EXPLAINER | 4:18 P.M.

What's Driving the Surge in Ransomware Attacks?

By Matt Stieb

A gas station runs out of fuel on May 12, 2021, after the ransomware cyberattack caused the Colonial Pipeline to shut down. Photo-Illustration: Yasin Ozturk/Anadolu Agency via Getty Images

As the United States emerges from the coronavirus lockdown, digital experts are combating a "pandemic of a different variety," as the former head of U.S. cybersecurity Chris Krebs warned in May. On several occasions in the past seven months, ransomware attacks have shut down large sectors of the American economy, with hackers taking advantage of lax security measures for an easy payday. The concept is fairly simple: Hackers use malicious software to break into and encrypt a company's data, then hold it ransom until the victim pays up, often in seven-figure installments.

The Biden administration has made stopping these extremely disruptive attacks a national-security priority, but many experts still think that the worst may be ahead of us. Here's what you need to know about the recent string of attacks and what's being done to stop them.

Which businesses have been attacked?

Cyber attacks have become a serious problem for the private sector in recent months:

- In June, an attack on the multi-national meat manufacturer JBS S.A. closed off a quarter of American beef operations for two days, as the firm shut down its computer systems to limit the scale of the breach.
- In May, a cyberattack on Colonial Pipeline forced the company to shut off gasoline supply to much of the Eastern Seaboard, resulting in shortages throughout the South. That same month, an attack shut down the databases of a hospital system in San Diego for two weeks.
- In April, hackers claimed to have stolen 500 gigabytes of data from the Houston Rockets, including contracts and non-disclosure agreements.
- In March, CNA Financial Corp, one of the largest insurance companies in the U.S., was locked out of their network for almost two weeks following a breach.
- And in February hackers accessed a water-treatment plant in Oldsmar, Florida, briefly raising the lye in drinking water to dangerous levels.

These are some of the most damaging break-ins, but they are far from the only examples: One security firm that tracks ransomware attacks estimated that there were some 65,000 successful breaches in 2020. Around the time that Colonial Pipeline's system was compromised, Homeland Security Secretary Alejandro Mayorkas estimated that $350 million in ransom payments were handed out to groups engaging in ransomware schemes last year.

What is a ransomware attack?

Groups engaging in ransomware attacks, the most common form of cybersecurity breach, target businesses or individuals by holding their information hostage, locking them out of their systems, and demanding ransom money from the victim so they can be let back in. This form of cyber crime is popular in part because it is relatively easy to execute: The most common tactics involve using software to get around security holes, or tricking users into downloading malware by pretending to be a source they trust. (This is known as a phishing scam.) As we've learned this year, some companies of profound national-security importance have atrocious security. In testimony before Congress, Colonial Pipeline CEO Joseph Blount admitted that the company wasn't using multifactor authentication to log-in — the simple step requiring users to plug in their password on a computer and confirm their identitiy on their phone or other device.

To end the breach, victims often pay. "Many high-profile ransomware attacks have occurred in hospitals or other medical organizations, which make tempting targets: attackers know that, with lives literally in the balance, these enterprises are more likely to simply pay a relatively low ransom to make a problem go away," the cybersecurity blog CSO explains.

Recent ransomware targets Colonial Pipeline and the chemical distribution firm Brenntag both paid the equivalent of $4.4 million ransoms to the groups that hacked them in May so that they could regain access to their systems and

relaunch operations. JBS paid $11 million to stop their attack. “I know that’s a highly controversial decision,” Colonial Pipeline CEO Joseph Blount said after his firm’s payment was announced. “I didn’t make it lightly. I will admit that I wasn’t comfortable seeing money go out the door to people like this. But it was the right thing to do for the country.”

Blount is not alone: According to a survey conducted by the security firm Kaspersky, more than half of ransomware victims in 2021 paid up to gain access to their own information. However, only a quarter of these firms regained full access.

Who is carrying out these attacks?

Groups known as ransomware gangs work in jurisdictions where American law enforcement can’t reach them; as with other notable breaches of U.S. cybersecurity, the threat is predominantly coming from Russia. The names of the groups are what you might expect from professional online criminals in the former Soviet Republic: REvil, Evil Corp, DarkSide. (Their software weapons have fitting monikers, too, including references to the Greek god of the dead and an iconic anime prankster.) Also unsurprisingly, their threats are often quite sinister: A hacker working with DarkSide, the group that shut down Colonial Pipeline, breached the data of a small education publisher earlier this year and threatened to contact their clients to say they had stolen information that could allow them to make fake ID cards, allowing pedophiles to get into their schools. Thankfully, the New York *Times* reports that the ultimatum was a bluff.

Some hackers have a direct affiliation with Russian intelligence: The NSA and FBI have stated that the historic SolarWinds breach first reported in December 2020 was conducted by groups with connections to Russia’s Foreign Intelligence Service. Notably, this was not a ransomware strike but something called a supply-chain attack; hackers infiltrated the information-technology company SolarWinds, then used that access to break into the systems of the firm’s clients, which included servers operated by NATO, the European

Parliament, the government of the United Kingdom, and several branches of the federal government, including the Treasury and Commerce Departments. In response, on April 15, the Biden administration announced a wave of economic sanctions against several Russian technology companies and financial institutions for their role in the attack and in other "harmful foreign activities."

SolarWinds represents one of the more direct collaborations between Russian intelligence and cybercriminals. More often, ransomware groups operate under an unstated agreement with the Kremlin, as cybersecurity experts recently told the AP:

> "Like almost any major industry in Russia, (cybercriminals) work kind of with the tacit consent and sometimes explicit consent of the security services," said Michael van Landingham, a former CIA analyst who runs the consultancy Active Measures LLC.
>
> Russian authorities have a simple rule, said Karen Kazaryan, CEO of the software industry-supported Internet Research Institute in Moscow: "Just don't ever work against your country and businesses in this country. If you steal something from Americans, that's fine."

To avoid a crackdown by Russian authorities, hackers in Russia generally avoid targeting any businesses in the Commonwealth of Independent States, the intergovernmental organization made up of former Soviet republics.

Why is this happening now?

The trend involves a complex blend of geopolitical and cybersecurity factors, but the underlying reasons for its recent explosion are simple. Ransomware attacks have gotten incredibly easy to execute, and payment methods are now much more friendly to criminals. Meanwhile, businesses are growing

increasingly reliant on digital infrastructure and more willing to pay ransoms, thereby increasing the incentive to break in.

As the New York *Times* notes, for years "criminals had to play psychological games to trick people into handing over bank passwords and have the technical know-how to siphon money out of secure personal accounts." Now, young Russians with a criminal streak and a cash imbalance can simply buy the software and learn the basics on YouTube tutorials, or by getting help from syndicates like DarkSide — who even charge clients a fee to set them up to hack into businesses in exchange for a portion of the proceeds. The breach of the education publisher involving the false pedophile threat was a successful example of such a criminal exchange.

Meanwhile, Bitcoin has made it much easier for cybercriminals to collect on their schemes. "Cryptocurrency provided the perfect answer to allowing hackers to prey on their victims and extort unlimited and anonymous cash payments while completely minimizing their exposure of being caught by law enforcement," programmer Stephen Diehl wrote in a Twitter thread following the Colonial Pipeline hack. As Dahl explained, before the crypto boom, cyber criminals had to resort to huge numbers of pre-paid gift cards in amounts as small as $1,500 for ransom payments — not exactly a perfect system when millions of dollars are at stake. In-person payments were obviously off the table owing to the threat of law enforcement raiding the hand-off. Wire transfers were out, too, as banks would never allow such a massive transfer to a criminal operation. But thanks to the anonymized nature of Bitcoin transfers, there is now a clean international method in which "there's no upper bound on the extortion amount." Thus, the real value of the Colonial Pipeline ransom was not $4.4 million, but 75 Bitcoin.

Finally, there's the behavioral aspect. With firms sending out hundreds of millions of dollars in Bitcoin, ransomware attacks have proven to be a successful way for criminal enterprises to make serious money without having to leave the house. "Attacks happen for one reason and one reason only," Brett

Callow, a threat analyst with the antivirus firm Emsisoft, told NPR. "They are profitable. If you make them unprofitable, the attacks will stop."

What can businesses and governments do to stop the attacks?

While the Biden administration has encouraged businesses to shore up their cyber defenses and "review corporate security," intelligence agencies are working to stop the attacks at their source. In April, the Department of Justice established a Ransomware and Digital Extortion Task Force to tackle the entire process, including efforts to take down services that "support the attacks, such as online forums that advertise the sale of ransomware or hosting services that facilitate ransomware campaigns," according to the *Wall Street Journal*. The task force has already had some success. On June 7, the Department of Justice announced that it had recovered 85 percent of the Bitcoin that Colonial Pipeline paid to DarkSide. While Bitcoin transactions are largely anonymized, the nature of Blockchain technology allows law enforcement to track how funds move to a limited extent. "Following the money remains one of the most basic, yet powerful tools we have," said Deputy Attorney General Lisa Monaco on the day of the announcement.

President Biden has also said he would bring up the surge in attacks with Russian president Vladimir Putin at their June 16 summit in Geneva, though the tacit support the Kremlin lends to hackers undermining their adversary suggests little will come of the conversation.

Closer to home, the Biden administration has encouraged firms to tell the FBI as soon as they are hacked and discouraged them from paying ransoms so as to break the lucrative cycle. "Whether you're private sector, public sector, whatever — you shouldn't be paying ransomware attacks, because it only encourages the bad guys," Energy Secretary Jennifer Granholm said on June 6. Granholm is in favor of the idea of legislation banning firms from paying ransoms to

cybercriminals, though she added, “I don’t know whether Congress or the president is at that point.”

Noted digital-security expert and former president Donald Trump has offered his own solution: In a June 7 interview with Fox Business, he recommended a return to “a much more old-fashioned” way of doing things, citing what he has learned from observing his tech-savvy teenage son. “He’s a young person, and he can make these things sing, and when you put everything on internet and on all of these machines — you never see a piece of paper,” Trump said. “I really think that you have to go back to a different form of accounting, a different form of compiling information.” So far, the idea isn’t getting much traction.

TAGS: EXPLAINER RANSOMWARE CYBERATTACKS HACKING MORE

1 COMMENT

THE Intelligencer FEED

4:55 P.M. AWARDS

Darnella Frazier, Who Filmed George Floyd’s Murder, Gets Pulitzer Nod

By NIA PRATER

The Pulitzer board awarded her a special citation, saying her video showed ”the crucial role of citizens in journalists’ quest for truth and justice.”

4:50 P.M. POLITICS

Merrick Garland Unveils Plan B for Protecting Voting Rights

By ED KILGORE

As new congressional legislation stalls, the Justice Department will utilize the powers it already possesses to fight voter-suppression measures.

4:18 P.M. EXPLAINER

What's Driving the Surge in Ransomware Attacks?

By MATT STIEB

From gas to meat, hackers keep disrupting large sectors of the economy. Here's why the attacks are getting easier and what's being done to stop them.

MOST POPULAR

1. **The Southern Baptist Church Is Going to Hell in a Handbasket**
   By ED KILGORE
2. **The Hot New Vaccine Conspiracy Theory: It Turns You Into a Magnet**
   By PAOLA ROSA-AQUINO
3. **The Tiger Mom and the Hornet's Nest**
   By IRIN CARMON
4. **Republicans Are Furious Fast-Food Workers Are Getting a Raise**
   By JONATHAN CHAIT
5. **What Can We Expect From the Pentagon's UFO Report?**
   By MATT STIEB

4:11 P.M. NYC MAYORAL RACE

Maya Wiley and Eric Adams Trade Jabs Over Cops and Guns

By NIA PRATER

During the most recent NYC mayoral debate, Wiley declined to say whether she would disarm NYPD officers. Adams called her answer "alarming."

3:50 P.M. COVID VACCINES

Johnson & Johnson Must Toss 60 Million Vaccine Doses Made at Troubled Plant

By CHAS DANNER

Only ten million J&J doses produced by Emergent BioSolutions' Baltimore facility have been cleared for use.

3:26 P.M. 2021 CALIFORNIA RECALL ELECTION

Why Recall Fever Is Sweeping California

By ED KILGORE

Easy rules, intense reaction to COVID-19 restrictions, and a Republican Party with nothing better to do have all fueled a wave of recall drives.

1:40 P.M. POLTIICS

Will Women Be Required to Register for the Military Draft?

By ED KILGORE

After the Supreme Court dodged the question, Congress could move to include women — or abolish registration altogether for the first time since 1940.

1:17 P.M. DEPARTMENT OF JUSTICE

Trump DOJ Seized Adam Schiff's Records in Search for Leaks

By MATT STIEB

Prosecutors seized metadata of the top House Intelligence Democrat, Eric Swalwell, and a minor in a failed hunt to find those leaking to reporters.

