بدافزار جدید Mozart که دستورات را گرفته و ترافیک را با استفاده از DNS پنهان می‌کند.

یک بدافزار درب‌ِپشتی جدید به نام Mozart با استفاده از پروتکل DNS با مهاجمین از راه دور ارتباط برقرار می‌کند تا از شناسایی‌شدن توسط نرم‌افزارهای امنیتی و سیستم‌های تشخیص نفوذ، جلوگیری کند.

معمولاً وقتی یک بدافزار برای دریافت دستوراتی که باید اجرا شود با سرور ارتباط می‌گیرد، این کار را با استفاده از پروتکل‌های HTTP/S برای سهولت استفاده و ارتباط انجام می‌دهد.

با این وجود، استفاده از ارتباط HTTP/S برای برقراری ارتباط، اشکالاتی دارد، زیرا نرم‌افزارهای امنیتی معمولاً ترافیک را برای فعالیت‌های مخرب نظارت می‌کنند. در صورت شناسایی توسط نرم‌افزار امنیتی، اتصال و بدافزاری که درخواست HTTP/S را دارد، مسدود می‌کند.

در درب‌ِپشتی جدید Mozart که توسط MalwareHunterTeam کشف شده است، این بدافزار از DNS برای دریافت دستورالعمل از مهاجمین و جلوگیری از شناسایی‌شدن، استفاده می‌کند.

استفاده از رکورد DNS TXT برای صدور دستورات

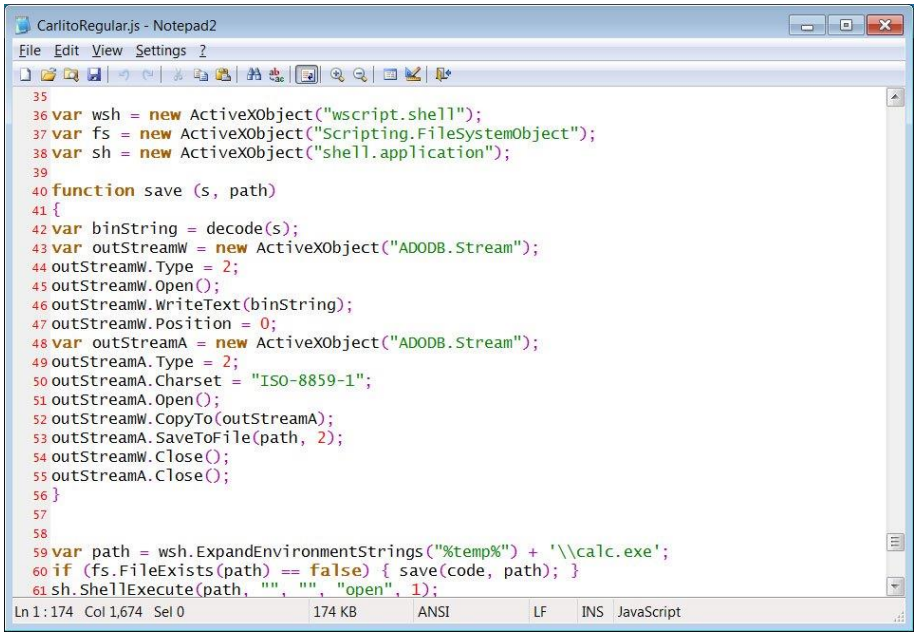
DNS پروتکلی برای تبدیل نام host مانند www.example.com به آدرس IP آن (92.25.25.36) است. علاوه بر تبدیل نام‌های میزبان به آدرس IP، پروتکل DNS به شما امکان می‌دهد رکورد TXT که حاوی داده‌های متنی است را نیز جستجو کنید. این ویژگی عموماً برای تأیید مالکیت دامنه برای سرویس‌های آنلاین و سیاست‌های ایمنی ایمیل مانند Sender Policy Framework یا DMARC استفاده می‌شود.

در زیر رکورد TXT برای "hi.bleepingcomputer.com " نشان داده شده است.

مهاجمان Mozart از این رکورد DNS TXT استفاده می‌کنند تا دستوراتی را که توسط نرم‌افزارهای مخرب بازیابی شده و بر روی سیستم آلوده اعمال می‌شوند، ذخیره کنند.

