禪

# چرا ویندوز 10 با این دو ویژگی امنترین سیستمعامل مایکروسافت شد (بخش پایانی)


Windows 10

تاکنون مطالب بسیاری در ارتباط با ویندوز 10، ترفندهای ویندوز 10 و مواردی که در ارتباط با جنبههای ظاهری ویندوز 10 هستند را به رشته تحریر درآوردهایم. اما امنیت در ویندوز 10 آنگونه که باید مورد بررسی قرار نگرفته است. در بخش اول این مقاله نگاهی به Device Guard داشتیم و سعی کردیم کمی به درون مؤلفههای امنیتی ویندوز 10 وارد شویم. در بخش پایانی این مقاله در نظر داریم، ضمن بررسی Credential Guard به تعاملات سازمانها و موانعی که بر سر راهکارهای امنیتی ویندوز 10 قرار دارند، اشاره کنیم.

ایان ترامپ رهبر گروه امنیتی LogicNow در توصیف ویژگی Device Guard گفته است:« این یک قابلیت بسیار شگفتانگیز برای ویندوز به شمار میرود. بهطوری که ظرفیت تبدیل شدن به یک استاندارد جهانی را دارد. »

مطلب پیشنهادی: چرا ویندوز 10 با این دو ویژگی امنترین سیستمعامل مایکروسافت شد (بخش اول)

## رازهای ایزولهسازی

Credential Guard شاید به اندازه Device Guard هیجانبرانگیز نباشد؛ اما به حقیقت مهمی در زمینه امنیت سازمانی اشاره میکند. Credential Guard این توانایی را دارد تا اعتبارنامههای دامنه را درون یک کانتیر مجازی ذخیره کند. بهطوری که این اطلاعات به صورت تفکیک شده از مدهای کاربری و

هسته ویندوز ذخیره شوند . این مکانیزم باعث میشود، حتی اگر یک ماشین در معرض تهدید قرار گیرد، اعتبارنامهها در دسترس هکرها قرار نگیرد . حملات پیشرفته پایدار برای آنکه بتوانند دامنه و اعتبارنامههای کاربری را به سرقت ببرند و به کامپیوترهای دیگر دسترسی داشته باشند، بهطور مستمر شبکههای کامپیوتری را زیر نظر دارند . بهطور معمول زمانی که کاربری به سیستم خود وارد میشود، هشهای مربوط به اعتبارنامه او در حافظه سیستمعامل ذخیره میشوند . نسخههای پیشین ویندوز اعتبارنامه را در Local Security Authority ذخیره میکردند . در این حالت سیستمعامل برای دسترسی به این اطلاعات از remote Procedure Calls استفاده میکرد . در این حالت بدافزار یا هکری که در کمین شبکهها نشسته بود، توانایی به سرقت بردن هش اعتبارنامهها را داشت . این هشهای به سرقت رفته برای حملات pass-the-hash مورد استفاده قرار میگرفت . با ایزوله کردن اعتبارنامهها در کانتینرهای مجازی، Credential Guard از دسترسی هکرها جلوگیری به عمل آورده و مانع از سرقت هشها میشود . ترکیب Device Guard و Credential Guard توانایی قفل کردن یک محیط و متوقف ساختن حملات ATP را نیز دارند . ترمپ با اشاره به این موضوع که هرچند پیادهسازی راهکار پیشنهاد شده از سوی مایکروسافت به سادگی راهحلهای سازندگان دیگر نیست، اما ترکیب ویژگیهای امنیتی همچون ، Device Guard، Credential Guard، Microsoft Hello، احراز هویت دو عاملی و BitLocker ویندوز 10 را تبدیل به سیستمعامل ارزشمندی برای سازمانها کرده است . ویندوز 10 به ویژه برای سازمانهایی که در معرض حملات شدید قرار دارند یک راهبرد استراتژیک محسوب میشود..»

