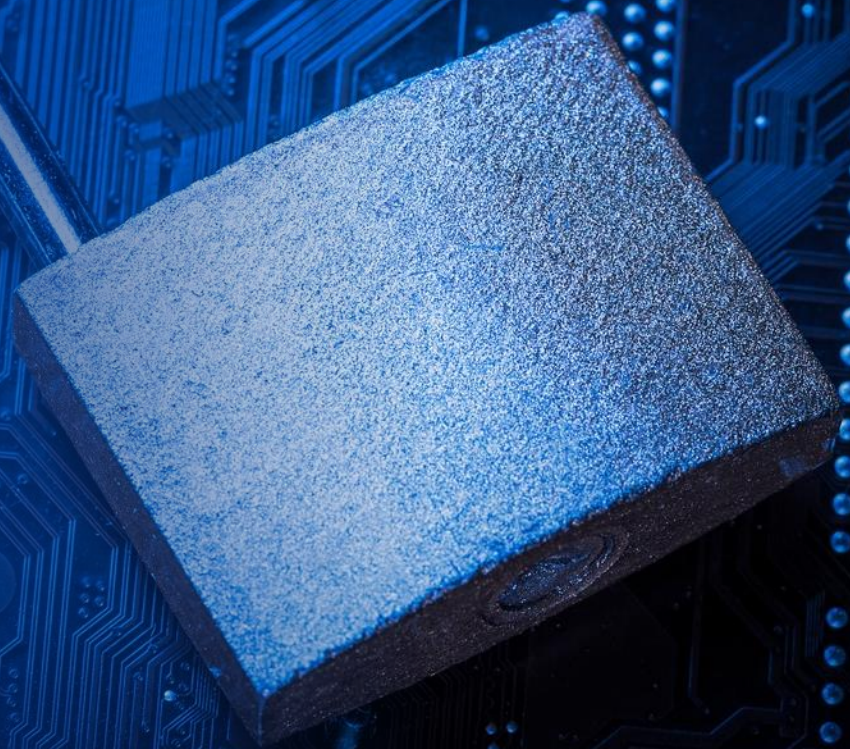
Marsh

Descifrando el ransomware Gazpromlock

Análisis técnico del ciclo de ataque



Latinoamérica
Febrero 2024

Cyber Risk Consulting
Marsh Advisory

Panorama General

Descripción General

El ransomware Gazpromlock inició sus operaciones en marzo 2023, es un software malicioso, capaz de bloquear los sistemas de una compañía y exigir el pago de un rescate para recuperar los sistemas afectados.

Gazpromlock reutiliza el código fuente de Conti Ransomware (este código, es la base sobre la cual se construyen aplicaciones y sistemas personalizados)

El código fuente de Conti fue utilizado como base para construir y personalizar nuevas muestras de ransomware.

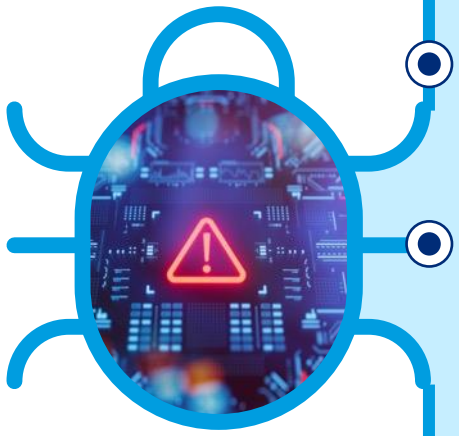
Al desarticularse el grupo de ransomware Conti, sus miembros se separaron en pequeñas células, mientras que otros se unieron a grupos como: **HelloKitty, AvosLoker, Hive, BlackCat, BlackByte.**

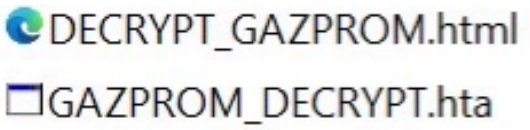
Industrias objetivo para las campañas de ransomware:

Aviación y espacio	Química	Comunicaciones, medios y tecnología	Construcción	Educación	Energía y potencia	Medio Ambiente
Instituciones financieras	Salud	Hotelería y juegos de azar	Infraestructura	Ciencias de la vida	Automóviles y manufactura	Marina
Minería	Entidad pública	Ferrocarril	Inmobiliario	Venta al por menor y al por mayor, Alimentación y bebidas	Deportes, entretenimiento y eventos	Transporte

[1] Malware Hunter Team [2] Bleeping Computer – Conti Ransomware Source code leaked [3] Bleeping Computer – Conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/

Objetivos del ransomware Gazpromlock





Nombre: Gazpromlock

Objetivo: Cifrado de archivos y extorsión; Este ransomware, al igual que otras familias, cifra los archivos del equipo de la víctima y una vez que se han modificado, se les agrega la extensión .**GAZPROM**.

