PROANALYSIS

WHAT YOU NEED TO KNOW ABOUT

Ransomware Attacks

BY JOHN SAKELLARIADIS AND ROSMERY IZAGUIRRE | 03/14/2024 05:00:00 AM EDT

PRO POINTS

- **Russian and Eastern European cybercriminal gangs have ramped up ransomware attacks that try to** extort money from U.S. schools, hospitals and private companies, despite long-running efforts by Washington to crack down on such hacks.
- **The scale and intensity of the problem has hit a new level — with a record $1 billion extorted** globally last year, the majority coming from U.S. and other Western organizations. The U.S. intelligence community warned in March that it saw a "massive increase" in ransomware attacks between 2022 and 2023 and that the extortion efforts are only becoming more profitable and more sophisticated.
- **Congress and the White House are facing pressure to consider additional policies to counter such** attacks, including more aggressive offensive cyber operations, new cybersecurity mandates for U.S. companies, and a partial ban on making ransom payments.

HOW WE GOT HERE

Washington lawmakers and White House officials first deemed ransomware gangs a major national security threat after one group breached the payment systems of a major U.S. pipeline in 2021, forcing the company to shut down fuel delivery to contain the impact. Ransomware attacks involve hackers breaking into organizations' networks and then threatening to delete or publish key data. They typically demand payment in cryptocurrency, which victims can send across borders instantaneously and without drawing public attention.

For example, in February, the group ALPHV took credit for a massive hack of the payments and medical claims subsidiary of UnitedHealth, disrupting health care providers' ability to collect payments across the country.

Since 2021, the Biden administration has unfurled a host of measures to tamp down on the problem. U.S. Cyber Command has said it is using offensive cyber operations to target the gangs, while the FBI has staged a slew of digital sting operations to thwart attacks and gather evidence needed to arrest or indict the groups' members.

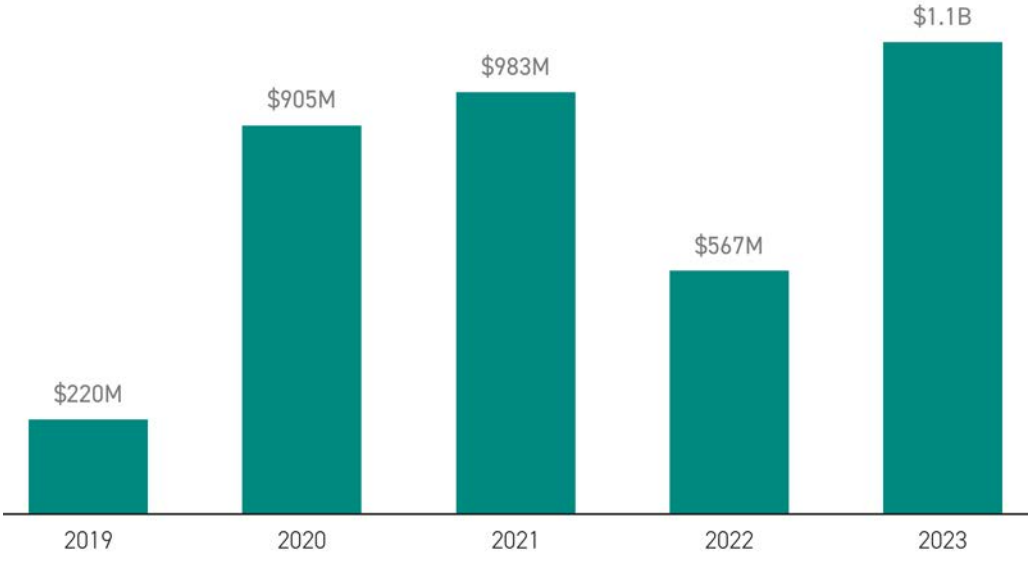
The Biden administration has also tightened cybersecurity requirements for a subset of critical infrastructure providers and sanctioned cryptocurrency firms that help groups launder the proceeds of their attacks. In some cases, officials have even managed to seize crypto wallets used by the gangs, returning multi-million dollar ransoms to the victims. Another big effort has been launching a 50-nation counter-ransomware taskforce to coordinate policy and enforcement against the gangs, which operate across borders.

One big challenge is that victims often conceal attacks due to fears of reputational harm and regulatory scrutiny, making it hard for the government to understand the scope of the problem. But private sector firms have gotten better at collecting data on the attacks. And in 2022, Congress passed a new law that will require victims to report ransom payments to the Cybersecurity and Infrastructure Security Agency starting in late 2025.

U.S. officials and experts suspect ransomware attacks haven't gone down for two major reasons: Russia, where many members of the hacking groups are thought to operate, offers safe harbor to cybercriminals who target the West, according to U.S. spy agencies. Second, ransomware is largely a profit-motivated crime — and victims keep paying as the attacks have gotten more damaging.

