Current Trends in Ransomware

with special notes on Monero usage

CipherTrace, a Mastercard Company

Cryptocurrency Intelligence

2021

```
{
    public sealed  class Program
    {

        const string name = "svch";
        private static Thread[] Threads;
        private object locker = new object();
        private static string server = "%SERVER%";
        private static string mail = "%FIRST_MAIL%";
        private static string vector = "%INC_VECTOR%";
        private static string text = "%TEXT_FOR_UNLOCK%";
        private static string RSA_MasterPublic = "%RSA_PUBLIC%";
        private static string CryptedExtension = "%EXTENSION%";
        private static bool LockerForValidKey = true;
        private static string PCID = "";
        private static string RSA_Public = "";
        private static string RSA_Private = "";
        private static int FilesCount = 0;
        private static bool SaveTextForUnlock = Boolean.Parse("%STFU%");
        //private static bool SaveTextForUnlock = Boolean.Parse("True");
        public static RSACryptoServiceProvider MasterRSA = new RSACryptoServiceProvider();
        public static RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
        public static List&lt;string&gt; directories = new List&lt;string&gt;();

        private static string CryptedPrivateKey = "";
        /// &lt;summary&gt;
        /// Главная точка входа для приложения.
        /// &lt;/summary&gt;
        [STAThread]
        static void Main(string[] args)
        {
            try
            {
                var handle = NativeMethods.GetConsoleWindow();
                NativeMethods.ShowWindow(handle, NativeMethods.SW_HIDE);

                string appdata = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
```

Table of Contents

Executive Summary

Ransomware continues to be a major growing cybersecurity issue facing public and private sectors, and individual victims. The risk of sending a payment to an OFAC-sanctioned entity remains of critical concern for those extorted; this risk may be mitigated by performing due diligence on the bad actors and the incident reported to relevant agencies, as highlighted in OFAC's updated Sept. 2021 advisory here.

Over the course of 2021 CipherTrace has uncovered the current trends in ransomware usage:

- There has been a 4.83X (nearly 500%) increase in double extortion ransomware attacks from 2020 to 2021.
- Double extortion attacks have increased an average of 1.85x quarter over quarter from 2020 – Q3 2021.
- 2021 has seen an increasing demand for ransom payment in monero (XMR) with added premiums for payments in bitcoin (BTC) ranging from 10-20%.
- In 2021 the most active ransomware groups have been REvil (now offline, possibly temporary), DarkSide (now offline, likely permanent), Conti-News, LockBit 2.0, Pysa, and Dopple Leaks.
- BTC is still the most requested payment method for ransom demands.

Ransomware trends reported by the US Department of Treasury and confirmed by CipherTrace analysts include:

- In the first half of 2021 the number of reported ransomware payments made was 30% greater than in all of 2020 and the total of all payments made in the first 6 months of 2021 was 42% higher than in all of 2020 ($590 million from $416 million).
- FinCEN has identified 17 ransomware-related reports requesting payment in XMR so far in 2021. According to CipherTrace data, at least 22 ransomware strains accept only XMR and at least 7 ransomware strains accept both BTC and XMR.

To mitigate the damage from a ransomware attack, public and private sector firms and individual or small businesses may put in place an incident response plan and may vet an incident response firm that employs necessary UTXObased tracing analytics like CipherTrace, which allow investigators to trace the funds from origin to destination with the highest fidelity to the blockchain.

Regarding payments – victims within U.S. jurisdiction who are unaware they have sent a payment to an illicit actor may be liable for civil penalties which are in violation of OFAC regulations.

