Eviction

Andres Valdivieso Pinilla - Líder de Ciberseguridad (Consultor)
www.linkedin.com/in/andres-valdivieso-pinilla

Introducción

Trata de una posible amenaza por parte del grupo APT28. Este actor de amenazas, conocido por sus sofisticadas campañas de ciber espionaje.

Como analista de SOC, la tarea consiste en utilizar el MITRE ATT&CK Navigator para identificar las tácticas, técnicas y procedimientos (TTPs) empleados por APT28, evaluar si la red ha sido comprometida. Este writeup documenta el proceso de análisis, correlación basado en inteligencia de amenazas

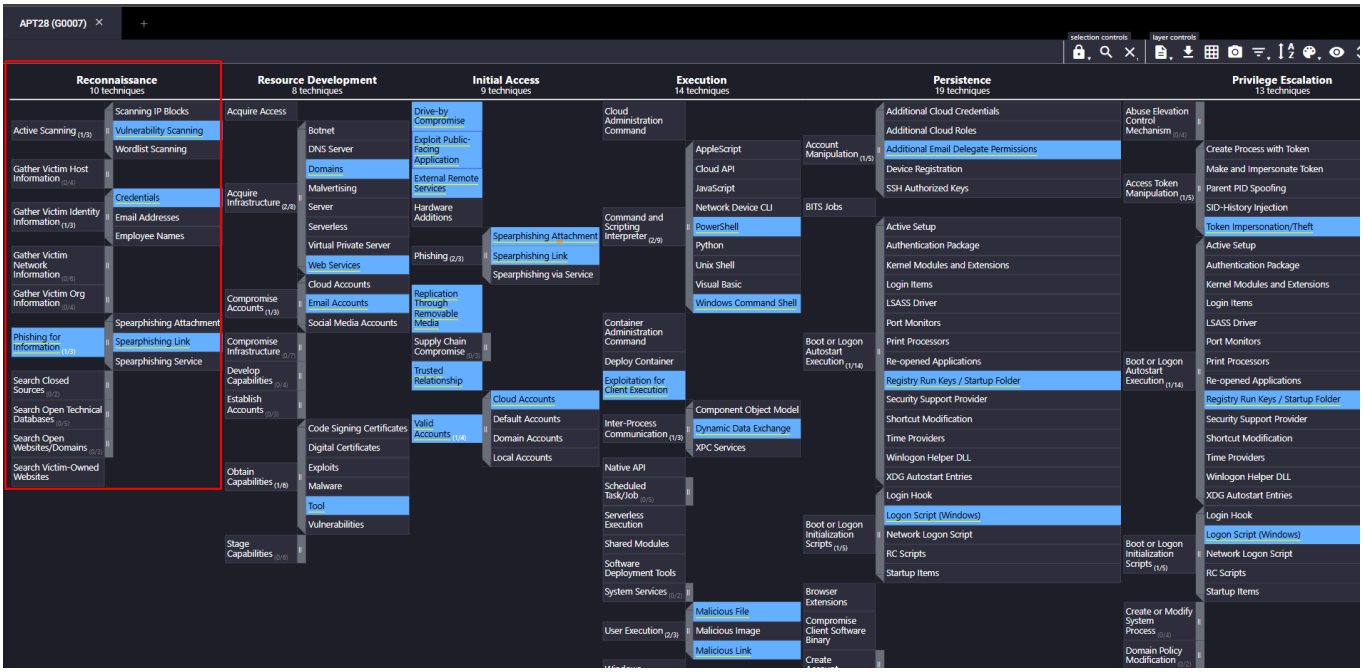
Entender al adversario

Sunny es analista de SOC en E-corp, que fabrica tierras raras para clientes gubernamentales y no gubernamentales. Recibe un informe de inteligencia clasificado que le informa que un grupo APT (APT28) podría estar intentando atacar a organizaciones similares a E-corp. Para actuar en función de esta información, debe utilizar el navegador MITRE ATT&CK para identificar las tácticas, técnicas y procedimientos utilizados por el grupo APT , asegurarse de que no se haya introducido ya en la red y detenerlo si lo ha hecho.

lo primero que debemos realizar es abrir el enlace este enlace para consultar la capa MITRE ATT&CK Navigator para el grupo APT y responder las preguntas a continuación.

Nos preguntan que si podemos saber cual es la técnica que utiliza la APT para realizar el reconocimiento y obtener acceso inicial?

Dentro de la vista inicial de navegación vemos las etapas, lo que nos preguntan esta asociado a la etapa de reconocimiento:

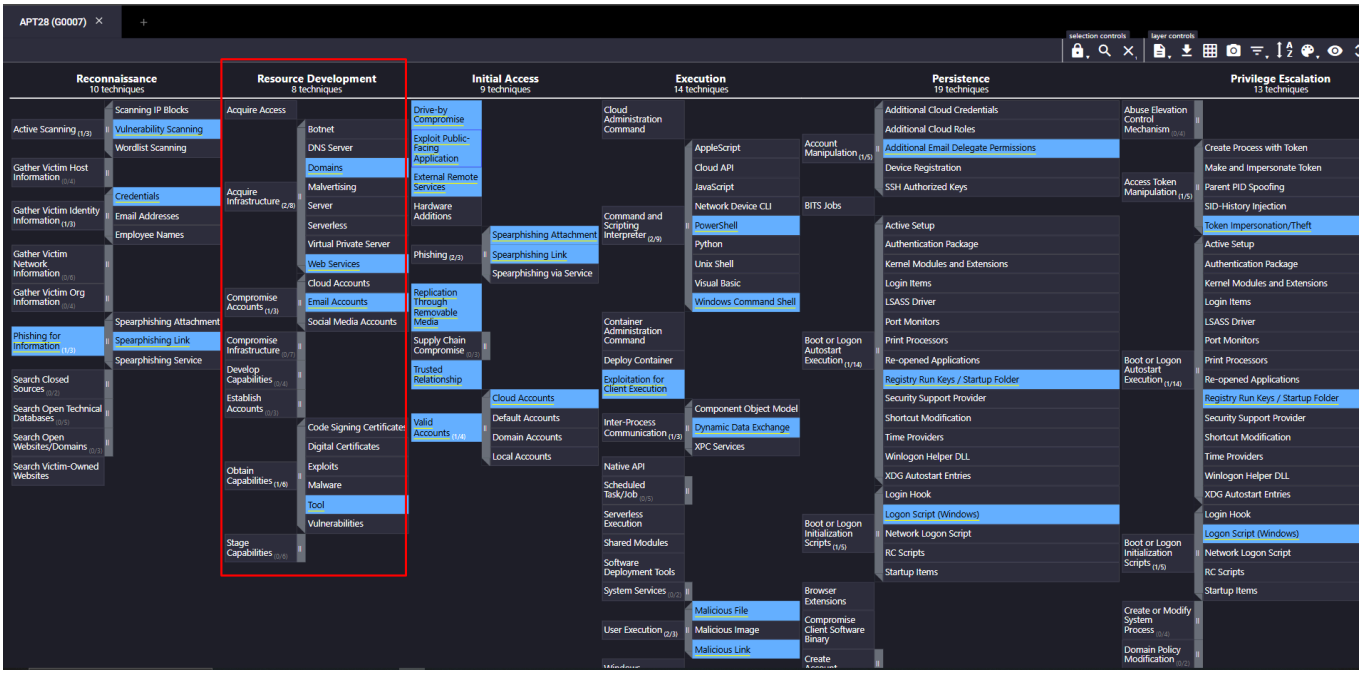


Podemos observar que ingresa por medio de phishing y que tiene asociado el Vunerability Scanning, Credencials y Spearphishing Link.

Al validar informacion sobre el *Spearphishing Link* vemos que el este es un método donde los adversarios pueden enviar mensajes de phishing selectivo a través de servicios de terceros para obtener información confidencial. El phishing selectivo lo usan para obtener la información con el fin de engañar a las víctimas para que divulguen información, con frecuencia credenciales u otra información procesable.

