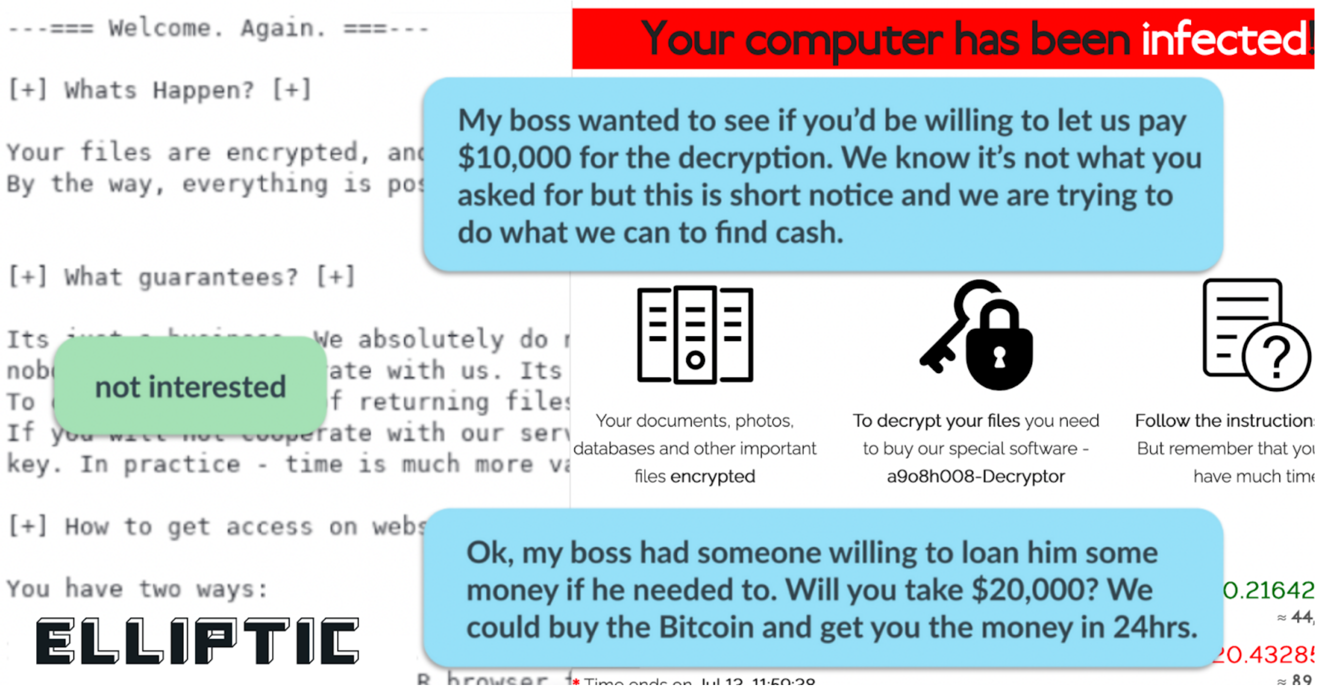
REvil Revealed - Tracking a Ransomware Negotiation and Payment

elliptic.co/blog/revil-revealed-tracking-ransomware-negotiation-and-payment



```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and
By the way, everything is pos

[+] What guarantees? [+]

Its                  We absolutely do
nob                  ate with us. Its
To                   f returning files
If you will not cooperate with our serv
key. In practice - time is much more va

[+] How to get access on webs

You have two ways:
```

Your computer has been infected!

My boss wanted to see if you'd be willing to let us pay $10,000 for the decryption. We know it's not what you asked for but this is short notice and we are trying to do what we can to find cash.

