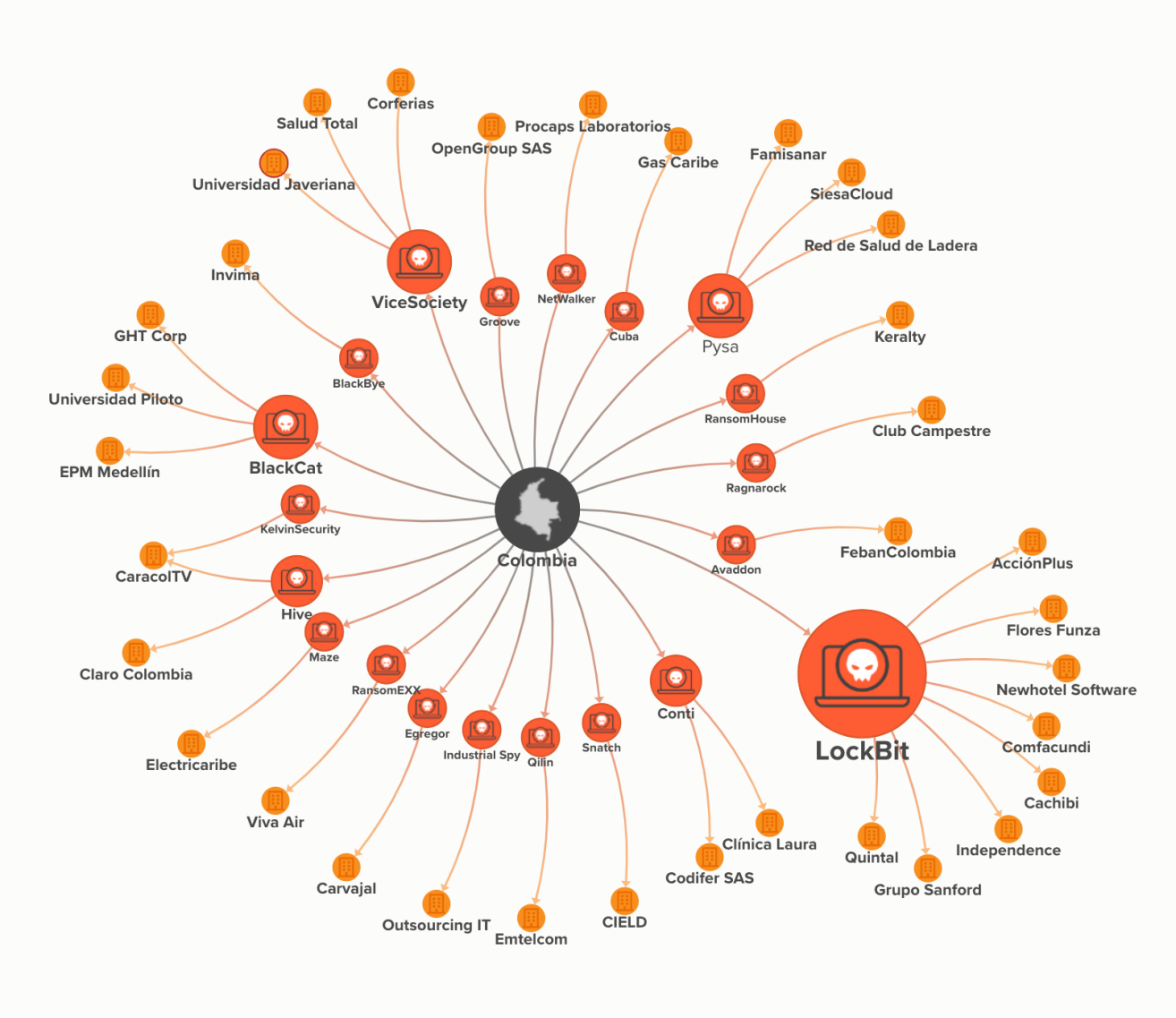
Alerta para organizaciones colombianas: **Cómo enfrentar la dura realidad del estado de ransomware en el país**

Nuestro equipo de Inteligencia de Amenazas ha estado haciendo seguimiento a la actividad de grupos de ransomware en el país. En este momento **Colombia registra un incremento de 133% comparado con el mismo periodo de 2021 en el número de instituciones afectadas por ransomware**. Los impactos de este tipo de ataques son los principales disruptores de operaciones de negocios, continúan causando gran impacto reputacional, producen miles de usuarios afectados y contribuyen a la presión mediática. Esta edición especial de Lumu Advisory provee detalles técnicos y pasos a seguir de cara al incremento mencionado.