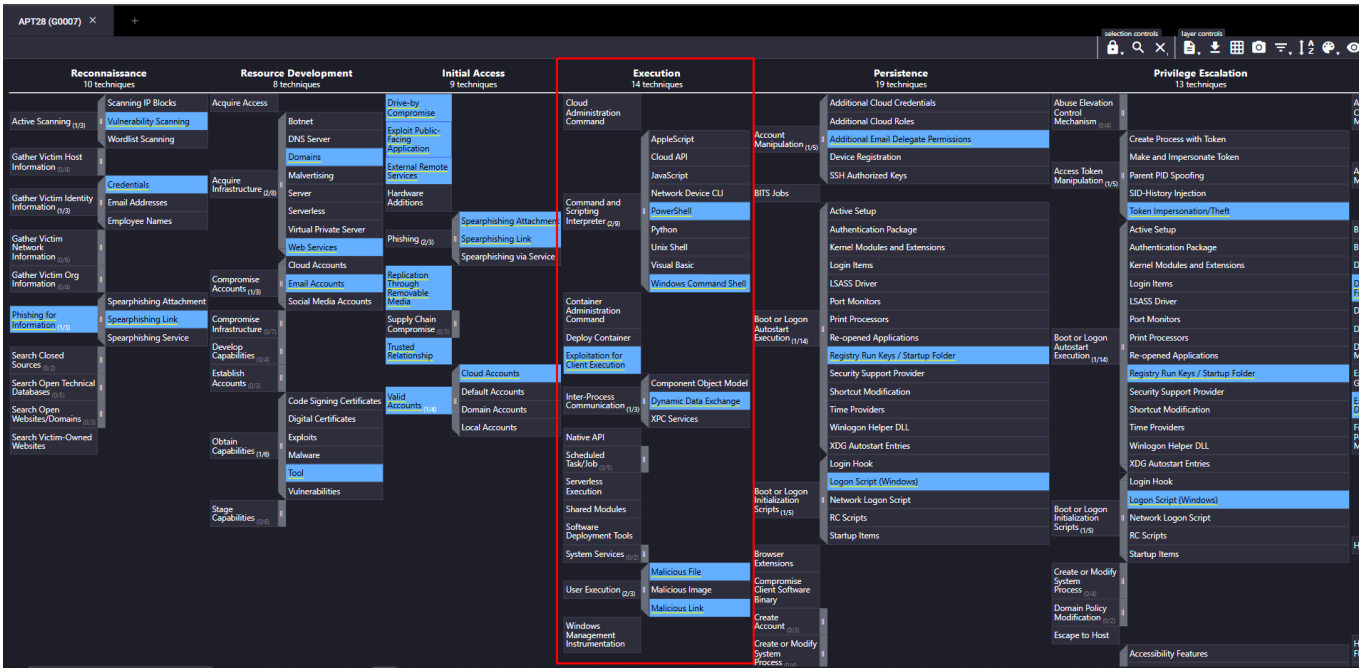
Ahora nos indican que el analista identificó que la APT podría haber avanzado desde la fase de reconocimiento. y que si podemos determinar que cuentas podría comprometer la APT mientras desarrolla recursos?

Dentro del panel de navegación vemos que el desarrollo de los recursos parte de las cuentas comprometidas:



Al verificar la tecnica encontramos que Los atacantes pueden utilizar cuentas de correo electrónico comprometidas para promover sus operaciones, como por ejemplo, para realizar campañas de phishing para obtener información , phishing o correos electrónicos no deseados a gran escala. lo que quiero al tener presente la información anterior nuestro vector de ataque el desarrollo de los recursos esta en los **Email Accounts**.

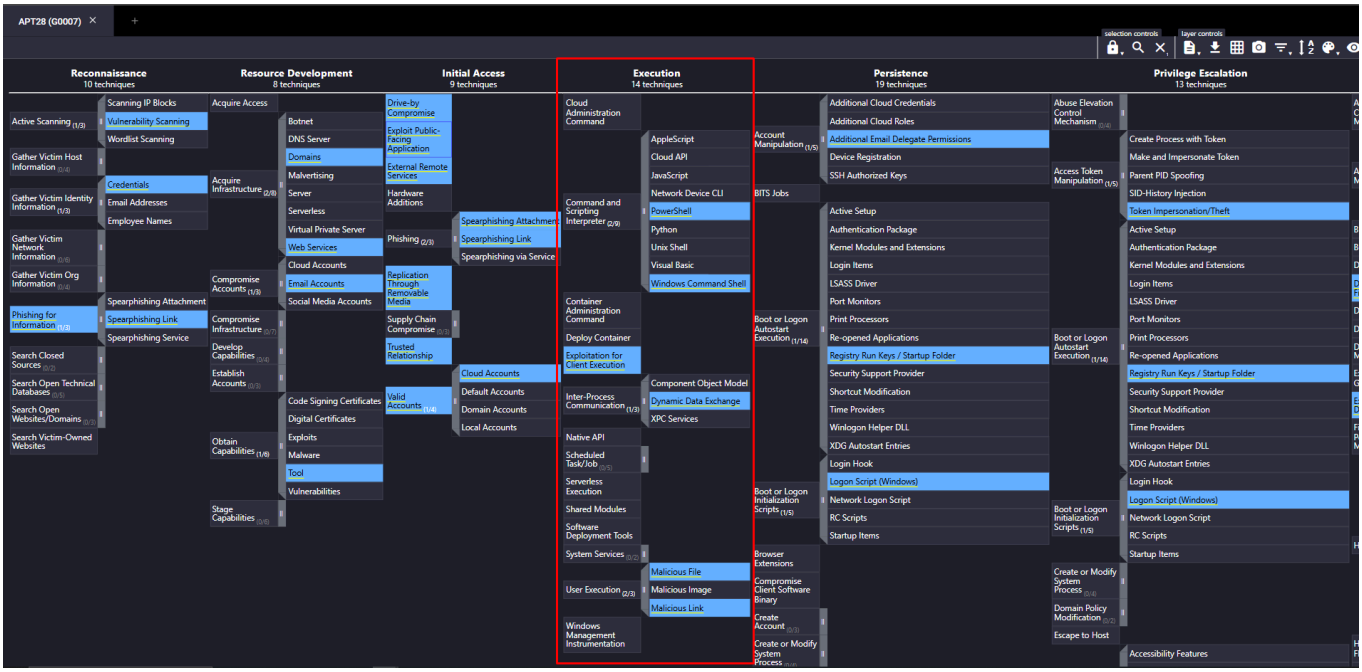
Ahora nos indican que han descubierto que la APT podría haber obtenido acceso inicial mediante ingeniería social para hacer que el usuario ejecutara código para el actor de la amenaza Y el analista quiere identificar si la APT también tuvo éxito en la ejecución. por lo que nos piden que indiquemos las dos técnicas de ejecución del usuario que se les debería prestar atención? (Nota también se indica que el **Formato de respuesta es: <técnica 1> y <técnica 2>**)



Partimos de validar la Ejecución, donde lo que nos importa validar son las ejecuciones que puede realizar un usuario debido al encabezado de la pregunta, lo que permite acortar la búsqueda a los dos parámetros asociados a la ejecución por parte del usuario **Malicious File** donde un atacante puede confiar en que un usuario abra un archivo malicioso para obtener la ejecución. Los usuarios pueden ser sometidos a ingeniería social para que abran un archivo que conduzca a la ejecución del código. Esta acción del usuario normalmente se observará como un comportamiento de seguimiento de Spearphishing Attachment . Los adversarios pueden utilizar varios tipos de archivos que requieren que un usuario los ejecute, incluidos .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, .cpl y .reg. y con un **Malicious Link** donde el atacante puede confiar en que un usuario haga clic en un enlace malicioso para obtener la ejecución. Los usuarios pueden ser sometidos a ingeniería social para que hagan clic en un enlace que conducirá a la ejecución del código. Esta acción del usuario normalmente se observará como un comportamiento de seguimiento de Spearphishing Link . Hacer clic en un enlace también puede conducir a otras técnicas de ejecución, como la explotación de una vulnerabilidad del navegador o de la aplicación a través de Exploitation for Client Execution . Los enlaces también pueden llevar a los usuarios a descargar archivos que requieren ejecución a través de Malicious File .