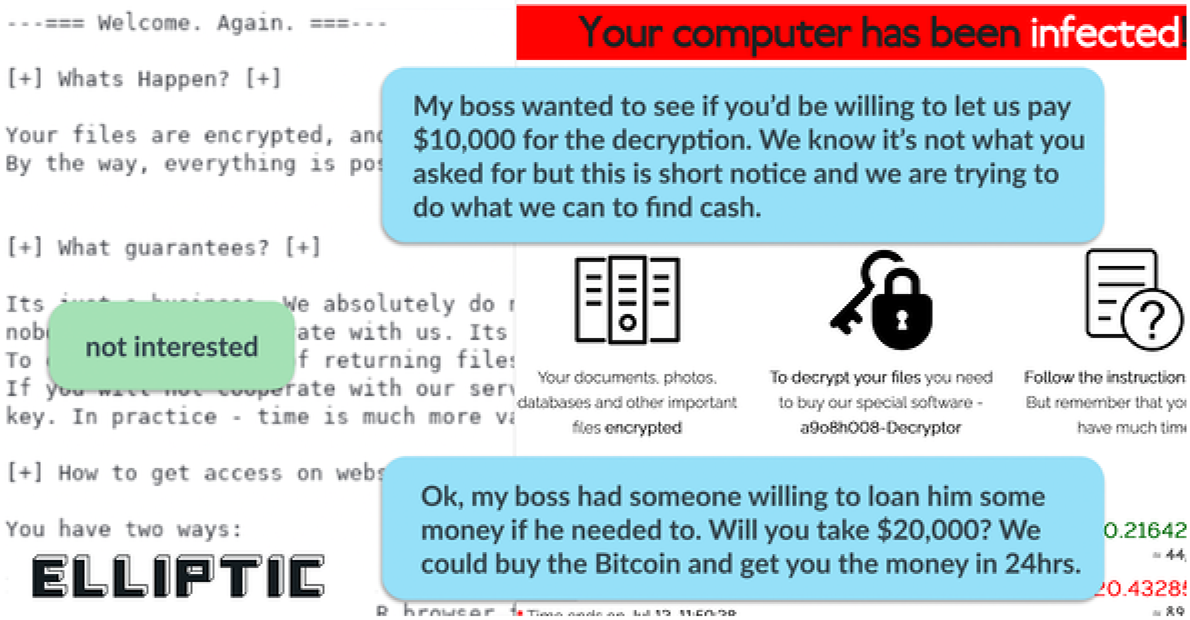
not interested

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - a9o8h008-Decryptor

Follow the instruction But remember that you have much time

Ok, my boss had someone willing to loan him some money if he needed to. Will you take $20,000? We could buy the Bitcoin and get you the money in 24hrs.



```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and
By the way, everything is pos

[+] What guarantees? [+]

Its                  We absolutely do
nob                  ate with us. Its
To                   f returning files
If you will not cooperate with our serv
key. In practice - time is much more va

[+] How to get access on webs

You have two ways:
```

Your computer has been infected!

My boss wanted to see if you'd be willing to let us pay $10,000 for the decryption. We know it's not what you asked for but this is short notice and we are trying to do what we can to find cash.

not interested

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - a9o8h008-Decryptor

Follow the instruction But remember that you have much time

Ok, my boss had someone willing to loan him some money if he needed to. Will you take $20,000? We could buy the Bitcoin and get you the money in 24hrs.

Elliptic Intel

What actually happens during a ransomware attack? We follow a real case involving the REvil ransomware - from initial infection and negotiation, through to the cryptocurrency payment and laundering of the funds.

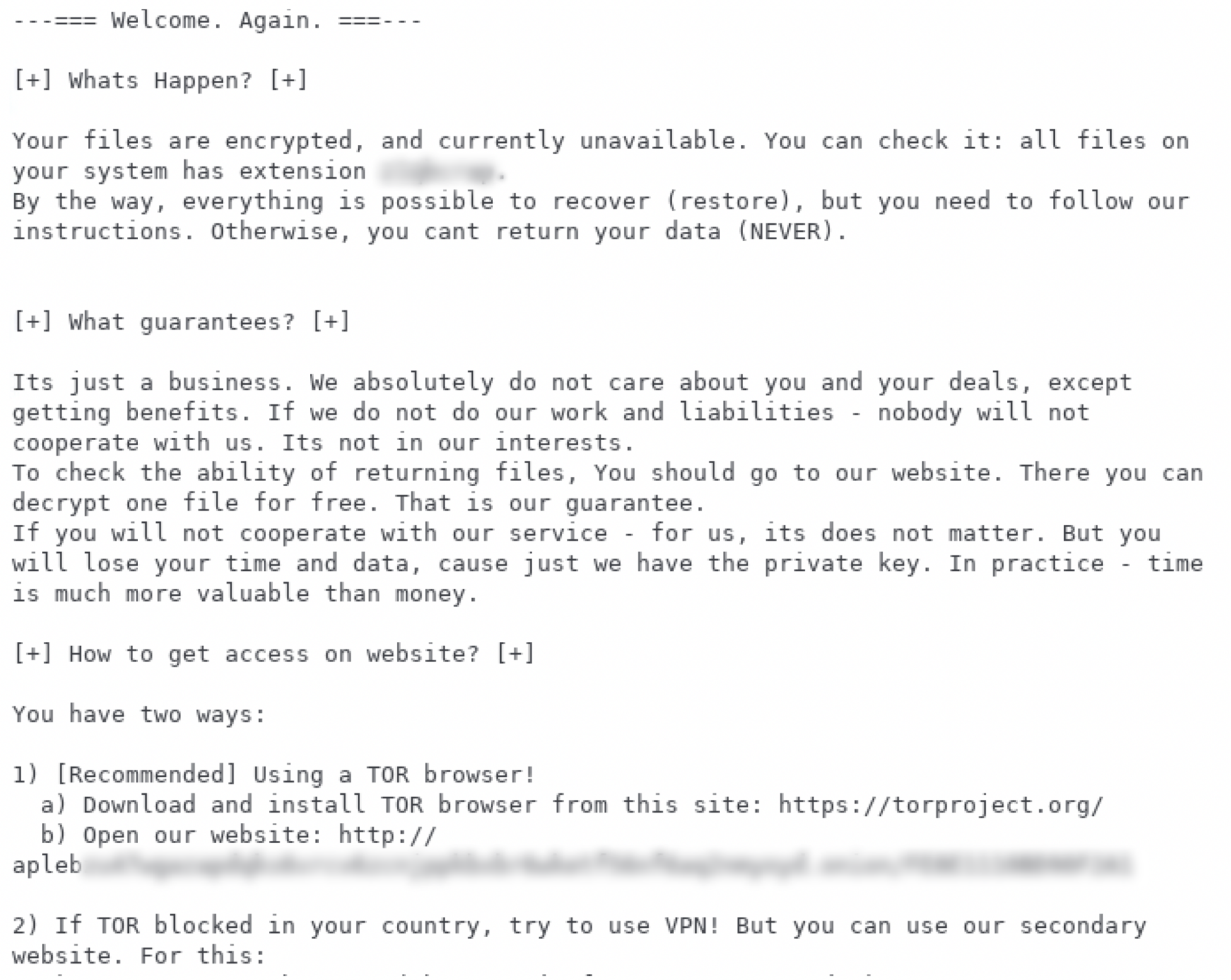
The scale and severity of ransomware attacks continue to grow. Cybercriminal groups such as DarkSide have received hundreds of millions of dollars in cryptocurrency ransom payments, having crippled critical infrastructure providers such as Colonial Pipeline. In early July, hundreds of businesses were infected with REvil ransomware (also known as Sodinokibi), through an attack on Kaseya - a provider of IT management software to those victims.

