بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش باج‌افزار Cactus

باج‌افزار

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۴۰۲/۰۲/۲۱

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر - پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴

(۰۲۱) ۸۸۱۱۵۷۲۴

cert.ir

فهرست مطالب

۱ شرح باج‌افزار

یک عملیات باج‌افزار جدید به نام کاکتوس (Cactus) از آسیب‌پذیری‌های موجود در دستگاه‌ها و تجهیزات VPNبرای دسترسی اولیه به شبکه‌های «موسسات تجاری بزرگ» سواستفاده می‌کند. این عملیات رمزگذاری Cactus از حداقل ماه مارس فعالیت خود را شروع کرده و در تلاش است تا از قربانیان خود پرداخت بزرگی بگیرد. درحالی‌که عامل تهدید جدید تاکتیک‌های معمولی را که در حملات باج‌افزار دیده می‌شود (مانند رمزگذاری فایل و سرقت داده)، به‌کار می‌گیرد، برای جلوگیری از شناسایی، ویژگی خاص خود را نیز به لیست توانایی‌های خود اضافه کرده است.

محققان در شرکت تحقیقاتی و مشاوره ریسک سازمان Kroll معتقدند که باج‌افزار کاکتوس با بهره‌برداری از آسیب‌پذیری‌های شناخته شده در دستگاه‌های VPN شرکت Fortinet، دسترسی اولیه به شبکه قربانی را به‌دست می‌آورد. این ارزیابی بر اساس مشاهداتی است که در تمام حوادث مورد بررسی قرار گرفته است که هکر از یک سرور VPN با یک حساب سرویس VPN به داخل نفوذ کرده است.

نکته مهمی که باج‌افزار کاکتوس را از سایر عملیات‌ها متمایز می‌کند، استفاده از رمزگذاری برای محافظت از باینری باج افزار است. مهاجم از یک اسکریپت بَچ برای به‌دست آوردن رمزگذار باینری با استفاده از ۷-Zip استفاده می‌کند. فایل آرشیو ZIP اصلی حذف می‌شود و باینری با یک فلگ خاص مستقر می‌شود که به آن اجازه اجرا می‌دهد. کل فرآیند غیرعادی است و محققان معتقدند که این کار را برای جلوگیری از شناسایی رمزگذار باج‌افزار انجام می‌دهند.