## ویژگیهای جدید و قدرتمندی که در اختیار همه کاربران قرار ندارند !

وینیوسکی پیشبینی کرده است که هر چند ویژگیهای امنیتی جدید هیجانبرانگیز هستند اما دارای محدودیتهایی هستند. در حالی که ویندوز 10 در ماههای آینده در حوزه سازمانی یکه تازی خواهد کرد، اما تغییرات زیرساختی و نیازهای سختافزاری Device Guard و Credential Guard حداقل به چهار یا پنج سال زمان نیاز دارند . همین موضوع عامل اصلی به تعویق افتادن نفوذ و گسترش این پلتفرم شده و میزان نفوذ آنرا دستخوش تغییراتی میکند . برای فعالسازی Device Guard و Credential ماشینها نیازمند Secure Boot، مجازیسازی 64 بیتی، رابط متحد توسعهپذیر سیستمعامل UEFI (سرنام Unified Extensible Firmware Interface ) و تراشه TPM ( سرنام Trusted Platform Module ) هستند.

این محدودیتهای سختافزاری تنها محدود به سازمانها نمیشود، بلکه کامپیوترهای مصرفکنندگان نیز با محدودیتهایی در این مواجه هستند . به طور مثال، در حالی که لپتاپهای تجاری Lenovo ThinkPad و Dell Latitude از ویژگیهای موردنیاز ویندوز 10 برخوردار هستند، اما در طرف مقابل مدلهایی از قبیل Lenovo Yoga 3 Pro این ویژگیها را در اختیار ندارند . محافظت سطح هایپرویزور تنها در ماشینهایی در دسترس است که پردازنده ماشین مجازی به فناوریهای مجازیساز از قبیل Inter VT-x و AMD-V مجهز باشد. بهطور مثال اولترابوکها فاقد تراشه TMP هستند. اما سختافزار تنها مانع تحقق یافتن این فناوریها نیست. بسیاری از سازمانها باید تغییراتی را در زیرساختها و فرآیندهای خود پیادهسازی کنند . بیشتر تیمهای IT هنوز هم از فناوریهایی همچون UEFI یا Secure Boot بوت استفاده نمیکنند، به دلیل اینکه این کار بر روند کاری آنها تأثیرگذار است . به همین شکل بعضی از سازمانها به ماشینهایی وابسته هستند که از برنامههای حیاتی خاص خود استفاده میکنند، همین موضوع باعث میشود، امکان ارتقا برای چنین سازمانهایی به سختی فراهم شود . اما خبر خوش این است که Device Guard و Credential Guard بهطور همزمان به همه این امکانات نیازی ندارند . شرکتهای فناوری میتوانند از یک راهکار ویژه در این زمینه استفاده کنند . به عبارت دیگر شرکتها میتوانند یک دامنه را همسو با Device Guard و Credential Guard ایجاد کرده و کاربرانی که از این نیازهای سختافزاری پشتیبانی میکنند را به سمت این دامنه هدایت کنند . ماشینهایی که توانایی ارتقا ندارند میتوانند از همان دامنه قبلی استفاده کنند .

تعداد کمی از سازمانها بر این باور هستند که وضعیت فعلی امنیت ویندوز برای سازمانها قابل قبول است. Device Guard و Credential Guard در واقع یک راهحل پیش برنده در این زمینه به شمار میروند . با گذشت حداقل شش ماه از عرضه ویندوز، میزان تقاضا برای این سیستمعامل افزایش خواهد یافت . وینیوسکی در اینباره میگوید : « مایکروسافت به سازمانها اعلام کرده است اگر به دنبال فناوریهای خوبی هستید، در نتیجه به امنیت نیاز دارید . ( البته به روش ما )». اما این زمان است که به ما خواهد گفت آیا سازمانها در مسیری که به آن اشاره کردیم گام برخواهند داشت یا خیر .

نویسنده :
حمیدرضا_تائبی

دسته بندی:
امنیت
تاریخ انتشار :
14:06 - 15/08/1394
برچسب:
ویندوز 10 - امنیت - Secure Boot - TPM - UEFI - Credential Guard - device guard - امنیت ویندوز 10

---

▯▯▯▯▯ منبع: https://www.shabakeh-mag.com/security/2094