Por lo que ahora la pregunta mas valida seria que si la técnica anterior fue exitosa, ¿qué intérpretes de secuencias de comandos deberíamos buscar para identificar una ejecución exitosa?(Nota: **Formato de respuesta: <técnica 1> y <técnica 2>**)

Partimos del mismo panel que tenemos de ejecución en este tambien podemos observar cuales son los vectores de comandos a validar si prestamos atencion veremos los Command and Scripting Interpreters:

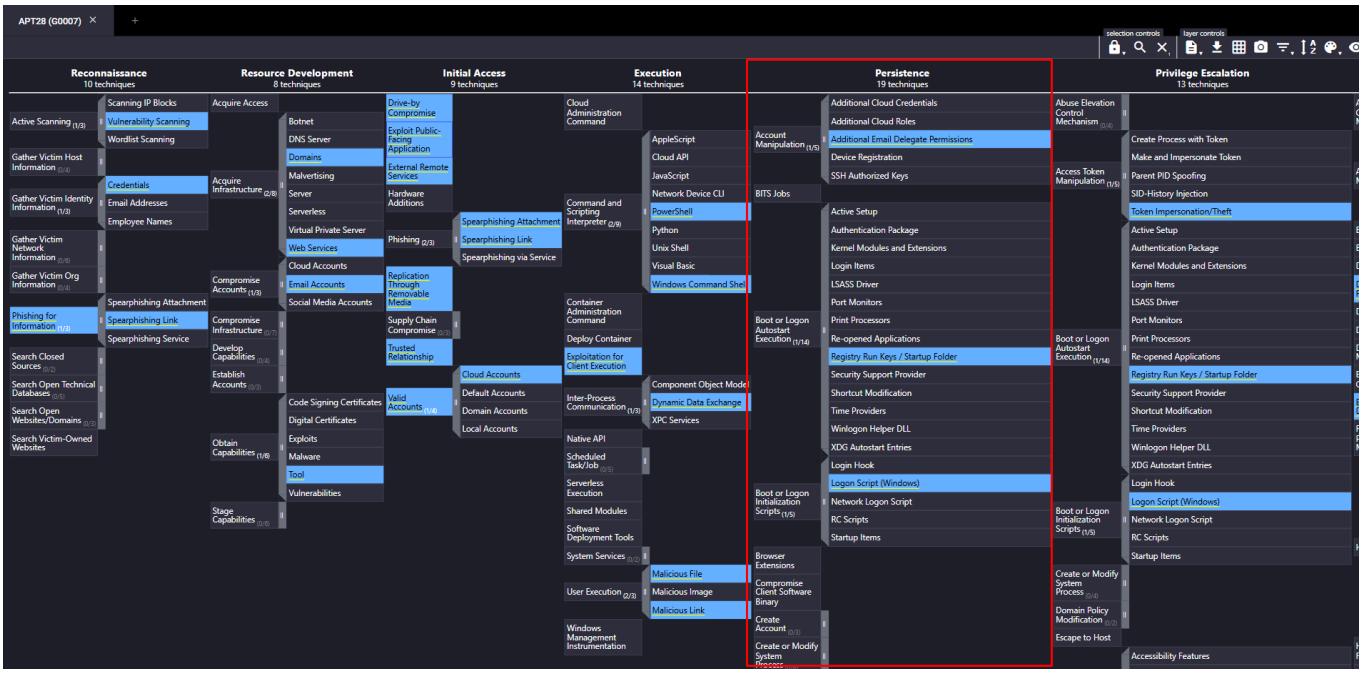


Donde Los atacantes pueden abusar de los comandos y scripts de PowerShell para su ejecución. PowerShell es una potente interfaz de línea de comandos interactiva y un entorno de scripts incluido en el sistema operativo Windows. Los adversarios pueden utilizar **PowerShell** para realizar una serie de acciones, como el descubrimiento de información y la ejecución de código. Además Los atacantes pueden abusar del **Windows command shell** para la ejecución.

Al examinar los intérpretes de secuencias de comandos identificaron que en el cuarto trimestre, se encontró algunas secuencias de comandos ofuscadas que modificaban el registro.

Suponiendo que estos cambios son para mantener la persistencia, ¿Qué claves de registro debería observar el analista para realizar un seguimiento de estos cambios?

Por lo que partimos de las persistencias si tenemos en cuenta lo que ya hemos encontrado y vemos cuales son las opciones tendríamos los Registry Run Keys y los Logon Script de Windows los dos son las opciones viables debido a que se ejecutaron interpretadores de comandos.



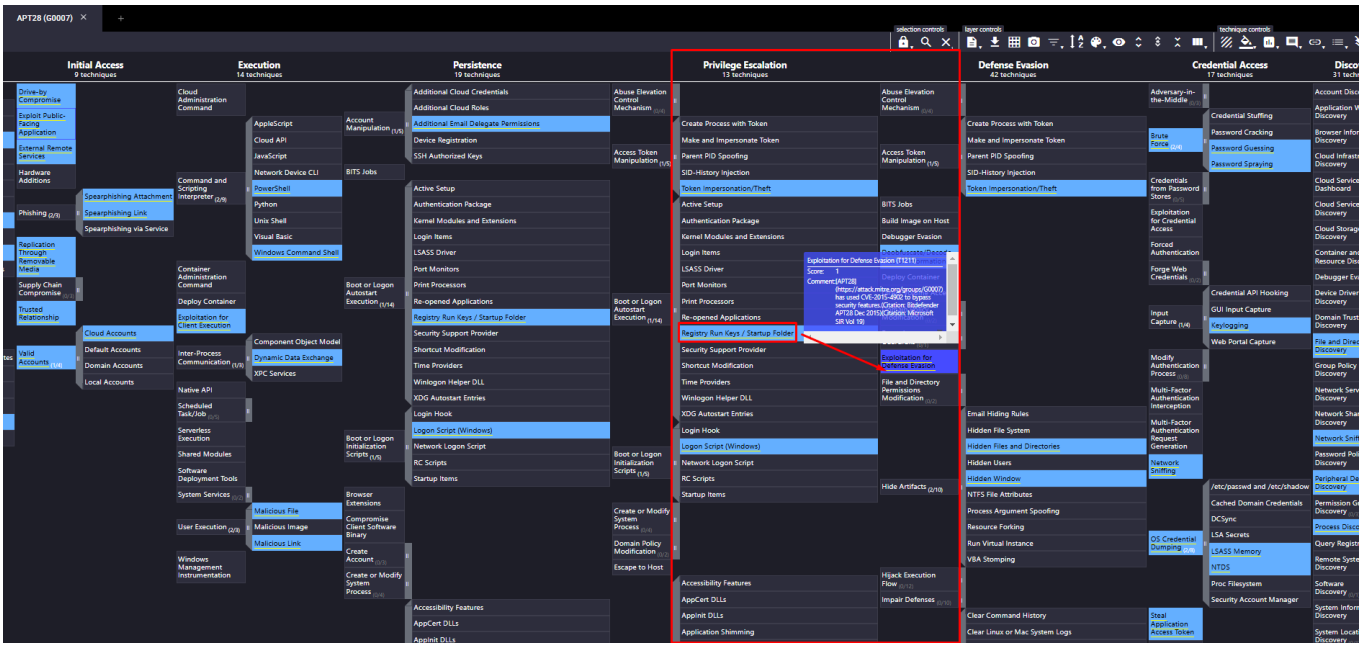
Para el caso de los Registry Run Keys Los atacantes pueden lograr la persistencia agregando un programa a una carpeta de inicio o haciendo referencia a él con una clave de ejecución del Registro. Agregar una entrada a las "claves de ejecución" en el Registro o la carpeta de inicio hará que el programa al que se hace referencia se ejecute cuando un usuario inicie sesión. 1(https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys) Estos programas se ejecutarán en el contexto del usuario y tendrán el nivel de permisos asociado a la cuenta. Para el caso del Logon Script de Windows Los atacantes pueden usar scripts de inicio de sesión de Windows que se ejecutan automáticamente al iniciar el inicio de sesión para establecer la persistencia. Windows permite que los scripts de inicio de sesión se ejecuten siempre que un usuario o un grupo de usuarios específicos inicien sesión en un sistema. Esto hace que los atacantes pueden usar estos scripts para mantener la persistencia en un único sistema. **Según la configuración de acceso de los scripts de inicio de sesión, es posible que se necesiten credenciales locales o una cuenta de administrador**.

Debido a esta verificación de las técnicas lo que tuve en cuenta fue que para este caso seria mejor usar la persistencia bajo el parámetro de las **Registry Run Keys** dado que los que se hace es agregar el programa a una carpeta de inicio o haciendo referencia a él con una clave de ejecución pero solo bajo el contexto del usuario activo y eso dará el nivel de permisos asociado a esa cuenta.

