اخطار: نصب درب‌ِپشتی توسط هکرها بر روی هزاران Microsoft SQL Servers

---

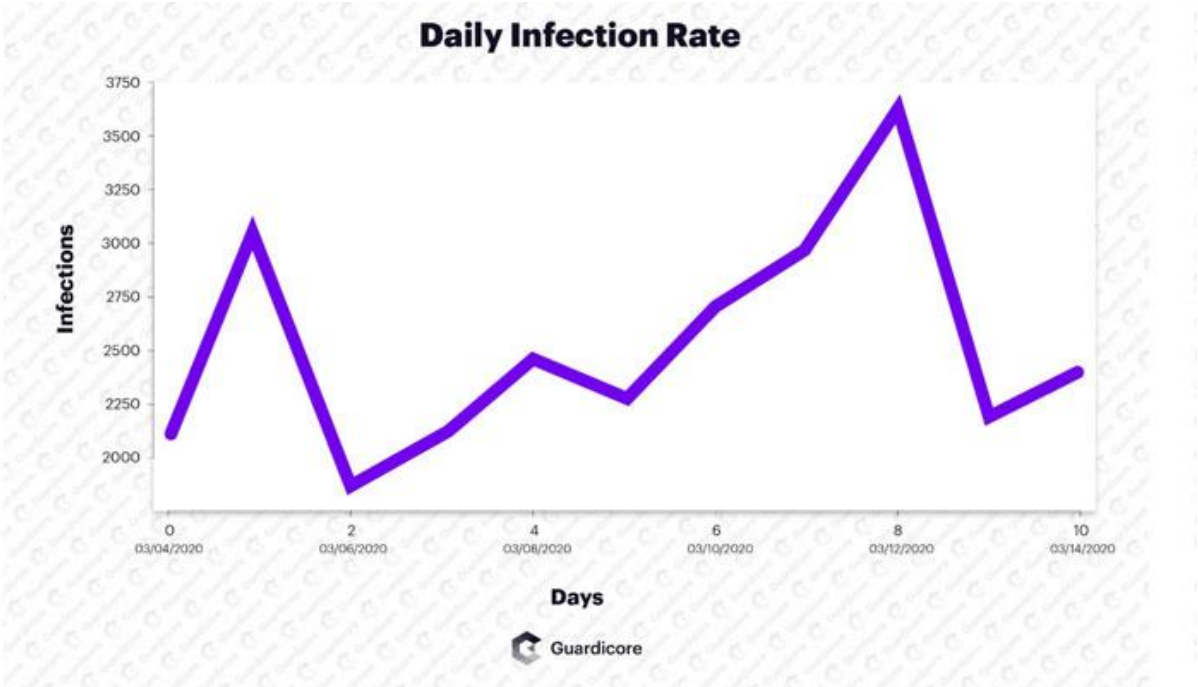
خلاصه‌ی گزارش:

یک کمپین مخرب قدیمی که سرورهای MS-SQL ویندوز را برای استقرار درب‌ِپشتی و انواع دیگر بدافزارها، از جمله ابزارهای دسترسی از راه دور (RAT) و رمزارز نگاری، هدف قرار می‌دهد، با نام Vollgar کشف شده است. مهاجمین این کمپین، موفق‌شده‌اند که طی چند هفته‌ی گذشته تقریباً ۲۰۰۰ تا۳۰۰۰ سرور پایگاه داده را آلوده کنند. آن‌ها عمدتاً از حملات brute-force استفاده می‌کنند. انگیزه‌ی مهاجمین جدا از بهره بردن از منابع سرور پایگاه‌های داده، وجود و ذخیره داشتن اطلاعات شخصی زیادی، مانند نام‌های کاربری، رمزهای عبور، شماره کارت‌های اعتباری و غیره‌ایست که فقط با یک پرس‌وجو ساده در اختیار آن‌ها قرار می‌گیرند. برای جلوگیری از این حملات ضروری‌ست سرورهای MS-SQL که در بستر اینترنت قرار دارند با اعتبارنامه‌های قوی ایمن شوند.

محققان فضای مجازی امروز یک کمپین مخرب طولانی‌مدت که از تاریخ مه ۲۰۱۸ قدمت‌دارد، را کشف کردند که سرورهای MS-SQL ویندوز را برای استقرار دربِ‌پشتی و انواع دیگر بدافزارها، از جمله ابزارهای دسترسی از راه (RAT) و رمزارز نگاری، هدف قرار می‌دهد.

پس از رمزارز Vollar که از آن استخراج شد و روش‌کار توهین آمیز و مبتذلش آن را Vollgar نامیدند. به گفته‌ی محققان آزمایشگاه Guardicore Labs که در این حمله از brute-force استفاده می‌شود تا بتواند سرورهای Microsoft SQL با اعتبارنامه‌ی ضعیف را در معرض خطر اینترنت قرار دهد.

