Nro. Alerta:	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Phishing para instalación de Troyano de Acceso Remoto (RAT)

Nivel de riesgo: Medio

II. ALERTA

Nuevo malware llamado 'DarkWatchman', de tipo RAT (troyano de acceso remoto), desarrollado en JavaScript liviano junto a un registrador de teclas (keylogger), se esconde en el registro de sistema de Windows para no ser detectado

```
function keylogger_hex_to_registry(hex_data) {
  var k = new Array();
  for (var i = 0; i < 4; i++) { k[i] = parseInt(hex_data.substr(i * 2, 2), 16); }
  var kl_plain_data = unxor(hex_data.substr(8), k);
  return cfg_set_param(uid + 1, kl_plain_data);
}
function keylogger_to_registry() {
  if (fso.FileExists(self_dir + '2204722946')) {
    var kl_hex_data = get_file_content(self_dir + '2204722946', false);
    erase_file(self_dir + '2204722946');
    return keylogger_hex_to_registry(kl_hex_data);
  }
  else return false;
}
```

Figura 1.- Función incrustada en DarkWatchman para instalación de keylogger en el registro del Sistema Operativo de Microsoft Windows
Fuente: TheHackerNews

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-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

III. INTRODUCCIÓN

A fines de noviembre, el Equipo de Contrainteligencia Adversario (PACT) de Prevailion, identificó lo que parecía ser un troyano malicioso de acceso remoto (RAT), basado en javascript, utiliza un algoritmo de generación de dominio (DGA) robusto para identificar su infraestructura de comando y control (C2) que utiliza métodos novedosos para la persistencia sin archivos, la actividad en el sistema y las capacidades dinámicas de tiempo de ejecución, actualización automática, y la recompilación. Este RAT, a la que PACT se refiere por su nombre en clave interno "DarkWatchman", se distribuye por correo electrónico y representa una evolución en las técnicas de malware sin archivos, ya que utiliza el registro para casi todo el almacenamiento temporal y permanente y, por lo tanto, nunca escribe nada en el disco, lo que le permite operar por debajo o alrededor del umbral de detección de la mayoría de las medidas de seguridad.

Según un informe técnico de investigadores de Prevailion, este RAT es empleado por actores de habla rusa que se dirigen principalmente a organizaciones rusas.

IV. VECTOR DE ATAQUE:

DarkWatchman se distribuye a través de correo electrónico, mediante técnicas de ingeniería social como el phishing. El archivo adjunto al correo electrónico, es un archivo .zip llamado como un documento legal de registro contable (factura), el cual contiene un ejecutable (.exe) con el mismo nombre. El icono del ejecutable está configurado para parecer un documento de texto básico. Este ejecutable es un archivo de autoinstalación WinRAR SFX;consta de dos archivos: '134121811.js' (el RAT de JavaScript) y '2204722946' (el código fuente de C # para el keylogger). El archivo de configuración WinRAR SFX contiene comentarios en ruso e instrucciones para colocar ambos archivos en % TEMP% antes de ejecutar el archivo .JS con el nombre del ejecutable WinRAR SFX como argumento de línea de comando.

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-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

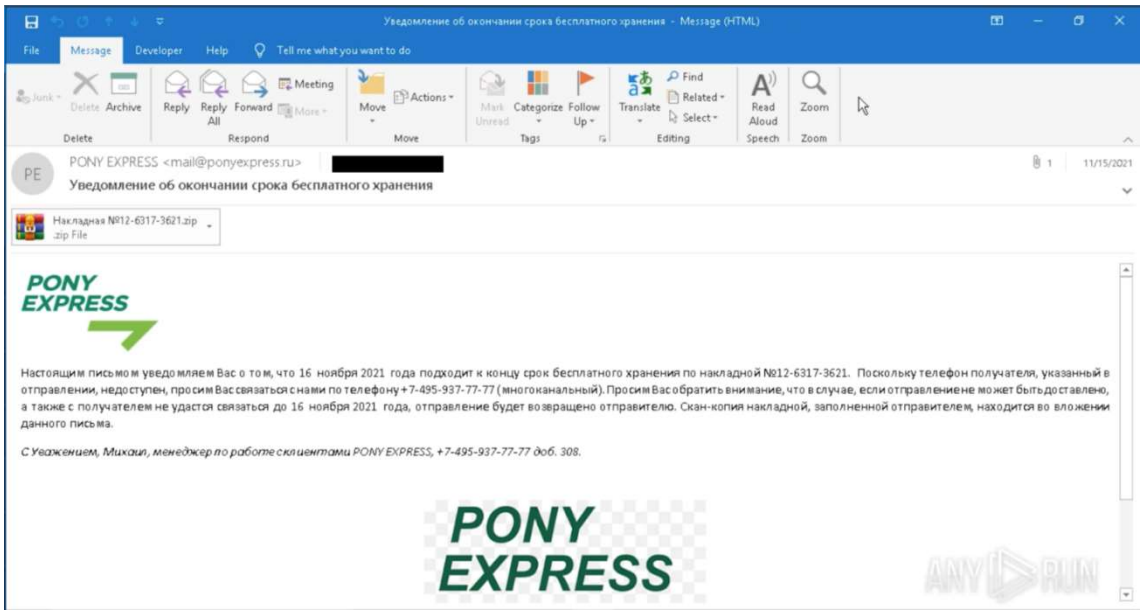

Figura 2: Correo electrónico utilizado en la distribución de malware DarkWatchman
Fuente: Prevailion