Entidades atacadas por grupos de ransomware en Colombia.

La gravedad de la situación actual

Afectaciones directas a la operación

Los ataques que se vienen presentando tienen como objetivo crear caos y disrupción de las operaciones al tiempo que le permiten a los atacantes monetizar el compromiso de las redes ejecutando los siguientes tipos de malware en simultáneo:

- **Crypters -** Encriptan información de los activos. Dejando fuera de operación a la compañía afectada.
- **Infostealers -** Sustraen información valiosa para ser comerciada en foros de DeepWeb, y adicionalmente extorsionar a proveedores y clientes de las víctimas amenazandolos con la divulgación de la misma.
- **Criptominers -** Utilizan el poder de cómputo disponible en la infraestructura de las compañías afectadas para realizar minado de criptomonedas. Esta afectación se realiza tanto en la red corporativa como en los dispositivos conectados a la misma.
- **Wipers -** Borran, destruyen o hacen indisponible la información clave de las organizaciones víctimas, afectando directamente la operación de las mismas.

Sofisticación tecnológica de los ataques

Se ha detectado que un gran número de los ataques que se vienen presentando están relacionados con el ransomware de la familia BlackCat o también conocido como ALPHV. De acuerdo a Microsoft Defender Threat Intelligence, BlackCat es una familia del tipo RaaS (Ransowmare as a Service), por primera vez vista es en Noviembre del 2021, es uno de los primeros ransomware escritos en el lenguaje Rust, lo cual permite ejecutar payloads más completos, habilitar técnicas de evasión más sofisticadas para no ser detectado por dispositivos comunes de seguridad, e infectar múltiples dispositivos y sistemas operativos como Windows, Linux, incluso instancias de VMWare. Adjuntamos algunas de las opciones de despliegue del payload usado por BlackCat.

Command	Description
[service name] /stop	Stops running services to allow encryption of data
vssadmin.exe Delete Shadows /all /quiet	Deletes backups to prevent recovery
wmic.exe Shadowcopy Delete	Deletes shadow copies
wmic csproduct get UUID	Gets the Universally Unique Identifier (UUID) of the target device
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f	Modifies the registry to change MaxMpxCt settings; BlackCat does this to increase the number of outstanding requests allowed (for example, SMB requests when distributing ransomware via its PsExec methodology)
for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"	Clears event logs
fsutil behavior set SymlinkEvaluation R2L:1	Allows remote-to-local symbolic links; a symbolic link is a file-system object (for example, a file or folder) that points to another file system object, like a shortcut in many ways but more powerful
fsutil behavior set SymlinkEvaluation R2R:1	Allows remote-to-remote symbolic links
net use \\[computer name] /user:[domain]\[user] [password] /persistent:no	Mounts network share

Cada vez son más entidades afectadas

En el último mes hemos visto que la problemática está involucrando a más y más empresas cada día. Lo que deja en evidencia que la situación no tiende a mejorar. La prueba de ello es que el seguimiento que hemos venido haciendo al número de empresas que tienen sus cuentas de correo electrónico comprometidas sigue en aumento. La gravedad de esta situación radica en que estas cuentas se están comerciando en mercados de cibercriminales y se están usando para comprometer masivamente a otras organizaciones. Te compartimos el listado de las empresas afectadas que tenemos identificadas.

