2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Lucha contra el Ransomware con validacion del SOC en tiempo real

By Daniel Regalado

Chief Offensive Security @ Metabase Q

daniel.regalado@metabaseq.com

ASOCIACION BANCARIA DE PANAMA

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Agenda

- Que es el Ransomware?
- Porque sigue en aumento?
- Rompiendo paradigmas
- Propuesta de Solución
- Takeaways
- Q & A

Quien soy yo?

- Ingeniero en Sistemas computacionales
- Dedicado a la Ciberseguridad desde el 2003
- He trabajado en los equipos de Research de Symantec, FireEye/Mandiant y Palo Alto Networks en Silicon Valley, USA
- Descubriendo y analizando malware de ATMs desde el 2013
- Analizando Advanced Persistent Threats (APTs) desde el 2014
- Ahora con Metabase Q, creación del primer Breach & Attack Simulation Product con Inteligencia Artificial
- Creación de equipo de Threat Intelligence dedicado a LATAM
- Conferencista en RSA San Francisco, RECon Canada y

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Ransomware

Que es y por qué debemos preocuparnos?

- Es un tipo de Malware que:
  1. Exfiltra información confidencial de la Organización:
     - Contratos, patentes, codigo fuente, informacion personal, resultados de auditoria, planes estrategicos, etc.
  2. Cifra dichos documentos confidenciales
  3. Bloquea equipos afectando la operación de los servicios
  4. Se mueve lateralmente por la red para entrar a un nuevo host y repetir las pasos 1, 2 y 3
  5. Amenazan a la Organización con publicar la información sensible sino se recibe el pago correspondiente

Ransomware en LATAM

En donde estan las víctimas?

2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

WinDev2102Eval (Estado actual) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Search

File Home Send / Receive View Help

New Email | Delete | Archive | Move | Reply | Reply All | Forward | Move to: ? | To Manager | Team Email | Unread/ Read | Search People | Read Aloud | Get Add-ins

Favorites

ocelot_rh@outlook.com

- Inbox
- Borradores
- Elementos enviados
- **Elementos eliminados**
- Archivo
- Bandeja de salida
- Correo no deseado
- Historial de conversaciones
- Suscripciones de RSS
- Search Folders

Elementos eliminados By Date

Recover items recently removed from this folder

We didn't find anything to show here.

Items: 0

Elementos elimina...

Escribe aquí para buscar

Actividades VirtualBoxVM 19 de ago 18:50

Iratrog-Server-Ubuntu [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal Thu 19:49

ubuntu@ubuntu1804: ~/Documents/Iratrog-consol-ubuntu/Iratrog-consol/Iratrog-consol

File Edit View Search Terminal Tabs Help

ubuntu@ubuntu1804: ~/Downloads/ngrok-stable-... | ubuntu@ubuntu1804: ~/Downloads/ngrok-stable-... | ubuntu@ubuntu1804: ~/Documents/Iratrog-cons...

```
ubuntu@ubuntu1804:~/Documents/Iratrog-consol-ubuntu/Iratrog-consol
/Iratrog-consol$ sudo dotnet run -f net5.0
```

