# Ransomware: Pay to Play?

By: Nir Kshetri and Jeffrey Voas

N. Kshetri and J. Voas, "Ransomware: Pay to Play?," in *Computer*, vol. 55, no. 3, pp. 11-13, March 2022, doi: 10.1109/MC.2021.3126529.



## Abstract:

Ransomware is fairly new, and many folks don't realize that it will affect them. Just as with shoplifting, we all pay.

**Keywords:** ransomware | cybersecurity

## Article:

A conservative estimate is that ransomware criminals received US$412 million in payments in 2020.[1] In 2020, the average payment increased by 171%, reaching US$310,000.2 The Chicago-based financial company CNA Financial Corporation paid US$40 million in ransom (Table 1). The company was attacked by Phoenix Locker, a spin-off of the Russian hacking organization Evil Corp (also known as REvil) in March 2021, and, at the time, the amount was reported to be larger than any previously disclosed ransom payment.[3]

**Table 1.** Ransomware incidents with the highest ransoms paid.

| Victim (Time) | Ransomware used | Ransom paid | Remarks |
|---|---|---|---|
| CNA Financial (March 2021) | Phoenix Locker | US$40 million[6] | The hackers had initially demanded US$60 million. The malware used was a variant of Hades, which was created by REvil to bypass U.S. sanctions.[3] |
| Global beef manufacturer JBS USA (May 2021) | REvil (Sodinokibi) ransomware | US$11 million (301 bitcoins)[7] | The company reported that it complied with the criminals' demand to prevent data from being compromised.[8] |
| U.S. pipeline operator Colonial Pipeline | DarkSide | US$4.5 million (75 bitcoins) | The FBI recovered 63.7 bitcoins.[9] |
| Backup storage vendor ExaGrid (May 2021) | Conti ransomware group[7] | US$2.6 million (50.75 bitcoins)[10] | The original demand was more than US$7 million[7] |

FBI: U.S. Federal Bureau of Investigation

Recognize that ransomware criminals are sophisticated. Recently, double extortion was their strategy. This involved asking organizations to pay for the decryption key to unlock the affected files and servers plus additional payments to destroy stolen data.[4] If unpaid, a corporation's brand and stock price could be damaged by reaching out to security journalists and investors.[5]

A newer extortion scheme was added in 2020: triple extortion. In this ploy, criminals demand payments from the attacked organization's customers and other third parties. One example was the ransomware attack against the Finnish psychotherapy clinic Vastaamo. The clinic's data for 40,000 patients were breached. The criminals demanded that the clinic and the patients had to pay. The financial losses forced Vastaamo to declare bankruptcy and close.[2]

Note that, in general, paying ransom is not currently illegal in the United States. Ransom payments are tax deductible. If an organization has cyberinsurance, the payment may come from the insurer.[11] In other cases, however, it is against U.S. law to pay. In December 2019, the U.S. Treasury Department sanctioned 17 individuals and six entities linked to REvil. In October 2020, an advisory alert was issued by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), warning that certain ransomware payments could be a sanctions violation for victims as well as for companies that facilitate payments for victims.[12] In September 2021, the OFAC further updated its guidance and official policy regarding sanctions risks associated with making payments.[13] The ransomware groups sanctioned by the OFAC include DoppelPaymer, WastedLocker, BitPaymer, SamSam, and Locky.[14] However, some victims broke the sanctions law and paid. In 2020, victims were reported to have paid more than US$50 million worth of cryptocurrency to addresses that were identified to have a sanctions risk.[14]

A further consideration is that, even if the "correct" decryption keys are received, the victims may not be able to fully restore everything.

Conflicting findings have been reported concerning how extortionists may respond after victims pay a negotiated ransom. One view is that ransomware criminals live up to their promise. When victim companies pay the ransoms, the criminals usually satisfy their portion of the agreement. A reputation for reliability is a core component of their business model.[15] Others argue that there is no honor among cyberthieves.[16] A study conducted by one of Canada's business law firms, Blake, Cassels & Graydon, found that 9% of victim organizations that complied with the criminals' ransom demand never received a functional decryption key after payment. A further consideration is that, even if the "correct" decryption keys are received, the victims may not be able to fully restore everything.[17] Recognize that what victims pay for is to obtain the key to decrypt the contents that were encrypted by the extortionists.