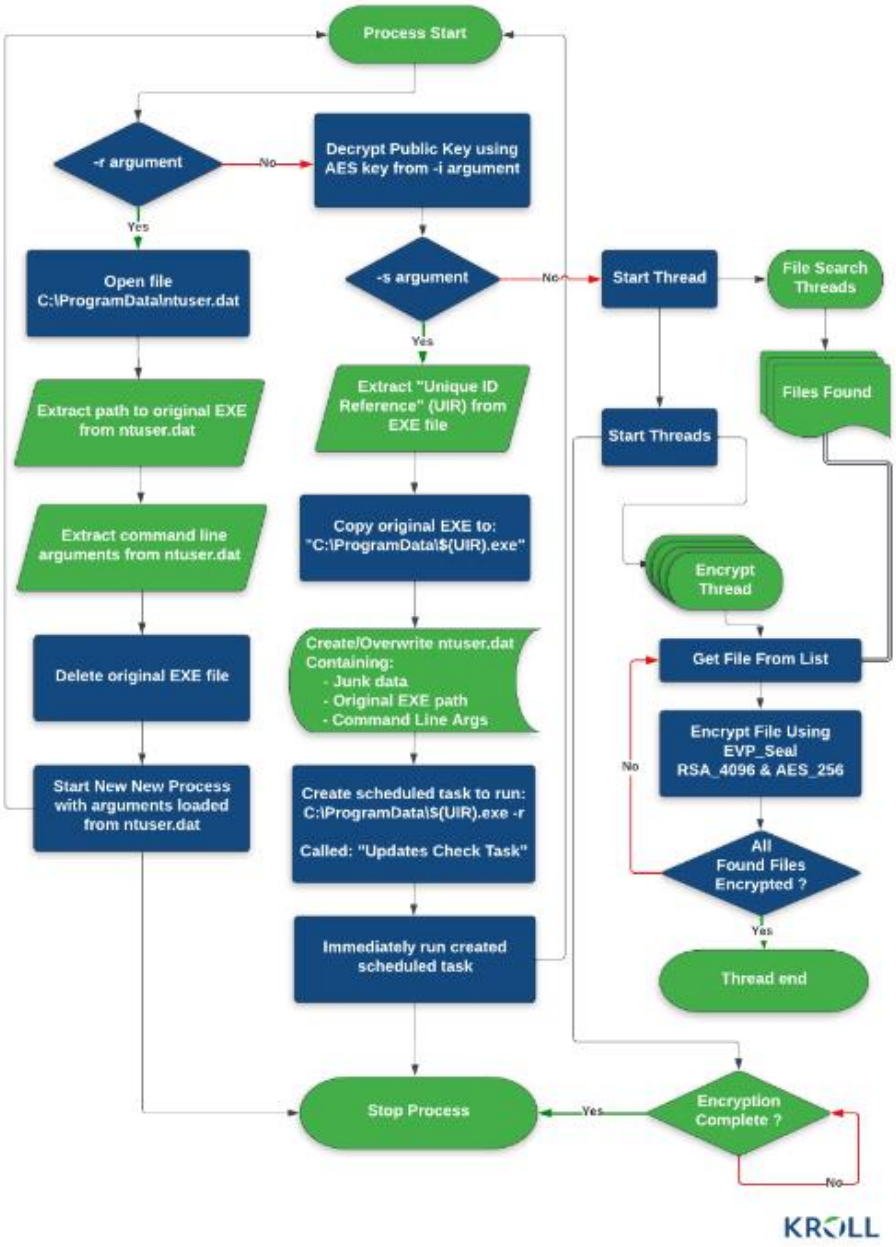
در یک گزارش فنی، محققان کرول توضیح داده‌اند که سه حالت اصلی اجرا وجود دارد که هرکدام با استفاده از یک سوئیچ خط دستور خاص انتخاب شده‌ان. این سوئیچ ها شامل : راه‌اندازی (-s)، پیکربندی خواندن (-r)، و رمزگذاری (-i) است. آرگومان‌های -s و -r به عاملان تهدید اجازه می‌دهند که پایداری را تنظیم کنند و داده‌ها را در یک فایل C:\ProgramData\ntuser.dat ذخیره کنند که بعدا هنگام اجرا با آرگومان کامندلاین -r توسط رمزگذار خوانده می‌شود.

برای اینکه رمزگذاری فایل ممکن باشد، یک کلید AES منحصربه‌فرد که فقط برای مهاجمان شناخته شده است باید با استفاده از آرگومان کامندلاین -i ارائه شود. این کلید برای رمزگشایی فایل پیکربندی باج افزار و کلید عمومی RSA مورد نیاز برای رمزگذاری فایل‌ها ضروری است. این به‌عنوان یک استرینگ HEX که به‌شدت کدگذاری شده، در باینری رمزگذار موجود است.

```
bash> strings -td -n1628 cactus.exe
4227632 d3d3d5aa22a2e5a2d8c8b9267360a7752c41f1e00827fcc31ff64aaf166e10908a04afe904c39a7
```

شکل ۱رمزنگاری شده پیکربندی Cactus ransomware

رمزگشایی استرینگ HEX قسمتی از داده‌های رمزگذاری شده را فراهم می‌کند که با کلید AES باز می‌شود. لوری یاکونو، معاون مدیر عامل ریسک سایبری در Kroll، گفت: «CACTUS اساسا خودش را رمزگذاری می‌کند و این امر، تشخیص آن را سخت‌تر می‌کند و به آن کمک می‌کند تا از سد آنتی‌ویروس‌ها و ابزارهای نظارت شبکه فرار کند». اجرای باینری با کلید صحیح برای پارامتر i- (رمزگذاری) قفل اطلاعات را باز می‌کند و به بدافزار اجازه می‌دهد تا فایل‌ها را جستجو کند و یک فرآیند رمزگذاری چند رشته‌ای را شروع کند. محققان کرول نمودار زیر را برای توضیح بهتر فرآیند اجرای باینری کاکتوس مطابق با پارامتر انتخاب شده ارائه کرده‌اند.



شکل ۲: فرآیند اجرای باینری کاکتوس

مایکل گیلسپی، کارشناس باج‌افزار، همچنین نحوه رمزگذاری داده‌های کاکتوس را تجزیه‌وتحلیل کرد و گفت که این بدافزار از پسوندهای متعددی برای فایل‌هایی که هدف قرار می‌دهد و بسته به وضعیت پردازش، استفاده می‌کند.

