گزارشِ تحقیق درباره‌ی اسنادِ Vault 7

تهیه و تنظیم: مبین خیری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

در گزارشِ پیش‌رو قصد داریم با بررسیِ موشکافانه، به بخش‌های مختلفِ اسنادِ منتشرشده در وبسایتِ رسمیِ سازمانِ ویکی‌لیکس درباره‌ی سازمانِ سیا بپردازیم. این گزارش به کمکِ منابعِ پرشمارِ موجود در سطح اینترنت و نیز پایگاهِ اینترنتیِ بنیاد ویکی‌لیکس تهیه شده است.

Vault 7 مجموعه ای از اسنادی است که ویکی لیکس در 7 مارس 2017 شروع به انتشار کرد و جزئیات فعالیت‌ها و توانایی‌های آژانس اطلاعات مرکزی ایالات متحده برای انجام نظارت الکترونیکی و جنگ سایبری را نشان می دهد. این فایل‌ها، مربوط به سال‌های 2013 تا 2016، شامل جزئیاتی در مورد قابلیت‌های نرم‌افزار آژانس، مانند توانایی به خطر انداختن خودروها، تلویزیون‌های هوشمند، مرورگرهای وب (از جمله Google Chrome، Microsoft Edge، Mozilla Firefox و Opera) و سیستم‌عامل‌های اکثر گوشی‌های هوشمند (از جمله iOS اپل و اندروید گوگل) و همچنین سیستم‌عامل‌های دیگر مانند Microsoft Windows، macOS و Linux می‌شوند.

یک ممیزی داخلی سیا 91 ابزار بدافزار از بیش از 500 ابزار مورد استفاده در سال 2016 را شناسایی کرد که با انتشار آن در معرض خطر قرار گرفتند. این ابزارها توسط شعبه پشتیبانی عملیات C.I.A توسعه داده‌شده‌اند.

انتشار اسنادِ Vault 7 باعث شد تا سازمانِ سیا، ویکی لیکس را به عنوان یک «سرویس اطلاعاتی متخاصم غیر دولتی» تعریف کند.

تاریخچه

در ژانویه و فوریه 2017 وزارت دادگستری ایالات متحده برای مذاکره از طریق وکیل جولیان آسانژ برای فراهم کردنِ مصونیت و عبور ایمن آسانژ جهت خروج از سفارت اکوادور در لندن و سفر به ایالات متحده برای بحث در مورد به حداقل رساندن ریسک نسخه های بعدی ویکی لیکس از جمله ویرایشِ منابع و اعلامِ اینکه روسیه منبع نسخه های ویکی لیکس در سال 2016 نبود، تلاش می‌کرد. در اواسط فوریه 2017 والدمن که طرفدار بونو بود از سناتور مارک وارنر که رییس کمیته اطلاعات سنای ایالات متحده بود خواست که اگر سوالی دارد آن را از آسانژ بپرسد. وارنر با جیمز کومی مدیر اف بی ای تماس گرفت و به

والدمن گفت: "بایستید و مذاکرات را با آسانژ پایان دهید". با این حال دیوید لافمن که همتای والدمن با وزارت دادگستری بود پاسخ داد: "این یک مدرک است. با توجه به ری مک گاورن در 28 مارس 2017 والدمن و لوفمن بسیار نزدیک به یک توافق بین وزارت دادگستری و آسانژ برای" کاهش خطر مربوط به انتشار اسناد سیا در اختیار ویکی لیکس بودند. مانند اصلاح پرسنل سازمان در حوزه های قضایی خصمانه "در ازای" ایمنی قابل قبول و شرایط عبور امن. اما هرگز یک توافق رسمی حاصل نشد و در نهایت اطلاعاتِ بسیار مخربی در مورد" Marble Framework" توسط ویکی لیکس در 31 مارس 2017 منتشر شد.