Location	Source	Website	Hosting	Price	Seller	Type	Niche	Check	Date Created	Buy
CO	cracked	supergiros.com.co	Columbus Networks Colombia	20.00	seller13	Office365 Webmail	Other	Check	2022-12-15 11:45:08	Buy
CO	cracked	colegiofontan.edu.co	EPM Telecomunicaciones S.A. E.S.P	15.00	seller30	Office365 Webmail	Other	Check	2022-12-13 23:59:58	Buy
CO	cracked	agoracsc.com	CTL LATAM, CTL Colombia	15.00	seller30	Office365 Webmail	Other	Check	2022-12-13 23:51:28	Buy
CO	cracked	unipamplona.edu.co	Level 3 Colombia S.A	20.00	seller13	Office365 Webmail	Other	Check	2022-12-13 12:47:56	Buy
CO	cracked	conquimica.com	Conquimica S.A	20.00	seller13	Office365 Webmail	Other	Check	2022-12-13 11:27:32	Buy
CO	cracked	uac.edu.co	Telmex Colombia S.A.	20.00	seller13	Office365 Webmail	Other	Check	2022-12-12 12:35:47	Buy
CO	cracked	escolme.edu.co	Telmex Colombia S.A.	20.00	seller13	Office365 Webmail	Other	Check	2022-12-12 12:22:24	Buy
CO	cracked	cbsjd.edu.co	Orden Hospitalaria De SAN Juan De Dios	20.00	seller13	Office365 Webmail	Other	Check	2022-12-12 09:47:00	Buy
CO	cracked	mincit.gov.co	Internexa S.a. E.S.P	20.00	seller13	Office365 Webmail	Other	Check	2022-12-11 23:03:44	Buy
CO	cracked	colegioaleman.edu.co	Colombia Hosting	20.00	seller13	Office365 Webmail	Other	Check	2022-12-11 19:46:04	Buy
CO	cracked	indeportesantioquia.gov.co	EPM Telecomunicaciones S.A. E.S.P	20.00	seller143	Office365 Webmail	Other	Check	2022-12-09 07:37:22	Buy
CO	cracked	eucaristicobaq.edu.co	Colombia Móvil	15.00	seller85	Office365 Webmail	Other	Check	2022-12-07 13:29:35	Buy
CO	cracked	cesup.edu.br	Ceuma-associacao De Ensino Superior	20.00	seller13	Office365 Webmail	Other	Check	2022-12-06 08:53:58	Buy
CO	cracked	oissupermercados.com	Telmex Colombia S.A.	20.00	seller143	Office365 Webmail	Other	Check	2022-12-02 18:14:37	Buy
CO	cracked	agenciauto.com	Telmex Colombia S.A.	15.00	seller85	Office365 Webmail	Other	Check	2022-11-28 11:17:13	Buy
CO	cracked	clinicazayma.org	Colombia Hosting	20.00	seller143	Office365 Webmail	Other	Check	2022-11-27 21:42:41	Buy
CO	cracked	academia.umb.edu.co	Megalinea S.A	15.00	seller85	Office365 Webmail	Other	Check	2022-11-27 15:27:46	Buy
CO	cracked	datatools.com.co	BT LATAM COLOMBIA S.A	20.00	seller141	Office365 Webmail	Other	Check	2022-11-24 23:43:01	Buy
CO	cracked	escuelanaval.edu.co	Red Nacional Académica de Tecnología Avanzada - RENATA	20.00	seller143	Office365 Webmail	Other	Check	2022-11-24 17:47:28	Buy
CO	cracked	betobee.com.co	Colombia Hosting	20.00	seller143	Office365 Webmail	Other	Check	2022-11-24 15:53:30	Buy
CO	cracked	royal-films.com	Telmex Colombia S.A.	20.00	seller143	Office365 Webmail	Other	Check	2022-11-23 09:41:39	Buy
CO	cracked	tecnocomfenalco.edu.co	Fundacion Universitaria Tecnologico Comfenalco - Cartagena	20.00	seller141	Office365 Webmail	Other	Check	2022-11-22 10:44:01	Buy
CO	cracked	circulemos.com.co	BT LATAM COLOMBIA S.A	15.00	seller19	Office365 Webmail	Other	Check	2022-11-20 10:31:51	Buy
CO	cracked	estrategiastributarias.com	Telmex Colombia S.A.	15.00	seller19	Office365 Webmail	Other	Check	2022-11-20 10:29:31	Buy
