How ransomware exploded in the age of Bitcoin

decrypt.co/15394/how-ransomware-exploded-in-the-age-of-btc

Adriana Hamacher December 21, 2019

FeaturesLong Reads

Thanks to superior strains of malware, 90% of ransom demands are now met—in bitcoin, the hackers' currency of choice. Ransomware celebrates its 30th birthday.

By Adriana Hamacher

Dec 21, 2019

9 min read

Image: Unspash

Ransomware turns 30 this month. And the malicious software, invented by the well meaning but wacko evolutionary biologist Joseph L. Popp, is thriving.

Attacks spiked by 118% during the first quarter of this year, with hackers singling out for punishment state and local governments, while continuing to target businesses, universities, and hospitals.

Ransomware's robust health is due to three symbiotic factors: our increasing reliance on digitization; ever more sophisticated crooks delivering more powerful viral strains, and the prevalence of untraceable ransoms—now almost always paid in bitcoin or other cryptocurrencies.

Hackers' demands are also increasing along with the chilling efficacy of their product. According to ransomware recovery specialists Coveware, the average ransom payment increased by 184% in the first half of 2019. Largely, that's thanks to an increasing number of attacks with new ransomware strains such as RYUK on large enterprises. The average ransom demanded, internationally, is now $4,300.

Desperate for a quick solution, most victims pay up, data recovery professionals told *Decrypt*. In fact, according to one report, many businesses have begun hoarding cryptocurrencies, in case of an attack. Is it any wonder then that some analysts believe major ransomware attacks could be affecting the price of cryptocurrency?

Happy Birthday ransomware

Ransomware refers to the category of computer viruses that are designed to quickly across computer networks and encrypt the files on them; the idea is to hold sensitive documents hostage until the victim pays ransom to the hacker.

The vulnerability of those targeted—nursing homes, providers of local infrastructure, and cities—gives them little alternative. In May, an RYUK attack on the City of Riviera Beach, Florida, forced the local government to cough up $600,000 to decrypt the frozen files. In October, hackers hit the administrative website of the City of Johannesburg, in South Africa, and threatened to publish the stolen data on the Internet—unless they received a $30,000 bitcoin ransom. The city refused to pay.

But as bad as the blight is, ransomware wasn't born bad.

Harvard-educated Popp, its inventor, was a polymath, and ransomware was born in 1989 out of his desire to combat AIDS, or so he claimed. In his misguided determination to amass funds to thwart the disease, he mailed more than 20,000 infected floppy disks to the delegate list of a World Health Organisation forum. When the recipients ran the disks, their computers froze, and an onscreen message instructed them to send funds to access a second disk that would restore their files.

Joseph L.Popp aged 18. Image: Eastlake North High School yearbook

Popp was arrested, but deemed mentally unfit to stand trial due to his increasingly strange behavior (which included wearing condoms on his nose and putting curlers in his beard to ward off radiation.) He died in 2006 in a car accident and didn't live to see his invention grow up, and—enhanced with a more effective method of encryption—become one of the world's most prevalent cybercrimes.

Ransomware and bitcoin

For many years, however, ransomware languished as a small-time enterprise. It wasn't until bitcoin began gaining traction, in 2012, that it really took off. Hackers fell in love with the decentralized digital currency, which made it difficult to trace or block payments, and it became ever easier to launder their ill-gotten gains as more cryptocurrencies hit the scene.

"I don't think there is much doubt that ransomware and cryptocurrencies go hand in hand," Edward Cartwright, Professor of Economics at De Montfort University, in the city of Leicester, UK, told *Decrypt*. "Ransomware is highly reliant on cryptocurrency and bitcoin in particular."

Bitcoin accounted for about 98% of ransomware payments made in the first quarter of 2019, according to data from Coveware. As a result, it's become an inextricable part of the ransomware model.

"Not only does it offer anonymity and untraceability to criminals it is also something that victims are willing to engage with, said Cartwright.

The ransomware industry

Indeed, some experts say the increasing acceptance and understanding of cryptocurrency has driven ransomware from being a rarified crime into something far more common.

“I strongly believe that cryptocurrency has played a role in the ransomware epidemic,” Victor Congionti cofounder and CEO of New York-based Proven Data Recovery, told *Decrypt*.

Of course, in some cases, victims are able to catch intruders before ransomware has been activated or fully spread. In other cases, when the particular strain is “in the wild,” it may be possible to reverse engineer or create a “decryption utility,” Congionti said. But nine times out of ten the only way to reinstate files is to obtain decryption tools by paying the ransom, he added.

Thus, a core service that Proven Data and other data recovery specialists offer is assisting victims willing to pay hackers’ bitcoin ransoms.