طبق گزارش‌های رسانه‌ها، در فوریه 2017، ویکی‌لیکس انتشار «Vault 7» را با یک سری پیام‌های رمزآلود در توییتر شروع کرد. بعداً در فوریه، ویکی‌لیکس اسناد طبقه‌بندی‌شده‌ای را منتشر کرد که نحوه نظارت سیا بر انتخابات ریاست‌جمهوری فرانسه در سال 2012 را شرح می‌داد. در بیانیه مطبوعاتی این افشاگری آمده است که "به عنوان ضمیمه‌ای برای سریِ آتیِ سیا Vault 7" منتشر شده است.

در مارس 2017 مقامات اطلاعاتی و مجری قانون ایالات متحده به آژانس بین المللی سیمی رویترز گفتند که از اواخر سال 2016 از حفره‌ی امنیتی سیا که منجر به Vault 7 شد آگاه بودند. دو مقام گفتند که بر روی "پیمانکاران" به عنوان منبع احتمالیِ نشت تمرکز کرده‌اند.

در سال 2017 مجری قانون فدرال، جاشوا آدام شولت، مهندس نرم افزار سیا را به عنوان منبع مشکوک Vault 7 شناسایی کرد. در جولای 2022 شولت به افشای اسناد به ویکی لیکس محکوم شد.

در 13 آوریل 2017، مایک پمپئو، مدیر سیا ویکی لیکس را یک "سرویس اطلاعاتی متخاصم" اعلام کرد. در سپتامبر 2021 خبرگذاریِ یاهو گزارش داد که در سال 2017 در پی افشای Vault 7، سیا به ربودن یا ترور آسانژ، جاسوسی از همکاران ویکی لیکس، اختلاف افکنی بین اعضای آن و سرقت دستگاه های الکترونیکی آنها فکر کرد. پس از ماه‌ها بررسی، تمامی طرح‌های پیشنهادی به دلیل ترکیبی از ایرادات قانونی و اخلاقی لغو شد. بر اساس مقاله 2021 یاهو نیوز، یک مقام سابق امنیت ملی ترامپ اظهار داشت: "ما هرگز نباید از روی تمایل به انتقام وارد عمل شویم".

بخش 1 - "سال صفر"

اولین دسته از اسناد به نام "سال صفر" توسط ویکی لیکس در 7 مارس 2017 منتشر شد که شامل 7818 صفحه وب با 943 پیوست بود که ظاهراً از مرکز اطلاعات سایبری درز شده بود که حاوی صفحات بیشتری نسبت به پیمانکار و افشاگر سابقِ NSA، ادوارد اسنودن بود. ویکی لیکس اوایل همان هفته سال صفر را به صورت آنلاین در یک بایگانی قفل شده منتشر کرده بود و عبارت عبور را در روز هفتم فاش کرد. این عبارت به نقل قولی از رئیس جمهور کندی اشاره داشت که می‌خواست «سیا را هزار تکه کند و به بادها بپراکند».

ویکی لیکس نام منبع را ذکر نکرد اما گفت که این پرونده ها "به طور غیرمجاز در میان هکرها و پیمانکاران دولت سابق ایالات متحده دست به دست شده است که یکی از آنها بخش هایی از آرشیو را در اختیار ویکی لیکس قرار داده است." و اکنون مایل است که یک بحث عمومی در مورد امنیت، ایجاد، استفاده، تکثیر و کنترل دموکراتیک سلاح‌های سایبری را آغاز کند. زیرا این ابزارها سؤالاتی را مطرح می‌کنند که «به فوریت،

نیاز به بحث در انظار عمومی دارد. از جمله اینکه آیا توانایی‌های هک C.I.A از اختیارات اجباری آن فراتر رفته است یا خیر. مشکل نظارت عمومی بر آژانس.»