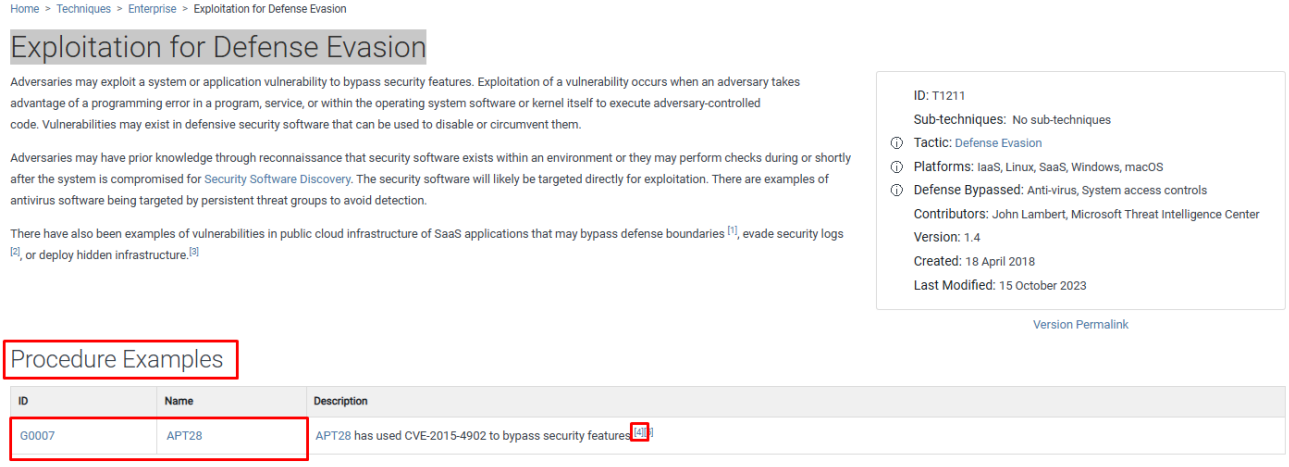
El analista identificó que el APT ejecuta binarios del sistema, esto hace referencia a una técnica en la que los atacantes utilizan herramientas legítimas del sistema

operativo para ejecutar acciones maliciosas sin ser detectados fácilmente por soluciones de seguridad como aplicaciones del sistema, antivirus, EDR o SIEM. por lo que nos solicitan saber ¿Qué ejecuciones de binarios del sistema se debería examinar para detectar la ejecución de proxy?

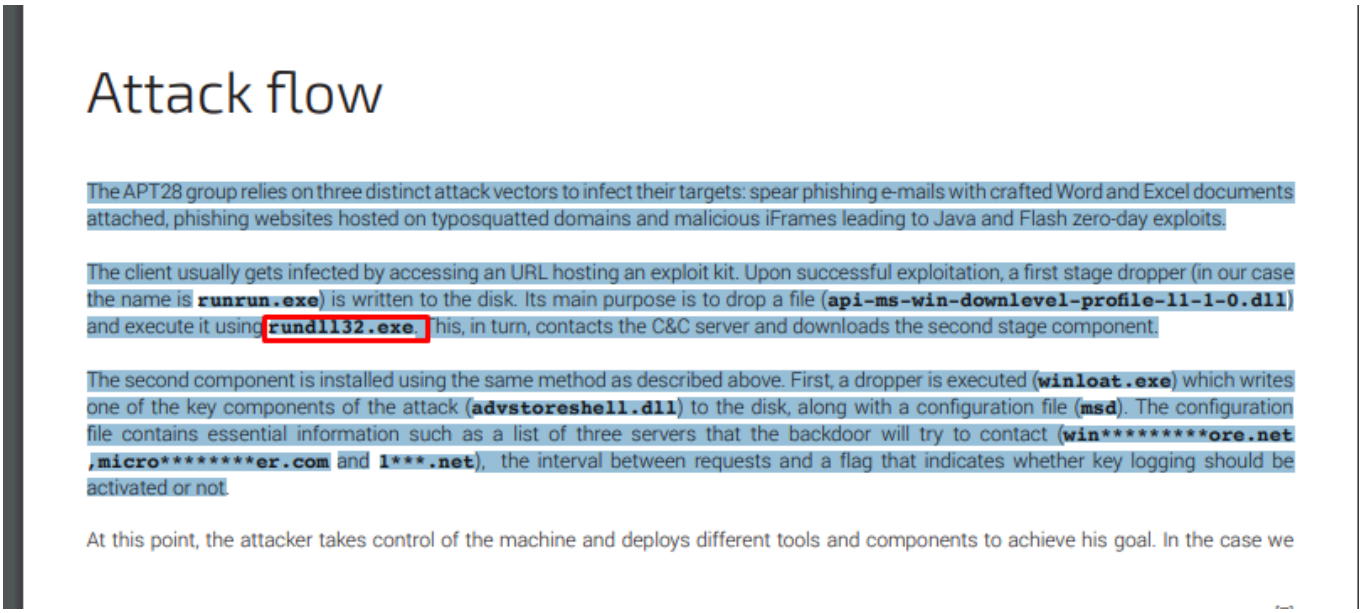
En este ya tenia que validar lo que eran los Privilegios de Escalación acá me enfoque en ver lo que ya se había analizado que eran los *Registry Run Keys* y la *Explotation for Defense Evasión*



Después de identificar lo que debia validar mire la Exploitation for Defense Evasion



en este la forma de bypass elsistema estaba asociada aun CVE por lo que mire los reportes de estos CVE que me proporcionaba la herramienta para esto vi el Análisis del apt28 Bitdefender este podemos encontrar que el flujo del ataque determina que:



Attack flow

The APT28 group relies on three distinct attack vectors to infect their targets: spear phishing e-mails with crafted Word and Excel documents attached, phishing websites hosted on typosquatted domains and malicious iFrames leading to Java and Flash zero-day exploits.

The client usually gets infected by accessing an URL hosting an exploit kit. Upon successful exploitation, a first stage dropper (in our case the name is **runrun.exe**) is written to the disk. Its main purpose is to drop a file (**api-ms-win-downlevel-profile-l1-1-0.dll**) and execute it using **rundll32.exe**. This, in turn, contacts the C&C server and downloads the second stage component.

The second component is installed using the same method as described above. First, a dropper is executed (**winloat.exe**) which writes one of the key components of the attack (**advstoreshell.dll**) to the disk, along with a configuration file (**msd**). The configuration file contains essential information such as a list of three servers that the backdoor will try to contact (**win*********ore.net ,micro********er.com** and **l***.net**), the interval between requests and a flag that indicates whether key logging should be activated or not.

At this point, the attacker takes control of the machine and deploys different tools and components to achieve his goal. In the case we

El Grupo APT28 se basa en tres vectores de ataque distintos para infectar sus objetivos. El cliente generalmente se infecta accediendo a una URL que aloja un kit de exploit. Tras la explotación exitosa, un gotero de la primera etapa (en nuestro caso El nombre es runrun.exe) se escribe en el disco. **Su objetivo principal es soltar un archivo (API-MS-WIN-Downlevel-Profile-L1-1-0.DLL) y ejecutarlo usando rundll32.exe**.

El analista identificó un dumpeo tcp (tcpdump) en uno de los hosts comprometidos. Por lo que suponiendo que el actor de la amenaza lo colocó allí, nos preguntan ¿Qué técnica podría estar usando la APT para el descubrimiento?

Ahora miramos la evasión de defensa y encontramos que el método tiene asociado 4 formas que son:

- Steal Application Access Token
- OS Credential Dumping
- Network Snnifing
- Brute Force

Debido a esta valide las técnicas para cada uno de las formas de evasión:

Volcado de credenciales del sistema operativo

Subtécnicas (8)

Los adversarios pueden intentar obtener credenciales para obtener datos de acceso y credenciales de la cuenta, normalmente en forma de hash o contraseña de texto sin formato. Las credenciales se pueden obtener de cachés, memoria o estructuras del sistema operativo. [1] Las credenciales se pueden utilizar para realizar movimientos laterales y acceder a información restringida.

Tanto los adversarios como los evaluadores de seguridad profesionales pueden utilizar varias de las herramientas mencionadas en las subtécnicas asociadas. Probablemente también existan otras herramientas personalizadas.

