SOCRadar®
Your Eyes Beyond

Whitepaper

Shaking Hands with Clenched Fists

A 100M+ USD Negotiator's Guide to Surviving Ransomware

socradar.io

Ransomware attacks present a paradoxical challenge, akin to the complexity captured by Mahatma Gandhi's metaphor of "shaking hands with clenched fists." On one hand, organizations must be prepared to engage with attackers in a delicate dance of negotiation, seeking resolution and the restoration of their systems. On the other hand, they must remain resolute, guarding against capitulation and the potential encouragement of future attacks.

As a seasoned negotiator with a history of leading negotiations in high-stakes ransomware incidents, amassing a cumulative experience with cases totaling around 100 Million USD, I bring a wealth of real-world insights to this intricate dilemma.

This whitepaper aims to unravel the complexities of deciding whether to pay a ransom, delve into the motivations behind ransomware attacks, and provide strategies for effective negotiation, all while navigating the treacherous terrain that these cyber threats present.

Huzeyfe Onal, CEO of SOCRadar

Quick view: Where we are, how we got to this point

Pay or Not to Pay? The Quintessential Dilemma

In May 2021, Colonial Pipeline, a major U.S. fuel pipeline operator, faced a ransomware attack that disrupted fuel distribution across the East Coast. The company chose to pay a ransom of 75 Bitcoins (around $4.4 million at the time) to regain access to their systems. This situation underscores the tough choices companies face when critical infrastructure is at stake, though paying the ransom contradicts the FBI’s general advice against making payments to cybercriminals.

Shakespeare, created by Bing Image Creator

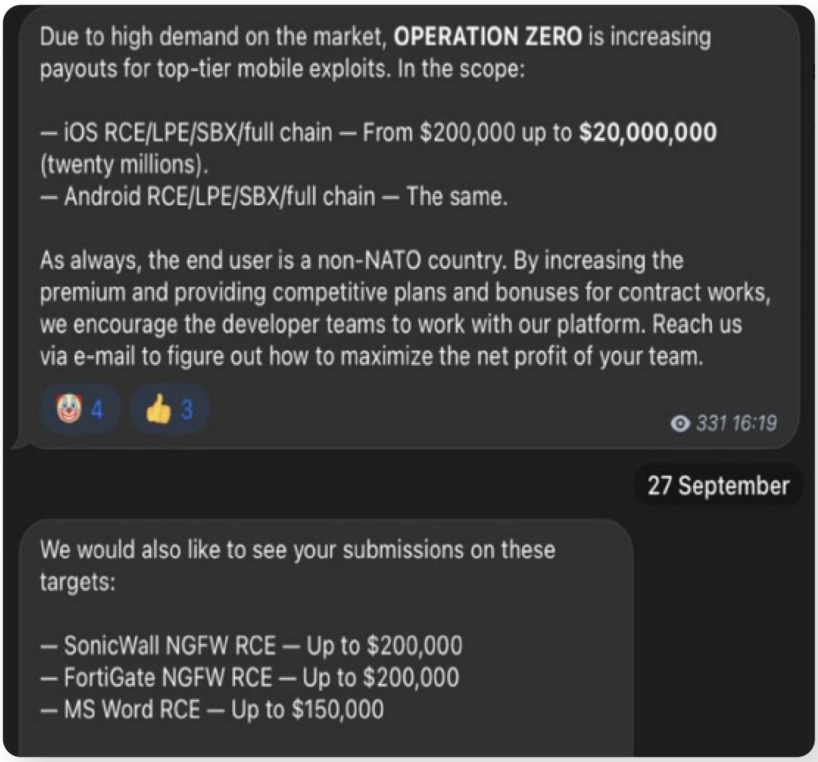
Furthermore, the U.S. Treasury's Office of Foreign Assets Control (OFAC) warns that paying ransoms to entities on its sanctions list can result in hefty fines, adding a legal risk to the equation. Drawing from my extensive experience as a negotiator, I understand the gravity of such situations and the pressure to make the right decision swiftly.

Victims of cyberattacks often explore legitimate options for data recovery before considering contacting cybercriminals. Paying a ransom is typically a last resort due to both legal concerns and the substantial financial burden it represents. However, a recent report from South Korean media has revealed a disturbing case where a purportedly legitimate data recovery company was found to be colluding with North Korean threat actors, specifically the Lazarus Group, while claiming to recover data. This company used Google Ads to present itself as a trustworthy data recovery service, concealing its affiliation with a notorious cyber group. The Lazarus Group is not only renowned for its advanced hacking techniques but also for its clever recruitment methods, such as posting job advertisements to entice potential candidates with knowledge or experience in targeted industries or organizations. Following a police operation targeting the alleged company, incriminating messages exchanged via Telegram between the company and the Lazarus Group were seized.

Last but not least, in 2021, the Biden administration inaugurated an annual worldwide summit with the primary objective of addressing cybersecurity issues. This summit initially comprised 31 nations but has since grown to encompass over 45 member countries. One noteworthy development in the present year is the launch of the anti-ransomware initiative, in which global leaders and the White House have collectively committed to rejecting ransom payments. This action is perceived as a daring move to deter cybercriminals and diminish the financial gains from such attacks. However, its effectiveness and the fulfillment of the commitments, as well as the success of the agreed-upon strategies, will become evident as time progresses.

Ransomware as a Business: Understanding the Allure of Ransomware

The WannaCry ransomware attack in May 2017 stands as a stark reminder of the pervasive and destructive nature of this form of cybercrime, affecting over 200,000 computers across 150 countries and causing havoc in various sectors. The estimated damages from this single incident range dramatically, with figures spanning from hundreds of millions to even billions of dollars. This unprecedented attack not only showcased the sheer scale at which ransomware could operate but also highlighted its immensely lucrative potential for attackers.



Due to high demand on the market, **OPERATION ZERO** is increasing payouts for top-tier mobile exploits. In the scope:

— iOS RCE/LPE/SBX/full chain — From $200,000 up to **$20,000,000** (twenty millions).
— Android RCE/LPE/SBX/full chain — The same.

As always, the end user is a non-NATO country. By increasing the premium and providing competitive plans and bonuses for contract works, we encourage the developer teams to work with our platform. Reach us via e-mail to figure out how to maximize the net profit of your team.

🤡 4 👍 3 331 16:19

27 September

We would also like to see your submissions on these targets:

— SonicWall NGFW RCE — Up to $200,000
— FortiGate NGFW RCE — Up to $200,000
— MS Word RCE — Up to $150,000

As we delve into the world of startups, we often hear the term 'market fit product.' This concept revolves around finding the perfect equilibrium where a product meets the specific needs and demands of a market, resulting in rapid growth and substantial financial success. Ransomware, in an unfortunate sense, has achieved a similar kind of 'market fit.' Cybercriminals have recognized that organizations of all sizes and across all industries are reliant on digital infrastructures, making them potential targets. The blend of widespread vulnerability and the willingness of victims to pay ransoms has created a thriving market for ransomware.

The lucrativeness of ransomware stems from several factors. Firstly, many organizations are still playing catch-up when it comes to cybersecurity, resulting in outdated systems and unpatched vulnerabilities that are easy targets for attackers. Secondly, the anonymizing capabilities of cryptocurrencies have provided a secure method for attackers to receive payments, further incentivizing this criminal activity. Thirdly, the low barrier to entry, with ransomware-as-a-service platforms available, allows even less technically skilled individuals to partake in ransomware campaigns. All these factors combine to create a 'perfect storm,' making ransomware a highly profitable venture for cybercriminals.