Rescate: Esta amenaza, genera en el equipo de la víctima dos archivos que contienen la nota de rescate, uno con extensión **.HTML** y otro con extensión **.HTA** mostrando una imagen **ASCII (**esta es un medio artístico que utiliza recursos computarizados fundamentados en los caracteres de impresión del Código Estándar) e indica a la víctima una dirección de Telegram a nombre de **@gazpromlock** para iniciar la negociación.

Descifrado: A la víctima se le proporciona en la nota de rescate una llave de descifrado, la cual debe ser proporcionada al atacante con el propósito de obtener el supuesto programa para descifrar.

Víctimas: Similar a otros grupos de ransomware, se tiene la hipótesis de que esta amenaza elige a sus víctimas independientemente del sector o tamaño de la compañía.

Industrias afectadas: En fuentes abiertas no se observan industrias que públicamente hayan documentado afectaciones por este ransomware. A la fecha se observa que la última muestra relacionada con Gazpromlock fue subida a plataformas de análisis de amenazas en noviembre 2023.

Presencia en Latinoamérica: De acuerdo al caso de estudio analizado por el Equipo de Respuesta ante Ciberincidentes de Marsh Advisory, se tiene una confianza alta de que este ransomware ha operado en América Latina.

Línea de tiempo y actividad del atacante

El ciclo de ataque de Gazpromlock dura un promedio de 30 días desde que reconoce e infiltra a su víctima, hasta que llega a la etapa de impacto (cifrado)

Etapa inicial del ataque | **Etapa de pre-ejecución del ataque** | **Etapa de impacto**

Ciclo de ataque

Semana 1

Escaneo de activos web expuestos

Explotación de vulnerabilidades web

Validación de vulnerabilidades

Semana 2

Uso de cuentas válidas
- Elevación de privilegios
- Descarga de arsenal inicial (escáner de red, clientes FTP)

Creación de webshells para garantizar el acceso

Semana 3

Uso de LOLBINS
- Descarga de arsenal adicional
- Evasión de defensas

Uso de backdoors y herramientas de túneles
- Persistencia
- Movimientos laterales

Comunicación C&C

Ejecución de herramientas de simulación de adversarios
- Post explotación
- Persistencia
- Ejecución de scripts maliciosos

Semana 4

Cifrado
- Ejecución masiva del ransomware en la red de la víctima

Uso de cuentas válidas
- Evasión de defensas
- Diseminación de artefactos maliciosos

Modelo Diamante

De acuerdo con las capacidades y herramientas observadas, en el caso de estudio se aprecia que los operadores del grupo cuentan con conocimientos, capacidades e infraestructura de nivel medio a alto.