ویکی لیکس تلاش کرد تا اسامی و سایر اطلاعات شناسایی را از اسناد قبل از انتشار آنها حذف کند. اما به دلیل عدم ویرایش برخی جزئیات کلیدی با انتقاد مواجه شد. ویکی لیکس همچنین تلاش کرد تا امکان ایجاد ارتباط بین افراد را از طریق شناسه های منحصر به فردِ ایجادشده توسط ویکی لیکس فراهم کند. همچنین اعلام کرد که انتشار کد منبع سلاح‌های سایبری را که بنا بر گزارش‌ها چندین صد میلیون خط دارد، به تعویق می‌اندازد تا زمانی که در مورد ماهیت فنی و سیاسی برنامه C.I.A و نحوه استفاده از این سلاح‌ها اجماع حاصل شود. و در نهایت تجزیه و تحلیل، خلع سلاح و منتشر شد."جولیان آسانژ، بنیانگذار ویکی لیکس ادعا کرد که این تنها بخشی از یک مجموعه بزرگتر است.

سیا بیانیه ای منتشر کرد و گفت: "مردم آمریکا باید عمیقاً از هرگونه افشای ویکی لیکس که برای آسیب رساندن به توانایی جامعه اطلاعاتی برای محافظت از آمریکا در برابر تروریست ها یا سایر دشمنان طراحی شده‌است، ناراحت شوند. چنین افشاگری‌ای نه تنها پرسنل و عملیات ایالات متحده را به خطر می اندازد، بلکه دشمنان ما را نیز تجهیز می کند. با ابزار و اطلاعاتی که به ما آسیب خواهند رساند."

آسانژ در بیانیه‌ای در 19 مارس 2017 گفت که شرکت‌های فناوری‌ای که با آنها تماس گرفته شده است، با آنچه او به عنوان طرح استاندارد افشای صنعت ویکی‌لیکس می‌خواند موافقت نکرده‌اند، مخالفت نکرده‌اند، یا زیر سوال نبرده‌اند. زمان استاندارد افشای یک آسیب پذیری، 90 روز پس از ارائه جزئیات کامل نقص به شرکت مسئول وصله نرم افزار است. به گفته ویکی لیکس، تنها به موزیلا اطلاعاتی در مورد آسیب پذیری ها ارائه شده است. در حالی که «گوگل و برخی شرکت های دیگر» تنها دریافت اعلان اولیه را تایید کرده اند. ویکی لیکس اظهار داشت: "بیشتر این شرکت های عقب مانده به دلیل کار طبقه‌بندی شده خود با آژانس های دولتی ایالات متحده، تضاد منافع دارند. در عمل، چنین انجمن هایی کارکنان صنعت دارای مجوزهای امنیتی ایالات متحده را از رفع حفره ها بر اساس اطلاعات درز یافته از سیا محدود می کنند. چنین شرکت هایی باید تصمیم بگیرند کاربران خود را در برابر حملات سیا یا NSA ایمن کنند. کاربران ممکن است سازمان‌هایی مانند موزیلا یا شرکت‌های اروپایی را ترجیح دهند که کاربران خود را بر قراردادهای دولتی ترجیح دهند.

قسمت 2 - "ماده تاریک"

در 23 مارس 2017، ویکی لیکس دومین نسخه از مطالب Vault 7 را با عنوان "ماده تاریک" منتشر کرد. این نشریه شامل اسنادی برای چندین تلاش سیا برای هک کردن آیفون‌ها و مک‌های اپل بود. اینها شامل بدافزار «Sonic Screwdriver» می‌شد که می‌توانست از رابط صاعقه‌ای برای دور زدن حفاظت سیستم‌عامل رمز عبور اپل استفاده کند.

قسمت 3 - "مرمر"

در 31 مارس 2017، ویکی لیکس بخش سوم اسناد Vault 7 خود را با عنوان "مرمر" منتشر کرد. این منبع شامل 676 فایل کد منبع برای چارچوب مرمر سازمان سیا بود. از آن برای مبهم کردن یا درهم‌کوبی کد بدافزار استفاده می‌شود تا آن را به گونه‌ای بسازد که شرکت‌های ضد ویروس یا محققان نتوانند کد را درک کنند یا منبع آن را نسبت دهند. به گفته ویکی لیکس، این کد همچنین دارای یک de-obfuscator برای معکوس کردن اثرات مبهم سازی است.