Identificación: T1003

Subtécnicas: T1003.001 , T1003.002 , T1003.003 , T1003.004 , T1003.005 , T1003.006 , T1003.007 , T1003.008

Táctica: Acceso a credenciales

Plataformas: Linux, Windows, macOS

Colaboradores: Ed Williams, Trustwave, SpiderLabs; Tim (Wadhwa-) Brown; Vicente Le Toux; Yves Yonan

Versión: 2.2

Creado: 31 de mayo de 2017

Última modificación: 15 de octubre de 2024

Versión Enlace permanente

Ejemplos de procedimientos

IDENTIFICACIÓN	Nombre	Descripción
G0007	APT28	APT28 implementa regularmente herramientas de recuperación de contraseñas tanto disponibles públicamente (por ejemplo, Mimikatz) como personalizadas en las víctimas. [2] [3] [4]

Fuerza bruta

Sub-técnicas (4)

Los adversarios pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando las contraseñas son desconocidas o cuando se obtienen hashes de contraseñas. [1] Sin el conocimiento de la contraseña de una cuenta o un conjunto de cuentas, un adversario puede adivinar sistemáticamente la contraseña utilizando un mecanismo repetitivo o iterativo. [2] La fuerza bruta de las contraseñas puede realizarse a través de la interacción con un servicio que verificará la validez de esas credenciales o fuera de línea contra datos de credenciales adquiridos previamente, como hashes de contraseñas.

La fuerza bruta para acceder a las credenciales puede tener lugar en varios puntos durante una vulneración. Por ejemplo, los adversarios pueden intentar forzar el acceso a cuentas válidas dentro de un entorno víctima aprovechando el conocimiento obtenido de otros comportamientos posteriores a la vulneración, como el volcado de credenciales del sistema operativo , el descubrimiento de cuentas o el descubrimiento de políticas de contraseñas . Los adversarios también pueden combinar la actividad de fuerza bruta con comportamientos como los servicios remotos externos como parte del acceso inicial.

Identificación: T1110

Subtécnicas: T1110.001 , T1110.002 , T1110.003 , T1110.004

Táctica: Acceso a credenciales

Plataformas: contenedores, IaaS, proveedor de identidad, Linux, red, paquete Office, SaaS, Windows, macOS

Colaboradores: Alfredo Oliveira, Trend Micro; David Fiser, @anu4is, Trend Micro; Ed Williams, Trustwave, SpiderLabs; Magno Logan, @magnologan, Trend Micro; Mohamed Kmal; Yossi Weizman, equipo de investigación de Azure Defender

Versión: 2.6

Creado: 31 de mayo de 2017

Última modificación: 14 de octubre de 2024

Versión Enlace permanente

Ejemplos de procedimientos

IDENTIFICACIÓN	Nombre	Descripción
C0025	Ataque a la central eléctrica de Ucrania en 2016	Durante el ataque a la energía eléctrica de Ucrania en 2016 , el equipo Sandworm utilizó un script para intentar la autenticación RPC contra varios hosts. [2]
G1030	Agrio	Agrius participó en varias actividades de fuerza bruta a través de SMB en entornos de víctimas. [3]
G0007	APT28	APT28 puede realizar ataques de fuerza bruta para obtener credenciales. [4] [1] [5]

Hogar > Técnicas > Empresa > Robar el token de acceso a la aplicación

Robar el token de acceso a la aplicación

Los adversarios pueden robar tokens de acceso a aplicaciones como medio para adquirir credenciales para acceder a sistemas y recursos remotos.

Los tokens de acceso a aplicaciones se utilizan para realizar solicitudes de API autorizadas en nombre de un usuario o servicio y se utilizan comúnmente como una forma de acceder a recursos en aplicaciones basadas en la nube y en contenedores y en software como servicio (SaaS). [1] Los adversarios que roban tokens de API de cuentas en entornos en la nube y en contenedores pueden acceder a datos y realizar acciones con los permisos de estas cuentas, lo que puede provocar una escalada de privilegios y un mayor compromiso del entorno.

Por ejemplo, en entornos Kubernetes, los procesos que se ejecutan dentro de un contenedor pueden comunicarse con el servidor API de Kubernetes mediante tokens de cuenta de servicio. Si un contenedor se ve comprometido, un adversario puede robar el token del contenedor y, de ese modo, obtener acceso a los comandos API de Kubernetes. [2] De manera similar, las instancias dentro de los canales de desarrollo continuo/integración continua (CI/CD) a menudo usarán tokens API para autenticarse en otros servicios para pruebas e implementación. [3] Si estos canales se ven comprometidos, los adversarios pueden robar estos tokens y aprovechar sus privilegios.

El robo de tokens también puede ocurrir a través de ingeniería social, en cuyo caso puede ser necesaria la acción del usuario para otorgar acceso. OAuth es un marco de trabajo comúnmente implementado que emite tokens a los usuarios para acceder a los sistemas. Una aplicación que desee acceder a servicios basados en la nube o API protegidas puede obtener entrada utilizando OAuth 2.0 a través de una variedad de protocolos de autorización. Un ejemplo de secuencia de uso común es el flujo de concesión de código de autorización de Microsoft. [4] [5] Un token de acceso OAuth permite que una aplicación de terceros interactúe con recursos que contienen datos de usuario en las formas solicitadas por la aplicación sin obtener credenciales de usuario.

Los adversarios pueden aprovechar la autorización OAuth mediante la construcción de una aplicación maliciosa diseñada para obtener acceso a los recursos con el token OAuth del usuario objetivo. [6] [7] El adversario deberá completar el registro de su aplicación con el servidor de autorización, por ejemplo, Microsoft Identity Platform mediante Azure Portal, el IDE de Visual Studio, la interfaz de línea de comandos, PowerShell o llamadas a la API REST. [8] Luego, pueden enviar un enlace de Spearphishing al usuario objetivo para incitarlo a otorgar acceso a la aplicación. Una vez que se otorga el token de acceso OAuth, la aplicación puede obtener acceso potencialmente a largo plazo a las funciones de la cuenta de usuario a través del token de acceso a la aplicación . [9]

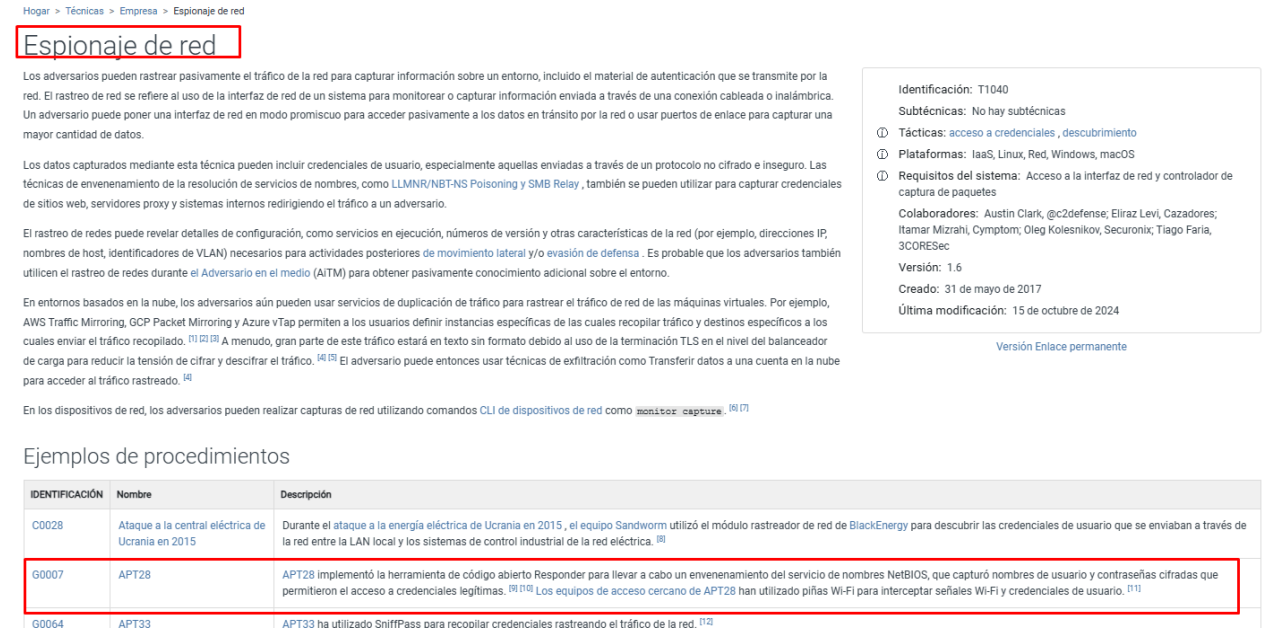
Los tokens de acceso a aplicaciones pueden funcionar durante un tiempo limitado, lo que limita el tiempo durante el cual un adversario puede utilizar el token robado. Sin embargo, en algunos casos, los adversarios también pueden robar tokens de actualización de aplicaciones [10] , lo que les permite obtener nuevos tokens de acceso sin solicitarlo al usuario.