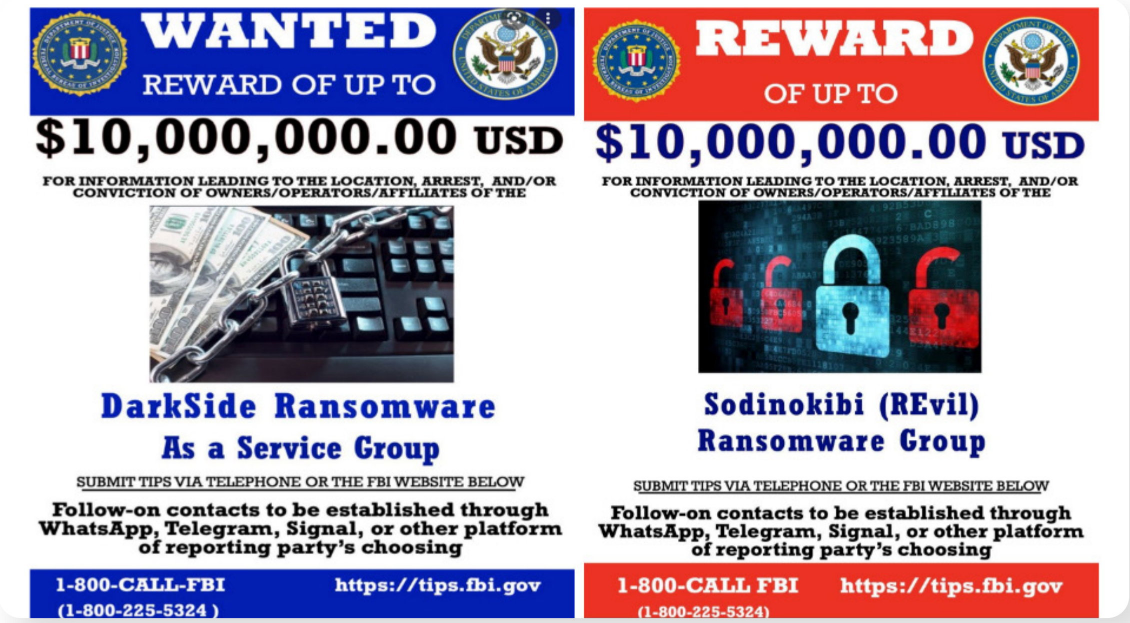
My experience as a negotiator, dealing with over 100 million USD worth of ransomware incidents, has underscored the importance of understanding the attacker’s mindset. Realizing that we are dealing with highly organized and profit-motivated entities helps in formulating a more effective and strategic response. It becomes paramount to approach negotiations with a deep understanding of the ransomware 'market' and the driving forces behind it, ensuring that victims are not just seen as targets, but as part of a larger economic model that we are actively working to dismantle.

The Financial Windfall of Ransomware

The attackers behind the NotPetya ransomware attack in June 2017 caused over $10 billion in damages worldwide, affecting major corporations like Maersk and Merck.

Although the ransomware's main purpose seemed to be disruption rather than financial gain, it showcased the potential for massive financial fallout from such attacks. In my role as a negotiator, I've seen firsthand the financial turmoil these attacks can create, emphasizing the importance of preparedness and swift action.

WANTED: The FBI's Bounty on Ransomware Operators



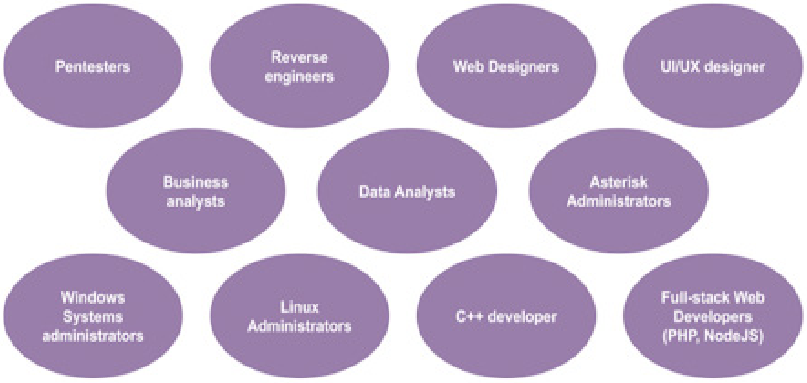
WANTED
REWARD OF UP TO
$10,000,000.00 USD
FOR INFORMATION LEADING TO THE LOCATION, ARREST, AND/OR CONVICTION OF OWNERS/OPERATORS/AFFILIATES OF THE
DarkSide Ransomware
As a Service Group
SUBMIT TIPS VIA TELEPHONE OR THE FBI WEBSITE BELOW
Follow-on contacts to be established through WhatsApp, Telegram, Signal, or other platform of reporting party's choosing
1-800-CALL-FBI (1-800-225-5324) https://tips.fbi.gov

REWARD
OF UP TO
$10,000,000.00 USD
FOR INFORMATION LEADING TO THE LOCATION, ARREST, AND/OR CONVICTION OF OWNERS/OPERATORS/AFFILIATES OF THE
Sodinokibi (REvil)
Ransomware Group
SUBMIT TIPS VIA TELEPHONE OR THE FBI WEBSITE BELOW
Follow-on contacts to be established through WhatsApp, Telegram, Signal, or other platform of reporting party's choosing
1-800-CALL FBI (1-800-225-5324) https://tips.fbi.gov

In 2020, the U.S. Department of Justice announced charges against two individuals believed to be part of a ransomware group responsible for distributing the Dridex malware and BitPaymer ransomware. The FBI also offered a reward of up to $5 million for information leading to the arrest and conviction of the group's members, demonstrating the government's commitment to combating this threat. Engaging in ransomware negotiations requires an acute awareness of the legal landscape and potential collaborations with law enforcement, areas in which my extensive experience proves invaluable.

EvilCorp on The Stage: The Professional Team Behind Ransomware

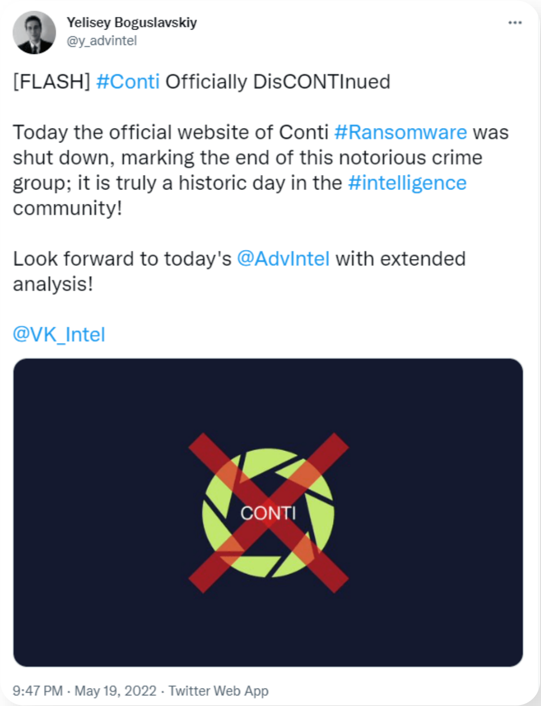
To grasp the true nature of our adversaries and anticipate their future moves, it's imperative that we delve into the inner workings of a professional ransomware group.



The data presented on the image originates from the Conti group, which found itself compromised two years ago amidst the onset of the Russia-Ukraine conflict, leading to the public exposure of their intricate operations.

Boguslavsky's tweet that Conti has ceased operations.

As is evident from the information at hand, this group operates with a level of professionalism akin to a corporate entity, boasting a diverse array of roles and responsibilities. Two particular departments warrant special attention: the Business Analyst and Data Analyst teams. These are the masterminds determining the potential ransom amount that could be extracted from each targeted company.



Yelisey Boguslavskiy
@y_advintel

[FLASH] #Conti Officially DisCONTInued

Today the official website of Conti #Ransomware was shut down, marking the end of this notorious crime group; it is truly a historic day in the #intelligence community!

Look forward to today's @AdvIntel with extended analysis!