But the tables can be turned! In rare cases, payments can be reversed. Out of the 75 bitcoins paid by Colonial Pipeline to DarkSide, the U.S. Federal Bureau of Investigation (FBI) tracked and recovered 63.7 bitcoins (US$2.3 million) from a wallet. The FBI was in possession of the bitcoin wallet's private key.[18] A judge in San Francisco had approved the seizure of the funds from the wallet.[19] (It is unknown how the FBI gained access to the private key.)

In summary, ransomware victims face an undesirable decision involving the asset that has been compromised plus all victim-specific circumstances. Information about the criminal and any assistance available from law enforcement should be factored into the decision about whether to pay.

**Disclaimer**

The authors are completely responsible for the content in this article. The opinions expressed are their own.

**References**


1. E. Nakashima, *U.S. aims to thwart ransomware attacks by cracking down on crypto payments*, 2021, [online] Available: https://www.washingtonpost.com/business/2021/09/17/biden-sanctions-ransomware-crypto/.
2. L. Whitney, *Ransomware attackers are now using triple extortion tactics*, May 2021, [online] Available: https://www.techrepublic.com/article/ransomware-attackers-are-now-using-triple-extortion-tactics/.
3. K. Mehrotra and W. Turton, *CNA financial paid \$40 million in ransom after March cyberattack*, May 2021, [online] Available: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.
4. D. Carmack, *What we know about DarkSide the Russian Hacker Group that just wreaked havoc on the East Coast*, 2019, [online] Available: https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc.
5. C. Graham, *Average ransomware payouts shoot up 171% to over \$300000*, 2021, [online] Available: https://www.tripwire.com/state-of-security/featured/average-ransomware-payouts-shoot-up/.
6. B. Chang, *One of the biggest US insurance companies reportedly paid hackers \$40 million ransom after a cyberattack*, 2021, [online] Available: https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5.
7. A. Waldman, *10 of the biggest ransomware attacks of 2021 - so far*, 2021, [online] Available: https://searchsecurity.techtarget.com/feature/The-biggest-ransomware-attacks-this-year.
8. D. V. Gerrit, R. Lerman, E. Nakashima and C. Alcantara, *The anatomy of a ransomware attack*, 2021, [online] Available: https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/.
9. L. Abrams, *DarkSide ransomware gang returns as new BlackMatter operation*, 2021, [online] Available: https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/.
10. R.-M. Valéry, *Exagrid pays \$2.6m to Conti ransomware attackers*, 2017, [online] Available: https://www.computerweekly.com/news/252501665/Exagrid-pays-26m-to-Conti-ransomware-attackers?_gl=1*1uomzml*_ga*NDkwMjUyOTE5LjE2MjE1Njc0MDM.*_ga_TQKE4GS5P9*MTYzMjkxNzcxOS4xNi4wLjE2MzI5MTc3MTkuMA.&_ga=2.30181372.2144667799.1632917720-490252919.1621567403.

11. E. Lopatto, *Ransomware funds more ransomware — how do we stop it?*, 2021, [online] Available: https://www.theverge.com/2021/6/24/22545675/ransomware-cryptocurrency-regulation-hacks.

12. *15% of all ransomware payments made in 2020 carried a risk of sanctions violations*, 2021, [online] Available: https://blog.chainalysis.com/reports/ransomware-sanctions-risk-2021.

13. L. Matthew and S. Kevin, *OFAC updates guidance on ransomware payments and sanctions risk*, 2021, [online] Available: https://www.technologylawsource.com/2021/09/articles/cybersecurity/ofac-updates-guidance-on-ransomware-payments-and-sanctions-risk/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

14. *15% of all ransomware payments made in 2020 carried a risk of sanctions violations*, Apr. 2021, [online] Available: https://blog.chainalysis.com/reports/ransomware-sanctions-risk-2021.

15. E. Javers, *The extortion economy: Inside the shadowy world of Ransomware payouts*, 2021, [online] Available: https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.

16. S. Sharwood, *REvil customers complain ransomware gang uses backdoors to filch ransoms*, 2021, [online] Available: https://www.theregister.com/2021/09/29/revil_customers_complain_about_backdoors/.

17. *Client alert: Ransomware – To pay or not to pay?*, Sep. 2021, [online] Available: https://www.corderycompliance.com/ransomware-pay-or-not/.

18. M. Demboski, *Why the FBI's recovery of colonial pipeline ransom signals hope for the future*, 2021, [online] Available: https://www.darkreading.com/attacks-breaches/why-the-fbi-s-recovery-of-colonial-pipeline-ransom-signals-hope-for-the-future.

19. C. BingJoseph, *U.S. seizes \$2.3 mln in bitcoin paid to Colonial Pipeline hackers*, 2021, [online] Available: https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.