Ransomware payments reached over $1B in 2023

Estimated value of ransomware payments made to suspected cyber criminals



Source: Chainalysis
Rosmery Izaguirre/POLITICO

WHAT'S NEXT

In late 2025, CISA is due to issue a new rule requiring critical infrastructure providers to report ransom payments. Some hope the final rule will provide badly needed transparency into the volume and scope of the problem — and potentially even discourage some companies from paying ransoms.

Pressure is also building on the White House and Congress to consider more forceful — and controversial — policies.

One option is for the National Security Agency and U.S. Cyber Command to target gang members with more fulsome cyber or influence operations in an effort to stop or deter their attacks. For example, many experts are pushing the intelligence community to more regularly infiltrate the groups' computer systems and disrupt their ability to stage attacks, distribute payments or communicate.

They argue those steps could undermine the trust and anonymity these decentralized groups need to operate. But others fear doing so could encourage the gangs — or Moscow — to retaliate more forcefully in the U.S.

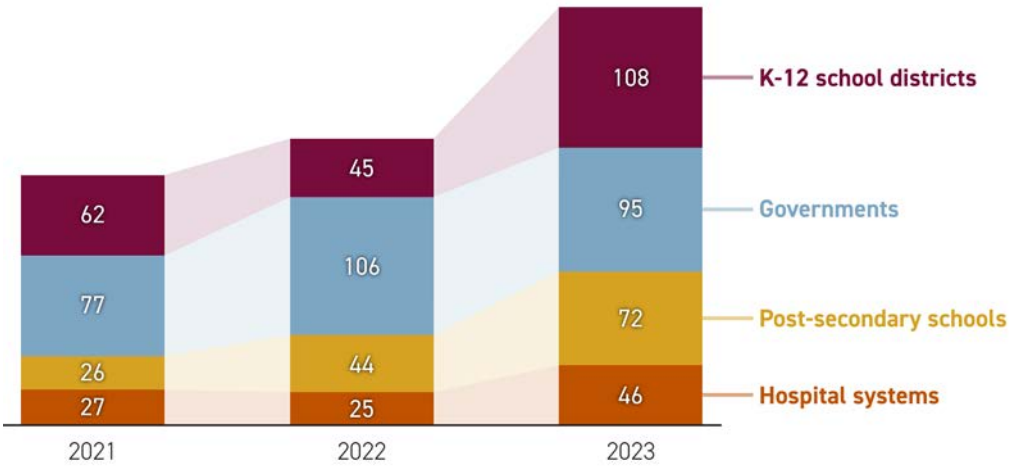
For instance, roughly two months before the UnitedHealth hack, the FBI staged a digital takedown operation against the cybercriminal gang that was responsible for it. Thereafter, the group intentionally targeted U.S. hospitals and healthcare providers, CISA and the FBI have said.

Others see ransomware attacks largely as a product of the poor cyber defenses many U.S. organizations have in place. They argue that the best way to fix the issue is to enforce or create new mandates to coax key organizations into doing more to secure their networks or build resilience for attacks. That could include fining firms, like healthcare providers, that fail to implement baseline cybersecurity standards — a plan the Health and Human Services Department pitched in its fiscal year 2025 budget request.

But industry groups have traditionally balked at increasing legal requirements because the most common victims of ransomware attacks often are the most cash-strapped — and technologically backward — to begin with.

K-12 school districts saw largest rise in ransomware attacks in 2023

Critical infrastructure organizations that reported ransomware attacks, by sector



Note: School districts and hospital systems are comprised of multiple schools and hospitals, respectively.
Source: Emsisoft
Rosmery Izaguirre/POLITICO

Finally, Congress or the White House could move to partially or fully ban victims from making ransom payments. Some believe that would undercut the financial incentives driving cybercriminal hacks, but skeptics fear a ban would merely drive some extortion payments underground — and prevent victims from being able to recover as easily after attacks.

POWER PLAYERS

- **Anne Neuberger:** The White House deputy national security adviser for cyber and emerging technology has spearheaded the Biden administration's efforts to tackle ransomware since 2021. She was instrumental in creating the international counter-ransomware initiative and has recently indicated she is open to a payments ban.

- **The international counter-ransomware initiative:** The 50-nation international partnership — which encompasses most major U.S. allies — will have to play a central role in tamping down on the problem since ransomware gangs recruit from all over the globe — and they are starting to launch attacks as far afield as Latin America and Southeast Asia.

- **The FBI's Cyber Division:** Since 2021, the United States' lead law enforcement agency has pioneered a series of operations to infiltrate and undermine ransomware groups. While the impact of those efforts can be short-lived, the bureau has said it intends to keep up the pressure so long as ransomware groups remain a major national security threat in the U.S.