فهرست

عنوان	صفحه
1- ابزار شبیه سازی حمله APT	2
2- بالابردن سطح دسترسی	2
3- پنهان مانده- فرار از دفاع امنیتی	2
4- ایجاد دسترسی به شبکه پایدار	3
5- ارتباط فرمان و کنترل	3
6- کشف اهداف جدید در شبکه محلی	4
7- منابع	

APT به حملات تحت شبکه اطلاق می شود که یک شخص یا سازمان احراز هویت نشده می تواند برای مدت زمان زیادی به صورت ناشناس به شبکه دسترسی پیدا کند

اغلب هدف این گونه حملات معمولا سازمان هایی است که اطلاعات مفیدی در اختیار دارند و مانند سازمان دفاع، صنایع تولیدی و مالی، زیرساخت ها و.... در یک حمله، نفوذگر تلاش می کند تا با سرعت وارد شود، اطلاعات را سرقت و از شبکه خارج شود تا سیستم های تشخیص نفوذ شانس کمتری برای یافتن این گونه حمله ها داشته باشند. هر چند در این حملات هدف ورود و خروج سریع نیست و معمولا این گونه حملات، پایدار Persistent هستند. بدین منظور حمله کننده باید دائما کد های فایل مخرب را بازنویسی نماید و تکنیک های پنهان سازی پیچیده ای استفاده کند، به همین دلیل به آن ها پیشرفته گفته می شود.

سازمان هایی که ممکن است توسط گروه های APT مورد هدف قرار گیرند، باید به طور منظم سیستم ها را مورد بررسی و نظارت قرار دهند تا خطر این حملات کاهش یابد.

حملاتAPT هنگامی اتفاق می افتد که برخی از سازمان ها تصمیم بگیرند که شما به طور خاص چیزی را که می خواهید داشته باشید و آن ها مایل به جذب منابع و زمان برای دستیابی به آن ها هستند. ماهیت سازمان یافته گروه های APT چیزی است که باعث پیشرفت آن ها می شود. عملیات آن ها با یک برنامه شروع می شود. اهداف تعریف شده و مجموعه ای از رویه های خوب تکرار شده و هماهنگ به مرحله اجرا در می آیند. این عملیات هدفمند را می توان در یک سری مراحل جدا کرد . فازهایی از قبیل آماده سازی و بدست آوردن نقطه ورود اولیه از پیش شرط های لازم است.

چرخه عمر حملات

1. ابزار شبیه سازی حمله APT

شبیه سازی حملات APT یک روش مفید برای ارزیابی راه حل های امنیتی می باشد. شبیه سازی حمله APT می تواند به شبکه شما، قابلیت های شناسایی خطرات و نظارت بر امنیت را متصور سازد. چند ابزار خودکار وجود دارد که می توانند برای شبیه سازی این حملات استفاده شوند:

APT Simulator – یک اسکریپت Batch Windows است که مجموعه ابزارها و فایل های خروجی استفاده می کند تا به یک سیستم نفوذ کند.

CALDERA – سیستم تقلید خودکار دشمن.

Infection monkey – یک ابزار تست نفوذ خودکار.

Flighsim – ابزاری برای تولید ترافیک شبکه مخرب و ارزیابی کنترل ها

2. بالابردن سطح دسترسی:

هنگامی که مهاجمان سایبری به ماشین هدف دسترسی پیدا می کنند، یکی از اولین کارهایی که انجام می دهند بالابردن سطح دسترسی است. چند تکنیک برای انجام این کار وجود دارد.

حافظه پردازش LSASS را به یک پوشه انتقال دهید.

Mimikatz-Invoke را در حافظه اجرا کنید.

خروجی mimikatz را بردارید و پسوردهای مهم را بیرون بکشید.

3. پنهان ماندن – فرار از دفاعی امنیتی:

گروه های تهدید به طور مداوم تکنیک های خودرا برای جلوگیری از دفاع امنیتی سازگار می کنند. برخی از تاکتیک های آنها که در گذشته بسیار موفق بوده اند عبارتند از:

یک حساب مهمان سرپرست (Guest admin) فعال کنید.

یک فایل مشکوک با نام پرونده سیستم مانند Exe.svchost را در پوشه %PUBLIC% انتقال دهید.

اضافه کردن بدافزار در قالب یک فایل در سیستم میزبان.

کد جاوا اسکریپت مبهم را با exe.wscript اجرا کنید و یک پوشته اتصال رمزگشایی شده را شروع کنید.

یک فایل RAR پنهان با محتوای مخرب را بارگیری کنید.