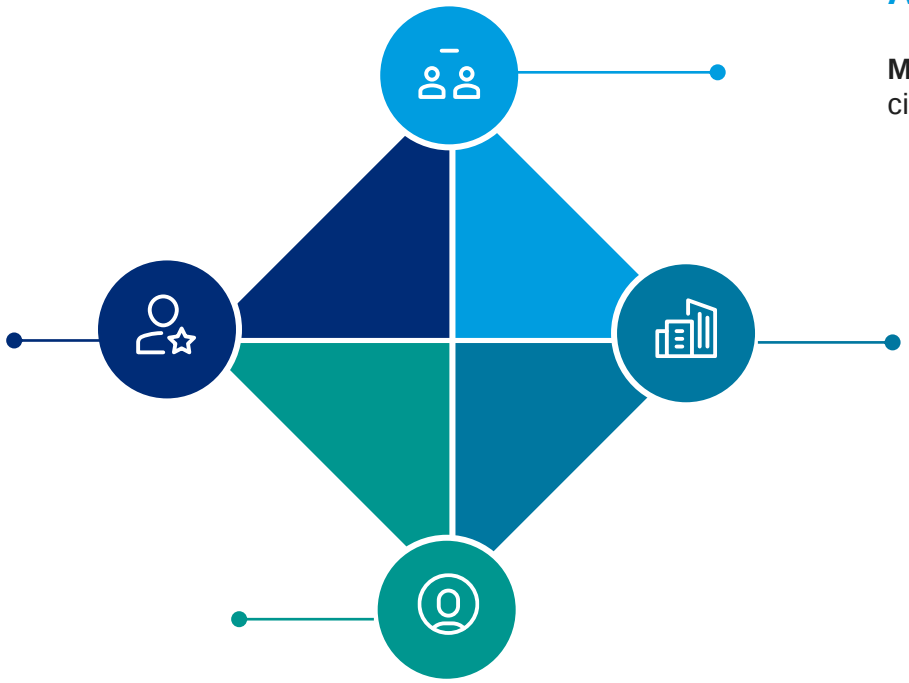
Capacidades

- Explotación de vulnerabilidades web de manera remota y del lado del servidor
- Uso de frameworks de simulación de adversarios (Cobalt Strike)
- Creación/modificación de scripts en powershell u otros lenguajes
- Uso de LOLBINS, Suelen ser ciberataques y se basan en unos pocos componentes comunes del sistema operativo.
-

Víctimas sin información publica

Herramientas usadas en la cadena de ataque:

- Mimikats
- Metasploit
- Cobalt Strike
- Chisel
- Interact
- Andesk
- Advanced IP scanner
- Webshells



Adversario - Gazpromlock

Motivaciones: Robo de información y ciberextorsión

Infraestructura

- Direcciones IP en Europa (C&C)
- Servicios de hosting y mensajería para alojamiento de artefactos maliciosos (anonfiles, discord)
- AnyDesk, WinSCP u otro software de administración remota

¿Sabe cómo afrontar estas amenazas? Escanee el código y conozca más

MITRE ATT&CK

Herramientas utilizadas por los operadores

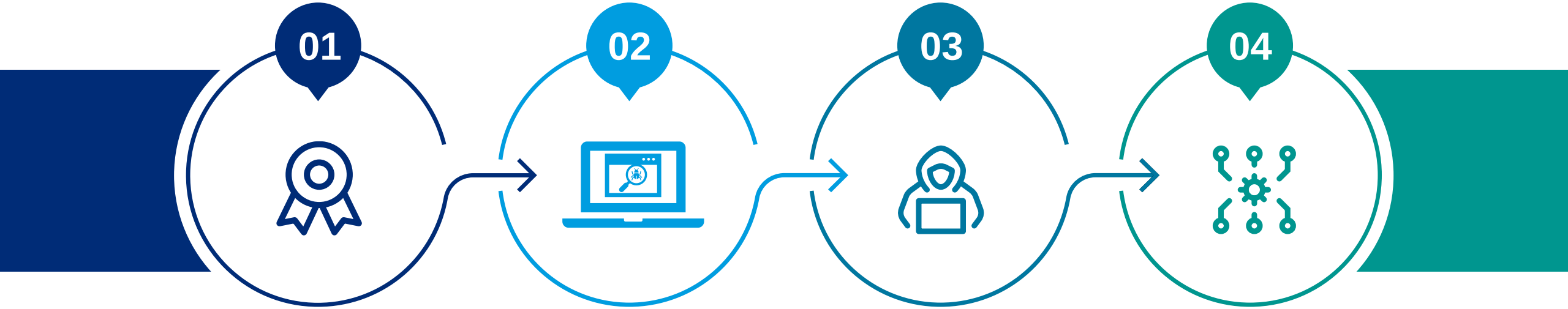
- Metasploit
- Cobalt Strike
- Impacket
- Chisel
- Interact sh
- Anydesk
- Advanced IP scanner
- Webshells

Tácticas y técnicas del framework de MITRE ATT&CK utilizadas por los operadores del ransomware Gazpromlock

Táctica	Técnicas						
Reconnaissance	T1595 Escaneo Activo						
Initial Access	T1190 Exploit Public-Facing Application						
Execution	T1203 Exploitation for client Execution	T1059.001 Command and Scripting Interpreter:PowerShell					
Persistance	T1505 Server Software Component: WebShell	T1098 Account Manipulation					
Privilege escalation	T1078 Valid Accounts	T1068 Exploitation for Privilege Escalation	T1484 Domain Policy Modification				
Defense Evation	T1564.001 Hide Artifacts:Hidden Files and directories	T1036.007 Masquerading: Double File Extension	T1570 Lateral Tool Transfer	T1562 Impair Defenses	T1070.004 Indicator Removal: File Deletion	T1036 Masquerading	T1112 Modify Registry
Credential Access	T1003.001 OS Credential Dumping: LSASS Memory	T1110.001 Brute Force: Password Guessing					
Discovery	T1046 Network Service Discovery	T1082 System Information Discovery	T1016 System Network Configuration Discovery				
Lateral Movement	T1563.001 Remote Service Session Hijacking: SSH Hijacking	T1021 Remote Services: Remote Desktop Protocol					
Command and Control	T1572 Protocol Tunneling	T1132.001 Data Encoding					
Impact	T1489 Service Stop	T1486 Data Encrypted for impact					