@VK_Intel

9:47 PM · May 19, 2022 · Twitter Web App

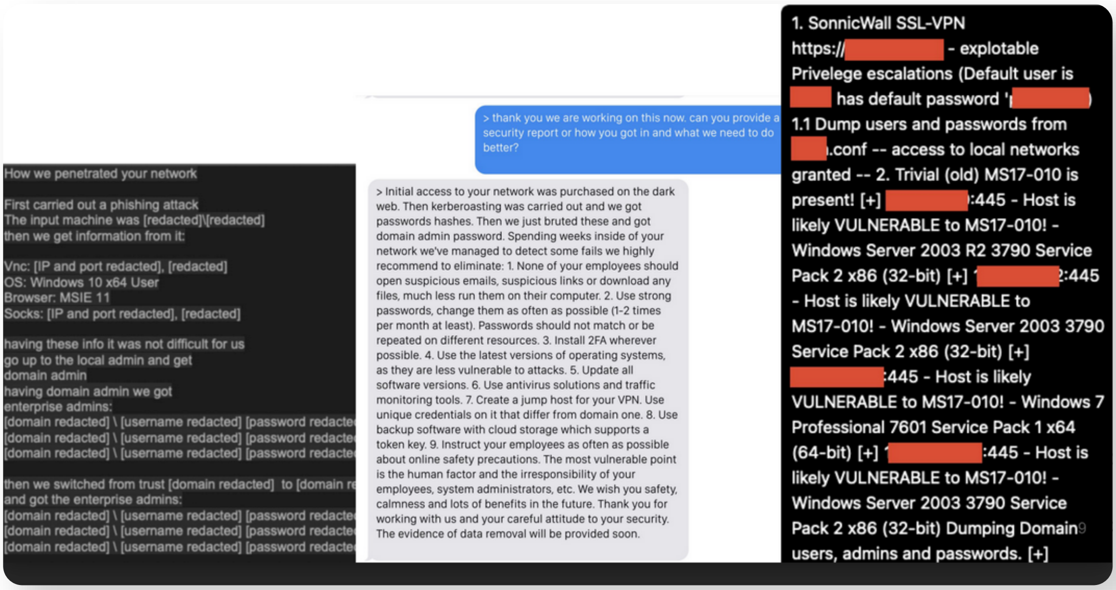
Boguslavsky's tweet that Conti has ceased operations.

These individuals possess an in-depth understanding of popular software and systems such as SAP, CRM, and ERP. Their expertise allows them to accurately gauge your financial standing, pinpointing where your funds are and just how much you can afford to pay.

Importantly, during negotiations, any attempt to plead financial instability or low profitability is bound to fall on deaf ears. They have done their homework, and they know your financial landscape better than you might believe. So, it's crucial to approach these negotiations with a strategy that goes beyond simply pleading financial incapacity.

Understanding the Attack Vector and Developing a Strategy

Ransomware often spreads via phishing emails or exploiting known software vulnerabilities. For instance, the WannaCry attack exploited a vulnerability in Microsoft Windows.



```
How we penetrated your network

First carried out a phishing attack
The input machine was [redacted]\[redacted]
then we get information from it:

Vnc: [IP and port redacted], [redacted]
OS: Windows 10 x64 User
Browser: MSIE 11
Socks: [IP and port redacted], [redacted]

having these info it was not difficult for us
go up to the local admin and get
domain admin
having domain admin we got
enterprise admins:
[domain redacted] \ [username redacted] [password redacte
[domain redacted] \ [username redacted] [password redacte
[domain redacted] \ [username redacted] [password redacte

then we switched from trust [domain redacted]  to [domain re
and got the enterprise admins:
[domain redacted] \ [username redacted] [password redacte
[domain redacted] \ [username redacted] [password redacte
[domain redacted] \ [username redacted] [password redacte
```

> thank you we are working on this now. can you provide a security report or how you got in and what we need to do better?

> Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security. The evidence of data removal will be provided soon.

1. SonnicWall SSL-VPN https://[redacted] - explotable Privelege escalations (Default user is [redacted] has default password '[redacted]) 1.1 Dump users and passwords from [redacted].conf -- access to local networks granted -- 2. Trivial (old) MS17-010 is present! [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2 x86 (32-bit) [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit) [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit) [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit) Dumping Domain users, admins and passwords. [+]

Understanding these common attack vectors is crucial for prevention, and developing a robust negotiation strategy can help mitigate the impact of an attack when prevention fails. My experience as a negotiator has taught me the importance of a proactive approach, emphasizing prevention, preparedness, and a well-thought-out response plan.

The Art of Negotiation and Ensuring Data Safety

In his renowned work "The Art of War," Sun Tzu emphasizes that the most significant triumph is one that can be attained without actual combat. When faced with conflict, it is wiser to possess the skills to negotiate and bring about resolution with minimal damage.

During the 2019 ransomware attack on the city of Riviera Beach, Florida, the city decided to pay the $600,000 ransom to regain access to their encrypted files. This decision came after careful consideration and negotiation with the attackers. Ensuring the safe return of their data and the restoration of city services was paramount, showcasing the importance of a balanced and thoughtful negotiation strategy. My role in various negotiations has honed my ability to navigate these tense situations, striking a balance between standing firm and making strategic concessions when necessary.

Sun Tzu, author of the famous book, The Art of War. Illustrated by Dall-E

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 1: You'll Never Walk Alone

Upon identifying a ransomware attack, it is important to acknowledge the situation's severity and understand that you are dealing with highly professional cybercriminals. Any attempts to resolve the issue on your own could potentially lead to further complications, underscoring the importance of not trying to play the hero in these scenarios. Instead, prioritize establishing a crisis management team comprising members from various departments, including IT, legal, and communications. This team will serve as your incident command center, steering all decision-making and actions. If your organization has yet to develop a comprehensive incident response playbook, now is the time to open it and meticulously follow the procedures outlined within.

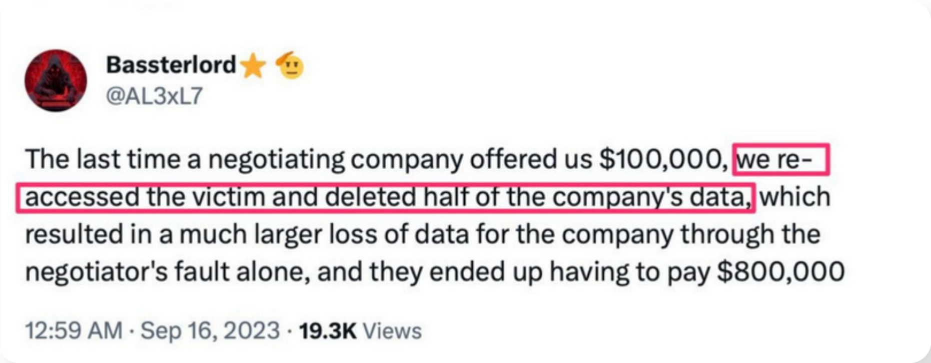
This step is crucial as a common pitfall in business continuity and disaster recovery is the lack of a well-prepared and rehearsed response plan, which can lead to delayed actions and increased damages.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 2 : Sit back, fasten your seat belts and be sure about that you are safe

In the immediate aftermath of a ransomware attack, it's crucial to ascertain whether the attackers still have active access to your systems. This step is paramount, as any ongoing access could lead to further exploitation and compromise of sensitive data.

To determine this, employ the assistance of cybersecurity professionals who can conduct a thorough analysis of your network, identify any malicious activities, and isolate compromised systems to prevent further damage.