Identificación: T1528
Subtécnicas: No hay subtécnicas
Táctica: Acceso a credenciales
Plataformas: Contenedores, IaaS, Proveedor de identidad, Suite Office, SaaS
Colaboradores: Arun Seelagan, CISA; Jack Burns, HubSpot; Jeff Sakowicz, Servicios de plataforma para desarrolladores de identidad de Microsoft (IDPM Services); Mark Wee; Ram Pliskin, Centro de seguridad de Microsoft Azure; Saisha Agrawal, Centro de inteligencia de amenazas de Microsoft (MSTIC); Shailesh Tiwary (Ejército de la India); Suzy Schapperle, Equipo rojo de Microsoft Azure
Versión: 1.4
Creado: 04 de septiembre de 2019
Última modificación: 14 de octubre de 2024

Versión Enlace permanente

Ejemplos de procedimientos

IDENTIFICACIÓN	Nombre	Descripción
S0677	AADInternals	AADInternals puede robar tokens de acceso de los usuarios a través de correos electrónicos de phishing que contienen enlaces maliciosos. [11]
G0007	APT28	APT28 ha utilizado varias aplicaciones maliciosas para robar tokens de acceso OAuth de usuarios, incluidas aplicaciones que se hacen pasar por "Google Defender", "Google Email Protection" y "Google Scanner" para usuarios de Gmail. También atacaron a usuarios de Yahoo con aplicaciones que se hacían pasar por "Delivery Service" y "McAfee Email Protection". [7]



Hogar > Técnicas > Empresa > Espionaje de red

Espionaje de red

Los adversarios pueden rastrear pasivamente el tráfico de la red para capturar información sobre un entorno, incluido el material de autenticación que se transmite por la red. El rastreo de red se refiere al uso de la interfaz de red de un sistema para monitorear o capturar información enviada a través de una conexión cableada o inalámbrica. Un adversario puede poner una interfaz de red en modo promiscuo para acceder pasivamente a los datos en tránsito por la red o usar puertos de enlace para capturar una mayor cantidad de datos.

Los datos capturados mediante esta técnica pueden incluir credenciales de usuario, especialmente aquellas enviadas a través de un protocolo no cifrado e inseguro. Las técnicas de envenenamiento de la resolución de servicios de nombres, como LLMNR/NBT-NS Poisoning y SMB Relay , también se pueden utilizar para capturar credenciales de sitios web, servidores proxy y sistemas internos redirigiendo el tráfico a un adversario.

El rastreo de redes puede revelar detalles de configuración, como servicios en ejecución, números de versión y otras características de la red (por ejemplo, direcciones IP, nombres de host, identificadores de VLAN) necesarios para actividades posteriores de movimiento lateral y/o evasión de defensa . Es probable que los adversarios también utilicen el rastreo de redes durante el Adversario en el medio (AiTM) para obtener pasivamente conocimiento adicional sobre el entorno.

En entornos basados en la nube, los adversarios aún pueden usar servicios de duplicación de tráfico para rastrear el tráfico de red de las máquinas virtuales. Por ejemplo, AWS Traffic Mirroring, GCP Packet Mirroring y Azure vTap permiten a los usuarios definir instancias específicas de las cuales recopilar tráfico y destinos específicos a los cuales enviar el tráfico recopilado. [1] [2] [3] A menudo, gran parte de este tráfico estará en texto sin formato debido al uso de la terminación TLS en el nivel del balanceador de carga para reducir la tensión de cifrar y descifrar el tráfico. [4] [5] El adversario puede entonces usar técnicas de exfiltración como Transferir datos a una cuenta en la nube para acceder al tráfico rastreado. [4]

En los dispositivos de red, los adversarios pueden realizar capturas de red utilizando comandos CLI de dispositivos de red como `monitor capture`. [6] [7]

Identificación: T1040
Subtécnicas: No hay subtécnicas
Tácticas: acceso a credenciales , descubrimiento
Plataformas: IaaS, Linux, Red, Windows, macOS
Requisitos del sistema: Acceso a la interfaz de red y controlador de captura de paquetes
Colaboradores: Austin Clark, @c2defense; Eliraz Levi, Cazadores; Itamar Mizrahi, Cymptom; Oleg Kolesnikov, Securonix; Tiago Faria, 3CORESec
Versión: 1.6
Creado: 31 de mayo de 2017
Última modificación: 15 de octubre de 2024

Versión Enlace permanente

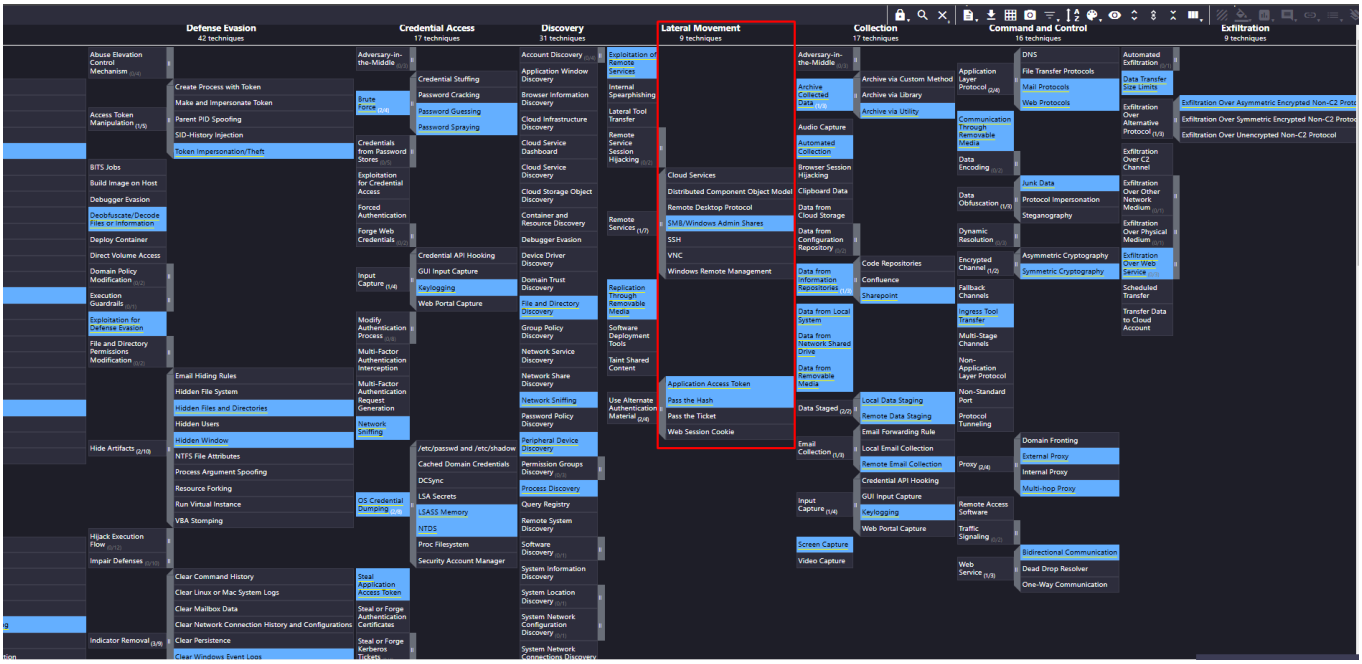
Ejemplos de procedimientos

IDENTIFICACIÓN	Nombre	Descripción
C0028	Ataque a la central eléctrica de Ucrania en 2015	Durante el ataque a la energía eléctrica de Ucrania en 2015 , el equipo Sandworm utilizó el módulo rastreador de red de BlackEnergy para descubrir las credenciales de usuario que se enviaban a través de la red entre la LAN local y los sistemas de control industrial de la red eléctrica. [8]
G0007	APT28	APT28 implementó la herramienta de código abierto Responder para llevar a cabo un envenenamiento del servicio de nombres NetBIOS, que capturó nombres de usuario y contraseñas cifradas que permitieron el acceso a credenciales legítimas. [9] [10] Los equipos de acceso cercano de APT28 han utilizado piñas Wi-Fi para interceptar señales Wi-Fi y credenciales de usuario. [11]
G0064	APT33	APT33 ha utilizado SniffPass para recopilar credenciales rastreando el tráfico de la red. [12]

Con esta información de cada una de las técnicas la que mas hace sentido bajo su descripción es un Espionaje de Red dado que se implementa un herramienta de código abierto y para llevar a cabo un envenenamiento del servicio de nombres NetBIOS, que capturan los nombres de usuario y contraseñas cifradas que permitieron el acceso a credenciales legítimas.