Mozart با استفاده از DNS خراب‌کاری می‌کند

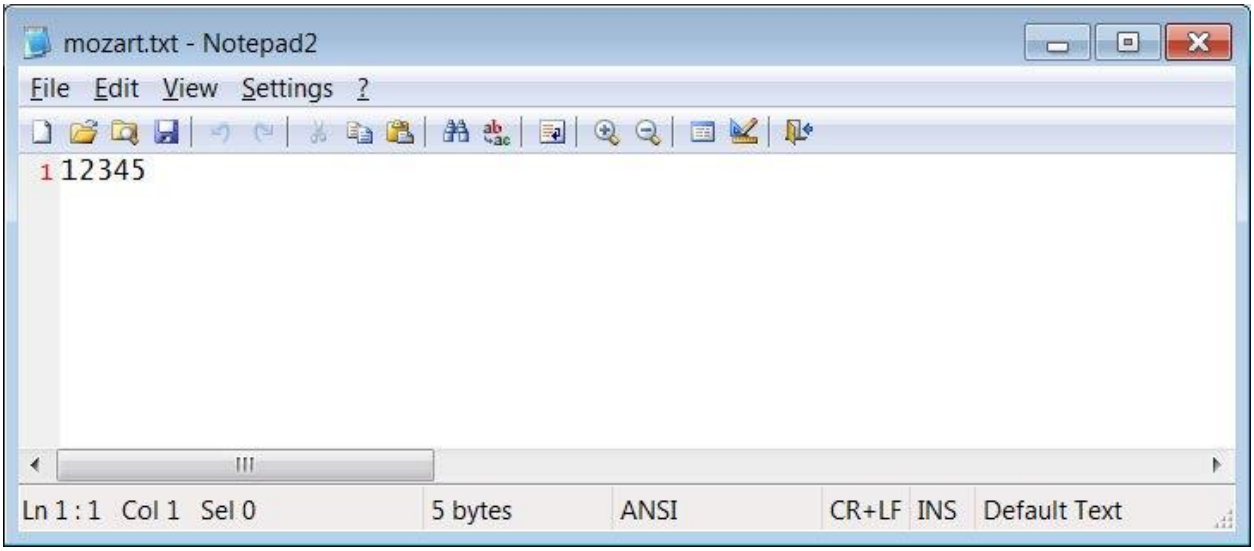
اعتقاد بر این است که بدافزار Mozart از طریق ایمیل‌های فیشینگ که شامل PDF هایی هستند که به یک فایل ZIP که در آدرس https://masikini[.]com/CarlitoRegular[.]zip. موجود است، توزیع می‌شود. این فایل فشرده حاوی یک کد JScript است که هنگام اجرا یک فایل اجرایی رمزگذاری شده base64 که با عنوان **%Temp%\calc.exe** در رایانه ذخیره شده است را استخراج و اجرا می‌کند.



نصب‌کننده Jscript در بدافزار Mozart

به گفته محقق SentinelLabs، Vitali Kremez که این درب‌پشتی را تجزیه و تحلیل کرده و یافته‌های خود را با BleepingComputer به اشتراک گذاشته است، این بدافزار ابتدا فایل .%Temp%\mozart.txt را بررسی می‌کند. اگر این فایل وجود نداشته باشد، آن را با محتوای ۱۲۳۴۵ ایجاد می‌کند و کارهای آماده‌سازی را بر روی رایانه انجام می‌دهد. این آماده‌سازی شامل کپی‌کردن فایل calc.exe از پوشه ٪Temp٪ در یک مسیر که بطور تصادفی نام‌گذاری شده و قرار دادن در مسیر زیر

%AppData%\Microsoft\Windows\Start Menu\Programs\Startup\ folder به منظور اینکه در هر بار واردشدن قربانی در ویندوز، راه‌اندازی شود.