Maquina de la victima

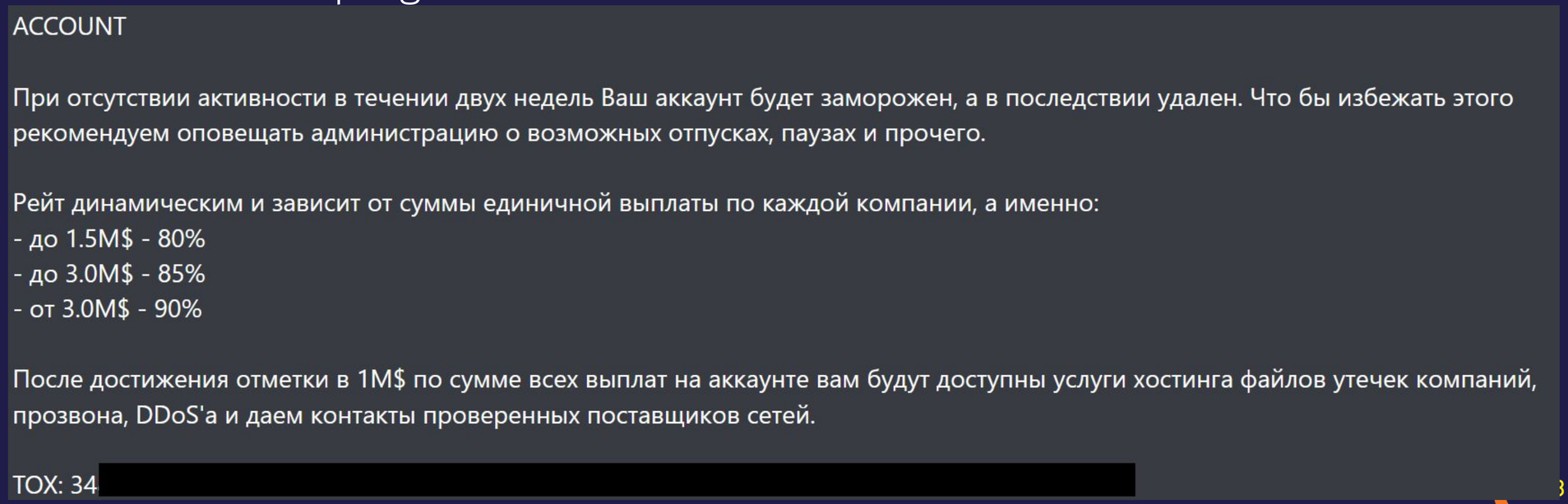
OCELOT SERVER

Ctrl Derecho

Ransomware

Por que siguen en aumento las víctimas?

1. Ransomware as a Service (RaaS):
   a) Es una renta de infraestructura donde es mas facil lanzar una campana de infección sin conocimientos técnicos
   b) Blackcat Partner program:


ACCOUNT

При отсутствии активности в течении двух недель Ваш аккаунт будет заморожен, а в последствии удален. Что бы избежать этого рекомендуем оповещать администрацию о возможных отпусках, паузах и прочего.

Рейт динамическим и зависит от суммы единичной выплаты по каждой компании, а именно:
- до 1.5M$ - 80%
- до 3.0M$ - 85%
- от 3.0M$ - 90%

После достижения отметки в 1M$ по сумме всех выплат на аккаунте вам будут доступны услуги хостинга файлов утечек компаний, прозвона, DDoS'a и даем контакты проверенных поставщиков сетей.

TOX: 34[redacted]

Source: **https://www.metabaseq.com/how-does-alphv-operate-the-raas-membership-program/**

Ransomware

Por que siguen en aumento las víctimas?

2. El enfoque de fortalecimiento esta incompleto

a) Los ejercicios de pentesting, si son hechos por una consultoría de calidad, siempre encontraran nuevas vulnerabilidades

b) Los ejercicios de Red Team terminan encontrando nuevas infecciones (malware)

c) El enfoque no deberia ser en si somos vulnerables o no, deberiamos asumir que si, y ademas de encontrar vulnerabilidades (pentesting) o debilidades en deteccion de malware (Red Team), tambien deberiamos enfocarnos en mejorar nuestro nivel de resiliencia

✔ Que capacidad temenos de contener, responder y recuperarnos ante un ataque de Ransomware

Ransomware

Por que siguen en aumento las víctimas?

3. La postura de las Organizaciones es reactiva y no proactiva

a) Cuantos ejercicios reales de infección de Ransomware haces al mes (no al año)
b) Ejecutas malware real (controlado) que burle las medidas de deteción y se mueva por la Red?
c) Durante estos ejercicios mides técnicas de MITRE no siendo detectadas?
d) Validas el proceso de respuesta a incidentes? El cual debería incluir:
   - ✔ Proceso de notificación inicial y War room
   - ✔ Seguimiento de política de la empresa en cuanto al pago del rescate
   - ✔ Negociación con el atacante
   - ✔ Pago en bitcoins de form anónima

Ransomware

Por que siguen en aumento las víctimas?

4. La postura de las Organizaciones es reactiva y no proactiva

a) Como medimos la capacidad de detección y respuesta de nuestro SOC?
b) Sabemos el % de visibilidad ante distintas infecciones?
   ✔ No podemos detener lo que no podemos ver
c) Sabemos el tiempo que pasa entre una infección y cuando el SOC lo identifica (Time to Detect)?
d) Asi como el tiempo que pasa una vez identicado hasta que el incidente es contenido y el equipo recuperado (Time to Response)?

