

KNOCK, KNOCK !

WHO'S THERE?

IT'S YOUR **RANSOMWARE** CHAT

LESSON LEARNING FROM RANSOMWARE NEGOTIATION



KNOCK, KNOCK! WHO'S THERE? IT'S YOUR RANSOMWARE CHAT – LESSON LEARNING FROM RANSOMWARE NEGOTIATION

Release Date

Saturday, 16 December 2023

Threat Intelligence Analyst

Rizqy Rionaldy, CTIA, CEH, CHFI, ECIH

Security Researcher @openhunting.io

CONTENTS

INTRODUCTION.....	2
METHODOLOGY	2
PRE-NEGOTIATION	3
UNDERSTANDING NOTES LEFT BY THE RANSOMWARE	3
STAGE: COMMUNICATION BEGINS.....	6
STAGE : DEMONSTRATING AUTHENTICITY	8
STAGE: NEGOTIATION	11
WHAT HAPPENS IF THE VICTIM MAKES A PAYMENT?.....	18
RANSOMWARE GROUP SECURITY ADVISORY	20
CONCLUSION.....	26
REFERENCE	28



INTRODUCTION

Ransomware is a serious cyber threat that increasingly targets large organizations in various sectors, such as Healthcare, Education, and Government. These attacks typically start with the ransomware group encrypting valuable data and then demanding a ransom, often in cryptocurrency, in exchange for the decryption key. This puts organizations in a challenging position, facing both the immediate loss of access to their data and the pressure of a time-sensitive ransom demand. In response, organizations affected by ransomware attacks often consider paying the ransom as the quickest solution. However, this method is generally not recommended because it not only supports further criminal activities but also does not guarantee the recovery of data. **On the other hand, negotiating with ransomware groups is very important in the investigation process. If done correctly, these negotiations can provide extremely valuable information. This information is very useful for strategic analysis and formulating ways to handle ransomware incidents.** This article is inspired by projects inspired by [mthcht Blog](#), [ransomch.at](#), and <https://github.com/Casualtek>. By comparing data from these sources, the aim is to understand how to negotiate with ransomware groups effectively.

METHODOLOGY

We will conduct a thorough analysis of several ransomware negotiation transcripts that have been obtained, including:

- Avaddon
- Avos
- Babuk
- BlackMatter
- Conti



- Darkside
- Hive
- Revil
- Ranzy
- Lockbit3.0
- Mount-locker

PRE-NEGOTIATION

In ransomware incidents, the approach and ransom demands by Ransomware Groups are typically anonymous, leveraging encrypted communication channels and cryptocurrency. **These groups usually provide an encrypted chat service for initial contact with the victim.**

The victim should try negotiating additional channels and methods of communication with the Ransomware Group to enhance the dialogue. Efforts should be made to establish a line of communication that fosters mutual trust to the extent possible in such circumstances.

Should the victim decide to engage in negotiations and consider paying the ransom, **keeping a meticulous record of all communications is crucial.** This includes any specific instructions for a ransom payment. Such **records are not only strategic for the victim but also assist law enforcement and cybersecurity experts in their investigation of the attack.** This comprehensive documentation can provide invaluable insights for both the immediate response to the current incident and for developing future preventive strategies.

UNDERSTANDING NOTES LEFT BY THE RANSOMWARE

Ransomware attacks often begin with the attackers leaving a note that details their demands and provides instructions for contact. **Understanding these notes is crucial in the negotiation process, as they offer insights into the ransomware group's modus operandi,**



preferred communication methods, and, sometimes, their psychology. This section delves into the analysis of ransom notes and how they can guide the negotiation strategy. We use data from [threatlabz](#) to review several notes left by ransomware groups. These notes contain a variety of instructions, but fundamentally, they provide information related to the following aspects:

1. **Most communication will be conducted through the TOR Browser.** Victims will be asked to install TOR Browser and access a link they have prepared for negotiation. However, some communications request to send a DM on Twitter to the Ransomware Group Admin.

```
5. HOW TO CONTACT US

5.1 Download and install TOR Browser https://torproject.org
5.2 Go to our contact form website at http://basemmnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion/contact
5.3 You can request sample files chat to review leaked data samples.
5.4 In case TOR Browser is restricted in your area use VPN services.
5.5 All leaked Data samples will be Disclosed in 4 Days if you remain silent.
5.6 Your Decryption keys will be permanently destroyed at the moment the leaked Data is Disclosed.
```

Example from 8base_note.txt

```
!Azov ransomware!

Hello, my name is hasherezade.
I am the polish security expert.

To recover your files contact us in twitter:
@hasherezade
@VK_Intel
@demonslay335
@malwrhunterteam
@LawrenceAbrams
@bleepincomputer

Слава Україні! #Всебудеукраїна
```

Example from azov/RESTORE_FILES.txt



2. Victims are often explicitly instructed not to modify, rename, or delete any files that have been encrypted.

```
* DO NOT TRY TO RECOVER FILES YOURSELF!
```

```
* DO NOT MODIFY ENCRYPTED FILES!
```

```
* * * OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER! * * *
```

avaddon.txt

3. **Instructions typically include a directive for victims not to contact law enforcement agencies like the police or FBI, or other authorities,** such as professional negotiators, during the negotiation process

