CYBER DEFENCE OPERATIONS

2023

Deconstructing Deception:

Linguistic and Psychological Insights into the ClOp Ransomware Group

Umar Javed & Kamran Saifullah

CyDefOps | June 28th, 2023 TLP: CLEAR www.cydefops.com

Contents

Introduction:

The Cl0p (TA505) ransomware collective, first surfacing in 2019, is believed to be an ensemble of Russian cybercriminals. This group has achieved global infamy by successfully intimidating and extracting ransoms from numerous businesses over the years.

Recently, the group, also known as TA505, claimed responsibility for attacks that exploited a vulnerability (CVE-2023-34362) identified in May 2023 in the MOVEit file transfer software. Through a message marked by irregular English, the collective indicated that they hold "information on hundreds of companies." These impacted companies are encouraged to engage via a supplied chat URL, where the Cl0p group plans to provide evidence of their data capture and discuss a ransom sum.

This article delves into the nuances of this message, providing a comprehensive analysis of its psychological and linguistic facets and their implications for the larger cybersecurity community. The pivotal points discussed in this piece can serve as a framework for evaluating communications from other threat actors or groups. This analysis can empower defenders with a profound understanding of the threat actor's objectives, intentions, and strategies, ultimately aiding in successfully thwarting attempts to victimize organizations.

The Ransomware Note:

Following the successful execution of their mission—exploiting the system vulnerability, accessing critical infrastructure and data to leverage for extortion—the threat actor leaves behind a carefully crafted note. This message frames the forthcoming engagement, delineating a path towards a potentially less damaging outcome for the victim, while also illustrating the harsh consequences of non-compliance with their demands. An example of this can be seen below:

DEAR COMPANIES. CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.
THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA
AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.
WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.
IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.
STEP 1 ***IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.***
STEP 2 ***EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM***
STEP 3 ***OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR***
WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE
STEP 1 ***IF WE DO NOT HEAR FROM YOU UNTIL JUNE 12 2023 WE WILL POST YOUR NAME ON THIS PAGE***
STEP 2 ***IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU***
STEP 3 ***OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE***
STEP 4 ***YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING***
STEP 5 ***YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED***
STEP 6 ***AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION***
STEP 7 ***YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH***
WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS ! DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU. CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE. ***FRIENDLY CLOP!*** ***PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.***

Credit: Twitter - @AlvieriD

Let's delve thoroughly into the message to decipher insights based on the actor's linguistic choices and the substance of their communication.

Core Linguistical Insights:

1. ### Non-native English Speaker:

   Numerous grammar and spelling mistakes suggest that the author is likely not a native English speaker. For instance, the use of "you company" instead of "your company," and "publish" instead of "published" shows a lack of fluency in English. There are also consistent mistakes in verb tenses, preposition use, and definite article usage.

2. ### Possibly Slavic Language Background:

   The omission of articles such as 'a', 'an' (indefinite), and 'the' (definite) which are used to demonstrate whether that noun refers to something specific or not. The inappropriate use of the article may suggest that the author's first language is one that does not use articles, such as a Slavic language. For example, "WE HAVE NO USE FOR FEW MEASLE DOLLARS" should properly be "We have no use for a few measly dollars."

   Articles are a type of determiner in English grammar that are used before a noun to demonstrate whether that noun refers to something specific or not. There are two types of articles in English: definite and indefinite. An example of a definite article is “the”, conversely an indefinite article, that which does not refer to something specific include “a” and “an”.

   - Slavic languages are divided into three subgroups: East, West, and South, which together constitute more than 20 languages spoken across Eastern Europe and Northern Asia.
   - The East Slavic languages include Russian, Ukrainian, and Belarusian. West Slavic languages include Polish, Czech, and Slovak, among others. The South Slavic languages include Bulgarian, Macedonian, Serbian, Croatian, Slovenian, and Bosnian, among others.