V. IMPACTO:

Una vez lanzado, DarkWatchmen, se ejecutará un script de PowerShell que compila el registrador de teclas usando el comando .NET CSC.exe y lo lanza a la memoria.

El keylogger se distribuye como código fuente C # ofuscado que se procesa y almacena en el registro como un comando de PowerShell codificado en Base64. Cuando se inicia el RAT, ejecuta este script de PowerShell que, a su vez, compila el keylogger (usando CSC), y, lo ejecuta.

En términos de la comunicación y la infraestructura de C2, los actores de DarkWatchman utilizan DGA (algoritmos de generación de dominio) con una lista inicial de 10 elementos para generar hasta 500 dominios al día.

Esto les proporciona una excelente capacidad de recuperación operativa y, al mismo tiempo, hace que el análisis y la supervisión de las comunicaciones sean un gran desafío.

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-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

Las capacidades funcionales de DarkWatchman son las siguientes:

- Ejecutar archivos EXE (con o sin la salida devuelta)
- Cargar archivos DLL
- Ejecutar comandos en la línea de comandos
- Ejecutar comandos WSH
- Ejecute varios comandos a través de WMI
- Ejecutar comandos de PowerShell
- Evaluar JavaScript
- Cargue archivos al servidor C2 desde la máquina víctima
- Detenga y desinstale de forma remota RAT y Keylogger
- Actualice de forma remota la dirección del servidor C2 o el tiempo de espera de llamada al hogar
- Actualice RAT y Keylogger de forma remota
- Configurar un JavaScript de inicio automático para que se ejecute en el inicio de RAT
- Un algoritmo de generación de dominio (DGA) para la resiliencia C2
- Si el usuario tiene permisos de administrador, elimina las instantáneas mediante vssadmin.exe

VI. INDICADORES DE COMPROMISO:

TIMESTAMP	HASH (SHA256)	NOMBRE DEL ARCHIVO
12/11/2021 12:31	409839f9c8327eff6208aeca4f7113f5a0abdfa97f266f404b14f9fa6ab1432f	Накладная №12-6317-3621.exe
12/11/2021 20:49	27c4e9f01e5142a021329163b074f0692a9b4e832e0b53a5e31d364fdbbcdef8	Накладная №12-6317-3621.zip
15/11/2021 0:24	a81d318f2d4caf23c50f3c280f88af3e3598dc1886711ff07f69371e41c924e4	mime-part–92187-14076.zip
15/11/2021 0:44	ce1eee6b86bbc352e9ad69b7e241dd7cf08dc60ced259087f72c33396f65093b	Накладная №12-6317-3621.exe
15/11/2021 1:10	ee9cd9a5ac70f7b55b52c02f54fd53186c294a940b2502bbe427d847dde83c85	134121811.js

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-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

TIMESTAMP	HASH (SHA256)	NOMBRE DEL ARCHIVO
15/11/2021 1:28	74c85df7a1f1af78fde252e52d0bfbdec75a626f613f080bd3ca8e3feee34ce5	[0]
15/11/2021 3:00	003ef083b27eb13b5ca6a39a7aaed359c5e7dae5a872cb569cdf69332bb56ad3	Накладная №12-6317-3621.exe
15/11/2021 4:06	e8681efd888395026e420acffe3df7b45e990d0a917aec3f09c741d4d8ccfba6	Накладная №12-6317-3621.exe
15/11/2021 4:17	b1d778643cd6667502c8fc7ff8a6f975420621cd929ee8bd2b1ff23d832eb8fe	Накладная №12-6317-3621.zip
15/11/2021 4:47	4aaee9f71d5f79d8d56c2e7d064cd45674f7bd6a0906ea635573bff83bd24e0b	Накладная №12-6317-3621.zip
15/11/2021 5:28	671ede00b5be118bab9238386fd3f7502ffa21f678d8f509b181d4a819524525	Уведомление об окончании срока бесплатного хранения.msg
15/11/2021 5:28	03af3bd4161f55797f597c0ab36a78342556fe7c578a7fc161ad5789eaa109f1	b77b41d5636145af853d4120d6be1e89
15/11/2021 5:37	003ef083b27eb13b5ca6a39a7aaed359c5e7dae5a872cb569cdf69332bb56ad3	Archivo
15/11/2021 5:38	ee9cd9a5ac70f7b55b52c02f54fd53186c294a940b2502bbe427d847dde83c85	Archivo
15/11/2021 5:39	4aaee9f71d5f79d8d56c2e7d064cd45674f7bd6a0906ea635573bff83bd24e0b	Archivo
15/11/2021 7:38	cd50319f992809ff49f3088f21c5ddf55305c62836997d1849cc350ad659cc98	Накладная №12-6317-3621.zip
15/11/2021 12:04	a81d318f2d4caf23c50f3c280f88af3e3598dc1886711ff07f69371e41c924e4	C: \ Usuarios \ usuario \ Escritorio \ adjuntos \ Накладная №12-6317-3621.zip
15/11/2021 12:14	b1d778643cd6667502c8fc7ff8a6f975420621cd929ee8bd2b1ff23d832eb8fe	C: \ Usuarios \ usuario \ Escritorio \ adjuntos \ Накладная №12-6317-3621.zip
15/11/2021 12:21	a81d318f2d4caf23c50f3c280f88af3e3598dc1886711ff07f69371e41c924e4	C: \ Usuarios \ usuario \ Escritorio \ adjuntos \ Накладная №12-6317-3621.zip

