Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Inyección de Código

Tipo de incidente: Zero Day Cross-site scripting (XSS)

Nivel de riesgo: Medio

II. ALERTA

Vulnerabilidad de seguridad de Zimbra de tipo cross-site scripting (XSS), se explota activamente en ataques dirigidos a organizaciones gubernamentales y medios europeos.

Figura 1. Logo Sistema de correo electrónico ZIMBRA **Fuente:** BleepingComputer

III. INTRODUCCIÓN

En diciembre de 2021, se identificó una serie de campañas de phishing dirigidos, por parte de un actor de amenazas conocido como TEMP_Heretic (de origen Chino aparentemente). El análisis de los correos electrónicos de estas campañas de spear phishing, condujo a un

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

descubrimiento: el atacante estaba intentando explotar una vulnerabilidad de día cero, de tipo cross-site scripting XSS (inyección de código malicioso), en la plataforma de correo electrónico de Zimbra; plataforma de correo electrónico de código abierto que Organizaciones/Instituciones suelen utilizar como alternativa a Microsoft Exchange.

Las campañas llegaron en múltiples oleadas en dos fases de ataque, la fase inicial estaba dirigida al reconocimiento, e involucraba correos electrónicos diseñados para simplemente rastrear si un objetivo recibió y abrió los mensajes. La segunda fase se produjo en varias oleadas, las cuales contenían mensajes de correo electrónico que atraían a los objetivos para que hicieran clic en un enlace creado por un atacante malicioso.

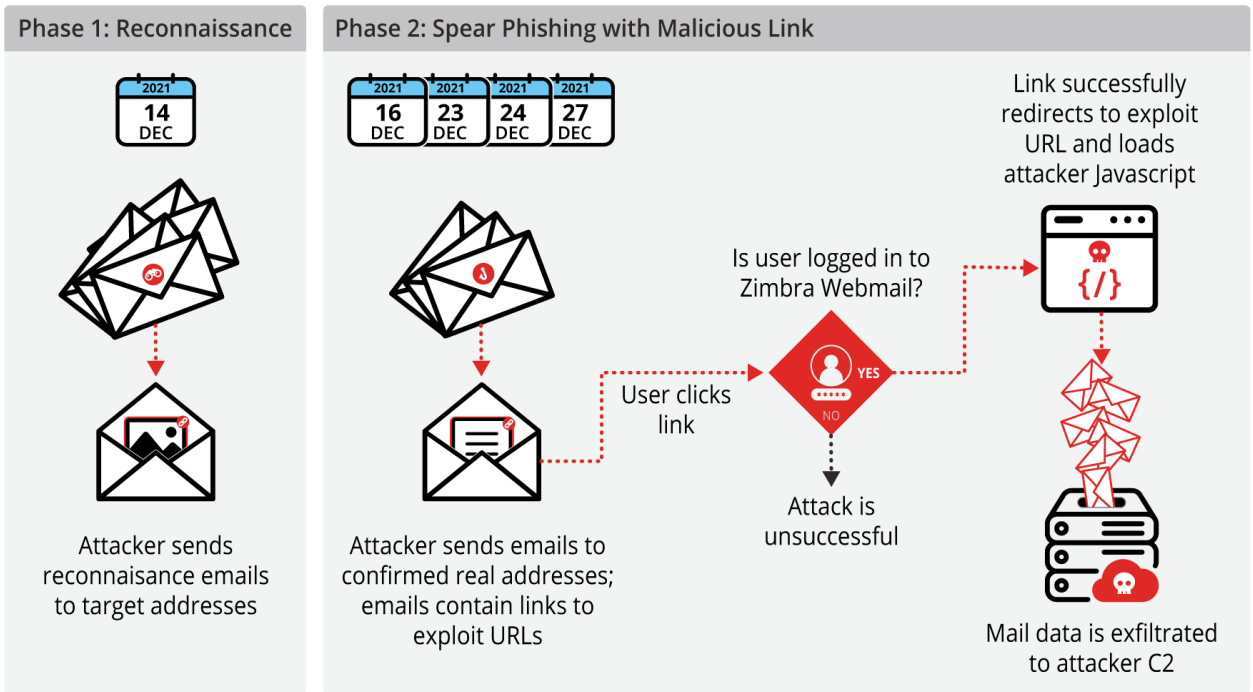

Figura 2. Etapas de ataque XSS Zimbra **Fuente:** Volexity

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

IV. VECTOR DE ATAQUE

Remoto, Spear Phishing

V. IMPACTO:

TEMP_Heretic intentaba robar correos electrónicos y archivos adjuntos, la vulnerabilidad XSS de Zimbra podría permitir fácilmente que un atacante realice otras acciones en el contexto de la sesión de correo web de Zimbra del usuario, como las siguientes:

- Filtre las cookies para permitir el acceso persistente a un buzón.
- Envíe más mensajes de phishing a los contactos de un usuario.
- Presente un aviso para descargar malware en el contexto de un sitio web de confianza.