قسمت 4 - "ملخ"

در 7 آوریل 2017، ویکی لیکس چهارمین مجموعه از اسناد Vault 7 خود را با نام "Grasshopper" منتشر کرد. این نشریه حاوی 27 سند از چارچوب Grasshopper CIA است که توسط CIA برای ایجاد بارهای بدافزار سفارشی شده و دائمی برای سیستم عامل های مایکروسافت ویندوز استفاده می شود. Grasshopper بر روی اجتناب از محصولات امنیتی شخصی (PSP) تمرکز کرد. PSP ها نرم افزارهای آنتی ویروس مانند MS Security Essentials، Symantec Endpoint یا Kaspersky IS هستند.

بخش 5 - "کندو"

در 14 آوریل 2017، ویکی لیکس قسمت پنجم اسناد Vault 7 خود را با عنوان "HIVE" منتشر کرد. بر اساس برنامه ویروس فوق سری سیا ایجاد شده توسط "شعبه توسعه جاسازی شده" (EDB). شش سند منتشر شده توسط ویکی لیکس مربوط به مجموعه بدافزار چند پلتفرمی سیا است. یک زیرساخت پشتیبان CIA با یک رابط HTTPS رو به عموم که توسط سیا برای انتقال اطلاعات از رایانه‌های رومیزی و گوشی‌های هوشمند مورد نظر به سیا و باز کردن آن دستگاه‌ها برای دریافت دستورات بیشتر از اپراتورهای سیا برای اجرای وظایف خاص استفاده می‌شود. در حالی که تمام اطلاعات را پنهان می‌کند. به کمکِ حضور در پشت دامنه های عمومی غیر مشکوک از طریق یک رابط پوشاننده به نام "Switchblade" (همچنین به عنوان Listening Post (LP) و Command and Control (C2) نیز شناخته می شود).

قسمت 6 - "فرشته گریان"

در 21 آوریل 2017، ویکی لیکس قسمت ششم مطالب Vault 7 خود را با نام رمز "فرشته گریان" منتشر کرد. ابزاری هک که توسط سیا و MI5 برای بهره برداری از یک سری تلویزیون های هوشمند به منظور جمع آوری اطلاعات مخفیانه استفاده می شود. . ابزار هک پس از نصب در تلویزیون‌های مناسب با یک USB، میکروفون‌های داخلی و احتمالاً دوربین‌های ویدیویی آن تلویزیون‌ها را قادر می‌سازد تا محیط اطراف خود را ضبط کنند. در حالی که به نظر می‌رسد تلویزیون‌ها به اشتباه خاموش هستند. سپس داده های ضبط شده یا به صورت محلی در حافظه تلویزیون ذخیره می شود یا از طریق اینترنت برای سیا ارسال می شود. گفته می شود که هر دو سازمان سیا و MI5 برای توسعه آن بدافزار همکاری کردند و کار خود را در کارگاه های توسعه مشترک هماهنگ کردند. از زمانِ انتشار این قسمت 6، "Weeping Angel" دومین ابزار مهم هک سیا است که به ویژه به برنامه تلویزیونی بریتانیا، Doctor Who، در کنار "Sonic Screwdriver" در "Dark Matter" اشاره می کند.