3. ### Education and Technical Awareness:

   The text, despite its linguistic errors, is quite coherent and understandable, suggesting a certain level of education or self-training. The writer demonstrates knowledge of technical terminology and processes, such as "penetration testing service," "exploit," and use of the TOR (The Onion Router) network for anonymous communication. This indicates a meaningful level of technological awareness and understanding of cybersecurity.

4. Group Affiliation:

The use of "we" and "our team" suggest that the writer is not acting alone but is part of a larger group or organisation.

- Indication of Group Activity: By using these pronouns, the author indicates that the actions are being carried out by a group rather than an individual. This can imply a higher level of organisation, resources, and potential threat.
- Shared Responsibility and Anonymity: The use of "we" and "us" can serve to distribute responsibility for the actions among multiple individuals, creating a sense of anonymity and collective decision-making. This might make it harder to attribute actions to specific individuals within the group.
- Establishing Authority: When referring to "our team", the writer could be attempting to establish a sense of authority and professionalism or inflating their capacity/ strength. Despite the criminal nature of their activities, this can make them seem more legitimate and intimidating to their targets.
- Psychological Distance: The use of "we" and "us" instead of personal pronouns like "I" or "me" creates psychological distance between the individual members of the group and their actions. This might help them rationalise or justify their activities.
- Building a Brand Identity: By consistently referring to themselves as a team, they are establishing a sort of brand identity. This can make them memorable and might contribute to their overall reputation in the criminal underworld.
- Intimidation: The psychological effect of the use of collective pronouns can serve to intimidate the reader. The idea of facing a group of adversaries, as opposed to a single individual, can increase the perceived threat level and pressure the reader into complying with the group's demands.

5. Explicit Threats and Extortion Tactics:

The letter is explicitly threatening, suggesting a willingness to expose sensitive company data if demands are not met. This is an indicator of malicious intent and can be categorised as a form of cyber-extortion.

6. Experience of Previous Operations:

Claims about the team's longevity and past reputation ("OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE.") suggest the group may have experience in such operations, indicating a potentially higher level of sophistication and threat.

7. Discretion:

The author doesn't want to interact with the media or researchers, suggesting a desire to keep their actions relatively low-profile and deal directly with their targets. This also has the added effect of luring the victim into a false sense of hope that the incident is not public, this is a fear for large organisations which have a global public presence.

Forensic Linguistical Insights:

Forensic linguistics is the application of linguistic knowledge, methods, and insights to the forensic context of law, crime investigation, trial, and judicial procedure. From this perspective, let's delve into the message a little deeper:

1. Lexical Choices and Syntax:

   Lexical choices such as 'penetration testing', 'exploit', 'exceptional exploit', and 'dedicated chat URL over TOR' suggest that the author is well-versed in technical language, indicating a background or at least some general knowledge in information technology or computer science.

2. Stylistic Consistencies and Idiosyncrasies:

   The author consistently writes in all-caps, uses minimal punctuation, and lacks proper article and preposition usage. They also make some unique lexical choices such as "measle dollars". These stylistic consistencies and idiosyncrasies can be used as linguistic fingerprints if similar writings from the same author are available for comparison.

   - Emphasis: Using all caps can indicate that the writer is emphasising a point. This is a common use of all caps in digital communication where nonverbal cues are absent. In the given text, the author might be using this to stress the importance of their messages and create a sense of urgency.

     Imitates Shouting: In internet etiquette, or "netiquette", all caps is often perceived as shouting. This could be used to portray anger, aggression, or intensity. However, in this text, it seems to be used more for emphasis than expressing emotion.

   - Commands Attention: The use of all caps can serve to command the reader's attention. It stands out visually compared to lowercase text, which might make the reader pay more attention to these passages. The author could be using this to highlight key instructions/ cues or warnings.

   - Indicates Formality or Seriousness: Sometimes, all caps can be used to indicate a level of formality or seriousness. In this case, the author might be attempting to communicate the serious nature of their threat.

   - Lack of Language Proficiency: The frequent use of all caps could be a sign of lower digital literacy or proficiency in the language. Some non-native English speakers may use all caps as they might not fully understand the nuances of case usage in English.