Ransomware Attacks Grow Exponentially

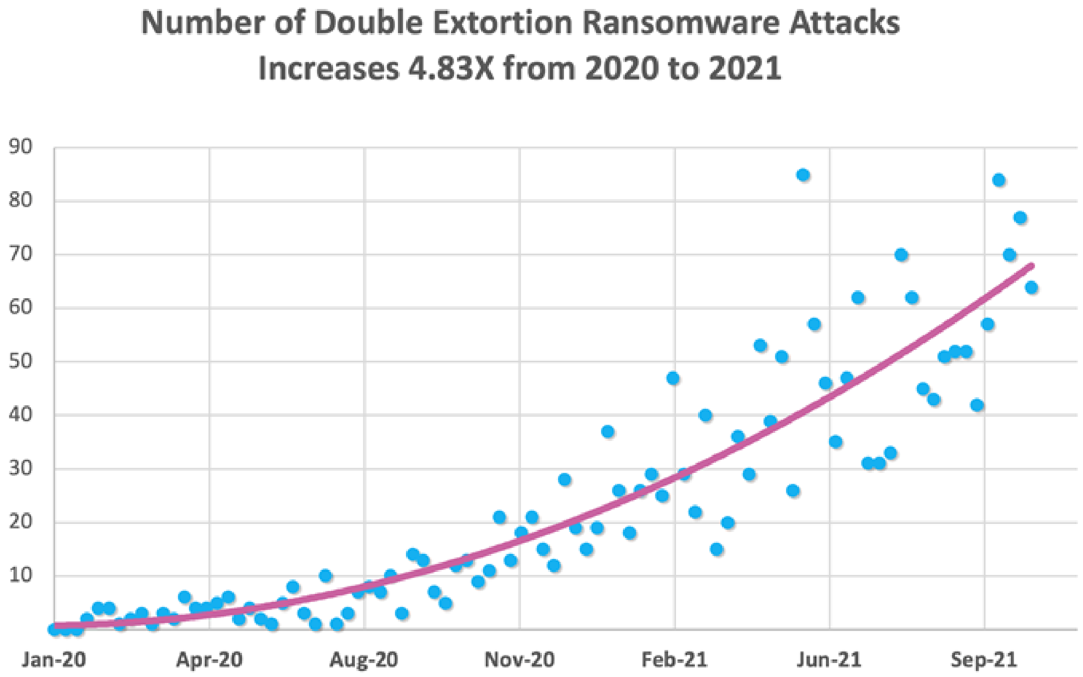
Ransomware attacks have flooded the headlines of 2021 with a series of high-profile attacks on companies with record-breaking ransom demands in the range of 6, 7, and even 8 figures. This increased attention has led many firms to harden their security practices to better combat ransomware attacks, including implementing a recovery strategy that involves regularly backing up important data, so ransomware demands do not need to be paid to restore critical functions.

Unfortunately, this has caused a new and alarming trend in the ongoing evolution of ransomware—the increasing use of **double extortion attacks**. In a traditional ransomware attack, a victim's data is encrypted until payment is received. In a double extortion attack, however, ransomware actors not only encrypt the victim's data but then threaten to publicly release stolen files if the ransom isn't paid.

The growth of these double extortion attacks is likely the result of increased hardening against ransomware attacks by the public and private sector. As ransomware continues to make headlines, more organizations are alerted to the severity of a potential attack and, in turn, increase their cyber security protocols to mitigate the risks. As such, more and more organizations are better prepared to not pay out ransom demands. This lack of payout requires ransomware actors to evolve their methodologies to ensure organizations pay—even if they have backups. Some groups like REvil take it a step further and allow anyone to pay the ransom during the payment period to receive the data, not just the victim.

The frequency of ransomware attacks being published on leak sites (both leaks and attacks published for victims to pay) has increased exponentially over the past year and a half. This has been driven by both an immense increase in ransomware attacks overall and the increasing trend of double extortion.

CipherTrace researchers collated data from these leak payment sites going back 22 months.



Number of Double Extortion Ransomware Attacks Increases 4.83X from 2020 to 2021

Every point is the number of new double extortion ransomware attacks posted that week on a ransomware leak sites between January 2020 and October 2021. The purple line shows the exponential growth trend of attacks.

Analyzing the double extortion ransomware data, CipherTrace analysts discovered there has already been a 4.83X increase in public attacks comparing all of 2020 to just January – October 2021. Double extortion attacks have increased an average of 1.85X quarter over quarter.

In 2021 the most active ransomware groups have been REvil (offline at the time of this report, possibly temporary), DarkSide (offline at the time of this report, likely permanent), Conti-News, LockBit 2.0, Pysa, and Dopple Leaks.

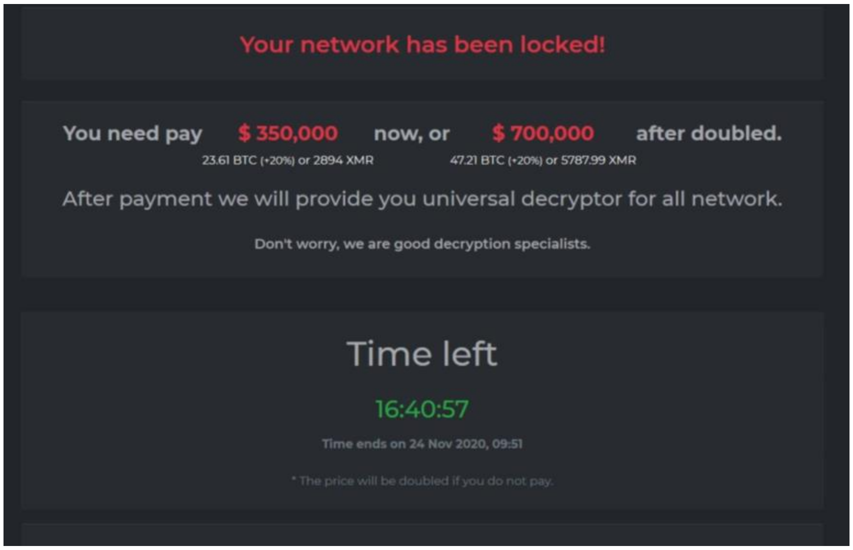
A FinCEN report published on October 15, 2021, states that in the first half of 2021 the number of reported ransomware payments made was 30% greater than in all of 2020 and the total of all payments made in the first 6 months of 2021 was 42% higher than in all of 2020 ($590 million from $416 million). This coincides with data collected by CipherTrace.

