بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

باج افزار Big Head و به روز رسانی جعلی

گزارش خبری

شناسه سند ..... MaherReport_14020419

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۴۰۲/۴/۱۹

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

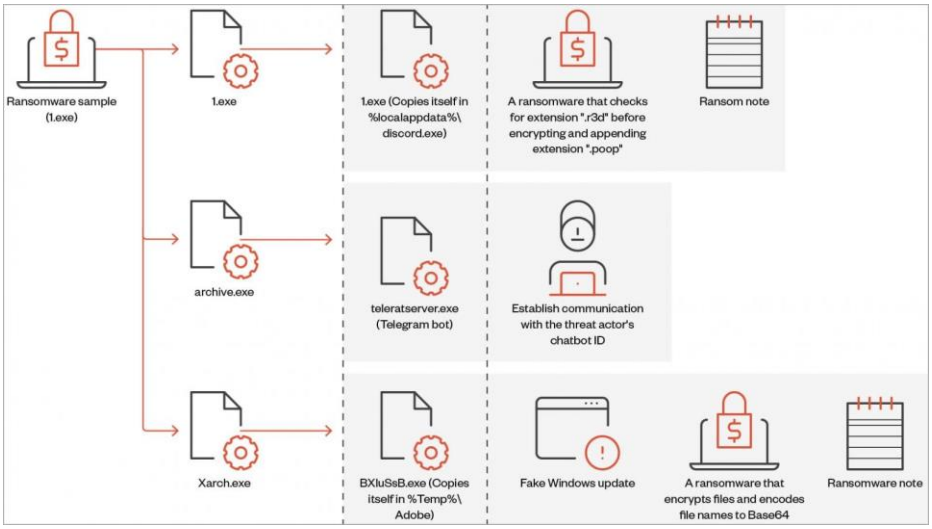
۱ باج افزار Big Head و به روز رسانی جعلی ویندوز

محققان امنیتی نوعی باج‌افزار جدید به نـام «Big Head» را کشـف کرده‌انـد کـه ممکـن اسـت از طریـق تبلیغات نادرست که به‌روزرسانی‌های جعلی ویندوز و نصب‌کننده‌های Microsoft Word را تبلیغ می‌کنند، منتشر شود. دو نمونه از بدافزار قبلاً توسط شرکت امنیت سایبری Fortinet تجزیه و تحلیل شده است.

امروز، Trend Microیک گزارش فنی درباره Big Head منتشر کرد کـه ادعـا می‌کـرد هـر ۳ نـوع کـه نمونه‌برداری کرده‌اند از یک اپراتور منشا می‌گیرند که احتمالاً رویکردهای مختلفی را برای بهینه‌سازی حملات خود آزمایش می‌کند.

۱-۱ جعل آپدیت ویندوز

باج افزار Big Head یک باینری دات نت است که سه فایل رمزگذاری شده با AES را روی سیستم هـدف نصب می‌کند: یکی برای انتشار بدافزار استفاده می‌شود، دیگری برای ارتباط با ربـات تلگـرام اسـت و سـومی فایل‌ها را رمزگذاری می‌کند و همچنین می‌تواند یک به‌روزرسانی جعلی ویندوز را به کاربر نشان دهد.



شکل ۱: روتین Big Head

در هنگام اجرا، باج‌افزار همچنین اقداماتی مانند ایجاد کلید رجیستری خودکار، بازنویسی فایل‌های موجود در صورت نیاز، تنظیم ویژگی‌های فایل سیستم و غیرفعال کردن Task Manager را انجام می‌دهد.

به هر قربانی یک شناسه منحصربه‌فرد اختصاص داده می‌شود که یا از فهرسـت %appdata%\ID بازیـابی می‌شود یا با استفاده از یک رشته تصادفی ۴۰ کاراکتری ایجاد می‌شود.

باج‌افزار پیش از رمزگذاری فایل‌های مورد نظر و افزودن پسوند «.poop» به نام فایل‌ها، کپی‌های shadow را حذف می‌کند تا از بازیابی آسان سیستم جلوگیری کند.

```
".mdf", ".db", ".mdb", ".sql", ".pdb", ".pdb", ".pdb", ".dsk", ".fp3", ".fdb",
".accdb", ".dbf", ".crd", ".db3", ".dbk", ".nsf", ".gdb", ".abs", ".sdb", ".sdb",
".sdb", ".sqlitedb", ".edb", ".sdf", ".sqlite", ".dbs", ".cdb", ".cdb", ".cdb", ".bib",
".dbc", ".usr", ".dbt", ".rsd", ".myd", ".pdm", ".ndf", ".ask", ".udb", ".ns2", ".kdb",
".ddl", ".sqlite3", ".odb", ".ib", ".db2", ".rdb", ".wdb", ".tcx", ".emd", ".sbf",
".accdr", ".dta", ".rpd", ".btr", ".vdb", ".daf", ".dbv", ".fcd", ".accde", ".mrg",
".nv2", ".pan", ".dnc", ".dxl", ".tdt", ".accdc", ".eco", ".fmp", ".vpd", ".his",
".fid"
```

شکل ۲: انواع فایل مورد هدف Big Head

همچنین، Big Head برای جلوگیری از دستکاری در فرآیند رمزگذاری و آزاد کردن داده‌هایی که بدافزار باید قفل کند، فرآیندهای زیر را خاتمه می‌دهد.

```
"taskmgr", "sqlagent", "winword", "sqlbrowser", "sqlservr", "sqlwriter", "oracle",
"ocssd", "dbsnmp", "synctime", "mydesktopqos", "agntsvc.exeisqlplussvc", "xfssvccon",
"mydesktopservice", "ocautoupds", "agntsvc.exeagntsvc", "agntsvc.exeencsvc",
"firefoxconfig", "tbirdconfig", "ocomm", "mysqld", "sql", "mysqld-nt", "mysqld-opt",
"dbeng50", "sqbcoreservice"
```

شکل ۳: فرآیندهای پایان یافته قبل از رمزگذاری

دایرکتوری های Windows ، Recycle Bin، Program Files، Temp، Program Data، Microsoftو App Data از رمزگذاری حذف می شوند تا سیستم غیرقابل استفاده نباشد.

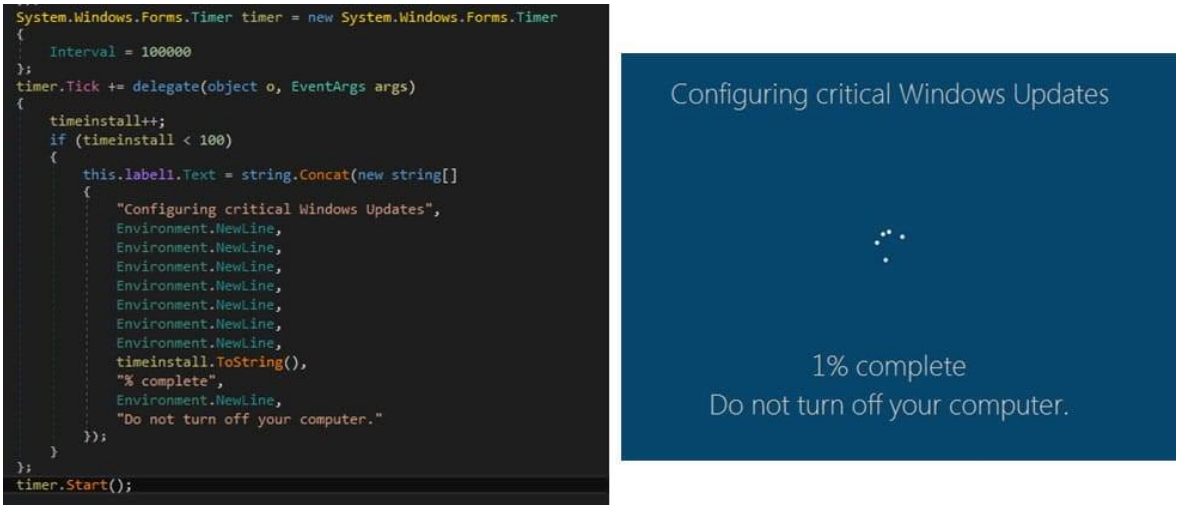
Trend Micro دریافته است که باج‌افزار بررسی می‌کند که آیا روی یک virtual box اجرا می‌شود یا نه، به دنبال زبان سیستم می‌گردد و فقط در صورتی به رمزگذاری ادامه می‌دهد که روی زبان یکی از کشورهای عضو مشترک المنافع (کشورهای شوروی سابق) تنظیم نشده باشد.

```
"ar-SA", "ar-AE", "nl-BE", "nl-NL", "en-GB", "en-US", "en-CA", "en-AU", "en-NZ", "fr-
BE", "fr-CH", "fr-FR", "fr-CA", "fr-LU", "de-AT", "de-DE", "de-CH", "it-CH", "it-IT",
"ko-KR", "pt-PT", "es-ES", "sv-FI", "sv-SE", "bg-BG", "ca-ES", "cs-CZ", "da-DK", "el-
GR", "en-IE", "et-EE", "eu-ES", "fi-FI", "hu-HU", "ja-JP", "lt-LT", "nn-NO", "pl-PL",
"ro-RO", "se-FI", "se-NO", "se-SE", "sk-SK", "sl-SI", "sv-FI", "sv-SE", "tr-TR"
```