yanluowang.txt

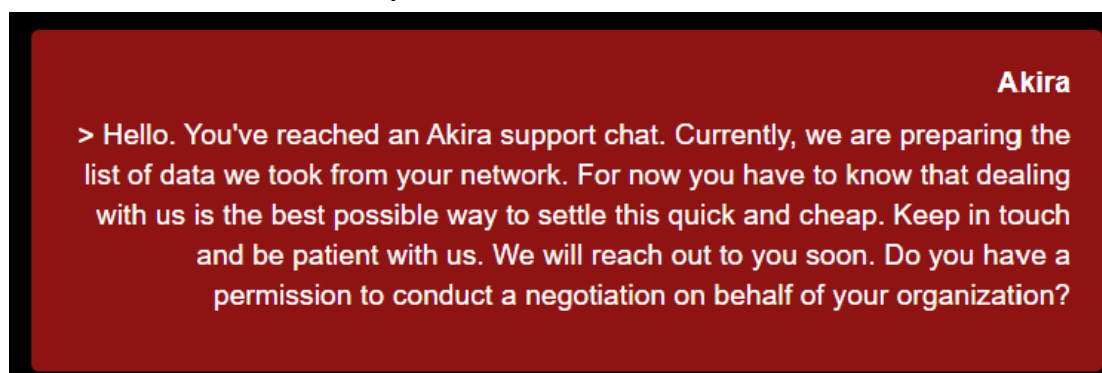
[illegible]

chilelocker/readme for unlock.txt

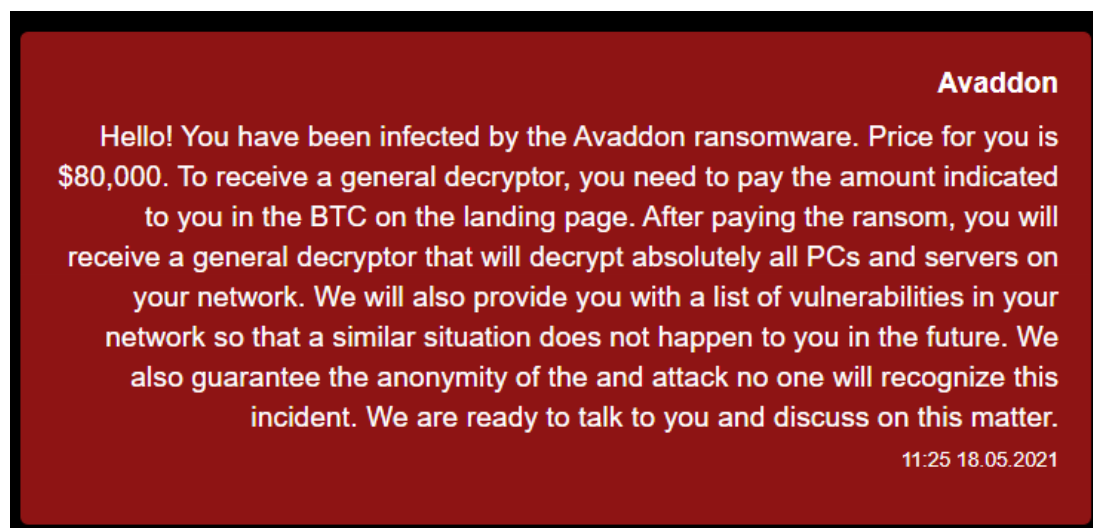
STAGE: COMMUNICATION BEGINS

Based on the data we have gathered, this section summarizes various initial conversation models typically employed by ransomware groups. Understanding how these groups initiate communication is crucial for organizations to prepare and respond effectively.

In the initial phase of a ransomware attack, the attackers introduce themselves and **confirm the successful encryption of data, immediately establishing control over the situation**. They then explain the circumstances and present their ransom demands, **typically requesting payment in cryptocurrency**. Detailed instructions for compliance are also provided, guiding the victim on how to fulfill these demands efficiently.