At Elliptic, we monitor and investigate ransomware groups in order to collect information on the cryptocurrency wallets they use to receive ransoms. These insights are then made available in our software, enabling law enforcement to follow the money and potentially freeze the funds or identify the individuals behind the attacks. Cryptocurrency exchanges and financial institutions use our software to screen customer deposits for links to these wallets, and ensure that the ransomware groups cannot cash-out their proceeds.

This research gives us unique insights into the entire lifecycle of a ransomware attack - from the initial malware infection and ransom demand, through the negotiation and payment process, and finally the laundering of the funds. In this article we follow one specific attack by the Russia-linked REvil ransomware group, which took place within the past few weeks. Some images have been edited to protect the identity of the victim.

1. The victim is infected with the REvil malware

Once the REvil malware has made its way onto the computer system, it encrypts the victim’s files - leaving behind a text file containing the ransom note, shown below:



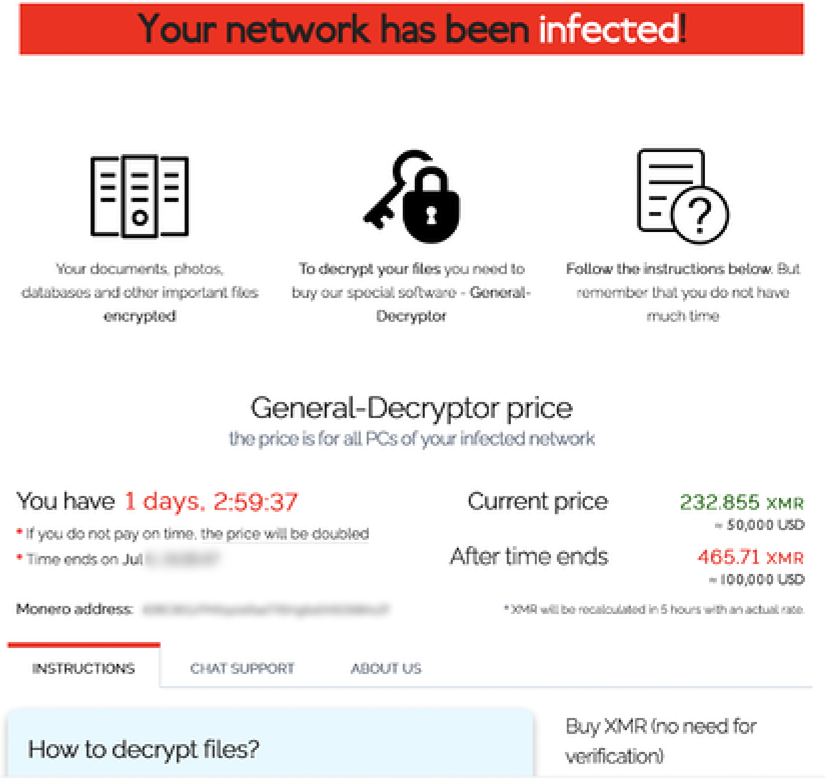
```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on
your system has extension [redacted].
By the way, everything is possible to recover (restore), but you need to follow our
instructions. Otherwise, you cant return your data (NEVER).


[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except
getting benefits. If we do not do our work and liabilities - nobody will not
cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can
decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you
will lose your time and data, cause just we have the private key. In practice - time
is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://
apleb[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary
website. For this:
```

The note directs the victim to a website (the “victim portal”) on Tor (an anonymous version of the internet often used to host darknet markets), to access further instructions.

2. Accessing the victim portal

The victim portal displays the ransom demand - $50,000 in Monero, a privacy-focused cryptocurrency that is very difficult to trace. If the ransom is not paid within a certain timeframe, the ransom will be doubled to $100,000.