Hasta la presente fecha, este exploit no tiene un parche disponible, tampoco se ha asignado un CVE (es decir, esta es una vulnerabilidad de día cero). Se ha podido confirmar que las versiones más recientes de Zimbra (8.8.15 P29 y P30) siguen siendo vulnerables; las pruebas de la versión 9.0.0 indican que es probable que no se vea afectada. Según los datos obtenidos, aproximadamente 33 000 servidores ejecutan el servidor de correo electrónico Zimbra, aunque es probable que el número real sea mayor. Según Zimbra, hay 200.000 empresas y más de mil instituciones gubernamentales y financieras que utilizan el software.

No se ha podido atribuir la actividad observada, a un actor de amenazas previamente conocido. Sin embargo, en base a una serie de factores observados, se cree que es probable que el atacante sea de origen chino. Se ha observado que TEMP_HERETIC se dirige a organizaciones en los siguientes sectores:

- Gobierno Europeo
- Media

La fase inicial del ataque se produjo en forma de campaña de spear-phishing enviada el 14 de diciembre de 2021. No involucró ningún tipo de señuelo de ingeniería social fuera de intentar que el usuario viera o abriera el correo electrónico. Esta primera ola simplemente incrustó imágenes remotas en el cuerpo de los mensajes de correo electrónico. Estos correos electrónicos no contenían más contenido que la imagen remota y tenían asuntos

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

genéricos a menudo asociados con spam no dirigido. A continuación se muestra una lista de los temas de la línea de asunto utilizados para los correos electrónicos de reconocimiento iniciales.

- Invitaciones
- Devoluciones de billetes de avión
- Advertencias
- <sin tema>

En la segunda fase de ataque, se observó varias campañas de spear-phishing ejecutadas el 16, 23, 24 y 27 de diciembre de 2021. En estas campañas, el atacante incrustó enlaces a la infraestructura controlada por el atacante. En algunos casos, parece que se hizo un mayor esfuerzo para crear un señuelo que fuera más atractivo para el individuo objetivo. Se utilizaron dos temas diferentes a diferencia de la primera ola de ataques.

