

CYBER SYNC UP

COMBATting CYBER CRIME



Welcome



TROY FILIPCEVIC

CEO & Founder
Emergence Insurance



Coordinating the National Response to Cybercrime Incidents

Insights from the
National Office of Cyber
Security

SLIDES REDACTED | TLP:AMBER



JOE SMITH

Assistant Secretary
of the Cyber Security Response
Coordination Unit (CSRCU)
National Office of Cyber Security



When Cyber Hits the Fan

Real-life cyber incidents



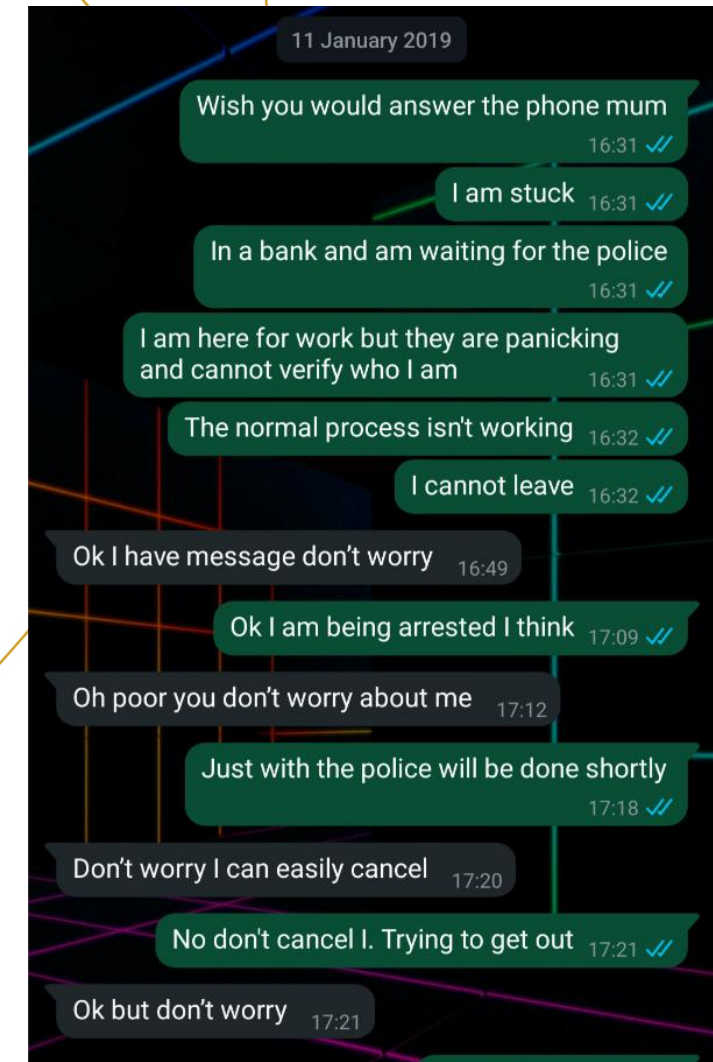
LUKE FARDELL

Lead Cyber Analyst
Tokio Marine Kiln

When Cyber Hits The Fan



TOKIO MARINE
KILN



Tokio Marine Kiln Role

- Lead Cyber Analyst
 - External attack surface scanning
 - Building tools
 - Helping on Complex Claims
 - Value Add services
 - Helping Group Companies
 - Bulk analysis of Coverholder portfolios

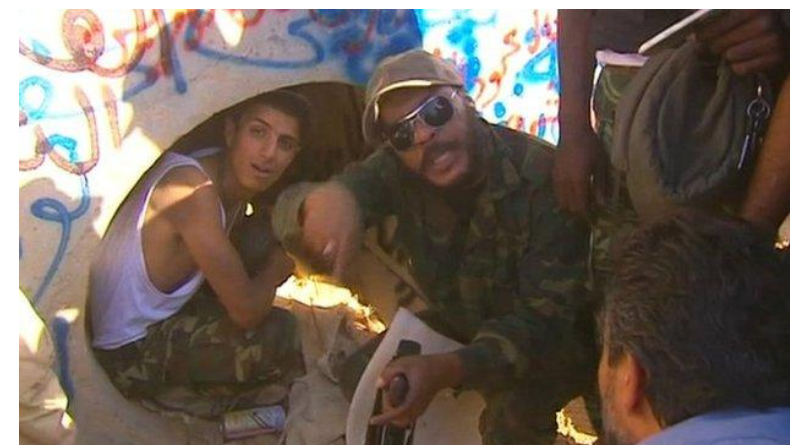
A screenshot of the Cyber Scanner dashboard. The dashboard has a dark theme with blue and white accents. It features several interactive panels: "Enter a Domain for a Risk Scan" with a search bar and a "Go" button; "Portfolio Management" with a dropdown menu and an "Open Portfolio" button; "Breach Search" with a search bar and a "Search" button; and "Search Company in Google for historic breaches" with a search bar and a "Search" button. On the right side, there is a "Flukey's Cyber Security News Feed" with several news items, including "Microsoft: Office 2016 and Office 2019 reach end of support in October", "CISA warns of increased breach risks following Oracle Cloud leak", "Identity Attacks Now Comprise a Third of Intrusions", "New Windows Server emergency updates fix container launch issue", and "This 'College Protester' Isn't Real. It's an AI-Powered Undercover Bot for Cops". At the bottom, there is a "Latest Ransomware Victims" table with columns for company name, ransomware type, and date.

