وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز ماهر
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش بد افزار جدید **Reductor**

که ترافیک **HTTPS** را سرقت می‌کند

مقدمه:

در آوریل ۲۰۱۹، بدافزار جدیدی کشف شد که ارتباطات وب رمزگذاری شده را به روشی چشمگیر به خطر می‌اندازد. تجزیه و تحلیل این بدافزار این اجازه را داد تا تأیید کنند که اپراتورها یک سری کنترل خاص روی کانال شبکه‌ی هدف دارند و می‌توانند نصب کننده‌های قانونی را با موارد آلوده در حال اجرا جایگزین کنند.

اسم این نسل جدید از بدافزار را که کشف کرده‌اند Reductor است که اجازه می‌دهد مهاجم ترافیک پروتکل HTTP را توسط آسیب پذیری موجود در فرآیند تولید اعداد تصادفی یک مرورگر که برای اطمینان از اتصال خصوصی بین مشتری و سرور استفاده می‌شود دستکاری کند. Reductor پس از یک مسیر .pdb در برخی از نمونه‌ها به جا مانده است. علاوه بر کارکردهای معمول تابع RAT، مانند: بارگذاری، بارگیری و اجرای فایل ها ، نویسندگان Reductor تلاش زیادی را برای دستکاری در صدور گواهینامه‌های دیجیتال و علامت گذاری برون مرزی ترافیک TLS با شناسه‌های مرتبط با میزبان انجام می‌دهند.

تیم جهانی تحقیقاتی و تجزیه و تحلیل (GReAT) در کاسپرسکی، این بدافزار را کشف کرده‌اند. طبق گفته‌ی آن ها هنگامی‌که کسی از طریق این بدافزارآلوده شود، از Reductor برای جاسوسی از فعالیت مرورگر قربانی استفاده می‌شود. محققان گفتند که از Reductor برای جاسوسی سایبری از اشخاص دیپلماتیک که عضوی از جمهوری های پس از اتحاد جمایر شوروی هستند و به عنوان کشورهای مستقل مشترک المنافع شناخته می‌شوند، استفاده می‌شود. این محققان گفتند Reductor ارتباط نزدیکی با تروجان COMpfun دارد. علاوه بر این، تحقیقات بیشتر در این زمینه نشان داد که تروجان COMpfun احتمالاً به عنوان بارگیر(Downloder) در یکی از طرح های توزیع استفاده می‌شود. بر اساس این شباهت‌ها، این تیم کاملاً مطمئن هستند که این بدافزار جدید توسط نویسندگان COMPfun ساخته شده است. بدافزار COMpfun در ابتدا توسط G-DATA در سال ۲۰۱۴ ثبت شد. اگرچه G-DATA مشخص نکرد که چه کسی از این بدافزار استفاده می‌کند، اما کسپرسکی به طور آزمایشی آن را براساس آسیب شناسی با Turla APT مرتبط کرده است. اندازه گیری‌های کاسپرسکی نشان می‌دهد که کمپین فعلی با استفاده از Reductor از انتهای آوریل ۲۰۱۹ آغاز شده و در زمان نوشتن این گزارش(آگوست ۲۰۱۹) همچنان فعال بوده است. اهداف در روسیه و بلاروس شناسایی شده اند.

محققان گفتند، آنچه که Reductor را بسیار هوشمندانه جلوه می‌دهد، این است که چگونه مهاجمان توانسته‌اند بدافزارها را روی سیستم‌های هدفمند نصب کنند و چگونه آنها موفق به جلوگیری از عملکرد درست سیستم محافظت از HTTPS شده‌اند.

نحوه‌ی انجام حمله

تاکنون دو طرح آلودگی اولیه برای حمله ثبت شده است:

۱- **Reductor** با آلوده کردن نرم افزارهای رایج مدیریت دانلود فایل از اینترنت (**IDM, WinRAR** و غیره) شیوع پیدا می‌کند. این محققان در بخشی عنوان کرده‌اند که ظاهراً مهاجمان هنگامی‌که کاربران کامپیوتر در حال دانلود کردن از وب سایت‌های قانونی هستند قادر به وصل شدن به نرم افزارهای درست هستند. آن‌ها گفتند: "نصب کنندگان نرم افزار، از وب سایت‌های warez روی **HTTP** که دانلود رایگان نرم افزارهای دزدی را ارائه می‌دهند، آمده‌اند. این در حالی است که نصب کننده‌های نسخه‌های اصلی آلوده نشده‌اند، آنها به رایانه‌های شخصی قربانیان که دارای بدافزار هستند، پایان می‌دهند.

