



LEMAGIT

Ransomware What breadcrumbs get left in negotiations?



Collecting 150+ ransomware negotiations

Revil, DarkSide, Avaddon, Ranzi, Avos, Hive, BlackMatter, Black Basta...

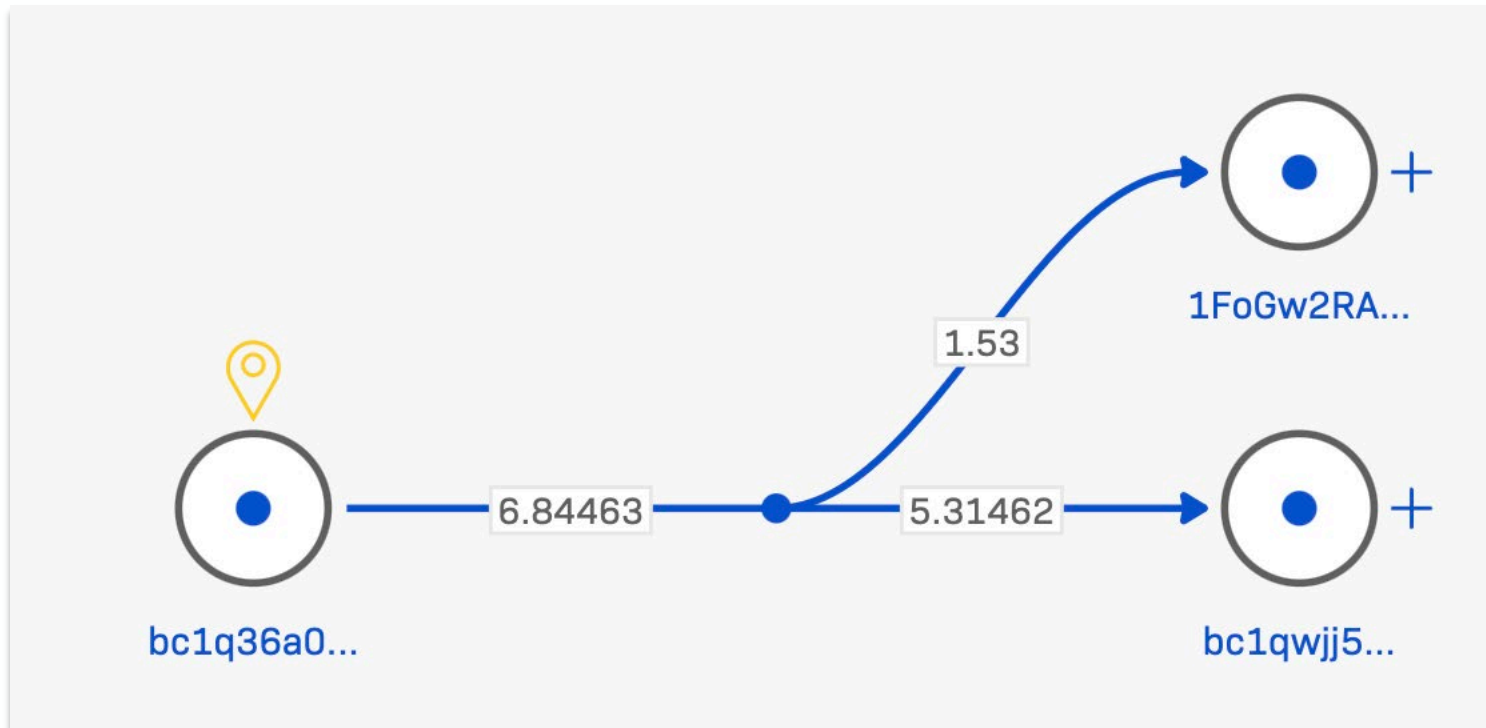
A privileged point of view
as negotiations are often dealt with away from the IR team.