Bassterlord⭐
@AL3xL7

The last time a negotiating company offered us $100,000, we re-accessed the victim and deleted half of the company's data, which resulted in a much larger loss of data for the company through the negotiator's fault alone, and they ended up having to pay $800,000

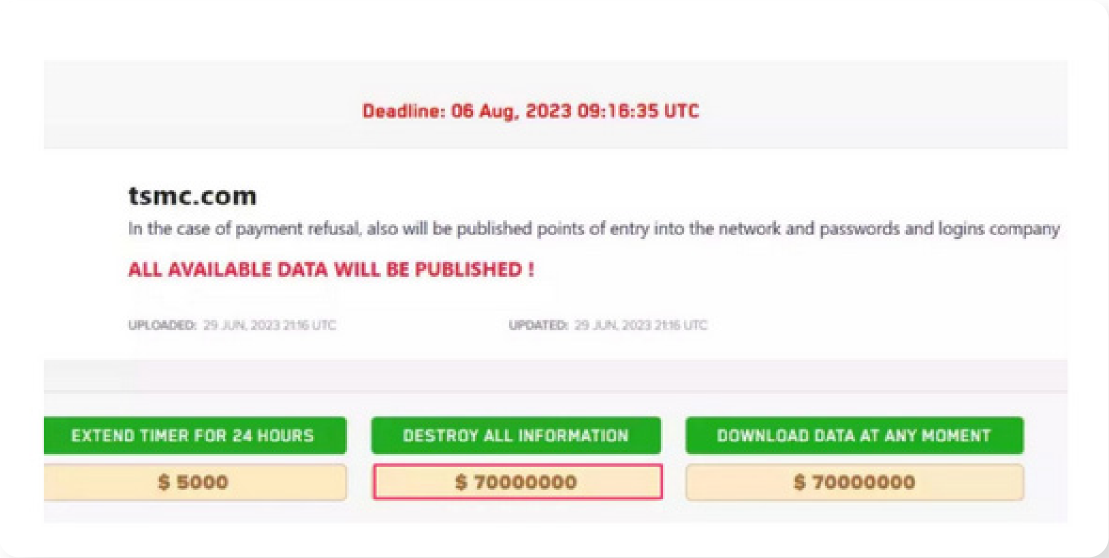
12:59 AM · Sep 16, 2023 · **19.3K** Views

During this critical period, it is vital to be wary of the channels you use for communication. Be aware that attackers could potentially have access to your internal communication tools, such as Slack or email, and might be monitoring your conversations. This represents a significant pitfall, as it can compromise your negotiation stance and strategy, making it imperative to switch to secure and encrypted modes of communication immediately.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 3 : Wheelin', Dealin', and Keepin' it Real: Mastering the Art of Ransomware Negotiation

Welcome to the big leagues of ransomware negotiation, where strategy is king, and keeping your cool is the name of the game. Think of this as a high-stakes poker match, and you're holding the cards to your company's digital kingdom. Before diving in, set your limits clear and firm. Know your breaking point and decide on the maximum ransom you’re willing to consider, but remember, showing your hand too early is a rookie mistake.



Deadline: 06 Aug, 2023 09:16:35 UTC

tsmc.com

In the case of payment refusal, also will be published points of entry into the network and passwords and logins company

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 29 JUN, 2023 21:16 UTC

UPDATED: 29 JUN, 2023 21:16 UTC

Start the conversation focused on the data and other non-monetary topics; make them sweat a little, wondering where this is all headed. Play the ‘helpless negotiator’ card, talking up your need to convince the higher-ups, and question them on the implications if the funds don't come through.

Remember, they’re not in this to lose; they’re in it for the payout. So, make it clear: walking away empty-handed isn't an option for them, and you're not an easy target. Time to negotiate like the digital world is watching, because, in this game, it's not just about getting your data back—it's about winning.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 4 : Don't Flash Your Executive Badge

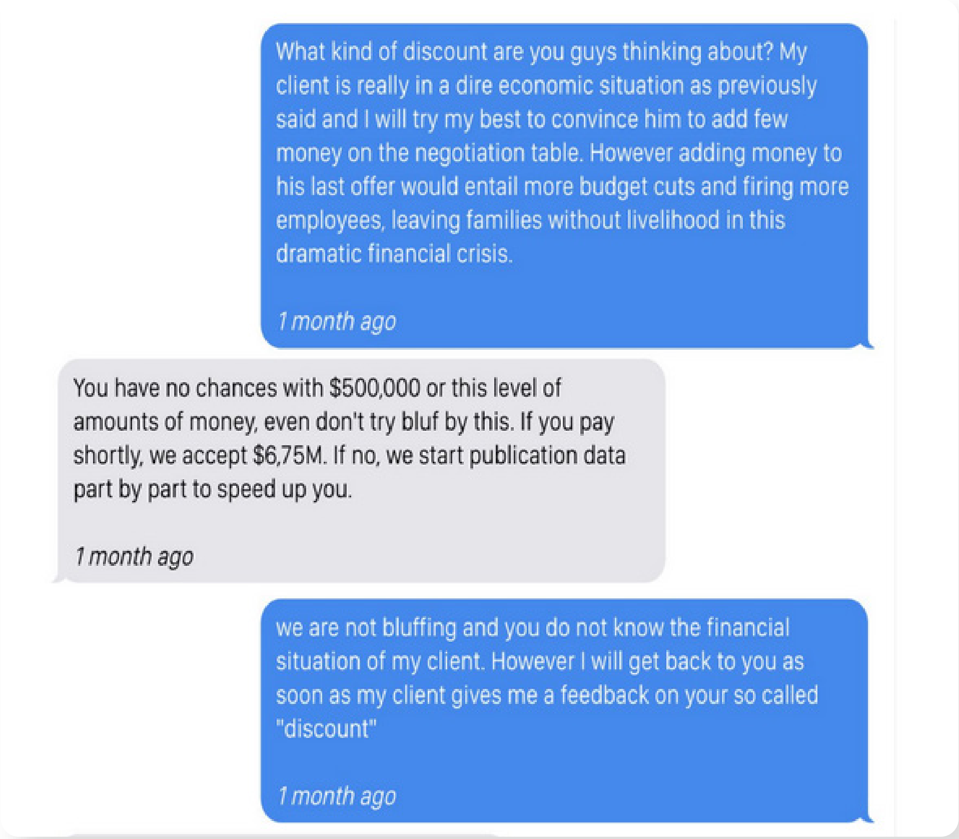
Ransomware negotiations are a bit like a spy movie - the less your adversary knows about your true identity and power, the better your chances of success. One of the cardinal sins in this high-stakes game is presenting yourself as a high-ranking company executive. It's like walking into a poker game and announcing you're holding all the aces - it just doesn't end well.

I've seen it firsthand; a CEO stepped into the negotiation ring, and it was nothing short of a disaster, leaving me to pick up the pieces and scramble to regain the upper hand. Our secret weapon? The 'going to top management' trick - it buys time and adds an extra layer of strategy to the game. So, put on your best IT employee or mid-level manager disguise. It's time to blend in, negotiate hard, and keep them guessing about who really holds the power. Because in this game of digital cat and mouse, being the undercover negotiator isn't just smart—it's essential.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 5 : Cut the Drama: Why Classical Excuses Won't Save You in Ransomware Negotiations

Ransomware negotiations are no place for a sob story—save the drama for your mama! Excuses like sick relatives and economic hardship might tug at heartstrings in other scenarios, but in the ransomware ring, they fall on deaf ears. The threat actors have heard it all before, hundreds of times, and they're not buying what you're selling.



What kind of discount are you guys thinking about? My client is really in a dire economic situation as previously said and I will try my best to convince him to add few money on the negotiation table. However adding money to his last offer would entail more budget cuts and firing more employees, leaving families without livelihood in this dramatic financial crisis.

1 month ago

You have no chances with $500,000 or this level of amounts of money, even don't try bluf by this. If you pay shortly, we accept $6,75M. If no, we start publication data part by part to speed up you.