Latest Ransomware Victims		
Red Chamber	play	2025-04-17
Koninklijke Ahold Delhaize N.V.	incransom	2025-04-17
EVERTECH INSTRUMENTAL	spacebears	2025-04-17



How I Ended Up Here

- It's complicated





TOKIO MARINE
KILN

Interesting Cases

- The Salisbury Poisonings
 - Salisbury Hospital
 - Public Health England / Porton Down
 - Police Mobile phones



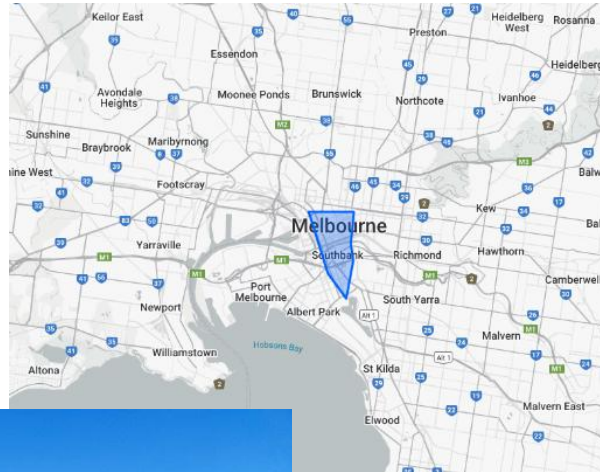
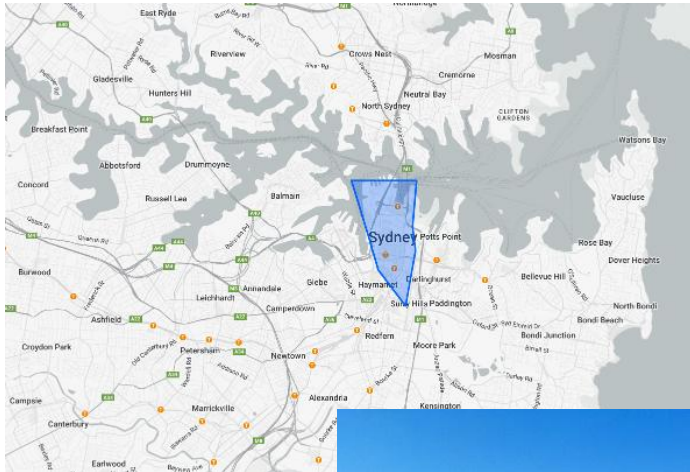
Prime Ministers Laptop

- Prime Minister Theresa May visits China in 2018



Gibraltar

- UK seizes Syria bound oil tanker off the coast of Gibraltar



TOKIO MARINE
KILN

Iran fury as Royal Marines seize tanker suspected of carrying oil to Syria

Iran summons UK ambassador over incident off Gibraltar as tensions escalate over nuclear deal



An image issued by the Ministry of Defence of the supertanker Grace 1, believed to be carrying 2m barrels of crude oil. Photograph: MoD/PA



Gibraltar



TOKIO MARINE
KILN

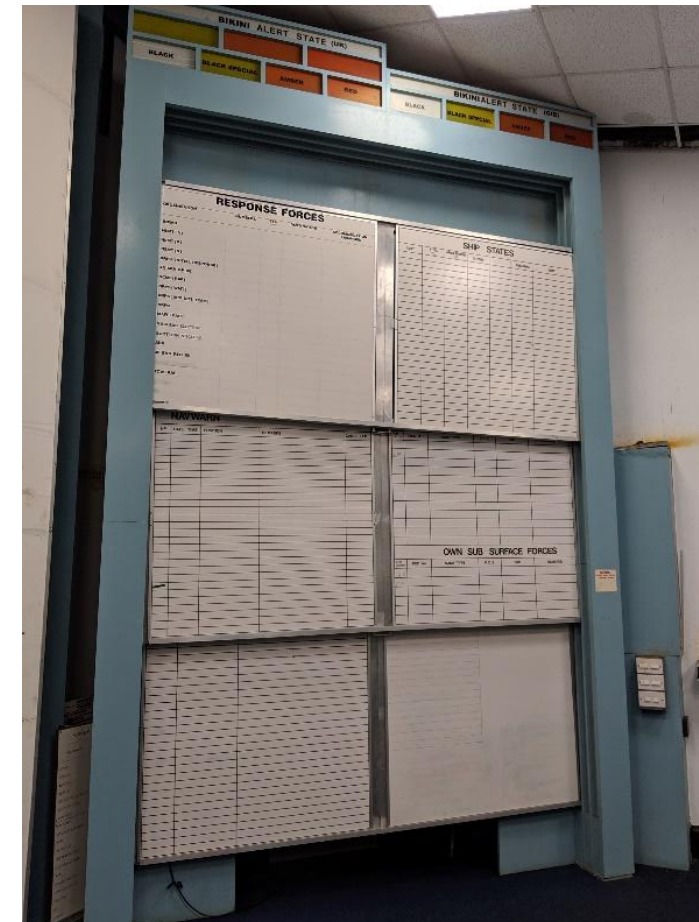
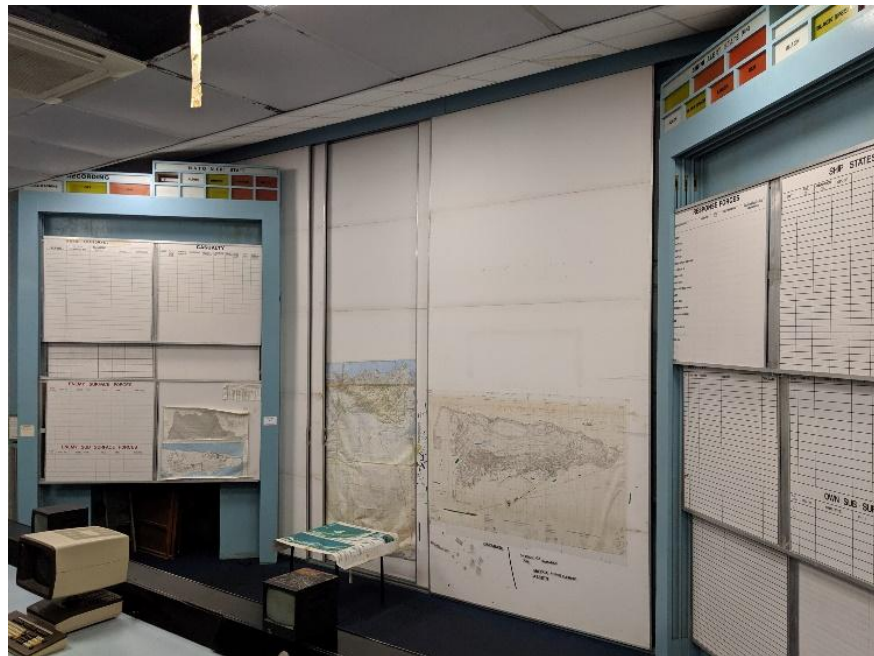