۲- یا اینکه با استفاده از توانایی **COMpfun** در دانلود فایل‌ها در میزبان‌های آلوده که قبلاً آلوده شده اند شیوع پیدا می‌کند

محققان به این نتیجه رسیدند که جایگزینی نصب نرم افزار در برنامه‌های در حال اجرا اتفاق می‌افتد و "اپراتورهای Reductor کانال شبکه هدف را کنترل می‌کنند."

چرخه آلوده سازی:

نحوه علامت زدن توافق TLS بدون حتی لمس کردن ترافیک: این بدافزار گواهی دیجیتالی را از بخش داده خود به میزبان هدف اضافه می‌کند و به اپراتورها اجازه می‌دهد تا گواهی‌های اضافی را از راه دور از طریق لوله نامگذاری شده اضافه کنند. هنگامی‌که یک سیستم آلوده شود، Reductor به دنبال ارتباطات اینترنتی می‌رود. این کار را با "وصله کردن" تولید کننده‌ی اعداد تصادفی مرورگر انجام می‌دهد که برای رمزگذاری ترافیک بین مرورگر کاربر و یک وب سایت از طریق HTTPS استفاده می‌شود. راه حلی که توسعه دهندگان Reductor برای نشان دادن ترافیک TLS یافتند، هوشمندانه ترین بخش است. آنها به هیچ وجه بسته های شبکه را لمس نمی‌کنند. در عوض توسعه دهندگان از کد منبع فایرفاکس و کد باینری Chrome برای وصله توابع تولید کننده اعداد شبه صادفی (PRNG) مربوطه در حافظه فرآیند استفاده کردند.مرورگرها در ابتدای توافق TLS از PRNG برای تولید دنباله ‘client random’ برای بسته‌های شبکه استفاده می‌کنندبه عبارت دیگر، مهاجمان به جای تلاش برای دستکاری در بسته های شبکه، مرورگرهای Firefox و Chrome و توابع تولید کننده اعداد تصادفی آنها را هدف قرار می‌دهند.

Reductor شناسه رمزگذاری شده منحصر به فرد مبتنی بر سخت افزار و نرم افزار را برای قربانیان به این قسمت ‘client random’ اضافه می‌کند. به منظور وصله کردن توابع PRNG سیستم، توسعه دهندگان از یک جداساز طول دستورالعمل Intel تعبیه شده استفاده کردند.

```
static SECStatus
ssl3_GetNewRandom(SSL3Random random)
{
    SECStatus rv;

    rv = PK11_GenerateRandom(random, SSL3_RANDOM_LENGTH);
    if (rv != SECSuccess) {
        ssl_MapLowLevelError(SSL_ERROR_GENERATE_RANDOM_FAILURE);
    }
    return rv;
}
```

شکل 1 - تولید اعداد تصادفی

```
/* Generate a new random if this is the first attempt. */
if (type == client_hello_initial) {
    rv = ssl3_GetNewRandom(ss->ssl3.hs.client_random);
    if (rv != SECSuccess) {
        goto loser; /* err set by GetNewRandom. */
    }
}

if (ss->vrange.max >= SSL_LIBRARY_VERSION_TLS_1_3) {
    rv = tls13_SetupClientHello(ss, type);
    if (rv != SECSuccess) {
        goto loser;
    }
}
```

شکل 2 - تولید اعداد تصادفی در اولین تلاش

همان طور که در شکل های ۱ و ۲ مشاهده می‌کنید به منظور وصله کردن توابع حافظه ی PRNG مرورگر و اضافه کردن یک شناسه ی کاربری واحد به توافق TLS، توسعه دهندگان Reductor ناچار به تجزیه و تحلیل Firefox و Chrome Chrome بودند.

تولیدکننده اعداد شبه تصادفی (PRNG) در تمام رمزنگاری‌ها استفاده می‌شود. در این حالت، هنگام ایجاد یک اتصال HTTPS امن بین مشتری و سرور یا مرورگر و وب سایت استفاده می‌شود. یک مرورگر و وب سایت، یک توافق TLS را ایجاد می‌کنند و تولید کننده اعداد شبه تصادفی یک"pre-master secret" (یا شماره) تصادفی ایجاد می‌کند که برای امنیت اتصال استفاده می‌شود. "pre-master secret" باید غیرقابل پیش بینی باشد تا یک اتصال ایمن برقرار باشد.

پیش بینی اعداد تصادفی

در اینجاست که Reductor وارد عمل می‌شود و قادر به تولید پیش بینی اعداد غیرقابل پیش بینی است. "مرورگرها از PRNG برای تولید دنباله‌ی 'client random' در ابتدای توافق TLS برای بسته شبکه استفاده می‌کنند. محققان کسپرسکی توضیح داده‌اند که Reductor شناسه رمزگذاری شده و سخت افزاری منحصر به فرد رمزنگاری شده و نرم افزار مبتنی بر تعیین کننده‌ی هویت قربانیان را برای این 'client random' اضافه می‌کند.

چرا آلودگی در برنامه‌های در حال اجرا رخ داده است؟

از آنجا که ما نمی‌دانیم که در سمت "سرور" چه اتفاقی می‌افتد، ما فقط می‌توانیم به تجزیه و تحلیل "مشتری" اعتماد کنیم. به منظور تمایز بین توافق‌های مورد علاقه از همه‌ی ترافیک‌های TLS، اپراتورهای کمپین ابتدا باید این قسمت "hello client" را رمزگشایی کنند. این بدان معناست که اپراتورها به نوعی باید به ترافیک هدف دسترسی داشته باشند. بدافزار Reductor خودش حمله‌ی مرد میانی (MitM) را انجام نمی‌دهد. با این حال، فرضیه‌ی اولیه این بود که گواهینامه‌های نصب شده ممکن است با شناسه منحصر به فرد موجود در توافق که ترافیک مورد علاقه را مشخص می‌کند حملات MitM به ترافیک TLS و زمینه 'client random' را تسهیل کنند.

طبق مشاهدات ثبت شده توسط محققان امنیتی، نصب کننده‌های آلوده از وب سایت‌های HTTPS warez دانلود می‌شوند اما همانطور که اغلب اتفاق می‌افتد، خود فایل‌ها از طریق HTTP بدون رمزگذاری دانلود می‌شوند. این باعث می‌شود که در طی فرایند دانلود، فایل ها را با فایل های مخرب جایگزین کنند. جالب است بدانید که داده‌های پیکربندی متعلق به برخی از وب سایت‌های قانونی بسیار مشهوری است. همچنین محققان فکر نمی‌کردند که سایت‌ها به عنوان سرورهای کنترل به خطر بیافتند. در هر صورت، در ابتدا نمی‌دانستند که چگونه نصب کننده‌ها آلوده می‌شوند، زیرا فایل‌های دانلود شده‌ی اصلی برای تجزیه و تحلیل در وب سایت های warez در دسترس نبودند و همیشه این احتمال وجود داشت که نصب کننده‌ها از زمانی که دانلود می‌شوند در وب سایت آلوده شده‌اند.

بررسی های اخیر در مورد Reductor سرنخ های دیگری را کشف کرده است. این بار نمونه‌ها دوباره از وب سایت‌های warez دانلود شد، اما محققان نمی‌توانستند تأیید کنند که در این مورد جدید، نصب کننده‌های اصلی آلوده نیستند. این به ما اجازه می‌دهد تا تأیید کنیم که اپراتورهای Reductor روی کانال شبکه هدف کنترل خاصی دارند و می‌توانند نصب کننده‌های مشروع را با موارد آلوده در حال اجرا جایگزین کنند.