1 month ago

we are not bluffing and you do not know the financial situation of my client. However I will get back to you as soon as my client gives me a feedback on your so called "discount"

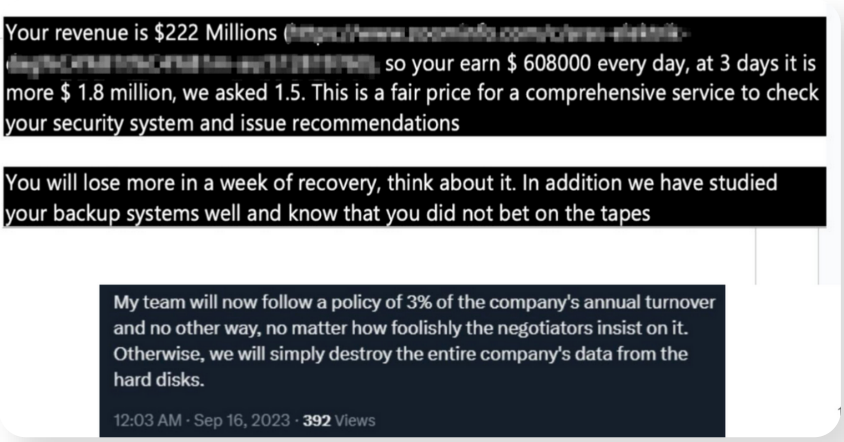
1 month ago

These digital bandits come prepared, doing their homework and crafting their demands with precision. So, bringing a script of classical excuses to the table? That's just a one-way ticket to nowhere-ville. It's time to get real, be honest, and play it straight. Remember, in the world of ransomware, time is money, and the last thing you want is to waste either of them on tales that won't win any sympathy points. So, drop the act, get down to business, and let's negotiate like the pros we are!

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 6 : Understand the 'Why' Behind Ransom Demands

In the high-stakes game of ransomware negotiation, understanding the 'why' behind the ransom demand is just as crucial as the 'how much'. Ransomware groups tend to pull numbers out of thin air, often demanding anywhere from 1–4% of a company's annual revenue. But wait, where did they get that number, and why should you just take their word for it?



Your revenue is $222 Millions ([redacted]) so your earn $ 608000 every day, at 3 days it is more $ 1.8 million, we asked 1.5. This is a fair price for a comprehensive service to check your security system and issue recommendations

You will lose more in a week of recovery, think about it. In addition we have studied your backup systems well and know that you did not bet on the tapes

My team will now follow a policy of 3% of the company's annual turnover and no other way, no matter how foolishly the negotiators insist on it. Otherwise, we will simply destroy the entire company's data from the hard disks.

12:03 AM · Sep 16, 2023 · 392 Views

Here's a pro tip straight from the negotiator's handbook: always, and I mean always, ask them to break it down for you. Why that specific amount? What's the logic behind the price tag? It's like haggling at a flea market; you wouldn't pay full price without a little back-and-forth, would you?

Flip the script and throw a curveball by suggesting a counter-offer based on annual profit, not revenue. It's like negotiating the price of a used car based on how much joy it brought its previous owner—it just makes more sense! So, put on your negotiation hat, ask the tough questions, and let's make sure that ransom demand is justified! Remember, in the world of ransomware, knowledge is power, and understanding the 'why' is your secret weapon.

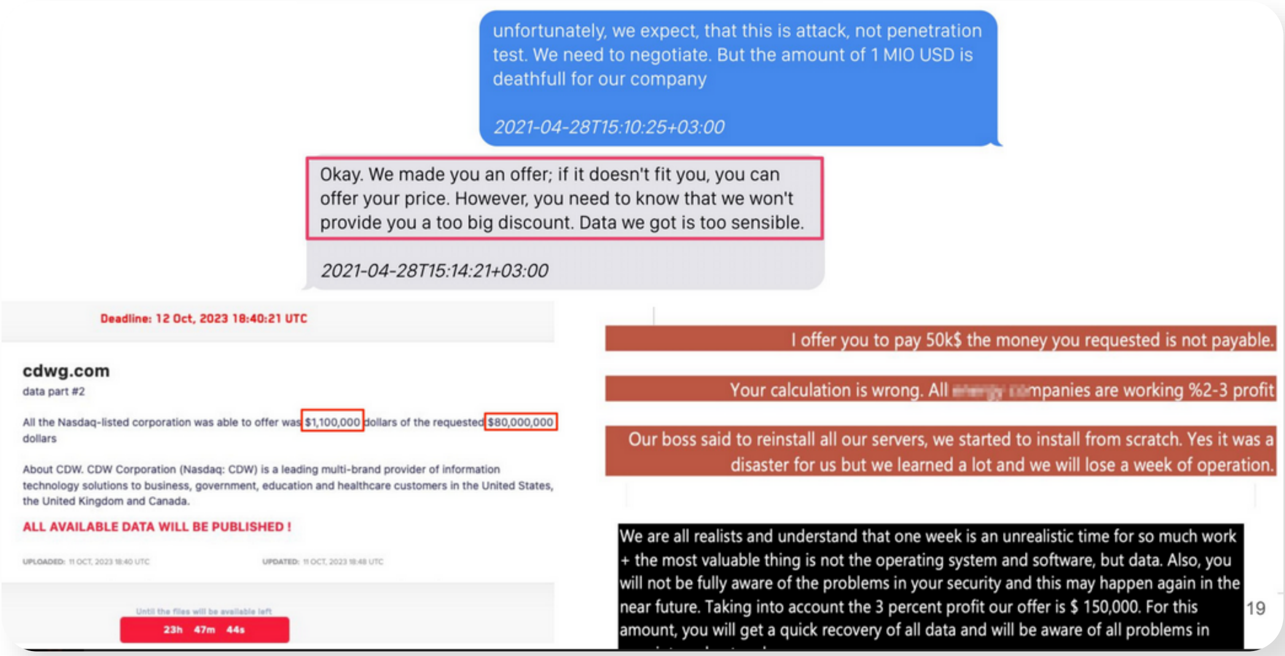
LockBit is currently considering implementing rules to ensure a minimum ransom payment, setting a standard at 3% of a victim company's annual revenue. While this ensures a lucrative return proportional to the victim's financial standing, affiliates are given leeway to offer up to a 50% discount, potentially lowering the demand to 1.5% of the annual revenue. However, to maintain a balance between flexibility and profit, LockBit is also contemplating capping the discount percentage at 50% of the initial ransom amount.

Furthermore, LockBit is looking to exploit information regarding the victim's ransomware insurance policy, potentially requiring the ransom payment not to fall below the maximum coverage of the victim's insurance. Alternatively, they are exploring setting a rule that mandates a minimum payment of 50% of the victim's ransomware insurance coverage. These strategies highlight LockBit's intention to ensure substantial payouts while strategically navigating the financial capacities and protections of their victims. Understanding these tactics is vital for negotiators, as it emphasizes the need for thorough preparation and strategic acumen in dealing with such calculated and complex cyber threats.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 7 : The Art of LAP (Logical, Acceptable, and Plausible)

When you find yourself in the midst of a ransomware negotiation, remember that making an offer is more than just throwing numbers around—it's a strategic move that requires careful consideration. Your offer should not only be reasonable but also LAP: Logical, Acceptable, and Plausible. This means presenting a counter-offer that makes sense given the context of the situation, is fair considering the impact of the attack, and is believable to ensure credibility in the eyes of the ransomware group.



unfortunately, we expect, that this is attack, not penetration test. We need to negotiate. But the amount of 1 MIO USD is deathfull for our company

2021-04-28T15:10:25+03:00

Okay. We made you an offer; if it doesn't fit you, you can offer your price. However, you need to know that we won't provide you a too big discount. Data we got is too sensible.

2021-04-28T15:14:21+03:00

Deadline: 12 Oct, 2023 18:40:21 UTC

cdwg.com

data part #2

All the Nasdaq-listed corporation was able to offer was $1,100,000 dollars of the requested $80,000,000 dollars

About CDW. CDW Corporation (Nasdaq: CDW) is a leading multi-brand provider of information technology solutions to business, government, education and healthcare customers in the United States, the United Kingdom and Canada.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 11 OCT, 2023 18:40 UTC

UPDATED: 11 OCT, 2023 18:48 UTC

Until the files will be available left

23h 47m 44s

I offer you to pay 50k$ the money you requested is not payable.

