

بررسی و تحلیل باج‌افزار **GANDCRAB**

شیوه‌ها و روش‌های آلوده‌سازی
کالبدشکافی و بررسی عملکرد
ابزارهای رمزگشایی

فهرست مطالب

۱	چکیده مدیریتی
۲	تبهکارانی متحد
۳	روش‌های آلوده‌سازی
۳	دست‌درازی به برنامه‌های معروف
۳	بسته‌های بهره‌جو
۵	شبکه‌های مخرب
۵	پودمان RDP
۶	فرایند اجرا
۶	جمع‌آوری اطلاعات اولیه
۷	متوقف کردن پروسه‌ها
۸	ایجاد جفت کلید
۸	برقراری ارتباط با سرور فرماندهی
۹	رمزگذاری
۱۲	اعلام نتیجه به سرور فرماندهی
۱۲	حذف نسخه‌های Shadowcopy
۱۳	اخاذی
۱۴	خطاهای برنامه‌نویسی
۱۴	ابزارهای رمزگشایی
۱۴	اولین رمزگشا
۱۵	رمزگشایی ویژه برای شهروندان سوری
۱۷	پیشرفته‌ترین ابزار رمزگشایی
۱۸	از نگویش تا ستایش
۱۸	انتقام از ضدویروس آن‌لب
۱۹	ادای احترام در فهرست سفید
۱۹	رمزگذاری به نام یک نهاد و دو محقق
۲۰	پیام به یک محقق
۲۰	مجازات یک کلاهبردار
۲۰	دامنه‌هایی آشنا
۲۱	GandCrab به‌عنوان سرویس
۲۲	نام‌های شناسایی
۲۳	فهرست منابع

چکیده مدیریتی

GandCrab از جمله معروفترین باجافزارهایی است که در کمتر از یک سالی که از ظهور نخستین نسخه از آن می‌گذرد بیش از نیم‌میلیون دستگاه را در کشورهای مختلف از جمله ایران به خود آلوده کرده است. شدت آلودگی‌ها به GandCrab به حدی بوده که برخی کارشناسان از آن با عنوان پادشاه جدید باجافزارها یاد کرده‌اند. در ۲۱ شهریور ماه، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) نیز در اطلاعیه‌ای نسبت به انتشار گسترده نسخه چهارم GandCrab در سطح کشور هشدار داد.

خلاقیت‌های گردانندگان GandCrab در حوزه بازاریابی در تالارهای گفتگوی اینترنتی ویروس‌نویسان و نفوذگران پایانی ندارد. GandCrab یکی از اصلی‌ترین باجافزارهایی است که در قالب خدمات موسوم به "باجافزار به‌عنوان سرویس" به سایر تبهکاران سایبری اجازه داده می‌شود. راه‌اندازی باشگاه مشتریان و برگزاری مناقصه برای جلب شرکای جدید از نوآوری‌های قابل توجه نویسندگان این باجافزار است.

فعالیت نویسندگان GandCrab نیز همواره پر از حاشیه و جنجال بوده است. از در افتادن با برخی از شرکت‌ها و کارشناسان امنیتی گرفته تا تقدیر و تحسین برخی دیگر.

در حالی که میانگین مبلغ اخاذی‌شده توسط اکثر باجافزارها مبلغی بین ۲۰۰ تا ۵۰۰ دلار است، در GandCrab بسته به نوع مشتری و ارزش داده‌های بر روی دستگاه آلوده‌شده بیش از ۶۰۰ دلار از کاربر طلب می‌شود. حتی در برخی نمونه‌ها قربانیان مبلغ باج را ۷۰۰ هزار دلار گزارش کرده‌اند!

برآورد می‌شود GandCrab تنها ظرف چند ماه گذشته حداقل ۳۰۰ میلیون دلار را نصیب نویسندگان و گردانندگان خود کرده باشد.

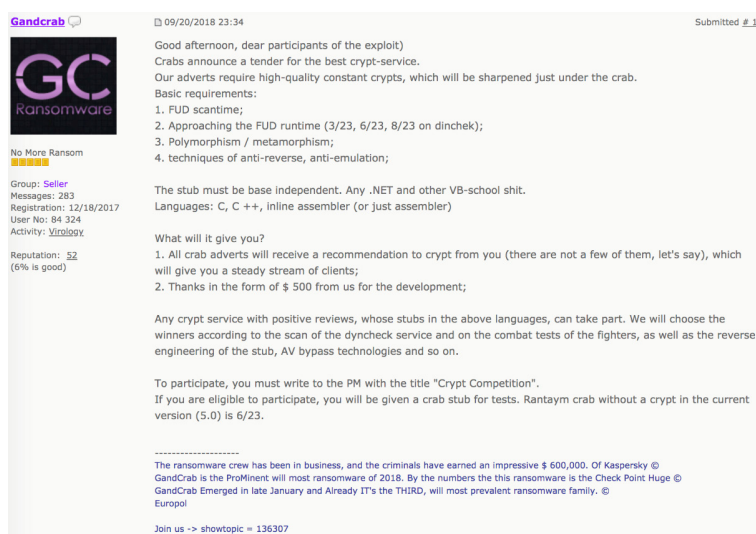
علیرغم رویکرد چابک و توانایی بالای نویسندگان GandCrab در بازاریابی و با وجود آن که طی عمر کوتاه آن نسخه‌های متعددی از این باجافزار منتشر شده، برنامه‌نویسی حرفه‌ای را نمی‌توان از مهارت‌های این افراد تلقی کرد. GandCrab که به زبان C++ نوشته شده پر از باگ و اشکالات فاحش برنامه‌نویسی است و روند تعداد این خطاها تا آخرین نسخه از آن نیز همچنان ادامه یافته است.

در این گزارش به بررسی و تحلیل نسخه‌های مختلف باجافزار GandCrab و ابزارهای رمزگشایی آن پرداخته شده است.

تبهکارانی متحد

این رویکرد جلب شرکای جدید، معروفیت GandCrab را در محافل زیرزمینی نفوذگران دوچندان کرد. برای یک کسب‌وکار تبهکاری سایبری نظیر GandCrab این گونه اتحادها روشی موثر برای از پا انداختن راهکارهای امنیتی است. در عمل بکارگیری چنین رویکردی ضمن ترکیب چندین ابزار مخرب و در نتیجه کارآمدتر شدن بدافزار، ریسک افشای کدها و فاش شدن هویت واقعی گردانندگان را نیز که در بسیاری مواقع به دلیل دخیل شدن تامین‌کنندگان ناآشنا و نامطمئن صورت می‌پذیرد کاهش می‌دهد. از نگاه امنیتی، موفقیت استراتژی‌های بازاریابی گردانندگان GandCrab موضوعی نگران‌کننده است. استراتژی‌هایی که با شراکت‌های هر چه بیشتر و تجهیز به ابزارهای تهاجمی مخرب و کارآمدتر، توان باج‌افزار GandCrab را افزایش داده و از سویی ممکن است خود به الگویی برای سایر تبهکاران تبدیل شود.

منافع مالی حاصل از انتشار GandCrab سبب ملحق شدن شرکای جدید به جمع گردانندگان این باج‌افزار گردیده است. در نسخه ۴، GandCrab مجهز به بسته بهره‌جویی جدید Fallout شد. موفقیت‌های ناشی از آن موجب گردید تا بکارگیری این بسته بهره‌جو در نسخه ۵ هم ادامه پیدا کند. به نحوی که نویسندگان GandCrab به‌طور عمومی از صاحبان Fallout قدردانی کردند. در نسخه ۵ شراکتی دیگر، این بار با یک سرویس رمزگذار با عنوان NTCrypt برقرار گردید. این سرویس کدهای بدافزار را مبهم‌سازی^۱ کرده و در عمل امکان فرار از سد محصولات امنیتی ضدبدافزار را برای کد مخرب فراهم می‌کند. مشارکت مذکور از طریق مناقصه‌ای که در روزهای ابتدایی مهر ماه در یک تالار گفتگوی اینترنتی^۲ توسط نویسندگان GandCrab برگزار شد حاصل گردید. در پنجم مهر ماه، NTCrypt خود را برنده این مناقصه اعلام کرد.



Submitted # 1

Good afternoon, dear participants of the exploit)
Crabs announce a tender for the best crypt-service.
Our adverts require high-quality constant crypts, which will be sharpened just under the crab.
Basic requirements:
1. FUD scantime;
2. Approaching the FUD runtime (3/23, 6/23, 8/23 on dinchek);
3. Polymorphism / metamorphism;
4. techniques of anti-reverse, anti-emulation;

The stub must be base independent. Any .NET and other VB-school shit.
Languages: C, C ++, inline assembler (or just assembler)

What will it give you?
1. All crab adverts will receive a recommendation to crypt from you (there are not a few of them, let's say), which will give you a steady stream of clients;
2. Thanks in the form of \$ 500 from us for the development;

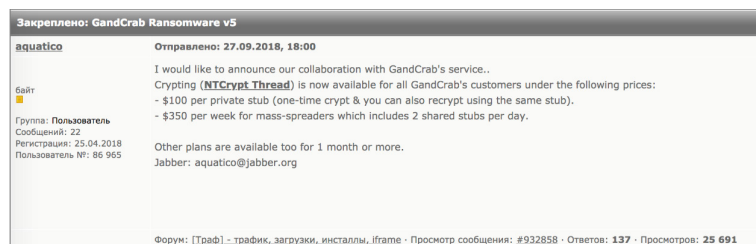
Any crypt service with positive reviews, whose stubs in the above languages, can take part. We will choose the winners according to the scan of the dyncheck service and on the combat tests of the fighters, as well as the reverse engineering of the stub, AV bypass technologies and so on.

To participate, you must write to the PM with the title "Crypt Competition".
If you are eligible to participate, you will be given a crab stub for tests. Rantaym crab without a crypt in the current version (5.0) is 6/23.

The ransomware crew has been in business, and the criminals have earned an impressive \$ 600,000. Of Kaspersky © GandCrab is the ProMinent will most ransomware of 2018. By the numbers the this ransomware is the Check Point Huge © GandCrab Emerged in late January and Already IT's the THIRD, will most prevalent ransomware family. © Europe!

Join us -> showtopic = 136307

مناقصه نویسندگان GandCrab
برای جذب سرویس رمزگذار



Закреплено: GandCrab Ransomware v5

aquatico Отправлено: 27.09.2018, 18:00

I would like to announce our collaboration with GandCrab's service..
Crypting (NTCrypt Thread) is now available for all GandCrab's customers under the following prices:
- \$100 per private stub (one-time crypt & you can also decrypt using the same stub).
- \$350 per week for mass-spreaders which includes 2 shared stubs per day.