TOKIO MARINE
KILN



Gibraltar



Gibraltar





Australia 2019

- Government wide cyber attack
- 5 eyes response
- Zero Day vulnerability
- ACSC lead



Exclusive: Australia concluded China was behind hack on parliament, political parties – sources

By Colin Packham

September 16, 2019 4:50 AM GMT+1 · Updated 6 years ago

Aa



A man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration/Files [Purchase Licensing Rights](#)

What it's like working in DFIR

- Long hours
- No Weekends
- High stress
- Difficult conversations
- Often anger taken out on DFIR team
- Conflict with rebuild stream
- Costing difficult

But we love it

- The most rewarding part is the challenge



Navigating Ransomware Engagement

Decision Factors,
Negotiation Dynamics, and
Business Implications



EVAN VOUGDIS

—
Cyber Director
NSB Cyber

What we'll cover

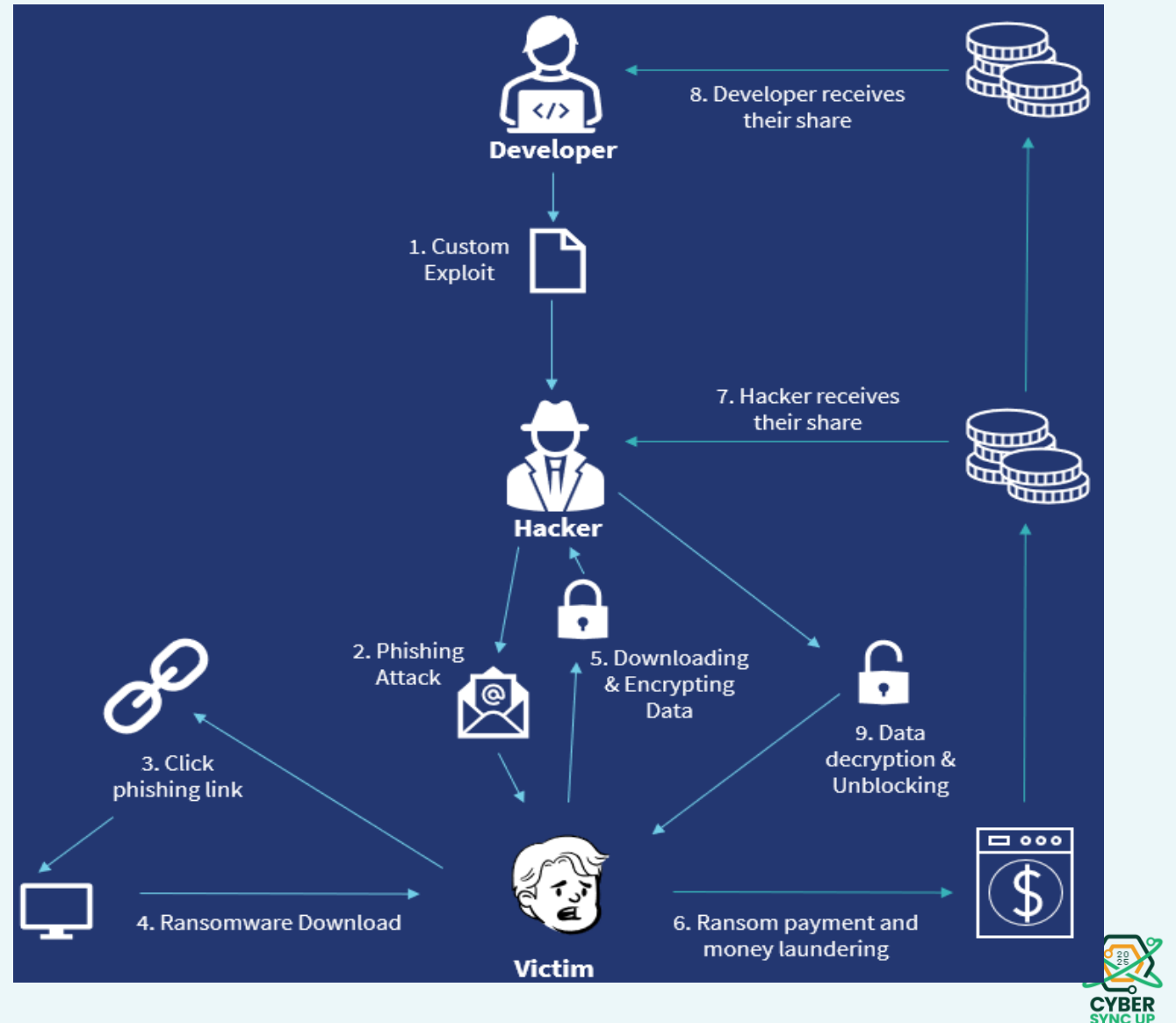
- Introduction
- Decision Factors for Engagement
- Lifecycle of a Negotiation
- Business Decisions: To Pay or Not to Pay
- What Happens When You Pay
- Key Takeaways

Introduction to Ransomware - RaaS

Ransomware is malicious software that encrypts or locks up your files and demands a ransom payment for the decryption key.

Ransomware can infect your device through various means, such as spam emails, malicious links, or unverified downloads.

Successful ransomware attacks can have devastating effects, including loss of essential data, financial damage, and reputational harm.



Introduction to Ransomware – Ransom Notes

Hi friends, ← **Friendly Greeting**

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption. ← **The "What"**

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal. ← **Want to work together**
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data. ← **Provision of Security Report**
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - <https://akirak2iz6a7qgd3ayp3l6yub7xx2uep76ldk3u2kol1pj5z3z636bad.onion>.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