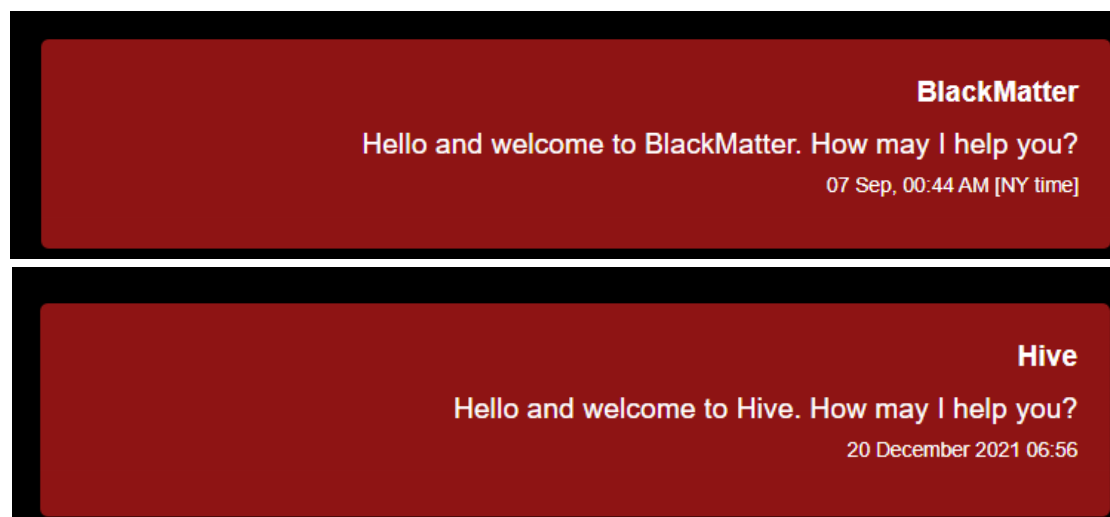


Akira Initial Chat



Avaddon Initial Chat

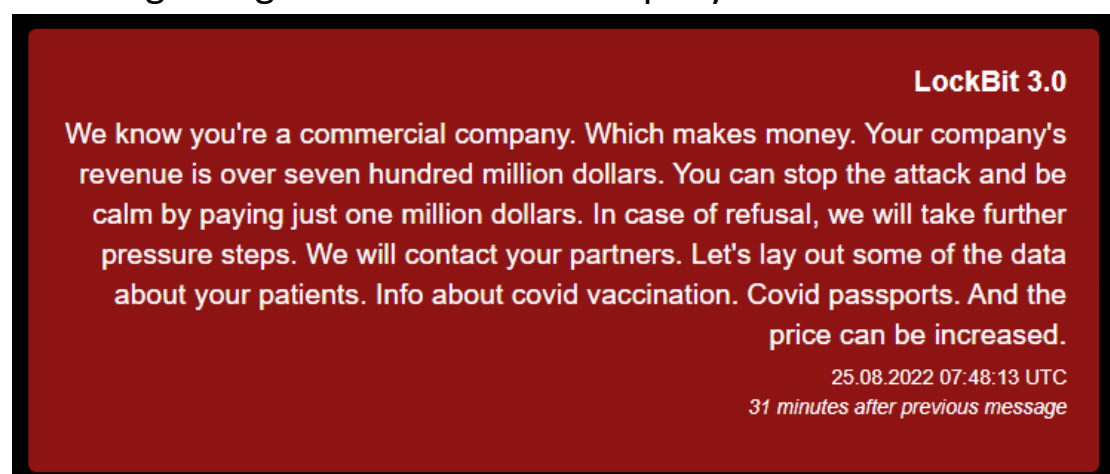




BlackMatter and Hive groups have the same Initial Chat.

Based on the collected data, a few key analyses have been made in the initial phase:

1. **Before launching an attack, ransomware groups conduct extensive information gathering about their target**, which means that in several conversations, the ransomware already possesses data regarding the value of the company.



2. Several conversations indicate technical issues, possibly because the company's negotiators aren't fully adept at handling negotiations through TOR chat. These technical challenges can lead to complications in communication with the Ransom Group.



Ensuring that your network and devices are properly functioning before starting the communication is crucial to avoid such issues.



STAGE : DEMONSTRATING AUTHENTICITY

In the ransomware negotiation process, the Stage of Proof plays a vital role when the Ransomware Group seeks to establish its credibility. During this stage, the **Ransomware Group typically requests the victim to send a small number of encrypted files (usually 2-3) for them to decrypt as a demonstration of their capability.** The Ransomware Group may impose conditions, such as selecting files that are not of critical importance, to avoid giving away crucial data prematurely. In some cases, like with the Akira ransomware, **the group provides the victim with a list of files they have compromised, allowing the victim to choose specific files for proof of decryption.**



1. Akira

Akira
> list.7z // 493 KB

Akira
> These files were taken from your network prior to encryption. You can pick 2-3 random files from the list and we will upload them to this chat as a proof of possession. To prove that we can properly decrypt your data you can upload 2-3 encrypted files to our chat and we will upload decrypted copies back.

2. Babuk

Babuk
Before we move on to discussing the price, upload 4-5 files of encrypted files no more than 10MB using any file exchanger, we will decrypt these files as a test

3. Black Basta

Black Basta
This is the full list of your taken data. You can choose any 3 file names from list and I will send them to you, like a proof. But these files must not contain the important information.
17:41

4. Conti

Conti
Yes, send 2-3 files to the chat room
13/08/2021, 17:26:13
an hour after previous message

5. Hive

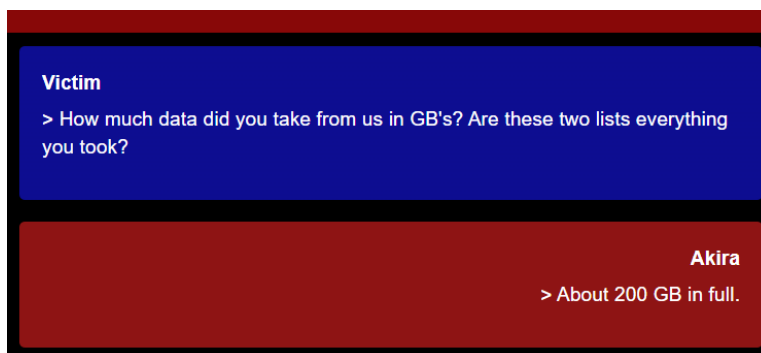
Hive
We performed files analysis. The impact of disclosure and undecryptable files will cost you few times more then \$3.5M. To prove that we have exfiltrated files I give you a sample archive.
<https://privatlab.com/s/v/NQqR2jo2B7SyQeBnp5y4>
2021-10-27 19:16

In the ransomware negotiation process, particularly during the Stage of Proof, the interaction between the victim and the Ransomware

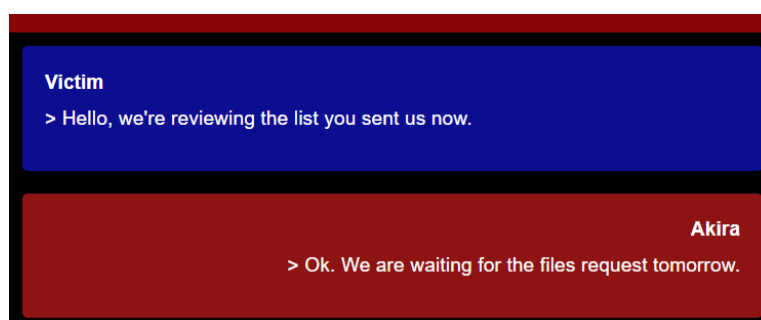


Group is crucial. Based on the data that has been collected, the following analyses have been made for this stage:

