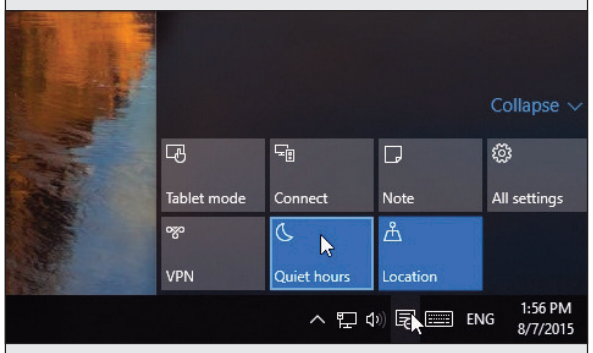
ترفند ویندوز

ساعت آرام در ویندوز ۱۰



در ویندوز ۱۰ حالتی به نام Quiet Hours یا ساعات آرام وجود دارد که در صورت فعال بودن آن، در ساعات بین ۱۲ نیمه‌شب تا ۶ صبح پیام‌های اطلاع‌رسانی ویندوز و نرم‌افزارها از حالت نمایش خارج شده و می‌توانید این ساعات را با آرامش سپری کنید. به عنوان مثال اگر تلگرام را بر روی ویندوز نصب کرده باشید، در این ساعات پیام‌های اطلاع‌رسانی آن نمایش داده نمی‌شود و مزاحمتی برای‌تان ایجاد نخواهد شد. اما ممکن است زمانی که نیاز به آرامش داشته باشید خارج از ۱۲ تا ۶ صبح باشد. در قسمت تنظیمات ویندوز گزینه‌ای برای تغییر این ساعات وجود ندارد و برای این کار بایستی از طریق ویرایشگرهای رجیستری یا Group Policy اقدام نمایید. در ادامه به نحوه انجام این کار می‌پردازیم.

فعال کردن Quiet Hours

برای فعال‌سازی ساعات آرام در ویندوز ۱۰ کافی است ابتدا کلیدهای ترکیبی Win+A را فشار دهید تا نوار Action Center نمایان شود. سپس با انتخاب Quiet Hours آن را فعال کنید.

تغییر زمان Quiet Hours از طریق ویرایشگر رجیستری

بر روی دکمه Start کلیک کرده و عبارت regedit را وارد نموده و Enter بزنید.

در محیط رجیستری به مسیر زیر بروید:

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion

اکنون بر روی کلید CurrentVersion راست‌کلیک کرده و از منوی New بر روی Key کلیک کنید. نام این کلید جدید را QuietHours قرار دهید.

حالا بر روی کلید QuietHours راست‌کلیک کرده و از منوی New بر روی DWORD (32-bit) Value کلیک کنید. نام این مقدار جدید را EntryTime قرار دهید. برای بار دوم نیز یک DWORD (32-bit) Value ایجاد کنید و نام آن را ExitTime قرار دهید. مقدار موجود در EntryTime بیان‌گر زمان آغاز ساعات آرام و ExitTime بیان‌گر زمان پایان ساعات آرام خواهد بود. بر روی EntryTime دوبار کلیک کنید. در پنجره بازشده، Decimal را فعال نمایید. سپس در قسمت Value data، میزان دقیقه بعد از نیمه شب که مایلید ساعات آرام فعال شود را وارد نمایید. به عنوان مثال اگر مایلید زمان خاموش از ساعت ۲ نیمه شب آغاز شود، بایستی عدد ۱۲۰ را وارد نمایید(۱۲۰ دقیقه بعد از نیمه شب برابر با ساعت ۲ نیمه شب). سپس روی OK کلیک کنید. همچنین در خصوص پایان زمان نیز روی ExitTime دوبار کلیک کنید، Decimal را انتخاب کنید و زمان را بر حسب دقیقه بعد از نیمه شب وارد نمایید. به عنوان مثال عدد ۶۰۰ به معنای ۶۰۰ دقیقه بعد از نیمه شب و برابر با ساعت ۱۰ صبح خواهد بود. در پایان روی OK کلیک کنید. تغییرات بلافاصله اعمال خواهد شد. در این مثال زمان ساعات آرام به ۲ نیمه شب الی ۱۰ صبح تغییر داده شد. برای بازگردانی به حالت اولیه نیز کافی است کلید QuietHours که ایجاد کردید را Delete نمایید.