4. ایجاد دسترسی به شبکه پایدار:

بعد از اینکه یک حمله اولیه صورت گرفت و مهاجمان سطح دسترسی خود را بالا بردند، آن ها تلاش خواهند کرد تا خود را در شبکه هدف Persist کنند که این امر سبب می شود دسترسی آن ها به شبکه دائمی شود. روش های مختلف زیادی برای دستیابی به این پایداری وجود دارد، برخی از آن ها عبارتند از:

یک Task برنامه ریزی شده ایجاد کنید که Mimikatz را اجرا کند و خروجی را به یک File منتقل کند.
با استفاده از ps.SchtasksBackdoor-Invoke 1 یک task برنامه ریزی شده از طریق فایل XML ایجاد کنید.
سوء استفاده از جایگزین کردن کلید های چسبنده با exe.cmd exe.sethc
یک پوسته وب مبهم در دایرکتوری ریشه وب استفاده ایجاد کنید.
استفاده از WMIBackdoor برای از بین بردن نمونه های کاوشگر محلی هنگام شروع کار.

5. ارتباطات فرمان و کنترل:

گروه های APT از نوعی زیرساخت برای ارتباط و دسترسی به شبکه هدفمند استفاده می کنند. برخی از تکنیک ها برای بازآفرینی این فعالیت عبارتند از:
یک پوسته Ncat powerShell را روی دایرکتوری کار بگذارید و آن را به یک دامنه مهاجم مشهور متصل کنید.
چندین آدرس شناخته شده c 2 را جستجو کنید تا باعث ایجاد درخواست DNS شود و آدرس ها را در حافظه محلی DNS محلی دریافت کند.
از WMIBackdoor برای تماس با C 2 در فواصل زمانی استفاده می کند.
برای دسترسی به سرورهای معروف C 2 از Curl استفاده می کند.

6. کشف اهداف جدید در شبکه محلی:

سرانجام، هنگامی که گروه های APT به یک دستگاه نفوذ کردند، سطح دسترسی را بالا می برند و دسترسی خود را persist می کنند آن ها به دنبال دستگاه بعدی خود می روند تا در شبکه هدف ماندگار شوند. برخی نشانه های این کشف جدید عبارتند از:
زیر شبکه های آدرس IP کلاس C را با استفاده از nbtscan اسکن کرده و خروجی را به فهرست شاخه کار اضافه کنید.
دستوراتی را که توسط مهاجمان برای به دست آوردن اطلاعات در مورد یک سیستم هدف استفاده می شود، اجرا کنید.
شرکت Nextron یکی از شرکت های بزرگ ارائه دهنده Simulation APT است. از اسکریپت Batch Windows که مجموعه ای از ابزارها می باشد استفاده می کند تا به یک سیستم نفوذ کند.
ریشه های Nextron به سال 2012 بر میگردد که اسکنر THIOR توسط GmbH Consulting BSK و AG Consulting HvS ساخته شده است. در آوریل سال 2017، هر دو شرکت تصمیم گرفتند تا توسعه THOR

را به همراه توسعه نرم افزاری برای کنترل اسکن مرکزی، اصلاح و آنالیز در یک شرکت مشترک با نام GmbH Systems Nextron متمرکز کنند.

مشخصات تکمیلی این شرکت نیز به شرح ذیل است:

https//:www.Com.systems-nextron

Adress : Germany Dietzenbach 631288 Bruchstrasse

Email : Com.systems-info@nextron

Phone: +49 6074 – 728 42 36

Fax: +49 03212 – 147 84 25

پیشنهاد: این گزارش از این جهت می تواند برای گروه های آفندی حائز اهمیت باشد که طبق شبیه سازی روش های مرسوم Attack (مثل استفاده از Mimikatz, PsExec , WMI و...) توسط بخش SOC سازمان ها و یا نهاد های هدف، که قصد نفوذ به آن ها می باشد با مخاتراتی همراه خواهد بود، زیرا اکثر آنتی ویروس و EDRهایی که در شبکه هدف هستند، آن ها را ارزیابی و آنالیز می کنند. پس ممکن است حمله به یکی از این APTها چسبانده و گزارش شود. این باعث می شود که هدف هوشیار شده و نفوذ به آن خیلی سخت تر شود. این مرکز پیشنهاد می کند با تحقیق و توسعه روی APTها و روش کار آن ها، از تکرار روش های مرسوم مندرج در گزارشات خوداری گردد.

7. منابع

https://www.nextrom-systems.com

https://github.com/nextronSystems/APTSimulator

https://www.redflare-security.com

والسلام