محققان ادعا می‌کنند مهاجمان موفق شده‌اند طی چند هفته گذشته تقریباً ۲ هزار تا۳ هزار سرور پایگاه داده را با موفقیت آلوده کنند. قربانیان احتمالی متعلق به بخش‌های مراقبت‌های بهداشتی، حمل و نقل هوایی، IT و ارتباطات و بخش‌های آموزش عالی در سراسر چین، هند، آمریکا، کره جنوبی و ترکیه هستند.



خوشبختانه برای کسانی که نگران این موضوع هستند، محققان اسکریپتی نیز منتشر کرده‌اند تا ادمین‌های سیستم تشخیص دهند که آیا هر یک از سرورهای Windows MS-SQL آن‌ها با این تهدید خاص به خطر افتاده‌است یا خیر.

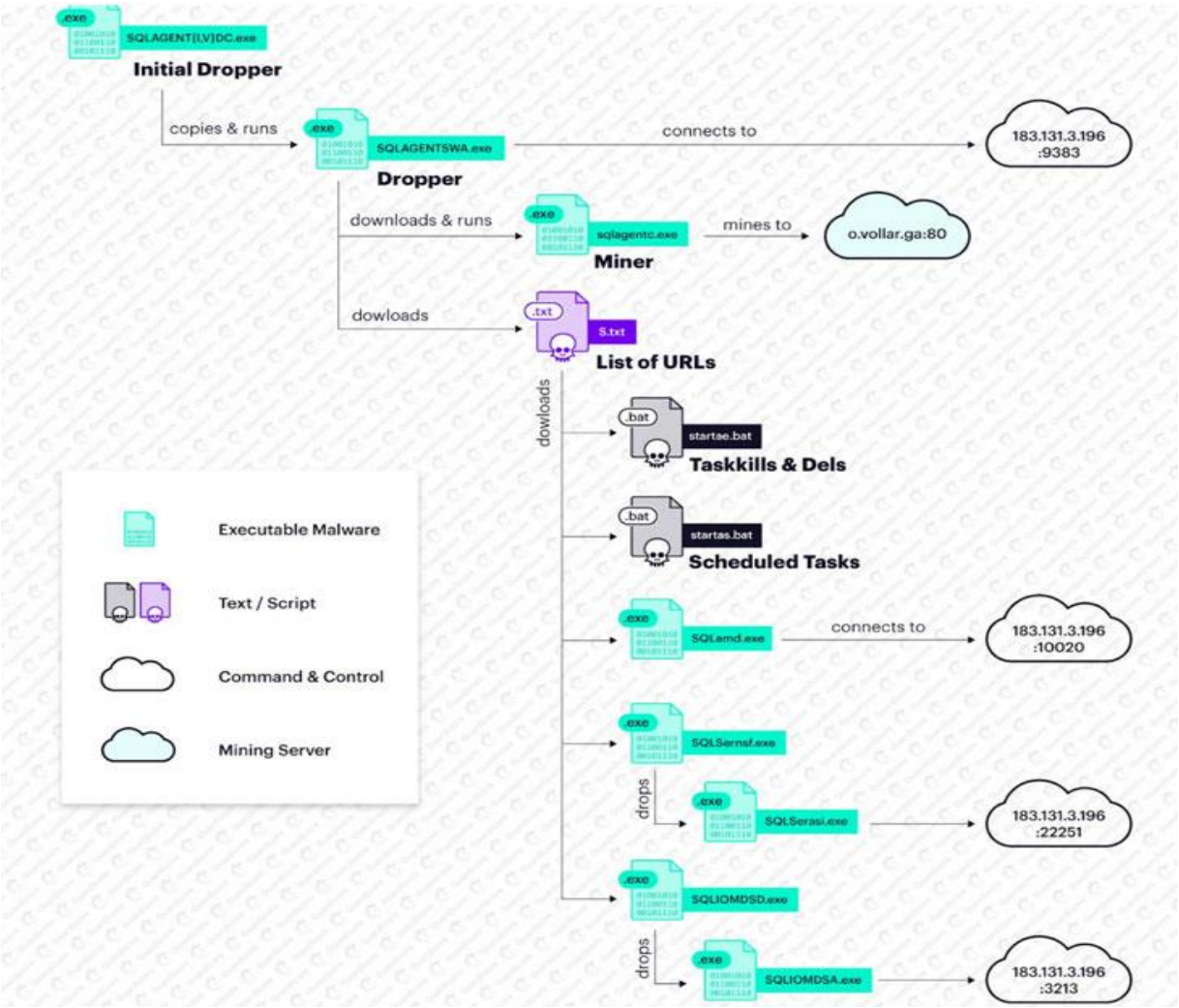
زنجیره‌ی حمله‌ی Vollgar: آلودگی **MS-SQL به بدافزار**

حمله Vollgar با تلاش‌های ورود به سیستم بر اساس brute-force، بر روی سرورهای MS-SQL شروع می‌شود، که در صورت موفقیت، به مهاجم اجازه می‌دهد پیکربندی‌هایی را برای اجرای دستورات مخرب MS-SQL تغییر دهد و بدافزارهای خود را بارگیری کند.