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-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

TIMESTAMP	HASH (SHA256)	NOMBRE DEL ARCHIVO
16/11/2021 2:06	3ac186a43d6e877b3804d2b56762f928b2cd2bd0e57225e8418082f4e05a10fb	671ede00b5be118bab9238386fd3f7502ffa21f678d8f509b181d4a819524525
16/11/2021 23:07	4aaee9f71d5f79d8d56c2e7d064cd45674f7bd6a0906ea635573bff83bd24e0b	Накладная №12-6317-3621.zip

Tabla 1: Indicadores de compromiso de Hash y nombre de archivo **Fuente:** Prevailion

VISTO POR PRIMERA VEZ	ULTIMA VEZ VISTO	FQDN	IP RESUELTA
26/02/2021	26/02/2021	smtp.673900 [.] ru	45 [.] 156.27.245
26/02/2021	26/02/2021	antispam.shiptechnology [.] ru	45 [.] 156.27.245
26/02/2021	26/02/2021	mail.shiptechnology [.] ru	45 [.] 156.27.245
13/04/2021	13/04/2021	mailx.psart [.] ru	45 [.] 156.27.245
20/04/2021	20/04/2021	mail2.vulkandlypotencii [.] ru	45 [.] 156.27.245
20/04/2021	20/04/2021	mx2.vulkandlypotencii [.] ru	45 [.] 156.27.245
20/04/2021	20/04/2021	mx7.vulkandlypotencii [.] ru	45 [.] 156.27.245
20/04/2021	20/04/2021	relay1.vulkandlypotencii [.] ru	45 [.] 156.27.245
13/07/2021	14/07/2021	mail.website-co-jp [.] tienda	45 [.] 156.27.245
25/10/2021	25/10/2021	pop3.tjsamy [.] cn	45 [.] 156.27.245
10/11/2021	13/11/2021	mail.rentbikespb [.] ru	45 [.] 156.27.245
14/11/2021	15/11/2021	smtp.rentbikespb [.] ru	45 [.] 156.27.245
24/11/2021	27/11/2021	smtp.e2cs3v6 [.] cn	45 [.] 156.27.245

Tabla 2: Indicadores de compromiso de dirección de dominio y número de IP. **Fuente:** Prevailion

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-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-dic-2021	**MALWARE "DARKWATCHMAN" UTILIZA EL REGISTRO DE WINDOWS PARA EVADIR DETECCIÓN**	V 1.0

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.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Mantener el control del uso de dispositivos de almacenamiento externos.
- Fortalecer las políticas de seguridad para evitar ser víctimas de cualquier técnica de ingeniería social.
- Mantener actualizados y, en funcionamiento, el software antivirus en cada computador personal o Institucional.
- Identificar y suspender el acceso de usuarios que exhiban una actividad inusual.
- 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.
- Actualizar las firmas de los dispositivos de seguridad perimetral/enpoint con las descritas en las tablas número 1 y número 2

VIII. REFERENCIAS:

Lakshmanan, R. (16 de diciembre de 21). TheHackerNews. Obtenido de TheHackerNews: https://thehackernews.com/2021/12/new-fileless-malware-uses-windows.html

Matt Stafford and Sherman Smith. (14 de diciembre de 2021). Prevailion. Obtenido de https://www.prevailion.com/darkwatchman-new-fileness-techniques/

Toulas, B. (19 de diciembre de 2021). Bleeping Computer. Obtenido de https://www.bleepingcomputer.com/news/security/new-stealthy-darkwatchman-malware-hides-in-the-windows-registry/

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