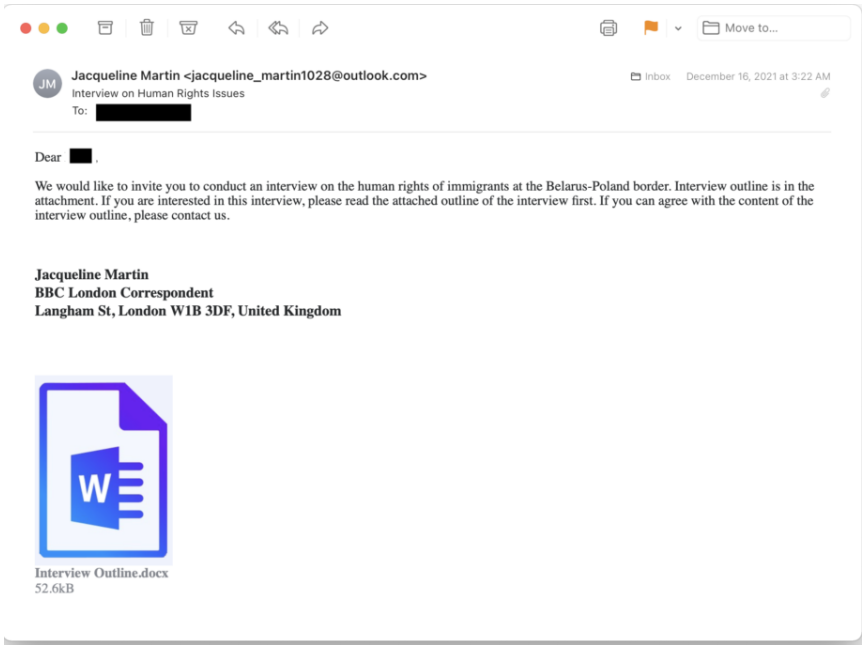

Figura 3. Muestra de correo electrónico malicioso **Fuente:** Volexity

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

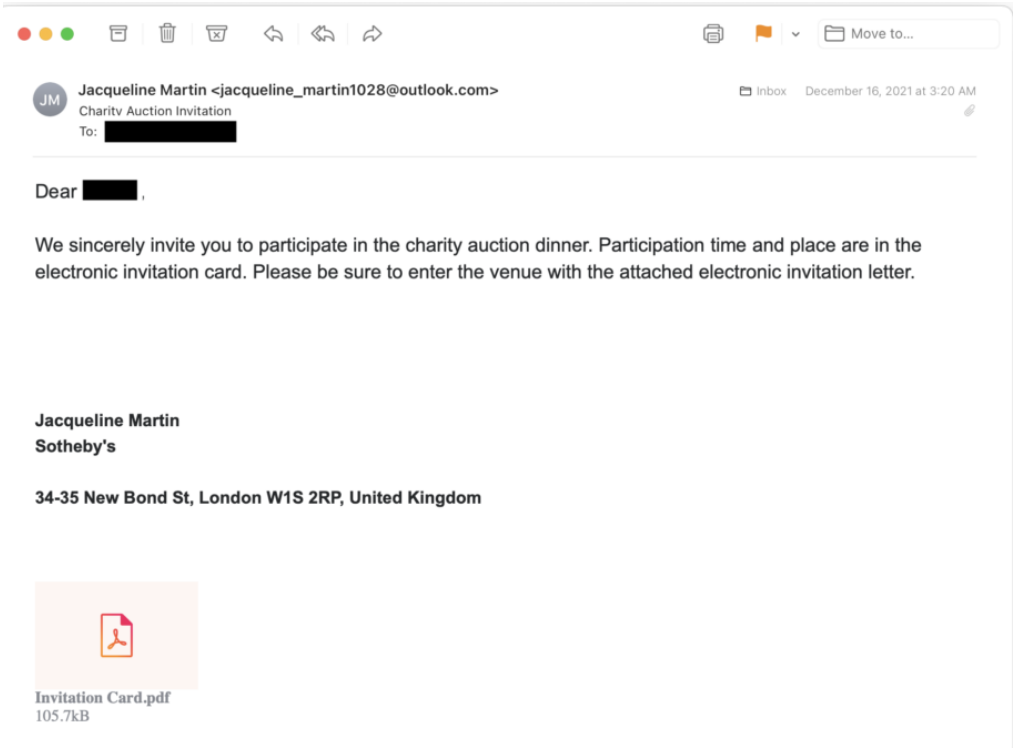

Figura 4. Muestra de correo electrónico malicioso **Fuente:** Volexity

La funcionalidad del código del atacante es simple:

- Recorre cada correo electrónico en la bandeja de entrada del usuario y las carpetas enviadas.
- Para cada correo electrónico encontrado, envíe el cuerpo del correo electrónico y los archivos adjuntos a la dirección de devolución de llamada configurada (mail.bruising-intellect[.]ml) a través de solicitudes HTTP POST.

El efecto general de este ataque, es que al hacer que un usuario haga clic en un enlace en un correo electrónico y deje abierta la ventana de su navegador durante un período de tiempo, el atacante puede robar el contenido de su buzón. El código JavaScript utilizado para facilitar el robo de correo debe personalizarse según la versión de Zimbra, ya que el atacante debe solicitar una página que contenga un token CSRF (token de seguridad

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

aleatorio) para realizar solicitudes posteriores para robar datos de correo.

Figura 5. Ejemplo de datos POST enviados por JavaScript que contienen datos completos del cuerpo del correo electrónico **Fuente:** Volexity

VI. INDICADORES DE COMPROMISO

ITEM	VALOR	NOMBRE DE ENTIDAD	DESCRIPCION
1	www.newsonline.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
2	mx.newsonline.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
3	www.spiritx.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
4	support.newsonline.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
5	www.thunderchannel.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