Access to
decryptors, payment addresses, and some more insights

Follow the trail

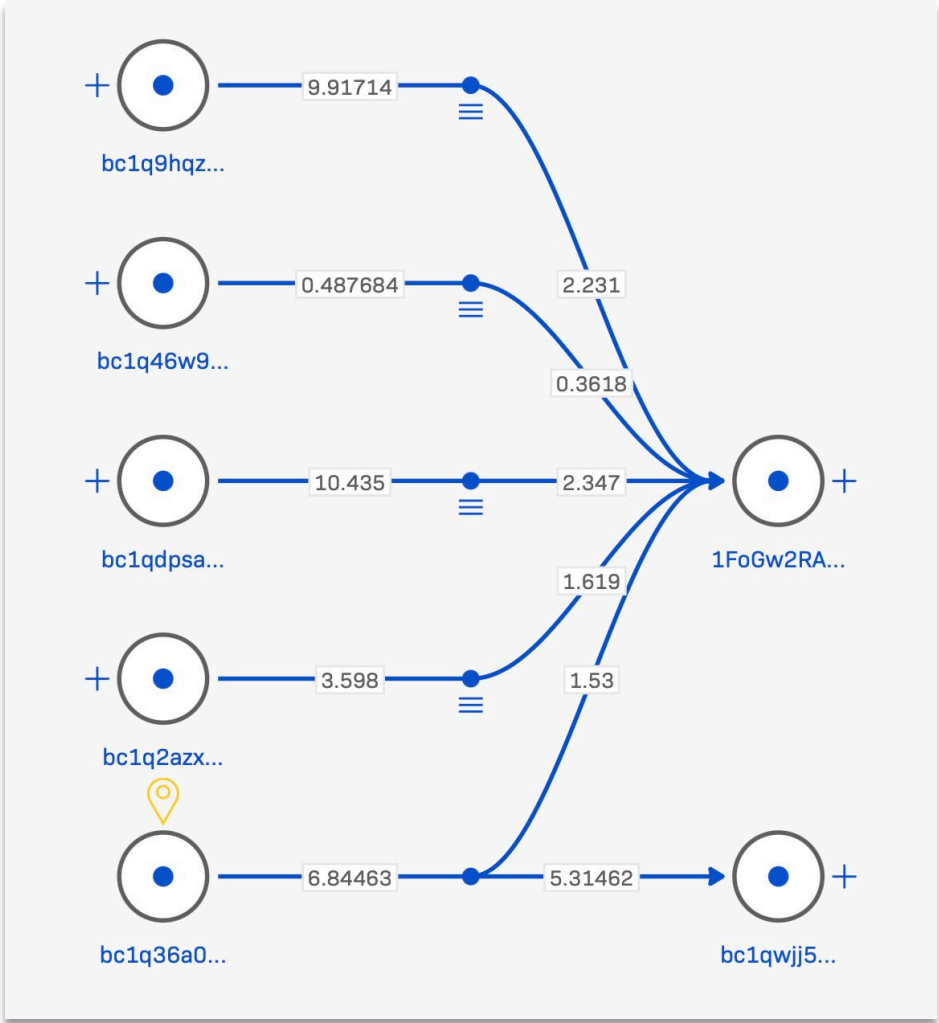
Show me the money

- Starting with an actually observed **ransom** payment.



Follow the trail

Show me the money

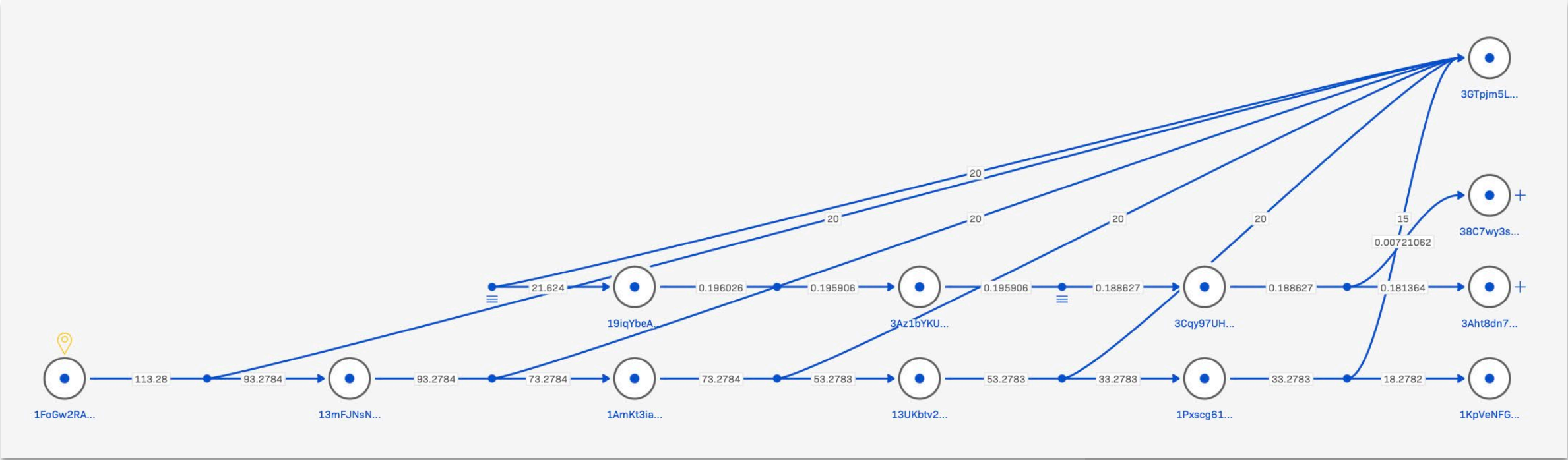


- Finding **consolidation nodes**.
- Assessing **past activity**
- ...

Follow the trail

Show me the money

- ... and following ongoing activity.



A peak into internal organisation

Tell me who you work with

This is ContiLocker Team.
Please, introduce yourself (Company name and your position) and we'll provide all necessary information.
Sometimes our staff is busy, but we will reply as soon as possible.
Be in touch, thank you

2 months ago

Hello, I'm with [REDACTED], one of the IT Engineers.
soon as possible with the necessary information.

As you already know, we penetrated your network and were in it for over 2 weeks (enough to study all your documentation), encrypted your file servers, sql-servers, downloaded all important information weighing over 100 GB: personal data of customers, employees (home addresses, scans of personal documents, phone numbers), consolidated financial reports, studies, payrolls, bank statements.
The good news is, we're businessmen. We want a ransom for anything that needs to be kept secret, and we don't want to ruin your business.
The amount at which we are willing to go out on a limb for you and leave everything as collateral is \$300,650. After payment, we will give you a tool to decrypt all your machines, a security report on how you were hacked, a file tree of what we downloaded from your network, and a log of the erasure of that information.

2 months ago

- A first script.
- Same for **17** negotiations.
- Exagrid, HSE, etc.

- Seems **based** on a script used with Fat Face and two previous victims.

A peak into internal organisation

Tell me who you work with

Hi There! This is Conti Team.

As you already know, we have infiltrated your networks, researched them, and found critical vulnerabilities which enabled us to access and exfiltrate your inner documentation and encrypt your file servers, SQL servers, subdomains, and local networks.

Due to poor security of your networks, we have downloaded your critical information with a total volume of more than 70 GB. This information includes personal data of your customers, employees, and vendors, as well as your legal, financial HR, IT, audit, and compliance directories (among other files). We obtained personal documents, phone numbers, contact information, consolidated financial statements, payroll, and banking statements.

Fortunately, Conti is here to prevent any further damages!

First, we can provide you with IT support by offering a decryption tool, as well as a security report that will address the initial issues with your network security that resulted in this situation.

Secondly, we offer you damage prevention services. At this point, all off your files are about to get public on our blog and will be available for anyone, including darknet criminals who are eager to abuse your information for their own evil purposes like social engineering attacks against your customers and vendors, spamming, and other bad actions.

Your customers, vendors, employees, and investors (lists are available from you inner documentation) will also be notified by us about the breach. This way then can know what to do, since their private data is getting public.

It goes with out saying that this privacy violation will lead to long-term legal, regulatory, financial, and reputational damages, including lost contracts and class action lawsuits from those whose info was exposed. However, as a part of our deal we offer a solution to prevent this from happening!

We will first give you a file tree to demonstrate which files we downloaded from your network. Then, you can chose certain file names from this listing and we will provide you with these files to prove that we have them. Then we transfer all the files that we have

- A second one.
- Seen with 8 negotiations.

A peak into internal organisation

Tell me who you work with

Support: Hi

Price for you is 1699btc. You need to pay this amount and we will give you decrypt tool for all your machines, security report on how you were hacked, file tree on what we have downloaded from your network and wiping log of that information.

Take into consideration that we have downloaded a lot of data from your network that in case of not payment will be published on public news website and sold on the black-markets. We remove it after payment and wiping log is provided as well. To start a business we offer you to make payment in two stages. What amount you can pay today?

 10/19/2020, 1:14:43 PM

- Already in 2020.
- Seen with **3** negotiations.

Bad habits

Tell me who you are

INSTRUCTIONS

CHAT SUPPORT

Proof

↓ **asteelflash_data_part1.7z**
8.5 MB

17 hours ago

Password: 123123

2 hours ago

We have your accounting, legal documents, finance, contracts and personal correspondence, DB, that's all I can say. It's about 200 Gigabate. You will receive a complete list of files after payment as well as a log of their removal from our server.

last month

[_proof.7z \[2.1MB \]](#)

last month

Proof Pack. Pass: 123123

last month

If you delay the negotiations, on Monday we will release information about the fact of hacking your network. Further, if you do not understand this, we will publish part of the data to find a buyer for them.

last month

We will also try to find a buyer for your data and access to your network if you refuse to pay.

last month

- Same password for the proof packs.
- **4** REvil cases, incl. Acer and Asteelflash.
- **4** Conti cases, nope public.

Merci !

Valéry Marchive (lemagit.fr)

@ValeryMarchive 