How Bitcoin helped fuel an explosion in ransomware attacks

Secure payment system Bitcoin has many legitimate uses, but like other technologies, it's also been beneficial to cybercriminals seeking new ways to extort money.

By Danny Palmer | August 22, 2016 -- 11:07 GMT (04:07 PDT) | Topic: Security

Ransomware is booming (http://www.zdnet.com/article/easy-to-carry-out-difficult-to-protect-against-why-ransomware-is-booming/). Be it Locky (http://www.zdnet.com/article/a-massive-locky-ransomware-campaign-is-targeting-hospitals/), CryptXXX (http://www.zdnet.com/article/one-of-the-nastiest-types-of-ransomware-has-just-come-back-to-life/) or one of the countless other variants of the data-encrypting malware, cybercriminals are making hundreds of thousands of dollars every month off the back of swathes of infected victims each paying a few hundred dollars each to get access to their files back.

MORE SECURITY NEWS

Cybersecurity researchers have warned that ransomware represents the most problematic cyber-threat (http://www.zdnet.com/article/ransomware-is-now-the-top-cybersecurity-threat-warns-kaspersky/). The most infamous ransomware attack this year took place at the Hollywood Presbyterian Medical Center, with the Los Angeles hospital forced to declare an "internal emergency" after its IT systems were locked down and held to ransom (http://www.zdnet.com/article/hollywood-hospital-becomes-ransomware-victim/) by hackers.

Ransom demands are typically made in Bitcoin, the cryptographic digital currency based on Blockchain distributed ledger technology (http://www.zdnet.com/article/disruptv-bitcoin-blockchain-and-payments/), which offers a secure, often untraceable, method of making and receiving payments -- a perfect currency for those who want their financial activities to remain hidden.

The popularity of Bitcoin has grown significantly in recent years and ransomware has spiked in 2016: could the growth of the two therefore be tied together?

Fitness app PumpUp leaked health data, private messages (https://www.zdnet.com/article/fitness-app-pumpup-leaked-health-data-private-messages/)

T-Mobile bug let anyone see any customer's account details (https://www.zdnet.com/article/tmobile-bug-let-anyone-see-any-customers-account-details/)

A hacker claims to be selling access to Apple internal tools (https://www.zdnet.com/article/hacker-claims-to-be-selling-access-to-apple-internal-tools/)

Blockchain: The 2 most important things to understand (https://www.zdnet.com/article/blockchain-the-2-most-important-things-to-understand/)

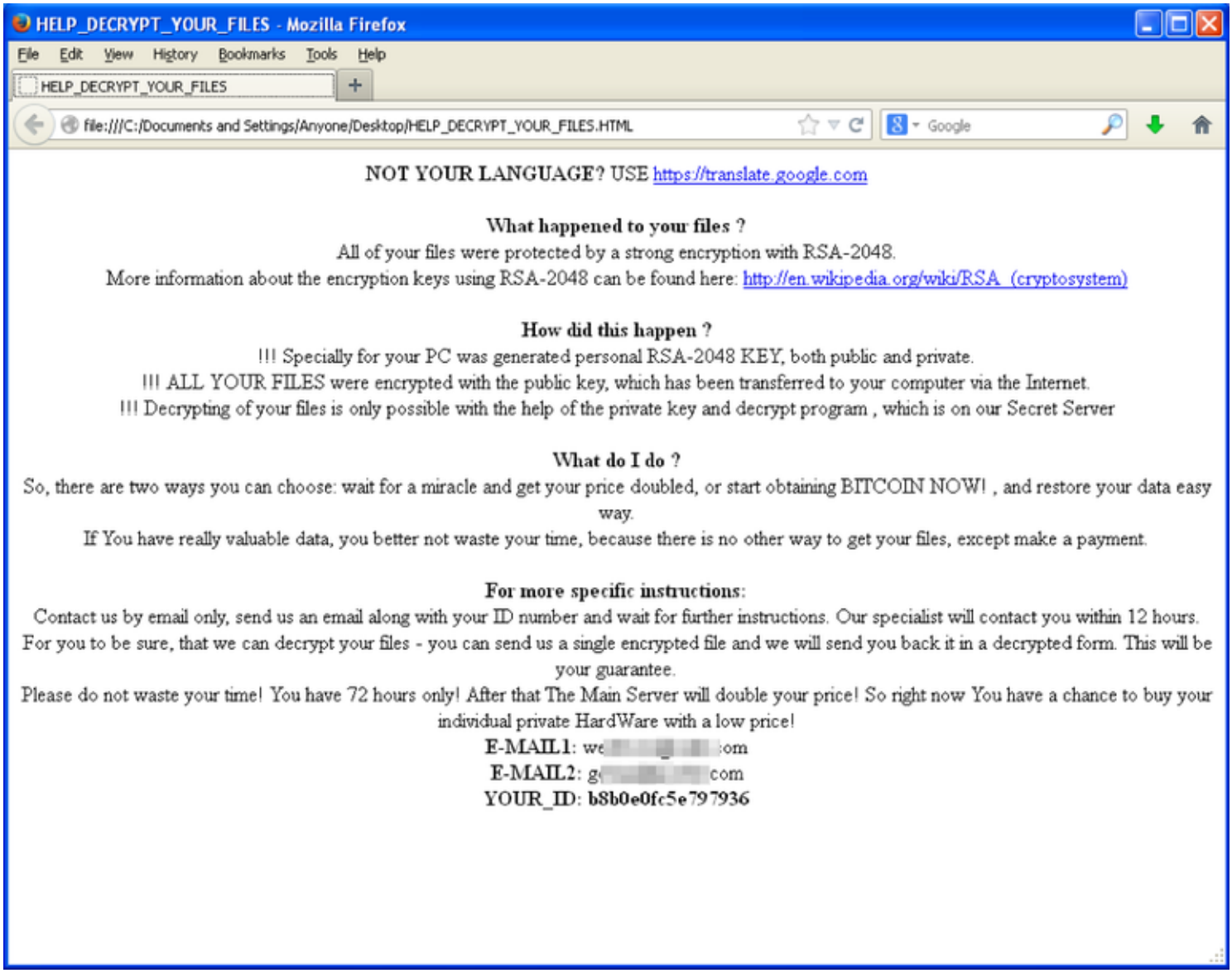
Your iPhone is tracking your movements and storing your favorite locations all the time (https://www.zdnet.com/article/your-iphone-is-tracking-your-movements-and-storing-your-favorite-locations-all-the-time/)

"It's helping. I think that's definitely true. The existence of effectively anonymised payment mechanisms definitely plays into the hands of cybercriminals," says David Emm, principal security researcher at Kaspersky Lab.

However, online extortion still took place regularly before the rise of Bitcoin. Emm recalls how some extortionists even attempted to use traditional postal services to receive payments for scams based on viruses.

Some of these viruses did the same sort of thing as ransomware, but were nowhere near as successful because authorities could watch the location where the payment was delivered to see who picked it up.

"It wasn't successful because police could monitor the PO boxes, so as soon as someone went to pick up the goods, you could arrest them," says Emm.



More often than not, hackers will demand a ransom payment be made in Bitcoin

Image: Proofpoint

This lack of success led cybercriminals to switch to online payment systems, using Western Union or PayPal to receive payments from victims of malicious software. However, all of these systems are still tied to a bank account, giving the authorities an opportunity to trace the perpetrators.

That's why the secretive nature of Bitcoin has proven so appealing for cybercriminals and why so many ransomware campaigns now want payment in that form -- because it's completely anonymous.

The Cerber ransomware campaign (http://www.zdnet.com/article/ransomware-as-a-service-for-allows-wannabe-hackers-to-cash-in-on-cyber-extortion/) is one of many which not only demand payment in Bitcoin, but also passes the currency through multiple Bitcoin wallets, effectively a form of money laundering, in order to further cover the tracks of the cybercriminals.