3. Pragmatics:

The author is using directive speech acts ('EMAIL OUR TEAM', 'CALL TODAY') indicating a commanding position, while the use of politeness in some parts of the text ('FRIENDLY CLOP', 'YOU DO NOT NEED TO CONTACT US') may serve to lessen the forcefulness of the threats.

Pragmatics refers to the branch of linguistics that studies how context influences the interpretation of meaning. Here are some ways pragmatics can be applied to the original passage:

- Deixis: Deixis refers to words that can't be fully understood without additional contextual information. For instance, the use of "this page" requires the reader to understand the medium of communication. In another case, the mention of a date "June 14, 2023" anchors the communication to a specific timeline.
- Implicature: Implicature refers to what is suggested in an utterance, even though neither expressed nor strictly implied. In this text, phrases such as "we have no use for few measle dollars to deceive you" imply that the group is reliable, though there's no explicit evidence is provided.
- Speech Acts: A speech act is a declaration that serves a function in communication. We see multiple speech acts in this message: directives ("email our team", "call today"), declarations ("we are the only one", "our team has been around for many years"), and representatives ("we downloaded a lot of your data").
- Politeness Theory: The writer uses a certain level of politeness, despite the threatening nature of the message. For example, "we do not wish to speak to media or researchers. Leave" is a directive, but the phrase "friendly clop" at the end attempts to mitigate the severity of their message.
- Presupposition: This refers to assumptions the writer makes about what the reader already knows. For instance, they presuppose that the reader is familiar with concepts like MOVEit software, TOR (The Onion Router), or the process of negotiating with hackers.

4. Discourse Analysis:

The way the message is structured, with steps and instructions, demonstrates a level of organisation and an attempt to control the narrative and actions of the intended recipients.

Discourse analysis refers to the examination of language beyond the sentence level, and looks at the context, social situation, and how different parts of the text are connected to form a cohesive whole. Here are some insights from a discourse analysis perspective of the original passage:

- Cohesion: Despite the ungrammatical sentences and lack of conventional punctuation, the text is structured in a logical sequence. There's a clear progression from introduction (announcing their action) to instructions

(steps to follow) to consequences (what will happen if these steps aren't followed).

- Code-switching: Although not explicitly occurring (where the writer would switch between two languages), the writer does switch between formal and informal language frequently. For instance, the language shifts from an almost business-like tone ("one of top organisation offer penetration testing service") to a more casual, colloquial tone ("few measle dollars").
- Intertextuality: This refers to the way texts refer to other texts. The writer draws upon conventions seen in other ransomware communications (such as offering proof of data theft, providing a timeline, etc.).
- Power Relations: The text clearly establishes the writer or group as holding power. They dictate terms, set timelines, and specify what the targeted companies should do.
- Genre and Register: The passage falls into the genre of ransom notes, which historically follows a similar structure, though it's highly unconventional due to its digital and corporate context. The register varies throughout the passage as the writer alternates between a formal and informal tone.
- Audience Design: The writer designs the message keeping in mind multiple audiences - companies using the specific software, the media, researchers, and potentially law enforcement.

This sort of discourse analysis can be helpful in identifying the writer's intent, their assumed relationship with the reader, and the broader social context in which they're writing.

5. Sociolinguistic Aspects:

Language use can tell us about the social identity of the writer. In this case, the misspellings, grammatical errors, and omission of articles point towards the author being a non-native English speaker, potentially from a Slavic language background.

- Language and Identity: The writer uses a specific type of English marked by non-standard grammar and spelling, unusual punctuation, and technical jargon. This could reflect the writer's educational background, linguistic background (possibly a non-native English speaker), and their identity as a part of the hacker community.
- Language and Power: The use of directive language, imposing instructions, and deadlines, shows a power dynamic where the writer is asserting authority over the recipients of the message. The writer is controlling the discourse (language beyond the sentence level), signalling their dominance and the recipients' vulnerability in this situation.
- Language and Social Distinction: The writer uses specialised language ("penetration testing service", "MoveIT product", "exploit") that could be understood by a specific audience - people with knowledge of cybersecurity.

