禪

[illegible]

[illegible] 10 [illegible] [illegible] [illegible] [illegible]

[illegible]

[illegible] Windows Defender ATP Research [illegible] TechNet [illegible] 10 [illegible] ATP [illegible] «[illegible]: [illegible] [illegible] [illegible]

مطلب پیشنهادی

Administrator

وقتی رمز عبور ویندوز را فراموش کردهاید ...

آموزش ورود به ویندوز 10 با تغییر رمز عبور مدیر سیستم **(Admin)**

مسدود کردن دستورات پاورشل

بهروزرسانی Creators Update قرار است قابلیتهای منحصر به فردی را در اختیار کاربران قرار دهد. به طور مثال در این بهروزرسانی دستگاههایی که به بدافزارها آلوده باشند از شبکه جدا شده و ایزوله میشوند. این رویکرد به مدیران شبکه این توانایی را میدهد تا زمان بیشتری برای مقابله با تهدیدات بدافزاری داشته باشند و همچنین فایلهای حساس را از روی کامپیوترهایی که در معرض تهدید قرار گرفتهاند، به سرعت پاک کنند. به طور مثال، ویژگی ATP در ویندوز 10 این توانایی را دارد تا یک دستور پاورشلی که ممکن است برای انتشار آلودگی Cerber مورد استفاده قرار میگیرد را شناسایی کرده و مانع از اجرای این دستور شود، حتا زمانی که آنتیویروس سیستم کاربر در وضعیت غیرفعال قرار دارد. بلیزاد میگوید: «این سیستمعامل به راحتی قادر به مسدود کردن اسکریپتهای پاورشلی خواهد بود که قصد دارند در پسزمینه فایلهای آلوده را دانلود کنند. در همین حال Windows Defender ATP هر زمان پاورشل به یک سایت ناشناس متصل شود هشداری را به کاربر نشان میدهد. سایتهایی که به منظور دانلود یک فایل اجرایی از یک پروکسی عمومی استفاده میکنند. پرسنل مرکز عملیاتهای امنیتی مایکروسافت (SOC) سرنام Security operations center میتوانند از چنین هشدارهایی برای استخراج آدرس IP مبدا و بلوکه کردن آدرس IP در یک دیوارآتش استفاده کنند. در نتیجه مانع از آن میشوند تا ماشینهای دیگر همان فایل اجرایی مخرب را دانلود کنند. ما متوجه شدهایم فایلهای اجرایی که به این شکل دانلود میشوند همواره باجافزار هستند».

مطلب پیشنهادی

بازگشت ویژگیهای مستتر و قدرتمند به ویندوز 10

ویژگیهای قدرتمند ویندوز 10 که ازشان بیخبر هستید!

اما در این میان نباید از نقش مرورگر مایکروسافت اج غافل شویم. این مرورگر به ویژگی قدرتمندی تجهیز خواهد شد که اجازه نخواهد داد کیتهای اکسپلویت و باجافزارها به درون یک سامانه کامپیوتری وارد شوند. برای این منظور مایکروساف اج از ویژگی SmartScreen Filter استفاده میکند. این ویژگی آدرسهای اینترنتی را بر مبنای یک سیستم اعتبارسنجی مورد ارزیابی قرار میدهد. در نتیجه دسترسی به سایتهایی که پذیرای بدافزارها هستند امکانپذیر نخواهد بود. تقریبا دو سال پیش بود که ساتیا نادلا اعلام کرد ویندوز 10 امنترین سیستمعاملی خواهد بود که کاربران از آن استفاده خواهند کرد. سیستمعاملی که به راحتی در ارتباط با اینترنت اشیا میتواند مورد استفاده قرار گیرد. اینگونه به نظر میرسد که در حال نزدیک شدن به زمانی هستیم که نادلا دو سال پیش وعده آنرا داده بودند.

نویسنده :
حمیدرضا تائبی

دسته بندی:
امنیت
تاریخ انتشار :
09:46 - 19/11/1395
برچسب:
ویندوز 10 - امنیت - سیستم عامل - بدافزار - باج افزار - Creators Update - Windows Defender ATP - مایکروسافت

▯▯▯▯▯ منبع: https://www.shabakeh-mag.com/security/6697