قسمت 7- "خط خطی"

در 28 آوریل 2017، ویکی لیکس قسمت هفتم مطالب Vault 7 خود را با نام "Scribbles" منتشر کرد. این نشت شامل اسناد و کد منبع ابزاری است که برای ردیابی اسناد فاش شده به افشاگران و روزنامه نگاران با جاسازی برچسب های وب بیکن در اسناد طبقه بندی شده برای ردیابی افرادی که آنها را فاش کرده اند، در نظر گرفته شده است. این ابزار بر اسناد مایکروسافت آفیس، به ویژه «Microsoft Office 2013 (در ویندوز 8.1 x64)، اسناد نسخه‌های آفیس 97-2016 (اسناد آفیس 95 کار نمی‌کنند) و اسنادی که قفل، رمزگذاری‌شده یا با رمز عبور محافظت نمی‌شوند، تأثیر می‌گذارد. هنگامی که یک سند واترمارک CIA باز می شود، یک تصویر نامرئی در سندی که در سرور آژانس میزبانی می شود بارگیری می‌شود و یک درخواست HTTP ایجاد می کند. سپس درخواست در سرور ثبت می شود و اطلاعاتی را در مورد اینکه چه کسی آن را باز می کند و کجا باز می شود به آژانس اطلاعاتی می دهد. با این حال، اگر یک سند واترمارک در یک پردازشگر کلمه جایگزین باز شود، ممکن است تصویر برای بیننده قابل مشاهده باشد. اسناد همچنین بیان می کنند که اگر سند به صورت آفلاین یا در نمای محافظت شده مشاهده شود، تصویر واترمارک شده نمی تواند با سرور اصلی خود تماس بگیرد. این فرآیند تنها زمانی لغو می شود که کاربر ویرایش را فعال کند.

قسمت 8- "ارشمیدس"

در 5 می 2017، ویکی لیکس هشتمین بخش از اسناد Vault 7 خود را با عنوان "ارشمیدس" منتشر کرد. به گفته جیک ویلیامز، مربی موسسه SANS ایالات متحده که اسناد منتشر شده را تجزیه و تحلیل کرد، ارشمیدس ویروسی است که قبلاً با نام رمز "Fulcrum" شناخته می شد. به گفته پیرلوئیجی پاگانینی، کارشناس امنیت سایبری و عضو ENISA، اپراتورهای سیا از Archimedes برای هدایت جلسات مرورگر وب شبکه محلی (LAN) از یک رایانه هدفمند از طریق رایانه ای که توسط CIA کنترل می شود، قبل از اینکه جلسات به کاربران هدایت شود، استفاده می کنند. این نوع حمله با نام Man-in-the-Middle (MitM) شناخته می شود. ویکی لیکس با انتشار خود تعدادی هش را شامل می شود که به ادعای آنها می توان از آنها برای شناسایی بالقوه ویروس ارشمیدس و محافظت در برابر آن در آینده استفاده کرد. پاگانینی اظهار داشت که رایانه‌های هدفمند بالقوه می‌توانند آن هش‌ها را در سیستم‌های خود جستجو کنند تا بررسی کنند که آیا سیستم‌های آنها توسط سیا مورد حمله قرار گرفته است یا خیر.

قسمت 9 - "قاتل" و "نیمه‌شب"

در 12 مه 2017، ویکی لیکس قسمت نهم از مطالب Vault 7 خود، "AfterMidnight" و "Assassin" را منتشر کرد. AfterMidnight یک بدافزار است که بر روی یک رایانه شخصی هدف نصب شده و به عنوان یک فایل DLL مبدل می شود که در هنگام راه اندازی مجدد رایانه کاربر اجرا می‌شود. سپس یک اتصال به رایانه فرماندهی و کنترل سیا (C2) را آغاز می کند که از آن ماژول‌های مختلف را برای اجرا دانلود می کند. در مورد Assassin، بسیار شبیه به همتای AfterMidnight خود است، اما به طور فریبنده ای در یک فرآیند سرویس ویندوز اجرا می شود. گزارش شده است که اپراتورهای سیا از Assassin به عنوان یک C2 برای اجرای یک سری وظایف، جمع‌آوری و سپس ارسال دوره‌ای داده‌های کاربر به پست (های) CIA Listening Post (LP) استفاده می‌کنند. مشابه رفتار تروجان درب پشتی. هر دو AfterMidnight و

Assassin که بر روی سیستم عامل ویندوز اجرا می شوند، دائمی هستند و به صورت دوره ای به LP پیکربندی شده خود نشان می دهند تا یا درخواست وظایف یا ارسال اطلاعات خصوصی به CIA، و همچنین به طور خودکار خود را در تاریخ و زمان تعیین شده حذف نصب کنند.