یک بازار زیر زمینی برای فروش اطلاعات سرورهای هک شده

اطلاعات ۷ هزار سرور هک‌شده، به‌حراج گذاشته‌شدند

مجرمان و مهاجمان سایبری در دو سال گذشته به نوع جدیدی از بازار زیرزمینی پرداختند که به xDedic معروف است، در این پلتفرم، مجرمان سایبری می‌توانند تعداد زیادی سرور هک‌شده از سراسر دنیا را خریداری کنند. براساس این گزارش از شبکه‌های دولتی گرفته تا سازمانی، هرگونه سروری در xDedic قابل دست‌یابی است و میانگین قیمت‌ها هم تنها ۶ دلار برای هر سرور است. به این معنی که با پرداخت این مبلغ، خریدار می تواند به تمام اطلاعات روی سرور دست یافته و حتی ممکن است بتواند حملات مجددی نیز انجام دهد. محققان در لابراتوار کسپرسکی در مورد فروم xDedic مقاله‌ای منتشر ساخته‌اند که ۷۰۰۰ سرور در آن قربانی حملات سایبری شده‌اند که این هک توسط یک گروه هکر روسی زبان بوده است. اعضای سازنده فروم با ابزار ریموت سرور چندین یوزر را پشتیبانی می‌کند و همچنین دیگر ابزارهای هک proxy installers و sysinfo collectors می باشد که توسط محققان کسپرسکی گزارش شده است. هدف اصلی فروم xDedic خرید و فروش سرورهای هک‌شده ای است که از طریق ریموت در دسترس هستند. محققان در مورد xDedic با همکاری یک ISP اروپایی به بررسی قربانیان پرداختند. بر اساس این گزارش در ماه مه ۲۰۱۶، نشان می‌دهد ۷۰۶۲۴ سرور از ۱۷۳ کشور جهان برای فروش گذاشته شده بود. محققان گفتند میزان ۴۱۶ فروش در ماه مه و کمتر از ۴۲۵ در ماه آپریل رخ داده است. این در حالی است که بالای ۵۱۰۰۰ سرور از ۱۸۳ کشور جهان برای فروش روی این پلتفرم قرار داده شده بود. این آمار نشان می‌دهد که بر روی این فروم مدیریت مستقیم وجود داشته است. هنگامی که کاربران برای استفاده از فروم xDedic ثبت نام می‌کنند آن‌ها می‌توانند برای دیدن لیستی از سرورهای در دسترس از داشبورد استفاده کنند. در این فروم برای هر سرور هک‌شده، لیستی از اطلاعات سیستم، دسترسی‌های مدیریتی، ران بودن آنتی‌ویروس بر روی سیستم، بروزر، اطلاعات آپ‌تایم، سرعت آپلود و دانلود قابل دسترس است. ۳۲ درصد از سرور های هک‌شده در ماه مه و در کشورهای برزیل، چین، روسیه، هند و اسپانیا بود. دسترسی از طریق ریموت دسکتاپ این امکان را به خریداران می دهد که بتوانند به‌صورت ریموت به سیستم‌های در معرض خطر دسترسی داشته باشند و همچنین بتوانند به‌طور فزاینده‌ای به سرورهای در دسترس، مانند؛ سرویس‌های سازمان‌های مالی، سیستم‌های شرطبندی، فروشگاه‌های اینترنتی، سایت‌های دوست‌یابی، شبکه‌های تبلیغاتی و ... حمله کنند. در بعضی موارد خریداران به دنبال میزبانی سرور برخی از نرم‌افزار های خاص مثل حسابداری، گزارش‌های مالیاتی و نرم‌افزار های فروش بودند و علاوه بر این‌ها در پی نرم‌افزار ایمیل برای استفاده اسپم بودند. نرم‌افزار point of sales (نرم‌افزار فروش) از جمله نرم‌افزارهای محبوبی بود که محققان کسپرسکی اشاره کردند این نرم‌افزار در ۴۵۳ سرور از ۶۷ کشور در دسترس قرار گرفته است. محققان کشف کردند که هریک از پارتنرها به پرتال و ابزار آن‌ها دسترسی جداگانه خود را همچنان دارند. همچنین محققان اعلام کردند این پارتنرها با استفاده از یکی ازابزارهای اعتبارسنجی که SysScan نام دارد برای دسترسی به سرورهایی که در این فروم‌ها فروخته شده است استفاده می‌کنند، آن‌ها همچنین می‌گویند این ابزار اطلاعات سیستمی مانند سرعت دانلود و آپلود و همچنین نرم‌افزارهای نصب‌شده روی سرور را گزارش می‌دهد. در یک دستگاهی که در آن SysScan پیدا شده بود محققان گزارش کردند آن‌ها ابزاری (DUBrute and XPC) را یافتند که با استفاده از روش Brute Force 1برای رسیدن به اطلاعات سرور استفاده می‌کردند. با استفاده از اطلاعات تروجان SCClient، کسپرسکی برای این بدافزار تله‌گذاری کرد تا سرورهای هک‌شده با بدافزار مشابه را شناسایی کند. لابراتوار کسپرسکی گفت در عرض ۱۲ ساعت نخست ۳۶۰۰ آی‌پی آدرس به آن‌ها متصل شدند که سازمان‌های دولتی و دانشگاه‌ها هم جزء این آمار بودند و کسپرسکی مشتریان خود را از وجود این بدافزار آگاه کرده است. همچنین یک ابزار دیگر روی دستگاه‌های به خطر افتاده پیدا شد که پورت‌های مشخصی را روی سرورها باز می‌کند و آن‌ها را به SOCKSهای غیرمجاز یا پروکسی‌های HTTPS تبدیل می‌کند. محققان گفتند، xDedic ریموت دسکتاپ مخصوص خود را ساخته که مشتریان مجبورند اطلاعات لاگین را در این ریموت دسکتاپ کپی کنند. کسپرسکی در گزارش خود حدس می‌زند تنوع و قیمت پایین سرور های موجود فقط در خدمت مجرمان نبوده بلکه باندهای 2ATP هم از آن به خوبی سود برده‌اند. این گزارش می‌گوید؛ تعداد زیادی از سرورهایی که در بازار زیرزمینی xDedic برای فروش گذاشته‌شده، جایگزین بسیار مناسب و ارزانی برای گردانندگان ATP هایی است که نمی‌خواهند ردی از خود باقی بگذارند. ۸ دلار، برای هدفی با منظور دسترسی به تمام اطلاعات پروفایل، قیمت ناچیز و ارزانی است. موضوعی که معمولاً نادیده گرفته می‌شود این است که؛ سرورهایی که با روش brute-force هک می شوند فرصت مناسبی را برای گردانندگان ATP ها فراهم می‌کنند تا بدون اینکه سوءظنی متوجه آن‌ها شود کار خود را انجام دهند.