Resumen de las etapas clave del ataque

El Equipo de Respuesta ante Ciberincidentes de Marsh Advisory observa cuatro etapas clave en la cadena de ataque de este ransomware



Reconocimiento

- Identificación de la infraestructura de la víctima
- Escaneo de vulnerabilidades web

Compromiso inicial y persistencia

- Explotación de vulnerabilidades web
- Acceso inicial
- Persistencia mediante uso de webshells

Movimientos laterales y planeación del ataque

- Uso de cuentas privilegiadas
- Uso de lolbins para movimientos laterales y descarga de payloads
- Uso de frameworks de simulación de adversarios

Cifrado

- Uso de cuentas privilegiadas para la diseminación del ransomware
- Cifrado mediante el ransomware Gazpromlock

Indicadores de compromiso

Hashes SHA1: A continuación, encontrará los hashes de algunos de los principales indicadores de compromiso asociados a esta amenaza:
2e3d18086b8a6b45469a9b3f1d05a1e5a1a94515
7a86238c994cfdf137d0a5ebd4b96afefbd8a76f
E8e1805f24e91bc5613edca043002877ac3e1bf7
86a5940293632c0ee125efda8f03fd16f7e9f44f
1e3dcf95cd2b5b193b3937d457c14021b9222dde
675fe7c66176f2dc3ffb8936798fd8bf8a5a1387
1c42de9aa0bd742b7dac2d34e9bc697c8ae97864
13cf1dc11a066e9d4953b8fd19cffe01c60c763e
A7bcfa4116d5f67b4fade18cbad34e4726276733
79599b7925b8b999ab8c8186ef0b94de2d21bd7e
1157c3cbe87405459dc6523ea10bac1d553c379e

Origen de las direcciones IP utilizadas por el ransomware Gazpromlock

Conclusiones

- El ransomware Gazpromlock es una amenaza que inició sus operaciones en marzo del año 2023 y es posible que continúe activo.
- Aunque no se tiene ataques públicamente documentados, se tiene una alta confianza de que ha operado en Latinoamérica.
- De acuerdo al caso de estudio analizado, se observa un nivel de sofisticación de nivel medio – alto. Al ser esta amenaza creada a partir del código fuente del extinto grupo Conti, se encuentran similitudes en sus TTPs.
- Las tácticas y técnicas de ataque utilizadas por el operador u operadores del ransomware Gazpromlock son similares a las empleadas por otras familias de ransomware como:
  - PYSA
  - Lorenz
  - Conti, entre otras
- Los ciberataques que implican ransomware se encuentran en aumento y son una de las amenazas más activas de forma global. Le invitamos a leer los siguientes artículos para conocer más sobre este ataque y cómo protegerse:
  - Caso IFX Networks: ¿cómo prepararse para un ataque de ransomware?
    ¿Cómo actuar en caso de un ataque de ransomware a un tercero?

¿Cómo puede ayudar Marsh?

Cyber Incident Management

Prevención

- Evaluación de las capacidades de respuesta ante ciberincidentes
- Desarrollo del Plan de Respuesta ante Ciberincidentes y Playbooks
- Desarrollo del protocolo de respuesta organizacional frente a ransomware
- Desarrollo del plan de recuperación tecnológica en caso de ransomware
- Entrenamiento en gestión de cibercrisis
- Implementación de Cygnvs
- Evaluación y remediación de riesgos en la superficie de ataque (ASM)
- Cyber Threat Hunting

Prueba

- Simulación de cibercrisis a nivel del Comité de Crisis
- Simulación de respuesta ante ciberincidentes a nivel táctico/operativo
- Pruebas de Red Team
- Simulación de adversarios y malware

Respuesta

- Respuesta ante ciberincidentes, incluyendo:
  - Gestión de cibercrisis
  - Recomendación de terceros (p.e. firmas legales, empresas de relaciones públicas, centrales de monitoreo, etc.)
  - Análisis forense digital
  - Ciberinteligencia
  - Cyber Threat Hunting
  - Entre otros

Post

- Cyber Claims
- Taller de lecciones aprendidas
- Implementación de mejoras de seguridad