ویژگی های Reductor

نویسندگان بدافزار خلاق هستند و حتی گاهی به نظر می‌رسد کمی‌سرگرم کننده هستند. به عنوان مثال، یکی از دامنه‌های وب که آنها برای COMpfun (نام شناخته شده عمومی) استفاده می‌کنند compfun[.]net است. در زیر خلاصه ای از انواع مختلف حملات نشان داده شده است:

	Initial infection	Escalation, detection avoidance	Main payload
Malware	COMpfun Trojan	Reductor dropper-decryptor	Reductor Trojan
Process	One of the browsers	Same browser	lsass.exe
Persistence	COM CLSID hijacking	Auxiliary module, N/A	LSA notification package
Net encryption	AES 128	Local module, N/A	AES 128

همانطور که قبلاً نیز اشاره شد، دو روش مختلف وجود دارد که مهاجمین برای پخش Reductor از آن استفاده می‌کنند. در سناریوی اول، مهاجمان از نصب کننده‌های نرم افزاری آلوده با نسخه های ۳۲ و ۶۴ بیتی Reductor استفاده می‌کنند. این نصب کننده ها ممکن است برای IDM، فعال ساز Office و غیره باشد. در سناریوی دوم، اهدافی که قبلاً با تروجان COMpfun آلوده شده‌اند، برای ادامه کار از COM CLSID استفاده می‌کند. پس از ورود به فضای آدرس مرورگر، تروجان می‌تواند دستور دانلود ماژول های اضافی از C2 را دریافت کند. در نتیجه، مرورگر هدف dropper-decryptor سفارشی Reductor را دانلود می‌کند. در جدول زیر سبک کد نویسی در تمام ماژول‌ها نشان داده شده است.

ویژگی	توضیحات
ذخیره سازی رشته ها	تمام رشته های مورد استفاده ، مانند نام عملکرد برای حل آدرس های پویا ، توسط توابع کوچک برمی‌گردند. توسعه دهندگان احتمالاً آنها را با استفاده از دستورالعمل C preprocessor #define به اجرا درآورده اند.
آدرس تابع با دقت پویا	برای هر کتابخانه پویا، توسعه دهندگان یک تابع مستقل و یک ساختار سفارشی برای ذخیره سازی آدرس توابع خود برای استفاده بیشتر پیاده سازی کرده اند.
استفاده‌ی گسترده از ساختارهای مرسوم	توسعه دهندگان برای هر کار از ساختارهای مرسوم استفاده می‌کنند: ارتباط C2، همگام سازی نخ (thread)، حل آدرس های توابع سیستم و غیره.

هش کردن اثر انگشت سیستم در داخل ‘client random’ متعلق به TLS

همانطور که پیش از این گفته شد، Reductor شناسه‌ی قربانی خود را در بسته‌های TLS اضافه می‌کند. اولین هش چهار بایت (cert_hash) با استفاده از همه گواهی نامه‌های دیجیتالی Reductor ساخته شده است. برای هر یک از آنها، مقدار اولیه‌ی هش، شماره نسخه‌ی X509 است. سپس آنها به ترتیب با تمام مقادیر چهار بایت از شماره سریال XOR می‌شوند. همه‌ی هش‌های حساب شده با یکدیگر XOR می‌شوند تا نمونه نهایی را بسازند. اپراتورها این مقدار را برای هر قربانی می‌دانند، زیرا با استفاده از گواهینامه‌های دیجیتال آنها ساخته شده است.

هش چهار بایت (hwid_hash) مبتنی بر ویژگی‌های سخت افزاری هدف یعنی: تاریخ و نسخه SMBIOS، تاریخ و نسخه BIOS Video و شناسه حجم دیسک سخت است. اپراتورها این مقدار را برای هر قربانی می‌دانند زیرا برای پروتکل ارتباطی C2 استفاده می‌شود. در نتیجه ساختار ۱۶ بایت مرسوم برای فریب مقادیر تولید شده توسط PRNG اصلی مطابق زیر است:

```
struct client_hello_system_fingerprint {
DWORD initial_xor_key; // First four bytes generated by original system PRNG function
DWORD predefined_const; // Set to 0x45F2837D
DWORD cert_hash; // Reductor's digital certificates hash
DWORD hwid_hash // Target's hardware hash
};
```

سه قسمت آخر با استفاده از چهار بایت اول رمزگذاری می‌شود (کلید اولیه PRN XOR). در هر دور، کلید XOR با الگوریتم (MUL 0x48C27395 MOD 0x7FFFFFFF) تغییر می‌کند. در نتیجه، بایت ها شبه تصادفی باقی می‌مانند، اما با شناسه‌ی میزبان منحصر به فرد در داخل رمزگذاری شده است.