As a result, the FinCEN report adds that if current ransomware trends continue, "SARs [suspicious activity reports] filed in 2021 are projected to have a higher ransomware-related transaction value than SARs filed in the previous 10 years combined."

Growing Use of Monero in Ransomware

Demanding payment in privacy coins like Monero (XMR) has been another trend among ransomware actors in 2021. While some ransomware groups demand XMR and XMR only, CipherTrace analysts have noted an interesting trend is to now offer payments in either XMR or bitcoin (BTC) but charging a higher ransom if the victim chooses to pay in BTC. Higher prices for BTC are most likely seen by the ransomware actors as a premium for dealing with the increased risk in using an easily traceable cryptocurrency like BTC.

For example, DarkSide—the group behind the US Colonial Pipeline attack—accept both BTC and XMR but charge a 10-20% higher price for payments in BTC. This can be seen in the image below, under the "$350,000" and "700,000", a note reads "(+20%)" for BTC. In other cases, CipherTrace analysts have observed premiums of only +10%.



Your network has been locked!

You need pay $ 350,000 now, or $ 700,000 after doubled.

23.61 BTC (+20%) or 2894 XMR

47.21 BTC (+20%) or 5787.99 XMR

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

Time left

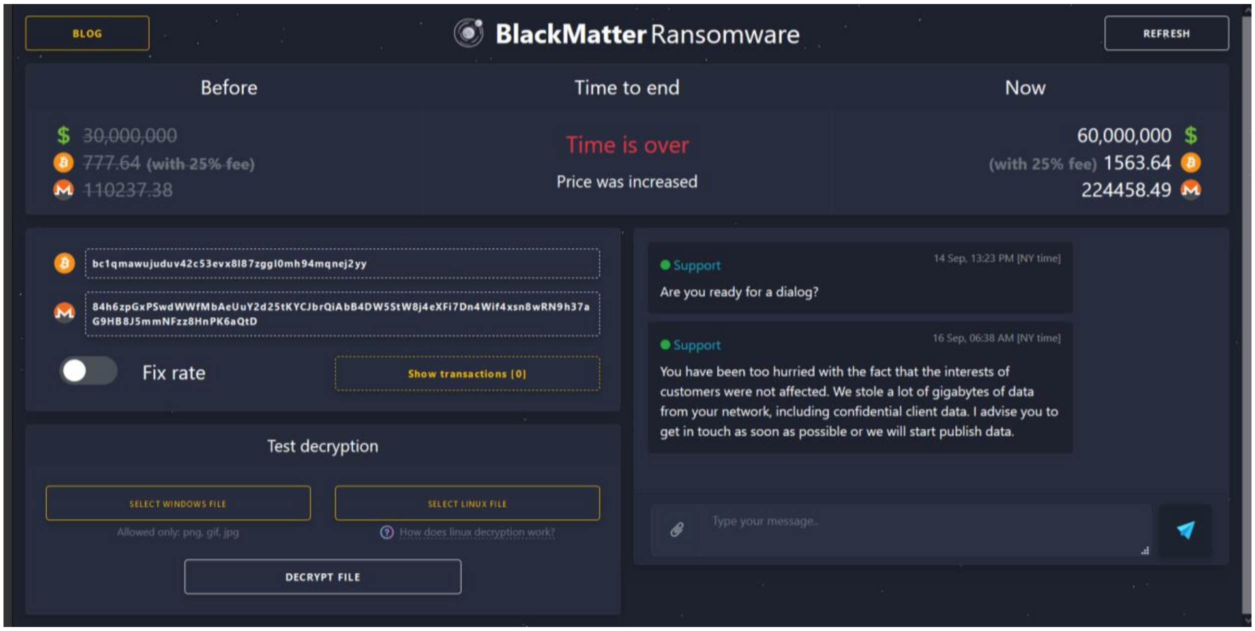
16:40:57

Time ends on 24 Nov 2020, 09:51

* The price will be doubled if you do not pay.

Example of DarkSide payment options in BTC (with an additional 20% fee) or XMR [Source: Collected by CipherTrace Intelligence]

DarkSide went offline after the Colonial Pipeline attack, but ransomware researchers have linked them to the new BlackMatter Ransomware group. It is most likely that DarkSide shutdown and rebranded themselves as BlackMatter, a common tactic to shake off the attention of the public and law enforcement after their high-profile attack. BlackMatter Ransomware has the same pattern of demanding payment in either BTC or XMR, with BTC ransom payments being 25% more expensive. In the image below you can see (in the top left and top right) the added 25% "fee" for paying in BTC.