قسمت 10 - "آتنا"

ویکی لیکس در 19 مه 2017 دهمین بخش از اسناد Vault 7 خود را با عنوان "آتنا" منتشر کرد. راهنمای کاربر منتشر شده، نسخه ی نمایشی و اسناد مرتبط بین سپتامبر 2015 و فوریه 2016 ایجاد شده است. همه آنها در مورد بدافزاری هستند که ظاهراً برای سیا در آگوست 2015 توسعه یافته است، تقریباً یک ماه پس از انتشار ویندوز 10 مایکروسافت با اظهارات قاطع خود در مورد دشواری آن. هر دو بدافزار اولیه "Athena" و بدافزار ثانویه آن به نام "Hera" از نظر تئوری شبیه به بدافزار Grasshopper و AfterMidnight هستند، اما با برخی تفاوت‌های قابل توجه. یکی از این تفاوت ها این است که آتنا و هرا توسط سیا با یک شرکت خصوصی نیوهمپشایر به نام Siege Technologies توسعه داده شدند. طی مصاحبه بلومبرگ در سال 2014، بنیانگذار Siege Technologies توسعه چنین بدافزاری را تایید و توجیه کرد. بدافزار Athena به طور کامل سرویس های دسترسی از راه دور ویندوز را ربوده است، در حالی که Hera سرویس Dnscache ویندوز را ربوده است. هم آتنا و هم هرا بر تمام نسخه‌های فعلی ویندوز از جمله، اما نه محدود به، ویندوز سرور 2012 و ویندوز 10 تأثیر می‌گذارند. تفاوت دیگر در انواع رمزگذاری مورد استفاده بین رایانه‌های آلوده و پست‌های شنیداری سیا (LP) است. در مورد شباهت‌ها، آنها از فایل‌های DLL دائمی برای ایجاد یک درب پشتی برای برقراری ارتباط با LP CIA، سرقت داده‌های خصوصی، ارسال آن به سرورهای CIA یا حذف داده‌های خصوصی روی رایانه مورد نظر و همچنین Command and Control (C2) استفاده می‌کنند. ماموران سیا برای ارسال نرم افزارهای مخرب اضافی برای اجرای بیشتر وظایف خاص بر روی رایانه مورد حمله قرار می گیرند. همه موارد فوق برای فریب نرم افزارهای امنیتی رایانه طراحی شده اند. علاوه بر اسناد دقیق منتشر شده، ویکی لیکس هیچ مدرکی مبنی بر استفاده یا عدم استفاده سیا از آتنا ارائه نکرد.

بخش 11 - "همه گیری"

در 1 ژوئن 2017، ویکی لیکس قسمت 11 از مطالب Vault 7 خود را با عنوان "همه گیری" منتشر کرد. این ابزار به عنوان یک ایمپلنت دائمی عمل می کند که بر دستگاه های ویندوز با پوشه های مشترک تأثیر می گذارد. این برنامه به عنوان یک درایور فیلتر سیستم فایل روی یک رایانه آلوده عمل می‌کند و به ترافیک Block پیام سرور گوش می‌دهد در حالی که تلاش‌های دانلود را از رایانه‌های دیگر در یک شبکه محلی شناسایی می‌کند. "پاندمی" به درخواست دانلود از طرف رایانه آلوده پاسخ می دهد. با این حال، فایل قانونی را با بدافزار جایگزین می کند. به منظور مبهم کردن فعالیت‌های خود، "Pandemic" فقط فایل قانونی در حال انتقال را تغییر داده یا جایگزین می‌کند و فایل اصلی را بدون تغییر در سرور باقی می‌گذارد. ایمپلنت اجازه می دهد تا 20 فایل را در یک زمان تغییر دهید، با حداکثر اندازه فایل جداگانه 800 مگابایت. اگرچه در اسناد فاش شده ذکر نشده است، اما این امکان وجود دارد که رایانه های تازه آلوده شده خود به سرورهای فایل «پاندمی» تبدیل شوند و به ایمپلنت اجازه دهند به اهداف جدیدی در یک شبکه محلی برسد.

