Grupo de ransomware: Clop

Resumen ejecutivo

Clop (también conocido como Cl0p) es un **grupo cibercriminal especializado en ransomware y extorsión de datos**. Desde su aparición en 2019 ha evolucionado rápidamente hasta convertirse en una de las ciberamenazas más graves para organizaciones públicas y privadas. Clop opera mediante campañas sofisticadas que combinan intrusiones en redes corporativas, cifrado de información crítica y robo de datos confidenciales para ejercer presión sobre sus víctimas. Su **modelo de ataque implica la doble extorsión**, no solo inutiliza sistemas mediante cifrado de archivos, sino que además exfiltra información sensible con la que amenaza a las organizaciones. Esto lo convierte en **una amenaza de alto impacto**, capaz de interrumpir operaciones esenciales y causar perjuicios económicos y reputacionales significativos a sus objetivos.

El **riesgo** que Clop representa es **elevado para todo tipo de organizaciones**, abarcando tanto al sector público como al privado, ya que la capacidad de Clop para explotar vulnerabilidades desconocidas, así como para llevar a cabo campañas de phishing dirigidas, le permite atacar incluso organizaciones con una buena madurez en ciberseguridad. Una vez dentro de las redes de sus victimas, sus tácticas de movimiento lateral le facilitan escalar privilegios y propagarse rápidamente por la red corporativa, maximizando el alcance del daño antes de ser detectado. Además, el **impacto de esta amenaza implica la inhabilitación de los sistemas afectados y la posible divulgación de datos sensibles**.

Por todo ello, se requiere un **enfoque integral y proactivo de ciberseguridad** para mitigar la amenaza. Fortaleciendo las defensas antes de un incidente mediante medidas como la actualización constante de sistemas, la segmentación de redes, la autenticación multifactor para proteger accesos remotos, y la concienciación del personal sobre ciberseguridad.

Grupo de ransomware: Clop

Clop es un grupo de ciberdelincuencia organizado dedicado principalmente a **ataques de ransomware con fines de lucro**. Desde sus inicios, Clop ha mostrado un **modelo de extorsión dual** a través del cifrado de información sensible y la amenaza de filtración de dicha información. El grupo surgió en febrero de 2019 como una variante del ransomware CryptoMix y con el paso del tiempo se transformó en una **plataforma RaaS** (Ransomware-as-a-Service), reclutando afiliados para ampliar el alcance de sus operaciones. Durante 2021, varias agencias de seguridad realizaron algunas intervenciones contra Clop, lo que generó una breve interrupción de su actividad. Sin embargo, en 2022 reapareció de nuevo hasta el día de hoy.

En cuanto a su infraestructura y modus operandi, Clop cuenta con un **portal de filtraciones en la red Tor**, conocido como “Clop Leaks”, donde expone públicamente la información robada de las víctimas. Además, la comunicación con las víctimas suele establecerse a través de **direcciones de correo electrónico seguras o portales de negociación en Tor**.

Países y sectores afectados

Las operaciones de Clop han tenido un **alcance global**, concentrando buena parte de su actividad en **América del Norte y Europa**. En términos generales, Clop apunta contra **organizaciones con alta dependencia de sus sistemas digitales y datos**.

En cuanto a los sectores afectados, Clop se caracteriza por una **amplia diversificación de sus víctimas**. Entre los sectores más afectados destacan el **sector gubernamental, sector salud, educación e investigación, manufactura e industria, tecnología de la información, finanzas y servicios profesionales, sector de transporte y medios de comunicación**.

Análisis técnico

Clop utiliza diferentes vías de **acceso inicial**, como por ejemplo, campañas de **phishing con malware**, **explotación directa de servicios vulnerables expuestos** y potencialmente el **uso de credenciales comprometidas**. Una vez conseguido el acceso inicial, procede a extender su control sobre el entorno a través de la **elevación de privilegios** en la máquina comprometida. En paralelo, los operadores de Clop despliegan **herramientas de post-explotación** como Cobalt Strike y otras utilidades para **mapear la red interna**, con el objetivo de enumerar segmentos de red, identificar servidores críticos y grupos en Active Directory. Posteriormente, realiza **movimientos laterales** para pasar del punto de entrada inicial a otros sistemas de mayor valor a través del uso de credenciales y exploits.

Además, recopila grandes volúmenes de documentos, bases de datos y comunicaciones internas, priorizando aquellos con mayor valor. Estos **datos son enviados hacia servidores externos**, normalmente a través de canales cifrados. Finalmente, Clop aplica un **esquema de cifrado híbrido**, combinando algoritmos de cifrado simétrico con cifrado asimétrico para la seguridad de la clave.