Before	Time to end	Now
$ ~~30,000,000~~ Ƀ ~~777.64 (with 25% fee)~~ M ~~110237.38~~	Time is over Price was increased	60,000,000 $ (with 25% fee) 1563.64 Ƀ 224458.49 M

Ƀ bc1qmawujuduv42c53evx8l87zggl0mh94mqnej2yy

M 84h6zpGxPSwdWWfMbAeUuY2d25tKYCJbrQiAbB4DW5StW8j4eXFi7Dn4Wif4xsn8wRN9h37aG9HB8J5mmNFzz8HnPK6aQtD

○ Fix rate

Show transactions [0]

Test decryption

Allowed only: png, gif, jpg

How does linux decryption work?

● Support 14 Sep, 13:23 PM [NY time]

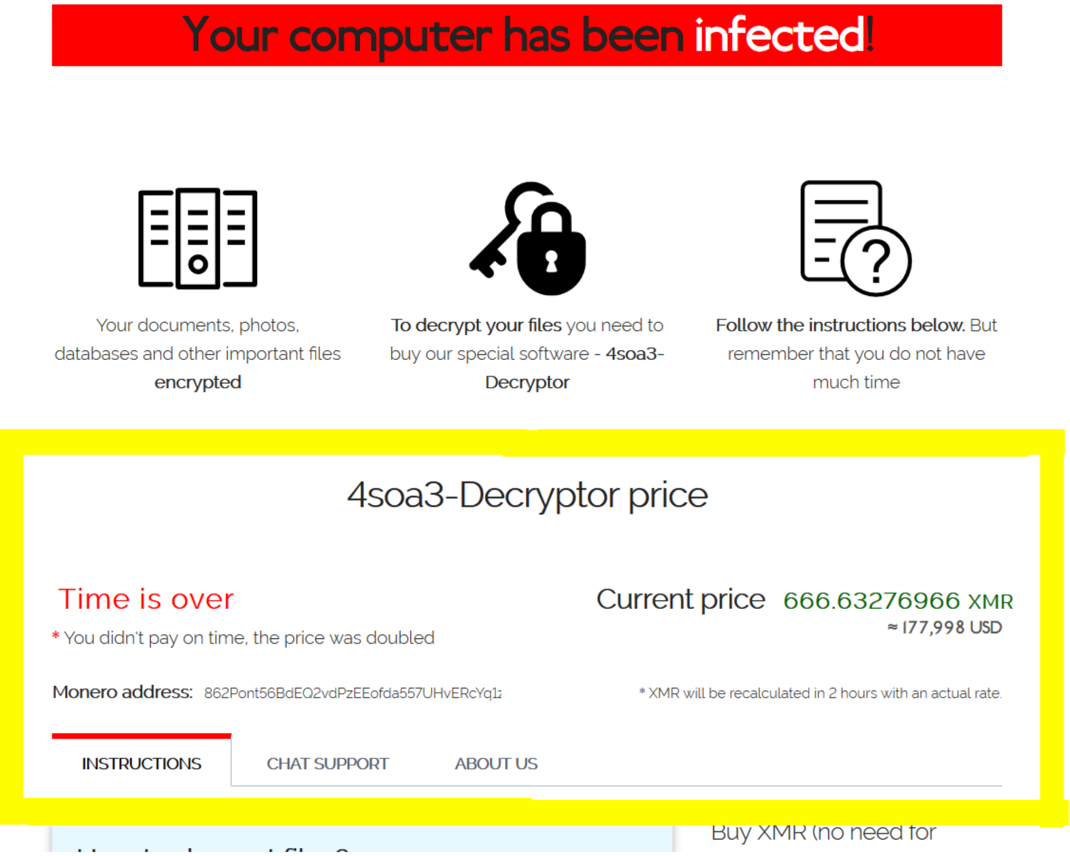
Are you ready for a dialog?

● Support 16 Sep, 06:38 AM [NY time]

You have been too hurried with the fact that the interests of customers were not affected. We stole a lot of gigabytes of data from your network, including confidential client data. I advise you to get in touch as soon as possible or we will start publish data.

Example of BlackMatter payment options in BTC (with a additional 25% fee) or XMR [Source: Collected by CipherTrace Intelligence]

REvil—the ransomware group behind the Kaseya attack—switched from demanding BTC to demanding payments in XMR only in early 2020.



Your computer has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **4soa3-Decryptor**

Follow the instructions below. But remember that you do not have much time

4soa3-Decryptor price

Time is over

* You didn't pay on time, the price was doubled

Current price 666.63276966 XMR

≈ 177,998 USD

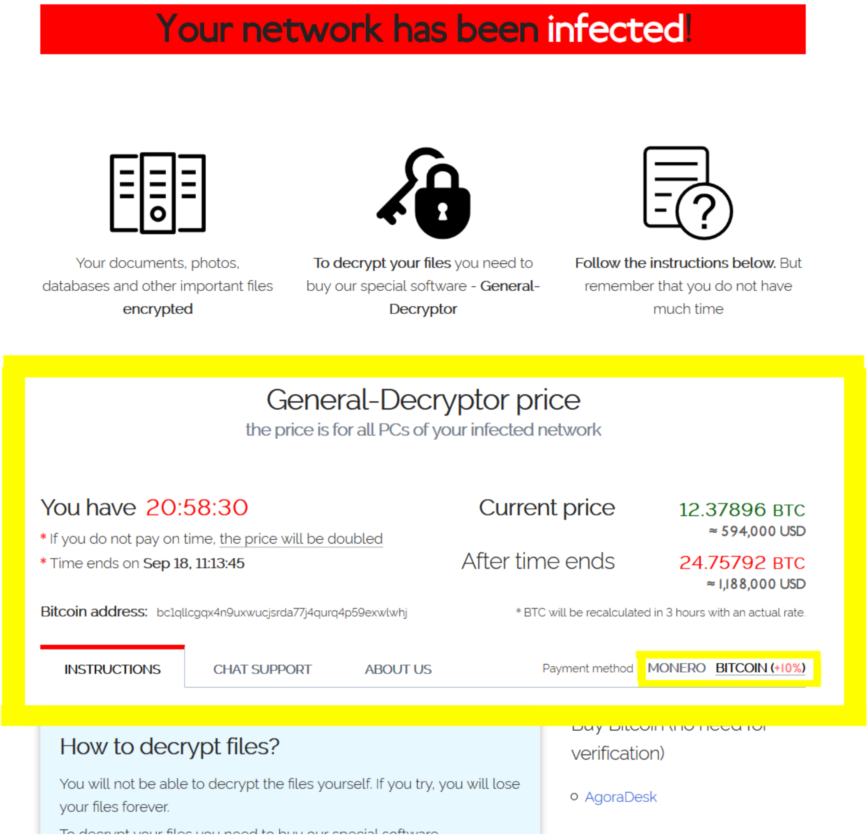
Monero address: 862Pont56BdEQ2vdPzEEofda557UHvERcYq1z

* XMR will be recalculated in 2 hours with an actual rate.

Buy XMR (no need for

Example of REvil payment options in XMR only [Source: Collected by CipherTrace Intelligence]

However, CipherTrace analysts have discovered that should REvil receive a message through their "chat support" and requesting to pay in BTC instead then they will enable the option. And like other ransomware groups, payment in BTC comes with a 10% premium.



Your network has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 20:58:30

* If you do not pay on time, the price will be doubled

* Time ends on Sep 18, 11:13:45

Current price 12.37896 BTC ≈ 594,000 USD

After time ends 24.75792 BTC ≈ 1,188,000 USD

Bitcoin address: bc1qllcgqx4n9uxwucjsrda77j4qurq4p59exwlwhj

* BTC will be recalculated in 3 hours with an actual rate.

Payment method MONERO BITCOIN (+10%)

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

To decrypt your files you need to buy our special software

Buy Bitcoin (no need for verification)

- AgoraDesk

Example of REvil payment options in BTC [Source: Collected by CipherTrace Intelligence]

FinCEN has identified 17 ransomware-related reports requesting payment in XMR so far in 2021.

According to CipherTrace data, at least 22 ransomware groups/strains accept only XMR. Not all are currently active. Those are as follows (alphabetical order):

1. _encrypted (RRansom)
2. !secure
3. AvosLocker
4. BlackSun
5. BleachGap
6. Creeper
7. Cripton
8. CRYPTEDPAY
9. Everest
10. JackSparrow
11. Kraken
12. Matryoshka
13. Monero
14. Onim
15. ORAL
16. Panther
17. Prometheus
18. Redeemer
19. Steel
20. Vovalex
21. Woodrat
22. Yogynicof

At least 7 Ransomware groups/strains accept both BTC and XMR. Those are as follows:

1. AstraLocker
2. Axiom
3. Assist
4. BlackMatter
5. DarkSide
6. Exe (JigSaw)
7. REvil

These lists are not complete; they simply include the ransomware variants we can say with certainty demand XMR based on our current data. The following is a list of 23 ransomware groups/strains that CipherTrace has XMR addresses for (on top of those previously mentioned), however, we either know that they do not demand XMR or we can't say with certainty that they do. Many of these addresses were obtained through social engineering (posing as someone wishing to purchase data and requesting XMR payment options, for example).

List of further ransomware that CipherTrace has XMR addresses for:

1. Avaddon
2. Bagli
3. CovidCry
4. Crylock
5. Cuba
6. 6Curator
7. 7Dharma/ Crysis
8. Encrypted
9. FilesRecoverEN
10. GlobeImposter 2.0
11. LockerXXS
12. Makop
13. MauriGo
14. Phobos
15. Prometheus
16. RedDot
17. Ryuk.Net Builder
18. Smaug
19. Snatch
20. Tell You the Pass
21. VoidCrypt
22. WannaDie
23. Zeppelin

Most of the groups and strains listed as using XMR are relatively new. CipherTrace analysts have observed a trend of increasing use of XMR by darknet markets and ransomware actors; however, while we have a list of over 50 groups and strains that use XMR, the list of those using BTC is well over 1,000. As ransomware strains come and go, most of those will no longer be active but BTC is still the dominant cryptocurrency used among criminals.