CO	cracked	deebasoc.com	Colombia Hosting	15.00	seller85	Office365 Webmail	Other	Check	2022-11-18 12:21:25	Buy
CO	cracked	inder.gov.co	EPM Telecomunicaciones S.A. E.S.P	20.00	seller141	Office365 Webmail	Other	Check	2022-11-15 12:27:29	Buy
CO	cracked	palermosj.edu.co	Congregacion De LAS Hermanas Franciscanas De Maria	20.00	seller141	Office365 Webmail	Other	Check	2022-11-15 12:26:58	Buy
CO	cracked	calasanzcucuta.edu.co	Orden Religiosa De LAS Escuelas Pias O Escolapios	15.00	seller19	Office365 Webmail	Other	Check	2022-11-14 13:27:47	Buy
CO	cracked	medplus.com.co	Telmex Colombia S.A.	15.00	seller19	Office365 Webmail	Other	Check	2022-11-14 10:54:39	Buy
CO	cracked	saludfamiliar.com.co	IFX NETWORKS COLOMBIA	23.00	seller30	Office365 Webmail	Other	Check	2022-11-13 16:45:17	Buy
CO	cracked	upb.edu.co	Universidad Pontificia Bolivariana	15.00	seller30	Office365 Webmail	Other	Check	2022-11-13 12:00:49	Buy
CO	cracked	fiduprevisora.com.co	Telmex Colombia S.A.	15.00	seller19	Office365 Webmail	Other	Check	2022-11-13 11:39:25	Buy
CO	cracked	simex.com.co	Colombia Hosting	15.00	seller30	Office365 Webmail	Other	Check	2022-11-13 09:21:04	Buy
CO	cracked	unimagdalena.edu.co	Universidad Del Magdalena	15.00	seller7	Office365 Webmail	Other	Check	2022-11-12 08:57:36	Buy
CO	cracked	dwsistemas.net.co	DataWare Sistemas	20.00	seller141	Office365 Webmail	Other	Check	2022-11-11 07:14:53	Buy
CO	cracked	unadvirtual.edu.co	MOVCORP	20.00	seller141	Office365 Webmail	Other	Check	2022-11-09 08:26:01	Buy
CO	cracked	ielamercedmosquera.edu.co	IFX NETWORKS COLOMBIA	20.00	seller141	Office365 Webmail	Other	Check	2022-11-08 18:05:56	Buy
CO	cracked	habitatbogota.gov.co	Secretaria Distrital Del Habitat	30.00	seller49	Office365 Webmail	Other	Check	2022-10-29 09:01:40	Buy
CO	cracked	edutechnia.com	Corporacion De Ferias Y Exposiciones SA	30.00	seller49	Office365 Webmail	Other	Check	2022-10-29 08:59:14	Buy
CO	cracked	friedrichherbart.edu.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-10-26 22:58:36	Buy
CO	cracked	carval.com.co	Vallecilla B Y M Y CIA	20.00	seller19	Office365 Webmail	Other	Check	2022-10-26 22:57:59	Buy
CO	cracked	arquidiocesanos.edu.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-10-26 21:59:16	Buy
CO	cracked	ucompensar.edu.co	Telmex Colombia S.A.	20.00	seller19	Office365 Webmail	Other	Check	2022-10-26 21:52:40	Buy
CO	cracked	esn.edu.co	Colombia Hosting	15.00	seller30	Office365 Webmail	Other	Check	2022-10-26 01:24:36	Buy
CO	cracked	eia.edu.co	Internexa S.a. E.S.P	15.00	seller30	Office365 Webmail	Other	Check	2022-10-25 23:52:44	Buy
CO	cracked	clinicapalermo.com.co	Colombia Hosting	15.00	seller19	Office365 Webmail	Other	Check	2022-10-24 10:58:36	Buy
CO	cracked	ipn.edu.co	Universidad Pedagogica Nacional	20.00	seller19	Office365 Webmail	Other	Check	2022-10-17 17:25:46	Buy
CO	cracked	ecomil.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-10-16 10:13:53	Buy
CO	cracked	crystal.com.co	Telmex Colombia S.A.	20.00	seller19	Office365 Webmail	Other	Check	2022-10-16 10:11:29	Buy
CO	cracked	dnp.gov.co	Telmex Colombia S.A.	20.00	seller19	Office365 Webmail	Other	Check	2022-10-13 23:32:44	Buy