وصله کردن PRNG

جدول زیروصله‌ی کمکی و توابع سیستم PRNG را نشان می‌دهد.

کتابخانه	توابع وصله شده	ویژگی‌ها
توابع کمکی		
“ntdll.dll”	RtlReleaseResource()	ذخیره داده های کمکی مانند شناسه نخ فعلی و تعداد علامت (tick) کنونی.

	memcpy()	اگر باید "client hello" کپی شود، باید cert_hash و hwid_hashرا بشمارید، بایت‌های منبع را به ساختار رمزگذاری شده‌ی client_hello_system_fingerprint تغییر دهید و با memcpy اصلی تماس بگیرید
یکی از کتابخانه‌های زمان اجرای C	time64()	صرفه جویی در وقت از ۱ ژانویه ۱۹۷۰ سپری شده است
"kernel32.dll" یا "kernelbase.dll"	GetSystemTimeAsFileTime()	
توابع PRNG		
"nss3.dll"	PK11_GenerateRandom()	با تابع PRNG اصلی تماس بگیرید و کلید XOR اولیه را از نتیجه آن تولید کنید. نتیجه PRNG را تغییر دهید: بایت هفتم را به ۱ تنظیم کنید، سپس ۰ x45F2837D، hwid و هش های cert را ذخیره کنید. نتیجه را رمزگذاری کنید و به جای PRN اصلی، آن را برگردانید. این بر حسب ssl3_SendClientHello () -> ssl3_GetNewRandom (ss-> ssl3.hs.client_random) بر تماس ها تأثیر می‌گذار
"advapi32.dll"	CryptGenRandom()	کلاهبرداری از تابع این سیستم PRNG به روش مشابه با برخی تغییرات جزئی انجام می‌شود.
"bcrypt.dll"	BCryptGenRandom()	
"chrome.dll"	PRNG function	تابع PRNG را با استفاده از الگوی کد باینری آن پیدا کنید و مانند تمام موارد ذکر شده آن را وصله کنید.

وصله‌ی irefox nss3.dll PK11_GenerateRandom()، که nss3.dll را برای فایرفاکس وصله می‌کند. منبع این کتابخانه در دسترس عموم قرار داده شده است. وصله‌ی PK11_GenerateRandom() در /security/nss/lib/ssl/ssl3con.c در تابع ssl3_GetNewRandom استفاده می‌شود. ثابت SSL3_RANDOM_LENGTH، ۳۲ بایت است بنابراین کد Reductor تمام نتایج و توابع را که به ssl3_GetNewRandom() فراخوانی می‌شوند تغییر می‌دهد، و داده‌های تصادفی اصلاح شده را با اثر انگشت رمزنگاری شده در داخل دریافت می‌کند. در این حالت، تابع فراخوان دهنده به ssl3_GetNewRandom(ss- >ssl3.hs.client_random) به منظور تولید داده "client random" برای توافق ارتباط اولیه ssl3_SendClientHello() ، است.

نویسندگان بدافزار توافق TLS، برای تأثیرگذاری()PK11_GenerateRandom را درون حافظه فرآیند Firefox وصله کردند. وصله ()PK11_GenerateRandom همچنین بر تولید هر بردار اولیه 256 (IV) بیتی (۳۲ بایت) تأثیر می‌گذارد، برای مثال، برای AES 256 در ()ssl_SelfEncryptProtect یا سایر توابع رمزنگاری شده در کتابخانه های NSS توسط Firefox مورد استفاده قرار گرفته است. از نظر ما، این می‌تواند یک اثر جانبی Reductor باشد که بدون هدف اضافی است.