Anti-virus providers such as Emsisoft sometimes find ways to disable ransomware, and post those fixes online for free. But they can decrypt ransomware only if there are errors in the underlying software or if a security lapse allows the researchers to hack into the attacker’s server, otherwise, it’s essentially bulletproof.

“The majority of cases require payment, because they’re using strong encryption. And there’s no other opinion than to pay or restore from backups,” said Congionti.

> Ransomware has helped put bitcoin in the news and we know that the price of bitcoin goes up whenever it is in the news.

—Edward Cartwright
Since 2016, there have been around 4,000 ransomware attacks a day, amounting to 1.5 million per year, according to statistics posted by the US Department of Homeland Security. Little wonder then that firms like Proven Data have formed relationships with hackers, and can often negotiate the price down. One hacker even offered data recovery firms exclusive “promo codes.” They were told that after paying they’d receive a code for a discount on a future ransom.

Congionti said that simply paying the ransom is sometimes not enough. Hackers often provide decryption keys that contain corrupted data, or missing files, which then needs to be checked and reversioned in-house,

Their methods are also becoming increasingly sophisticated. Some have even initiated automated schemes via smart contracts that ensure decryption when a victim sends a payment. There’s no negotiating between humans; the crime is automated on the blockchain.

Stockpiling bitcoin for ransom

It can cost three times as much to recover data than to pay the ransom. The speed of unlocking frozen accounts is often key for enterprises and organisations—for some, such as law firms, any downtime can be life threatening.

An October 2019 survey by data security startup Datto, polled 2,400 managed service providers, finding that the average ransom attack cost $46,800 in downtime—10 times the average ransom demand.

As a result, companies such as Proven Data stockpile bitcoin for contingencies. “That’s part of the service—having that bitcoin readily available so there’s no delay in getting a company up and running as soon as possible.” said Congionti.

Another survey, in 2018, by security solutions provider Code24 suggested that victims were stockpiling cryptocurrency to minimize costs and disruption in the wake of a ransomware attack. The research found that almost three-quarters of Chief Information Security Officers chose to stash cryptocurrency for such an eventuality. But it’s notable that the study was conducted at the height of the cryptocurrency boom, when prices were marching ever upward.

The policies of insurance companies may also be compounding the issue. Driven partly by the spread of ransomware, the cyber insurance market has grown rapidly. Between 2015 and 2017, US cyber premiums doubled to an estimated $3.1 billion, according to the most recent data available.

Investigative non profit ProPublica published a report in August which found that insurance companies are helping to pay ransoms—inadvertently but essentially encouraging hackers to continue these attacks for profit.

Industry giant AIG reported in July that ransomware was its second leading cause of claims in 2018 and expected to increase in 2019. While the number of attacks had actually decreased, AIG said they have also become more costly, as the targets have become more specific. Criminals increasingly extort institutions that have deeper pockets and readily pay the ransom to minimize disruption to their operations

Ransomware’s impact on bitcoin

Some analysts believe all this ransomware activity is bound to affect bitcoin’s price.

“Ransomware has helped put bitcoin in the news and we know that the price of bitcoin goes up whenever it is in the news,” said De Montfort University’s Cartwright “So, ransomware also partly drives the price of bitcoin.”

Cartwright believes that the effect of a ransomware attack is significant enough to warrant inclusion in any algorithmic trading model that factors in external events, thus taking advantage of prospective price movement in the wake of an attack.

But that doesn't help local governments, businesses and law enforcement agencies, who are desperate for solutions to ransomware attacks that threaten to cripple them.

RYUK ransomware is named after the god of death in the anime Death Note. Image: Flickr
Last summer, in response to hackers demands for millions of dollars, a coalition of 227 US mayors vowed not to pay. Which might well be the best solution.

Data recovery experts, including Proven Data, report that ransomware attacks increasingly show the characteristics of organized cybercrime, and fear that many ransom payments end up in the hands of terrorist groups. Through paying a ransom, local governments are inadvertently funding them.

A concerted attack

Government officials hope that, though better security, they can properly protect cities from these kinds of attacks. Congionti suggested that the government should make it mandatory for businesses to go through some basic security protocols, as well.

And this year, the White House and U.S. Senate approved versions of a bill that would allow the Department of Home Security to invest in resources to help states and cities deal more effectively with ransomware attacks.

Either way, a policy of not paying ransom ought to help eradicate the scourge of ransomware.

But for now, RYUK, a particularly robust ransomware that can sometimes even find and destroy backups, is on the rise. It's named after the god of death in the anime, *Death Note*, and is believed to have originated in North Korea.

Over the first five months of 2019, RYUK hit more than 500 schools and earned hackers more than $3 million in bitcoin. And security experts expect it, and new ransomware attacks against local governments, will only ramp up in 2020.

At the ripe adult age of 30, Popp's invention is adept at outrunning most efforts to thwart it. This is not a happy birthday