BOLETÍN DE ALERTA

Boletín Nro.: 2016-11
Fecha de publicación: 25/08/2016
Tema: Ataques de fuerza bruta en servidores de correo

Descripción:

En los últimos días se ha observado un incremento en los ataques de fuerza bruta sistemáticos a cuentas de correo electrónico, especialmente en el sector gubernamental. Si bien los ataques de fuerza bruta no representan una técnica nueva, y existen múltiples soluciones a este problema, hemos observado que, debido a las características de estos ataques en particular, la mayoría de las soluciones no lo mitigan de forma eficiente. Los intentos se producen con un ratio tal que, la mayoría de las herramientas, tanto firewalls, sistemas IDS/IPS, etc., en sus configuraciones más frecuentes, no lo detectan, ya que no superan los límites de las mismas. En los casos observados, el ratio por IP es de 1 intento cada 11 minutos, a cada cuenta.

Muchas empresas e instituciones gubernamentales utilizan Zimbra como servidor de correo, una solución de correo corporativo de código abierto, colaborativa, que cuenta con una edición sin costo. Si bien, cuenta con numerosas características de seguridad, incluidas las políticas de control de acceso como bloqueo por intentos erróneos, estas bloquean las cuentas de los usuarios bajo ataque, sin diferenciar la IP desde la cual se produce el intento, causando inconvenientes a la persona que legítimamente quiere utilizar su cuenta, ya que el bloqueo se produce sobre la cuenta y no sobre la IP.

Además, teniendo en cuenta que las políticas de control de acceso vienen desactivadas por defecto, por lo que, en caso de que el administrador del servidor de correo no lo hubiera activado y configurado adecuadamente, es posible que el ataque de fuerza bruta sea exitoso y logre comprometer una o más cuentas de correo.

Otras soluciones de correo electrónico como Exchange Server tienen también políticas de control de acceso básicas, configurables, mediante Exchange Active Sync o Microsoft Active Directory, por ejemplo. Sin embargo, tampoco realiza controles sobre la IP sino sobre la cuenta, por lo que no es eficiente para ataques de fuerza bruta de bajo ratio como los descritos.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Impacto:

Un atacante puede lograr acceder a una cuenta de correo electrónico, obteniendo así información sensible y/o confidencial. También podría utilizar la cuenta comprometida para enviar correos maliciosos y/o suplantar la identidad de la persona cuya cuenta comprometió. En caso de que el servidor de correo tenga implementado un bloqueo de cuenta por intentos fallidos, estos bloqueos interrumpirán la actividad normal de los usuarios afectados.

Los ataques de fuerza bruta, independientemente de su éxito en el acceso de una cuenta, generan una sobrecarga a la interfaz de red de los sistemas afectados.

Mitigación y Prevención:

Se recomienda la configuración de políticas de contraseña y de control de acceso en los servidores de correo, asegurando la utilización de contraseñas robustas, cambio de contraseñas, y minimizando los intentos fallidos, no solo por cuenta sino también por IP. Las instrucciones específicas varían de acuerdo a cada software de correo.

En el caso de Zimbra, las políticas de contraseña y de fallos de inicio de sesión se configuran desde el panel de administración, de la siguiente manera:

1. "Configurar" > "Clase de servicio" > "default" o la clase que haya establecido (en caso de que lo hubieran personalizado).
2. Seleccionar "Avanzado"
3. Valores recomendados:
    a. Tamaño mínimo de la contraseña: 10
    b. Mínimo de caracteres en mayúsculas: 1
    c. Mínimo de caracteres en minúsculas: 1
    d. Mínimo de signos de puntuación: 1
    e. Mínimo de caracteres numéricos: 1
    f. Antigüedad máxima de la contraseña (días): 90
    g. Número mínimo de contraseñas únicas en el registro: 3
    h. Activar bloqueo de inicio de sesión fallido: Tildado
    i. Número de intentos fallidos permitidos para iniciar sesión: 5 *
    j. Tiempo antes de bloquear la cuenta: 1 hora
    k. Período de tiempo dentro del cual deben tener lugar los intentos fallidos de iniciar sesión para bloquear la cuenta: 30 min.

* Obs.: Debe encontrarse un balance para este valor, ya que el mismo no contempla los intentos de IPs diferentes. En caso de que activará adicionalmente fail2ban o similar, se recomienda aumentar dicho valor, por ejemplo a 10, o personalizarlo de acuerdo a sus necesidades.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

En el caso de Exchange Server, se recomienda seguir la documentación oficial, de acuerdo a la versión utilizada. Además, el procedimiento varía de acuerdo a su arquitectura.
En caso de que utilice Exchange ActiveSync, puede seguir las siguientes guías:
https://technet.microsoft.com/en-us/library/dn282287(v=ws.11).aspx
https://technet.microsoft.com/en-us/library/bb123994(v=exchg.141).aspx
https://technet.microsoft.com/en-us/library/bb125004(v=exchg.141).aspx

Para monitorear los intentos fallidos de inicio de sesión de una cuenta y realizar bloqueos de acuerdo a IPs, existen diferentes soluciones y herramientas de terceros que se pueden integrar. En el caso de Zimbra, una herramienta eficaz es fail2ban, una aplicación para la prevención de intrusos en un sistema, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta. Funciona en sistemas POSIX que tengan interfaz con un sistema de control de paquetes o un firewall local, como iptables o TCP Wrapper. Es integrable no solo a Zimbra sino también puede ser utilizado para proteger accesos SSH, FTP, web, etc.
Puede seguir la siguiente guía para instalar y configurar fail2ban:
http://www.cert.gov.py/index.php/download_file/view/775/209

Para Exchange Server existen scripts y herramientas desarrollados por terceros que se pueden personalizar e integrar. Algunas pueden ser:
https://github.com/jjxtra/Windows-IP-Ban-Service
https://github.com/EvanAnderson/ts_block
https://github.com/MichaelApproved/powershell-block-windows-attack/blob/master/block-brute-force-windows-attack-attempts.ps1

Información adicional:
http://www.cert.gov.py/index.php/download_file/view/775/209

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py