According to FinCEN's 2021 Ransomware report, in the first half of 2021, only seven reported ransomware payments were offered in either XMR or BTC, totaling $34 million. There were also seven reported transactions in which the attacker demanded XMR only, totaling roughly $2.4 million.

With reported ransomware payments totaling $590 million in the first half of 2021, ransomware payments where the attackers demanded either BTC or XMR made up just 5.7% of all transactions. Payments where attackers demanded only XMR made up just 0.4% of all reported ransomware related transactions at this time. This is in line with CipherTrace analysis that BTC is still the dominant cryptocurrency used among ransomware actors.

Ransomware Demands in Monero Only

Many new ransomware actors demand Monero (XMR) only. A recent double extortion ransomware attack of interest that demanded XMR only came from Everest Ransomware on October 5, 2021. Everest posted on their leak website that they had allegedly hacked the US Government. As the US Government does not pay ransom demands, the choice to target an undisclosed US government agency is an interesting choice for ransomware actors. At the time of this report, the Everest ransomware team is selling the purported stolen data to whoever wants it.

Everest Ransomware is currently trying to sell the data for $500,000 in XMR and refuse to accept BTC. However, they are also refusing to provide any proof of the stolen data, which is unusual for ransomware leakers. This is an evolving story and CipherTrace analysts are continuing to collect data around this supposed attack.

While the hack remains unsubstantiated, when coupled with the rise of double extortion attacks over the past two years, this attack could be indicative of the future of ransomware where more interest is placed on payments for leaks rather than the unlocking of data.

Ransomware Demands in Additional Cryptocurrencies

A few ransomware groups and strains use cryptocurrencies other than BTC and XMR, but this is rare. Anatova and GandCrab Ransomware demand payment in DASH. DeroHE Ransomware demands payment in DERO, another privacy coin like XMR. ZCash (ZEC) is the second largest privacy coin (or anonymity enhanced cryptocurrency: AEC) in market cap, behind XMR, but CipherTrace researchers haven't yet seen any ransomware actors demand payment in ZEC. However, there are several darknet markets that have recently accepted ZEC (Mega Market, ToRReZ Market, etc), so it stands that ZEC could be another cryptocurrency demanded by ransomware actors in the future.

Where are Ransomware Funds Going?

CipherTrace conducted an on-chain forensic investigation into the flow of funds of major ransomware actors in 2021. This section covers a few examples of common typologies observed when analyzing ransomware funds movements. These typologies are not distinct to ransomware and have been observed in various criminal actors laundering crypto assets, including terrorist organizations. More than one typology is typically observed when washing funds.

One observation CipherTrace forensic analysts have detected that is more specific to ransomware, however, is that ransomware operators are more likely than other criminals (such as hackers or fraudsters) to consolidate and hold funds long-term rather than immediately move funds to a fiat off-ramp such as an exchange.

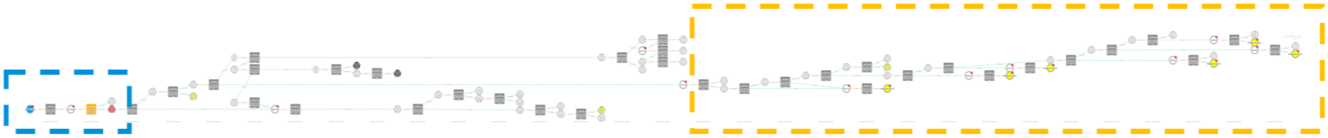
In a ransomware-as-a-service (RaaS) model, however, where **ransomware affiliates** buy specific ransomware strains from **ransomware operators** to deploy on victims, the RaaS affiliates are often more likely to move funds immediately whereas the RaaS operators are still more likely to hold.

Mixers and Coinjoins

It's common for any criminal operating in BTC to attempt to wash funds through mixers or coinjoins to obfuscate their trails. However, CipherTrace analysts have observed that mixing funds in general is not as common by ransomware actors.

While mixers offer higher transactional anonymity because of the custodial nature of their services, Wasabi coinjoins are seen more often by CipherTrace analysts. The non-custodial nature of a coinjoin means the user remains in full control of his or her funds and does not need to rely on a trusted-third party that could potentially abscond with the cryptocurrency or keep records of the transactions.

JBS, the world's largest meat supplier, fell victim to a REvil ransomware demand of $11 million in bitcoin on June 1, 2021. While the majority of these funds had remained in unhosted addresses since the attack, not long after the October arrest of Yaroslav Vasinskyi, linked to REvil, funds started to move again. This time, the funds were immediately washed through coinjoins to obfuscate their trail.