The portal provides instructions on where the Monero can be purchased, and where exactly it should be sent:



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 1 days, 2:59:37

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

* Time ends on Jul [redacted]

Current price 232.855 XMR ≈ 50,000 USD

After time ends 465.71 XMR ≈ 100,000 USD

Monero address: [redacted]

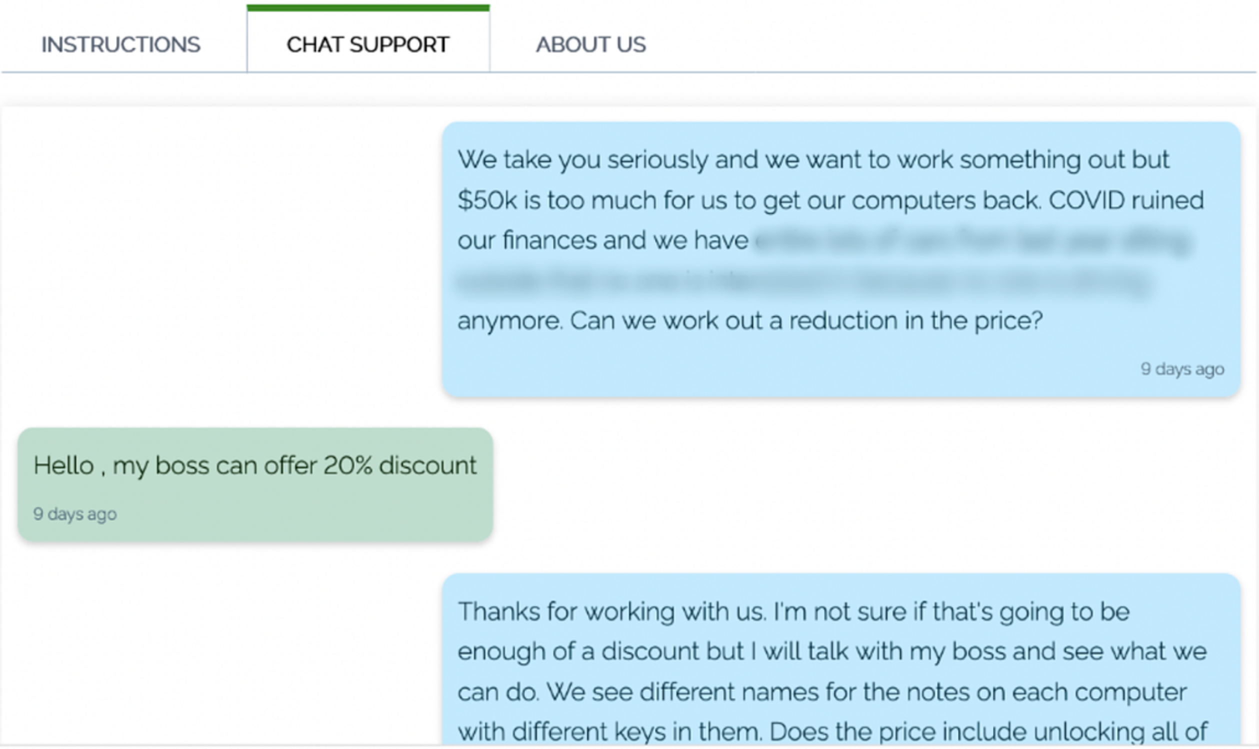
*XMR will be recalculated in 5 hours with an actual rate.

How to decrypt files?

Buy XMR (no need for verification)

3. Chat support

Similar to an e-commerce site, the portal allows the victim to speak directly to REvil, through the "Chat Support" tab. Here we see the victim (blue) initiate a conversation with REvil (green) and begin to negotiate the ransom down:



We take you seriously and we want to work something out but $50k is too much for us to get our computers back. COVID ruined our finances and we have [redacted] anymore. Can we work out a reduction in the price?

9 days ago

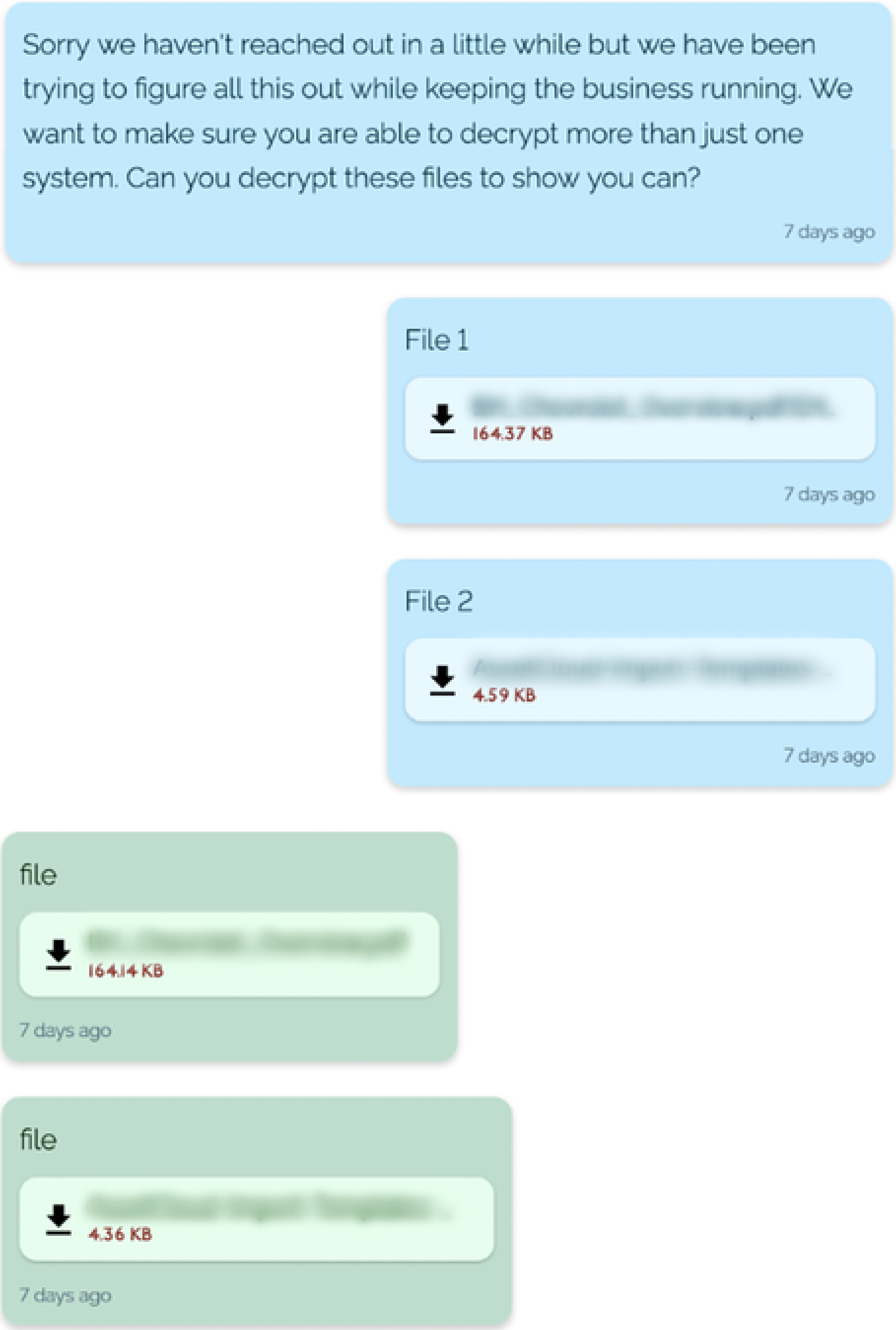
Hello , my boss can offer 20% discount

9 days ago

Thanks for working with us. I'm not sure if that's going to be enough of a discount but I will talk with my boss and see what we can do. We see different names for the notes on each computer with different keys in them. Does the price include unlocking all of

4. Verifying that paying a ransom will lead to decryption

The victim then asks for proof that paying the ransom will work - i.e. that their files will be decrypted. They upload two of their encrypted files, and REvil responds with the proof - the decrypted files:



Sorry we haven't reached out in a little while but we have been trying to figure all this out while keeping the business running. We want to make sure you are able to decrypt more than just one system. Can you decrypt these files to show you can?

7 days ago

File 1

[redacted]
164.37 KB

7 days ago

File 2

[redacted]
4.59 KB

7 days ago

file

[redacted]
164.14 KB

7 days ago

file

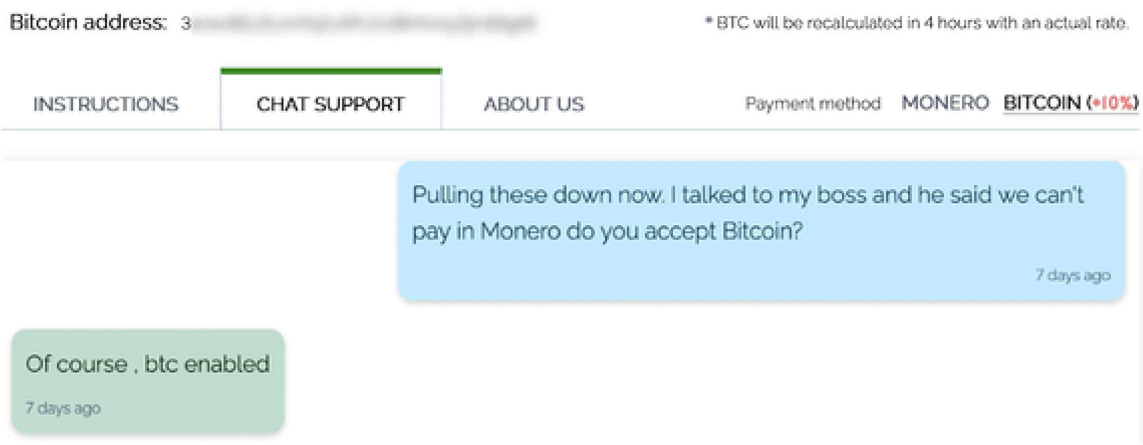
[redacted]
4.36 KB

7 days ago

5. Requesting payment in Bitcoin instead of Monero

Many ransomware victims find it difficult to obtain the Monero required to pay a ransom (not many exchanges list it, especially in the US), or do not want to pay in Monero due to concerns about violating sanctions. Most of the ransomware response companies that negotiate and pay on behalf of victims simply refuse to pay Monero ransoms.

In this case the victim has requested to pay in Bitcoin instead and REvil has allowed it, albeit with a 10% surcharge. This higher amount reflects the increased risk faced by REvil when accepting Bitcoin payments, due to its traceability. The portal updates to show a Bitcoin payment address:



Bitcoin address: 3[redacted]

* BTC will be recalculated in 4 hours with an actual rate.

Payment method MONERO BITCOIN (+10%)

Pulling these down now. I talked to my boss and he said we can't pay in Monero do you accept Bitcoin?

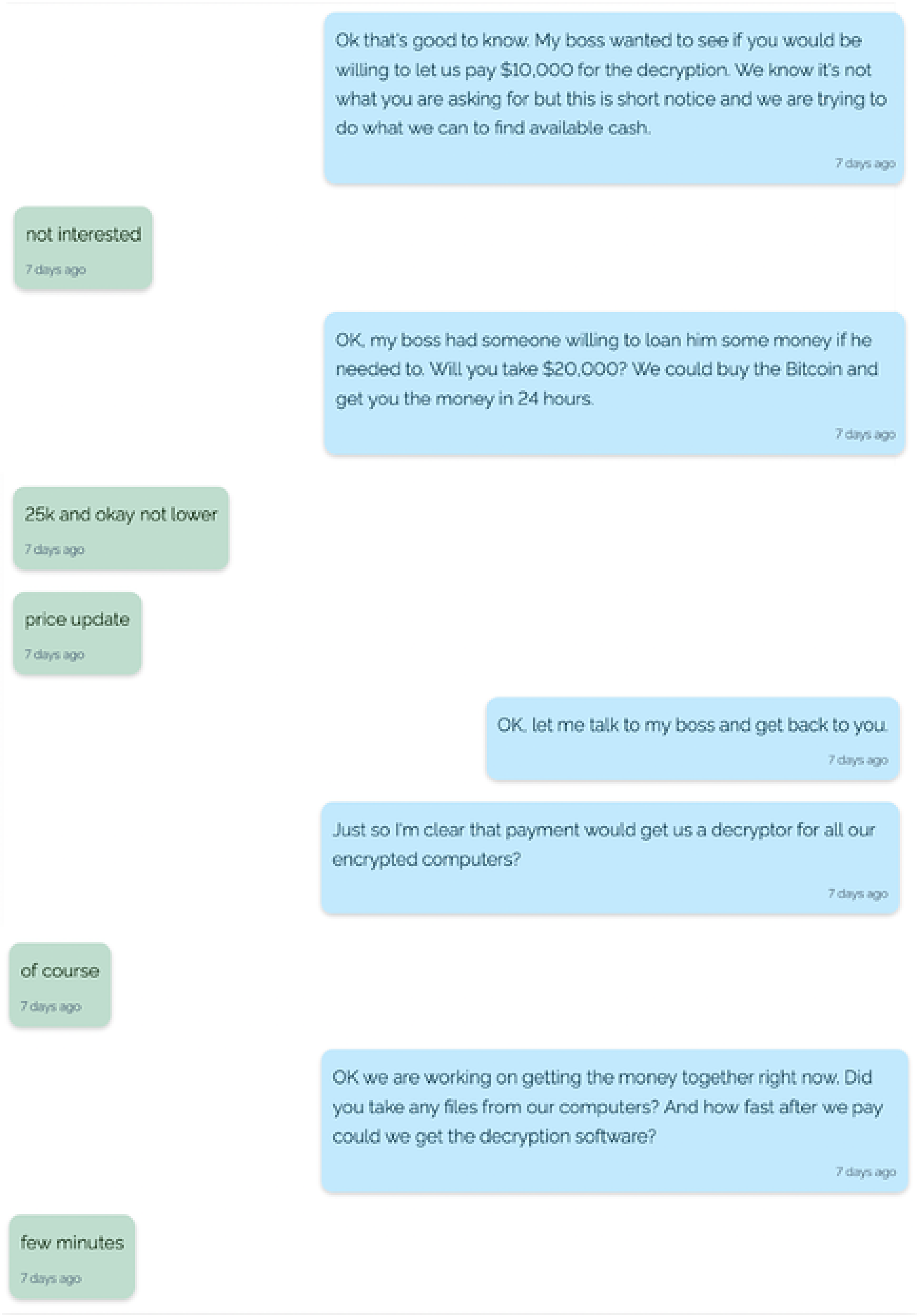
7 days ago

Of course , btc enabled

7 days ago

6. Negotiating the ransom amount

Having already negotiated a 20% discount on the original $50,000 ransom demand, the victim goes further - offering just $10,000. They claim that this is all they can pay at such short notice, but the offer is rejected by REvil. The victim then says that they may be able to borrow some extra money, and they eventually agree on a ransom payment of $25,000.



Ok that's good to know. My boss wanted to see if you would be willing to let us pay $10,000 for the decryption. We know it's not what you are asking for but this is short notice and we are trying to do what we can to find available cash.

7 days ago

not interested

7 days ago

OK, my boss had someone willing to loan him some money if he needed to. Will you take $20,000? We could buy the Bitcoin and get you the money in 24 hours.

7 days ago

25k and okay not lower

7 days ago

price update

7 days ago

OK, let me talk to my boss and get back to you.

7 days ago

Just so I'm clear that payment would get us a decryptor for all our encrypted computers?

7 days ago

of course

7 days ago

OK we are working on getting the money together right now. Did you take any files from our computers? And how fast after we pay could we get the decryption software?

7 days ago

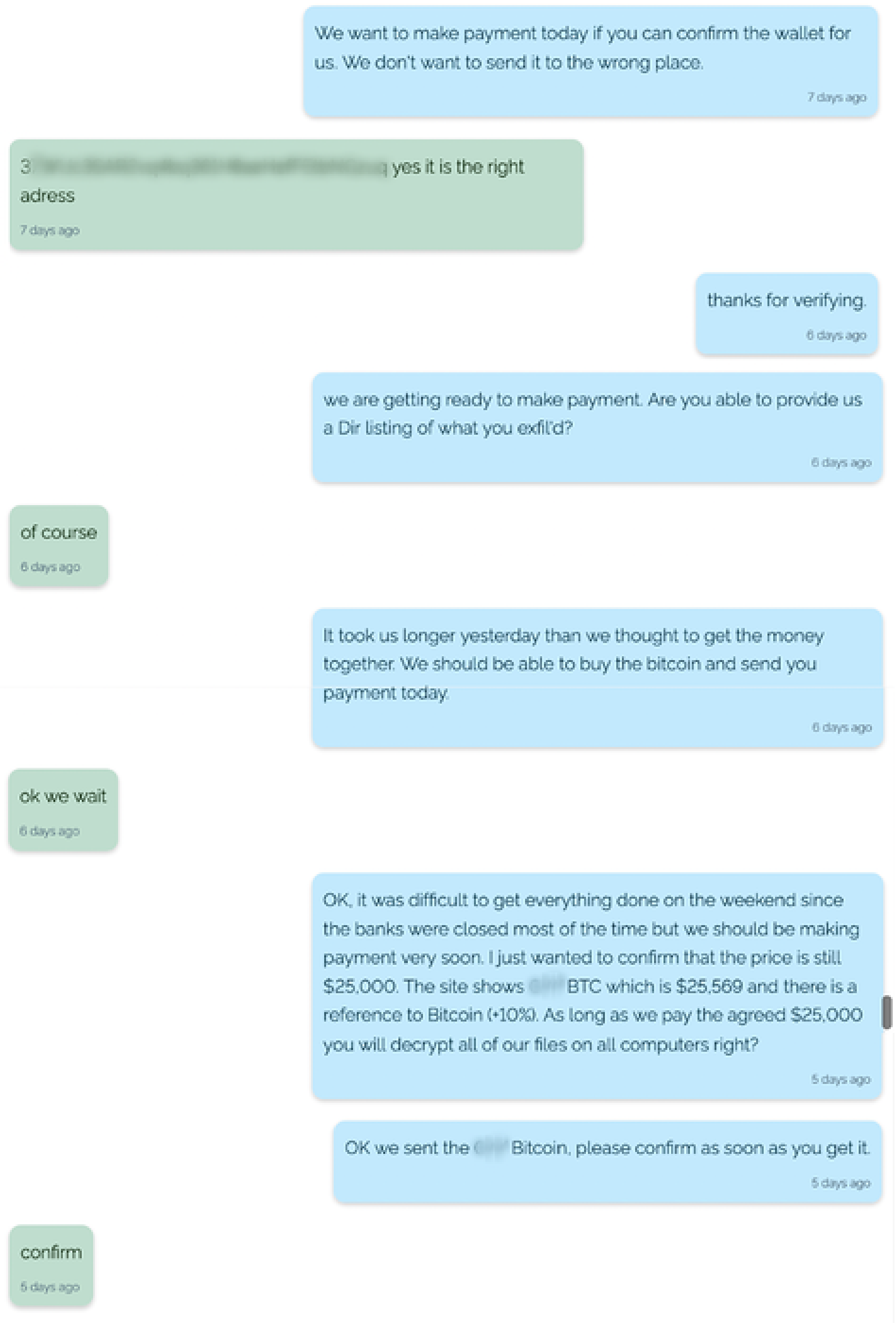
few minutes

7 days ago

7. Sending the Bitcoin ransom payment

The address that the bitcoin ransom should be sent to is displayed at the top of the portal, but the victim asks REvil to confirm that it is correct. Cryptocurrency payments are irreversible, so it is important to verify the destination address before making a transaction.

The victim sends the $25,000 in Bitcoin, and REvil confirms that they have received it:



We want to make payment today if you can confirm the wallet for us. We don't want to send it to the wrong place.

7 days ago

3[redacted] yes it is the right adress

7 days ago

thanks for verifying.

6 days ago

we are getting ready to make payment. Are you able to provide us a Dir listing of what you exfil'd?

6 days ago

of course

6 days ago

It took us longer yesterday than we thought to get the money together. We should be able to buy the bitcoin and send you payment today.

6 days ago

ok we wait

6 days ago

OK, it was difficult to get everything done on the weekend since the banks were closed most of the time but we should be making payment very soon. I just wanted to confirm that the price is still $25,000. The site shows [redacted] BTC which is $25,569 and there is a reference to Bitcoin (+10%). As long as we pay the agreed $25,000 you will decrypt all of our files on all computers right?

5 days ago

OK we sent the [redacted] Bitcoin, please confirm as soon as you get it.

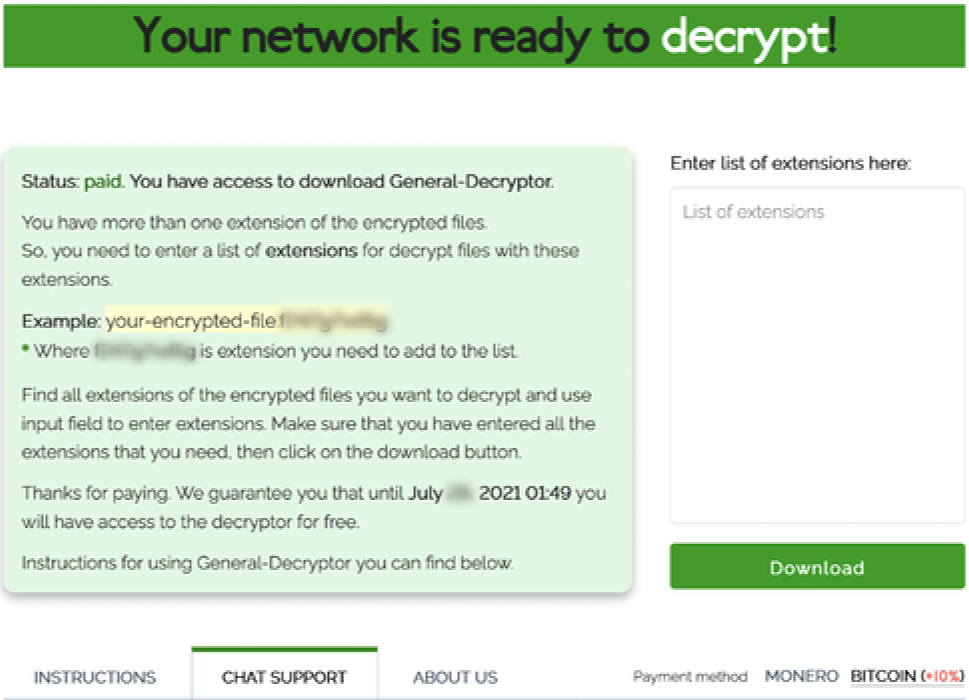
5 days ago

confirm

5 days ago

8. The decryption tool is provided

Once the ransom is paid, the victim portal updates to provide access to the decryptor. (Of course in general there is no guarantee that such a tool will be provided.)



Your network is ready to decrypt!

Status: paid. You have access to download General-Decryptor.

You have more than one extension of the encrypted files.
So, you need to enter a list of extensions for decrypt files with these extensions.

Example: your-encrypted-file.[redacted]
- Where [redacted] is extension you need to add to the list.

Find all extensions of the encrypted files you want to decrypt and use input field to enter extensions. Make sure that you have entered all the extensions that you need, then click on the download button.

Thanks for paying. We guarantee you that until July [redacted] 2021 01:49 you will have access to the decryptor for free.

Instructions for using General-Decryptor you can find below.

Enter list of extensions here:

For the victim, the process is now complete. They can use the decryptor tool to regain access to their files and resume operations.

9. The Bitcoin is laundered

For REvil the next step is to launder and cash-out the Bitcoin ransom payment. The image below is from our cryptocurrency investigations software, Elliptic Forensics, showing the destination of the Bitcoin ransom paid by this specific victim. Most exchanges that allow Bitcoin to be converted into traditional currency make use of Elliptic's tools in order to trace customer deposits and ensure that they are not connected to illicit activity such as this.

REvil must therefore attempt to launder the funds and break the transaction trail. They attempt this by "layering" the funds - splitting them and passing them through many different wallets, and by mixing them with bitcoins from other sources. This laundering process in this case is still ongoing, but nevertheless we can already trace some of the funds to exchanges. Those exchanges will have information on the identities of people whose accounts received the funds - providing strong leads for law enforcement.

The victim in this case appears to have been a small business rather than a large corporation - reflected in the relatively small ransom demanded. Small businesses make up 50-75% of all ransomware victims, and the impact on these attacks can be catastrophic.

At Elliptic we believe that ransomware can be combated by limiting the degree to which the criminals responsible can profit from their crimes. By mapping and understanding the cryptocurrency flows from ransomware wallets, we can aid law enforcement and financial institutions to identify the perpetrators and freeze their funds.

Join our upcoming webinar, on July 29: **Tracking Ransomware with Blockchain Analytics,** as we discuss how and why ransomware makes use of cryptocurrency, and showcase how it can be countered using blockchain analytics - including ‘following the money’ from cybercriminal wallets.

Disclaimer

This blog is provided for general informational purposes only. By using the blog, you agree that the information on this blog does not constitute legal, financial or any other form of professional advice. No relationship is created with you, nor any duty of care assumed to you, when you use this blog. The blog is not a substitute for obtaining any legal, financial or any other form of professional advice from a suitably qualified and licensed advisor. The information on this blog may be changed without notice and is not guaranteed to be complete, accurate, correct or up-to-date.