Your calculation is wrong. All [redacted]mpanies are working %2-3 profit

Our boss said to reinstall all our servers, we started to install from scratch. Yes it was a disaster for us but we learned a lot and we will lose a week of operation.

We are all realists and understand that one week is an unrealistic time for so much work + the most valuable thing is not the operating system and software, but data. Also, you will not be fully aware of the problems in your security and this may happen again in the near future. Taking into account the 3 percent profit our offer is $ 150,000. For this amount, you will get a quick recovery of all data and will be aware of all problems in

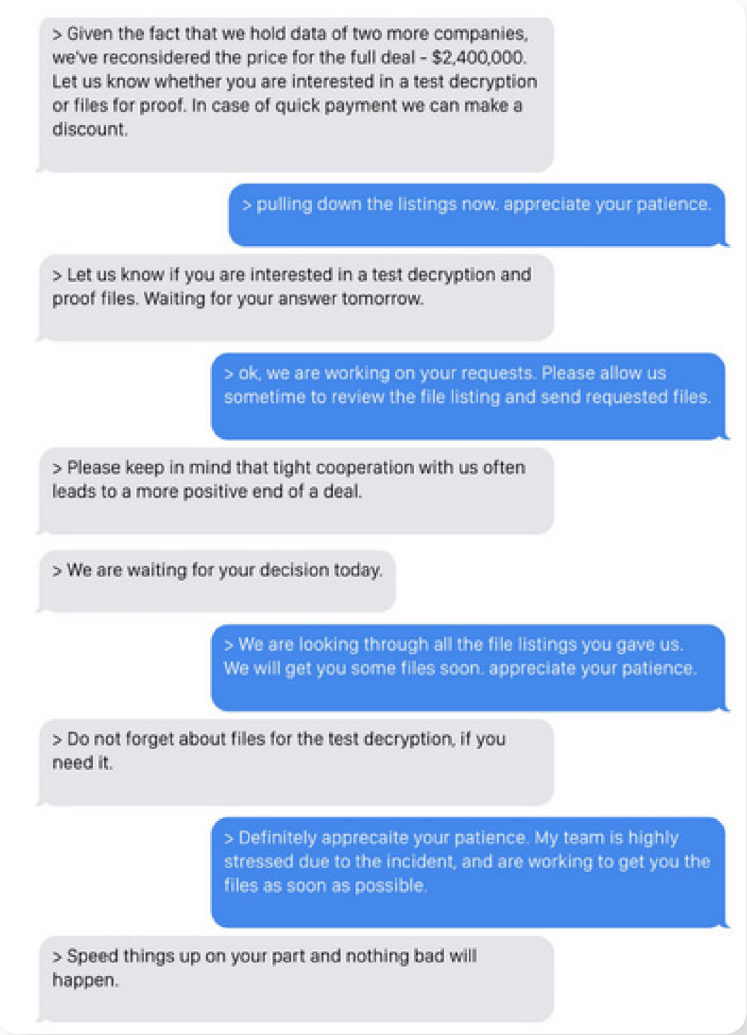
19

Steer clear of lowballing to an extent that it insults the intelligence of the threat actors; these are seasoned criminals, and they can smell desperation and deceit from a mile away. Instead, ground your offer in facts and figures, such as the actual cost of the damage done or the realistic value of the encrypted data. Explain your reasoning in a calm and composed manner, ensuring that your offer is backed by a solid rationale. By doing so, you are not just negotiating; you are engaging in a psychological battle, striving to establish a rapport and build trust with the attackers to facilitate a favorable outcome.

Remember, in the world of ransomware negotiation, a well-thought-out, LAP offer is your ticket to turning the tables and regaining control of the situation.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 8 : Extend the Negotiation Dance



> Given the fact that we hold data of two more companies, we've reconsidered the price for the full deal - $2,400,000. Let us know whether you are interested in a test decryption or files for proof. In case of quick payment we can make a discount.

> pulling down the listings now. appreciate your patience.

> Let us know if you are interested in a test decryption and proof files. Waiting for your answer tomorrow.

> ok, we are working on your requests. Please allow us sometime to review the file listing and send requested files.

> Please keep in mind that tight cooperation with us often leads to a more positive end of a deal.

> We are waiting for your decision today.

> We are looking through all the file listings you gave us. We will get you some files soon. appreciate your patience.

> Do not forget about files for the test decryption, if you need it.

> Definitely apprecaite your patience. My team is highly stressed due to the incident, and are working to get you the files as soon as possible.

> Speed things up on your part and nothing bad will happen.

When locked in the delicate dance of ransomware negotiation, time is a tool that can be wielded with precision and purpose. If the ticking clock isn't your enemy, take a moment, breathe, and prepare to embrace the art of stalling. Extending the negotiation process in a controlled manner isn't about playing games; it's about creating a strategic advantage.

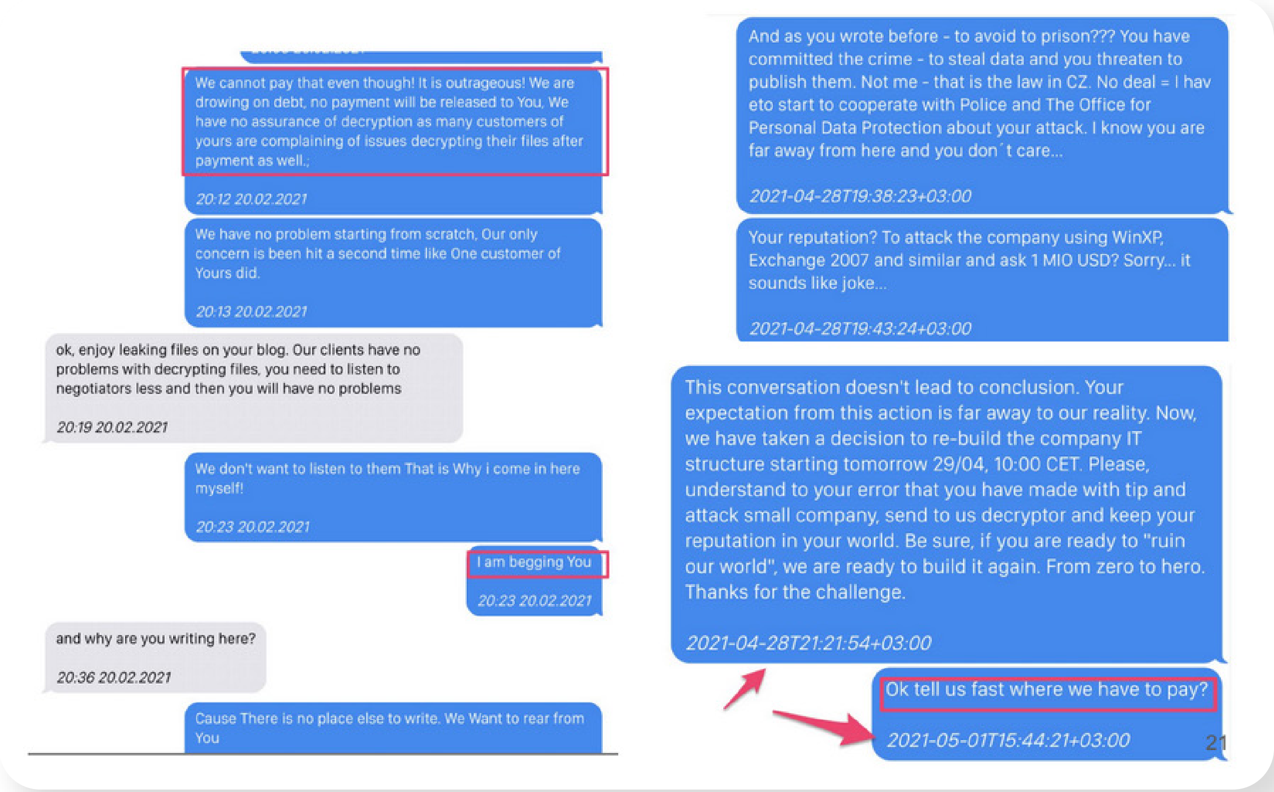
Transform yourself into a master negotiator by understanding that these cybercriminals are juggling multiple victims simultaneously. Your goal? Become the partner in this dance that demands the least attention. Engage in the conversation, respond to their messages, but do it in a way that doesn't scream urgency. As the minutes turn into hours, and hours possibly into days, their interest in your case will wane, and their impatience might just become your golden ticket. They'll grow weary, and in their weariness, you might find them more willing to lower their demands or even make mistakes. However, be cautious, as this is a double-edged sword; ensure you're constantly assessing the risk to ensure that this strategy doesn't backfire. In the grand ballet of ransomware negotiation, learning how to extend the negotiation process with grace and control could very well be your most elegant move.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 9 : The Power of Politeness: Tread Lightly, Save Big

Rumi says that a sharp sword cannot cut silk.