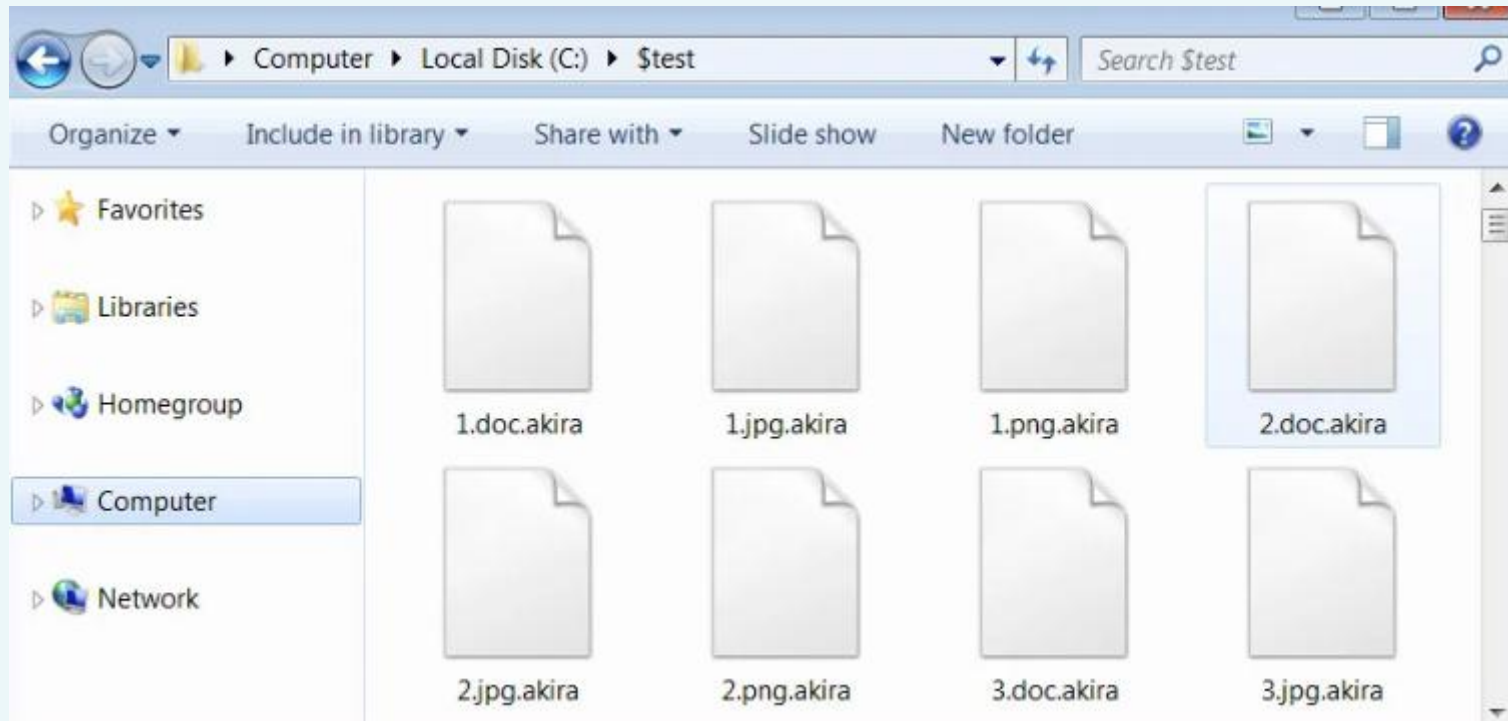
1. Install TOR Browser to get access to our chat room - <https://www.torproject.org/download/>.
2. Paste this link - <https://akirakzqxq2dsrzsrvbr2xgbbu2wgsxmryd4csgfameg52n7efvr2id.onion>
3. Use this code - `4416-PA-70MC-3RIT` - to log into our chat.

← **User-friendly Instructions**

Keep in mind that the faster you will get in touch, the less damage we cause.

Decision Factors for Engagement - Severity

1. Data Encryption Impact – Assess which systems are impacted?
2. Business Disruption – Quantify downtime costs.
3. Scope and spread – Is the Incident contained and what is the current scope of the compromise (i.e., Backup Environments).



