Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

AMPER SUFRE DEVASTADOR CIBERATAQUE: 650 GB DE DATOS ROBADOS POR BLACK BASTA

19 / 06 / 2024

CONTENIDO

INTRODUCCIÓN

El reciente ciberataque sufrido por Amper, una destacada empresa española de ingeniería y tecnología, pone de manifiesto la creciente amenaza que representan los grupos de ransomware como Black Basta. En este ataque devastador, se exfiltraron 650 gigabytes de datos críticos, incluyendo información de proyectos, usuarios y empleados. Black Basta, conocido por su sofisticación y técnicas avanzadas de infiltración, ha afectado a más de 500 organizaciones a nivel mundial desde su aparición en 2022. La conexión con el grupo de ciberdelincuentes rusos FIN7 añade una capa adicional de complejidad a la amenaza, subrayando la urgente necesidad de fortalecer las defensas cibernéticas para proteger la información crítica y mantener la integridad de las infraestructuras digitales.

AMPER SUFRE DEVASTADOR CIBERATAQUE: 650 GB DE DATOS ROBADOS POR BLACK BASTA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_06_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/06/2024
Es día cero (0 day):	No

RESUMEN

En un ataque que resalta la creciente amenaza cibernética, la empresa española de ingeniería y tecnología Amper ha sido víctima de un devastador ciberataque perpetrado por el grupo de ransomware Black Basta. Los atacantes lograron exfiltrar 650 gigabytes de datos críticos, incluyendo información de proyectos, usuarios y empleados, como nóminas y datos financieros.

Black Basta ha emergido rápidamente como un actor significativo en el ámbito del RaaS (Ransomware as a Service). Según el Instituto Nacional de Ciberseguridad de España (Incibe), este grupo utiliza técnicas avanzadas para evadir las defensas tradicionales y cifrar datos críticos, lo que ha resultado en un número alarmante de víctimas a nivel mundial.

El éxito de Black Basta se debe a su habilidad para infiltrarse y moverse lateralmente dentro de las redes de sus objetivos utilizando una combinación de herramientas sofisticadas. Entre las herramientas empleadas destacan:

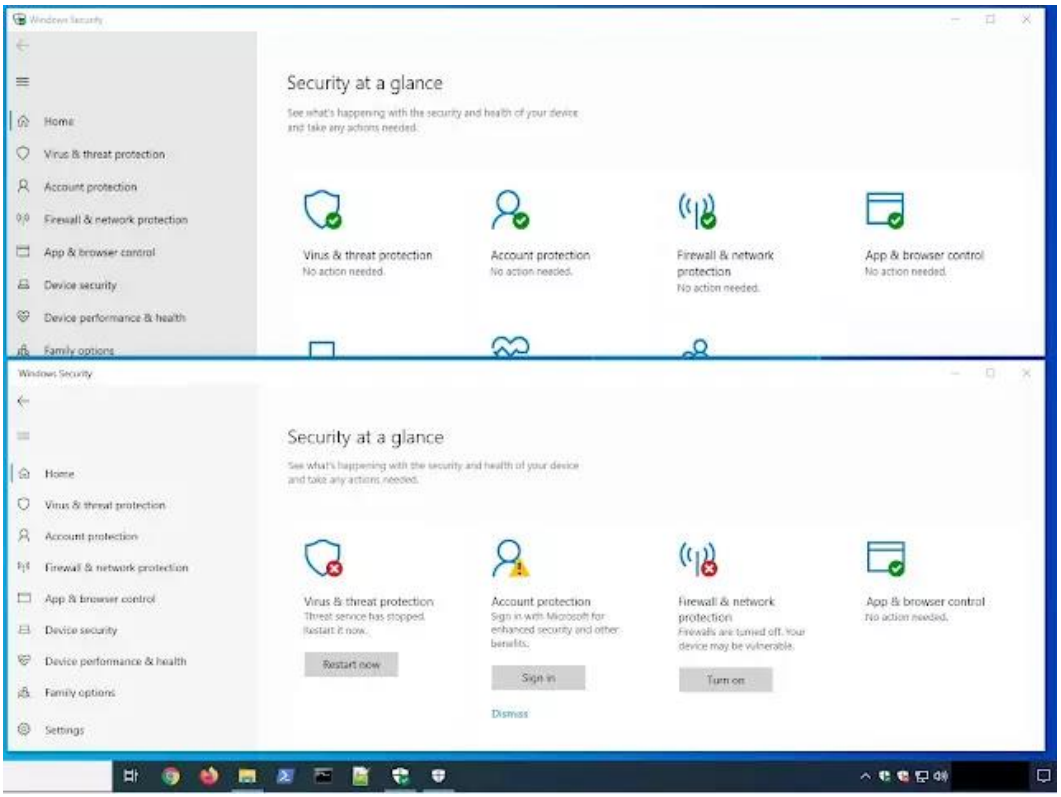
- SoftPerfect Network Scanner
- BITSAdmin
- Cobalt Strike
- ConnectWise ScreenConnect
- PsExec

Para la escalada de privilegios, utilizan Mimikatz y para la exfiltración de datos antes del cifrado, RClone. Además, aprovechan vulnerabilidades como ZeroLogon (CVE-2020-1472), NoPac (CVE-2021-42278 y CVE-2021-42287) y PrintNightmare (CVE-2021-34527).

Black Basta emplea técnicas de phishing altamente efectivas. Los atacantes envían correos electrónicos con archivos ZIP que contienen imágenes ISO diseñadas para evadir los mecanismos de seguridad.

Una vez dentro, el malware lleva a cabo diversas acciones maliciosas, como monitorear y registrar pulsaciones de teclas, recolectar credenciales de acceso y propagarse a otros sistemas de la red mediante técnicas de movimiento lateral.

Investigaciones recientes sugieren una conexión entre Black Basta y el grupo de ciberdelincuentes rusos FIN7, también conocido como Carbanak. Esta relación añade una capa adicional de complejidad a la amenaza, ya que FIN7 es conocido por su sofisticación en ataques cibernéticos. Herramientas como WindefCheck.exe, utilizadas por Black Basta, han sido vinculadas a FIN7, indicando una posible colaboración o compartición de integrantes.



Black Basta cifra los datos de sus víctimas utilizando una combinación de ChaCha20 y RSA-4096. Este cifrado robusto dificulta la recuperación de archivos, aunque existe una herramienta llamada 'Black Basta Buster' que intenta descifrar los datos. No obstante, debido a la complejidad del cifrado, la recuperación no siempre es posible.

El ataque a Amper es un claro recordatorio de la sofisticación creciente de los ciberdelincuentes y la necesidad urgente de fortalecer las defensas digitales. Black Basta sigue siendo una amenaza significativa, y su conexión con FIN7 complica aún más el panorama de ciberseguridad. Las empresas deben priorizar la ciberseguridad para proteger su información crítica y mantener la integridad de sus infraestructuras digitales.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240619_BlackBasta

NOTICIA COMPLETA

https://devel.group/blog/amper-sufre-devastador-ciberataque-650-gb-de-datos-robados-por-black-basta/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente