Do Crypto-Currencies Fuel Ransomware?

By: Nir Kshetri and Jeff Voas

Kshetri, Nir and Voas, J. (2017). "Do Crypto-Currencies Fuel Ransomware?" *IEEE IT Professional* 19(5) 11-15.

Made available courtesy of IEEE: https://doi.org/10.1109/MITP.2017.3680961

Abstract:

As ransomware spreads, victimization rates escalate. A Finnish cybersecurity firm's F-Secure State of Cyber Security 2017 report stated that there was only one ransomware "variant" in 2012. This increased to 35 in 2015 and 193 in 2016.(1) Individuals, corporations, banks, educational establishments, hospitals, and government agencies have all been held hostage by ransomware and blackmailed into paying out in crypto-currency—typically, bitcoin—to retrieve their data.(2)

Keywords: cybersecurity | crypto-currencies | bitcoin | WannaCry | ransomware

Article:

As ransomware spreads, victimization rates escalate. A Finnish cybersecurity firm's F-Secure State of Cyber Security 2017 report stated that there was only one ransomware "variant" in 2012. This increased to 35 in 2015 and 193 in 2016.(1) Individuals, corporations, banks, educational establishments, hospitals, and government agencies have all been held hostage by ransomware and blackmailed into paying out in crypto-currency—typically, bitcoin—to retrieve their data.(2)

As a recent example, the WannaCry ransomware started on 12 May 2017. It infected about 300,000 computers in 150 countries(3) and cost computer users thousands of dollars in ransom money and billions in lost productivity.(4) Hospitals in the UK's National Health Service were forced to cancel surgeries. Ambulances were diverted, and patient records were inaccessible. WannaCry used 28 languages to release ransom messages, including European and Asian dialects.(5) The extortionists demanded that victims pay US$300–$600 in bitcoin (about 0.17–0.34 BTC based on the price of bitcoin at that time). WannaCry extortionists relied on three bitcoin wallet addresses, yet they still needed to perform manual decryption of victims' files after receiving payment. In other attacks, more sophisticated ransomware programs were employed.

These attacks dynamically generated a new bitcoin address for each infected machine, and a smart contract governed the process of decrypting victims' computers: if ransom money is paid to X address, the files in victim Y's computers get decrypted.(6)

The escalation of ransomware could be fueled in part by the diffusion of crypto-currencies. Without crypto-currencies, the creation of ransomware such as WannaCry would not be as desirable because other forms of payment have greater "criminal" traceability. Surveys have revealed that some companies hold supplies of bitcoins so that they can pay extortionists if ever necessary.(7) In this article, we examine cryptocurrencies' effects on ransomware and look at what might influence a victim's decision to pay.

Crypto-Currency Ransomware: How It Works

Before crypto-currencies, extortionists usually asked victims to send money via money transfer agencies or deposit directly to bank accounts. However, such transfers had more traceability if law enforcement got involved. Crypto-currencies are somewhat of an online extortionists' dream come true. For instance, it is almost impossible to pinpoint the perpetrators based on bitcoin addresses.

Bitcoins can be converted into cash secretively through third parties. Pinpointing the extortionist is of little value if that person is in a jurisdiction that does not cooperate in detection. For instance, cybersecurity researchers at Google, Symantec, FireEye, and others reportedly found evidence linking WannaCry ransomware attacks to North Korea.(8) Given that North Korea maintains few diplomatic ties, it is difficult to take actions against such an isolated country.

Ransomware involving cryptocurrencies might increase because such currencies are becoming more widely adopted. According to the World Economic Forum (WEF), 10 percent of global GDP will be stored on blockchain by 2027(9) compared to 0.025 percent in 2016.(10)

While bitcoin transactions are difficult to track, they are not completely anonymous. All transactions are recorded in a permanent public ledger. After the bitcoins are moved from that address, financial movements can be traced. Users can be traced through IP addresses and money flows. Elliptic, a blockchain intelligence company, uses artificial intelligence to scan and analyze the bitcoin network to identify suspicious behavior patterns in bitcoin transactions. It can trace transactions to individuals or groups. Elliptic's services are used by online exchanges and law enforcement to detect money laundering.(11)

Extortionists can further reduce the probability of detection using next-generation crypto-currencies such as Monero, Dash, and Z-Cash. These have built-in anonymity features. For instance, Monero is arguably the most anonymous crypto-currency. In 2016, Alpha-Bay, which might be the most widely used darknet market, started accepting Monero.(12) Monero is less widespread than bitcoin—for instance, as of May 2017, Monero's total value was around $425 million, or about 1 percent of bitcoin's.(13) Moreover, converting Monero into real-world cash is more difficult than with bitcoin. However, this problem might not be as significant in the future if there is more diffusion and competition in crypto-currencies.

Factors Affecting the Propensity to Pay Ransom

According to Elliptic, as of 16 May 2017, four days after Wanna-Cry spread, the amount of ransom paid out by victims to the bitcoin wallet addresses was about $86,000 (46.4 BTC). If everyone infected had paid, the criminals would have received at least $60 million. What they did receive translated to a payout rate of about 0.14 percent.(14) Even after more than a week, the amount paid out did not increase much. Data from Elliptic indicated that, as of 23 May 2017, WannaCry victims had paid less than $120,000 to three bitcoin wallets (www.elliptic.co/wannacry).

Another estimate of the WannaCry impact suggested that as of 15 May 2017, payments had been made by about 190 computers out of approximately 300,000 computers that were believed to be infected.(15) This put the number of computers complying with the extortionists' demands at 0.06 percent.

So, what factors are associated with this low payout ratio? We summarize some of these key factors in Table 1 and discuss them in detail next.

Table 1. Victim characteristics and situational factors affecting propensity to pay ransom.

		Gravity and urgency of the problem (relative to the ransom demanded)	
		Low	High
Complexity of complying with demands or perceived degree of uncertainty about outcome	Low	1 Likely to have backup and data-retrieval plans in place More likely to use available fixes Unaffordable ransom (as with students in China)	2 High degree of readiness to pay ransom (mission-critical digital data is threatened)
	High	4 Often new users Might use older technologies and pirated software (for example, most computer users in India and China) Low degree of digitization of values and economic activities	3 Follow detailed step-by-step instructions provided by extortionists Consult with cybersecurity firms and experts regarding the process and appropriateness of complying with extortionists demands

Complexity of Complying with Extortionists' Demands

First, the amount of money the WannaCry extortionists asked their victims to pay—$300 to $600—is not high. Rather, one key reason why victims do not pay is that complying with the extortionists' demands can be complicated. This is because of idea of crypto-currency is a new concept for many victims. Furthermore, attaining bitcoins is not easy. It can take days to create an account by registering with a bitcoin brokerage or exchange. Users are required to go through

a verification process. The account then needs to be connected a bank account able to receive bitcoins.(16)

Second, consider this problem for non-US countries. In some countries, exchanges that handle bitcoin transactions are licensed and regulated like traditional money transfer businesses. It is reported that as of May 2016, there were around 44 exchanges worldwide for bitcoins.(17) The first Malaysian Bitcoin Exchange, Xbit Asia, was opened in September 2016 (bit.ly/2v8clcs). Before that, most Malaysians who wanted bitcoins got them through exchanges in Singapore.(17) Likewise, to purchase bitcoins in India, a buyer needed to provide a permanent account number (or PAN, a unique, 10-digit alphanumeric identity assigned to a taxpayer by the Income Tax Department) and know your customer (KYC) details.(18) Loading a bitcoin wallet through startups such as Zebpay, Coinsecure, and Unocoin can take 48 hours. Bitcoin transactions are currently a regulatory grey area of economic activity in India and are also considered taboo. The three-day deadline for the WannaCry ransom payments was thus too short for most Indian victims.

Countries that do not have bitcoin brokerages or exchanges add further complexity. As was the case with Malaysian consumers before 2016, money had to be converted into another currency before being depositing into a bitcoin wallet.

Still another source of complexity is that victims lack control over the extortionists' guarantees. There is no guarantee of data unlock even if victims pay.(19) According to a 2016 Fortinet report, about a quarter of organizations that paid ransoms were not able to recover their data.(18) Recent WannaCry victims are believed to be in a worse situation. According to the Israeli computer security consultancy Check Point, due to a fault in WannaCry's encryption software, it is almost impossible to decrypt a user's data after payment has been made.(20)

A further complexity arises from the fact that most cyber-liability insurance policies have exclusion and cooperation clauses that prohibit businesses from paying ransoms without pre-approval. If a victim fails to comply and pays the ransom, insurers might cancel the insurance coverage, including the costs of disruptions to the businesses, remediation expenses, and costs associated with notifying customers.(21)

Gravity of the Problem

Extortionists might threaten that if victims fail to pay after a specified time interval, their files will be permanently locked—that is, the data is not coming back. This becomes a terrible problem for those who do not backup their data. If one victim faces more severe consequences than others, they might be more likely to pay out. For instance, it was reported that extortionists held an Austrian hotel network for ransom, demanding $1,800 in bitcoin. The gravity of the situation became clearer when the guests could not check in and out and were locked out of their rooms. The hotel complied, and paid.(22)

Combined Factors

We now look at each of Table 1's four cells in detail.

Cell 1: Larger organizations will likely have data retrieval plans in place.(23) Ransomware attacks should have smaller impacts on them, so ransom payments might not occur. Furthermore, following the WannaCry ransomware attack, Microsoft published a patch for operating systems for which it was no longer providing support. They included Windows XP, Windows Server 2003, and Windows 8.(24) Larger organizations should be technically savvy enough to implement these available fixes quickly.

Cell 2: If critical data is at risk, organizations in this situation should realize that they require a higher degree of immediate response. One study reported that 33 percent of UK corporations had bought bitcoins so that they would be prepared to pay ransoms. More than 35 percent of large firms (with more than 2,000 employees) were willing to pay as much as £50,000 (US$65,000) to unlock files containing critical data, such as intellectual property.(25) And a university in the US reportedly created an account to be prepared for ransomware attacks.(7)

Cell 3: Extortionists might operate call centers to offer technical support to simplify the payout process for victims.(2) There are reports that when victims call, extortionists will walk them through the process of getting their files back.(20) Criminals can provide detailed explanations about attaining bitcoins and then transferring them. From the extortionists' standpoint, such services are likely to be effective for situations represented by cell 3, which have both high complexity and high gravity.

However, some organizations might lack cybersecurity expertise and experience in dealing with cyberattacks such as those involving ransomware. It is suggested that 85 percent of US medical institutions lack qualified personnel to perform basic cybersecurity tasks, such as patching software and monitoring threats.(26)

Cell 4: Most users from developing countries belong to cell 4. Pirated software in developing countries arguably accelerates the spread of ransomware.(27) About 4,000 of the 40,000 institutions affected by WannaCry in China were universities. Concerns were raised about students being unable to access their work.(19) However, the amount asked by the extortionists—$300 to $600—was too expensive for most students.(23)

At the time of this writing, another attack, known as Petya, occurred, impacting the Ukraine government's banks and electricity grid, as well as other countries and corporations (https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companiesacross-europe). One frightening aspect here is that these attacks are mainly on computers, not devices. It is not far-fetched to imagine future scenarios in which devices, such as pacemakers and infusion pumps, become targets—for example, pay now, or your insulin pump will be turned off. The growth in ransomware is one of the "darker" activities created by the diffusion of cryptocurrencies. Crypto-currency is too complicated for many computer users to understand. And even if they are willing to pay, victims might not know where to start or how to navigate the process. However, IT professionals need to learn about crypto-currencies and blockchain. Crypto-currencies and ransomware are not going away. By employing more sophisticated modus operandi, more resourceful and skilled extortionists will increase their

success rates. IT professionals need to understand this space and how to help their organizations address it when it occurs.

References

1. “Bitcoin a Favourite of Ransomwares—Cyber Extortion to Shoot Up If Govts Don’t Act Soon,” Moneycontrol.com, 27 Apr. 2017; bit.ly/2qiMSrr.

2. A. Mizrahi, “Hackers Release New TV Episodes after Netflix Refuses to Pay Bitcoin Ransom,” Finance Magnates, 5 Apr. 2017; bit.ly/2uvagDL.

3. “North Korean Hackers Behind Global Cyberattack?” CBS News, 16 May 2017; cbsn.ws/2qnYHjt.

4. J. Berr, “‘WannaCry’ Ransomware Attack Losses Could Reach $4 Billion,” CBS News, 16 May 2017; cbsn.ws/2rluoXx.

5. “WannaCry Outbreak: Ransom Payments Reach $64,000, Around 48,000 Attack Attempts in India,” Moneycontrol.com. 19 May 2017; bit.ly/2pQaio5.

