The Problem

Companies are paying off hackers to the tune of more than $450 million a year, and experts say new technology will give thieves even more power.

Why It Matters

Ask any CEO whose company operations have been hit by a hacker—few things can be more disruptive.

Adam Smigielski/Getty Images

Ransomware groups as sophisticated as S&P firms are scooping up astounding sums from organizations. We get an inside look at a cloak-and-dagger world from an anti-espionage company.

By Peter Lauria

The Solution

Build better defenses, largely by making sure employees follow security steps and installing greater intelligence.

It was into the small hours of what was technically Saturday morning, but really was still Friday night. Earlier that evening, a group of hackers had broken into the network of an undisclosed company, gained possession of proprietary data, and demanded money for its return—a so-called ransomware attack—setting off a mad scramble. Posing as a company IT manager, an outside negotiator from Arete Incident Response, a cybercrime prevention firm, had begun negotiating with the hackers over an encrypted messaging platform. After more than eight hours and dozens of messages, the negotiator had finally reached a deal to exchange Bitcoin for the release of the data.

Or so he thought.

At the last minute, the hackers came back with an additional demand: an extra 20 percent payment, in a different cryptocurrency, to be deposited into a separate account. The request wasn't unusual—what criminal doesn't try to get as much money as possible? But fending off this kind of request can take quick thinking. Arete's Moscow-born negotiator realized the malware was of Russian orgin. So he made a seemingly casual offer. "Can I buy you a case of Baltika [beer]?" he asked, gambling that the hacker was from the region. And he was right: "Ha ha, it would take a lot more than a case," the hacker replied, and dropped the additional demand—saving the firm about $300,000.

It's no secret that ransomware has come a long way from the days when lone-wolf hackers would take control of personal computers and demand a few hundred dollars to unlock them. But the pace of ransomware's growth—and its brazenness—continue to astound and confound the corporate world. Today, hacker groups as big and sophisticated as S&P 500 companies are operating in pretty much every country around the world, often with tacit approval from, or in concert with, nation-states. According to one watchdog group, last year's 490 million-plus global ransomware cases cost companies some $457 million. Firms are now forking over an average of $260,000 each time they're hacked, a figure large enough to crack, if not

Gremlin/Getty Images

break the bank, of many independent businesses.

Joe Mann, CEO of Arete, calls it "the digital pandemic of our times." His firm has worked on cases for many major corporations, most of which don't want their names revealed. In fact, seldom does anyone in the industry talk about specific clients. It's a cloak-and-dagger, nameless, faceless world. For both business and negotiation purposes, it's better for hackers to believe they're talking to a company representative rather than a professionally trained negotiator.

But make no mistake: corporate leaders and boards are increasingly turning to companies like Arete, Coveware, CyberSecOp, and others to help them deal with what are essentially "large, professional, criminal organizations," Mann says. Since its founding in 2015, Arete has been involved in roughly 7,000 ransomware-prevention or ransomware-response engagements for companies around the world. Over the last two years, Mann's staff—encompassing forensic investigators, data and analytics experts, AI and machine-learning specialists, cybersecurity-defense and intelligence officers, and others—has grown by more than 500 people.

Still, how do negotiations with hackers really work? And how do firms feel about caving in and paying staggering sums to nameless thieves, especially at a time when artificial intelligence can seemingly track the comings and goings of just about anyone? In a series of interviews, Mann gave *Briefings* a rare inside look into this hidden corner of corporate espionage—one in which many firms are running scared and are desperate for his help. Arete, he says, has "facilitated" payments of a few thousand to tens of millions of dollars on behalf of firms that are, for obvious reasons, notoriously shy about all of this. In nearly every case, he says, what they're asking him to do is simple: make it go away, as fast and as quietly as possible.

Big-Game Hunting

The first known ransomware attack took place in 1989, when floppy disks were mailed to 20,000 guests of the World Health Organization's AIDS conference. Once users loaded the disks into their hard drives, malware took control of their computers, and a message appeared demanding $189 be mailed to a post-office box in Panama.