ITEM	VALOR	NOMBRE DE ENTIDAD	DESCRIPCION
6	shadownight.playquicksand.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
7	www.windsoft.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
8	tigerstrike.iceywindflow.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
9	shadowmaster.iceywindflow.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
10	www.iceywindflow.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
11	chargedboltsentry.spiritfield.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
12	newsonline.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
13	spiritx.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
14	secretstep.tk	hostname	Infrastructure used in conjunction with Zimbra 0-day. Initial domain used to redirect users to malicious Zimbra URL.
15	spiritfield.ga	hostname	Infrastructure used in conjunction with Zimbra 0-day. Used in reconnaissance emails to validate if addresses were real before sending real payload later.
16	www.news-voice.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
17	www.findtruth.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
18	news-online.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
19	iceywindflow.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
20	playquicksand.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

ITEM	VALOR	NOMBRE DE ENTIDAD	DESCRIPCION
21	windsoft.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
22	findtruth.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
23	iceywindflow.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
24	news-voice.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
25	bruising-intellect.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
26	thunderchannel.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
27	spiritfield.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
28	iceywindflow.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
29	thunderchannel.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
30	spiritfield.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
31	update.secretstep.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
32	mail.bruising-intellect.ml	hostname	Infrastructure used in conjunction with Zimbra 0-day. Hosted malicious JS used to steal user mail and was C2 for that malicious JS.
33	www.news-online.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
34	www.thunderchannel.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
35	www.spiritfield.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
36	winderosion.spiritfield.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

ITEM	VALOR	NOMBRE DE ENTIDAD	DESCRIPCION
37	flameshock.spiritfield.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
38	windsource.thunderchannel.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
39	yahoo-movie.spiritx.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
40	windsource.thunderchannel.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
41	opticaleel.iceywindflow.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
42	shadownight.spiritfield.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
43	206.166.251.141	ipaddress	Resolution for known domain associated with Zimbra Exploitation
44	206.166.251.166	ipaddress	Resolution for known domain associated with Zimbra Exploitation
45	108.160.133.32	ipaddress	Suspected related C2 server
46	172.86.75.158	ipaddress	Resolution for known domain associated with Zimbra Exploitation
47	www.yahoo-corporation.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
48	amazon-check.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
49	amazon-team.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
50	yahoo-corporation.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
51	playquicksand.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
52	yahoo-corporation.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
53	playquicksand.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

ITEM	VALOR	NOMBRE DE ENTIDAD	DESCRIPCION
54	spiritfield.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
55	amazon-check.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
56	amazon-check.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
57	amazon-check.tk	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
58	playquicksand.ml	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
59	www.playquicksand.cf	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
60	www.amazon-check.ga	hostname	Infrastructure likely used in conjunction with Zimbra 0-day
61	www.playquicksand.gq	hostname	Infrastructure likely used in conjunction with Zimbra 0-day

Tabla 1. Indicadores de compromiso utilizados en campaña día cero XSS Zimbra **Fuente:** Volexity

VII. RECOMENDACIONES

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

- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales.
- Instalar y utilizar software antivirus de confianza.
- Mantener actualizado el sistema de correo electrónico Zimbra, aplicando las últimas actualizaciones y parches de seguridad disponibles.
- Todos los indicadores de compromiso descritos en la tabla número 1, deben bloquearse en la puerta de enlace de correo y, a nivel de red a través de plataformas de seguridad perimetral.
- Los administradores del sistema de correo electrónico Zimbra, deben analizar los datos de referencia históricos en busca de referencias y accesos sospechosos. La ubicación predeterminada de estos registros, se puede encontrar en

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-019	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**Vulnerabilidad XSS de día cero en Zimbra, es utilizada para para robar correos electrónicos**	V 1.0

/opt/zimbra/log/access*.log.

- Los usuarios del sistema de correo electrónico Zimbra, deberían considerar actualizar a la versión 9.0.0, ya que actualmente no existe una versión segura de 8.8.15 o anteriores.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Identificar y suspender el acceso de usuarios que exhiban una actividad inusual.
- Implementar un plan de respuesta a emergencias en la Organización/Institución, considerar la gama completa de impactos potenciales que los ciberataques plantean a las operaciones, incluida la pérdida o manipulación de la información, la pérdida o manipulación del control y, las amenazas a la seguridad.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. REFERENCIAS:

Steven Adair, Thomas Lancaster. (3 de febrero de 2022). Volexity. Obtenido de https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/

Sergio Gatlán. (3 de febrero de 2022). Bleeping Computer. Obtenido de https://www.bleepingcomputer.com/news/security/zimbra-zero-day-vulnerability-actively-exploited-to-steal-emails/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec