Los perpetradores detrás del ransomware BlackCat han cerrado su sitio web en la darknet y posiblemente han llevado a cabo un engaño de salida después de publicar una falsa pancarta de confiscación por parte de las fuerzas del orden.

> *«ALPHV/BlackCat no fue incautado. Están estafando a sus colaboradores. Es evidentemente claro al revisar el código fuente del nuevo aviso de cierre»,* afirmó el investigador de seguridad Fabian Wosar.
>
> *«No hay ninguna razón lógica por la cual las autoridades simplemente pondrían una versión guardada del aviso de cierre durante una incautación en lugar del aviso original».*

La Agencia Nacional contra el Crimen del Reino Unido (NCA, por sus siglas en inglés) le comunicó a Reuters que no tenía ninguna conexión con las interrupciones en la infraestructura de BlackCat.

Dmitry Smilyanets, investigador de seguridad de Recorded Future, compartió capturas de pantalla en la plataforma de redes sociales X, en las que los actores de BlackCat afirmaban que *«los federales nos arruinaron»* y que planeaban vender el código fuente del ransomware por $5 millones.

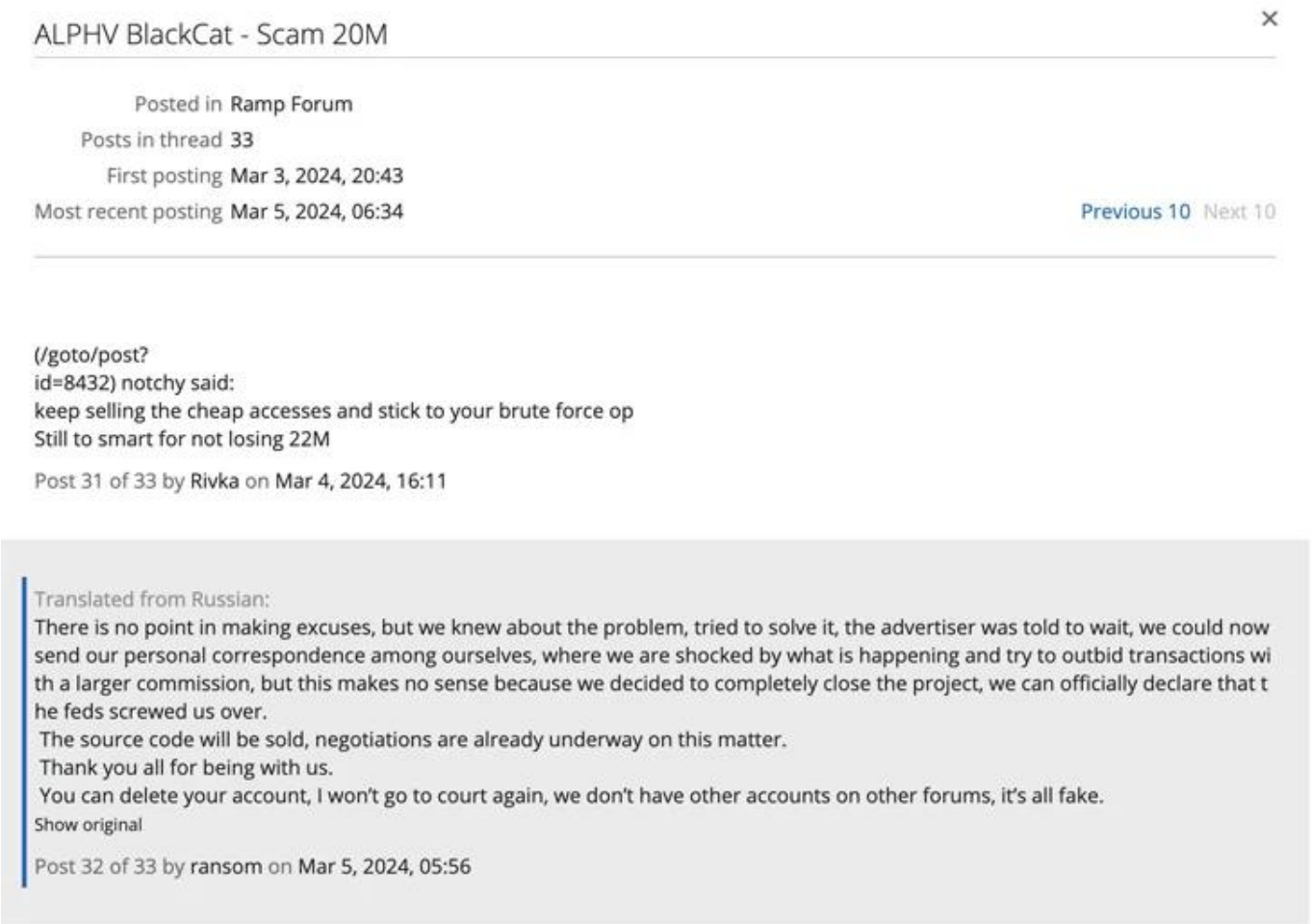
La desaparición se produce después de que supuestamente recibieran un pago de rescate de $22 millones de la unidad Change Healthcare de UnitedHealth (Optum) y se negaran a compartir las ganancias con un colaborador que llevó a cabo el ataque.

La empresa no ha comentado sobre el supuesto pago de rescate, declarando que solo se enfoca en los aspectos de investigación y recuperación del incidente.

Según DataBreaches, el colaborador descontento, cuya cuenta fue suspendida por el personal administrativo, realizó las acusaciones en el foro de ciberdelincuencia RAMP.

«Vaciaran la billetera y se llevaron todo el dinero», expresaron.

Esto ha generado especulaciones de que BlackCat ha llevado a cabo un engaño de salida para evadir la atención y reaparecer en el futuro bajo una nueva marca. *«Un cambio de identidad está en proceso»,* afirmó un exadministrador del grupo de ransomware.



ALPHV BlackCat - Scam 20M

Posted in Ramp Forum
Posts in thread 33
First posting Mar 3, 2024, 20:43
Most recent posting Mar 5, 2024, 06:34

Previous 10 Next 10

(/goto/post?
id=8432) notchy said:
keep selling the cheap accesses and stick to your brute force op
Still to smart for not losing 22M

Post 31 of 33 by Rivka on Mar 4, 2024, 16:11

Translated from Russian:
There is no point in making excuses, but we knew about the problem, tried to solve it, the advertiser was told to wait, we could now send our personal correspondence among ourselves, where we are shocked by what is happening and try to outbid transactions wi th a larger commission, but this makes no sense because we decided to completely close the project, we can officially declare that t he feds screwed us over.
The source code will be sold, negotiations are already underway on this matter.
Thank you all for being with us.
You can delete your account, I won't go to court again, we don't have other accounts on other forums, it's all fake.
Show original

Post 32 of 33 by ransom on Mar 5, 2024, 05:56

BlackCat tuvo su infraestructura incautada por las autoridades en diciembre de 2023, pero la banda logró retomar el control de sus servidores y reiniciar sus operaciones sin mayores consecuencias. Anteriormente, el grupo operaba bajo los nombres de DarkSide y

BlackMatter.

> *«Internamente, BlackCat podría estar preocupado por infiltrados dentro de su grupo, y cerrar sus operaciones de manera preventiva podría evitar una intervención antes de que ocurra»*, mencionó Malachi Walker, asesor de seguridad de DomainTools.
>
> *«Por otro lado, este engaño de salida podría ser simplemente una oportunidad para que BlackCat tome el dinero y huya. Dado que las criptomonedas han vuelto a alcanzar su punto más alto, la banda podría vender su producto a un precio 'elevado'. En el mundo del cibercrimen, la reputación lo es todo, y BlackCat parece estar quemando puentes con sus colaboradores con estas acciones».*

El aparente fin del grupo y el abandono de su infraestructura coinciden con el informe del grupo de investigación de malware VX-Underground, que señala que la operación de ransomware LockBit ya no respalda Lockbit Red (también conocido como Lockbit 2.0) y StealBit, una herramienta personalizada utilizada por el actor de amenazas para la extracción de datos.

LockBit también ha tratado de mantener su reputación trasladando algunas de sus actividades a un nuevo portal en la darknet después de una operación coordinada de las autoridades que derribó su infraestructura el mes pasado tras una investigación de varios meses.

Esto también ocurre cuando Trend Micro revela que la familia de ransomware conocida como RA World (anteriormente RA Group) ha logrado infiltrarse con éxito en empresas de atención médica, finanzas y seguros en EE. UU., Alemania, India, Taiwán y otros países desde su aparición en abril de 2023.

Los ataques llevados a cabo por el grupo *«involucran componentes de varias etapas*

diseñados para garantizar el máximo impacto y éxito en las operaciones del grupo», señaló la firma de ciberseguridad.