Características técnicas principales:

- **Plataformas objetivo:** Clop afecta principalmente a sistemas Windows, Linux y entornos VMware ESXi, evidenciando su capacidad multiplataforma.

- **Uso de binarios legítimos (LOLBins):** Clop aprovecha herramientas y utilidades nativas del sistema operativo para pasar inadvertido (Living off the Land). Como por ejemplo, PowerShell y utilidades administrativas estándar (wmic, net, schtasks, entre otras).

- **Herramientas dañinas asociadas:** El arsenal de Clop incluye múltiples familias de malware y utilidades de ataque que son desplegadas a lo largo de la intrusión.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1566** — Phishing **T1566.001** — Phishing: Spearphishing Attachment **T1190** — Exploit Public-Facing Application **T1078** — Valid Accounts
Execution	**T1059.001** — Command and Scripting Interpreter: PowerShell **T1059.003** — Command and Scripting Interpreter: Windows Command Shell **T1204** — User Execution
Persistence	**T1505.003** — Server Software Component: Web Shell **T1546.011** — Event Triggered Execution: Application Shimming **T1547** — Boot or Logon Autostart Execution **T1543** — Create or modify system process: Windows service
Privilege Escalation	**T1068** — Exploitation for Privilege Escalation
Defense Evasion	**T1055** — Process Injection **T1070** — Indicator Removal **T1574** — Hijack Execution Flow **T1036** — Masquerading **T1562** — Impair Defenses **T1140** — Deobfuscate/Decode Files or Information
Discovery	**T1018** — Remote System Discovery **T1083** — File and Directory Discovery
Lateral Movement	**T1021.002** — Remote Services: SMB/Windows Admin Shares
Collection	**T1005** — Data from Local System
Command and Control	**T1071** — Application Layer Protocol **T1105** — Ingress Tool Transfer
Exfiltration	**T1041** — Exfiltration Over C2 Channel
Impact	**T1486** — Data Encrypted for Impact

Medidas de mitigación

Proactivas

- ❑ Implementar autenticación multifactor (MFA) para evitar accesos no autorizados. (T1078 – Valid Accounts)
- ❑ Mantener copias de seguridad seguras y probar restauraciones periódicas. (T1486 – Data Encrypted for Impact)
- ❑ Segmentar la red y limitar la visibilidad entre hosts, reduciendo el descubrimiento de procesos, sistemas y directorios. (T1083 – File/Directory Discovery)
- ❑ Auditar y limitar usuarios RDP y SSH, deshabilitar los servicios si no es necesario. (T1021 – Remote Services)
- ❑ Actualizar el software periódicamente empleando una correcta gestión de parches. (T1190 – Exploit Public-Facing Application)

Reactivas

- ❑ Monitorizar tráfico saliente y bloquear conexiones SMTP/FTP/HTTP no autorizadas usados para exfiltración. (T1041 – Exfiltration Over C2 Channel)
- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos, desactivar PowerShell cuando no sea necesario o usar el modo "Constrained Language“ para restringir el acceso. (T1059.001 – Command and Scripting Interpreter: PowerShell)
- ❑ Implementar sistemas de detección y prevención de intrusiones que permitan identificar tráfico anómalo o patrones de red asociados a malware. (T1071 – Application Layer Protocol)

Conclusiones y recomendaciones

El grupo de ransomware Clop representa una **amenaza significativa** que ha demostrado la capacidad de causar **un impacto severo en organizaciones de todos los tamaños y sectores**. Esto es debido a que Clop combina técnicas de ransomware avanzadas con una estrategia de extorsión agresiva, explotando vulnerabilidades y errores humanos para infiltrarse en redes corporativa. Y una vez dentro, llevar a cabo robos masivos de información y cifrado de sistemas críticos. Además, su **modelo de doble extorsión** ha ampliado la capacidad de este atacante, elevando el riesgo para las organizaciones y provocando posibles daños reputacionales, sanciones legales y comprometimiento la confianza pública.

Por todo ello, se recomienda **mantener los sistemas actualizados** y correctamente parcheados, especialmente aquellos expuestos a Internet. Asimismo, se recomienda fortalecer la autenticación y los accesos remotos a través de **autenticación multifactor** en todos los accesos externos y en las cuentas privilegiadas internas. De igual modo, es necesario mejorar la detección temprana mediante **soluciones EDR/XDR** e integrar **inteligencia de amenazas** en los sistemas de monitorización. Finalmente, se recomienda llevar a cabo una **segmentación de la red y aislar las copias de seguridad**.