به گفته‌ی محققین: "مهاجمین همچنین تأیید می‌کنند که کلاس‌های COM کاملی در این حوزه شامل WbemScripting.SWbemLocator ، Microsoft.Jet.OLEDB.4.0 و Windows Script - Host Object Model (wshom) وجود دارند. این کلاس‌ها هم از WMI و هم از اجرای دستور از طریق MS-SQL پشتیبانی می‌کنند که بعداً برای بارگیری بدافزار اولیه مورد استفاده قرار خواهد گرفت."

گذشته از اطمینان از داشتن مجوزهای لازم در cmd.exe و ftp.exe، مجوزهای موجود در پشت Vollgar نیز کاربران دربِ‌پشتی جدیدی را در پایگاه داده MS-SQL و همچنین در سیستم‌عامل با سطح‌دسترسی بالا، ایجاد می‌کند.

پس از اتمام راه‌اندازی اولیه، ادامه حمله به ایجاد اسکریپت‌های بارگیری‌کننده (دو VBScripts و یک اسکریپت FTP) می‌کند، که "دو بار" ، هر بار با یک مکان هدف متفاوت در سیستم فایل محلی برای جلوگیری از شکست‌های احتمالی، اجرا می‌شوند.



یکی از payloadهای اولیه با نام SQLAGENTIDC.exe یا SQLAGENTVDC.exe، ابتدا اقدام به بستن(Kill) لیستی طولانی از فرایندها که هدف‌شان تأمین امنیت حداکثر منابع سیستم و همچنین از بین بردن فعالیت‌های دیگر عاملان تهدید و حذف آن‌ها از دستگاه آلوده است، می‌کنند.

علاوه بر این، به عنوان dropper برای RAT های مختلف و ماینرهای رمزارز مبتنی بر XMRig که Monero و alt-coin به نام VDS یا Vollar استخراج می‌کند، عمل می‌کند.

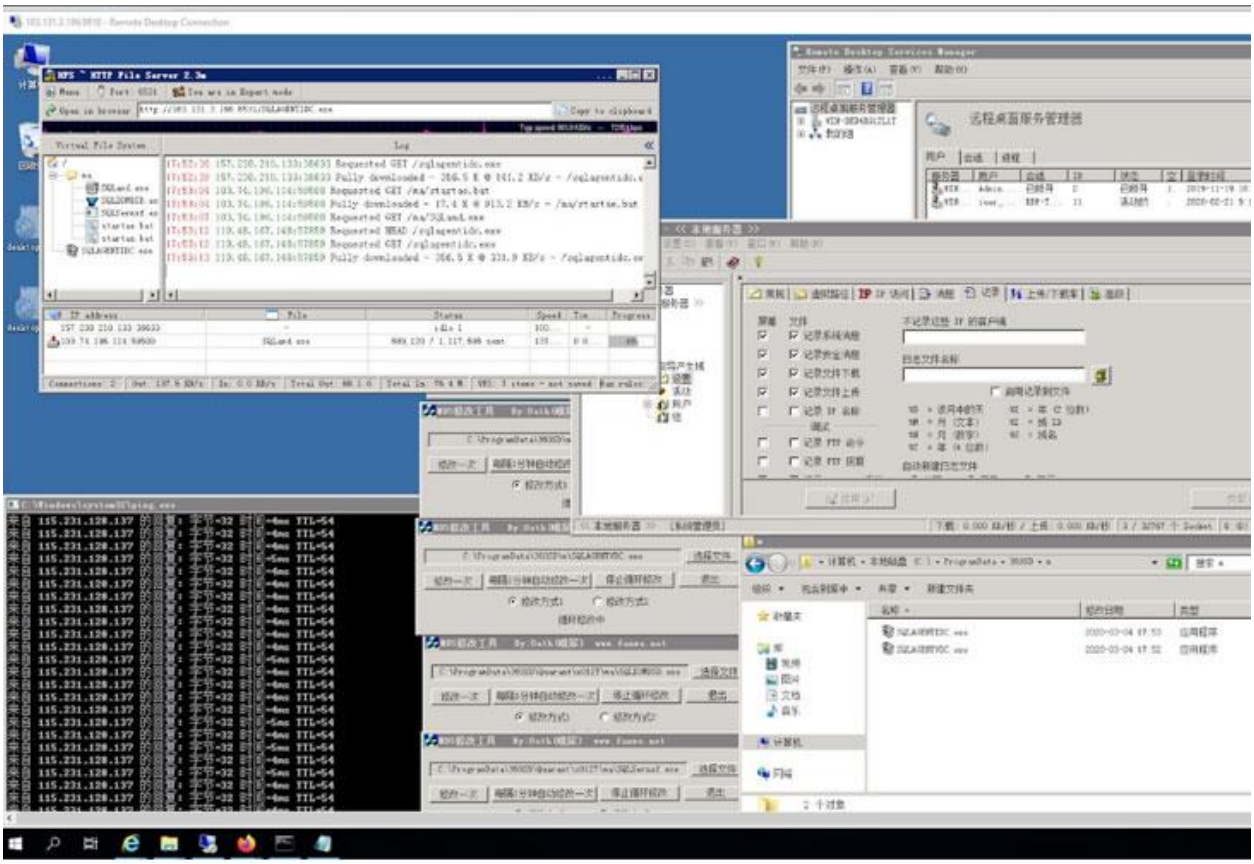
حمله به زیرساخت‌های میزبان بر روی سیستم‌های تحت‌کنترل