CO	cracked	unisimon.edu.co	UNIVERSIDAD SIMÓN BOLÍVAR	20.00	seller19	Office365 Webmail	Other	Check	2022-10-13 23:21:46	Buy
CO	cracked	est.colmayor.edu.co	Colegio Mayor de Antioquía	20.00	seller19	Office365 Webmail	Other	Check	2022-10-13 05:01:44	Buy
CO	cracked	iejosehgarcescali.edu.co	Centro Cristiano Amor Y FE	20.00	seller19	Office365 Webmail	Other	Check	2022-10-13 04:15:44	Buy
CO	cracked	azzorti.bo	Industrias Inca S A	20.00	seller19	Office365 Webmail	Other	Check	2022-10-12 08:57:55	Buy
CO	cracked	sdis.gov.co	SECRETARIA DISTRITAL DE INTEGRACIÓN SOCIAL	20.00	seller139	Office365 Webmail	Other	Check	2022-10-11 08:14:33	Buy
CO	cracked	cies.edu.co	Colombia Hosting	20.00	seller139	Office365 Webmail	Other	Check	2022-10-07 22:53:01	Buy
CO	cracked	sanmartin.edu.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-10-07 22:02:40	Buy
CO	cracked	telecolombia.com	IFX NETWORKS COLOMBIA	20.00	seller141	Office365 Webmail	Other	Check	2022-10-05 08:30:47	Buy
CO	cracked	azzorti.com	IFX NETWORKS COLOMBIA	20.00	seller141	Office365 Webmail	Other	Check	2022-09-30 22:04:32	Buy
CO	cracked	utp.edu.co	Universidad Tecnologica de Pereira	20.00	seller19	Office365 Webmail	Other	Check	2022-09-21 17:49:41	Buy
CO	cracked	asocajas.org.co	EPM Telecomunicaciones S.A. E.S.P	20.00	seller141	Office365 Webmail	Other	Check	2022-09-16 04:35:32	Buy
CO	cracked	unisalle.edu.co	Universidad De LA Salle	20.00	seller141	Office365 Webmail	Other	Check	2022-09-16 04:21:10	Buy
CO	cracked	etb.com.co	ETB - Colombia	20.00	seller19	Office365 Webmail	Other	Check	2022-09-10 13:31:45	Buy
CO	cracked	funpadua.org	Colombia Hosting	20.00	seller92	Office365 Webmail	Other	Check	2022-08-26 13:24:31	Buy
CO	cracked	salazaryherrera.edu.co	EPM Telecomunicaciones S.A. E.S.P	20.00	seller92	Office365 Webmail	Other	Check	2022-08-24 16:00:32	Buy
CO	cracked	iser.edu.co	RYO COMUNICACIONES	25.00	seller49	Office365 Webmail	Other	Check	2022-08-05 14:04:30	Buy
CO	cracked	ensjerico.edu.co	EPM Telecomunicaciones S.A. E.S.P	25.00	seller49	Office365 Webmail	Other	Check	2022-08-05 11:43:15	Buy
CO	cracked	institucionzoraida.edu.co	Hosting RED	20.00	seller19	Office365 Webmail	Other	Check	2022-06-18 08:54:28	Buy
CO	cracked	asicamericas.com	IFX NETWORKS COLOMBIA	20.30	seller92	Office365 Webmail	Other	Check	2022-06-13 23:36:52	Buy
CO	cracked	uniagraria.edu.co	IFX NETWORKS COLOMBIA	20.00	seller19	Office365 Webmail	Other	Check	2022-06-10 13:21:19	Buy
CO	cracked	udenar.edu.co	Universidad de Nariño	20.00	seller19	Office365 Webmail	Other	Check	2022-06-08 07:22:29	Buy
CO	cracked	mail.colegiocisneros.edu.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-05-19 08:13:29	Buy
CO	cracked	sanmateo.edu.co	IFX NETWORKS COLOMBIA	20.00	seller19	Office365 Webmail	Other	Check	2022-05-12 10:31:52	Buy
CO	cracked	esap.edu.co	IFX NETWORKS COLOMBIA	20.00	seller19	Office365 Webmail	Other	Check	2022-05-07 12:26:45	Buy
CO	cracked	student.cbr.edu.co	IFX NETWORKS COLOMBIA	20.00	seller49	Office365 Webmail	Other	Check	2022-04-25 00:28:27	Buy
CO	cracked	educosta.edu.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-04-12 04:20:53	Buy
CO	cracked	cidca.edu.co	Colombia Móvil	20.00	seller19	Office365 Webmail	Other	Check	2022-04-03 10:08:36	Buy
CO	cracked	worldef.net	CloudFlare, Inc.	20.00	seller19	Office365 Webmail	Other	Check	2022-02-23 12:44:32	Buy
CO	cracked	carmelsaintjoseph.edu.lb	CloudFlare, Inc.	20.00	seller19	Office365 Webmail	Other	Check	2022-02-15 03:27:11	Buy
CO	cracked	rs.edu.jo	CloudFlare, Inc.	29.30	seller92	Office365 Webmail	Other	Check	2022-02-12 20:34:19	Buy
CO	cracked	seminariopopayan.edu.co	Colombia Hosting	20.00	seller19	Office365 Webmail	Other	Check	2022-02-12 14:21:14	Buy
CO	cracked	orthosynetics.com	CloudFlare, Inc.	20.30	seller92	Office365 Webmail	Other	Check	2022-02-02 11:13:35	Buy
CO	cracked	leadcollege.edu.au	CloudFlare, Inc.	25.30	seller92	Office365 Webmail	Other	Check	2022-01-30 23:41:43	Buy
CO	cracked	esrg.pt	CloudFlare, Inc.	22.00	seller26	Office365 Webmail	Other	Check	2022-01-30 14:10:38	Buy
CO	cracked	colegionsprovidencia.edu.co	Colombia Hosting	25.30	seller92	Office365 Webmail	Other	Check	2022-01-20 14:34:33	Buy