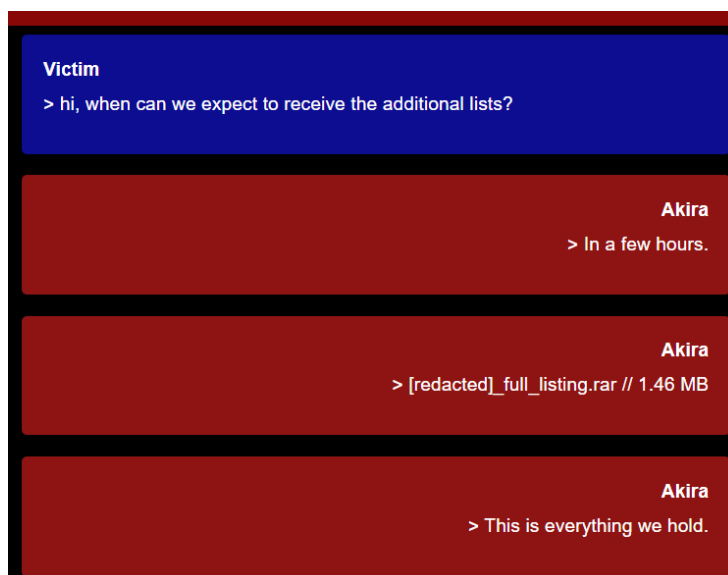
1. **Ask the Ransomware Group how many files they have accessed if this information hasn't been provided already.**



2. **Check the list of files that the Ransomware Group claims to have encrypted.**



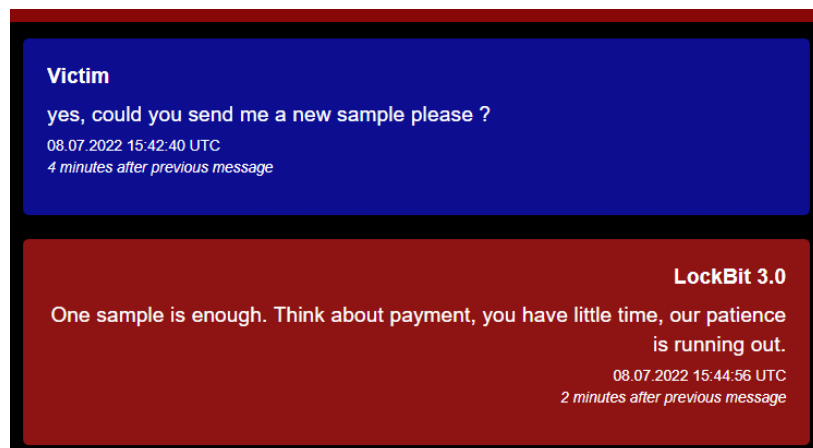
3. If possible, **consider asking for additional lists of encrypted files.** There's always a chance that the Ransomware Group might have more data than initially revealed.



4. After reviewing the provided list, **ask the Ransomware Group to send a few of the encrypted files as proof** of their control and ability to decrypt.



5. **Asking for fresh samples of the encrypted data.** It can help to understand how long the Ransomware Group has had access to the company's data.



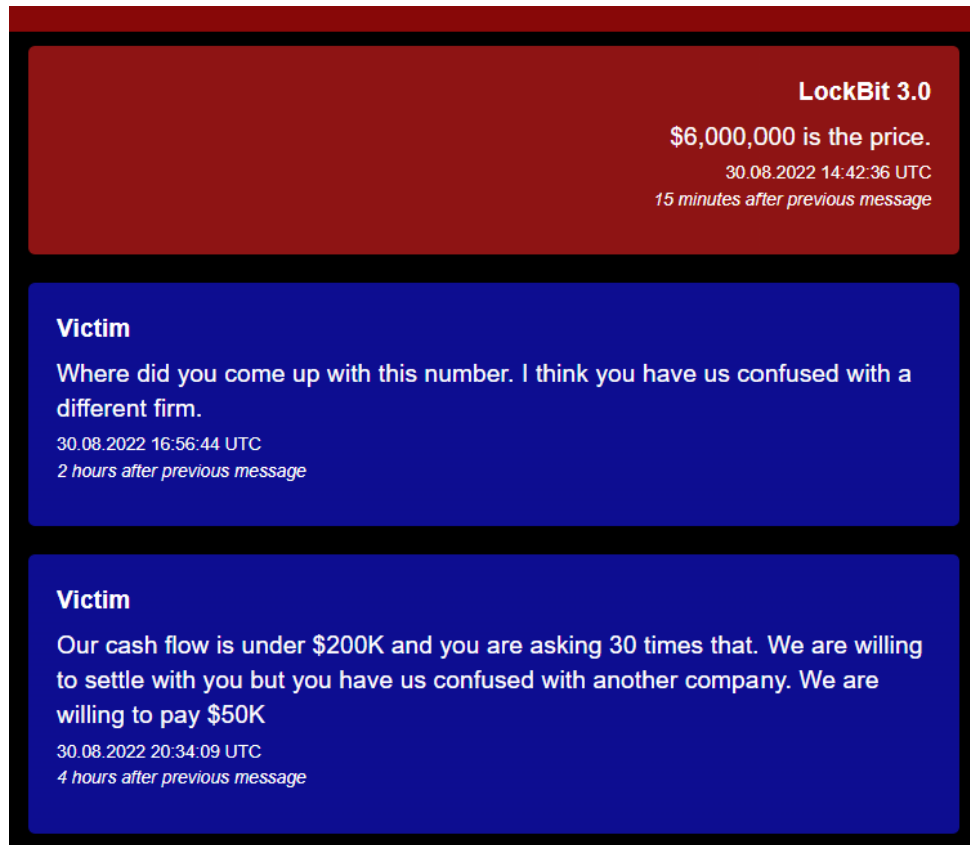
STAGE: NEGOTIATION

The Negotiation Stage is a critical phase in ransomware incidents where both the victim (negotiator) and the Ransomware Group engage in dialogue to determine a suitable ransom amount and terms.



This section explores the various conversation models typically employed by ransomware groups during negotiations and the tactics used by both sides to achieve their objectives.

1. Ransomware groups often **start by proposing exorbitant ransom amounts, creating room for negotiation**. The victim's goal is to bring down the price.



The screenshot shows a chat interface with a dark background. The first message is from 'LockBit 3.0' in a red bubble, stating '\$6,000,000 is the price.' with a timestamp of '30.08.2022 14:42:36 UTC' and '15 minutes after previous message'. The second message is from the 'Victim' in a blue bubble, asking 'Where did you come up with this number. I think you have us confused with a different firm.' with a timestamp of '30.08.2022 16:56:44 UTC' and '2 hours after previous message'. The third message is also from the 'Victim' in a blue bubble, stating 'Our cash flow is under \$200K and you are asking 30 times that. We are willing to settle with you but you have us confused with another company. We are willing to pay \$50K' with a timestamp of '30.08.2022 20:34:09 UTC' and '4 hours after previous message'.

LockBit 3.0
\$6,000,000 is the price.
30.08.2022 14:42:36 UTC
15 minutes after previous message

Victim
Where did you come up with this number. I think you have us confused with a different firm.
30.08.2022 16:56:44 UTC
2 hours after previous message

Victim
Our cash flow is under \$200K and you are asking 30 times that. We are willing to settle with you but you have us confused with another company. We are willing to pay \$50K
30.08.2022 20:34:09 UTC
4 hours after previous message

2. Ransomware groups **frequently set deadlines for payment**. Request extensions, using time as leverage to secure a better deal.



The screenshot shows a chat interface with a dark background. The message is from 'Akira' in a red bubble, stating '> Guys, your 600GB of data will be published soon, in case we don't have a reply from you within 12 hours.'

Akira
> Guys, your 600GB of data will be published soon, in case we don't have a reply from you within 12 hours.



3. Ransomware groups may **imply the potential harm from exposing the victim's company data, creating fear and urgency.**

LockBit 3.0

We are open to negotiations about the price, we have given everything you need. Files will not be opened until publication.

08.07.2022 16:37:04 UTC
5 minutes after previous message

LockBit 3.0

Think about your reputation, you have money, pay and keep customer data safe.

08.07.2022 16:38:04 UTC
a minute after previous message

4. Ransomware groups display **patience and wait for communication and negotiation** from the victim's side.

LockBit 3.0

Hi, what's the news?

20.02.2023 13:28:55 UTC
3 days after previous message

Victim

My leadership assessing the value of the data. How much to keep it from being published?

21.02.2023 13:10:00 UTC
a day after previous message



5. Some groups attempt to appear cooperative by **offering discounts**, **potentially to encourage payment**.

The screenshot displays a chat interface with four messages. The first message is from LockBit 3.0, offering a discount for quick payment. The second message is also from LockBit 3.0, stating that the timer has been paused and the victim has been hidden from the blog. The third message is from the victim, asking for the type of discount. The fourth message is from LockBit 3.0, offering a 30% discount if payment is made within 48 hours.

LockBit 3.0
If you pay quickly, we'll give you a discount.
21.02.2023 13:22:47 UTC
2 minutes after previous message

LockBit 3.0
While we're negotiating we've paused the timer and hidden you from the blog
21.02.2023 13:24:02 UTC
a minute after previous message

Victim
What kind of discount?
21.02.2023 13:25:04 UTC
a minute after previous message

LockBit 3.0
If you pay within 48 hours, we will give you a 30% discount
21.02.2023 13:26:06 UTC
a minute after previous message

In this stage, several valuable lessons can be learned to navigate ransomware negotiations effectively:

1. **Ensure you convey a sense of seriousness and readiness to negotiate.** This smooths the negotiation process and encourages continued interaction with the Ransomware Group.

The screenshot displays a chat interface with one message from the victim, thanking the ransomware group for their response and expressing commitment to resolving the situation.

Victim
Thank you for your response which we will respond to shortly. Please note that we remain fully committed to resolving the situation with you to the benefit of us both.
29.06.2022 19:10:04 UTC
a few seconds after previous message



2. communicate that you are not the decision-maker and that all decisions must be relayed to superiors or higher-ups.

Victim
OK i will take this to my boss and see what he says
30.01.2023 13:46:25 UTC
19 hours after previous message

3. Don't be complacent with the given deadlines. Verify the provided data and engage your team to evaluate the risks associated with encrypted data.

Akira
> The files are ok. In 24 hours we will announce your corporate data leak on your blog. Early next week your data will be published. Thank you.

Victim
> We are not stalling for time, we are wanting to make sure that the decryption process brings back the data in its entirety. The 2 files we are asking about it appears that it dropped fields off at the end of the files.

4. If possible, request new data as evidence of the group's willingness to cooperate. Make it clear that negotiations won't proceed without fresh data.

Victim
if I don't have the list of files I couldn't negotiate with the management..
09.07.2022 10:06:28 UTC
4 minutes after previous message

Victim
I know that you have the cards in hand, but my hands are tied without the list
09.07.2022 10:07:15 UTC
a minute after previous message



Victim

I have nothing more to offer you at the moment and the screenshot of the database does not speak to us..

09.07.2022 10:15:27 UTC

3 minutes after previous message

LockBit 3.0

Now I will send you a couple more tables from this database.

09.07.2022 10:17:20 UTC

2 minutes after previous message

Victim

ok if I have marbles I can negotiate without marbles I cannot .. it's a french expression

09.07.2022 10:19:57 UTC

3 minutes after previous message

5. In some cases, **you may be fortunate enough to have an opportunity to negotiate**. For example, mention that it's Friday and express difficulty in making a payment. This can buy time for analysts to evaluate the situation. If this is your final decision point, negotiate a payment that aligns with the situation. However, never actually make a payment to ransomware groups.

Victim

We offer you \$100,000 for everything, knowing that it's the weekend and everything is complicated

09.07.2022 08:24:21 UTC

14 hours after previous message

Victim

in addition it is the holidays in France

09.07.2022 08:26:40 UTC

2 minutes after previous message



6. Law enforcement agencies can investigate the Bitcoin wallet data of the attackers. **Attempt to obtain information about their wallets if possible**

Victim
you will have to leave the wallet for at least a day, otherwise it is not even worth imagining the payment, the decision-making circuits are very very long with us.
10.07.2022 15:08:30 UTC
3 hours after previous message

LockBit 3.0
bc1qp5erh27wesmm8sxljg9p39nua02gd02e4cwk2e
10.07.2022 15:09:20 UTC
a minute after previous message

Victim
i transfert .. thanks
10.07.2022 15:10:06 UTC
a minute after previous message

At this stage, you have obtained some crucial information, including:

1. Number of files they possess.
2. Timestamp of the latest file they have.
3. Bitcoin wallet address they own, which can facilitate law enforcement investigations.

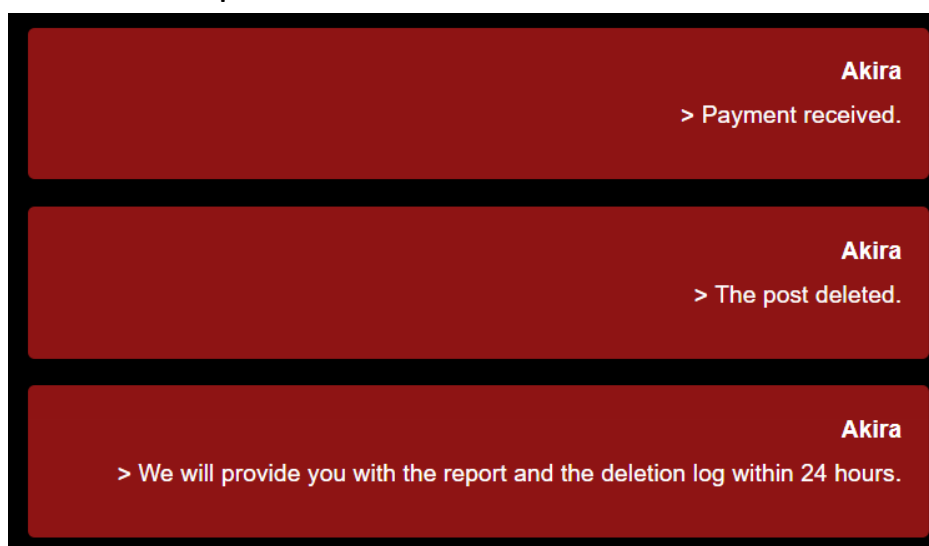
After getting crucial information, you can end the conversation with the ransomware group if you do not intend to make a payment. Interestingly, they may contact you to inquire about the latest updates on the negotiation.



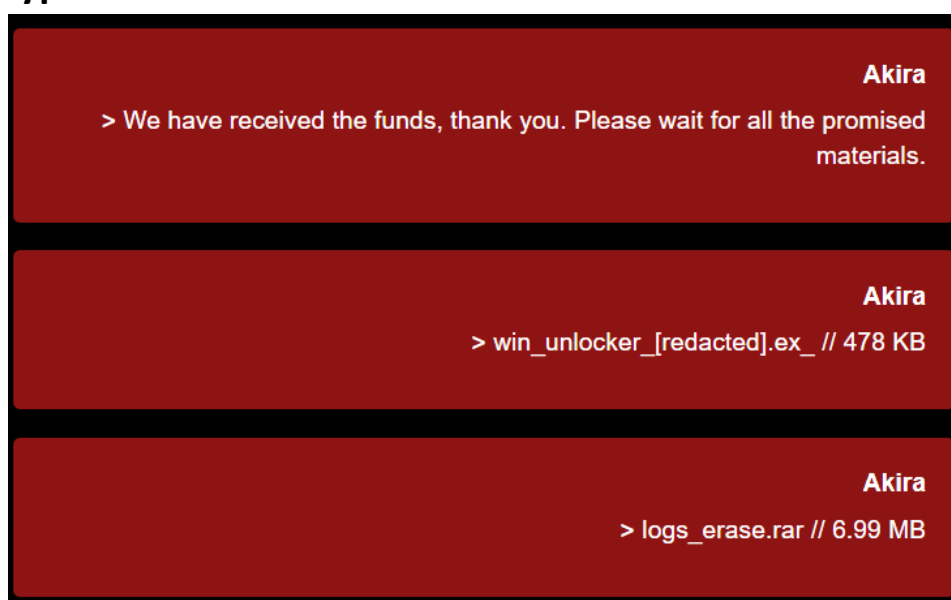
WHAT HAPPENS IF THE VICTIM MAKES A PAYMENT?

Despite strong advice against making payments to ransomware groups, it's important to understand what may transpire if a victim decides to pay the ransom. This section explores the potential outcomes of making a payment to ransomware groups:

1. Ransomware groups may **delete any content or information related to your company on their website** that they had previously accessed or compromised.



2. Upon receiving the ransom payment, the group is likely to **provide the victim with the decryptor key necessary to unlock the encrypted files.**



3. Along with the decryptor key, the **victim** may receive detailed instructions on how to use the key to decrypt their files effectively.