Visita nuestro centro de recursos de respuesta ante incidentes cibernéticos

Principales servicios de Consultoría en Riesgo Cibernético

Herramientas especializadas

Estrategia y gobierno

- Diagnóstico de seguridad y ciberseguridad
- Desarrollo de la estrategia de ciberseguridad
- Diagnóstico de ciberseguridad ICS/SCADA
- Diagnóstico de ciberseguridad Cloud
- Diagnóstico de prevención del fraude digital
- Definición de políticas y procedimientos de seguridad de la información y ciberseguridad
- Definición del dashboard ejecutivo de ciberseguridad
- Tercerización de la Oficina de Seguridad
- Diagnóstico frente a ransomware

Cumplimiento

- Auditoría de Controles Generales de TI
- Evaluación de cumplimiento regulatorio
- Implementación de requerimientos regulatorios
- Diagnóstico de PCI DSS
- Desarrollo del diagrama de flujo de datos del tarjetahabiente (PCI DSS)
- Diagnóstico de Protección de Datos Personales
- Implementación del programa de privacidad

Gestión y cuantificación de riesgos

- Identificación y clasificación de activos de información
- Definición de la metodología cualitativa y cuantitativa de gestión de riesgos de seguridad de la información y ciberseguridad
- Evaluación de riesgos de seguridad de la información y ciberseguridad
- Cuantificación de la exposición al riesgo cibernético (CyberXQ, Cyber RFO, Marsh Blue[i] Cyber)

Gestión de riesgos con terceros

- Definición del marco de gestión de ciber-riesgos con terceros (TPRM - Cyber)
- Evaluación de riesgos de seguridad de la información y ciberseguridad con terceros
- Due-diligence de ciberseguridad para fusiones y adquisiciones (M&A)

Desarrollo seguro de software

- Desarrollo de la metodología de desarrollo seguro de software
- Capacitación de desarrollo seguro
- Revisión de seguridad en el código fuente
- Web & Mobile Application Hacking
- Revisión de estándares ASVS y MASVS

Seguridad defensiva y ofensiva

- Ciberinteligencia (búsqueda de información fugada en Internet)
- Gestión de vulnerabilidades
- Revisión de la configuración de ciberseguridad (hardening)
- Pruebas controladas de intrusión (ethical hacking)
- Web & Mobile Application Hacking
- Pruebas de ingeniería social
- Pruebas de red team

Cyber Risk Analytics

Cultura de ciberseguridad

- Cyber Chemistry – Evaluación de cultura de ciberseguridad
- Desarrollo del programa de concientización en ciberseguridad
- Capacitaciones especializadas en ciberseguridad
- Evaluación de las capacidades del equipo de Seguridad de la Información y Ciberseguridad*

Seguro de riesgo cibernético

- Autoevaluación de madurez de ciberseguridad para el seguro de riesgo cibernético*
- Cyber IDEAL - Estimación de pérdidas para el seguro (brecha de privacidad, ransomware y lucro cesante de un ciberataque)*
- Cybersecurity Rating (BitSight y SecurityScorecard)*
- Evaluación de riesgos para el seguro cyber
- Contratación del seguro de riesgo cibernético*
- Cyber Claims & Crisis Orchestration (soporte en el reclamo de siniestros cyber)

Gestión de incidentes

- Respuesta ante ciberincidentes y análisis forense
- Evaluación de las capacidades de respuesta ante ciberincidentes
- Desarrollo del plan de respuesta ante ciberincidentes y playbooks
- Desarrollo del protocolo organizacional de ransomware
- Simulaciones de cibercrisis / Cyber war games
- Simulación de adversarios y malware
- Cyber Threat Hunting (cacería de ciberamenazas)
- Desarrollo del plan de mejoras post-incidente

Para conocer cómo podemos apoyar a su organización en la gestión del riesgo cibernético, póngase en contacto con nuestros profesionales.

Gerardo Herrera

Director de Marsh Advisory para Latinoamérica
Marsh Advisory
Gerardo.Herrera@Marsh.com

Oscar Santoyo

Líder de Servicios de Respuesta ante Ciberincidentes para Latinoamérica
Marsh Advisory
Oscar.Santoyo@Marsh.com

Edson Villar

Líder de Consultoría en Riesgo Cibernético para Latinoamérica
Marsh Advisory
Edson.Villar@Marsh.com

Armando Pérez

Consultor Senior de Servicios de Respuesta ante Ciberincidentes
Marsh Advisory
Armando.Perez@Marsh.com