Decision Factors for Engagement - Trust

1. Group Reputation– Who am I dealing with?
2. Deal Reliability – Are they likely going to stick to our agreed terms?
3. Risk of Deception– Is the Incident contained and what is the current scope of the compromise ie Backup Environments.

~~~ AlphaCat ~~~

>>>> Your data are stolen and encrypted

>>>> What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.  
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.

Therefore to us our reputation is very important. We attack worldwide and there is no dissatisfied victim after payment.



# Decision Factors for Engagement – Legal & Recovery

1. Jurisdictional Laws – Understand legal constraints – OFAC / Sanctions
2. Backup Viability – What is the current backup position of the victim?
3. Alternate Recovery – Explore free backup tools (i.e., No more Ransom)
4. Insurance and Counsel – What is your advice?

## NEWS

Press Releases

Statements & Remarks

Readouts

Testimonies

Featured Stories

Webcasts

Press Contacts

## PRESS RELEASES

### United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group

February 20, 2024

*The United States imposes sanctions on affiliates of group responsible for ransomware attacks on the U.S. financial sector*

WASHINGTON — Today, the United States is designating two individuals who are affiliates of the Russia-based ransomware group LockBit. This action is the first in an ongoing collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation, and our international partners targeting LockBit.

# Lifecycle of a Negotiation

The lifecycle of a ransomware negotiation begins with **establishing secure communication protocols** to safely engage with attackers, followed by an **initial response and decision-making framework** to assess demands and motivations, and progresses through **counter-offer strategies, a decision point, and exit considerations**

01

## 1. Establishing Communication Protocols

- Establishing secure communication method.
- Documenting all communications for legal, analytical, and record-keeping purposes.

02

## 2. Initial Response

- Standardised initial response to ransom demands without committing to action.
- Neutral in tone to avoid provocation or perceptions.

03

## 3. Decision Making Framework

- Understanding the motivation, financial thresholds and limits of the organisation in terms of ransom payment.

04

## 4. Counter-Offer Strategies

- Prepared guidelines for making counter-offers, if deemed necessary, which could involve negotiating a lower ransom or extended deadlines.
- Evaluate the ability to recover operations without paying the ransom.

05

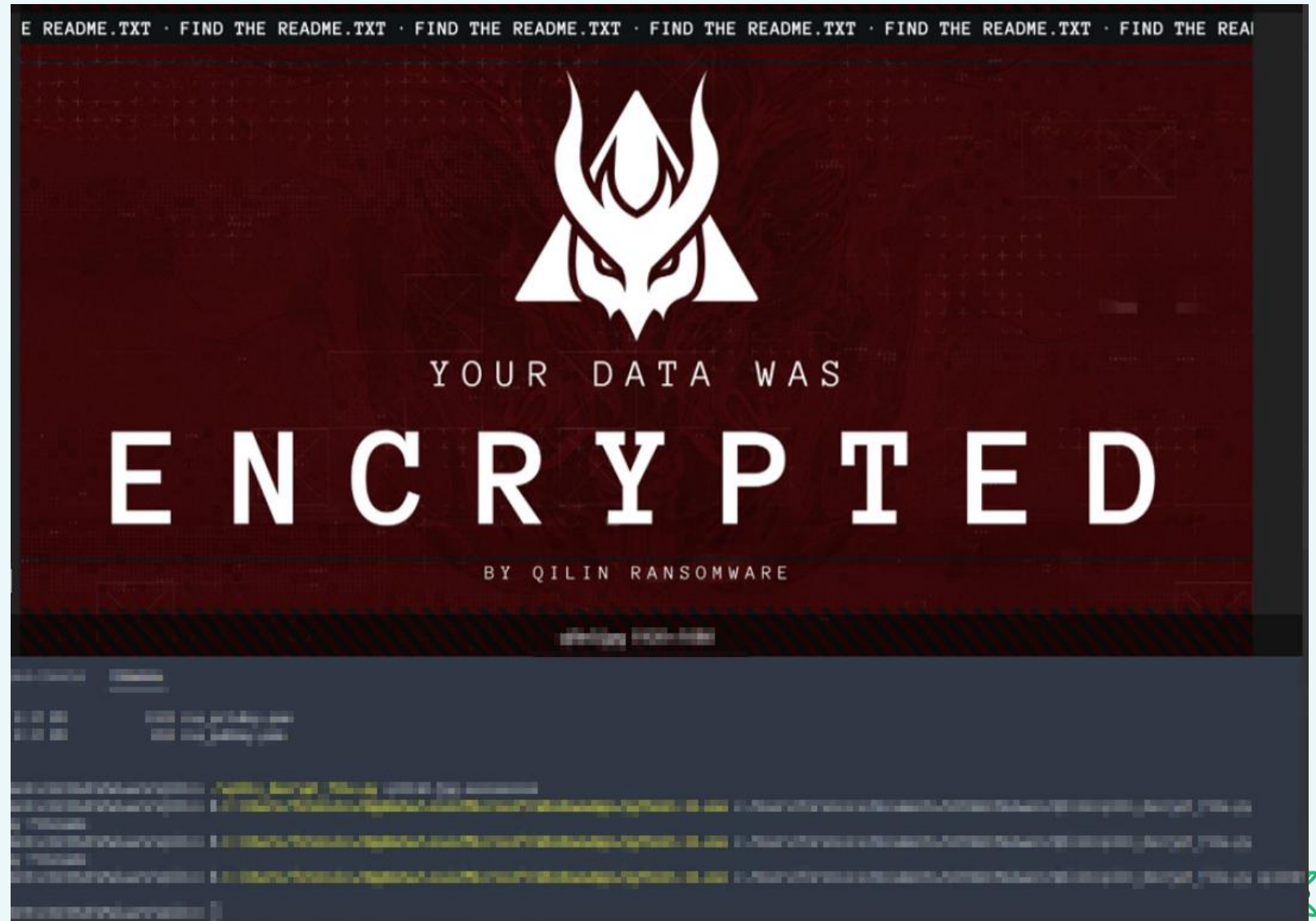
## 5. Exit Strategy Considerations

- Planning for different negotiation outcomes, including successful negotiation, failure to reach an agreement and escalation to law enforcement.



# Case Study – Qilin Ransomware Negotiation

- Qilin, emerged in 2022 as a Russian-speaking Ransomware-as-a-Service (RaaS) group.
- Qilin employs double extortion, encrypting data and exfiltrating sensitive information.
- Notable incidents include the 2024 Synnovis attack affecting NHS hospitals, up to 5.6M impacted.



# Lifecycle of a Negotiation – Initial Response T-0

\*Support 28.11.2023 8:

Hello, if you need help you can post any questions in this chat

Client-tc8Jlq8TDG 30.11.2023 7:

hello support, are you able to receive this message? ← Initial Contact - Neutral

Support 30.11.2023 7:

Yes, of course.

Client-tc8Jlq8TDG 30.11.2023 7:

ok good. we are still working through what has gone on with our environment. can you tell us what has happened?\* ← Initial Contact - Information Gathering

\*Support 30.11.2023 9:

All your systems have been encrypted Some data has also been taken from your servers.

Client-tc8Jlq8TDG 30.11.2023 22:

yes we have noticed, our server vms are currently not able to be accessed.

Client-tc8Jlq8TDG 30.11.2023 22:

our leadership team is requesting further information regarding the data taken. is there some sort of proof that can be provided for our checking ← Initial Contact - Information Gathering

\*Support 30.11.2023 22:

wait for answer

\*Support 1.12.2023 7:

we're preparing a list, and we'll send it out shortly. ← Success - Information Retrieval

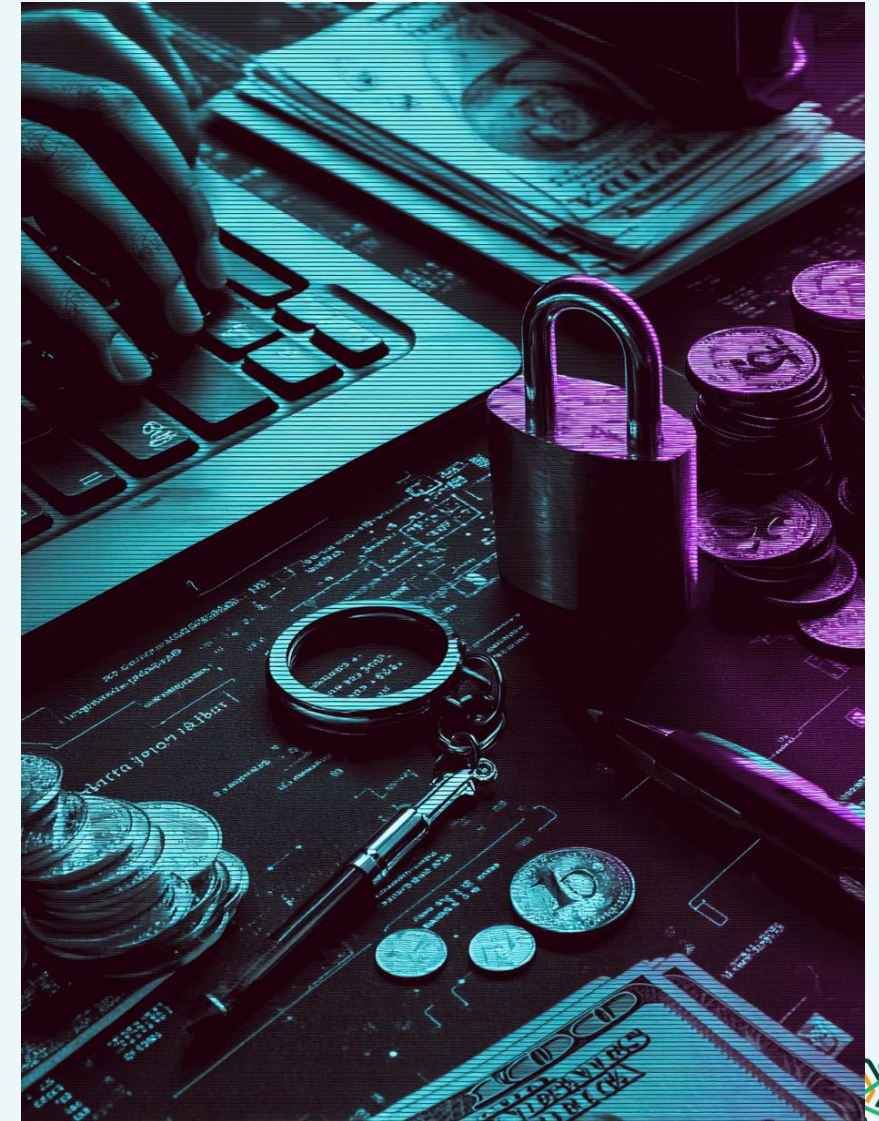
# Lifecycle of a Negotiation





# Business Decision – To Pay or not to Pay

- **Impact Assessment** – Assess short term & long-term impacts, is the situation existential? Operational? Reputational?
- **Recovery Feasibility** – Assessment on effectiveness of backups and how long it will take? Maximum downtime?
- **Legal & Sanctions Issues** – Payment to known sanctioned entities can carry significant penalties and regulatory issues. Australian government strongly discourages payment, however there is no ban in place.