1:02 P.M. SIDE EFFECTS

CDC Flags Rare Cases of Heart Swelling in Young People After COVID Jab

By PAOLA ROSA-AQUINO

Reported myocarditis cases make up a tiny fraction of the nearly 130 million Americans who have had both doses of the Pfizer or Moderna vaccine.

9:57 A.M. INTELLIGENCER CHATS

Why It's So Hard to Hire Restaurant Workers Right Now

By CHRIS CROWLEY AND BENJAMIN HART

For one thing, the pandemic allowed servers, cooks, and others to reevaluate their place in a precarious industry.

9:44 A.M.

Doubles as a pretty good album cover

Photo: @justinsink/Twitter

8:00 A.M. INEQUALITY

The Limits of Wealth-Tax Populism

By ERIC LEVITZ

Safeguarding democracy from inequality will require much more than soaking the superrich.

6/10/2021 NYC MAYORAL RACE

Key Moments From the Third NYC Mayoral Debate

By MATT STIEB

Highlights from a shorter and arguably more contentious contest.

6/10/2021 POLITICS

Ilhan Omar Backs Down In Latest Blowup With Democrats

By ED KILGORE

The congresswoman's remarks about Israel, Hamas, the U.S., and the Taliban were taken out of context, and she was forced to issue a "clarification."

6/10/2021 SPORTS

Rafael Nadal Is an Artist Too

By CAIRA CONNER

Federer gets all the odes. But there's beauty in the King of Clay's game — and in his foibles.

6/10/2021 MEDIA

Jeffrey Toobin Returns From 'Zoom Dick' Exile

By NIA PRATER

CNN welcomed him back eight months after he was fired by *The New Yorker*, which he called "excessive punishment."

6/10/2021 THE NATIONAL INTEREST

Republicans Are Furious Fast-Food Workers Are Getting a Raise

By JONATHAN CHAIT

It's almost as if they object to any outcome that gives low-wage workers more money.

6/10/2021

Say what?

> Feinstein, asked about some Dems saying they'd choose democracy over the filibuster: "If democracy were in jeopardy, I would want to protect it. But I don't see it being in jeopardy right now."
>
> **—@AndrewSolender**

6/10/2021 POLITICS

Joe Manchin's Silent Partners in the Senate

By ED KILGORE

The West Virginian is happy to take the heat for Democrats who quietly oppose filibuster reform, and they are happy he's happy.

6/10/2021 INFLATION

Why Inflation Is Lower Than It Looks

By ERIC LEVITZ

Prices are returning to the pre-pandemic norm, which looks like a giant spike in annual inflation.

6/10/2021 ENVIRONMENT

Keystone XL Pipeline Canceled

By PAOLA ROSA-AQUINO

The developer is ending the controversial pipeline project, which would have pumped 800,000 barrels of Canadian crude oil to Nebraska per day.

6/10/2021 D.C.

Inside the Big-Donor Scramble for a Biden Ambassadorship

By GABRIEL DEBENEDETTI

"They are the closest things we have to somebody being declared a lord or a lady." But the White House might be changing the rules.

6/10/2021 COVID-19

The People Who Transformed Themselves During the Pandemic

By EVE PEYSER

Is there such a thing as post-traumatic growth?

6/9/2021 NYC MAYORAL RACE

Where Exactly Does Eric Adams Live?

By MATT STIEB AND NIA PRATER

Mayoral front-runner gave a tour to the media of a Brooklyn brownstone he owns following a report that suggests he may be shacking up in New Jersey.

6/9/2021 UBER

Uber Drivers Aren't Making More Money As Prices Surge Amid Shortage: Report

By MATT STIEB

Despite the 50 percent surge in rideshare prices amid the reopening, drivers reportedly aren't reaping the benefits.

6/9/2021 NYC MAYORAL RACE

Dianne Morales Fires Dozens of Staffers As Turmoil Continues

By NIA PRATER

Just three days before early voting begins, the leftist candidate's campaign remains in crisis.

6/9/2021 CORONAVIRUS VACCINE

U.S. to Buy 500 Million Pfizer Doses to Donate Abroad

By MATT STIEB

The shots are a big improvement on the White House's global effort but far from the estimated 11 billion doses needed worldwide to end the pandemic.

READ MORE ON THE Intelligencer HOMEPAGE