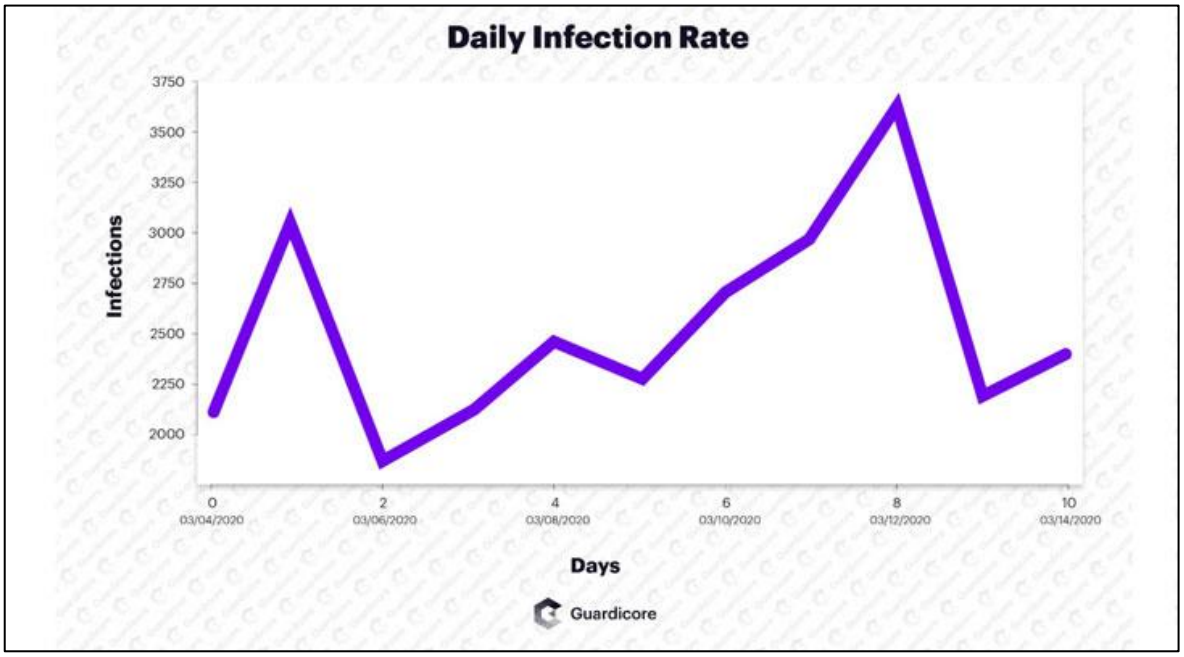
بسمه تعالی

هشدار: هکرها روی SQL Serverهای مایکروسافت Backdoorهای مخفی نصب می‌کنند

محققان امنیتی از یک کمپین مخرب که از ماه مارس ۲۰۱۸ سیستم‌های ویندوزی اجراکنندهٔ SQL Server را هدف قرار می‌دهند، پرده برداشتند. این کمپین اقدام به نصب انواع بدافزار شامل ابزارهای کنترل از راه دور چند کارکردی (RATها)، ماینرها و بکدور روی سرورهای SQL می‌کردند. این کمپین با توجه به استخراج رمز Vollar و شیوهٔ کار تهاجمی خود به نام«Vollgar» نامگذاری شده است. به گفتهٔ محققان امنیتی در آزمایشگاه Guardicore مهاجمان از brute force پسوردها برای نفوذ به سرورهای Microsoft SQLی که اعتبارنامه آنها در سطح اینترنت منتشر شده است، استفاده می‌کنند. محققان عقیده دارند که مهاجمان هر روز تعداد ۲.۰۰۰ تا ۳.۰۰۰ سرور پایگاه‌داده را طی چند هفتهٔ اخیر آلوده کرده‌اند. این اهداف شامل سازمان‌های بهداشت و درمان، هواپیمایی، IT و تلکام و دیگر بخش‌های آموزشی در چین، هند، ایالات متحدهٔ آمریکا، کرهٔ جنوبی و ترکیه هستند.

شکل شماره ۱ نرخ روزانهٔ آلوده شدن اهداف مهاجمان Vollgar را نشان می‌دهد.