Rompiendo paradigmas

Debemos actualizar nuestra postura

1. CISO: “No quiero agentes instalados en mis endpoints”

a) Toda infección necesita un humano que caiga en el engaño, dandole doble click al link malicioso, descargando software, abriendo documentos, etc
   - ✔ La excepcion es un zero day remoto, muy poco comun

b) Los agentes juegan el papel de los empleados engañados en la Organización y ayudan a fortalecer mejor el SOC (ver el siguiente slide)

c) Sin agente, la empresa que diga que puede infectar con Ransomware, miente

d) Bonus extra: Estos agentes no consumen como un AV/EDR, son muy ligeros

Rompiendo paradigmas

Debemos actualizar nuestra postura

3. El SOC siempre sabe cuando hay un ejercicio ofensivo
   a) Poner un nombre diferente al equipo, cambiar la IP, no decirle nada al equipo defensivo, al segundo dia, el SOC ya sabe que es un ejercicio y **se relaja**
   b) Pero que pasa si la infección sale de un nodo de un empleado corporativo?
      - ✔ Como distingue el SOC un simulación de un ataque real?
      - ✔ Esta obligado a responder sin relajarse
   c) Entre mas nodos detonando infecciones en distintos puntos de la red (agentes) mejor fortaleceremos el SOC porque aumentamos su capacidad de detección y respuesta

Propuesta de solución

Como podemos ir un paso adelante de los atacantes

1. Infectar con distintas variantes de Ransomware real de forma automatizada
2. Las infecciones deben aparecer de forma asíncrona desde distintos nodos en la red
   a) Y si es posible, incluso desde equipos de usuarios finales
3. Medir y mejorar el algoritmo de Machine Learning de los Productos de Seguridad:
   a) Los algoritmos se entrenan para identificar ataques no conocidos de forma automática
   b) El simulador debe tener Inteligencia artificial que genere nuevos ataques desconocidos constantemente

Propuesta de solución

Como podemos ir un paso adelante de los atacantes

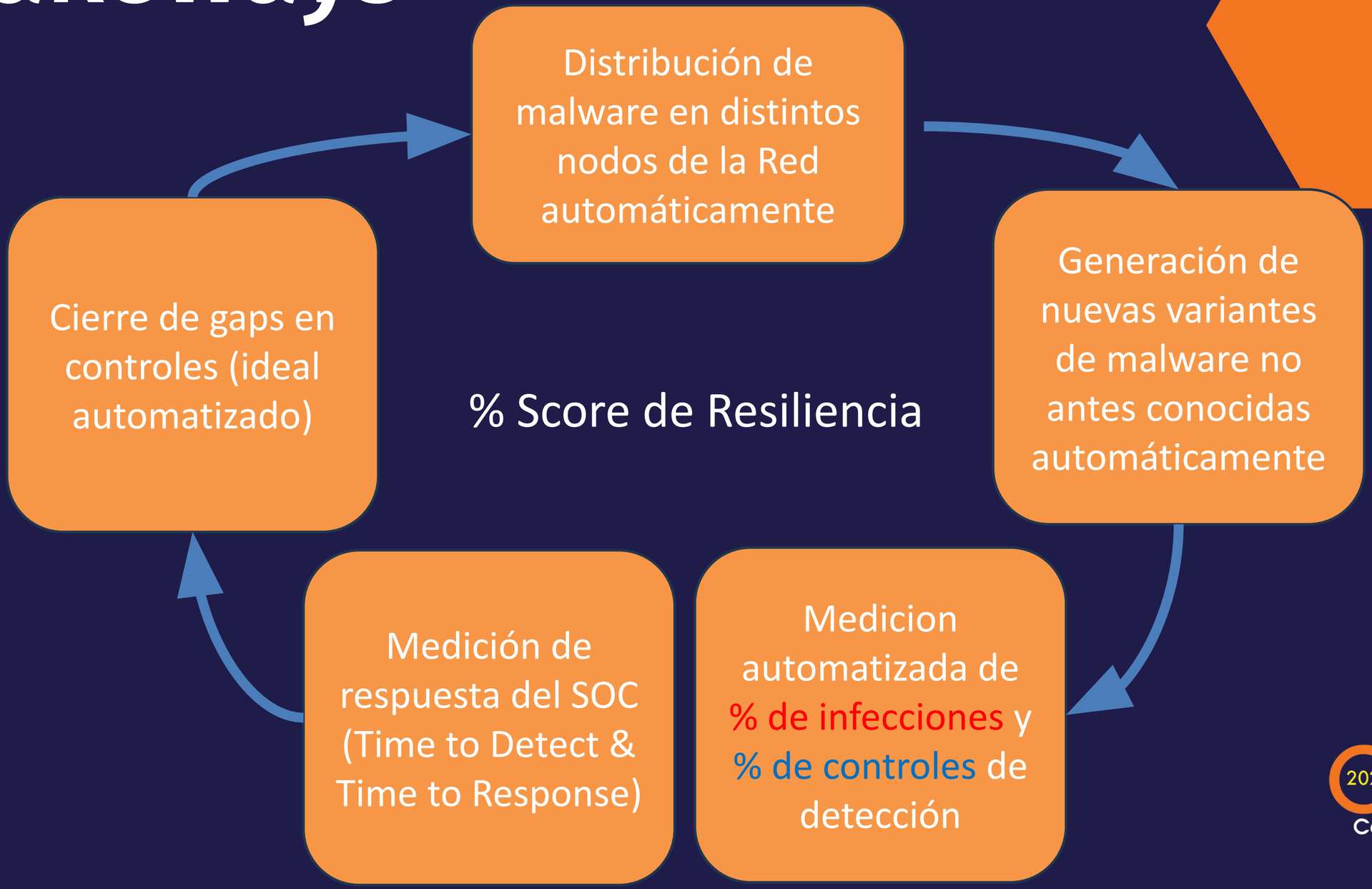
4. Medir tiempos de actualización de detecciones automaticas en los productos:
   a) El simulador debe medir el tiempo que tarda un malware no detectado inicialmente, en ser detectado automáticamente
   b) A nivel granular de las técnicas de MITRE
5. Los ejercicios de infección deben ser basados en las tecnologías y procesos que la Organización quiera medir:
   a) Infección de Ransomware? Movimiento Lateral a activos críticos? Accesos por VPN de consultores? Infección desde VDI?
6. Mediante un equipo de Threat intelligence, identificar los actores que estan enfocados en la Organización, para replicar sus técnicas en el corporativo

