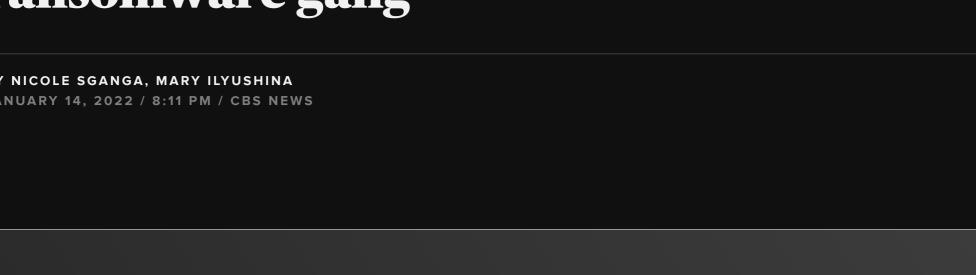


Ukraine government websites hit by cyberattac...

02:25

JANUARY 14, 2022 / 8:11 PM / CBS NEWS





Now Playing

Ukraine government websites hit

by cyberattac...

invasion

Preparing for possible Russian

ransomware group, REvil, Friday. According to the Federal Security Service (FSB), Russian authorities raided 25 \$600,000, 500,000 euros, computer equipment, crypto wallets and 20 luxury cars.

How to taste sparkling wine

Russia's domestic intelligence service announced a special operation campaign against the notorious criminal addresses, resulting in the arrest of 14 individuals and seizure of more than \$1 million worth of assets: 426 million rubles,

Biden, Congress weigh Russian

attack response...

Russia, Jan.14, 2022: FSB officer checks laptop of a detained hacker. At request of the U.S., FSB detains a group of hackers who sent ransomware viruses. VIDEO SCREEN GRAB/FSB/TASS The Russia-based REvil gang has waged a spate of high-profile attacks on major U.S. and international companies, including the July 4 attack on software company Kaseya and a May ransomware attack on JBS USA, the world's largest meat processing company.

Fighting Diabetes? This Discovery Leaves Doctors Speechless!

PAID CONTENT BY BLOOD SUGAR BLASTER

Colonial Pipeline, the nation's largest oil producer.

ceased to exist," the statement boasted.

payment, in custody for two months.

Andrei Bessonov, Russian news agencies reported, Friday.

"informed about the results of the operation."

these groups will continue to operate with impunity."

damage to a protected computer, and money laundering.

facades.

technology to some degree."

Trending News

Trump accounting firm recants a

decade of his financial statements

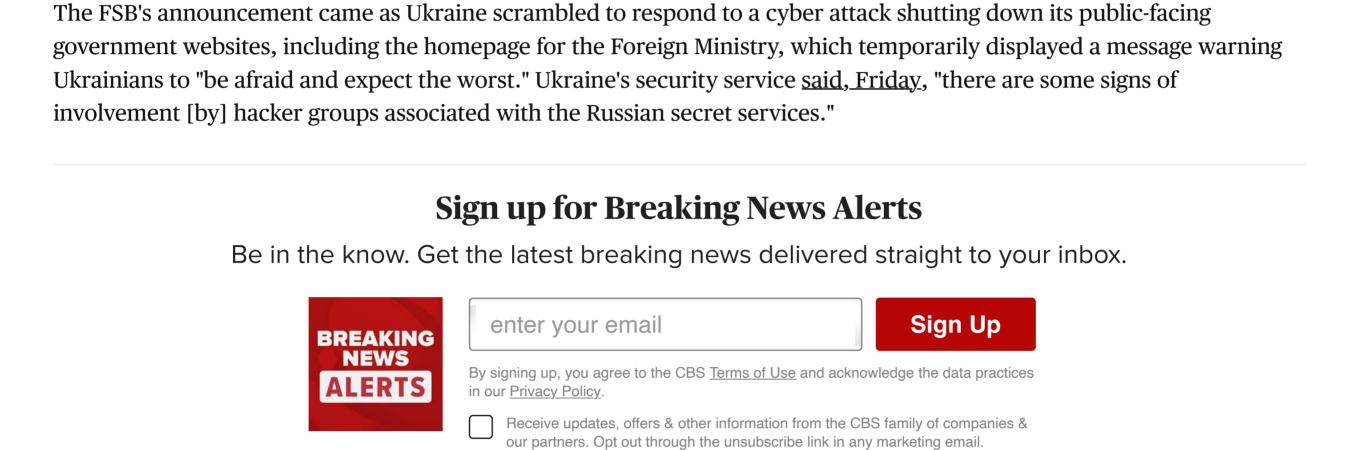
location of key REvil group leaders.

specifying whether all the detained hackers were Russian nationals.

the Kremlin is actively preparing the battlefield by using information warfare.

conducting ransomware attacks against Americans brought to justice."

incident.



The FSB claimed those arrested Friday, had "developed malicious software and organized the theft of funds from the bank

"As a result of the joint actions of the FSB and the Ministry of Internal Affairs of Russia, the organized criminal group

The White House acknowledged, Friday, that one of the hackers arrested had been involved in the Colonial Pipeline

"We understand that one of the individuals who was arrested today was responsible for the attack against Colonial

Pipeline last spring," a senior administration official briefed reporters, Friday. "We're committed to seeing those

accounts of foreign citizens and cashed them out, including by purchasing expensive goods on the Internet."