"We saw tens of thousands of victims' Bitcoin wallets transferred into one huge wallet. From there it's

"If you want your money in one wallet but you don't want anyone to be able to trace it back and know how you got it, then you take it though a mixing service -- like money laundering -- and then it all eventually gets back to you after being mixed with other money," she adds.

That ability to remain undetected is very much the reason cybercriminals trade in Bitcoin. "It makes it much easier to avoid law enforcement," Horowitz said, noting how in the rare instances that cybercriminals convert Bitcoin into another currency law enforcement is able to link criminal wallets to real bank accounts and occasionally determine who the perpetrators are.

"From time to time it happens, especially if they don't use mixing services, the authorities are able to trace a specific account back to a person and make an arrest," she said.

Bitcoin not only makes it easier to remain anonymous, but also enables the extorted funds to be immediately transferred into criminal hands. Even other forms of financial cybercrime, such as data-stealing banking Trojans (http://www.zdnet.com/article/banking-trojans-grow-smarter-but-are-banks-keeping-up/), don't offer this sort of advantage. In the case of a Trojan, there will be a transaction using the stolen details, which may provide enough details to trace the perpetrator.

"That's part of why threat actors move to ransomware, because it's easier to operate in using just Bitcoin," says Horowitz.

Operating in Bitcoin also brings other advantages to those dealing in ransomware. It's much more flexible than traditional payment methods, which require specific financial or login details to use. If the criminal feels they've extorted enough using one campaign -- or that the authorities are closing in -- they can easily take their business and move on.

(https://www.zdnet.com/pictures/a-guide-to-ransomware-and-ways-to-protect-yourself/)

The ransomware guide: protection and eradication (https://www.zdnet.com/pictures/a-guide-to-ransomware-and-ways-to-protect-yourself/)

It's nasty, but you don't have to be held to ransom by it.

Read More (https://www.zdnet.com/pictures/a-guide-to-ransomware-and-ways-to-protect-yourself/)

"In the modern age of online transactions, particularly when payments are easy to setup, then anyone can potentially become the online equivalent of Del Boy; you go along with a suitcase, you set up, when you see the police on the horizon, you pick it up and go somewhere else," says Kaspersky Lab's Emm.

"You have a mechanism for a particular attack, once you get enough money you're off and using a different email address or account. That fluidity and the speed of business operation allows them to hide between the cracks a lot easier," he adds.

But while Bitcoin has aided the rise of ransomware, it can't be singled out as the specific cause for the boom. However, the nature of Bitcoin means cybercriminals have jumped at the opportunity to use it, as they have with other identity-hiding technologies, such as Tor (http://www.zdnet.com/pictures/the-10-step-guide-to-using-tor-to-protect-your-privacy/) or the wider dark web in general (http://www.zdnet.com/article/silk-road-dark-web-marketplace-just-does-not-want-to-die/).

"The reality is cybercriminals will always use what is available to them. In many ways they're inherently lazy, so if Bitcoin wasn't there they'd find a different process to channel funds through. But because it exists, it's certainly something which has provided them with an existing process to perform that money flow," says Greg Day, VP and CSO, EMEA at Palo Alto Networks.

Ultimately, it could be said that the internet itself has been a huge gift for criminals, who are now using it not only for ransomware, but also malware, Trojans, hacking, and all manner of illegal activities on the dark web. In that case, Bitcoin is just the latest in a long line of technologies that have brought benefits to the wider world while unfortunately boosting the criminal underground.

