禪

[illegible]

File Edit View VM Tabs Help
Recycle Bin
Mozilla Firefox
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\localadmin>query user
USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME
sensitiveuser 1 Disc . 3/12/2017 12:34 PM
>localadmin console 2 Active none 3/12/2017 12:45 PM
C:\Users\localadmin>tscon _
YouTube
1:00 / 2:22

[illegible]

[illegible] (sessions) [illegible]

[illegible]

[illegible]

آینده دنیای امنیت را به دستان پرتوان هوش مصنوعی بسپاریم

این اتفاق در شرایطی رخ میدهد که هیچگونه هشداری از بابت به سرقت رفتن نشست به کاربر نشان داده نخواهد شد. کوزینوفسکی گفته است: «تکنیکی که موفق به شناسایی آن شدم، همیشه دسترسی کامل به یک حساب با حداکثر مجوزها را امکانپذیر نمیسازد . اما این پتانسیل را دارد تا از سوی مدیران شبکه برای دسترسی به حسابهایی با مجوزهای کمتر مورد استفاده قرار گیرد . همچنین این پتانسیل را دارد تا دسترسی به یکسری برنامههای حساس شرکتی و بانکهای اطلاعاتی را امکانپذیر سازد .»

او در پست خود نوشته است: «کارمندی را فرض کنید که سامانه صدور صورتحسابها در اختیار او قرار دارد . او روز کاری خود را با ورود به سامانه صدور صورتحساب شروع میکند . در یک استراحت کوتاه ایستگاه کاری خود را قفل میکند . در ادامه مدیر سیستم با حساب کاربری خود به سیستم وارد میشود . با توجه به سیاستهای بانک، مدیر نباید به سامانه صدور صورتحساب تحت کنترل کارمند خود وارد شود . اما مدیر از طریق فرمانهای از پیش ساخته شده در ویندوز، این توانایی را دارد تا نشستها روی دسکتاپ کارمندان خود را به سرقت ببرد . این موضوع کاملا شوکه کننده است. اکنون مدیر این توانایی را خواهد داشت تا یکسری فعالیتهای خرابکارانه را در سامانه صدور صورتحساب و با همان حسابکاربری مسئول مربوطه پیادهسازی کند . همانگونه که در ویدیو نحوه پیادهسازی چنین حملهای را نشان دادم، تمامی این کارها در کمتر از 30 ثانیه انجام میشود .»

مطلب پیشنهادی

معرفی بهترین کتابهای دنیای فناوری

۵ کتاب پیشنهادی برای علاقهمندان امنیت

کورزینوفسکی این مکانیزم حمله را "آسیبپذیری با درجه بالا " نامگذاری کرده است . اما گفته است: «مطمئن نیستم این تکنیک یکی از ویژگیهای ویندوز است یا در اصل یک رخنه امنیتی است .»

در مستندات مایکروسافت آمده است ابزارهای ویندوز با محدودیتهایی همراه هستند . به طور مثال، زمانی که کاربر در وارد کردن گذرواژه دچار اشتباه میشود، یکسری محدودیتها برای او در نظر گرفته میشود. اما به نظر میرسد نمونه ارائه شده از سوی این کارشناس امنیتی چیز دیگری را نشان میدهد . کوین بیومونت، کارشناس امنیتی وجود این باگ را در توییتی تایید کرده و گفته است به شکل خیلی سادهای میتوان حسابها را به سرقت برد .

کورزینوفسکی میگوید : «این باگ را روی سیستمهای ویندوز 7، ویندوز 10، ویندوز 2008 و ویندوز سرور 2012 سرویس پک دو مورد آزمایش قرار دادهام . این رخنه در این سیستمعاملهای فوق وجود دارد . من وجود این رخنه را هنوز به مایکروسافت گزارش نکردهام . همه فعالیتهای مخرب تنها از طریق ابزارهای از پیش ساخته شده انجام میشود . هر مدیری میتواند خود را به جای یک کاربری که به طور محلی و از طریق فیزیکی یا از راه دور به سیستمی وارد شده است جا بزند . » اما بیومونت میگوید این رخنه در تمامی سیستمعاملهای ویندوز وجود دارد .

سخنگوی مایکروسافت در واکنش به این اظهارنظرها گفته است : «این یک رخنه امنیتی نیست بلکه ویژگی است که مدیران محلی برای دسترسی درست به یک ماشین به آن نیاز دارند .»

نویسنده :