It might have been small-time stuff, but from such humble beginnings, ransomware and digital extortion would grow up alongside the internet, then piggyback off the proliferation of mobile devices. But it wasn't until the mid-2010s that hackers started going after corporations as part of a phenomenon known as "big-game hunting." Its premise is simple: corporations are easy targets,

"THE REALITY IS THESE SITUATIONS ARE VERY MUCH LIKE HOSTAGE NEGOTIATIONS."

says Craig Stephenson, managing director of the North America CIO/CTO practice at Korn Ferry. "Most companies attempt to be prepared for these events, but each situation is unique," he says. Or as Bob Irwin, a Korn Ferry senior client partner, puts it, "The approach is pretty much, 'I hope it doesn't happen to me.'"

Firms do have money, though, which means they can afford to pay high ransoms. As a result, digital extortionists have pretty much declared open season on them. In 2021, a watershed year for ransomware criminals, there were 623 million attacks costing businesses $765 million in payouts. One oil and gas behemoth alone admitted paying a ransom of $4.4 million after its systems were compromised. In the same year, Saudi Aramco, the state oil company of Saudi Arabia, had to shut down its network and destroy 30,000 computers following an attack involving a $50 million ransom demand.

Incidents like that are why leaders and boards are increasingly turning to firms like Arete for help. Based out of a tiny suite in a Pentagon-esque complex in Boca Raton, Florida, the firm not only provides technical and operational assistance to protect networks and data, but also specializes in negotiating with ransomware groups. To broker deals, it employs everyone from ex-military to law enforcement veterans to government officials and others skilled in digital forensic investigations and hostage communications. Two of Arete's top executives previously held high-ranking positions in intelligence and cybersecurity in the U.S. military, the National Security Agency, and other federal departments.

"The reality is these situations are very much like hostage negotiations," says Mann.

Double Extortion

Like any enterprising criminal, digital extortion groups are getting more sophisticated in both techniques and targets. It's widely known, for instance, that hackers target companies that have bought cybersecurity insurance, asking for the upper limit, knowing the company will most likely just pay whatever its policy covers. That's small-time

Yacobchuk/Getty Images

now. Today, hackers target specific business areas that are getting investments or growing at advanced rates. They're using tactics like escalating privileges to dig deeper into the bowels of an organization's data.

"It's not about giving data back to the company," says Dima Rabadi, assistant professor of cybersecurity at Penn State Shenango. "Now it's about not giving data to someone else." The practice, known as double extortion, has become de rigueur for digital extortionists: they not only restrict access to a company's networks, but also extract data to sell to the highest bidder on the dark web. Double extortion is rampant in data-sensitive businesses like financial services, health care, and aerospace and defense.

Moreover, experts worry that ChatGPT and other so-called generative artificial-intelligence platforms will lower the bar for entry into ransomware, given how adept they are at reproducing images, code, and other data. Lieutenant General (ret) Bill Mayville, a Korn Ferry consultant and former vice commander, US Cyber Command, says AI-enabled tools "make it easier for the bottom rung of criminals to get

Corporate Ransomware: 3 Infamous Incidents

They rarely, if ever, become public, but multimillion-dollar demands from organized hackers with colorful names are surprisingly common.

WHERE'S THE BEEF?

What was stolen:
REvil, one of the most notorious ransomware groups, took down the processing plants of a meat producer.

Ransom demanded:
$22.5 million
(in Bitcoin)

Resolution:
Following negotiations, the company agreed to pay an $11 million ransom, still one of the largest payouts ever.

GROUNDED

What was stolen:
In 2020, the Ragnar Locker ransomware gang infiltrated a global travel-services company, corrupting 30,000 computers and obtaining financial, security, and employee data.

Ransom demanded:
$10 million
(in Bitcoin)

Resolution:
Citing the impact of COVID-19 on its business, the company negotiated the payment down to $4.5 million.