Black Basta

How to decrypt windows? 1. Drop executable to any folder. 2. Start new terminal session with administrator rights. (run cmd.exe or powershell.exe with admin rights) 3.1. In cmd.exe type full path to the executable file and press Enter. 3.2. In powershell.exe type: "& c:\full\path\to\executable.exe" without quotes and press Enter. OR 1. Drop file. 2. Click right mouse button on the file and press run as admin. (!) IMPORTANT, READ ALL BEFORE DECRYPTION PROCESS 1. Yoy can decrypt only 1 folder (test decrypt for example) decrypt.exe -forcepath c:\users\1\Desktop\folder 2. DO NOT CLOSE decryptor yourself 3. MAKE BACKUPS of important files what you will decrypt, then you can rerun decryptor if something happens 4. You can decrypt partially encrypted files: 4.1. Make backup 4.2. Add encrypted extension (random for every company, you can ask in chat) to file 4.3. Run decryptor to folder what contains file 4.4. Now you can test file 5. Every decryption process saves file in same location with name of decrypted file with extension .kbckp. In this file you can find individual chacha keys for better recovery experience. 6. You can ask in chat about ECC keys (used to encrypt chacha keys) for your company. 7. Make sure you have at least 10 gb of free space on each disk. 8. To choose folder on linux decrypt.linux -forcepath /path

23:44

Akira

> decrypt.zip // 479 KB

Akira

> decrypt.exe Name: decrypt Usage: cli args Flags: --path : Start path --secret : Private key --logs : Print logs. Valid values for: trace, debug, error, info, warn. Default: off -h, --help : Show help -----
Build information: Version: 2023.9.5 SECRET KEY: "[redacted]" -----
----- decrypt.exe --path --secret : Private key --logs -
--- decrypt.exe --path C:\ --secret [redacted] --logs trace decrypt.exe --secret [redacted] --logs trace

4. Some ransomware groups may offer a security advisory, providing insights into how the attack was executed on the victim's network.



This information could be used for preventive measures and future security enhancements.

It's crucial to emphasize that while these outcomes may occur, **making a ransom payment is not recommended due to the legal, ethical, and security risks involved**. It's often more prudent to explore alternative approaches, such as data recovery methods and cybersecurity measures, rather than succumbing to ransom demands.

RANSOMWARE GROUP SECURITY ADVISORY

This section delves into the **insights that can be gained from ransomware security advisories provided by ransomware groups**. After a victim has made a payment, some ransomware groups may offer a security advisory that provides valuable information on the techniques they used to exploit the victim's system. While it's important to reiterate that making ransom payments is strongly discouraged, analyzing these advisories can offer significant lessons in understanding the tactics employed by cybercriminals. This knowledge can be used to enhance cybersecurity measures and protect against future attacks.

A. Akira

Initial Access: Dark Web

Privilege Escalation: Credential Access (Kerberoasting)

Advisory:

1. None of your employees should open suspicious emails, suspicious link or download any files, much less run them on their computer
2. Use strong password, change them as often as possible (1-2 times per month at least). Password should not match or be repeated on different resources.



3. Install 2FA wherever possible
4. Use the latest version of the operating system, as they are less vulnerable to attack
5. Update all software version
6. Use antivirus solutions and traffic monitoring tools
7. Create a jump host for your VPN. Use unique credentials it that differ from domain one.
8. Use backup software with cloud storage that 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.

Akira

> Initial access to your network was purchased on the dark web. 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 deletion log is coming later.

B. Avaddon

Exploit weak passwords and old operating system vulnerability

Advisory:



1. Use Strong Password
2. Update all your OS to the latest version

Avaddon

About vulnerabilities in your network. These are weak passwords and old operating systems, the operating systems that you used have vulnerabilities, with the help of them an attack was carried out on your network. Use strong passwords and hide them as best as possible and update all your OS to the latest versions.

10:02 19.05.2021

C. Avos

Protecting against Mimikatz and Enhancing Network Security

Advisory:

1. Defend Credentials from Mimikatz:

Implement measures to defend against credential theft tools like Mimikatz.

2. Limit Administrator Privileges:

Restrict administrator privileges to a minimal group, ideally 2-5 accounts.

Require justification for any additional accounts added to the administrator group.

Upgrade Domain Functional Level:

Upgrade the forest and domain schema to at least 2012 R2, introducing the "Protected Users" group.

Members of the "Protected Users" group cannot authenticate using NTLM, Digest Authentication, or CredSSP.

Install KB2871997 Security Update:

Verify that the KB2871997 security update has been installed for required additional security.

Adjust the TokenLeakDetectDelaySecs registry setting if necessary.

Stop Storing Passwords in Memory:



Change the "UseLogonCredential" registry setting to '0' to prevent passwords from being available to Mimikatz.

Monitor for Unauthorized Software and Malware:

Implement monitoring for unauthorized software and malware, aiding in identifying Mimikatz installation and activity.

Update Forti VPN and Monitor for Updates:

Address critical vulnerabilities in Forti VPN by updating it.

Continuously monitor for updates, including Windows updates.

Password Management:

Inform IT staff to prevent the storage of user passwords within the network.

Recommend Additional Security Tools:

Suggest using SentinelAV and Datto backup systems.

Consider Veeam Tapes with a separate PC in WORKGROUP mode and a different user from the main domain.

Ensure that every PC has antivirus (AV) protection.

Implement 2FA for Remote Desktop:

Configure two-factor authentication (2FA) on all network PCs for remote desktop connections.

Utilize password protection on AV solutions.

Consider Alternative VPN Solutions:

Caution against using Sonic VPN and Pulse Secure due to known vulnerabilities.

