ILLUSTRATION BY ERIK CARTER

CRYPTOCURRENCIES | FEATURE

How Ransomware Gangs Are Fueling a New Cybersecurity Arms Race

Ransomware and crypto have become inseparable, and they're fueling a new arms race for protection. Demand for cyber insurance is growing.

By Jack Denton Follow

Updated December 6, 2023 / Original December 6, 2023

Trading options in Chicago, Matthew Leidlein made a living off volatility. These days he's into Bitcoin, though not for its wild price swings. Rather, he's lending it to companies being extorted by ransomware gangs. Clients this year included a local government in Mississippi that paid a ransom of more than $250,000 in crypto to end an attack that took down county systems for almost three weeks.

"These threats are a reality for anybody that has data on the internet," says Leidlein, 47. His firm, Digital Asset Redemption, has lent more than $90 million in crypto in around 175 incidents this year.

Ransomware is booming, with Bitcoin at the heart of it. Attacks have surged in recent years, often using Bitcoin and other cryptocurrencies for ransom payments and trafficking in stolen data. Attacks hit a wide range of targets, including large and small companies, hospitals, schools, and government entities.

Crypto has legitimate backers and applications. Firms like Fidelity and BlackRock may soon win approval to launch exchange-traded funds holding Bitcoin—a prospect that has pushed up the token's price more than 150% this year. A vast blockchain-based ecosystem is also developing for trading, payments, and other apps.

At the same time, ransomware and crypto have become inseparable, and they're fueling a new arms race for protection. Demand for cyber insurance is growing. While cybersecurity stocks have surged and valuations are steep, there is a long-term bull case for names like CrowdStrike, Palo Alto Networks, and Zscaler, according to some analysts (see 3 Stocks to Play the Cybersecurity Boom).

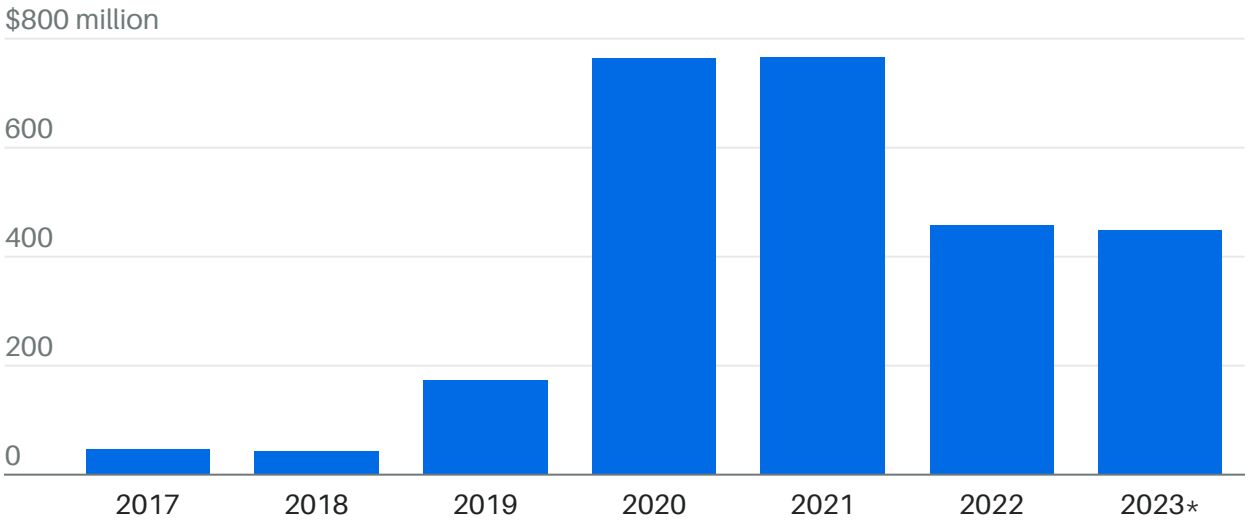
New regulations could fuel demand for cyber protection, too. A Securities and Exchange Commission rule going into effect in mid-December will require publicly traded companies to report material breaches within four days of discovery by the firm, assuming there

isn't a national security risk. An associated rule will require companies to disclose protection measures in annual reports.