¿Cuáles son las familias de malware más usadas como precursores en los ataques actuales?

- **Qakbot -** Malware enfocado al robo de información y control de botnets. Hemos evidenciado un aumento de 1.040% respecto de Q3-2022 en las detecciones de este malware, haciendo que este sea el precursor de ransomware más popular y usado hoy en día. Es importante mencionar que comparte bastante similitud con el comportamiento del malware Emotet.
- **Emotet -** Si bien de Q3 a Q4 de 2022 hubo una disminución de 15% en la cantidad de detecciones de este tipo de malware, este sigue siendo uno de los principales precursores de control de botnets para robo de información. Es conocido por ser usado por Conti Group, la banda de ciberdelincuentes que se dice estuvo detrás del ataque a diferentes entidades públicas y de gobierno en Costa Rica y otros países de Latinoamérica.

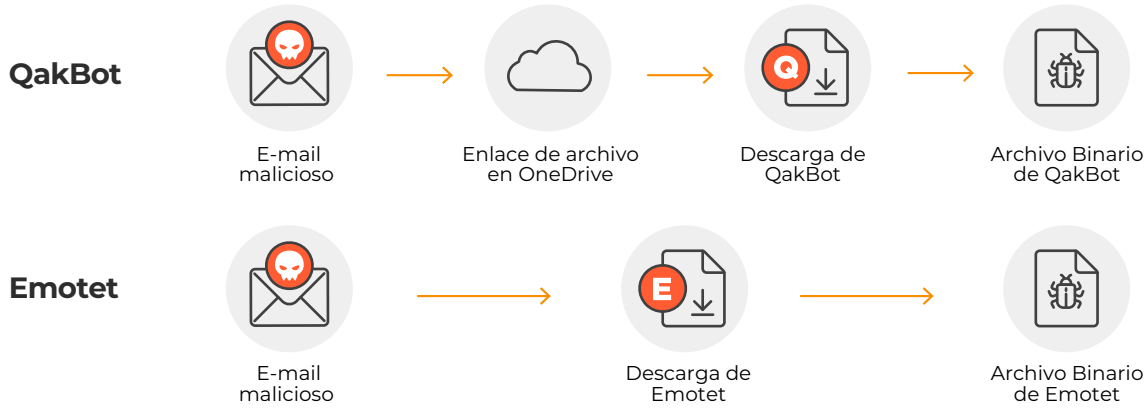
Top 5 de técnicas que están siendo usadas por los delincuentes

Hemos identificado y mapeado las técnicas de la matriz MITRE ATT&CK más usadas en los recientes ataques de ransomware. Es urgente que las organizaciones tomen medidas para identificar su ejecución y neutralizarlas con precisión.

1. **Application Layer Protocol -** T1071
2. **Phishing -** T1566
3. **User Execution: Malicious File -** T1204.002
4. **Automated Exfiltration -** T1020
5. **Exfiltration Over Command and Control Channel -** T1041

¿Cómo identificar un ataque en progreso?