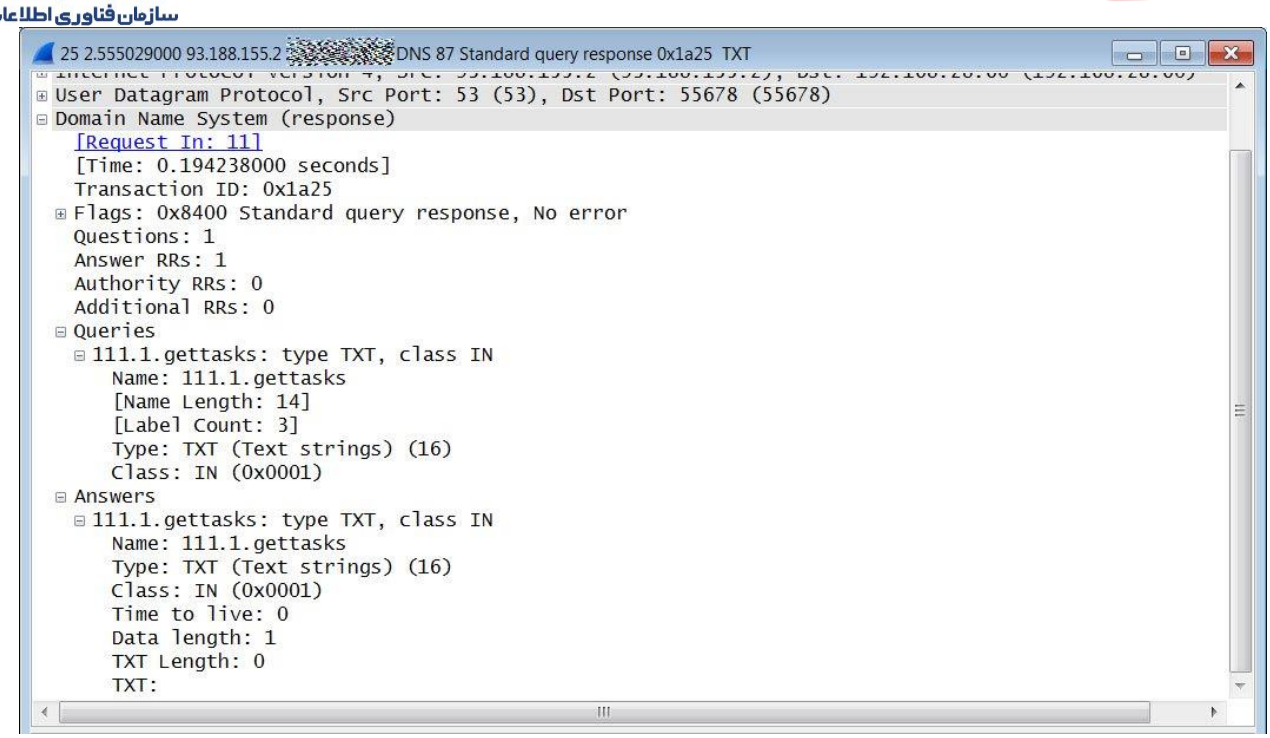


فایل mozart.txt

طبق گفته‌ی Kremez ، بدافزار Mozart با یک سرور DNS hardcoded تحت کنترل مهاجم در

93.188.155.2 ارتباط برقرار خواهد کرد و به دنبال درخواست DNS برای دریافت دستورالعمل یا داده پیکربندی می‌شود:

به عنوان مثال، در آزمایشات BleepingComputer، ما به بات شناسه '۱۱۱' را اختصاص داده‌ایم، که باعث شده Mozart برای موارد: 111.1.getid, 111.1.getupdates, and 111.1.gettasks به جستجوی DNS TXT بپردازد.



درخواست gettasks DNS

در هنگام نظارت بر Mozart ، متوجه شدیم که این بدافزار بطور مداوم سؤالات "gettasks" را به سرور DNS مهاجم صادر می‌کند تا دستوراتی را برای اجرای آن پیدا کند.

اگر پاسخ یادداشت TXT خالی باشد، همانطور که در بالا نشان داده شد، بدان معنی است که هیچ دستوری برای اجرا وجود ندارد و بدافزار تا زمانی که یک وظیفه انجام شود، این بررسی را بارها و بارها ادامه می‌دهد.

در حال حاضر مشخص نیست چه دستوراتی توسط Mozart به عنوان تست توسط Kremez اجرا می‌شود و Kremez هیچ پاسخی به درخواستهای DNS نداده است.

ممکن است به‌این دلیل باشد که ما برای مدت طولانی تست نکردیم و یا اینکه مهاجمان در حال ساخت بات‌نت خود قبل از انتقال دستورات بوده‌اند.

مسدود کردن این نوع تهدیدات

توجه به این نکته ضروری است که از قبل بدافزارهایی وجود داشته‌اند که از DNS برای برقراری ارتباط استفاده می‌کنند و درب‌ِپشتی Mozart منحصر به فرد نیست.

در سال ۲۰۱۷، گروه Cisco Talos یک بدافزار به نام DNSMessenger را کشف کرد که برای ارتباطات مخرب نیز از رکورد TXT استفاده می‌کرد. برای مسدود کردن فعالیت Mozart، می توانیم بگوییم که درخواست‌های DNS را به 93.188.155.2 مسدود کنید، اما انواع جدید می‌توانند به سادگی آنقدر به سرورهای مختلف DNS سوئیچ کنند و این بازی موش و گربه ادامه پیدا خواهد کرد.

درعوض، باید مراقب روش‌های جدید ارتباطات مخرب باشید و اگر نرم‌افزارهای امنیتی و سیستم‌های تشخیص نفوذ شما می‌توانند بر روی DNS TXT نظارت داشته باشند، باید آن را فعال کنید.

منبع:

https://www.bleepingcomputer.com/news/security/new-mozart-malware-gets-commands-hides-traffic-using-dns/