READ MORE ON CYBERCRIME

- Encryption ransomware now 'tried and trusted' attacker business model (http://www.zdnet.com/article/encryption-ransomware-now-tried-and-trusted-attacker-business-model/)
- This initiative wants to help ransomware victims decrypt their files for free (http://www.zdnet.com/article/this-initiative-wants-to-help-ransomware-victims-decrypt-their-files-for-free/)

- Pay up or else: Ransomware is the hot hacking trend of 2016 (http://www.cnet.com/uk/news/pay-up-or-else-ransomware-is-the-hot-hacking-trend-of-2016/) (CNET)
- How to mitigate ransomware, DDoS attacks, and other cyber extortion threats (http://www.techrepublic.com/article/how-to-mitigate-ransomware-ddos-attacks-and-other-cyber-extortion-threats/) (TechRepublic)

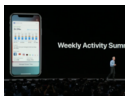
RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

SPECIAL FEATURE

Sensor'd Enterprise: IoT, ML, and big data

Toshiba sells PC business to Sharp for $36 million

53 minutes ago by Charlie Osborne in PCs



Apple, Google have similar phone addiction approaches with iOS, Android

58 minutes ago by Larry Dignan in Mobility

How Mezzanine allows graphical visualization inside black boxes of ML and AI systems

1 hour ago by Tonya Hall in Artificial Intelligence

Apple CarPlay: iOS 12 will finally let you use Google Maps, Waze

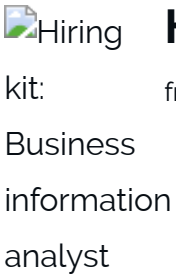
1 hour ago by Liam Tung in Mobility

Best Bluetooth in-ear headphones for active geeks

2 hours ago by Eileen Brown in Hardware

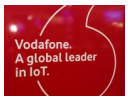
Computex 2018: Asus launches Zenbook Pro with touchpad that works as a secondary display

5 hours ago by Chris Duckett in Hardware



Hiring kit: Business information analyst

from Tech Pro Research



Deutsche Telekom and Vodafone trial NB-IoT international roaming

5 hours ago by Corinne Reichert in Mobility

Singapore council to assess ethical use of AI, data

6 hours ago by Eileen Yu in Artificial Intelligence

Samsung hires two AI experts for R&D push

7 hours ago in Innovation

VIDEO

WWDC 2018: How Apple plans to break iPhone addiction

UX Design as a Service: nice idea, but only part of the story

7 hours ago by Joe McKendrick in Enterprise Software

Cancelled My Health Record data to be kept in limbo

7 hours ago by Asha McLean in Security

WWDC 2018: Can Apple cure us of smartphone addiction?

8 hours ago by Dan Patterson in Innovation

Apple stays top of slowing wearables market

8 hours ago by Jonathan Chadwick in Mobility

ACCC needs AU$6m more to monitor NBN fixed-wireless speeds

9 hours ago by Corinne Reichert in Mobility

Qualcomm launches Snapdragon 850 platform, boosts "Always Connected" Windows 10 PCs

9 hours ago by Charlie Osborne in Mobility

Cultivating creative and empowered workers

10 hours ago by Evan Williams in Intelligent Communications / Brought to you by Microsoft Intelligent Communications

Westpac turns to IBM for hybrid cloud

11 hours ago by Asha McLean in Cloud

Kogan launches mobile services off Vodafone in NZ

11 hours ago in Mobility

GALLERY

WWDC 2018: Software, hardware and everything Apple is rumored to reveal

LOAD MORE

Article

How to install, reinstall, upgrade and activate Windows 10

How Mezzanine allows graphical visualization inside black boxes of ML and AI systems

Samsung hires two AI experts for R&D push

WWDC 2018: Can Apple cure us of smartphone addiction?

Kogan launches mobile services off Vodafone in NZ

Blockchain projects will be put aside from 2018: GlobalData

AI's deep learning rush forces industry to find new architectures

Article

What's up with IoT? Everything you need to know about the Internet of Things right now

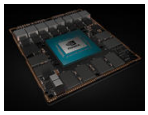
INNOVATION

Apple CarPlay: iOS 12 will finally let you use Google Maps, Waze

UX Design as a Service: nice idea, but only part of the story

Accor Hotels starts facial recognition trials in Brazil

Stanford makes a startling new discovery. Ethics



Meet Jetson Xavier: Nvidia says this AI chip will be brains of new wave of smart robots

Robby the last-mile delivery robot gets an update

MORE FROM INNOVATION +