Update Exchange Server:

Ensure that the Exchange Server is updated as it was the main entry point.



Defend your credentials from mimikatz Limit administrator privileges to the smallest group possible. Even if you have thousands of user accounts, you should probably only have 2-5 administrator accounts. Start with two accounts and force users to justify any additional accounts added to the administrator group. The next thing that you should do is upgrade the schema and functional level of your forest and domain to at least 2012 R2. This domain functional level adds a fairly new group called "Protected Users". Along with other protections, the members of the Protected Users group cannot authenticate by using NTLM, Digest Authentication, or CredSSP. These changes provide powerful protections that make Mimikatz almost worthless. Verify KB2871997 has been installed to apply additional required security. After you install this security update, the default setting for non-protected users on Windows 7 and Windows 8 is to not force clear leaked logon session credentials.

Thu, 09 Sep 2021 15:04:38 GMT

To override this default you can add the following registry dword, TokenLeakDetectDelaySecs, and set it to a recommended value of 30 seconds. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Stop storing passwords in memory by changing the "UseLogonCredential" registry setting to '0' instead of the default value of "1" and passwords are no longer available to Mimikatz . HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest Start monitoring your systems for unauthorized software and malware, which should help identify Mimikatz installation and activity. You'll have to test these changes to see what breaks, but the idea is to implement some fairly basic changes to protect your network. In your specific case the critical vulnerability contained Forti VPN, please update FortiVpn and monitor for updates and Windows updates. Inform your IT stuff to remove the possibility of storing user passwords within the network.

Also we recommend you to use SentinelAV and dattoo backup system. Also Veeam Tapes is good ,but pc with veeam should be in WORKGROUP and user should be different from main domain. Every PC should have AV. Don't let any pc without AV. Also try configure 2FA (at all network pc) when you connect to remote desktop. Use password on AV. Also tip for you: If you want chage Fortigate VPN to other . We dont reccomend you to use Sonic VPN,Pulse Secure, because its under massive hack

Avos

And finally, update your Exchange Server, since it was the main entry point.



D. Black Basta

Network has experienced a compromise through the distribution of malicious email attachments, leading to malware execution by a user

Advisory

1. Use a sandbox to analyze the contents of letters and their attachments.
2. Use the password security policies
3. Make protection from attack like a Pass-the-Hash and Pass-the-ticket attack
4. Update all OS and software to the latest versions, especially Microsoft Defender Antivirus.
5. Implement the hardware firewalls with filtering policies, modern DLP and IDS, and SIEM systems.
6. Block kerberoasting attacks
7. Conduct full penetration tests and audit
8. Use and update Anti-virus/anti-malware and malicious traffic detection software
9. Configure group policies, disable the default administrator's accounts, and create new accounts.
10. Backups. You must have offline backups, and does not have access to the network.

Security report and recommendation: Your network has been compromised by mailing of messages to the emails with malicious attachments. One of the users launched malware. To avoid this in the future, give you recommendations of network protection: 1. Use sandbox to analyze the contents of letters and their attachments. 2. Use the password security policies 3. Make protection from attack like a Pass-the-Hash and Pass-the-ticket attack 4. Update all OS and software to the latest versions, especially Microsoft Defender Antivirus. 5. Implement the hardware firewalls with filtering policies, modern DLP and IDS, SIEM systems. 6. Block kerberoasting attacks 7. Conduct full penetrations tests and audit 8. Use and update Anti-virus/anti-malware and malicious traffic detection software 9. Configure group policies, disable the default administrators accounts, create new accounts. 10. Backups. You must have offline backups, does not have access to the network.



CONCLUSION

This summary encapsulates the key insights and strategies derived from a detailed analysis of various ransomware incidents:

1. Understanding the Attacker's Approach and Demands

Ransomware groups often use anonymous communication channels and demand payment in cryptocurrency.

Analysis of ransom notes reveals the attacker's preferred communication methods and initial demands.

2. Pre-Negotiation Strategy

Documentation of all communication and specific instructions for ransom payment aids in strategic decision-making and assists law enforcement.

3. Insights from Ransom Notes

Ransom notes provide crucial information about the ransomware group's methods. These notes often instruct victims not to contact law enforcement or modify encrypted files, indicating the group's attempt to maintain control.

4. Initial Communication Patterns

Ransomware groups assert control by confirming data encryption and presenting ransom demands.

Early conversations reveal that attackers often have pre-gathered information about the target's value.

5. Stage of Demonstrating Authenticity

Ransomware Group may prove their capability by decrypting a few files, allowing victims to assess the seriousness of the attack.

Victims should inquire about the extent of data access and encrypted files.

6. Negotiation Dynamics

Ransomware groups start with high ransom demands, expecting negotiation.



Negotiators should use deadlines as leverage and understand the implied threats.

7. Tactics for Effective Negotiation

Convey seriousness and readiness to engage in negotiations.

Communicate as a mediator, not as the decision-maker.

Verify the attackers' claims and engage a team to evaluate risks.

8. Gathering Crucial Information:

Obtain information about the number of files accessed, timestamps, and Bitcoin wallet addresses of the attackers.

This information is valuable for law enforcement and strategic response.

9. Consequences of Making a Payment

Understanding potential outcomes, such as receiving decryption keys and possibly security advisories.

Ethical, legal, and security implications of making a ransom payment.



REFERENCE

<https://github.com/Casualtek/Ransomchats>

https://ransomch.at/lockbit3.0-vitalityhp_net

<https://mthcht.medium.com/ransomware-negotiation-chats-what-can-we-learn-19c275462df5>

https://github.com/threatlabz/ransomware_notes



OPENHUNTING.IO

Project To Make Threat Hunting and Intelligence
Information & Tools Available for Every One.