گواهینامه‌های دیجیتال نصب شده

نمونه‌های کاهش دهنده دارای گواهینامه‌های رمزگذاری شده DER ریشه X509v3 در بخش data هستند تا روی میزبان هدف اضافه شوند. این بدافزار همچنین می‌تواند از طریق لوله نامگذاری شده گواهینامه‌های اضافی را از اپراتورها دریافت کند.

Certificate SHA1 fingerprint	CA for root cert	Valid till (GMT)
119B2BE9C17D8C7C5AB0FA1A17AAF69082BAB21D	ie-paypal	2031.11.17 22:56:10
546F7A565920AEB0021A1D05525FF0B3DF51D020	GeoTrust Rsa CA	2031.11.17 22:56:10
959EB6C7F45B7C5C761D5B758E65D9EF7EA20CF3	GeoTrust Rsa CA	2031.11.17 22:56:10
992BACE0BC815E43626D59D790CEF50907C6EA9B	VeriSign, Inc.	2031.11.17 22:56:10

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fa:9b:b7:53:21:86:97:bd:ed:1a:8c:85:59:fb:f6:94
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = EN, CN = GeoTrust Rsa CA, O = GeoTrust Rsa CA
        Validity
            Not Before: Oct 23 22:56:10 2011 GMT
            Not After : Nov 17 22:56:10 2031 GMT
        Subject: C = EN, CN = GeoTrust Rsa CA, O = GeoTrust Rsa CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d1:02:fa:c5:94:71:f2:45:4e:80:b9:ee:08:61:
                    ed:6b:c6:2c:3a:df:c7:99:48:a7:4c:ab:64:31:22:
```

شکل ۳- یکی از گواهی های رمزگشایی CA X509v3 در داخل بدافزار Reductor

ارتباطات C2

همه ارتباطات C2 در یک نخ (thread) بدافزار مستقل به کار برده می‌شوند. بدافزار Reductor سپس جستجوگرهای HTTP POST را به اسکریپت‌های query.php/ در C2 هایی که در پیکربندی آن ذکر شده

است ارسال می‌کند. جستجو POST حاوی شناسه سخت افزاری منحصر به فرد هدف است که با AES 128 رمزگذاری شده است. C2 یکی از دستورات رمزگذاری شده زیر را برمی‌گرداند.

به منظور وصله کردن (یا دستکاری) توابع PRNG مورد هدف، توسعه دهندگان نرم افزارهای مخرب از یک جداساز کوچک تعبیه شده درطول دستورالعمل Intel به عنوان بخشی از توالی حمله استفاده کردند. این کار به آنها اجازه می‌دهد تا به جای بسته‌های TLS از یک 'شناسه قربانی' استفاده کنند.

محققان کسپرسکی گفتند: "حمله کننده‌ها این مقدار را برای هر قربانی می‌دانند، زیرا با استفاده از گواهی‌های دیجیتالی آنها ساخته شده است. همچنین اجرا کننده ی تهدید تمام اطلاعات و اقدامات انجام شده با این مرورگر را دریافت می‌کند، در حالی که قربانی همچنان مظنون چیزی نیست و اطلاعی از حمله ندارد."

دستورات C2	ویژگی‌ها
hostinfo	گرفتن نام میزبان
gettimeout	مقدار زمان پایان را از مقدار رجیستری مربوطه دریافت کنید
options	رشته ها را تجزیه کرده و مقادیر مربوطه را در ثبات های سیستم تنظیم کنید. تاکنون فقط از یک گزینه پشتیبانی می شود - زمان پایان
domainlist	دامنه های فعلی C2 را که توسط هدف استفاده می شود انتقال دهید
downfile	دانلود فایل مورد علاقه
upfile	بارگذاری فایل مورد علاقه
execfile	فرآیندی را ایجاد کنید که فایل ذکر شده را اجرا کند
nop	کاری نکن. احتمالاً برای بررسی ارتباط با هاست استفاده می‌شود
kill	گواهی‌های دیجیتالی نصب شده، فایل‌ها، کوکی‌ها (cooki) و مقادیر رجیستری سیستم از جمله موارد مربوط به ماندگاری بسته اعلان COM CLSID یا LSA را حذف کنید