Earlier this year, REvil reportedly demanded \$50 million from Apple ahead of its product launch after hacking one of its

suppliers, Quanta Computer. Associates of the criminal ransomware group have been linked to the May shut down of

with blurred-out faces and sorting through stacks of Russian rubles. Suspected REvil hacker Roman Muromsky, 33, has been detained following the raids, though it's unclear if the former leader of cybercriminal gang EvilCorp appears in the handout video.

Moscow's Tverskoi District Court has placed the Muromsky, a Russian national suspected of illegal trafficking of means of

The FSB also <u>handed out footage</u> depicting agents raiding homes, tackling suspects to the floor, handcuffing individuals

But Russia won't extradite to the U.S. those members of the REvil hacker group who have Russian citizenship, a knowledgeable source told Interfax Friday.

"The law of the Russian Federation prohibits extradition of Russian citizens to a foreign state," the source said, without

In their statement, the FSB said Friday's investigation came at "the request of competent US authorities," who were later

The U.S.-Russia collaboration marks a bright spot in an otherwise tense moment for the two countries, following a week of

failed diplomatic efforts to curb Russia's military buildup bordering on Ukraine. As Ukraine's communication intelligence

service responds to the cyberattacks targeting as many as 70 of its websites, U.S. and Ukrainian officials tell CBS News that

"These arrests are another example of the significant actions taken by the United States to curb the multifaceted extortion

"Taking down a ransomware leader is like cutting the head off a hydra," Westin added. "New leaders will step in to fill the

void. The relationship between ransomware gangs and Russian APT groups are well known and the true actors behind

On Thursday, prior to public reports of the Russian-led REvil operation, U.S. Secret Service cyber chief Jeremy Sheridan

told the Washington Post that ransomware criminal actors often mature, evolve or adjust, reappearing under different

crisis. Threat actors are reevaluating whether they should continue their criminal activities in light of the arrests and

"The court has granted the motion from the investigation to select two-month custody until March 13 as a measure of

restraint for Roman Gennadyevich Muromsky," court spokesperson Kseniya Rozina said Friday. The court has also jailed

indictments," Charles Carmakal, SVP and CTO of Mandiant told CBS News. "Still, the timing is strange here," Ken Westin, Director of Security Strategy for Cybereason cautioned, in an interview with CBS News. The Russian-led raids "could be a smokescreen or red herring."

"With these small groups working with illicit exchanges, there's an expression that a colleague of mine uses," Sheridan said. "It's the same 200 people chasing the same 200 people. There are certainly the influx of new actors in this space. But a lot of times what we see with a new variant or a new cyberattack, it's the same developers who have just changed their

Last summer, the State Department offered a reward of up to \$10 million for information leading to the identification or

The Perfect Home Massage Chair

In November, Attorney General Merrick Garland announced seizure of more than \$6 million in cryptocurrency after REvil

leader and Russian national Yevgeniy Igorevich Polyanin, scooped up \$13 million from ransomware victims. The suspected

"author" of the REVIL ransomware, Polyanin, has been charged with 14 counts of conspiracy to commit fraud, intentional

CBS News has reached out to the Department of Justice, FBI and National Security Council for comment.

Margaret Brennan, Arden Farhi, Dan Patterson and Rob Legare contributed to this report.

Russian units near Ukraine moved

into "attack positions," official says

We Offer Most Advanced Automatic Massage

Open >

NYC fires 1,400 workers over vaccine

Tab2la Feed

mandate – less than 1%

Technologies Available In the UK Today.

WEYRON MASSAGE CHAIRS

Judge speeds up review of lawyer's

emails sought by January 6

committee

Nicole Sganga CBS News reporter covering homeland security and justice. **Twitter** First published on January 14, 2022 / 8:11 PM © 2022 CBS Interactive Inc. All Rights Reserved.

We've partnered with the National Portrait Gallery to add over 125,000

portraits from their collection to our website and you can browse them all f...

Browse the entire collection for free

unforgettable family ski holiday

Everyone In The UK Should Get This £39 Monocular

Telescope

PAID ZTECH

PAID ANCESTRY®

PAID CLUB MED

Manage Cookies

"The best pizza oven." Wirecutter These recommendations come from seasoned chefs and professional <u>pizzaioli</u> who all agree, independently, that Ooni pizza ovens help people ... PAID OONI PIZZA OVENS

Your Will Professionally Written for Only £19.99

Don't be a no-will nightmare! Limited-Time Offer for Over 50's!

Unsold Mediterranean Cruise Cabins Are Almost Being

PAID LEGACY WILLS & ESTATE PLANNING

Given Away

PAID CRUISE DEALS | SEARCH ADS

CBS News Live on Paramount+ **CBS News Store** Site Map **Contact Us** Help (O)

Closed Captioning

©CBS NEWS Copyright © 2022 CBS Interactive Inc. All rights reserved. **Privacy Policy**

New Club Med ski resort in the French Alps | Experience an

Do Not Sell My Personal Information **Cookies Policy Terms of Use** About **Advertise**