Other plans are available too for 1 month or more.
Jabber: aquatico@jabber.org

Форум: [Траба] - трафик, загрузки, инсталлы, игате - Просмотр сообщения: #932858 - Ответов: 137 - Просмотров: 25 691

اعلام شراکت NTCrypt با GandCrab

^۱ Exploit Kit
^۲ Obfuscation
^۳ Forum

روش های آلوده سازی

باج افزار GandCrab از چندین مکانیزم برای آلوده سازی سیستم ها استفاده می کند که در ادامه به متداول ترین آنها پرداخته شده است.

هرزنامه

ارسال ایمیل های با پیوست مخرب یکی از اصلی ترین روش های انتشار GandCrab محسوب می شود. در اکثر مواقع پیوست ایمیل های ناقل این باج افزار فایلی فشرده شده با پسوند ZIP است که در یک اسکریپت (از نوع JavaScript، PowerShell و ...) جاسازی شده است. PowerShell از پروسه های معتبر سیستم عامل Windows است؛ چندین سال است که برخی مهاجمان حرفه ای کدهای مخرب خود را در قالبی غیراجرایی توسط این پروسه به اجرا در می آورند؛ تکنیکی که به "بدون فایل" معروف شده است. نمونه هایی نیز گزارش شده که در آنها پیوست ایمیل یک فایل Word حاوی ماکروی^۲ با کدهای مخرب است.



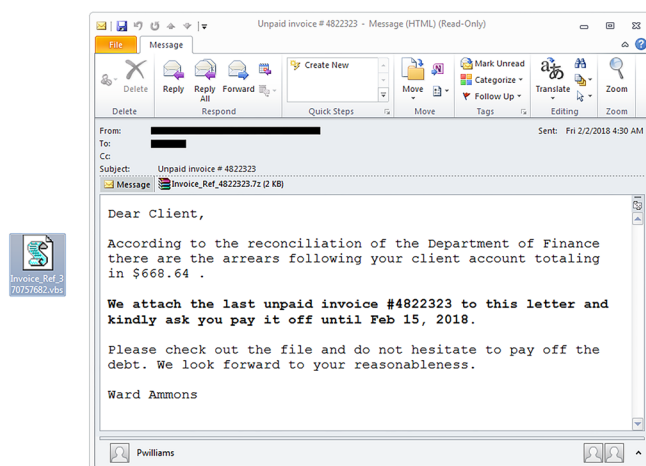
Hey there! How are you?

I'm absolutely interested in a opening.
Find my attached CV and reply ASAP.

The password for the file is 123123

Best regards!
Faith

نمونه هرزنامه های ناقل GandCrab



Fileless^۱
Macro^۲

Fallout

بسته بهره‌جو Fallout، نخستین بار در اوایل شهریور ماه توسط یک محقق امنیتی شناسایی شد. Fallout از آسیب‌پذیری CVE-2018-8174 در بخش مدیریت‌کننده کدهای VBScript و از آسیب‌پذیری CVE-2018-4878 در محصول Flash Player سوءاستفاده کرده و کد مخرب مورد نظر مهاجمان را بر روی دستگاه قربانی به صورت از راه دور نصب و اجرا می‌کند. ابزار بهره‌جوی مذکور در ابتدا تلاش می‌کند تا از آسیب‌پذیری VBScript سوءاستفاده کند. در صورت آسیب‌پذیر نبودن آن (به دلیل نصب بودن اصلاحیه مربوطه) و یا غیرفعال بودن VBScript به سراغ بهره‌جوی دوم به منظور سوءاستفاده از نرم‌افزار Flash Player می‌رود. چنانچه فرایند بهره‌جویی موفق باشد، یک اسب تروا^۱ بر روی دستگاه نصب می‌شود. یکی از وظایف این اسب تروا بررسی وجود هر یک از پروسه‌های زیر است:

- vmwareuser.exe
- vmwareservice.exe
- vboxservice.exe
- vboxtray.exe
- Sandboxiedcomlaunch.exe
- procmon.exe
- regmon.exe
- filemon.exe
- wireshark.exe
- netmon.exe
- vmttoolsd.exe

از آنجا که پروسه‌های مذکور معمولاً توسط تحلیلگران بدافزار مورد استفاده قرار می‌گیرند، در صورت مشاهده هر یک از آنها، اسب تروا وارد یک حلقه^۲ بی‌پایان شده و عملاً هیچ اقدام مخربی را از خود بروز نمی‌دهد. در غیر این صورت یک فایل DLL دریافت شده و باج‌افزار GandCrab بر روی دستگاه نصب می‌شود. آسیب‌پذیری CVE-2018-8174 در ۱۸ اردیبهشت ماه در مجموعه اصلاحیه‌های ماه میلادی می مایکروسافت ترمیم شد.

بهره‌جوهای متفرقه

سوءاستفاده از آسیب‌پذیری Task Schedule

یکی از بهره‌جوهای استفاده شده در نسخه ۵ باج‌افزار GandCrab، مجموعه کدی است که در ماه آگوست توسط هکری با عنوان SandboxEscaper بر روی توییتر و GitHub به اشتراک گذاشته شد.

^۱ Trojan

^۲ Loop

دست‌درازی به برنامه‌های معروف

در چند نوبت گردانندگان GandCrab با تزریق کد مخرب به برخی برنامه‌های پرستفاده و معروف و به اشتراک‌گذاری آنها در سطح اینترنت دستگاه کاربرانی را که اقدام به دریافت این برنامه‌ها می‌نمودند به باج‌افزار آلوده کردند.

بسته‌های بهره‌جوها

استفاده از بسته‌های بهره‌جوی مبتنی بر وب نیز یکی از دیگر روش‌های انتشار باج‌افزار GandCrab بوده که به تعدادی از آنها در ادامه اشاره شده است.

GrandSoft

GrandSoft از جمله بسته‌های بهره‌جویی است که در انتشار نسخه‌های اولیه GandCrab نقشی اساسی داشته است. این بسته بهره‌جو مهاجمان را قادر می‌کند تا با سوءاستفاده از آسیب‌پذیری CVE-2016-0189 در مرورگر Internet Explorer، به صورت از راه دور کد مخرب را بر روی دستگاه قربانی نصب و اجرا کنند. مایکروسافت آسیب‌پذیری مذکور را در اصلاحیه‌های MS16-051 و MS16-053 ترمیم کرده است.

Magnitude

در برخی از نسخه‌های GandCrab، مهاجمان با بکارگیری بسته بهره‌جوی Magnitude از آسیب‌پذیری‌های حیاتی CVE-2016-0189 و CVE-2018-4878 به ترتیب در مرورگر Internet Explorer و نرم‌افزار Flash Player سوءاستفاده کردند. این دو ضعف امنیتی، مهاجم را قادر به اجرای کد مخرب، به صورت از راه دور و بدون نیاز به هر گونه دخالت کاربر می‌کنند. بنابراین باز شدن یک صفحه اینترنتی دستکاری‌شده که حاوی بسته بهره‌جوی Magnitude است سبب می‌گردد تا بدون آن‌که کاربر بر روی لینکی کلیک کند یا فایلی را به اجرا در آورد، دستگاهی که دارای هر یک از آسیب‌پذیری‌های مذکور است به باج‌افزار GandCrab آلوده شود. در این حملات نیز مهاجمان با ارسال ایمیل‌های حاوی عناوین و محتوای جذاب کاربران را تشویق به کلیک بر روی لینک درج شده در داخل ایمیل کرده و در ادامه کاربر را به صفحه اینترنتی حاوی بسته بهره‌جو هدایت می‌کردند. همان‌طور که پیش‌تر اشاره شد آسیب‌پذیری CVE-2016-0189 توسط اصلاحیه‌های MS16-051 و MS16-053 شرکت مایکروسافت ترمیم و اصلاح شده است. شرکت ادوبی نیز ضعف امنیتی CVE-2018-4878 را در به‌روزرسانی APSA18-01 وصله کرده است.

می‌رسد که این افراد، با ارسال فایل خود به سایت تحلیلگر بدافزار، قصد بررسی واکنش ضدویروس‌ها به آن را داشته‌اند. اما فایل ارسال‌شده، در ادامه مورد تحلیل یکی از کارشناسان ضدویروس ای‌ست قرار گرفته و دو ضعف امنیتی که تا پیش از آن شرکت‌های ادوبی و مایکروسافت از آنها بی‌اطلاع بودند شناسایی می‌شود. در پی اعلام موضوع، مایکروسافت ۱۹ اردیبهشت ماه، همزمان با عرضه اصلاحیه‌های ماه میلادی می‌آسیب‌پذیری CVE-2018-8120 را ترمیم کرد. شرکت ادوبی نیز آسیب‌پذیری CVE-2018-4990 را در به‌روزرسانی APSA18-17 اصلاح و برطرف کرد.

شبکه‌های مخرب

نویسندگان GandCrab در مواردی اقدام به مشارکت با گردانندگان شبکه‌های مخرب^۳ کرده‌اند. هدف از این کار آلوده کردن دستگاه‌های تحت سیطره شبکه مخرب به باج‌افزار یا ارسال ایمیل‌های ناقل باج‌افزار از طریق این شبکه‌هاست. از جمله این شبکه‌های مخرب می‌توان به Phorpiex و Necurs اشاره کرد که البته هر دوی آنها در انتشار بسیاری از بدافزارهای دیگر نیز نقش داشته‌اند.

پودمان RDP

روش دیگر انتشار GandCrab سوءاستفاده از پودمان Remote Desktop - به اختصار RDP - با اجرای حملات موسوم به Brute-force است. هدف از اجرای حملات Brute-force رخنه به دستگاه از طریق پودمانی خاص - در اینجا RDP - با بکارگیری ترکیبی از نام‌های کاربری و رمزهای عبور رایج / افشاشده است. بنابراین در صورتی که دسترسی به پودمان RDP از طریق کاربری با رمز عبور ساده و غیرپیچیده باز شده باشد مهاجمان نیز به راحتی امکان اتصال به دستگاه آسیب‌پذیر را خواهند داشت. مهاجمان GandCrab پس از رخنه ارزش داده‌های بر روی دستگاه هک‌شده را که معمولاً از نوع سرور است ارزیابی نموده و بر اساس نتیجه حاصل‌شده مبلغ اخاذی ویژه‌ای را در اطلاعیه باج‌گیری درج می‌کنند.

بهره‌جوی مذکور، از ضعفی امنیتی از نوع "ترغیب امتیازی"^۱ در قابلیت Task Scheduler سیستم عامل Windows که از مدیریت ناصحیح بخش Advanced Local Procedure Call ناشی می‌شود سوءاستفاده می‌کند. بهره‌جویی از این ضعف که در آن زمان روز-صفر^۲ محسوب می‌شد، مهاجم یا برنامه مخرب را قادر به ارتقای دسترسی خود تا سطح سیستم بر روی دستگاه قربانی می‌کند. Advanced Local Procedure Call مکانیزمی داخلی در سیستم عامل Windows است که وظیفه آن سرعت بخشیدن و امن نمودن تبادل داده میان پروسه‌ها در حالت موسوم به User Mode است. شرکت مایکروسافت در ۲۰ شهریور، همزمان با عرضه اصلاحیه‌های ماه میلادی سپتامبر آسیب‌پذیری مذکور به شناسه CVE-2018-8440 را برطرف کرد.