deletefile	فایل را در یک مسیر مشخص حذف کنید
certlist	گواهی های دیجیتالی نصب شده روی هدف را تمدید کنید

Kurt Baumgartner، محقق امنیتی در کسپرسکی، خاطرنشان کرد: "شناسه منحصر به فردی که Reductor به توافق هر جلسه TLS اضافه می‌کند می‌تواند به شناسایی منبع جلسه روی سیم کمک کند، در حالی که اضافه کردن و حذف گواهی‌های ریشه می‌تواند بی سر و صدا به رمزگشایی این ارتباطات قطع شده کمک کند. به عبارت دیگر، این گروه بسیار علاقه مند به دسترسی مخفی به محتوای ارتباط رمزگذاری شده، اعتبار احراز هویت و به طور کلی اطلاعات بسیار حساس هستند.

همچنین عنوان شده که علاوه بر حفظ دسترسی مداوم، این تنوع در توابع کتابخانه رمزنگاری، وصله گذاری، علامت گذاری TLS، اصلاح و دسترسی گواهی ریشه را به عنوان یک تلاش بالقوه برای تسهیل حملات TLS MitM نمایان می‌کند.

توسعه دهندگان بدافزار Reductor با تحلیل سورس کدهای مرورگرهای فایرفاکس و کروم توانایی دستکاری تایع مولد اعداد تصادفی مرورگر و اضافه نمودن شناسه کاربر در دست تکانی TLS را عملی نموده اند.

نتیجه گیری

در گذشته Turla روش‌های ابتکاری بسیاری را برای تحقق اهداف خود نشان داده است، مانند استفاده از زیرساخت‌های ماهواره‌ای ربوده شده. این بار، اگر ما درست بگوییم که Turla بازیگر این موج جدید از حملات است، پس با Reductor روشی بسیار جالب را برای علامت گذاری در TLS رمزگذاری شده میزبان با وصله کردن مرورگر بدون تجزیه بسته‌های شبکه به کار گرفته است. قربانی این کمپین جدید با علایق قبلی Turla مطابقت دارد. هیچ عملکرد MitM در نمونه‌های بدافزار مورد بررسی مشاهده نشده است. با این حال، Reductor قادر به نصب گواهینامه‌های دیجیتال و علامت گذاری در TLS اهداف است. از نصب کننده‌های آلوده برای آلودگی اولیه از طریق دانلود HTTP از وب سایت‌های warez استفاده می‌کند. با این واقعیت که فایل های اصلی در این سایت ها آلوده نیستند، همچنین به شواهدی از دستکاری بعدی در ترافیک اشاره دارد.

باومگارتنر یکی از اعضای تیم تحقیقاتی گفته است که وی قبلاً ندیده بود که توسعه دهندگان بدافزار با این روش درگیر رمزگذاری مرورگر باشند. وی همچنین اشاره کرد، سطح دسترسی که توسط خالق Reductor نشان داده شده است ، نشان می‌دهد که یک سازمان کاملاً حرفه ای، معمولاً با دولتها در ارتباط هستند. باومگارتنر گفت: "ما از کلیه ی سازمان‌هایی که با داده های حساس کار می‌کنند، هشیار باشند و بررسی‌های امنیتی منظم و کامل را داشته باشند."

فایل هش

- 27CE434AD1E240075C48A51722F8E87F

- 4E02B1B1D32E23975F496D1D1E0EB7A6
- 518AB503808E747C5D0DDE6BFB54B95A
- 7911F8D717DC9D7A78D99E687A12D7AD
- 9C7E50E7CE36C1B7D8CA2AF2082F4CD5
- A0387665FE7E006B5233C66F6BD5BB9D
- F6CAA1BFCCA872F0CBE2E7346B006AB4

دامنه و IP ها

- adstat.pw
- bill-tat.pw

مراجع

1 "**New Reductor Malware Hijacks HTTPS Traffic**," https://threatpost.com/new-reductor-malware-hijacks-https-traffic/148904/.

2 " COMpfun successor Reductor infects files on the fly to compromise TLS traffic ", https://securelist.com/compfun-successor-reductor/93633/