6. K. Collins, “Inside the Digital Heist that Terrorized the World—and Only Made $100k,” Quartz, 21 May 2017; bit.ly/2qO0e0e.

7. T. Simonite, “Companies Are Stockpiling Bitcoin to Pay Off Cybercriminals,” *MIT Tech. Rev.*, 7 June 2016; bit.ly/1YeQSpU.

8. E. Chan and S. Kim, “Cybersleuths Unearth More Clues Linking WannaCry to North Korea,” *Bloomberg News*, 23 May 2017; bloom.bg/2v9Hbzt.

9. Deep Shift Technology Tipping Points and Societal Impact Survey Report, World Economic Forum, Sept. 2015; bit.ly/1KlN8ZR.

10. R. Huckstep, “What Does the Future Hold for Blockchain and Insurance?” Daily Fintech, 14 Jan. 2016; bit.ly/2dRLBkz.

11. J. Titcomb, “Bitcoin Surveillance Firm Elliptic Raises $5M as Banks Push into Blockchain,” *The Telegraph*, 20 Mar. 2016; bit.ly/1T3SBwc.

12. S. Usborne, “Digital Gold: Why Hackers Love Bitcoin,” *The Guardian*, 15 May 2017; bit.ly/2qlaMW2.

13. “Bitcoin’s Murkier Rivals Line Up to Displace it as Cybercriminals’ Favorite,” *Fortune*, 18 May 2017; for.tn/2qY6kOv.

14. “Bitcoin Tracker: WannaCry Doesn’t Pay,” Pymnts.com, 19 May 2017; bit.ly/2ucjLby.

15. S. Petulla, “Ransomware Attack: This Is the Total Paid and How the Virus Spread,” NBC News, 15 May 2017; nbcnews.to/2wi3bIR.

16. “Few Victims Are Paying Hackers Because Using Bitcoin Is Hard,” Newsmax, 15 May 2017; nws.mx/2v9WnN6.

17. B.K. Sidhu, “Should You Stock Up on Bitcoins to Pay for Future Ransomware Attacks?” *The Star*, 19 May 2017; bit.ly/2qHMjul.

18. A. Sarkhel and N. Christopher, “Indian Companies WannaCry over Bitcoin Payments Too,” *Economic Times*, 17 May 2017; bit.ly/2ryiGcd.

19. M. Scott and N. Wingfield, “Hacking Attack Has Security Experts Scrambling to Contain Fallout,” *New York Times*, 13 May 2017; nyti.ms/2pJnD0I.

20. “WannaCry Should Make People Treat Cyber-Crime Seriously,” *Economist*, 20 May 2017; econ.st/2r0g3Uv.

21. M. Scott and N. Perlroth, “With Ransomware, It’s Pay and Embolden Perpetrators, or Lose Precious Data,” *New York Times*, 17 May 2017; nyti.ms/2pNWizm.

22. “Hotel Ransomed by Hackers as Guests Locked Out of Rooms,” *The Local*, 28 Jan. 2017; bit.ly/2v9wjlb.

23. P. Mozur, M. Scott, and V. Goel, “Victims Call Hackers’ Bluff as Ransomware Deadline Nears,” *New York Times*, 19 May 2017; nyti.ms/2ryx4SM.

24. M. Kan, “Old Windows PCs Can Stop WannaCry Ransomware with New Microsoft Patch,” *PC World*, 15 May 2017; bit.ly/2wirIx8.

25. A. Mizrahi, “33% of UK Firms Are Buying Bitcoin in Anticipation of Cyber Attacks,” Finance Magnates, 6 Aug. 2016; bit.ly/2v7t4wb.

26. “WannaCry Attack Is Good Business for Cyber Security Firms,” *Fortune*, 19 May 2017; for.tn/2q4GpRa.

27. P. Mozur, “China, Addicted to Bootleg Software, Reels from Ransomware Attack,” *New York Times*, 15 May 2017; nyti.ms/2wi5ATT.

Nir Kshetri *is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu.*

Jeffrey Voas *is a cofounder of Cigital and Computer’s Cybertrust column editor. He’s an IEEE Fellow. Contact him at j.voas@ieee.org.*