- **Stakeholder Alignment** – Ensure payment aligns with business goals, financial and ethical. Important to have a Ransomware Framework for these decisions to be laid out.



# Lifecycle of a Negotiation – Decision Making (Pay)

Confirming willingness to negotiate

Client-tc8Jlq8TDG 6.12.2023 21:

Separately to the files, our leadership team is seeking to understand whether there is negotiation available on the current \$400k demand. I am sure you have researched who we are, we help financially motivated organisation.

\*Support 6.12.2023 22:

We understand what you do. You have to understand that it's just business for us. You should also understand that we have your financial documents in our hands. We know you have that money. But, of course, you can count on some discount if we solve this issue quickly. In case you can't get to the page. close TOR Browser and open it again.

Reiterating they can see financials

Client-tc8Jlq8TDG 7.12.2023 0:

Ok understand. Let me speak this through with the leadership team, as I don't have the visibility into company finances to that degree.

Client-tc8Jlq8TDG 7.12.2023 5:

Hello, a few more questions. Can you please explain the process of which the decryptor works? Is this an application that we get from you to which we run in our environment. As you know, our exsi is crippled at the moment so how would we go about decrypting the datastore if we come to an agreement.

Client-tc8Jlq8TDG 7.12.2023 5:

I also would like to put forward an offer for consideration of US\$75,000.

Initial Offer

\*Support 7.12.2023 9:

That's right, after payment, you will receive a program that you run inside your Linux servers, and it will restore everything to the state it was. You will receive detailed instructions and our support until full recovery. As for the amount - no one can give you a 75% discount, it's at least harmful to business. My boss is willing to consider a 20% discount on the original amount. As your company benefits society.

Current Bid \$75,000 | Current offer \$320,000

# Lifecycle of a Negotiation





# Lifecycle of a Negotiation – Decision Making (Pay) T-9

Client-tc8Jlq8TDG 7.12.2023 23:

Hello support, our leadership appreciates your understanding of our business and what we do, however this amount is not able to be met. I would like to provide a second offer at US\$100,000 for your consideration. Whilst a discount, we are clearly interested in coming to a commercial agreement with the team to close out this issue.

→ **Second Commercial Offer**

Support 8.12.2023 7:

I'll tell you again, we understand what your customers are doing. But that doesn't bother us. My boss immediately agreed on a good discount for you. Attention, I repeat: the amount of the buyout was taken on the basis of the company's finances. Your suggestion sounds like a joke. If I go to my boss with this offer, I'm afraid tomorrow there may be an announcement in the news that your company has been attacked and the data has been stolen. We are waiting for a normal offer. Close to the initial amount, taking into account the discount already provided. And remember that time is not in your favor. ← **Requesting Serious Offer / Continued Threats**

Support 8.12.2023 7:

Your client needs to understand in case we don't come to an agreement. In addition to permanently losing access to your data, your customer will publish blogs and dates. Call partners and investors. All of this will cost much more than the solution we are proposing. ← **Reiterating the Threat**

Client-tc8Jlq8TDG 8.12.2023 8:

Understood. I will chat to our executive team and pass on this information. We understand time is not in our favor, but we are trying to work towards a sensible outcome. We will come back to you. ← **Continued Delays**

# Lifecycle of a Negotiation



# Lifecycle of a Negotiation – Decision Making (Pay) T-11

Client-tc8Jlq8TDG 11.12.2023 0:

Hello, after working with executives over the weekend on coming to a suitable amount, we would like to put forward an offer of \$200,000US for your consideration. We want to reiterate that we appreciate the seriousness of this and that we want to come to a commercial agreement as you do.

Support 11.12.2023 1:

Hello, my boss can accept 300,000 USD. So discount for you is 100,000 USD. It's the best offer we can give.

Client-tc8Jlq8TDG 11.12.2023 4:

Our leadership has requested further information regarding what has been taken in order to make an informed decision regarding payment. Is there anything else that can be provided to us?

Support 11.12.2023 5:

We gave you test decrypted files, small part of stolen data list, and files that you chose. After payment you'll get: full list of stolen data (we'll delete it from our servers), decryptor for all your systems, and we garantee that this case stay between ourselves.