- **Incremento en contactos con sitios de Phishing -** En Colombia este tipo de ataques han aumentado 31.35% de Q3 a Q4. Se ha comprobado que las infecciones relacionadas con Emotet y QakBot iniciaron con el envío de phishing, ya que esto le permite a los atacantes descargar el contenido malicioso directamente a los equipos de las víctimas. Esta sin duda sigue siendo la puerta de entrada a las organizaciones.



- **No pasar por alto las conexiones hacia componentes Javascript maliciosos -** Se ha detectado que muchos sitios web legítimos pueden estar comprometidos y presentar códigos modificados por ciberdelincuentes. Esto les permite infectar equipos corporativos y realizar ataques de critomining.
- **Detección intencional de Criptomining -** Si bien estos ataques se pueden presentar en un escenario "in-browser" es decir embebidos en el navegador web, también se pueden presentar en máquinas y dispositivos corporativos comprometidos. Tenemos evidencia de que los casos de ransomware están precedidos por una alta actividad de criptomining, ya que es el momento en que los delincuentes buscan monetizar al máximo el compromiso de la red antes de encriptar los archivos.
- **Aumento de incidentes de DGA -** Al igual que con la actividad de criptomining, los incidentes de DGA (Domain Generation Algorithm) son síntoma de una red comprometida, que está siendo controlada por atacantes y sobre la cual se están haciendo tareas de monetización.
- **Análisis de integridad en archivos de SO -** Se ha detectado que en el caso de malware tipo Wiper, los atacantes comprometen archivos ejecutables legítimos del SO para que su código se ejecute una vez el programa legítimo es iniciado.
- **Movimiento lateral en la red -** Previo a un ataque de ransomware, los atacantes buscan comprometer la mayor cantidad de dispositivos conectados a la red. Para esto se valen de la instalación de herramientas como Cobalt Strike. Es crucial contar con estrategias que permitan identificar estos movimientos laterales a tiempo y de forma intencional.

- **Identificar presencia de ExMatter/Fender -** Es una herramienta usada para la filtración y robo de información sensible en organizaciones víctimas de ransomware. Se deben implementar estrategias para identificar la presencia y ejecución remota de estas herramientas en los activos de la organización. Los ataques que hemos analizado hacen uso de PsExec() y dominios comprometidos para desplegar ExMatter/Fender en los dispositivos de las organizaciones.

¿Cómo evitar que su red sea comprometida?

- **Asumir que se está comprometido y comprobar lo contrario -** Está comprobado, ante la coyuntura actual cualquier empresa, sin importar su tamaño, vertical, o madurez tecnológica puede ser víctima de un ataque de ransomware. Se debe asumir una posición proactiva y para esto lo mejor es asumir que los atacantes ya están dentro de la infraestructura y demostrar lo contrario.
- **No existen amenazas pequeñas -** Es mejor erradicar las amenazas pequeñas a tiempo antes de que estas abran el camino a situaciones catastróficas. Una red comprometida se comporta diferente, y es por esto que cualquier anomalía debe ser tratada a tiempo y dándole la mayor importancia.
- **No hay un momento adecuado para estar preparado -** Si bien cualquier empresa puede ser víctima de ransomware, la diferencia radica en qué tan preparado se está para afrontar la crisis. No espere para tomar las medidas que le brinden una capa adicional de protección. Recuerde que Lumu tiene disponible una herramienta totalmente gratuita que le ayuda a incrementar su resiliencia ante amenazas.
- **Realizar verificación de identidades y credenciales de acceso -** Cierrele la puerta a los criminales, incluso si alguno de sus usuarios ya fue comprometido, está a tiempo de retirarle ese privilegio a los delincuentes.
- **Deshabilitar puertos innecesarios -** Los atacantes son extremadamente oportunistas, no van a desaprovechar las puertas de acceso que usted deje abiertas innecesariamente.
- **Deshabilitar la ejecución automática de Macros en aplicaciones de MS Office -** Las familias de malware que se están utilizando en los ataques actuales se valen de técnicas para evadir las soluciones de antivirus y EDR. Se deben tomar medidas a nivel de los aplicativos corporativos.
- **Abstenerse de descargar adjuntos sin antes verificar la identidad del remitente -** Complementario a lo mencionado en el ítem anterior, se debe mantener alerta constante ante el recibo de archivos adjuntos. Esto ayuda a reducir la exposición.