JBS Payment to REvil on June 1, 2021
301 BTC

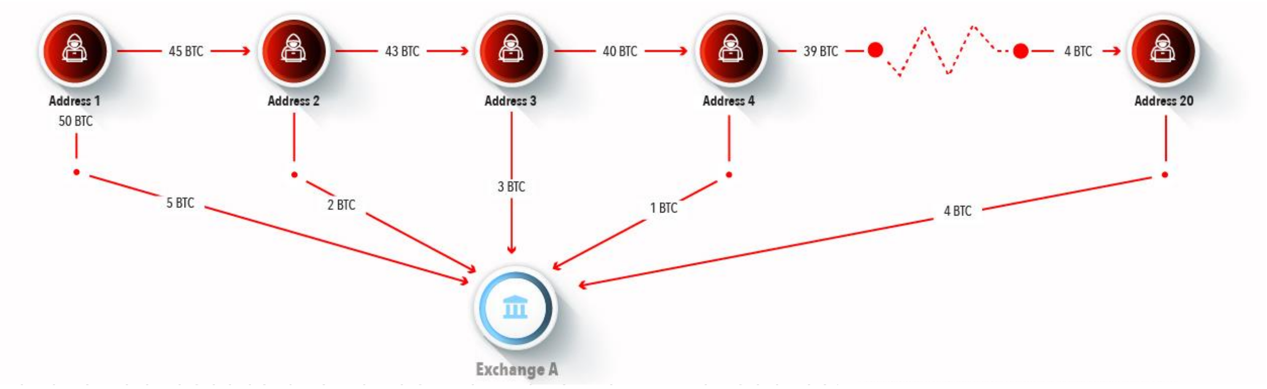
Movement of funds after October 28, 2021
Multiple deposits into Wasabi Coinjoins totaling 199 BTC

Source: CipherTrace Intelligence

Peel Chains into High-Risk Services

It is common for any criminal actors to use peel chains when laundering victim funds and ransomware operators are no different.

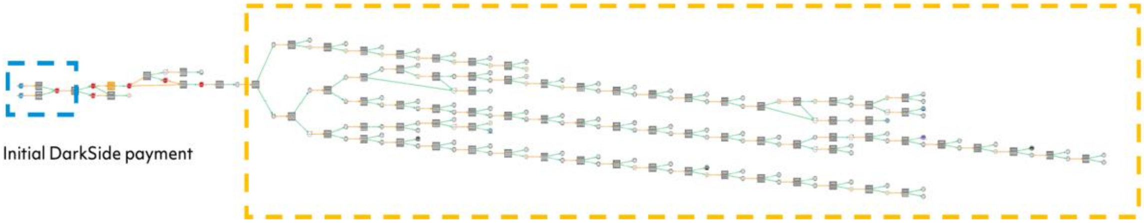
A peel chain occurs when a large amount of BTC sitting at one address is sent through a series of transactions in which a slightly smaller amounts of BTC is transferred—or "peeled"— off the chain to other addresses and the remaining balance is transferred to the next address in the chain.



Source: CipherTrace Intelligence

In the example below, DarkSide ransomware payments are consolidated and then peeled and eventually deposited into multiple global, off-shore, and P2P exchanges, as well as World Market—a dark market known for hacking tools and services.

While most criminals empty peel chains into exchanges, it's common to see ransomware actors and other hacking groups peel into dark markets where they can continue to purchase hacker tools and services that facilitate their illicit business. Dark markets can also be used to purchase stolen credentials and iTunes gift cards as additional means to launder stolen crypto.



Initial DarkSide payment

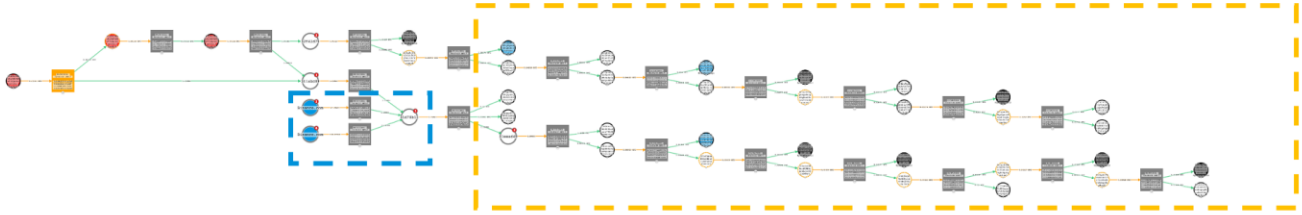
Peel chains eventually deposit into multiple global, off-shore, P2P exchanges, and dark markets

Source: CipherTrace Intelligence

Moving Funds After Increased Scrutiny

Ransomware operators are usually more willing to park funds and wait instead of eagerly looking to cash out. However, increased global scrutiny around ransomware at the end of May 2021 resulted in some ransomware actors moving their cryptocurrency off of exchanges, likely to safeguard funds out of fear of potential seizures.

An example of this can be seen when the Lockbit Ransomware Group moved funds off of a large, global exchange at the end of May and peeled the funds into high-risk exchanges known for dealing in crypto-to-ruble exchanges and Hydra Market, a large Russian dark market.



