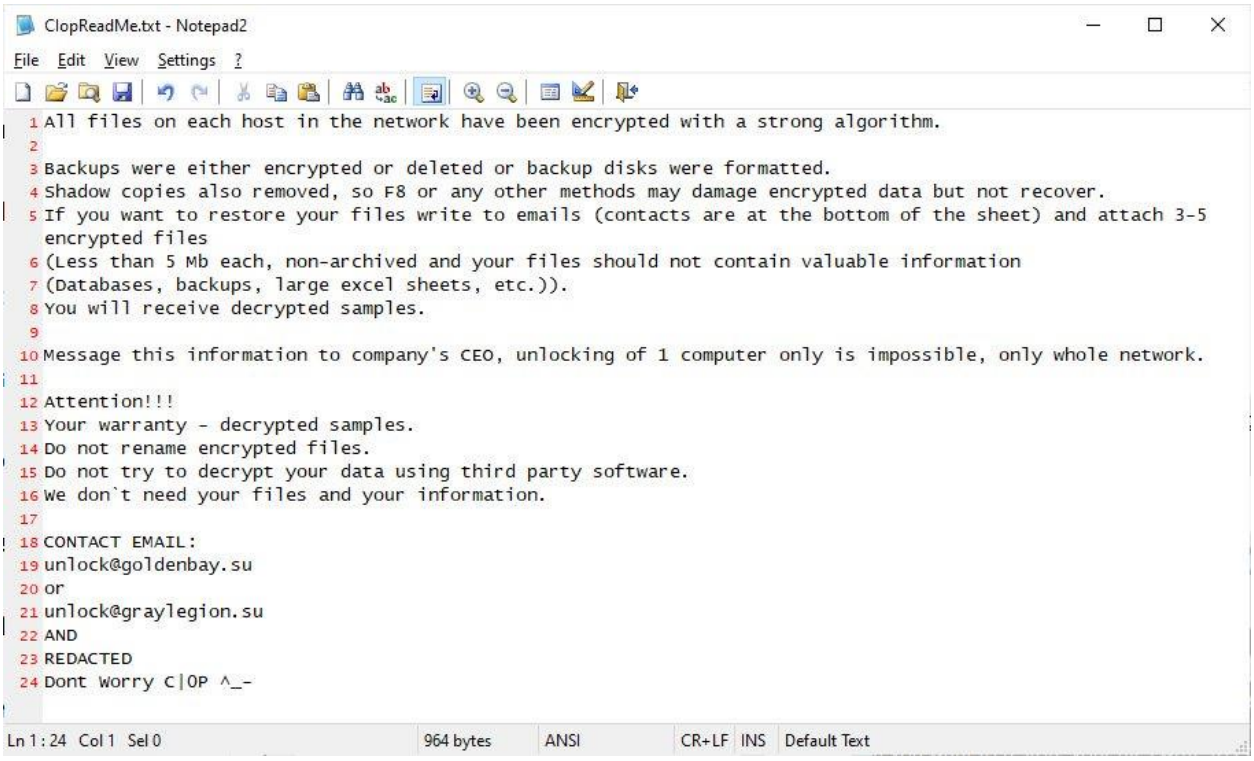
انتشار باج افزار Clop که سعی در غیرفعال‌سازی Windows Defender را دارد.



اخیراً باج‌افزاری به نام Clop CryptoMix به صورت گسترده منتشر شده است که به‌منظور رمزنگاری موفقیت‌آمیز داده‌های یک قربانی، سعی در غیرفعال کردن windows defender و همچنین حذف windows security essentials و برنامه‌های مستقل ضد باج افزار(امنیتی) Malwarebytes را دارد.

Clop نوعی از باج‌افزار CryptoMix است که از پسوند Clop استفاده می‌کند و یادداشت‌های باج‌خواهی خود را در قالب یک فایل ClopReadMe.txt با پیام "Don’t Worry C|oP " امضا می‌کند. به همین دلیل این باج‌افزار به Clop Ransomware معروف شده است.

تلاش برای غیرفعال کردن Windows Defender

طبق تجزیه و تحلیل انجام شده توسط محقق امنیتی و مهندس معکوس ویتالی کرمز (Vitali Kremez) برنامه کوچکی توسط عاملان Clop قبل از رمزنگاری درحال اجرا است که سعی در غیرفعال کردن انواع نرم-افزارهای امنیتی از جمله windows defender را خواهد داشت.

این کار برای جلوگیری از شناسایی الگوریتم‌های رفتاری برای رمزنگاری پرونده و مسدود کردن باج افزار انجام می‌شود.

برای غیرفعال سازی windows defender، این باج‌افزار مقادیر مختلف registry شامل:

- Behavior monitoring
- Real time protection
- Sample uploading to Microsoft
- Tamper protection
- Cloud detections
- Antispyware detections

را پیکربندی کرده و غیرفعال می‌کند. دستورات به شکل زیر هستند.

```
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v
"DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v
"DisableOnAccessProtection" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v
"DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d
"2" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\Real-Time Protection" /v
"DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Microsoft\Windows
Defender\Features" /v "TamperProtection" /t REG_DWORD /d "0"
/f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows
Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
```

```
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpCloudBlockLevel" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
```

خبر خوب این است که اگر tamper detection را در ویندوز ۱۰ فعال کرده باشید، این تنظیمات به سادگی به تنظیمات پیش‌فرض آن‌ها بازگردانده خواهند شد و windows defender غیرفعال نخواهد شد.

با این حال برای کسانی که از tamper protection استفاده نمی‌کنند، این کار بطور مؤثری windows defender را غیرفعال می‌کند تا این امر باعث شناسایی اقدامات باج‌افزار نگردد.

علاوه بر Windows Defender، Clop با حذف برنامه‌های امنیتی دیگر مایکروسافت، سیستم‌های قدیمی را نیز هدف قرار داده است. از آنجا که CryptoMix با امتیازات administrator توسط مهاجمین اداره می‌شود، این دستور باعث می‌شود آن برنامه‌ها بدون مشکل حذف شود.

```
cmd.exe /C "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

تلاش برای لغو نصب ضدباج‌افزار Malwarebytes

علاوه بر Windows Defender، محقق امنیتی MalwareHunterteam کشف کرد که این ابزار همچنین برنامه مستقل ضد باج‌افزار Malwarebytes را هدف قرار داده است.

با اجرای برنامه، سعی خواهد شد محصول ضدباج‌افزار Malwarebytes را با استفاده از دستور زیر حذف کند:

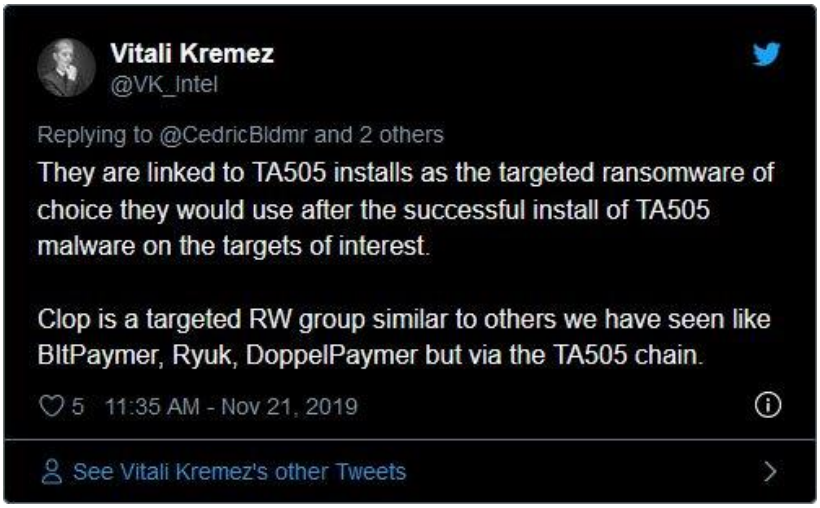
```
C:\Program Files\MalwareBytes\Anti-Ransomware\unins000.exe /verysilent /suppressmsgboxes /norestart
```

با توجه به بازنشسته شدن محصول ضدباج‌افزار Malwarebytes و وصل شدن آن به نرم‌افزار پیشتاز آن‌ها "ضدبدافزار Malwarebytes " تلاش فوق کمی عجیب به‌نظر می‌رسد.

همزمان، از آنجایی که CryptoMix معمولاً از طریق Remote Desktop یا سایر شبکه‌ها نصب می‌شود، با هدف قرار دادن محصولاتی که ممکن است از ایستگاه‌های کاری شرکت‌های قدیمی‌تر استفاده کنند، این امکان را فراهم می‌آورد که باج‌افزار را هنگام رمزنگاری کل شبکه، بی‌پرده اجرا کند.

Clop مورد استفاده در حملات گسترده شبکه

در حالی که CryptoMix یک باج افزار قدیمی است، از لحاظ تاریخی توسط شرکت‌های وابسته که از طریق Remote Desktop به یک رایانه یا شبکه دسترسی پیدا کردند، مورد استفاده قرار گرفت. اخیراً یک گروه APT با نام TA505 پس از به خطر انداختن شبکه در حملات مشابه Ryuk، BitPaymer و DoppelPaymer، از آن به عنوان پیلود استفاده کرده است.



همین هفته، رسانه‌های فرانسوی گزارش داده‌اند که دانشگاه بیمارستان مرکزِ دو روئن (De Rouen) توسط باج‌افزار Clop مورد هدف قرار گرفته شده است که برخی از خدمات آن‌ها را تحت تأثیر قرار داد.

در ماه گذشته ، دانشگاه آنتورپ در بلژیک نیز با Clop روبرو شد که این امر بر سیستم‌های پرداخت آن‌ها، بایگانی سخنرانی‌های ویدیویی و سیستم پستی آن‌ها تأثیر گذاشت.

منبع:

https://www.bleepingcomputer.com/news/security/clop-ransomware-tries-to-disable-windows-defender-malwarebytes/