OUT OF GAS

What was stolen:
In 2021, the DarkSide hacker group gained access to the network of a major oil and gas company, infecting billing, tracking, and other files, and forcing operations to shut down for two days.

Ransom demanded:
$5 million
(in Bitcoin)

Resolution:
The company ultimately paid $4.4 million.

Sources: *NPR*, *Reuters*, *The Wall Street Journal*

into ransomware." Given that most ransomware attacks are launched when an employee opens a corrupted email or clicks on a link to malware, it's not an insignificant fear. In fact, it is a very real possibility in the age of remote work.

Every year around the holidays, for instance, Casey Cegielski, a professor in the department of business analytics and information systems at Auburn University's Harbert College of Business, mocks up a fake email about a package delivery, which he then sends to business leaders and employees associated with his research or the school. It's the most basic of phishing scams—and every year most of the email's recipients click on the link. They are sent to a page featuring a holiday greeting and text reading, "You just got infiltrated."

"Business leaders think ransomware is a technology issue," says Cegielski. "It's not. It's a people issue."

As with all things in business, ransomware is also a financial issue, and the current economic environment could put even more businesses at risk, says Josephine Wolff, associate professor of cybersecurity at The Fletcher School at Tufts University. In economic downturns, she says, when companies are laying off workers and looking to save money, cybersecurity is often a target of cost cuts. Some firms take the approach that simply having cybersecurity insurance is enough, for instance. "Information and technology leaders are always under pressure to protect the company in the most cost-effective way possible," says Wolff.

LockBit, REvil, and WannaCry

In the event of an attack, it's critical to get systems back up and running as fast as possible. Of course, companies want their data returned safely or the disruption to operations halted. Of course, they loathe the idea of paying a ransom. Of course, if they have to pay one, they want it to be as little as possible. But the longer operations are paused, the worse it is for the company. "You can't put a price on reputation and trust," says Cegielski.

Mann recounts one incident in which hackers took down a division of a large retail bank. As concerned as they were about the attack, bank leaders were just as concerned about some customers being frozen out of their accounts. "If people couldn't get their money the next morning," says Mann, "that could have cost the bank more than the ransom."

But the good news, surprisingly enough, is that some high-tech corporate espionage cases can be foiled as fast as they emerge—at least by the right anti-ransomware firm. Mann maintains that his firm, with its army of intelligence personnel, has managed to avoid payment in 74 percent of the ransomware attacks it has handled. When his clients have had to pay, he estimates, his firm has successfully negotiated the fee down by an average of 80 percent.

In the bank case, in fact, Mann says his negotiators got the hackers to agree to a payment 95 percent below their original demand—"and all before customers hit the ATM in the morning."

Much like graffiti artists, the biggest ransomware groups in the world aren't shy about leaving the digital signatures of their groups, with names like Hive, LockBit, REvil, and WannaCry. Both the malware and the requests of each group exhibit distinct, identifiable traits and characteristics.

Knowing this, Mann's

PHOTO CREDIT: Maxiphoto/Getty Images

"BUSINESS LEADERS THINK RANSOMWARE IS A TECHNOLOGY ISSUE. IT'S A PEOPLE ISSUE."

team can track and analyze the digital keys of the various groups. Through techniques like parent-child modeling, they can quickly tell whose "fingerprints" are on an attack, or how a source code has been tailored or modified by a splinter group or lone wolf. After making an identification, Arete's model can predict the hacker's behavior and how far they're likely to take the extortion. Firms like Arete also have the ability to jump in, stop the damage, and retrieve the stolen information from right under the hacker's nose—or block the effects of any malware.

But even with the bad guys showing their hand, most cyber pros expect that hackers' power will only grow as their techniques and tactics become more sophisticated and widespread. Ultimately, says Tufts' Wolff, preventing ransomware attacks will hinge as much on negotiations and communications as on digital solutions. She says the rise of double—and even triple and quadruple—extortion makes negotiating with ransomware actors that much more delicate. "It just adds so much more complexity to the negotiation," she says, creating more chances for the company to make a mistake or be further exposed.