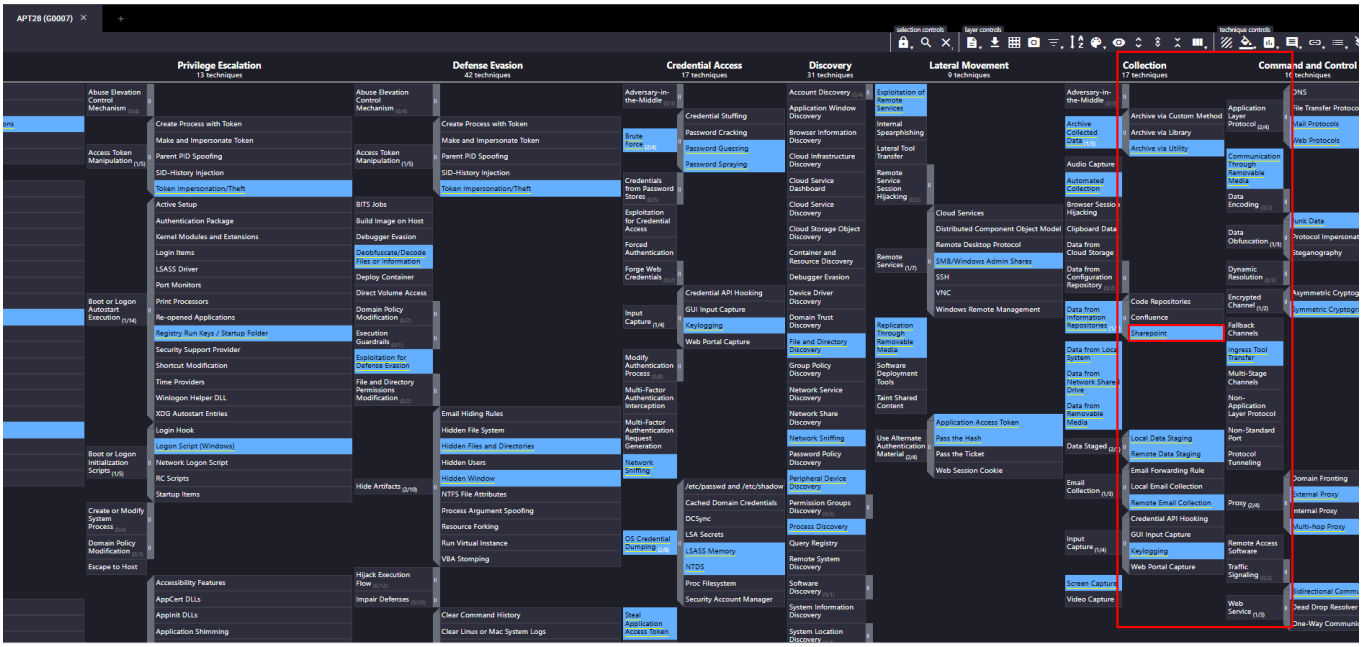
Ahora nos indican que bajo el comportamiento parece que el APT logró un movimiento lateral al explotar servicios remotos. y que veamos ¿Qué servicios remotos debería observar el analista para identificar rastros de actividad del APT?

Dentro del análisis de los movimientos laterales tenemos el SMB/Windows Admin Shares, Application Access Token y Pass the Hash como tácticas de movimiento lateral:



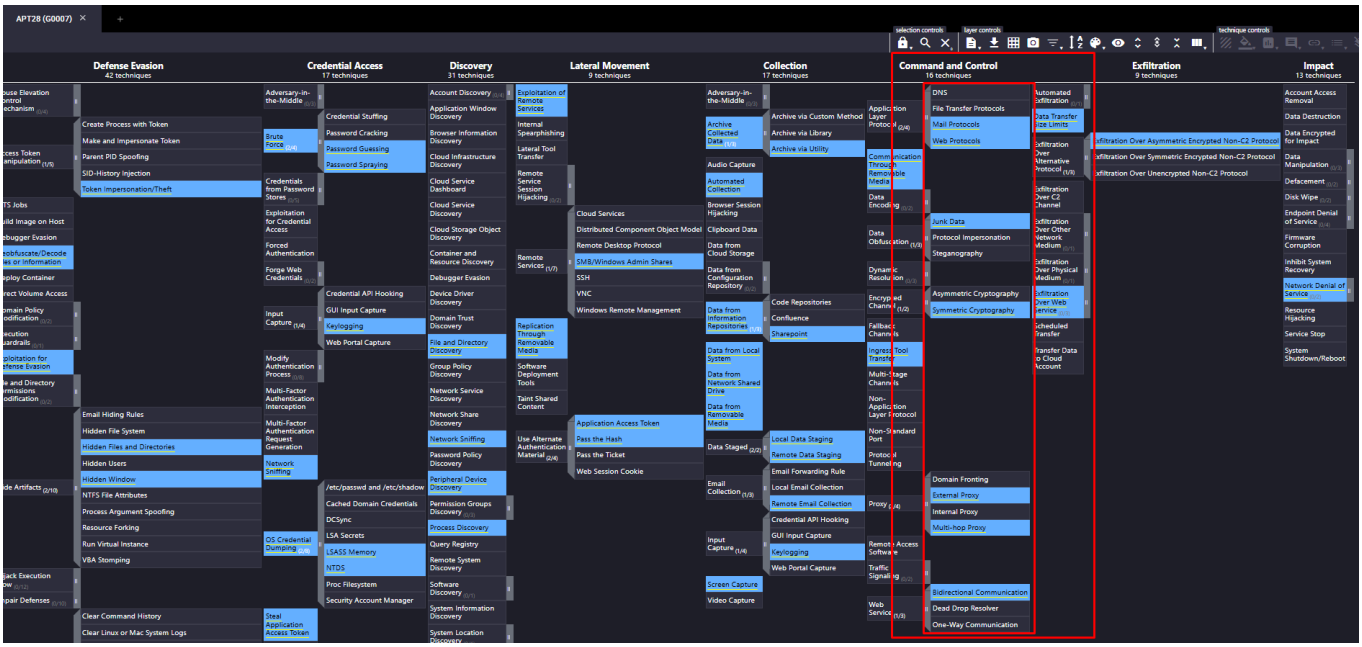
Realizando el mismo proceso que en el anterior punto lo que encontré es que una de las tecnicas los atacantes puedian usar cuentas válidas para interactuar con un recurso compartido de red remoto mediante el bloque de mensajes del servidor (SMB). El adversario puede entonces realizar acciones como el usuario conectado por lo que sabiendo que entro por medio del espionaje de red bajo este método ya tenían los nombres de usuario y contraseñas cifradas que permitieron el acceso a credenciales legítimas lo mas lógico es que este asociado con la técnica de *SMB/windows Admin Shares*.

Parecía que el objetivo principal de la APT era robar propiedad intelectual de los repositorios de información de . ¿Qué repositorio de información puede ser el objetivo probable de la APT?



Para este solo tenia en mente el **Sharepoint** debido al tipo de movimiento lateral dado que en los sistemas Windows se tienen recursos compartidos de red ocultos a los que solo pueden acceder los administradores y que brindan la posibilidad de realizar copias de archivos de forma remota y otras funciones administrativas. Los atacantes pueden usar esta técnica junto con cuentas válidas de nivel de administrador para acceder de forma remota a un sistema en red a través de *SMB*, 1(https://en.wikipedia.org/wiki/Server_Message_Block) para interactuar con sistemas mediante llamadas a procedimientos remotos (RPC), 2(https://technet.microsoft.com/en-us/library/cc787851.aspx) *transferir archivos y ejecutar binarios transferidos a través de la ejecución remota*.