Support 11.12.2023 5:

you have about 24 hours to accept the offer

**Current Bid \$200,000 | Current Offer \$300,000**



# Lifecycle of a Negotiation – Decision Making (Pay) T-11

Client-tc8Jlq8TDG 11.12.2023 20:

hello, our leadership has met overnight and have increased their offer, **which this is their final offer, of \$250,000 US.** Whilst we very much acknowledge the seriousness of this situation, our business cannot financially support a higher payment. We have taken this commercial outcome serious from the start, and hope you can acknowledge that in your decision. **Final Offer - Additional Pressure**

Support 11.12.2023 21:

Ok. We agree. You can pay. **Commercial Agreement Acquired. 37.5% Discount on initial \$400,000**

Client-tc8Jlq8TDG 11.12.2023 21:

ok. we are working out payment now, I will keep you updated as soon as things progress. So in addition to our decryptor, we will get advice from you on how this happened? We want to ensure this does not happen again. **Requesting Report**

Support 11.12.2023 22:

Yes, you will receive information from us about the method of infiltration and some practical security tips. You can also be sure that our team's attack on your company will not happen again.

Client-tc8Jlq8TDG 11.12.2023 23:

ok thanks. **As mentioned, we are working on payment right now. Please confirm that in event we cannot pay before 8 hour deadline is up, we will be afforded another day since we have agreement?**

**Ensuring Logistics are set - Expectations Met**

Support 12.12.2023 0:



Yes, we are ready to extend the timer as an exception. **We have added 24 hours for you**

# Lifecycle of a Negotiation – Sanctions Sanity Check

13. Based on your instructions, we have conducted preliminary searches of the Consolidated List of sanctions targets maintained by Australia<sup>9</sup> and the SDN List<sup>10</sup> maintained by the US (both as defined below) for the Wallet Address as well as the following names:

- 13.1 Qilin;
- 13.2 Agenda;
- 13.3 Spider (for Scattered Spider and Wizard Spider);
- 13.4 BlackCat;
- 13.5 Gold Ulrick;
- 13.6 UNC (for UNC3364, UNC2727 and UNC3944);
- 13.7 Starfraud;
- 13.8 Scatter Swine; and
- 13.9 Muddled Libra;

**PAYMENT INFORMATION**

 bc1q332np5dt38szmjckuqv6d6khqzjnd0xv6 

[Show transactions](#)

1. Buy bitcoin.
2. Send specified amount to our bitcoin address.
3. Wait for payment confirmation in bitcoin network.
4. After 2 confirmations we will send our decryptor software. You still be able to contact us for assistance.

**OFAC**  
Office of Foreign Assets Control

**Sanctions List Search**

Sanctions List Search is a tool that allows users to search for individuals and entities on the Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

[Download the SDN List](#)[Sanctions List Search: Rules for use](#)[Visit The OFAC Website](#)

[Download the Consolidated Non-SDN List](#)[Program Code Key](#)

**Lookup**

Type:

Name:

ID # / Digital Currency Address:

Program: 

561-Related  
BALKANS  
BALKANS-EO14033

Minimum Name Score:

Address:

City:

State/Province\*:

Country:

List:

Lookup Results: 0 Found

| Name                                      | Address | Type | Program(s) | List | Score |
|-------------------------------------------|---------|------|------------|------|-------|
| Your search has not returned any results. |         |      |            |      |       |

\* U.S. states are abbreviated on the SDN and Non-SDN lists. To search for a specific U.S. state, please use the two letter U.S. Postal Service abbreviation.

SDN List last updated on: 12/11/2023 10:08:36 AM  
Non-SDN List last updated on: 11/14/2023 7:48:10 AM

# Lifecycle of a Negotiation – Decision Making (Pay) T-13

Client-tc8Jlq8TDG 12.12.2023 5:  
the money is clearing with our payment provider. As soon as it does, you will have it.

Client-tc8Jlq8TDG 13.12.2023 6:  
hello, our payment is still clearing so we will require some more time on the timer. please note this is out of our hands and the money has been transferred out from our account. We are awaiting our provider. we hope you can understand.

Support 13.12.2023 6:  
Hello. We increased the timer by 12 hours. It's enough ?

Client-tc8Jlq8TDG 13.12.2023 6:  
I am guided by our provider, I am hoping so. They have advised it could be another 24 hours. As mentioned, the money has left our account (can send proof if needed), we are awaiting our vendor.

→ **Minor Logistical Delay. Keeping Qilin Informed**

Support 13.12.2023 6:  
Timer increased. We hope this time is enough

Client-tc8Jlq8TDG 14.12.2023 6:  
Hello, I have been advised 10 minutes ago that the funds have cleared and payment will be in your wallet either this evening or tomorrow morning. Please confirm once it arrives, and I will also update if we hear back from our vendor as to which one it'll be.