بهره‌جویی از آسیب‌پذیری Win32k

بهره‌جوی دیگری که در نسخه ۵ باج‌افزار GandCrab مورد استفاده نویسندگان این باج‌افزار قرار گرفت، ابزار مخربی است که با سوءاستفاده از ضعفی با شناسه CVE-2018-8120 در بخش Win32k سیستم‌های عامل زیر امکان ارتقای سطح دسترسی را برای مهاجمان فراهم می‌کند.

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

ماجرای آسیب‌پذیری CVE-2018-8120 به ارسال یک فایل PDF حاوی کدهای مخرب توسط گروه ناشناسی از نفوذگران به یک سایت بررسی‌کننده بدافزار در تابستان امسال باز می‌گردد. موضوعی که سبب افشای نقطه ضعف مذکور و اشکالی خطرناک در نرم‌افزارهای Adobe Acrobat/Reader شد. این نفوذگران با تزریق کدهای JavaScript حاوی بهره‌جوی دو ضعف روز-صفر مذکور، فایلی PDF را به یک ابزار پیشرفته هک و انتشار بدافزار تبدیل کرده بودند. نقطه ضعف دوم با شناسه CVE-2018-4990 امکان اجرای از راه دور کد مخرب را از طریق نرم‌افزارهای Adobe Acrobat/Reader فراهم می‌کند. نفوذگران با مهارتی خاص، بهره‌جوی هر دو ضعف را در یک فایل در ظاهر بی‌خطر PDF جاسازی کرده بودند. به‌نظر

^۱ Privilege Escalation
^۲ Zero Day
^۳ Botnet

فرایند اجرا

به‌طور کلی مراحل اجرای باج‌افزار بر روی دستگاه قربانی را می‌توان به‌شرح زیر فهرست کرد:

- ۱- جمع‌آوری اطلاعاتی در خصوص دستگاه
- ۲- متوقف کردن پروسه‌هایی که ممکن است در صورت فعال بودن مانع از رمزگذاری شدن برخی از فایل‌های مورد نظر باج‌افزار بر روی دستگاه قربانی شوند
- ۳- ایجاد یک جفت کلید عمومی/خصوصی^۱
- ۴- اعلام به سرور فرماندهی^۲ با ارسال یک درخواست HTTP
- ۵- ایجاد یک کلید تصادفی AES-256 و استفاده از آن برای رمز کردن فایل، رمزگذاری آن توسط یک کلید عمومی RSA و الصاقش به فایل رمز شده
- ۶- ارسال پیام تایید به سرور فرماندهی
- ۷- حذف فایل‌های موسوم به Shadowcopy

جمع‌آوری اطلاعات اولیه

باج‌افزار GandCrab از طریق تابع GetNativeSystemInfo اطلاعات زیر را از روی دستگاه جمع‌آوری می‌کند:

- نام کاربری
- نام دستگاه
- دامنه Active Directory
- نام ضدویروس اجرا شده بر روی دستگاه؛ در صورت وجود
- قالب صفحه کلید (برای بررسی ملیت قربانی)
- نسخه و معماری سیستم عامل
- شماره سریال ذخیره‌ساز اصلی
- نام پردازشگر
- نوع درایوهای سیستمی

GandCrab هیچ قربانی در کشورهای عضو سابق اتحاد جماهیر شوروی نمی‌گیرد؛ احتمالاً با این هدف که گرفتار قوانین مشترک بین این کشورها نشود. بدین‌منظور چنانچه قالب صفحه کلید بر روی مقدار ۴۱۹ که ویژه صفحه کلید زبان روسی است تنظیم شده باشد باج‌افزار اجرای خود را متوقف می‌کند.

همچنین باج‌افزار اقدام به ایجاد یک شناسه برای دستگاه می‌کند که مهاجمان از آن با عنوان Ransom ID یاد می‌کنند. قالب شناسه مذکور به‌صورت زیر است.

`volume_serial_number||CRC32(volume_serial_number||processor_name)`

^۱ Public/Private Key
^۲ Command and Control

متوقف کردن پروسه ها

GandCrab، پیش از آغاز رمزگذاری، اقدام به بستن نرم افزارهای نمایش دهنده و ویرایش کننده اسناد، نرم افزارهای مدیریت کننده ایمیل، مرورگرها، برنامه های پایگاه داده و حتی برخی بازی های کامپیوتری می کند. اجرا بودن پروسه این نرم افزارها ممکن است منجر به شکست فرایند رمزگذاری فایل باز شده توسط آنها شود؛ به همین خاطر پروسه های زیر در ابتدای کار متوقف می شوند.

- sqlservr.exe (Microsoft SQL Server)
- msftesql.exe (Microsoft SQL Server)
- sqlagent.exe (Microsoft SQL Server Agent)
- sqlbrowser.exe (Microsoft SQL Browser Service)
- sqlwriter.exe (Microsoft SQL Server VSS writer)
- oracle.exe (Oracle Database Server)
- ocssd.exe (Oracle CSS Service)
- dbnmp.exe (Oracle Intelligent Agent)
- synctime.exe (SNTP Client by Rayslab Inc.)
- mydesktopqos.exe (Oracle MyDesktop QOS Service)
- agntsvc.exe sqlplussvc.exe (Oracle SNMP Listener)
- isqlpussvc.exe (Oracle iSQL*Plus Application Server)
- xfssvccon.exe (Oracle Drive XFS Service Console)
- mydesktopservice.exe (Oracle MyDesktop Service)
- ocautoupds.exe (Oracle Connector Automatic Updates Service)
- encsvc.exe (Citrix Encryption Service)
- firefoxconfig.exe (Oracle Firefox Config)
- tbirdconfig.exe (Oracle ThunderBird Config)
- ocomm.exe (Oracle Communicator)
- mysqld.exe (MySQL Daemon Process)
- mysqld-nt.exe (MySQL)
- mysqld-opt.exe (MySQL)
- dbeng50.exe (Sybase SQL Anywhere)
- sqbcoreservice.exe (SQL Backup Pro 7)
- excel.exe (Microsoft Excel)
- infopath.exe (Microsoft InfoPath)
- msaccess.exe (Microsoft Access)
- mspub.exe (Microsoft Publisher)
- onenote.exe (Microsoft OneNote)
- outlook.exe (Microsoft Outlook)
- powerpnt.exe (Microsoft PowerPoint)
- stream.exe (Steam)
- thebat.exe (Ritlabs The Bat)
- thebat64.exe (Ritlabs The Bat - x64)
- Thunderbird.exe (Mozilla Thunderbird)
- visio.exe (Microsoft Visio)
- winword.exe (Microsoft Word)
- wordpad.exe (Microsoft Wordpad)

GandCrab برای متوقف نمودن پروسه ها از توابع زیر بهره می گیرد: نمونه ای از درخواست در زیر قابل مشاهده است.

```
POST curl.php?token=[TOKEN_VAL] HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1;
WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/55.0.2883.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded
data=[ENCRYPTED_REPORT]
```

- CreateToolhelp32Snapshot
- Process32First
- Process32Next

ایجاد جفت کلید

• TOKEN_VAL: رشته ای متشکل از چهار عدد است که در فایل اجرایی GandCrab تزریق شده و احتمالا شناسه توزیع کننده باج افزار است. • ENCRYPTED_REPORT: رشته گزارش قربانی است که با الگوریتم RC4 و با یک کلید BASE64 که در کد باج افزار تزریق شده رمزگذاری شده است. این رشته می تواند شامل موارد زیر باشد:

- Action: برابر با مقداری است که در زمان فراخوانی به آن ارسال گردیده است.
- ip: نشانی IP قربانی که با برقراری ارتباط با سایت ip4bot.whatismyipaddress.com حاصل می شود.

- pc_user: نام کاربری کاربر جاری
- pc_group: نام دامنه کاربر جاری
- pc_lang: زبان تنظیم شده بر روی دستگاه
- pc-keyb: ۱، در صورتی که زبان صفحه کلید روسی باشد؛ ۰ برای هر زبان دیگر
- os_major: عنوان سیستم عامل (برای مثال، Windows 7 Starter)
- os_bit: معماری سیستم عامل (برای مثال x64)
- ransom_id: شناسه دستگاه که همان طور که توضیح داده شد در قالبی مشخص است.
- hdd: اطلاعاتی حاوی دیسک سخت دستگاه قربانی
- pub_key: کلید عمومی ایجاد شده که به یک Public key BLOB ارسال می شود.
- priv_key: کلید خصوصی ایجاد شده که به یک Private key BLOB ارسال می شود.
- version: نسخه باج افزار

روال های رمزگذاری GandCrab بر پایه دو الگوریتم RSA-2048 و AES-256 استوار هستند. این باج افزار یک جفت کلید کوتاه مدت مبتنی برای الگوریتم RSA 2048 را بر روی هر دستگاه ایجاد می کند. از این جفت کلید در ادامه برای رمزگذاری کلید AES 256-bit و بردار اولیه^۱ که در رمزگذاری فایل های کاربر مورد استفاده قرار می گیرند استفاده می شود. به ازای هر فایل کاربر، کلید AES جداگانه ای تعریف شده و به صورت رمزگذاری شده به همان فایل الصاق می شود. جفت کلید RSA در ادامه تبدیل به قالب BASE64 شده و اطلاعات دیگر استخراج شده به آنها افزوده می گردد.

برقراری ارتباط با سرور فرماندهی

در ادامه باج افزار اقدام به برقراری ارتباط با سرور فرماندهی می کند. فهرست سرورهای فرماندهی GandCrab به شرح زیر است:

- bleepingcomputer[.]bit
- nomoreransom[.]bit
- esetnod32[.]bit
- emsisoft[.]bit
- gandcrab[.]bit
- politiaromana[.]bit
- malwarehunterteam[.]bit
- gdcab[.]bit
- gandcrab[.]bit
- zonealarm[.]bit
- ransomware[.]bit
- carder[.]bit
- herbal-treatment-advisory[.]com
- pushpakcourier[.]net

دو مورد آخر، سایت های معتبری هستند که توسط گردانندگان GandCrab هک شده بودند.

^۱ Initialization Vector

رمزگذاری

هدف GandCrab نیز همانند بسیاری از باج افزارهای دیگر رمزگذاری فایل های بر روی دستگاه قربانی و اخاذی در ازای آنچه که بازگردانی فایل ها خوانده می شود است. فایل های با هر یک از پسوندهای زیر از اهداف این باج افزار تلقی می شوند.

.1cd, .3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .7z, .7zip, .aac, .ab4, .abd, .acc, .accdb, .accde, .accd, .accdt, .ach, .acr, .act, .adb, .adp, .ads, .agdl, .ai, .aiff, .ait, .al, .aoi, .apj, .apk, .arw, .ascx, .asf, .asm, .asp, .aspx, .asset, .asx, .atb, .avi, .awg, .back, .backup, .backupdb, .bak, .bank, .bay, .bdb, .bgt, .bik, .bin, .bkp, .blend, .bmp, .bpw, .bsa, .c, .cash, .cdb, .cdf, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfg, .cfn, .cgm, .cib, .class, .cls, .cmt, .config, .contact, .cpi, .cpp, .cr2, .craw, .crt, .crw, .cry, .cs, .csh, .csl, .css, .csv, .d3dbsp, .dac, .das, .dat, .db, .db_journal, .db3, .dbf, .dbx, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .def, .der, .des, .design, .dgc, .dgn, .dit, .djvu, .dng, .doc, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dx, .dxg, .edb, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fhd, .fla, .flac, .flb, .flf, .flv, .flvw, .forge, .fpx, .fxg, .gbr, .gho, .gif, .gray, .grey, .groups, .gry, .h, .hbk, .hdd, .hpp, .html, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .info, .info_, .ini, .iwi, .jar, .java, .jnt, .jpe, .jpeg, .jpg, .js, .json, .k2p, .kc2, .kdbx, .kdc, .key, .kpdx, .kwm, .laccdb, .lbf, .lck, .ldf, .lit, .litemod, .litesql, .lock, .log, .ltx, .lua, .m, .m2ts, .m3u, .m4a, .m4p, .m4v, .ma, .mab, .mapimail, .max, .mbx, .md, .mdb, .mdc, .mdf, .mef, .mfw, .mid, .mkv, .mlb, .mmw, .mny, .money, .moneywell, .mos, .mov, .mp3, .mp4, .mpeg, .mpg, .mrw, .msf, .msg, .myd, .nd, .ndd, .ndf, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nvram, .nwb, .nx2, .nxi, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .ogg, .oil, .omg, .one, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pb, .pbf, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .pif, .pl, .plc, .plus_muhd, .pm, .pmi, .pmj, .pml, .pmm, .pmo, .pmr, .pnc, .pnd, .png, .pnx, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .private, .ps, .psafe3, .psd, .pspimage, .pst, .ptx, .pub, .pwm, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .qcow, .qcow2, .qed, .qtb, .r3d, .raf, .rar, .rat, .raw, .rdb, .re4, .rm, .rtf, .rvt, .rw2, .rwl, .rwz, .s3db, .safe, .sas7bdat, .sav, .save, .say, .sd0, .sda, .sdb, .sdf, .sh, .sldm, .sldx, .slm, .sql, .sqlite, .sqlite3, .sqlitedb, .sqlite-shm, .sqlite-wal, .sr2, .srb, .srf, .srs, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stl, .stm, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxx, .sxi, .sxm, .sxw, .tax, .tbb, .tbk, .tbn, .tex, .tga, .thm, .tif, .tiff, .tlg, .tlx, .txt, .upk, .usr, .vbox, .vdi, .vhd, .vhdx, .vmdk, .vmsd, .vmx, .vmxf, .vob, .vpd, .vsd, .wab, .wad, .wallet, .war, .wav, .wb2, .wma, .wmf, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlb, .xlm, .xlr, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xml, .xps, .xxx, .ycbcr, .yuv, .zip

GandCrab از رمزگذاری فایل ها و پسوندهای زیر چشم پوشی می کند:

desktop.ini, autorun.inf, ntuser.dat, iconcache.db, bootsect.bak, boot.ini, ntuser.dat, thumbs.db, GDCB-DECRYPT.txt, .ani, .cab, .cpl, .cur, .diagcab, .diagpkg, .dll, .drv, .lock, .hlp, .ldf, .icl, .icns, .ico, .ics, .lnk, .key, .idx, .mod, .mpa, .msc, .msp, .msstyles, .msu, .nomedia, .ocx, .prf, .rom, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .exe, .bat, .cmd, .gandcrab, .KRAB, .CRAB, .yassine_lemmou

این باج افزار از دست درازی به پوشه های با هر یک از شناسه های CSIDL^۱ زیر خودداری می کند:

مسیر متداول	مقدار CSIDL
C:\Program Files (x86)	CSIDL_PROGRAM_FILESX86
C:\Program Files\Common	CSIDL_PROGRAM_FILES_COMMON
C:\Windows	CSIDL_WINDOWS
C:\Documents and Settings\[username]\Local Settings\Application Data	CSIDL_LOCAL_APPDATA

GandCrab قادر به شناسایی پروسه های ضدبدا افزارهای زیر است:

- VP.EXE
- ekrrn.exe
- avgnt.exe
- ashDisp.exe
- NortonAntiBot.exe
- Mcshield.exe
- avengine.exe
- cmdagent.exe
- smc.exe
- persfw.exe
- pccpfw.exe
- fsguiexe.exe
- cfp.exe
- msmtpeng.exe

همچنین وجود هر یک از راه اندازهای^۲ زیر نیز مورد بررسی قرار می گیرد:

- klif.sys متعلق به محصول Kaspersky Anti-Virus
- kl1.sys متعلق به محصول Kaspersky Anti-Virus
- fsdfw.sys متعلق به محصول F-Secure Anti-Virus Internet Shield
- srtsp64.sys متعلق به محصول Symantec Auto Protect
- srtsp.sys متعلق به محصول Symantec Auto Protect
- NavEx15.sys متعلق به محصول Symantec AV engine
- NavEng.sys متعلق به محصول Symantec AV engine

^۱ Constant Special Item ID List

^۲ Driver

فایل اصلی بدافزار، معمولاً - و نه همیشه - ترکیب شده از چندین فایل است. در بسیاری از نمونه‌های این باج افزار فایل اصلی EXE با چندین فایل DLL ترکیب شده است.

برای ماندگاری GandCrab، کلیدی در مسیر زیر در محضرخانه^۱ سیستم عامل ایجاد می‌شود.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Name	Type	Data
(Default)	REG_SZ	(value not set)
cyrzssyepsr	REG_SZ	"C:\Users\ [redacted] \AppData\Roaming\Microsoft\hhizen.exe"

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

▲
کلید اضافه شده در محضرخانه سیستم عامل

GandCrab اطلاعاتی باج‌گیری را با یک عملیات ساده XOR و مقداری که در کد آن درج شده رمزگشایی می‌کند. اطلاعاتی باج‌گیری حاوی متغیری با عنوان {USERID} است که در آن شناسه دستگاه آلوده درج می‌شود.

```
do
{
    v12 += 8;
    _mm_storeu_si128((__m128i *)v12 - 1, _mm_xor_si128(_mm_loadu_si128((const __m128i *)v12 - 1), v11));
    --v13;
}
while ( v13 );
do
{
    *((_BYTE *)&String1 + v14++) ^= 5u;
    while ( v14 < 0x10C2 );
    v15 = &String1;
    lpBuffer = &String1;
    if ( String1 )
    {
        v16 = String1;
        lpString2[32] = (LPCWSTR)((char *)&String1 - (char *)L"{USERID}");
        v17 = (char *)&String1 - (char *)L"{USERID}";
        while ( 1 )
        {
            v18 = L"{USERID}";
            if ( v16 )
                break;
            v16 = v15[1];
            ++v15;
            v17 += 2;
            if ( !v16 )
                goto LABEL_35;
        }
    }
}
```

▲
اشاره به متغیر {USERID} در کد باج افزار

^۱ Registry

جدول زیر پسوند الصاق‌شده به فایل‌های رمزگذاری‌شده توسط نسخه‌های مختلف باج‌افزار را نشان می‌دهد.

نسخه	پسوند الصاق‌شده	عنوان اطلاعیه باج‌گیری
۱	GDCB	=== GANDCRAB ===
۲	GDCB	=== GANDCRAB ===
۳	CRAB	=== GANDCRAB V3 ===
۴	KRAB	=== GANDCRAB V3 ===
۵	(+[A-Z])، نظیر:	=== GANDCRAB V5.0 ===
	UKCZA	=== GANDCRAB V5.0.2 ===
	YIAQDG	=== GANDCRAB V5.0.2 ===
	CQXGPMKNR	=== GANDCRAB V5.0.2 ===
	HHFEHIOL	

اعلام نتیجه به سرور فرماندهی

موفقیت‌آمیز بودن فرایند رمزگذاری به همراه اطلاعات زیر به سرور فرماندهی اطلاع‌رسانی می‌گردد. درخواست HTTP قالب دقیق و یکسانی با پیام ارسال‌شده اولیه دارد (شامل سرآیندها، منبع مورد درخواست و ...). تنها تفاوت رشته، گزارشی است که در بدنه رمزگذاری شده در ادامه data= می‌آید. مجدد، رشته، پارامتر استاندارد HTTP است که می‌تواند مقادیر زیر را داشته باشد:

- Action: همیشه برابر با result است.
- e_files: تعداد فایل‌های رمزگذاری شده را نشان می‌دهد.
- e_size: مجموع اندازه فایل‌های رمزگذاری شده را نمایش می‌دهد.
- e_time: مجموع زمان صرف شده از ابتدای فرایند تا پایان رمزگذاری بر حسب میلی‌ثانیه را بیان می‌کند.

حذف نسخه‌های Shadowcopy

دیگر توانایی GandCrab قابلیت است که به یک ویژگی مشترک تمامی باج‌افزارها تبدیل شده و آن چیزی نیست جز حذف فایل‌های موسوم به Shadowcopy. به محض ارسال گزارش نهایی به سرور فرماندهی با اجرای AllocateAndInitializeSid و CheckTokenMembership عضویت کاربر جاری در گروه Administrators (با SID به شناسه S-1-5-32-544) مورد بررسی قرار می‌گیرد. اگر نتیجه این بررسی مثبت باشد فایل‌های Shadowcopy حذف می‌شود.