Guardicore گفت که مهاجمان تمام زیرساخت‌های خود را در دستگاه‌های تحت‌کنترل و آلوده از

جمله سرور اصلی فرمان و کنترل واقع در چین،که به طرز طعنه‌آمیزی توسط بیش از یک گروه حمله، تحت‌کنترل قرار گرفت، نگهداری می‌کنند.

این شرکت امنیت‌سایبری خاطرنشان کرد: "در بین فایل‌ها [در سرور C &C] ابزار حمله MS-SQL، مسئول اسکن دامنه‌های IP، ایجاد مجدد پایگاه داده هدفمند و اجرای دستورات از راه دور وجود داشته است. "

همچنین در ادامه افزودند: "علاوه بر این، ما دو برنامه CNC با GUI که ابزاری برای تغییر مقادیر هش فایل‌ها هستند را به زبان چینی، یک سرور قاب انتقال فایل HTTP (HFS) ، سرور Serv-U FTP و یک کپی از mstsc.exe (Microsoft Terminal Services Client) قابل اجرا که برای اتصال به قربانیان از طریق RDP استفاده می‌شود، پیدا کردیم. "



به‌محض اینکه یک کلاینت آلوده ویندوز سرور C2 را پینگ می‌کند، متعاقباً نیز جزئیات مختلفی در مورد دستگاه از قبیل IP عمومی، مکان، نسخه سیستم عامل، نام رایانه و مدل CPU را دریافت می‌کند.

Guardicore با بیان اینکه دو برنامه C2 نصب شده بر روی سرور مستقر در چین توسط دو فروشنده مختلف تولید شده است، گفت: در قابلیت کنترل از راه دور آن‌ها مانند بارگیری فایل‌ها، نصب سرویس‌های جدید ویندوز، keylogging، ضبط صفحه، فعال کردن دوربین و میکروفون و حتی یک حمله‌ی منع از سرویس (DDoS) توزیع شده، شباهت‌هایی وجود دارد.

برای جلوگیری از حملات brute-force از رمزهای عبور قوی استفاده کنید

با حدود نیم میلیون دستگاه در حال اجرای پایگاه داده MS-SQL ، این کمپین نشانه‌ی دیگری‌ست مبنی بر اینکه مهاجمان در پی سرقت اطلاعات حساس به دنبال سرورهای پایگاه داده ای هستند که امنیت آن‌ها ضعیف است. ضروری است سرورهای MS-SQL که در معرض اینترنت قرار دارند با اعتبارنامه‌های قوی ایمن شوند.

محققان Guardicore نتیجه گرفتند: "آنچه باعث می‌شود این سرورهای پایگاه داده جدا از توان ارزشمند پردازنده، برای مهاجمین جذاب شوند حجم عظیم داده‌های آن‌هاست." "این ماشین‌ها احتمالاً اطلاعات شخصی زیادی، مانند نام‌های کاربری، رمزهای عبور، شماره کارت‌های اعتباری و غیره را ذخیره می‌کنند که فقط با یک پرس‌وجوی ساده در اختیار مهاجمان قرار می‌گیرند".

منبع:
https://thehackernews.com/2020/04/backdoor-.html