قسمت 12 - "شکوفه های گیلاس"

در 15 ژوئن 2017، ویکی لیکس قسمت 12 از مطالب Vault 7 خود را با عنوان "شکوفه های گیلاس" منتشر کرد. Cherry Blossom از یک سرور فرمان و کنترل به نام Cherry Tree و سیستم عامل روتر سفارشی به نام FlyTrap برای نظارت بر فعالیت های اینترنتی اهداف، اسکن "آدرس های ایمیل، نام های کاربری چت، آدرس های MAC و شماره های VoIP" و تغییر مسیر ترافیک استفاده کرد.

قسمت 13 - "کانگوروی بی‌رحم"

در 22 ژوئن 2017، ویکی لیکس بخش 13 از مطالب Vault 7 خود، کتابچه راهنمای "کانگوروی بی رحم" را منتشر کرد. Brutal Kangaroo پروژه ای متمرکز بر بدافزار سیا بود که برای به خطر انداختن شبکه های کامپیوتری دارای شکاف هوا با درایوهای USB آلوده طراحی شده بود. Brutal Kangaroo شامل ابزار Drifting Deadline، ابزار اصلی، Shattered Assurance، سروری که عفونت درایو انگشت شست را خودکار می کند، Shadow، ابزاری برای هماهنگ کردن ماشین‌های در معرض خطر، و Broken Promise، ابزاری برای استخراج داده‌ها از شبکه‌های دارای شکاف هوا بود.

قسمت 14 - "السا"

در 28 ژوئن 2017، ویکی لیکس بخش 14 از مطالب Vault 7 خود، کتابچه راهنمای پروژه را با عنوان "السا" منتشر کرد. السا ابزاری بود که برای ردیابی دستگاه‌های ویندوز در شبکه‌های WiFi مجاور استفاده می‌شد.

قسمت 15 - "کشور غیرقانونی"

در 29 ژوئن 2017، ویکی لیکس بخش 15 از مطالب Vault 7 خود را منتشر کرد. کتابچه راهنمای پروژه با عنوان "کشور غیرقانونی" که یک ماژول هسته برای لینوکس 2.6 بود که به مأموران سیا اجازه می داد از سرورهای لینوکس جاسوسی کنند و ترافیک خروجی را از یک رایانه لینوکس به یک سایت انتخابی هدایت کنند.

قسمت 16 - "بوتان‌افزار"

در 6 ژوئیه 2017، ویکی لیکس بخش 16 از مطالب Vault 7 خود، کتابچه راهنمای پروژه با عنوان "BothanSpy" را منتشر کرد. BothanSpy یک ابزار هک CIA بود که برای سرقت اطلاعات کاربری SSH از رایانه‌های ویندوز ساخته شده بود.

قسمت 17- "بلند مرتبه"

در 13 ژوئیه 2017، ویکی لیکس بخش 17 از مطالب Vault 7 خود را منتشر کرد. کتابچه راهنمای پروژه با عنوان "Highrise". ابزار هک Highrise که با نام Tidecheck نیز شناخته می‌شود، برای رهگیری و هدایت پیام‌های SMS به گوشی‌های اندرویدی با استفاده از نسخه‌های 4.0 تا 4.3 استفاده می‌شود. Highrise همچنین می تواند به عنوان یک کانال ارتباطی رمزگذاری شده بین ماموران و ناظران سیا استفاده شود.