در صورت فعال بودن Windows Management Instrumentation، GandCrab اقدام به اجرای فرمان زیر به منظور حذف فایل‌های Shadowcopy می‌کند:

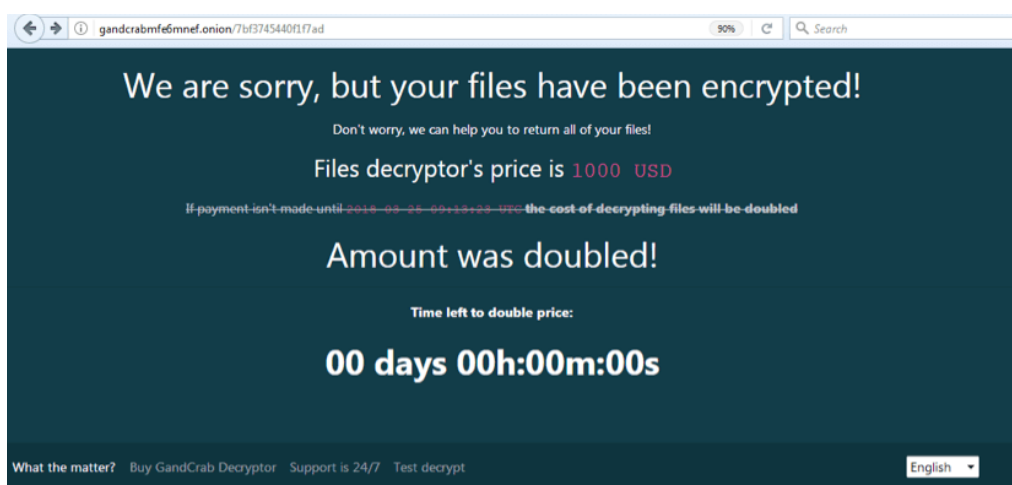
```
ShellExecute: C:\Windows\system32\wbem\wmic.exe shadowcopy delete
```

و در صورت غیرفعال بودن Windows Management Instrumentation با استفاده از پروسه vssadmin فرمان زیر اجرا می‌شود:

```
C:\Windows\system32\cmd.exe /c vssadmin delete shadows /all /quiet
```

اخاذی

در نسخه‌های ابتدایی GandCrab پرداخت مبلغ اخاذی شده تنها از طریق ارز رمز دش^۱ امکان پذیر بود. در نسخه‌های بعدی، ارز رمز متداول بیت کوین^۲ نیز مورد پشتیبانی نویسندگان این باج افزار قرار گرفت. از ویژگی‌های این ارز رمزها شناسایی بسیار دشوار و در حقیقت غیرممکن هویت واقعی پرداخت/دریافت کننده و در عین حال سهولت و سرعت بالای فرایند انتقال است. برای پرداخت باج کاربر باید از طریق شبکه ناشناس Tor به سایتی که در اطلاعیه باج گیری به آن اشاره شده متصل شود.



What the matter?

Your computer has been infected with **GandCrab Ransomware**. Your files have been encrypted and you can't decrypt it by yourself. In the network, you can probably find [decryptors](#) and third-party software, but it won't help you and **it only can make your files undecryptable**

What can I do to get my files back?

You should buy **GandCrab Decryptor**. This software will help you to decrypt all of your encrypted files and remove GandCrab Ransomware from your PC. Current price: **\$1,000.00**. As payment, you need cryptocurrency [DASH](#) or [Bitcoin](#)

What guarantees can you give to me?

You can use test decryption and decrypt **1 file for free**

What is *cryptocurrency* and how can I purchase GandCrab Decryptor?

You can read more details about cryptocurrency at Google or [here](#). As payment, you have to buy [DASH](#) or [Bitcoin](#) using a credit card, and send coins to our address.

How can I pay to you?

You have to buy Bitcoin or DASH using a credit card. Links to services where you can do it: [Dash exchanges list](#), [Bitcoin exchanges list](#). After it, go to our payment page [Buy GandCrab Decryptor](#), choose your payment method and follow the instructions

▲
نمونه‌ای از سایتی که در اطلاعیه باج گیری به آن اشاره شده

در سامانه‌ای که قربانی در شبکه Tor با آن روبرو می‌شود امکان رمزگشایی رایگان یک فایل فراهم است.

^۱ Dash
^۲ Bitcoin

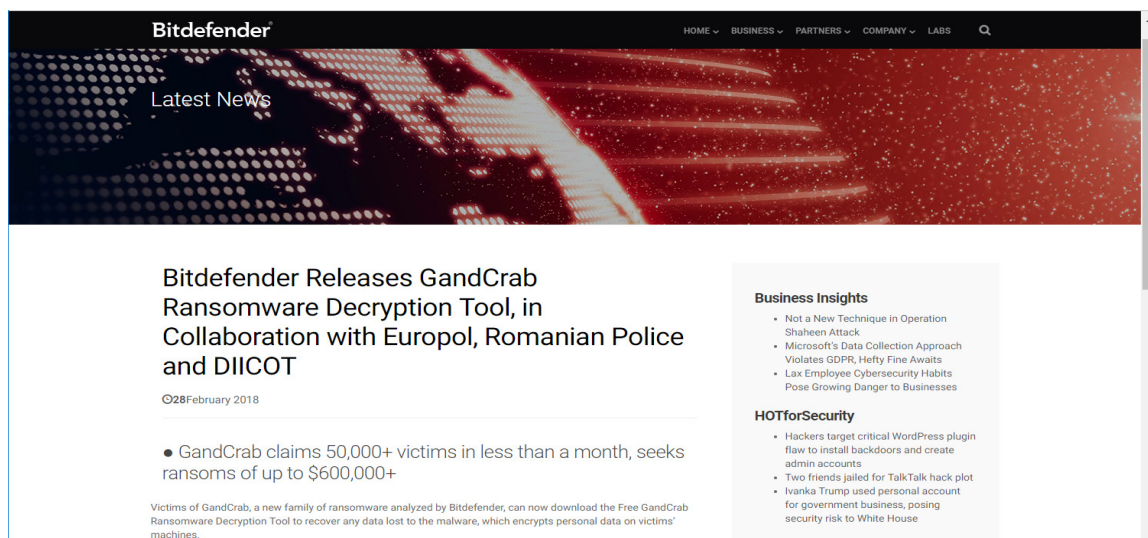
خطاهای برنامه‌نویسی

وجود اشکالات برنامه‌نویسی در GandCrab همواره یکی از موضوعات قابل بحث در خصوص این باج‌افزار بوده است. برای مثال، در نسخه ۵ این باج‌افزار، بخاطر اشتباهی ناشیانه در زمان کامپایل، امکان اجرای آن بر روی نسخه‌های XP و Vista سیستم عامل Windows فراهم نمی‌شود. دلیل این موضوع اجرای یک بهره‌جو از طریق توابع و فراخوانی‌های معمول است. در زمان کامپایل، کد دودویی از جدول موسوم به IAT^۱ که حاوی فایل‌های DLL مورد نیاز است فراخوانی می‌شود. DLL مذکور در نسخه‌های XP و Vista سیستم عامل Windows موجود نیست و بنابراین بخاطر این اشتباه، GandCrab بر روی این سیستم‌های عامل قابل اجرا نمی‌بود. یا در نسخه ۵/۰/۲ تغییرات مختصری در محضرخانه انجام شد که منجر به اجرای نادرست باج‌افزار گردید.

ابزارهای رمزگشایی

اولین رمزگشا

تقریباً دو ماه پس از انتشار نخستین نسخه از GandCrab، در اسفند ماه سال ۹۶، شرکت ضدویروس بیت‌دیفندر ابزار رایگانی را عرضه کرد که قربانیان را قادر به رمزگشایی فایل‌ها بدون نیاز به پرداخت مبلغ اخاذی‌شده توسط نویسندگان این باج‌افزار می‌کرد. گفته می‌شد که شرکت بیت‌دیفندر از طریق رخنه به یکی از سرورهای فرماندهی این باج‌افزار و شناسایی کلیدهای رمزگشایی اقدام به ساخت ابزار مذکور کرده است. نویسندگان GandCrab نه‌تنها این اقدام بیت‌دیفندر را تلافی نکردند که حتی با عبارت "good work" مهارت آنها را در رخنه به یکی از سرورهای فرماندهی این باج‌افزار و شناسایی کلیدهای رمزگشایی تحسین کردند!



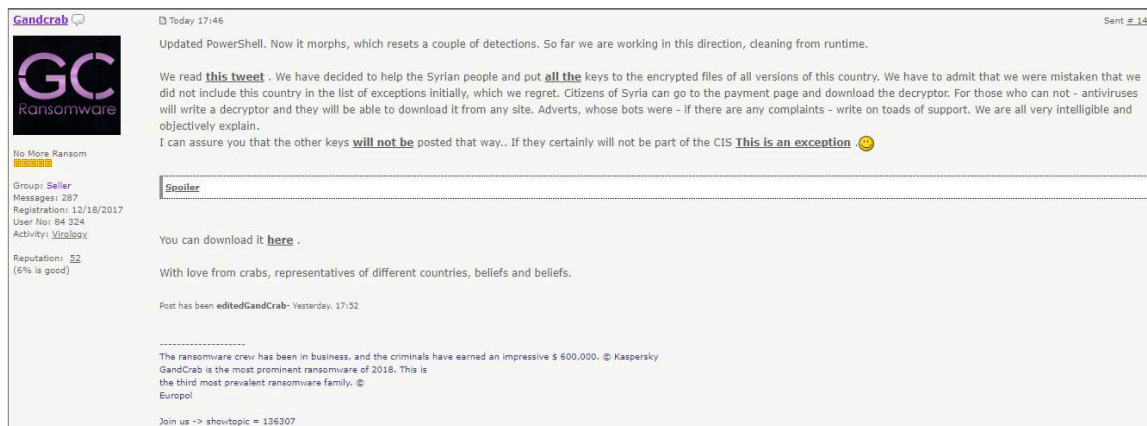
The screenshot shows the Bitdefender website's 'Latest News' section. The main headline reads: 'Bitdefender Releases GandCrab Ransomware Decryption Tool, in Collaboration with Europol, Romanian Police and DIICOT'. Below the headline, it states: 'GandCrab claims 50,000+ victims in less than a month, seeks ransoms of up to \$600,000+'. A sub-headline mentions: 'Victims of GandCrab, a new family of ransomware analyzed by Bitdefender, can now download the Free GandCrab Ransomware Decryption Tool to recover any data lost to the malware, which encrypts personal data on victims' machines.' To the right, there are two sidebars: 'Business Insights' with bullet points about a new technique, Microsoft's data collection approach, GDPR, and lax employee cybersecurity habits; and 'HOTforSecurity' with bullet points about WordPress plugin flaws, TalkTalk hack plot, and Ivanka Trump's account.

انتشار خبر اولین ابزار رمزگشایی GandCrab

^۱ Import Address Table

رمزگشایی ویژه برای شهروندان سوریه

در اواخر مهر ماه ۱۳۹۶، نویسندگان GandCrab در پیامی که در یک تالار گفتگوی اینترنتی ارسال شد، کلیدهای رمزگشایی متعلق به قربانیان سوری این باج‌افزار مخرب را منتشر کردند.



GandCrab

Updated PowerShell. Now it morphs, which resets a couple of detections. So far we are working in this direction, cleaning from runtime.

We read [this tweet](#). We have decided to help the Syrian people and put **all the** keys to the encrypted files of all versions of this country. We have to admit that we were mistaken that we did not include this country in the list of exceptions initially, which we regret. Citizens of Syria can go to the payment page and download the decryptor. For those who can not - antiviruses will write a decryptor and they will be able to download it from any site. Adverts, whose bots were - if there are any complaints - write on toads of support. We are all very intelligible and objectively explain.

I can assure you that the other keys **will not be** posted that way.. If they certainly will not be part of the CIS **This is an exception** 😊

Spoiler

You can download it [here](#).

With love from crabs, representatives of different countries, beliefs and beliefs.

Post has been edited by GandCrab - Yesterday, 17:52

The ransomware crew has been in business, and the criminals have earned an impressive \$ 600,000. © Kaspersky
GandCrab is the most prominent ransomware of 2018. This is the third most prevalent ransomware family, © Europol

Join us -> showtopic = 126307

انتشار کلیدهای رمزگشایی متعلق به قربانیان سوری GandCrab

این اقدام نویسندگان GandCrab در پاسخ به توییت‌هایی صورت گرفت که در آنها یک قربانی اهل سوریه برای بازگرداندن تصاویری از فرزندان فوت‌شده‌اش که فایل آنها توسط باج‌افزار مذکور از دسترس خارج شده بود درخواست کمک کرده بود. متن توییت‌های این شهروند سوری که خود را جمیل سلیمان معرفی کرده در تصویر زیر نمایش داده شده است.



جمیل سلیمان @kvbNDbxL0kmlqRU · Oct 15

@coveware Hello, my name is Jameel, I am a Syrian father who lost both his sons to the cruel war the country is going through
All I have left of my children is the photos and videos I took of them before they were mercilessly killed. And now GandCrab V5.0.3 has locked all of them

4 1

جمیل سلیمان @kvbNDbxL0kmlqRU Follow

They want 600 dollars to give me back my children, that's what they've done, they've taken my boys away from me for a some filthy money. How can I pay them 600 dollars if I barely have enough money to put food on the table for me and my wife?

10:55 PM - 15 Oct 2018

1

توییت شهروند سوری در خصوص رمزگذاری شدن تصاویر فرزندش

در پیام ارسالی توسط نویسندگان GandCrab رمزگذاری فایل‌ها بر روی دستگاه شهروندان سوریه یک اشتباه دانسته شده است. در پیام مذکور لینکی به یک فایل ZIP به چشم می‌خورد که خود حاوی دو فایل SY_keys.txt و readme.txt است.

در فایل readme.txt توضیحاتی در خصوص قالب و ساختار کلیدها و اطلاعاتی در مورد دلایل عرضه آنها به زبان روسی درج شده که ترجمه انگلیسی آن به شرح زیر است.

format:

id - ver - key

GandCrab for help SY people.

For antiviruses:

Decryptor to develop independently for each version.

We believe in the "power" of Bitdefender, since they all promise the decryptor constantly, and it is not yet ready, but now it is being developed and will soon be ready. Without keys, true. We would very much like the decryptor to be written by Kaspersky or Eset.

The most important thing is not to indicate that he will help everyone. He will help only a citizen of Syria. Because of their political situation, economic and relations with the CIS countries.

We regret that we did not initially add this country to the exceptions. But at least that way we can help them now.

Whose keys are not (only for citizens of Syria and the CIS, Ukraine including) - you need to come to us and take a picture of yourself with a passport and payment page. After that, we will issue a decryptor for free.

This is indicated just in case any clever people patch the file so that it works everywhere.

Hi, Polish kurvy.

As for other countries - we will not share the keys, even if we are closed someday. We will remove them. It is necessary to resume the punitive process in respect of some countries.

Let me remind you that you can only decrypt using our keys that are stored on our server. We issue them only after payment. There are no other miracle ways.

With love from crabs, representatives of different countries, religions, beliefs and beliefs.

--- With the support of the forum xss.is (ex. Damagelab) ---

فایل SY_keys.txt نیز حاوی ۹۷۸ کلید رمزگشایی از نسخه ۱/۰ تا نسخه ۵/۰ باج‌افزار GandCrab است.

به نظر می‌رسد که تشخیص سوری بودن قربانی، با بررسی نشانی IP دستگاه‌های آلوده به باج‌افزار انجام شده است. این نویسندگان از آن دسته از قربانیان سوری که شناسه دستگاه آنها در فایل مذکور نبود خواستند تا تصویری از خود، گذرنامه و اطلاعاتی باج‌گیری نمایش داده شده بر روی دستگاه را برایشان ارسال کنند تا احتمالاً با این کار مهاجران سوری نیز مشمول قانون جدید آنها قرار بگیرند.

علیرغم انتشار این کلیدها، قربانیان ناچار بودند تا منتظر عرضه ابزاری برای بازگردانی فایل‌ها توسط این کلیدها بمانند. در ۳۰ مهر ماه شرکت بیت‌دیفندر اقدام به عرضه ابزاری بدین‌منظور کرد.

همانطور که در فایل readme.txt نیز مشاهده می‌شود نویسندگان GandCrab تاکید کردند که بجز سوریه، کشورهای مشترک‌المنافع و اوکراین، در خصوص شهروندان کشورهای دیگر هیچ رحم و بخششی در کار نخواهد بود!

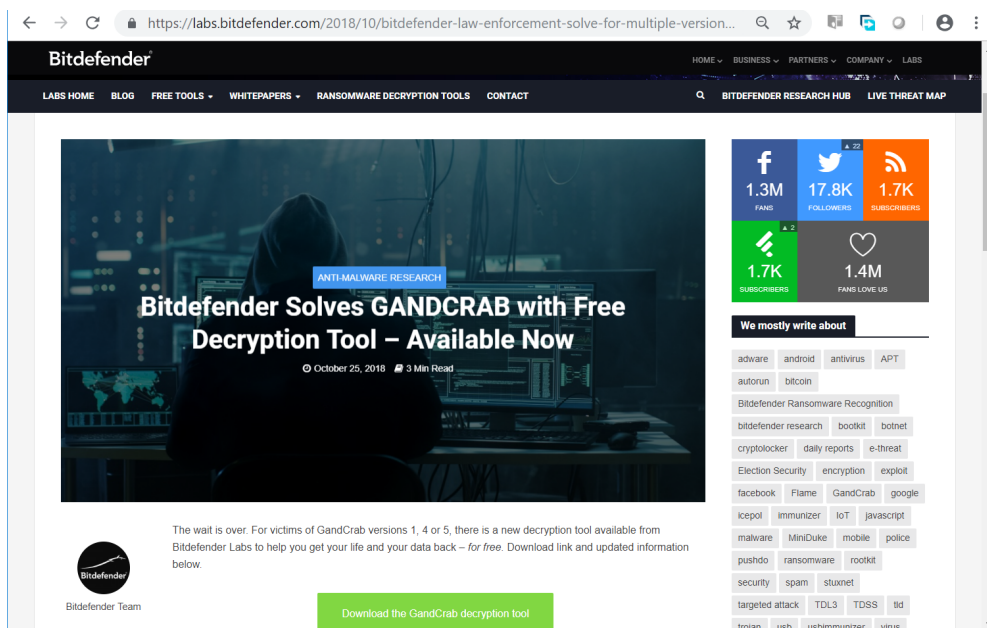
پیشرفته‌ترین ابزار رمزگشایی

در اوایل آبان ماه، شرکت ضدویروس بیت‌دیفندر ابزار رایگانی را عرضه کرد که امکان بازگرداندن فایل‌های رمزگذاری‌شده توسط اکثر نسخه‌های باج‌افزار معروف GandCrab را فراهم می‌کند.

بر طبق اعلام بیت‌دیفندر، ابزار مذکور قادر به رمزگشایی فایل‌های قفل‌شده توسط نسخه‌های ۱، ۴ و ۵ باج‌افزار GandCrab است.

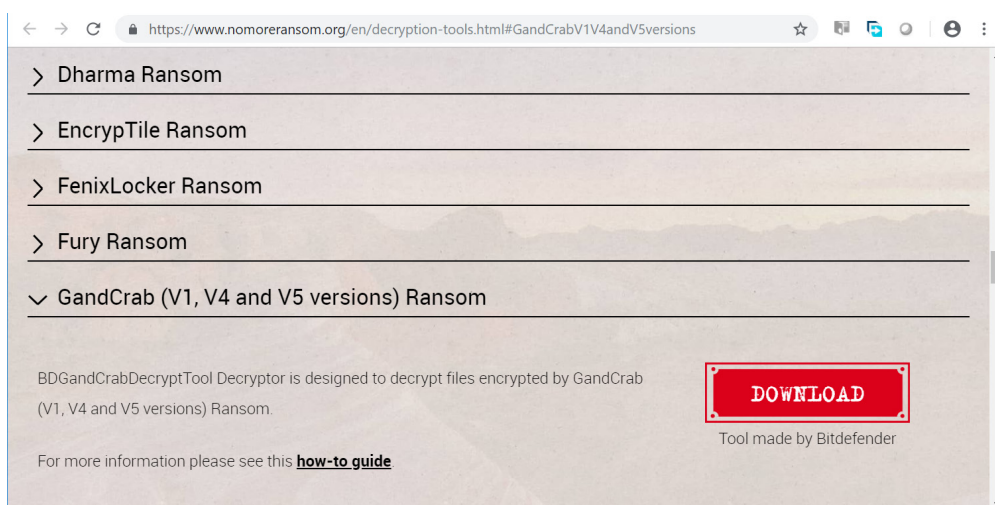
همچنین این شرکت از تلاش برای یافتن راهی به‌منظور بازگرداندن فایل‌های دست‌درازی شده توسط نسخه‌های ۲ و ۳ این باج‌افزار خبر داد.

به‌نظر می‌رسد عرضه این ابزار در پی کشف یک آسیب‌پذیری در فرایند رمزگذاری GandCrab ممکن شده است.



انتشار خبر عرضه کاملترین ابزار رمزگشایی GandCrab توسط شرکت بیت‌دیفندر

کاملترین ابزار رمزگشایی GandCrab بر روی سایت [nomoreransom.org](https://www.nomoreransom.org)



از نكوهش تا ستایش

انتقام از ضدویروس آن‌لب

در اواخر تیر ماه شرکت ضدویروس آن‌لب اقدام به انتشار ابزاری برای جلوگیری از رمزگذاری فایل‌ها توسط باج‌افزار GandCrab کرد. مدتی کوتاه پس از آن، نویسندگان این باج‌افزار در اقدامی تلافی‌جویانه، دو نسخه جدید GandCrab را مجهز به بهره‌جویی نمودند که با سوءاستفاده از یک آسیب‌پذیری روز-صفر، عملکرد این ضدویروس کراهی را دچار اختلال می‌کرد.

ابزار آن‌لب با ایجاد فایلی بر روی دستگاه، GandCrab را متقاعد می‌کرد که دستگاه پیش‌تر به باج‌افزار آلوده شده و با این روش عملاً از رمزگذاری فایل‌ها جلوگیری می‌کرد. نویسندگان GandCrab در پیامی که به سایت BleepingComputer ارسال کرده بودند اعلام نمودند که ابزار آن‌لب را تنها در عرض چند ساعت بی‌مصرف کرده‌اند.