شکل شماره ۱

همچنین محققان، اسکریپتی منتشر کرده‌اند که بوسیلهٔ آن آدمین‌های سیستم می‌توانند آلودگی سرورهای MS-SQL تحت مدیریت خود را نسبت به این حملات بررسی کنند. برای دریافت اسکریپت به لینک زیر مراجعه کنید:

https://github.com/guardicore/labs_campaigns/tree/master/Vollgar

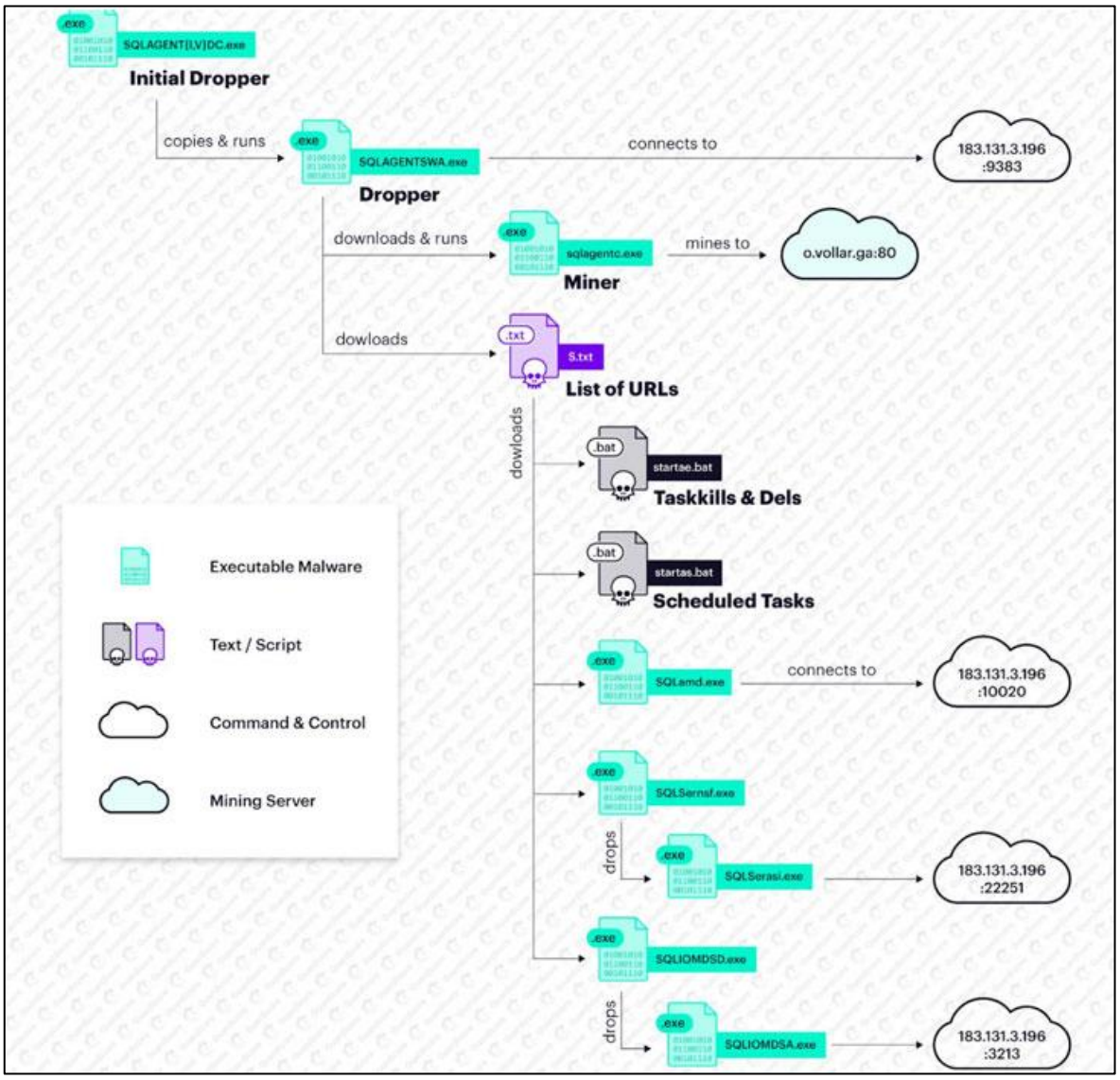
۱ زنجیرهٔ حملهٔ Vollgar

حملهٔ Vogllar با حملات brute force برای نفوذ به سرورهای SQL مایکروسافت آغاز می‌شود؛ اگر حمله موفقیت‌آمیز باشد مهاجم می‌تواند تنظیمات پیکربندی را برای اجرای دستورات مخرب SQL و دانلود بدافزارها تغییر دهد.

به گفتهٔ محققان مهاجمان پس از نفوذ، وجود تعدادی از کلاس‌های COM از جمله WbemScripting.SWbemLocator، Microsoft.Jet.OLEDB.4.0 و wshom را بررسی می‌کنند. این کلاس‌ها امکان اسکریپت‌نویسی WMI و اجرای دستورات در MS-SQL که می‌تواند بعدها برای دانلود بدافزار به کار گرفته شود، را فراهم می‌کنند. مهاجم بعد از اطمینان حاصل کردن از اینکه فایل‌های اجرایی cmd.exe و ftp.exe مجوزهای اجرایی لازم را دارا هستند، بکدورهایی را به صورت ایجاد حساب کاربری جدید در پایگاه‌داده‌های MS-SQL و خود سیستم‌عامل ایجاد می‌کند.

با کامل شدن راه‌اندازی اولیه، مهاجم به تولید اسکریپت‌های دانلودکننده (دو VBScript و یک اسکریپت FTP) اقدام می‌کند. این اسکریپت‌ها چندین بار در موقعیت‌های مختلف در فایل سیستم محلی اجرا می‌شوند تا در صورت ناموفق بودن اجرا در یکی از موقعیت‌ها در موقعیت دیگر باموفقیت اجرا شوند.

روند آلودگی سیستم و نحوهٔ عملکرد Vollgar در شکل شماره ۲ نشان داده شده است.



شکل شماره ۲

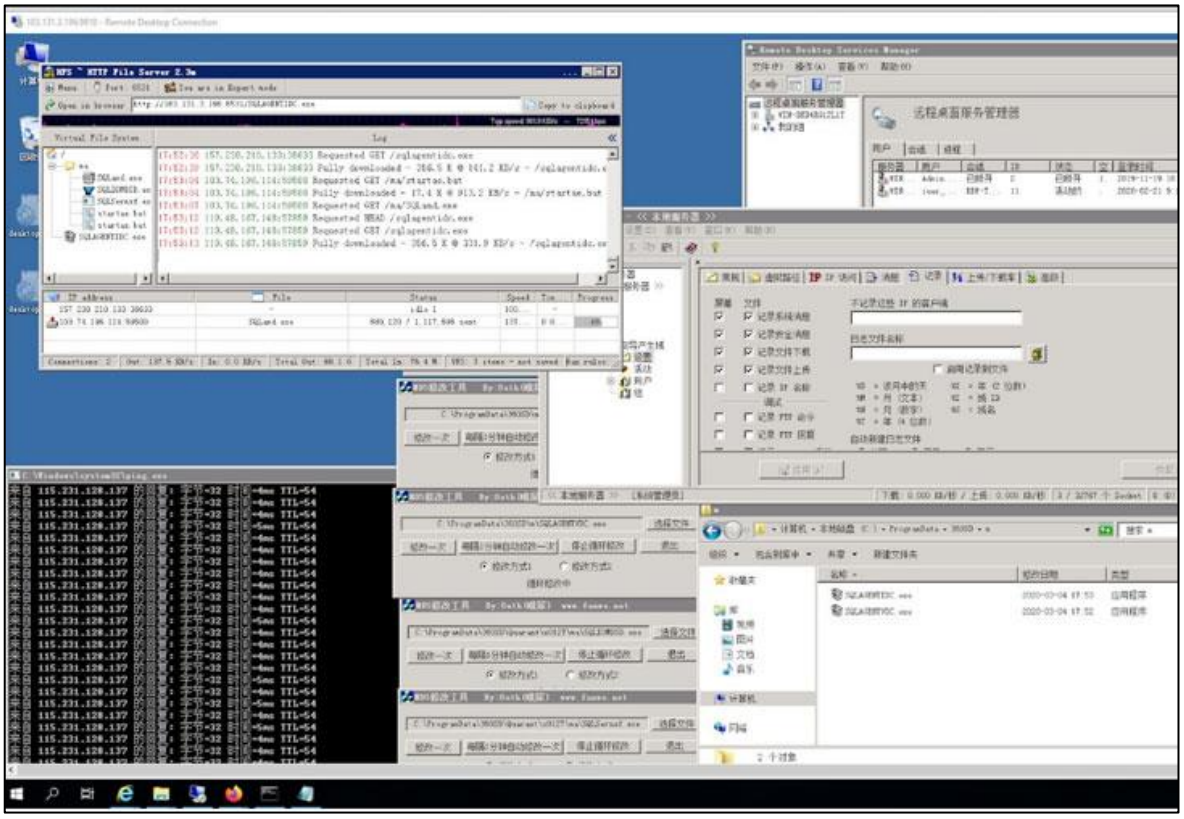
یکی از payloadهای اولیه به نام SQLAGENTIDC.exe یا SQLAGENTVDC.exe در اولین اقدام تعداد زیادی از فرآیندها را برای آزادسازی حداکثری منابع سیستم متوقف می‌کند. علاوه بر این برای دیگر RATهای مختلف و یک استخراج‌کنندهٔ مبتنی بر XMRig که رمزارز Monero و VDS استخراج می‌کنند، به عنوان dropper عمل می‌کند.