قسمت 18 - "UCL / Raytheon"

در 19 ژوئیه 2017، ویکی لیکس قسمت 18 از مطالب Vault 7، UCL / Raytheon را منتشر کرد.

قسمت 19 - "امپراتوری"

در 27 ژوئیه 2017، ویکی لیکس بخش 19 از مطالب Vault 7 خود، کتابچه راهنمای پروژه را با عنوان "امپریال" منتشر کرد. امپریال شامل سه ابزار به نام‌های آشیل، ایریس و نخود دریایی بود. آشیل ابزاری برای تبدیل فایل‌های نصب MacOS DMG به بدافزار تروجان بود. Aeris یک بدافزار برای سیستم‌های POSIX بود و SeaPea یک rootkit OS X بود.

قسمت 20 - "دامبو"

در 3 آگوست 2017، ویکی لیکس بخش 20 از مطالب Vault 7 خود، کتابچه راهنمای پروژه را با عنوان "Dumbo" منتشر کرد. Dumbo ابزاری بود که آژانس برای غیرفعال کردن وب‌کم‌ها، میکروفون‌ها و سایر ابزارهای نظارتی از طریق WiFi و بلوتوث استفاده می‌کرد تا به ماموران میدانی اجازه دهد تا مأموریت‌های خود را انجام دهند.

قسمت 21 - "CouchPotato"

در 10 آگوست 2017، ویکی لیکس بخش 21 از مطالب Vault 7 خود، کتابچه راهنمای پروژه CouchPotato را منتشر کرد. CouchPotato ابزاری برای رهگیری و ذخیره جریان‌های ویدیویی از راه دور بود که به سیا اجازه می‌داد از سیستم‌های نظارتی افراد دیگر استفاده کند.

قسمت 22 - "ExpressLane"

در 24 آگوست 2017، ویکی لیکس قسمت 22 از مطالب Vault 7 خود را از پروژه "ExpressLane" سیا منتشر کرد. این اسناد یکی از عملیات‌های سایبری را که سیا علیه سایر سرویس‌هایی که با آنها در ارتباط است، از جمله آژانس امنیت ملی (NSA)، وزارت امنیت داخلی (DHS) و اداره تحقیقات فدرال (FBI) انجام می‌دهد.

ExpressLane، یک ابزار مخفی جمع آوری اطلاعات، توسط سیا برای نفوذ در سیستم های جمع آوری داده های بیومتریک خدماتی که با آنها در ارتباط است استفاده شد. ExpressLane تحت پوشش ارتقاء

نرم افزار بیومتریک خدمات رابط توسط ماموران دفتر خدمات فنی (OTS) CIA بدون اطلاع آنها نصب و اجرا شد.

قسمت 23 - "آتش فرشته"

در 31 اوت 2017، ویکی لیکس بخش 23 از اسناد Vault 7، کتابچه راهنمای پروژه Angelfire را منتشر کرد. Angelfire یک چارچوب بدافزار بود که برای آلوده کردن رایانه‌های دارای ویندوز XP و Windows 7 ساخته شده بود که از پنج بخش ساخته شده بود. Solartime بدافزاری بود که بخش بوت را برای بارگیری Wolfcreek تغییر داد، که درایور خود بارگیری بود که درایورهای دیگر را بارگیری می کرد. Keystone مسئول بارگیری بدافزارهای دیگر بود. BadMFS یک فایل سیستم مخفی بود که بدافزار را پنهان می کرد و Windows Transitory File System جایگزین جدیدتری برای BadMFS بود. این کتابچه راهنمای شامل فهرست طولانی از مشکلات ابزارها بود.

قسمت 24 - "پروتگو"

Protego، قسمت 24 از اسناد Vault 7، در 7 سپتامبر 2017 منتشر شد.

پایان.