Propuesta de solución

Como podemos ir un paso adelante de los atacantes

7. La identificación de controles débiles o ausentes en detección debe ser automatizada
8. Debe haber un score de resiliencia entre infecciones vs controles detectivos que permita medir la mejora constante

Takeways



Constante medición

Resumen de la simulación
Technology + Soc

Escenarios
80

Resilience score
41 %

Fases
Endpoint, Phishing, Lateral Movement, Exfiltration

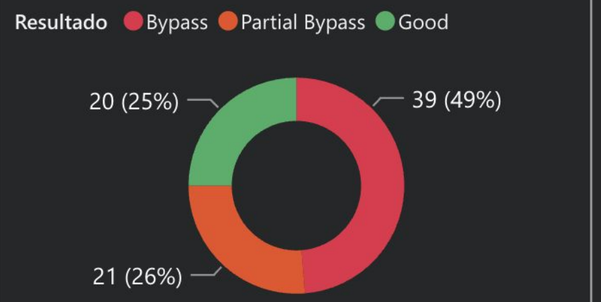
Sistema Operativo
10 pro

Controles de seguridad

Tipo	Nombre
SEGW	TrendMicro Email Security
AV	Trellix Endpoint Security
AV	Apex One

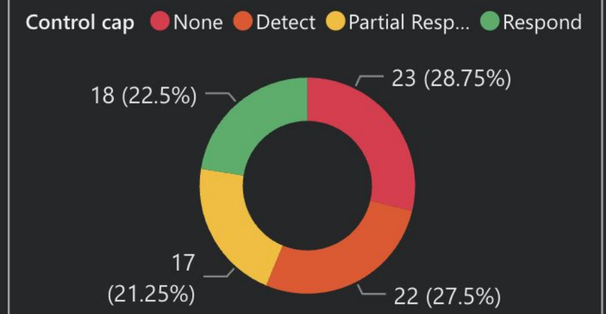
Porcentaje exitoso de infecciones
75 %

Desglose de resultados



Porcentaje exitoso de detecciones
56 %

Desglose de resultados



2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Q&A

Thanks!

daniel.regalado@metabaseq.com

@danuxx