شکل ۴: زبان‌های سیستم معتبر برای رمزگذاری

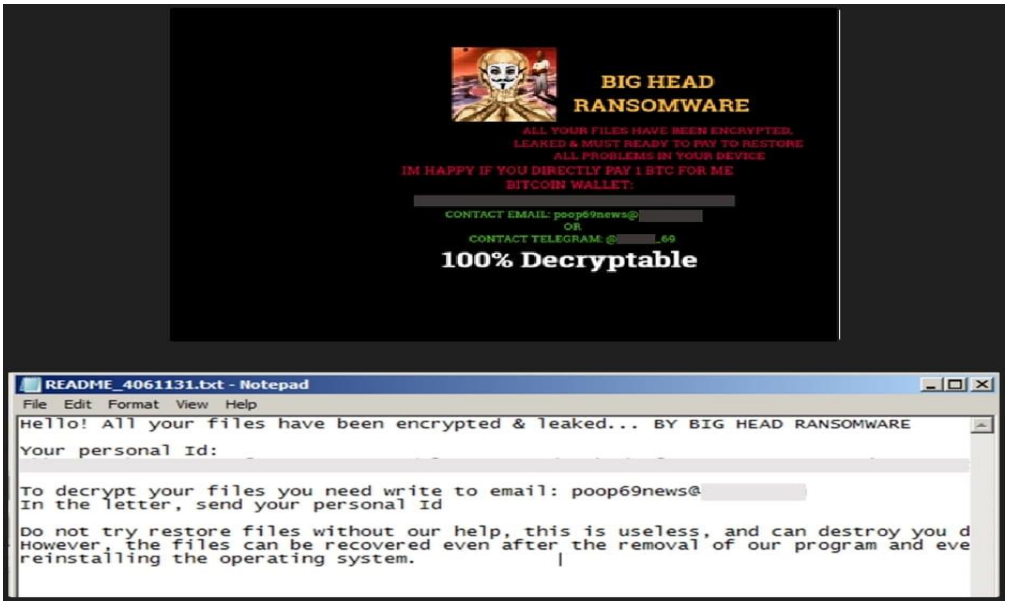
در طول رمزگذاری، باج‌افزار صفحه‌ای را نمایش می‌دهد که ظاهراً به‌روزرسانی قانونی ویندوز است.

.



شکل ۵: به روز رسانی جعلی ویندوز رمزگذاری فایل را پنهان می کند

پس از تکمیل فرآیند رمزگذاری، باج زیر در چندین فهرست حذف می‌شود و تصویر زمینه قربانی نیز برای هشدار آلودگی تغییر می‌کند.



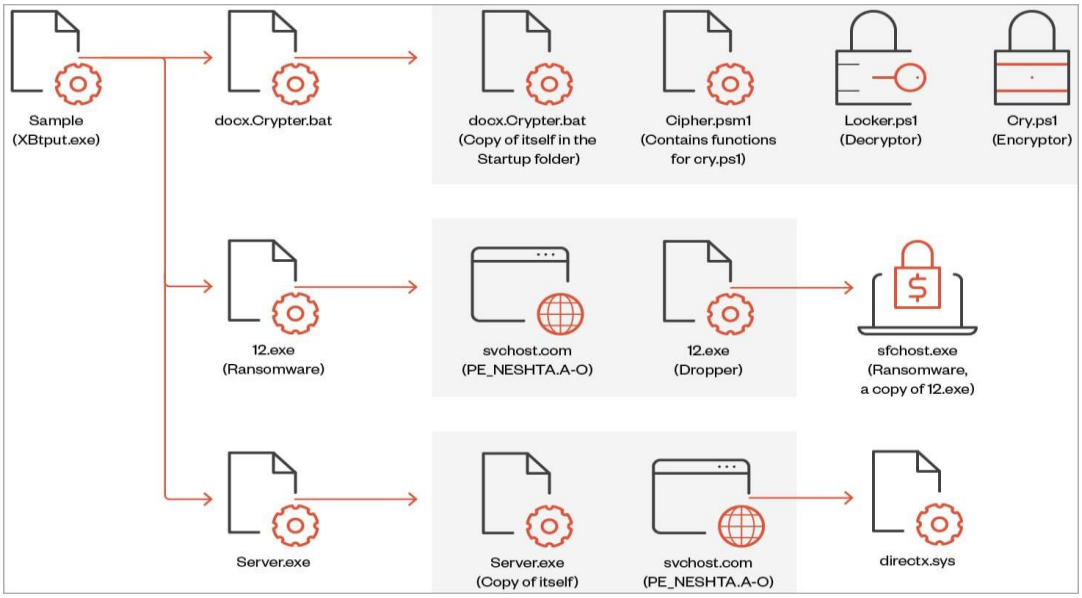
شکل ۶: والپیپر و یادداشت باج

Trend Micro همچنین دو نوع Big Head دیگر را تجزیه و تحلیل کرد و برخی از تفاوت‌های کلیدی را در مقایسه با نسخه استاندارد باج‌افزار برجسته کرد.

نوع دوم قابلیت‌های باج‌افزار را حفظ می‌کند، اما رفتار مهاجم را با عملکردهایی برای جمع‌آوری و استخراج داده‌های حساس از سیستم قربانی نیز در بر می‌گیرد.

داده‌هایی که این نسخه از Big Head می‌تواند به سرقت ببرد شامل تاریخچه مرور، فهرست دایرکتوری‌ها، درایورهای نصب شده، فرآیندهای در حال اجرا، کلید محصول و شبکه‌های فعال است و همچنین می‌تواند اسکرین‌شات بگیرد.

نوع سوم که توسط Trend Micro کشف شده است، یک آلاینده‌ی فایل به نام Neshta ارائه می‌دهد که کد مخرب را به فایل‌های قابل اجرای روی سیستم اضافه می‌کند. با اینکه هدف دقیق این امر نامشخص است، تحلیلگران Trend Micro حدس می زنند که این کار برای فرار از تشخیص‌هایی است که به مکانیزم های مبتنی بر امضا تکیه می‌کنند. شایان ذکر است که این نوع، از یادداشت باج متفاوتی نسبت به دو نوع دیگر استفاده می‌کند ولی همچنان به همان عامل تهدید گره خورده است.



شکل ۷: روال آلودگی نوع سوم

Trend Micro اظهار می‌کند که Big Head یک گونه باج‌افزار پیچیده نیست؛ متدهای رمزنگاری آن بسیار استاندارد و تکنیک‌های فرار از آن به سادگی قابل تشخیص هستند. با این وجود به نظر میرسد این باج روی مصرف‌کنندگانی تمرکز می‌کند که با ترفندهای ساده‌ای فریب می‌خورند(مانند آپدیت ویندوز جعلی) یا در درک تدابیر لازم برای دور شدن از خطرات امنیت سایبری مشکل دارند.

اظهار می‌شود که سازندگان Big Head به طور مداوم در حال توسعه و اصلاح بدافزار هستند، و رویکردهای مختلف را آزمایش می‌کنند تا ببینند چه چیزی بهترین کار را انجام می‌دهد.

۲ منابع

1. https://www.trendmicro.com/en_us/research/23/g/tailing-big-head-ransomware-variants-tactics-and-impact.html
2. https://www.bleepingcomputer.com/news/security/new-big-head-ransomware-displays-fake-windows-update-alert/#nlatest