حالت عادی به دلیل فونت سفید رنگ مشخص نیست، پنهان شده است. بدافزار دانلود کننده Ostap بین خطوط سفید رنگ پنهان شده که توسط سیستم خوانده می‌شود ولی کاربر از وجود آن بی‌اطلاع خواهد بود.



شکل شماره ۲: نمونه فایل ورد دانلود شده از ایمیل فیشینگ دریافت شده

بررسی ActiveX control توسط محققان، استفاده‌ی آن از کلاسی به نام MsRdpClient10NotSafeForScripting را برای کنترل از راه دور اثبات می‌کند. همان طور که در شکل زیر مشاهده می‌شود فیلد مربوط به Server در اسکریپت خالی است که بعدها منجر به بروز خطا و سو استفاده‌ی مهاجمان از آن برای اجرای کد دلخواه می‌شود.



شکل شماره ۳

۱-۱ بررسی ماکرو

تابعی به نام «*<name>_OnDisconnected*» در ماکرو که وظیفه حل DNS دریافتی را دارد درصورت دریافت یک رشته خالی، خطا برمی‌گرداند و بدافزار OSTAP تنها درصورتی اجرا می‌شود که شماره‌ی خطا برابر با ۲۶۰ یعنی «*disconnectReasonDNSLookupFailed*» باشد. در ادامه OSTAP، به یک فایل BAT تغییر شکل داده و منجر به اجرای آن فایل و متعاقباً بسته شدن فایل ورد می‌شود.

با توجه به مشکلات امنیتی متعدد ویندوز ۱۰ و روش‌های گوناگون برای سوءاستفاده از آنها توسط مهاجمان، توصیه می‌شود هر چه سریع تر به به‌روزرسانی سیستم عامل ویندوزی خود اقدام کنید.

جهت اطلاع از جزییات فنی بیشتر به لینک زیر مراجعه کنید:

https://blog.morphisec.com/trickbot-delivery-method-gets-a-new-upgrade-focusing-on-windows

۲ مراجع

[۱] https://blog.morphisec.com/trickbot-delivery-method-gets-a-new-upgrade-focusing-on-windows

[۲] https://www.bleepingcomputer.com/news/security/hackers-use-windows-10-rdp-activex-control-to-run-trickbot-dropper/