در بخشی از کد نسخه‌های جدید GandCrab که از آسیب‌پذیری آن‌لب بهره‌جویی می‌کنند عبارت "سلام آن‌لب، نتیجه یک بر یک" (hey ahnlab, score - 1:1) به چشم می‌خورد.

```
push    offset aId      ; "&id="
call    esi ; lstrcatW
push    offset a128     ; "128"
call    esi ; lstrcatW
push    offset aSubId   ; "&sub_id="
call    esi ; lstrcatW
push    offset a453     ; "453"
call    esi ; lstrcatW
mov     [ebp+var_4], offset aHeyAhnlabScore ; "'hey ahnlab, score - 1:1. 0day exploit for Ahnlab V3 Lite Denial of service.
Possibly can trigger full write-what-where condition with privilege escalation, pass GandCrab http://filestorage.biz/
download.php?file=e541302686cca000584050d41e254261"
lea     eax, [ebp+var_4]
push    offset aVersion ; "&version="
call    esi ; lstrcatW
push    offset a421     ; "4.2.1"
call    esi ; lstrcatW
push    offset aActionCall ; "&action=call"
```

▲
اشاره به شرکت آن‌لب در کد باج‌افزار

آسیب‌پذیری مذکور ضعفی از نوع از کاراندازی سرویس^۱ است که سوءاستفاده از آن منجر به غیرفعال شدن یکی از اجزای ضدویروس آن‌لب و حتی در برخی مواقع بروز خطای موسوم به صفحه آبی مرگ^۲ در سیستم عامل می‌شود.

در بخشی دیگر از کدهای این بدافزار نیز علاوه بر آن‌لب، تلاش‌های شرکت امنیتی فورتینت نیز که مقالاتی در مورد GandCrab منتشر کرده است بی‌ارزش دانسته شده است.

```
push    eax
lea     eax, [ebp+var_408]
push    offset aXFortinetAhnla ; "%X fortinet & ahnlab, mutex is also kil"..|.
push    ; const WCHAR aXFortinetAhnla
call    aXFortinetAhnla ; DATA XREF: sub_402231+85fo
add     eax, 1
lea     eax, [ebp+var_1008]
push    eax
call    sub_402152
xor     eax, eax
pop     ecx
mov     [ebp+var_BE0], ax
lea     eax, [ebp+var_C08]
push    eax
lea     eax, [ebx+200h]
push    eax
push    offset aSSLock ; "%s\\%s.lock"
push    ebx ; LPWSTR
```

^۱ Denial of Service

^۲ Blue Screen of Death

▲
اشاره به شرکت‌های فورتینت و آن‌لب در کد باج‌افزار

ادای احترام در فهرست سفید

یکی از پسوندهایی که در فهرست سفید GandCrab جلب توجه می‌کند، yassine_lemmou است. yassine_lemmou به محقق اشاره دارد که در مورد این باجافزار مطالبی را توییت کرده است.

```
. .ani .cab .cpl .cur .diagcab .diagpkg .dll .drv .hlp .ldf .icl
. .icns .ico .ics .lnk .key .idx .mod .mpa .msc .msp .msstyles .m
su .nomedia .ocx .prf .rom .rtp .scr .shs .spl .sys .theme .them
epack .exe .bat .cmd .CRAB .crab .GDCB .gdcb .gandcrab .yassine_
lemmou
```

نام یک محقق در فهرست سفید باجافزار

رمزگذاری به نام یک نهاد و دو محقق

در فرایند ایجاد کلیدهای RC4 رشته‌هایی همچون "<3 fabian wosar"، "europol"، به چشم می‌خورد. Fabian Wosar یکی از کارشناسان شرکت امنی‌سافت است که چند ابزار رمزگشایی برای تعدادی باجافزار عرضه کرده است. Europol هم از جمله نهادهایی است که در عرضه دو ابزار رمزگشایی این باجافزار توسط بیت‌دیفندر نقش داشته است.

```
.rdata:005308C4 ; CHAR aFabianWosar3[]
.rdata:005308C4 aFabianWosar3 db 'fabian wosar <3',0 ; DATA XREF: sub_525900:loc_52596B↑o
.rdata:005308C4 ; sub_525AC0:loc_525C7F↑o ...
```

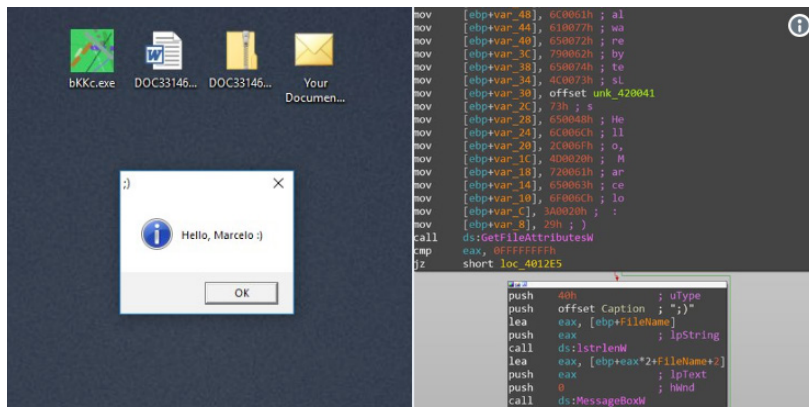
نام کارشناس امنی‌سافت در کد باجافزار

اشاره به Europol در کد باجافزار

```
00526A92 push esi
00526A93 push offset ProcName ; "RtlComputeCrc32"
00526A98 push eax ; hModule
00526A99 call ds:GetProcAddress
00526A9F push [ebp+lpString] ; lpString
00526AA2 mov esi, eax
00526AA4 call ds:lstrlenA
00526AAA push eax
00526AAB push [ebp+lpString]
00526AAE push 29Ah
00526AB3 call esi
00526AB5 push eax
00526AB6 push offset aXeupol ; "%Xeupol"
00526ABB push edi ; LPSTR
00526ABC call ds:wprintfA
00526AC2 add esp, 0Ch
00526AC5 pop esi
```

پیام به یک محقق

اگر بر روی دستگاه قربانی پوشه C:\MalwarebytesLabs موجود باشد پنجره‌ای حاوی پیام زیر ظاهر می‌شود. Marcelo Rivero یکی از محققان شرکت ملوربایت است!



اشاره به نام یکی از محققان شرکت ملوربایت

مجازات یک کلاهبردار

در یک تالار گفتگوی اینترنتی به نشانی exploit.in با ارسال مطالبی تلاش شد تا با استفاده از عنوان "Sick Children" (کودکان بیمار) از کاربران این تالار کلاهبرداری شود. کلاهبردار به سرعت توسط اعضای این تالار از جمله نویسندگان GandCrab شناسایی شد. برای مجازات او، نویسندگان GandCrab بر آن شدند تا شماره تلفن او (+380668846667) را در کد باج‌افزار خود افشا کنند.

```
v81 = 0;
v62 = (BYTE *)"&advert=+380668846667";
lstrcatW(v63, String2);
v39 = lpString1;
v63 = (LPWSTR)(16 * lstrlenW(lpString1) + 18);
lpMultiByteStr = (LPCSTR)VirtualAlloc(0, (SIZE_T)v63, 0x3000u, 0x40u);
v40 = 8 * lstrlenW(v39) + 2;
```

درج شماره تماس یک کلاهبردار در کد باج‌افزار

دامنه‌هایی آشنا

نشانی برخی از سرورهای فرماندهی GandCrab برگرفته‌شده از چند سایت متعلق به شرکت، نهاد، گروه و محقق امنیتی است که در مقابله با باج‌افزارها نقش داشته‌اند. این نشانی‌ها به شرح زیر است:

- bleepingcomputer[.]bit: برگرفته‌شده از سایت bleepingcomputer.com که یکی از منابع خبری در حوزه باج‌افزارهای جدید است.
- nomoreransom[.]bit: سایت متعلق به پروژه "اخاذی بس است" که شامل یک سایت اختصاصی به نشانی nomoreransom.org است. این پروژه توسط مرکز جرایم سایبری پلیس اروپا و با مشارکت بخش جرایم فرافرن پلیس هلند و چندین شرکت امنیتی از جمله مک‌آفی راه‌اندازی شده است.
- esetnod32[.]bit: برگرفته‌شده از عنوان ضدویروس ESET NOD32
- emsisoft[.]bit: برگرفته‌شده از سایت شرکت ضدویروس ام‌سی‌سافت به نشانی emsisoft.com
- politiaromana[.]bit: برگرفته‌شده از سایت پلیس رومانی به نشانی politiaromana.ro
- malwarehunterteam[.]bit: برگرفته‌شده از نشانی malwarehunterteam.com که با مشارکت چندین محقق امنیتی، در آن، اطلاعات و ابزارهای مختلف در خصوص مقابله با باج‌افزار و رمزگشایی فایل‌ها ارائه می‌شود.

GandCrab

به عنوان سرویس

چند سالی است که به اشتراک گذاری باج افزارها در قالب خدمات موسوم به "باج افزار به عنوان سرویس" متداول شده است. در این خدمات، صاحب باج افزار، فایل مخرب را به عنوان یک خدمت به متقاضی اجاره می دهد. متقاضی که ممکن است در برنامه نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج افزار را برعهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به نویسنده و بخشی دیگر به متقاضی می رسد. برای مثال، در GandCrab سهمی که به نویسندگان تعلق می گیرد ۳۰ درصد است.

معمولا در این مدل، متقاضی قادر به سفارشی کردن باج افزار خود است. از زبان استفاده شده در اطلاعیه باج گیری گرفته تا مقدار مبلغ اخاذی شده همگی در رابط های کاربری تحت وب به سادگی قابل انجام است.

علاوه بر کنسول مدیریتی کاربر پسند برای عرضه نسخه هایی کاملا مطابق با میل متقاضیان، نویسندگان GandCrab خدماتی همچون پشتیبانی ۲۴ ساعته، کمک تلفنی، مستندات راهنما در خصوص نحوه پیکربندی، توزیع و استفاده از باج افزار را ارائه می کنند.

حتی در برخی موارد در ازای مبلغی ناچیز، دسترسی به شبکه های مخربی را فراهم می کنند تا از آن طریق متقاضی اقدام به ارسال ایمیل هایی با پیوست های آلوده به این باج افزار کند. به عبارتی دیگر با چند کلیک می توان کارزاری مخرب از باج افزار GandCrab را در سطح جهان برپا کرد.