The push for protection comes as attacks take a growing economic and social toll. Ransomware hacks will cost an estimated $30 billion in 2023, according to cybersecurity software company Acronis. The costs can be 10 times the amounts paid in ransom—averaging $4.5 million per incident, according to IBM; additional costs include legal and consulting fees, upgrades to computer systems, and regulatory fines.

Profiting off Ransomware

Hackers have extorted more than $2.7 billion in crypto through ransomware attacks since 2017.



*Through June 30

Source: Chainalysis

"The current environment is probably one of the worst I've seen," says George Kurtz, CEO of CrowdStrike. Hacking speed has increased sharply in the past 18 months, he points out. The average "breakout time"—how long it takes criminals to begin moving across corporate systems after a security breach—is now 79 minutes, he says, with top hackers breaking through in seven minutes.

Attacks have become a fact of corporate life. An estimated 72% of firms with annual revenue over $5 billion were attacked in the past year, according to Sophos, a cybersecurity software firm. The number of attacks in the third quarter was up 95% from a year earlier, says cyber specialty insurer Corvus. Hackers could reap $1 billion in ransoms this year, more than the years 2018 through 2020 combined, according to estimates from crypto data firm Chainalysis.

Scores of big names have been hit. Recent victims include Clorox, rail company Wabtec, Fresh Del Monte Produce, Caesars Entertainment, MGM Resorts—even the U.S. Marshals Service.

The toll extends to consumers, too, as hackers post stolen data on the internet. Emails urging a password change due to a data leak often result from hacks exposing Social Security numbers, credit cards, or other financial data.

The healthcare industry appears particularly vulnerable. Hackers often hit hospitals because disrupting their operations can take a high toll, affecting patient care and damaging a hospital's reputation. Hackers stole health data of nearly nine million people from a medical transcription service this spring, for instance, and a hospital/clinic chain in the Midwest was recently targeted. Medical data are valuable, partly because hospitals and insurers may face personal liability claims if the data are leaked, exposing highly sensitive information about patients.

From Floppy Disks to Bitcoin and Ransomware Gangs

Before the internet took off in the early 1990s, ransomware circulated via floppy disks, and cash payments went through the mail. Bank transfers weren't ideal because they could be traced. The advent of Bitcoin in 2008 made getting paid and trafficking in stolen data far more seamless. While Bitcoin transactions are visible publicly on the

network's ledger, or blockchain, they consist of alphanumeric internet addresses that are anonymous and difficult to trace. The growth of crypto coincided with a sharp rise in malicious code: From 2010 to 2015, the number of unique ransomware variations exploded from 10,000 to four million, according to CrowdStrike.

"Without crypto being a main part of the ecosystem, ransomware would be a lot harder," says Kurtz. "It's a relatively smooth process to get paid cross-border with a lot of anonymity."

Armed with crypto as a currency, cybercrime is now often conducted by gangs based in hostile countries like Russia, running the operations like multinational businesses. Several gangs sell "ransomware as a service," providing code and other hacking tools on the black market in exchange for a cut of the profit. A software kit may include 24/7 tech support, user reviews, and other features similar to traditional "software as a service," according to CrowdStrike.

Kits go from $40 a month up to thousands of dollars. When hackers breach a network, they may then sell access to other gangs in online auctions, spreading the damage. "Twenty-five years ago, if you wanted to be a good hacking crew, you needed a high level of technical acumen," says Matt Gorham, a former Federal Bureau of Investigation cyber official, now at consulting firm PwC. "Today, a credentialed criminal group, particularly Russian-speaking, can purchase everything they need to be a good hacking crew overnight."

Gangs operate like businesses in other ways, including employees, overhead, and expenses for specialists in areas like network-penetration testing, according to Jacqueline Burns Koven, a former U.S. intelligence officer who now heads cyberthreat intelligence at Chainalysis. Based on hacking activity, it appears that gangs also take vacations: Activity tends to fall in summer and pick up again in the fall.

Hackers no longer just encrypt data, moreover, demanding a ransom to free it up. Now, a typical attack is a double extortion, encrypting data as well as threatening to "exfiltrate" the data, or release it publicly. The threats often extend to disrupting operations; when the city of Baltimore refused to pay a $76,000 Bitcoin ransom, damage to the city's infrastructure eventually hit $18 million.

Companies and governments face tough choices—whether to pay the extortion or suffer the consequences.

To make it personal, hackers often begin with harassment. In a recent case involving a large financial firm, threatening phone calls and text messages went out to executives, board members, and even clients, says Justin Harvey, vice president of response services at cybersecurity consultant Kivu. Hackers demanded $20 million worth of Bitcoin, and the first interaction was "we want Bitcoin or we hurt you," he says. "It gets quite emotional and can be utterly debilitating for an organization," he adds.

Many companies and customers can become vulnerable in a single hack, says Koven, especially as hackers increasingly target services like payroll providers. After a gang called CLOP exploited a hole in a corporate file-transfer system in June, for instance, entities such as the BBC, British Airways, and Shell were among thousands of organizations targeted.

Because the risks are so high, far more companies are buying cyber insurance. Cyber premiums reached $12 billion in 2022, and could grow up to 30% each year to $23 billion by 2025, according to S&P Global Ratings. Most of the big insurers, including AIG, Chubb, and Travelers offer cyber policies. "Cyber risk premiums are growing rapidly because it's a risk that virtually every enterprise out there faces," says Meyer Shields, an insurance analyst at Keefe, Bruyette & Woods.

Yet as attacks proliferate, insurance is getting stingier and costlier. Many insurers won't write a cyber policy without a growing array of security upgrades, says Jason Krauss, a cyber product leader at broker WTW. Lloyd's of London, which runs the world's largest insurance marketplace, recently changed rules for carriers and brokers, requiring that cyber policies include exemptions for losses arising from state-sponsored attacks. Without those restrictions, Lloyd's said in August, losses from cyber could be so large that they "expose the market to systemic risks."

Insurance has another downside: It could actually increase ransom demands. According to Candid Wüest, head of intelligence at Acronis, hackers breached a European company and demanded $4 million, to which the firm countered with $1.1 million. "The response was, 'Well, we've seen your policy, and you're insured for $6 million, so we think $4 million is actually fair, and it's not even your money,' " Wüest says.

Law enforcement has had some success at recovering ransom paid in crypto. A majority of the 75 Bitcoins paid by Colonial Pipeline in 2021 — worth $4.4 million at the time—was recovered, for instance. Governments are also trying to choke off crypto from criminal enterprises. The U.S. and dozens of other countries recently agreed to share a blacklist of crypto wallets linked to ransomware hackers. Some governments, including the U.S., also pledged not to pay ransoms in attacks on official institutions.

Even if governments refuse to pay, however, companies aren't likely to follow suit. A recent survey of chief information security officers by software firm Splunk found that 96% of respondents had suffered a ransomware attack and 83% of executives said they paid the ransom. Banning ransom payments is also controversial with law enforcement. The FBI cautioned Congress in 2021 against a blanket ban, arguing that it may only exacerbate the chronic underreporting of attacks.

The SEC, for its part, is pushing for more transparency with its new disclosure and reporting requirements. But the rules, while well intentioned, may only exacerbate the problem—especially by mandating disclosures of corporate breaches within four days. Industry groups like the Chamber of Commerce and Bank Policy Institute have said the rules could prematurely expose hacks publicly, even while they're ongoing, raising security risks and encouraging more hackers to attack. Companies now take an average of 5.5 days to contain an incident, according to Palo Alto Networks. Republicans in the House want the disclosure rules repealed, though that is unlikely under Democratic control of the Senate and White House.

Hackers in some cases are bragging about their attacks to the SEC to ramp up the pressure during negotiations. The hacking gang BlackCat reported one of its victims, MeridianLink, to the SEC in November, as it pressured the financial-software company to pay a ransom. MeridianLink, in a statement, said it found no evidence of unauthorized access to its production platforms and that the incident caused "minimal business interruption."

For Leidlein, the massive growth of ransomware has turned into a thriving business. His firm is now busy with cases, he says, working alongside insurance companies, law firms, and consultants dealing with hacks. For his services, he generally charges 1% to 2% of the Bitcoin lent, plus consulting fees. Ideally, he says, the goal is to "salvage the best outcome from a bad situation."

Write to Jack Denton at jack.denton@barrons.com