Ahora nos indican que aunque el APT había recopilado los datos, no se pudo conectar al C2 para la exfiltración de datos. Y nos piden que frustrar cualquier intento de hacerlo, ¿Qué tipos de proxy podría utilizar el APT? (Nota: *Formato de respuesta: <técnica 1> y <técnica 2>*), acá tenemos los 7 formas de comando y control:



Por lo que validando encontré que:

Hogar > Técnicas > Empresa > Apoderado > Proxy externo

Proxy: Proxy externo

Otras subtécnicas del Proxy (4)

Los adversarios pueden utilizar un proxy externo para actuar como intermediario en las comunicaciones de red con un servidor de comando y control para evitar conexiones directas a su infraestructura. Existen muchas herramientas que permiten la redirección del tráfico a través de proxies o redirección de puertos, entre ellas HTRAN , ZXProxy y ZXPortMap. [1] Los adversarios utilizan este tipo de proxies para gestionar las comunicaciones de comando y control, para proporcionar resiliencia ante la pérdida de conexión o para pasar por encima de las rutas de comunicación de confianza existentes para evitar sospechas.

Los servidores proxy de conexión externa se utilizan para enmascarar el destino del tráfico C2 y, por lo general, se implementan con redireccionadores de puertos. Para estos fines, se pueden utilizar sistemas comprometidos fuera del entorno de la víctima, así como infraestructura adquirida, como recursos basados en la nube o servidores privados virtuales. Los servidores proxy se pueden elegir en función de la baja probabilidad de que se investigue una conexión a ellos desde un sistema comprometido. Los sistemas de la víctima se comunicarían directamente con el servidor proxy externo en Internet y, luego, el servidor proxy reenviaría las comunicaciones al servidor C2.

Identificación: T1090.002
Subtécnica de: T1090
Táctica: Mando y control
Plataformas: Linux, Red, Windows, macOS
Versión: 1.1
Creado: 14 de marzo de 2020
Última modificación: 16 de abril de 2024

Versión Enlace permanente

Ejemplos de procedimientos

IDENTIFICACIÓN	Nombre	Descripción
G0007	APT28	APT28 utilizó a otras víctimas como proxy para retransmitir el tráfico de comandos, por ejemplo, utilizando un servidor de correo electrónico militar georgiano comprometido como punto de enlace a las víctimas de la OTAN. El grupo también ha utilizado una herramienta que actúa como proxy para permitir el acceso C2 incluso si la víctima está detrás de un enrutador. APT28 también ha utilizado una máquina para retransmitir y ocultar las comunicaciones entre CHOPSTICK y su servidor. [2] [3] [4]

Hogar > Técnicas > Empresa > Apoderado > Proxy multisalto

Proxy: Proxy multisalto

Otras subtécnicas del Proxy (4)

Los adversarios pueden encadenar varios servidores proxy para ocultar la fuente del tráfico malicioso. Normalmente, un defensor podrá identificar el último tráfico proxy atravesado antes de que ingrese a su red, el defensor puede o no ser capaz de identificar cualquier servidor proxy anterior al proxy de último salto. Esta técnica hace que la identificación de la fuente original del tráfico malicioso sea aún más difícil, ya que requiere que el defensor rastree el tráfico malicioso a través de varios servidores proxy para identificar su origen.

Por ejemplo, los adversarios pueden construir o usar redes de enrutamiento de cebolla (como la red Tor , disponible públicamente) para transportar tráfico C2 cifrado a través de una población comprometida, lo que permite la comunicación con cualquier dispositivo dentro de la red. [1] Los adversarios también pueden usar redes de cajas de retransmisión operativas (ORB) compuestas por servidores privados virtuales (VPS), dispositivos de Internet de las cosas (IoT), dispositivos inteligentes y enrutadores al final de su vida útil para ofuscar sus operaciones. [2]

En el caso de la infraestructura de red, es posible que un adversario aproveche varios dispositivos comprometidos para crear una cadena de proxy de múltiples saltos (es decir, dispositivos de red). Al aprovechar Patch System Image en los enrutadores, los adversarios pueden agregar código personalizado a los dispositivos de red afectados que implementarán el enrutamiento de cebolla entre esos nodos. Este método depende del método Network Boundary Bridging que permite a los adversarios cruzar el límite de red protegido del perímetro de Internet y entrar en la red de área amplia (WAN) de la organización. Se pueden utilizar protocolos como ICMP como transporte.

De manera similar, los adversarios pueden abusar de la infraestructura peer-to-peer (P2P) y orientada a blockchain para implementar el enrutamiento entre una red descentralizada de pares. [3]

Identificación: T1090.003
Subtécnica de: T1090
Táctica: Mando y control
Plataformas: Linux, Red, Windows, macOS
Colaboradores: Eduardo Chavarro Ovalle
Versión: 2.2
Creado: 14 de marzo de 2020
Última modificación: 25 de septiembre de 2024

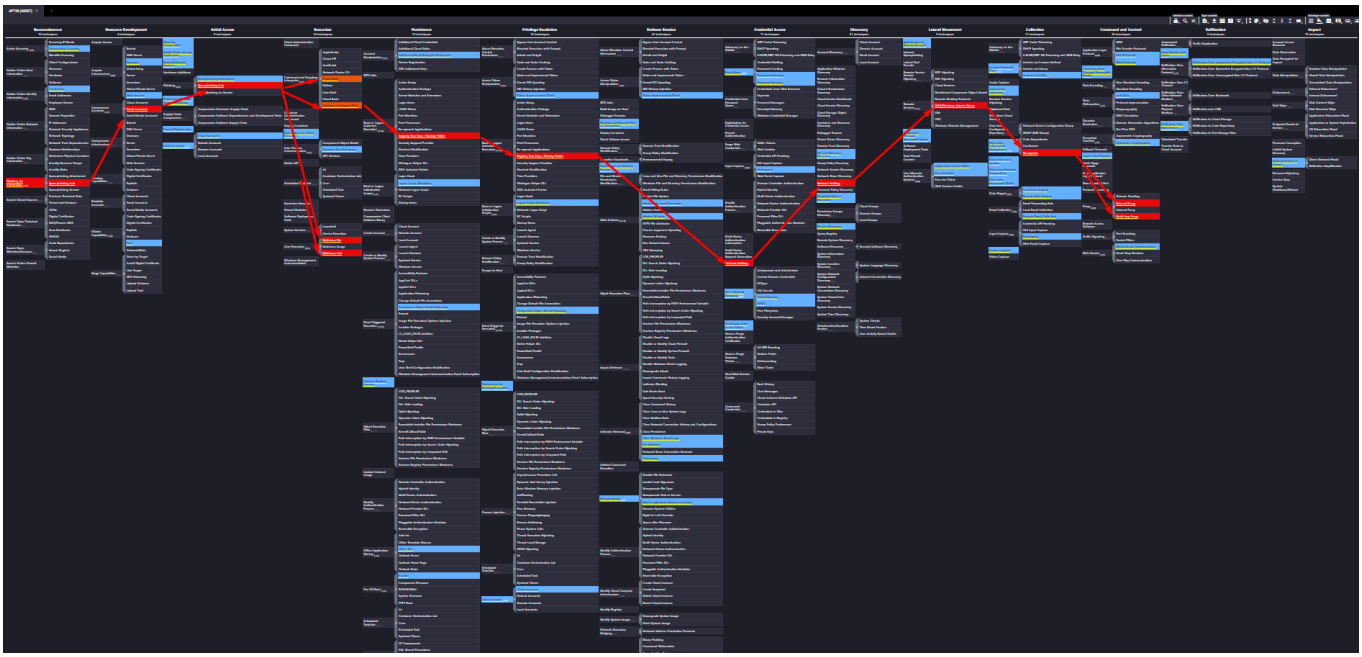
Versión Enlace permanente

Ejemplos de procedimientos

IDENTIFICACIÓN	Nombre	Descripción
G0007	APT28	APT28 ha enrutado el tráfico a través de servidores Tor y VPN para ofuscar sus actividades. [4]

Estas dos técnicas están enfocadas en el uso de la red de comunicaciones para retransmitir el tráfico de comandos, por ejemplo, utilizando un servidor de correo electrónico o enrutando el tráfico a través de servidores Tor y VPN para ofuscar sus actividades.

Con todo esto ya hemos ayudado al analista a frustrar con éxito los planes del APT dejando así una hoja de ruta del evento en cada fase al impedirle lograr su objetivo de robar la propiedad intelectual de la organización.



Gracias!.