Dashboard

Ransoms list

Support

Transactions

Options

Administrator

2019-02-22 00:12:35

1 DASH = 678.461 \$

Ransoms list

[Home](#) [Ransoms list](#)

Ransoms list (3662)

Countries

Countries

Advert

wa

HWD

HWD

Registration

Registration

Decrypt price

Decrypt price

PC Key (Rs)

PC Key (Rs)

Test file

Test file

Status

Status

Filter

Reset

Country	IP address	Owner	HWD	Decrypt price / Discount	Registration	Encrypt datetime (last)	OS	AV	HDD	Views	Status
48.124.1			800 /	2019-02-21 21:53:54			Windows 7 Ultimate (x64 bit)		0	0	Not encrypted
85.103.1			800 /	2019-02-21 21:52:10			Windows 7 Ultimate (x64 bit)		0	0	Not encrypted
89.244.1			800 /	2019-02-21 21:43:08	2019-02-21 22:30:44		Windows 8.1 Connected Sin (x86 bit)	MalwareEng.exe	0	0	Encrypted
46.155.1			800 /	2019-02-21 21:42:41			Windows 7 Home Basic (x64 bit)		0	0	Not encrypted
176.42.1			800 /	2019-02-21 21:41:18	2019-02-21 22:13:14		Windows 7 Ultimate (x64 bit)		0	0	Encrypted
95.12.1			800 /	2019-02-21 21:39:48			Windows 7 Ultimate (x64 bit)		0	0	Not encrypted
95.5.1			800 /	2019-02-21 21:32:45	2019-02-21 21:42:48		Windows 7 Home Premium (x86 bit)		0	0	Not encrypted
78.190.1			800 /	2019-02-21 21:30:59			Windows 7 Professional (x86 bit)	elim.exe	0	0	Not encrypted
176.89.1			800 /	2019-02-21 21:30:07			Windows 8.1 Pro (x64 bit)	elim.exe, MalwareEng.exe	0	0	Not encrypted
176.89.1			800 /	2019-02-21 21:28:22			Windows 7 Ultimate (x64 bit)	elim.exe	0	0	Not encrypted
88.220.1			800 /	2019-02-21 21:27:12			Windows 8 Single Language (x64 bit)	MalwareEng.exe	0	0	Not encrypted

ViewGraph (1/2 10)

کنسول مدیریتی RaaS

Ransomware-as-a-Service - RaaS^۱
Bitcoin^۲

نام‌های شناسایی

عنوان شناسایی توسط بیت‌دیفندر	عنوان شناسایی توسط مک‌آفی	درهم‌ساز
Generic.Ransom.GandCrab4.91AB4FD5	Ran-GandCrabv4!E168E9E0F4F6	e168e9e0f4f631bafc47ddf23c9848d7
Gen:Variant.Zusy.104387	Generic.dyq	6884e3541834cc5310a3733f44b38910
Generic.Ransom.GandCrab4.A814F0F1	Ran-GandCrabv4!2D351D67EAB0	2d351d67eab01124b7189c02cff7595f
Generic.Ransom.GandCrab4.A814F0F1	Ran-GandCrabv4!41C673415DAB	41c673415dabbfa63905ff273bdc34e9
Trojan.GenericKD.40525310	RDN/Generic.dx	1e8226f7b587d6cd7017f789a96c4a65
Trojan.Ransom.27002	RDN/Ransom	fb25dfd638b1b3ca042a9902902a5ff9
Generic.Malware.SYddld.80AD0C92	RDN/Generic.hbg	df1a09dd1cc2f303a8b3d5097e53400b
Generic.Ransom.GandCrab4.8CBC6992	Ran-GandCrabv4!07FADB006486	07fadb006486953439ce0092651fd7a6
Gen:Variant.Brresmon.102	GenericRXGB-AG!97A910C50171	97a910c50171124f2cd8cfc7a4f2fa4f
Trojan.Ransom.GandCrab.Gen.2	Trojan-FPOH!F7C072A322CB	f7c072a322cb0b4ce491307ddad466da
Trojan.Ransom.GandCrab.C	Generic.ayp	be7b200d211566a3a91c7f832559b461
Trojan.GenericKD.30700043	GenericRXFG-WC!0CDDD7F2E0F6	0cddd7f2e0f61895e40df348aa3c01ff
Trojan.GenericKD.30699403	RDN/Ransom	a7af2c9b8c040970b886bf255757c9de
Trojan.GenericKD.30685240	GenericRXFG-AZ!96DC3E20ED85	96dc3e20ed8581139d1ee270041fe050
Trojan.GenericKD.30644881	RDN/GenericTroj	ed33e32e29b9562954495895005715d4
Trojan.GenericKD.30645418	GenericRXFA-HY!B5DC95BC3400	b5dc95bc340047eba2440b61212cb8d1
Trojan.GenericKD.30643402	GenericRXFQ-TQ!07F2AC3CA63B	07f2ac3ca63b6eff0761e0184123c492
Trojan.Agent.CYDD	Generic.ayp	a2bbae61bf0cf64b9d04b18cdd2a419d
Trojan.GenericKD.30749203	Trojan-FPQB!BBB97CA64607	bbb97ca6460707a4f0fecdd302a33c9ec
Trojan.GenericKD.30718240	RDN/Generic.grp	f67843981e331b4034352506bee02293
Trojan.Emotet.Gen.3	GenericRXFH-CQ!A9A0EC2F171B	a9a0ec2f171b9aa400912a80334b2470
Trojan.GenericKD.30709695	RDN/Generic.dx	f11c2c3bd013d10f8cdfc43018327725
Trojan.Ransom.GandCrab.Gen.2	GenericRXFH-VN!11CFF7EF2406	11cff7ef24061d8d59c6e1c2981a40e4
Trojan.GenericKD.30725877	RDN/Generic.hbg	b28cbc90bee7153a2050a476b9f34ce1

فهرست منابع

- <https://blog.malwarebytes.com/cybercrime/2018/06/exploit-kits-spring-2018-review/>
- <https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/>
- <https://blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html>
- <https://cdn.versa-networks.com/wp-content/uploads/2018/10/versa-sr-grandcrab-final.pdf>
- <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-051>
- <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-053>
- <https://docs.microsoft.com/en-us/windows/desktop/api/sysinfoapi/nf-sysinfoapi-getnativesysteminfo>
- <https://docs.microsoft.com/en-us/windows/desktop/api/tlhelp32/nf-tlhelp32-createtoolhelp32snapshot>
- <https://docs.microsoft.com/en-us/windows/desktop/api/tlhelp32/nf-tlhelp32-process32first>
- <https://docs.microsoft.com/en-us/windows/desktop/api/tlhelp32/nf-tlhelp32-process32next>
- <https://helpx.adobe.com/security/products/acrobat/apsb18-09.html>
- <https://helpx.adobe.com/security/products/flash-player/apsa18-01.html>
- https://kc.mcafee.com/resources/sites/MCAFFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27511/en_US/McAfee_Labs_Threat_Advisory-Ransom-GandCrab.pdf
- <https://labs.bitdefender.com/2018/10/bitdefender-gandcrab-decryptor-for-syrian-users-now-available/>
- <https://labs.bitdefender.com/2018/10/bitdefender-law-enforcement-solve-for-multiple-versions-of-gandcrab-with-new-decryptor/>
- <https://labs.bitdefender.com/2018/10/gandcrab-ransomware-decryption-tool-available-for-free/>
- <https://labs.bitdefender.com/2018/10/gandcrab-the-most-popular-multi-million-dollar-ransomware-of-the-year/>
- [https://msdn.microsoft.com/en-us/library/windows/desktop/bb762494\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx)
- <https://newsroom.shabakeh.net/19493/free-bitdefender-decrypter-for-gandcrab-ransomware-victims.html>
- <https://newsroom.shabakeh.net/19508/news-version-of-gandcrab-released.html>
- <https://newsroom.shabakeh.net/19644/gandcrab-ransomware-using-ie-and-flash-vulnerability.html>
- <https://newsroom.shabakeh.net/19688/gandcrab-version-3-released.html>
- <https://newsroom.shabakeh.net/19856/gandcrab-v4.html>
- <https://newsroom.shabakeh.net/19935/gandcrab-and-ahnlab.html>
- <https://newsroom.shabakeh.net/20004/alpc-zero-day-vulnerability.html>
- <https://newsroom.shabakeh.net/20046/gandcrab-and-fallout-exploitkit.html>
- <https://newsroom.shabakeh.net/20057/maher-and-gandcrab.html>
- <https://newsroom.shabakeh.net/20094/gandcrab-v5.html>
- <https://newsroom.shabakeh.net/20133/kraken-cryptor-using-fallout-ek.html>
- <https://newsroom.shabakeh.net/20174/decryption-keys-for-syrian-victims-of-gandcrab-released.html>
- <https://newsroom.shabakeh.net/20211/free-decrypter-available-for-almost-all-versions-of-gandcrab.html>
- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8120>
- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174>
- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8440>
- <https://research.checkpoint.com/gandcrab-ransomware-mindset/>
- <https://securingtomorrow.mcafee.com/mcafee-labs/gandcrab-ransomware-puts-the-pinch-on-victims/>
- <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rapidly-evolving-ransomware-gandcrab-version-5-partners-with-crypter-service-for-obfuscation/>
- <https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems>
- <https://support.microsoft.com/en-us/help/324097/list-of-language-packs-and-their-codes-for-windows-2000-domain-control>
- <https://www.acronis.com/en-us/articles/gandcrab/>
- <https://www.europol.europa.eu/newsroom/news/pay-no-more-universal-gandcrab-decryption-tool-released-for-free-no-more-ransom>
- <https://www.fortinet.com/blog/threat-research/gandcrab-v4-0-analysis-new-shell-same-old-menace.html>
- <https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.gandcrab-ransomware.html>
- <https://www.vmrays.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/>
- <https://www.welivesecurity.com/2018/10/25/eset-releases-new-decryptor-syrian-victims-gandcrab-ransomware/>
- <https://www.zdnet.com/article/gandcrab-ransomware-teams-up-with-crypter-service/>

در اتاق خبر شبکه گستر بخوانید...

گروگان گرفته نشوید!

حفاظت از سازمان در برابر باج‌افزارها

انواع باج‌افزار
انتشار و کودسازی
نمونه‌های واقعی
راهکارهای پیشگیری و مقابله

شبکه‌گستر
امنیت‌ها | راهکارها

حفاظت از سازمان در برابر تهدیدات مبتنی بر

Remote Desktop Protocol

شبکه‌گستر
امنیت‌ها | راهکارها

بررسی و تحلیل روش انتشار بدافزار از طریق

Internet Query File

کشف‌شدگی یک کارزار هراتانه‌ای
راهکارهای مقابله
نشانه‌های آلودگی

شبکه‌گستر
امنیت‌ها | راهکارها

بررسی و تحلیل کارزارهای سایبری

TEMP.ZAGROS

شیوه‌ها و روش‌های نفوذ
کشف‌شدگی بدافزارها
نشانه‌های آلودگی

شبکه‌گستر
امنیت‌ها | راهکارها

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده

است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat 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.



ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

گروه فروش

داخلی ۱ ۴۲۰۵۲ | sales@shabakeh.net

گروه پشتیبانی

داخلی ۲ ۴۲۰۵۲ | support@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