In the high-stakes world of ransomware negotiation, your words carry weight, and politeness can be your most valuable currency. Remember, you're not dealing with amateurs; you're up against a group that treats this as a commercial enterprise, cold and calculating. Treating this situation as a business transaction, rather than a personal attack, is pivotal.



We cannot pay that even though! It is outrageous! We are drowing on debt, no payment will be released to You, We have no assurance of decryption as many customers of yours are complaining of issues decrypting their files after payment as well.;

20:12 20.02.2021

We have no problem starting from scratch, Our only concern is been hit a second time like One customer of Yours did.

20:13 20.02.2021

ok, enjoy leaking files on your blog. Our clients have no problems with decrypting files, you need to listen to negotiators less and then you will have no problems

20:19 20.02.2021

We don't want to listen to them That is Why i come in here myself!

20:23 20.02.2021

I am begging You

20:23 20.02.2021

and why are you writing here?

20:36 20.02.2021

Cause There is no place else to write. We Want to rear from You

And as you wrote before - to avoid to prison??? You have committed the crime - to steal data and you threaten to publish them. Not me - that is the law in CZ. No deal = I hav eto start to cooperate with Police and The Office for Personal Data Protection about your attack. I know you are far away from here and you don´t care...

2021-04-28T19:38:23+03:00

Your reputation? To attack the company using WinXP, Exchange 2007 and similar and ask 1 MIO USD? Sorry... it sounds like joke...

2021-04-28T19:43:24+03:00

This conversation doesn't lead to conclusion. Your expectation from this action is far away to our reality. Now, we have taken a decision to re-build the company IT structure starting tomorrow 29/04, 10:00 CET. Please, understand to your error that you have made with tip and attack small company, send to us decryptor and keep your reputation in your world. Be sure, if you are ready to "ruin our world", we are ready to build it again. From zero to hero. Thanks for the challenge.

2021-04-28T21:21:54+03:00

Ok tell us fast where we have to pay?

2021-05-01T15:44:21+03:00

Keeping your cool and maintaining a polite demeanor can make all the difference. Accusations and hostility could escalate the situation, potentially inflating the ransom demand and making the attackers less willing to cooperate. Instead, aim to create a professional rapport.

Acknowledge the situation calmly, express your intent to resolve the issue, and negotiate firmly but respectfully. The art of diplomacy can be your shield and sword in this digital battlefield, potentially leading to a more favorable outcome and saving your organization a substantial amount of money.

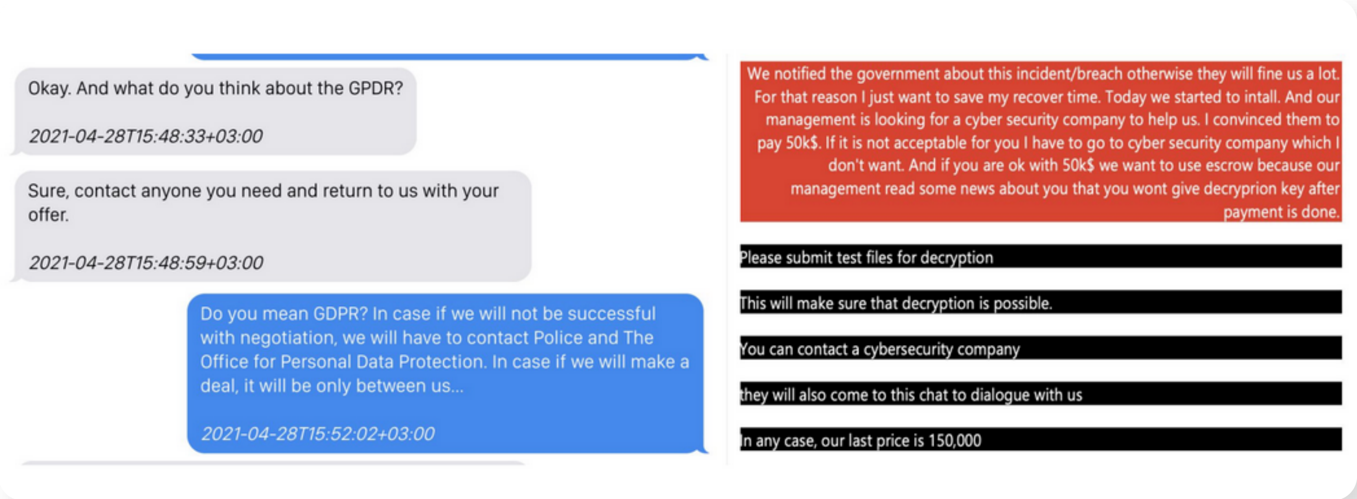
Remember, in the world of ransomware negotiation, keeping a level head and a polite tongue could be your ticket to a less costly resolution.

Time is now for soft power!

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 10 : Be Proactive: Report First, Gain the Upper Hand

In the digital chess game of ransomware negotiation, preemptive moves can make all the difference. Ransomware groups often wield the threat of reporting stolen data to public authorities as a weapon, aiming to corner you into compliance. Don't let them gain the upper hand.



Okay. And what do you think about the GPDR?

2021-04-28T15:48:33+03:00

Sure, contact anyone you need and return to us with your offer.

2021-04-28T15:48:59+03:00

Do you mean GDPR? In case if we will not be successful with negotiation, we will have to contact Police and The Office for Personal Data Protection. In case if we will make a deal, it will be only between us...

2021-04-28T15:52:02+03:00

We notified the government about this incident/breach otherwise they will fine us a lot. For that reason I just want to save my recover time. Today we started to intall. And our management is looking for a cyber security company to help us. I convinced them to pay 50k$. If it is not acceptable for you I have to go to cyber security company which I don't want. And if you are ok with 50k$ we want to use escrow because our management read some news about you that you wont give decryprion key after payment is done.

Please submit test files for decryption

This will make sure that decryption is possible.

You can contact a cybersecurity company

they will also come to this chat to dialogue with us

In any case, our last price is 150,000

Take control by reporting the incident to your local authorities promptly. This strategic move accomplishes two vital things: it removes a significant leverage point from the attackers' arsenal, and it positions you as a responsible actor in the situation. Even if you're hesitant about engaging with the authorities, make it abundantly clear in all your communications with the ransomware group that you have already reported the incident.

This not only nullifies their threats but also reinforces your position in the negotiation. By being proactive and strategic, you turn a potential vulnerability into a strength, ensuring that the ransomware group knows they can't use intimidation tactics to sway you.