هنگام آماده‌سازی فایل برای رمزگذاری، کاکتوس پسوند آن را به .CTS0 تغییر می‌دهد. پس از رمزگذاری، پسوند .CTS1 می‌شود. بااین‌حال، گیلسپی توضیح داد که کاکتوس همچنین می‌تواند یک *حالت سریع* داشته باشد که شبیه به یک رمزگذاری سبک است. اجرای بدافزار در حالت سریع و عادی به طور متوالی منجر به رمزگذاری دو مرتبه‌ای یک فایل و افزودن پسوند جدید پس از هر فرآیند می‌شود (به عنوان مثال.CTS1. CTS8). کرول مشاهده کرد که تعداد در انتهای پسوند. CTS در چندین رویداد منتسب به باج افزار کاکتوس متفاوت است.

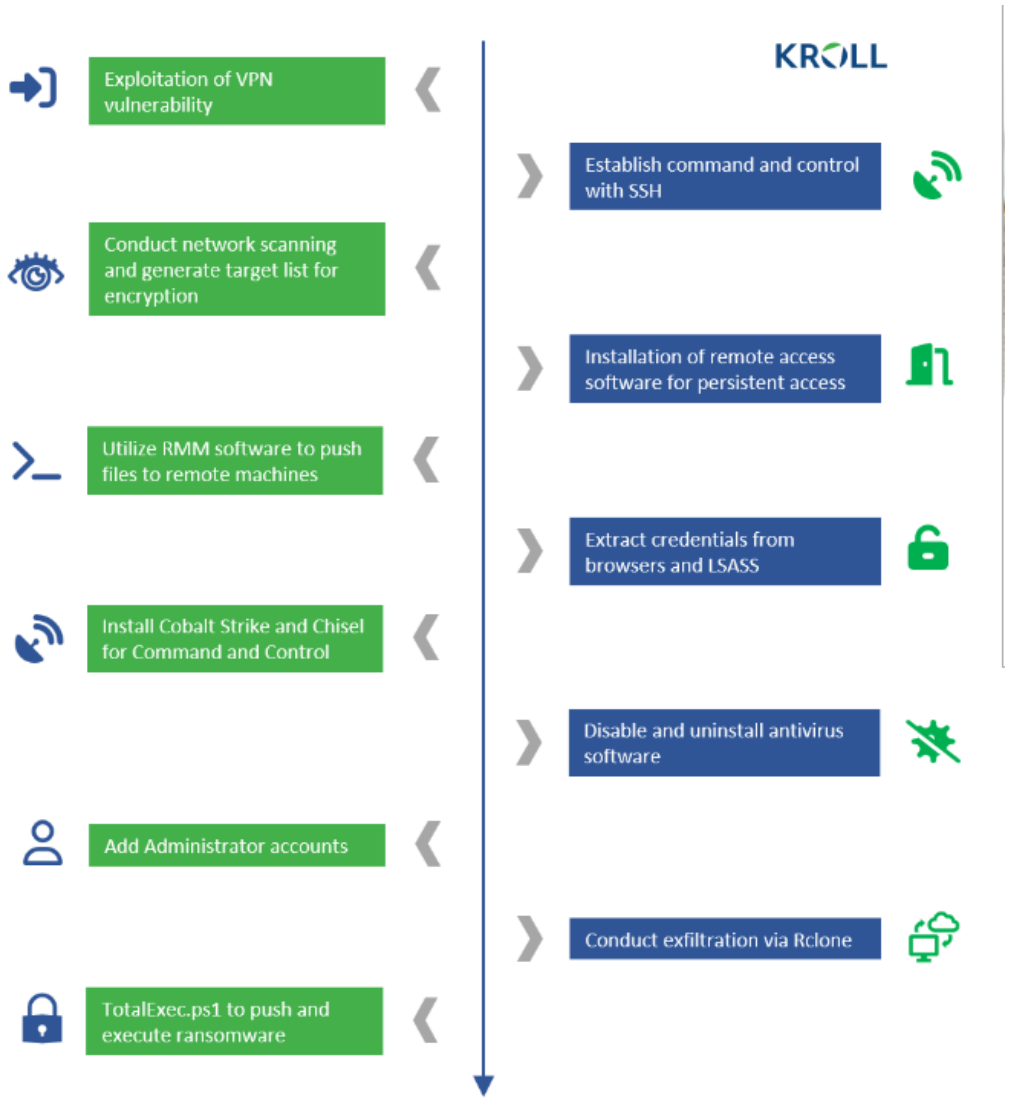
باج افزار کاکتوس و روش ها و فرایندها (TTP)

هنگامی که عامل تهدید وارد شبکه شد، از یک task برنامه‌ریزی شده برای دسترسی مداوم با استفاده از SSH Backdoor قابل دسترسی از سرور C2) command-and-control) استفاده کرد. به گفته محققان Kroll، باج افزار کاکتوس برای جستجوی اهداف جالب در شبکه به SoftPerfect Network Scanner (netscan) اتکا کرده است.