Support 14.12.2023 7:  
hello, ok

Support 14.12.2023 20:  
We have already received your payment. As soon as we see 10 confirmations in the Bitcoin network, we will send you decryption software

Support 14.12.2023 21:  
aftp.com.decryptor.zip (5.826 MB) ← **Decryptor Received**

← **Payment Received**



# Lifecycle of a Negotiation

01

## 1. Establishing Communication Protocols

- Establishing secure communication method.
- Documenting all communications for legal, analytical, and record-keeping purposes.

02

## 2. Initial Response

- Standardised initial response to ransom demands without committing to action.
- Neutral in tone to avoid provocation or perceptions.

03

## 3. Decision Making Framework

- Understanding the motivation, financial thresholds and limits of the organisation in terms of ransom payment.

04

## 4. Counter-Offer Strategies

- Prepared guidelines for making counter-offers, if deemed necessary, which could involve negotiating a lower ransom or extended deadlines.
- Evaluate the ability to recover operations without paying the ransom.

05

## 5. Exit Strategy Considerations

- Planning for different negotiation outcomes, including successful negotiation, failure to reach an agreement and escalation to law enforcement.

# Lifecycle of a Negotiation – Decision Making (Pay) T-13

Support 15.12.2023 15:

I hasten to inform you that the server on which your information was stored has been completely destroyed and deleted from our data center. All the information is now yours alone. Our team got into your network through a spam attack on your employees' emails. One of them opened our attachmend and download payload to one of the computers on your network. Hold a meeting with your employees, give them online security courses, and tell them not to open attachments inside emails unless they are sure it's from a trusted person. You can rest assured that this case will only be between you and us. Good luck. Best regards. ← **Data Deleted - Initial Access Confirmed**

Client-tc8Jlq8TDG 15.12.2023 20:

hello, thank you for confirmation on both, this will help us moving forward. to ensure that we have remediated this user, are you able to advise which workstation this was on? we are also currently decrypting, whilst this seems to be working, is the technical suport available for this period just incase? ← **Attempted Information Extraction**

Support 17.12.2023 0:

I don't have info about name of workstation. Technical support is online, you can write this chat if you'll need.

Support 17.12.2023 7:

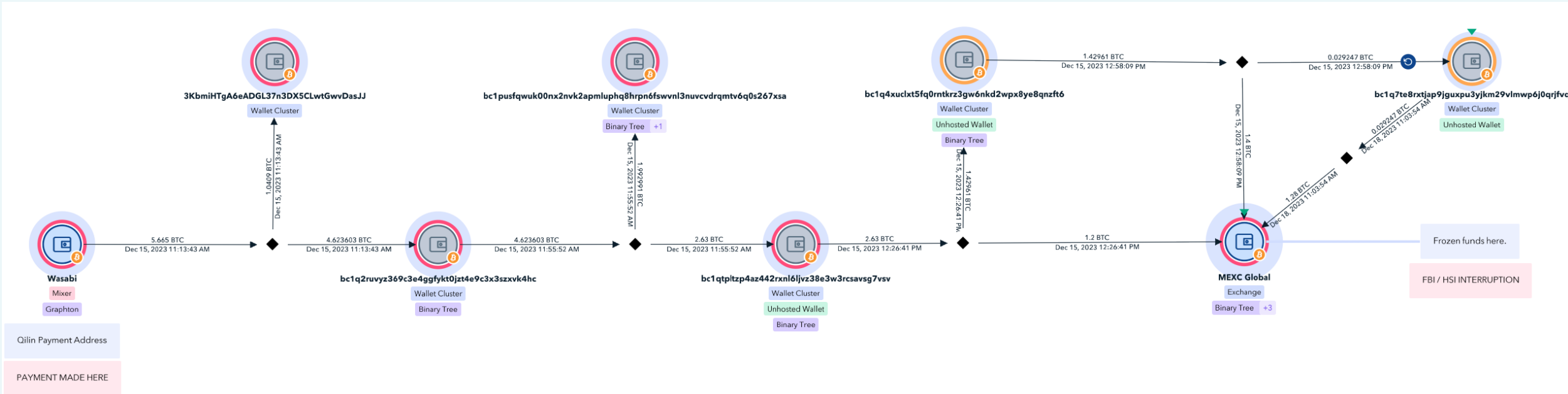
We can't tell you the date and the person who received our email, so we'll compromise our attack vector and our payload.

This will be useful for Internet security specialists and will harm our further work. ← **Didn't Provide the Information**

Client-tc8Jlq8TDG 19.12.2023 0:

ok no worries. We are still decrypting, so we will keep this chat open for the moment. ← **Soft Exit. Leave Door Ajar**

# Lifecycle of a Negotiation – Post-Payment T-15



Exchange DEX+ Buy Crypto Markets Spot Futures Rewards Hub Events 100% More Celebra7e

## YOUR EASIEST WAY TO CRYPTO

At MEXC, we believe in making crypto simple and accessible for everyone. Since 2018, our ultra-fast trading engine and a broad selection of tokens have empowered millions to explore the world of digital assets. As pioneers in financial services and blockchain technology, we are committed to simplifying crypto trading and unlocking its boundless possibilities.

# Key Takeaways

---

1. Engagements are unique, dynamic, and rely on organisational factors/dependencies + threat actors' behaviours
2. Threat actor will directly engage and attempt to get the most favorable payout.
3. Ransomware impacts a plurality of business operations and logistic. Cost can grow exponentially.
4. The decision to pay relies on factors such as the threat actor, the intent, the extent of damages, the timeframe and the financial ability of the organisation.
  - The incident does not stop with the payment of ransom
5. Legal issues may prevent an organisation from making payment and/or engaging with a threat actor.





# The Shifting Legal Landscape

Recent cases and updates



ANDREW MIERS

—  
Partner  
HWL Ebsworth Lawyers



COLIN PAUSEY

—  
Chief Operating Officer  
Emergence Insurance



# Dispatches from the Frontline



ZOE TISHLER

Special Counsel  
HWL Ebsworth Lawyers



SHANE BELL

Co-Founder and CEO  
NSB Cyber



LUKE FARDELL

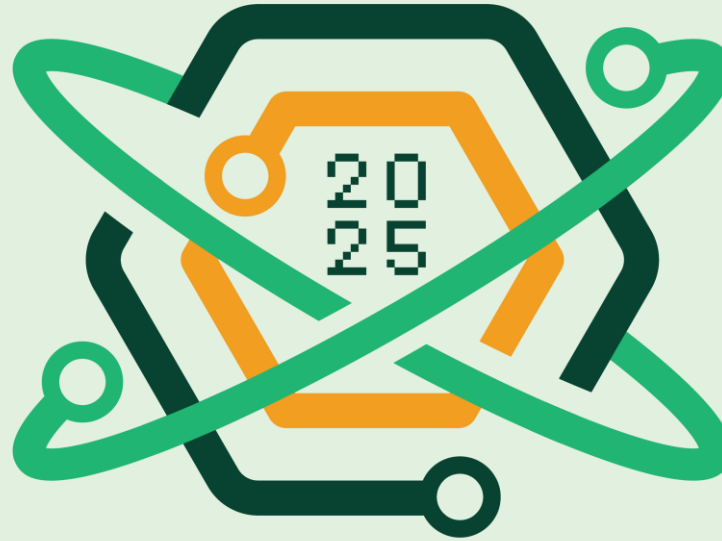
Lead Cyber Analyst  
Tokio Marine Kiln



PETER FURST

Head of Incident Response  
Emergence Insurance

THANK YOU



# CYBER SYNC UP

COMBATting CYBER CRIME