Lockbit Ransomware Group
moves funds off large, global exchange

Funds are peeled into a series of different
high-risk exchanges and Hydra Market

Source: CipherTrace Intelligence

This tactic of moving funds off of one large, global exchange and peeling into dark markets and other exchanges (or in one case, into a different account at the same exchange) was also observed by CipherTrace analysts in the movement of funds by terrorist organization al Qassam Brigades after seizures by Israel's National Bureau for Counter Terror Financing (NBCTF).

Conclusion

In the wake of large-scale ransomware attacks like those against the Colonial Pipeline and JBS, cybercrime and ransomware continue to be top of mind for global corporations and governments alike. As consumer purchasing moved to online transactions (digital trade) during the COVID-19 pandemic, the incidence of cybercrime also grew. Earlier this year, FBI Director Christopher Wray compared the bureau's shift to global ransomware threats to the agency's shift to the threat of global terrorism after the 9/11 attacks.

As the digital economy grows, cyberattacks are increasing and federal investigations into ransomware are growing at exponential rates. It's now a business imperative for companies to have a disaster preparedness plan in place for cyberattacks & security breaches in order to mitigate risk and limit their liability.

The exponential increase in double extortion attacks over 2021 highlight the importance of proper cyber security protocols and training to not just recover after a ransomware attack but prevent and detect ransomware actors before they have the opportunity to attack in the first place. It's no longer enough to just have backups to mitigate the effects of a ransomware attack when hackers are now more than ever threatening to leak stolen information if payments are not made.

Best Practices to Minimize Ransomware Attacks

There are several steps that companies can take to minimize the damage from a ransomware attack, including:

- Prepare an incident response plan and have it on hand before an attack occurs.
- Choose an incident response firm using effective blockchain analytics and cryptocurrency intelligence software, such as CipherTrace, to track the cryptocurrency payments made to the hackers.
- Consider purchasing cybersecurity insurance.
- Gather as much information as possible about the hackers and the attack before making the ransom payment.
- Evaluate whether or not making a ransomware payment qualifies as a sanction violation. Sanctions violations can result in costly civil fines and even prison time for the ransomed party.
- Pay in BTC; avoid using anonymity-enhancing technology or privacy coins to pay ransoms.
- Report all ransomware attacks to national law enforcement and agencies listed in OFAC's updated advisory, and apply for a special license to make a payment to illicit actors.

There's a lot of information that you can gather within a relatively short amount of time, before deciding to make a payment. That's where the incident response firms, due diligence and blockchain analytics companies like CipherTrace can step in and help. Should a payment be made inadvertently to sanctioned actors, OFAC takes into consideration the victim's steps during the incident including reporting which may mitigate any potential enforcement action.

In addition to formulating an incident response plan, businesses should work with lawmakers and international law enforcement agencies to prevent future attacks. There's a valuable role that both public and private sector can play in working together to prevent cybercrimes.

Blockchain analytics provides critical cryptocurrency intelligence needed to trace ransomware actors. Only by working together through public-private partnerships can cryptocurrency intelligence firms counter these transnational threat actors. It is crucial to not only trace ransomware proceeds to find and stop the operators, but also to harden systems and educate the public on how these compromises occur in order to properly mitigate disruption. Incident Response Firms have vast databases of ransom payments from their clients;

identifying and tracking these funds can aid in building a full profile of the ransomware group.

Because ransomware actors use public blockchains for receiving payments, all transactions can be viewed on the chain, enabling law enforcement (or anyone) to trace the flow of funds. Utilizing a blockchain analytics tool like CipherTrace Inspector provides additional intelligence to the trace and investigation, such as identifying when the funds have been deposited into an exchange. Once the funds reach a centralized exchange, law enforcement can stop the movement of funds by requesting that the exchange freeze the account and obtain additional information from the centralized exchange to inform their investigation.

For more information on how CipherTrace can help, email:
contact@ciphertrace.com

This Report contains the proprietary information of CipherTrace Inc ("CipherTrace"). It is intended to be used internally within your organization and by receiving this information, you agree that except with the prior written permission of CipherTrace, such information shall not be used for any unauthorized purpose and shall not be published or disclosed by you to third parties, in whole or part.

The information contained in this Report, including all forecasts and projections are provided to you on an "AS IS" basis for use at your own risk. CipherTrace will not be responsible for any action you take, or do not take, as a result of this Report or any inaccuracies, inconsistencies, formatting errors, or omissions in this Report. CipherTrace makes no representations or warranties, express or implied, as to the accuracy or completeness of the information contained herein, and CipherTrace will not have any liability to you or any other person resulting from the use of such information by you or any of your representatives.

Follow this code to read all CipherTrace's quarterly reporting and learn more.

https://ciphertrace.com/resources/

CipherTrace protects financial institutions from cryptocurrency laundering risks and helps grow the blockchain economy by making it safe for consumers, trusted by investors and accepted by governments.