برای شناسایی عمیق‌تر و دقیق‌تر، مهاجم از دستورات PowerShell برای شمارش اندپوینت، شناسایی حساب‌های کاربری با مشاهده لاگین‌های موفق در Windows Event Viewer و پینگ کردن هاست‌های راه دور استفاده کرد. محققان همچنین دریافتند که باج‌افزار کاکتوس از یک نوع تغییر یافته از ابزار متن باز PSnmap استفاده می‌کند که معادل PowerShell اسکنر شبکه nmap است.

برای راه اندازی ابزارهای مختلف مورد نیاز برای حمله، محققان می‌گویند که باج افزار Cactus چندین روش دسترسی از راه دور را از طریق ابزارهای قانونی (مانند Splashtop، AnyDesk، SuperOps RMM) همراه با Cobalt Strike و ابزار پروکسی مبتنی بر Go (Chisel) امتحان می‌کند.

محققان کرول می‌گویند که پس از افزایش اختیارات روی یک دستگاه، اپراتورهای کاکتوس یک اسکریپت بَچ را اجرا می‌کنند که رایج‌ترین محصولات آنتی ویروس مورد استفاده را حذف نصب می‌کند. مانند اکثر عملیات‌های باج افزار، کاکتوس نیز داده‌ها را از قربانی سرقت می‌کند. برای این فرآیند، عامل تهدید از ابزار Rclone برای انتقال مستقیم فایل‌ها به فضای ذخیره‌سازی ابری استفاده می‌کند. پس از استخراج داده‌ها، هکرها از یک اسکریپت PowerShell به نام TotalExec که اغلب در حملات باج‌افزار BlackBasta دیده می‌شود، برای خودکارسازی فرآیند رمزگذاری استفاده کردند. گیلسپی افزود که روال رمزگذاری در حملات باج‌افزار کاکتوس منحصربه‌فرد است. با وجود این، به نظر نمی‌رسد که این‌روش مختص Cactus باشد، زیرا اخیرا گروه باج‌افزار BlackBasta نیز فرآیند رمزگذاری مشابهی را اتخاذ کرده است.



شکل ۳ تکنیک‌ها، تاکتیک‌ها و فرایندهای باج افزار کاکتوس

در حال حاضر هیچ اطلاعات عمومی در مورد باج‌هایی که کاکتوس از قربانیان خود می‌خواهد وجود ندارد، اما برخی منابع گفته‌اند که آنها میلیون‌ها دلار درخواست باج نموده‌اند. با این‌حال، عامل تهدید قربانیان را به انتشار فایل‌های دزدیده شده تهدید می‌کند مگر اینکه پولی به‌عنوان باج دریافت کنند. این مسئله به صراحت در یادداشت درخواست باج آمده است :

cAcTuS.readme.txt

```
Your systems were accessed and encrypted by Cactus.
To recover your files and prevent data disclosure contact us via email: cactus@mexicomail.com
Your unique ID reference: <redacted>
Backup contact: TOX (https://tox.chat/):
<redacted>
```

جزئیات گسترده‌ای در مورد عملیات کاکتوس، و اینکه قربانیانی که آنها را هدف قرار می‌دهند و اگر هکرها به قول خود عمل کنند و در صورت پرداخت، یک رمزگشای مطمئن ارائه کنند، در حال حاضر در دسترس نیست. استفاده از آخرین بروزرسانی‌های نرم‌افزاری از سوی تامین‌کنندگان تجهیزات، نظارت بر شبکه برای مواردی چون استخراج داده‌های بزرگ و پاسخ سریع به حملات، میتواند از آخرین و مخرب‌ترین مراحل حملات باج‌افزاری، محافظت کند.

۲ مراجع

https://www.bleepingcomputer.com/news/security/new-cactus-ransomware-encrypts-itself-to-evade-antivirus/

https://be.hardware.info/nieuws/85053/cactus-ransomware-ontwijkt-antivirus-door-zichzelf-te-versleutelen