Remember, in the realm of ransomware negotiation, knowledge is power, and proactivity is your shield.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

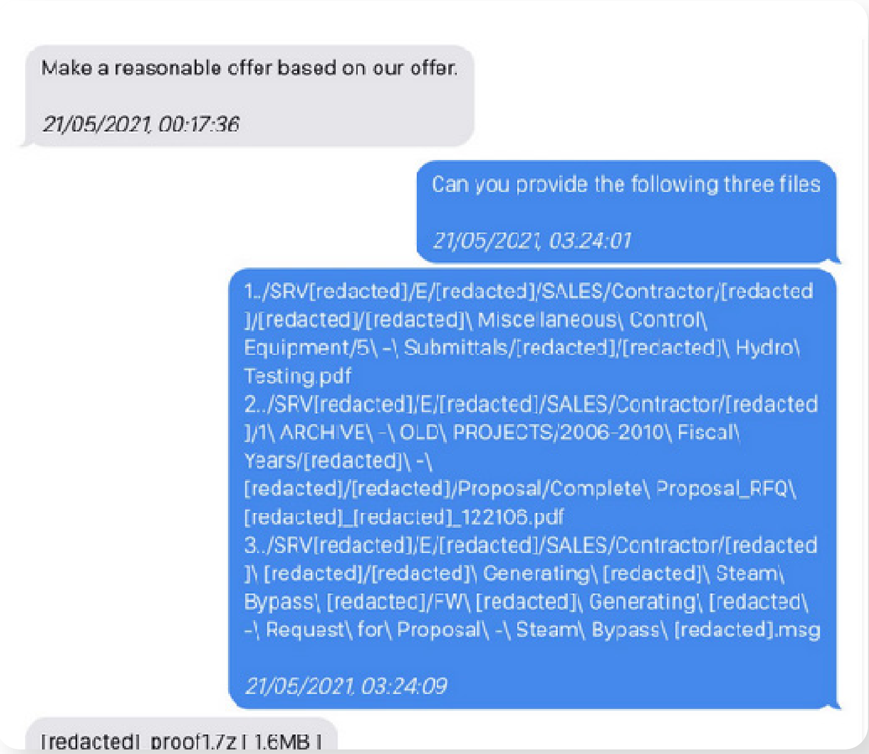
Lesson 11 : Threat is cheap, show me the data as proof.

Verifying before you trust is vital. Always demand proof of stolen data.

Navigating the treacherous waters of a ransomware negotiation requires a sharp mind and a demand for proof. When a ransomware group claims to have your data, take nothing at face value. Ask them to provide a list of files they've extracted from your system.

Why?

Because seeing is believing, and in this high-stakes game, you need to verify their claims before making any moves.



Make a reasonable offer based on our offer.

21/05/2021, 00:17:36

Can you provide the following three files

21/05/2021, 03:24:01

```
1../SRV[redacted]/E/[redacted]/SALES/Contractor/[redacted
]/[redacted]/[redacted]\ Miscellaneous\ Control\
Equipment/5\ -\ Submittals/[redacted]/[redacted]\ Hydro\
Testing.pdf
2../SRV[redacted]/E/[redacted]/SALES/Contractor/[redacted
]/1\ ARCHIVE\ -\ OLD\ PROJECTS/2006-2010\ Fiscal\
Years/[redacted]\ -\
[redacted]/[redacted]/Proposal/Complete\ Proposal_RFQ\
[redacted]_[redacted]_122106.pdf
3../SRV[redacted]/E/[redacted]/SALES/Contractor/[redacted
]\ [redacted]/[redacted]\ Generating\ [redacted]\ Steam\
Bypass\ [redacted]/FW\ [redacted]\ Generating\ [redacted\
-\ Request\ for\ Proposal\ -\ Steam\ Bypass\ [redacted].msg
```

21/05/2021, 03:24:09

[redacted] proof1.7z [1.6MB]

Once you have the list in hand, pick three to five files at random and request them to be decrypted. This step is your litmus test, your way of ensuring the group isn't bluffing and they truly possess what they claim to.

Pay special attention to large files – they need to decrypt correctly and entirely. If they can't do this, it's a red flag. This process not only validates the authenticity of the group's claims but also puts you in a position of informed power. You're not just a victim anymore; you're an active player, making calculated moves to protect your assets and navigate your way out of the crisis.

Remember, in the high stakes world of ransomware negotiation, trust is earned, not given. Demand proof, verify their claims, and ensure they're holding the cards they say they are before making your next move.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 12 : Less Now or More Later?

When you find yourself in the midst of a ransomware negotiation, remember: time is of the essence, but so is strategy. Bad actors are eager to close the deal and move on, making them sometimes more amenable to accepting a smaller sum if it means quicker payment.

- **Quick Closure, Smaller Sum:** Consider offering to pay a smaller amount immediately as opposed to a larger sum later on. This taps into the attacker's desire for swift resolution and could potentially save you money.

- **Guard Your Insurance Secrets:** Whatever you do, don’t let slip if you have cyber insurance. And make sure any documents related to your policy are stored securely, far from the reach of potential infiltrators. Revealing that you have insurance could embolden the attackers, as they might assume you’re capable of paying a larger ransom.

This lesson is your guide to navigating the treacherous waters of payment strategy.

Remember, in this high-stakes game, knowledge is power, and keeping your cards close to your chest could make all the difference. So, adopt a stance of strategic ambiguity, be cautious about what you reveal, and you might just find yourself in a better position to negotiate and resolve the crisis at hand.

Life Saving Lessons for Ransomware Victims from an Experienced Negotiator

Lesson 13 : Sealing the Deal: Ensure Data Deletion with Video Proof

Congratulations, you've navigated the treacherous waters of ransomware negotiation and reached an agreement. The ransom has been paid, and your data is finally back in your hands.

But wait, there's one more crucial step to take—making sure the bad guys hold up their end of the bargain and actually delete the data they took.

Demand Video Proof: Don’t just take their word for it; ask for a sample video showcasing the deletion of your data. This isn’t just about trusting their word; it’s about verifying their actions. A video provides tangible proof that they’ve held up their end of the deal, giving you that much-needed peace of mind.

Stay Vigilant: Even after receiving the video, don’t let your guard down. Keep a close eye on your systems, watching for any signs of further intrusions. The last thing you want is to go through this whole ordeal again.

This lesson is all about dotting your i's and crossing your t's. You’ve come this far; don’t let complacency set in now. Demand proof, stay vigilant, and ensure that the threat actors have truly deleted your data. This is your final step in closing this chapter and safeguarding your systems for the future. Remember, in the world of cybersecurity, trust but verify is the name of the game.

End of ongoing story

Navigating through the stormy seas of a ransomware attack is no small feat, and it requires a blend of technical acumen, strategic thinking, and psychological insight. The lessons and tactics shared in this whitepaper, drawn from extensive experience in leading negotiations worth over $100 million USD, serve as a vital playbook for anyone finding themselves in the crosshairs of a ransomware attack.

First and foremost, remember you are not alone. Assemble your crisis management team promptly, consult with professionals, and exhaust every available resource to retrieve your data before considering payment. Ensure that the attackers no longer have access to your systems, and be vigilant about potential espionage in your communication channels. In every interaction with the threat actors, maintain a posture of professionalism and politeness, keeping in mind that you are dealing with seasoned criminals for whom this is a lucrative business.

Negotiate strategically. Understand that every ransom demand has a rationale behind it, and it’s your job to uncover that and use it to your advantage. Offer reasonable and well-justified counterproposals, and extend the negotiation process deliberately to wear them down. Maintain an air of authority without revealing your true position within the organization, and always, always demand proof before and after payment to ensure data deletion.

But beyond the tactical maneuvers, foster a culture of preparedness within your organization. Ransomware attacks are not a matter of ‘if’ but ‘when,’ and your best defense is a proactive approach. Invest in cybersecurity measures, conduct regular training, and have an incident response plan ready to roll out at a moment’s notice.

In the end, the journey through ransomware negotiation is treacherous, but with the right tools, team, and tactics, you can navigate through it successfully, minimizing damage and safeguarding your organization’s future. Remember, in this high-stakes game of digital cat and mouse, knowledge is power, preparation is key, and resilience is your greatest ally.