۲ زیرساخت حمله به سیستم‌های آسیب‌پذیر

به گفتهٔ محققان در آزمایشگاه Guardicore، مهاجمان همهٔ زیرساخت خود شامل سرور اصلی C&C را در کشور چین نگهداری و مدیریت می‌کنند. لازم به ذکر است که این سرور نسبت به حملات گروه مشخصی از

مهاجمان آسیب‌پذیر شناخته شده بود. در میان فایل‌های موجود در سرور C&C، یک ابزار حمله به MS-SQL وجود دارد. این ابزار وظیفهٔ اسکن محدودهٔ IP آدرس‌ها، اجرای حملهٔ brute force روی پایگاه‌داده‌های هدف و اجرای دستورات از راه دور را برعهده دارد.

همان طور که در شکل شماره ۳ مشاهده می‌شود، علاوه بر موارد ذکر شده در بند قبلی، دو برنامهٔ CNC با رابط گرافیکی به زبان چینی، یک ابزار برای تغییر مقدار هش فایل‌ها، یک فایل سرور HTTP (HFS) قابل حمل، سرور Serv-U FTP و یک نسخهٔ قابل اجرا از mstsc.exe (Client Microsoft Terminal Services) برای اتصال به سیستم قربانی از طریق RDP یافت شده است.



شکل شماره ۳

زمانی‌که یک سیستم ویندوزی آلوده، سرور C2 را پینگ می‌کند، سرور C2 جزییات مختلفی درمورد سیستم قربانی از قبیل آدرس IP، موقعیت مکانی، نسخه سیستم‌عامل، نام کامپیوتر و مدل پردازنده دریافت می‌کند.

۳ برای مقابله با حملات brute force از پسوردهای قوی استفاده کنید

با توجه به اینکه نیم میلیون سیستم وجود دارد که سرویس پایگاه داده MS-SQL را اجرا می‌کند، قطع به یقین مهاجمان سعی در دستیابی به سرورهای پایگاه داده‌ای که به طور صحیح محافظت نشده‌اند، دارند تا اطلاعات حساس درون آنها را استخراج کنند. ضروری است که پایگاه‌داده‌های موجود در بستر اینترنت توسط اعتبارنامه‌های قوی محافظت شوند. بدیهی است علاوه بر قدرت باارزش پردازنده این سروهای پایگاه داده چیزی که مهاجمان را به سوی آنها سوق می‌دهد، اطلاعات زیادی است که نگهداری می‌کنند. احتمالا این اطلاعات شامل اطلاعات شخصی مانند نام کاربری و رمز عبور و شمارهٔ کارت‌های اعتباری است.

۴ مراجع

[1] https://thehackernews.com/2020/04/backdoor-.html