This can be seen as a social distinction, separating the in-group (those who understand the terminology) from the out-group (those who do not).

- Language and Politeness: Despite the threatening nature of the communication, there are instances of politeness ("Friendly CLOP", "Relax because your data is safe"). This could be seen as an attempt to mitigate the threatening acts being presented in the text.
- Language and Context: The text's medium (probably an email or a digital message) and purpose (a ransom note) are essential parts of understanding the language choices. For instance, the use of all caps, which might be seen as shouting in other contexts, could be intended here as a means to stress seriousness or to create a sense of urgency.
- Societal Attitudes and Stereotypes: The language errors, coupled with the threatening content, may reinforce societal stereotypes about hackers or cybercriminals, even if these may not accurately represent the diverse individuals involved in these activities.

6. Anonymous and Confidential Communication:

The writer suggests email contact and communication over the Tor (The Onion Router) network, which is designed for anonymous communication. This suggests they are aware of, and attempting to avoid, potential tracking and tracing of their communications.

- Use of Pseudonym or Collective Identity: The author refers to themselves as "CLOP", a pseudonym, or the name of their group. This is a common strategy for maintaining anonymity and avoiding personal identification in digital communication.
- Untraceable Contact Information: The email addresses provided do not contain any personal identifiers that could lead to the perpetrators. Emails can often be routed through servers that hide the sender's original IP address, further contributing to the anonymity.
- Use of TOR for Communication: The text mentions that the group will provide a "dedicated chat URL over TOR". TOR (The Onion Router) is a network that enables anonymous communication by routing traffic through multiple servers and encrypting it at each step. This makes it extremely difficult to trace the source or destination of the communication.
- Promise of Confidentiality: The perpetrators attempt to reassure the victims that their data is safe and won't be misused, in essence offering a form of confidentiality, albeit under a threat.
- Potential for Anonymous Payments: While the passage does not directly mention this, ransomware attackers often demand payments in cryptocurrencies like Bitcoin. These can be difficult to trace and therefore help maintain the attacker's anonymity.

- Deniability: The use of collective pronouns ("we", "us", "our") instead of individual identifiers provides a degree of plausible deniability, making it harder to attribute actions to specific individuals.

7. Self-Perception:

The language indicates a perception of power and control, with phrases like "OUR TEAM HAS BEEN AROUND FOR MANY YEARS" and the use of steps to guide the potential victim's actions. They see themselves as the party in control of the situation.

- Self as Professional: Despite the nature of their activities, the author refers to themselves as offering a "penetration testing service", portraying their actions as a professional service rather than a criminal act. The use of technical jargon and phrases like "our team" further reinforce this perception.
- Self as Powerful: The author presents themselves as powerful and in control- having the upper hand. They dictate the terms and conditions, set timelines, and determine the potential outcomes. This power dynamic is further emphasised by their assertion that they are "the only one who performs such attacks", suggesting uniqueness and skill.
- Self as Reliable: The author emphasises their reliability, asserting that they have never failed to do as promised, this adds the sense of fear and the potential for the victim to yield to their demands. They even go as far as offering to provide proof of their claims and provide a “guarantee” about the safety of the victim's data, there is no assurance in place that they won’t dump the victim’s data upon payment.
- Self as Just: Interestingly, the author seems to view their actions as justified or even moral to some extent. They make a point to mention that they have "no interest to expose" information related to governments, cities, or police services. This suggests a sort of 'hacker ethic' where certain targets are off-limits, despite their overall illegal activities.
- Self as Business-minded: The step-by-step process they offer for negotiations, their mention of proof, and the talk of pricing all indicate that they view this as a business transaction. The phrase "few measle dollars" seems to underscore that they perceive the requested ransom as trivial compared to the perceived value they provide (i.e., not releasing the data).

These insights suggest that the authors perceive themselves as professional, powerful, reliable, and business-oriented, with their own form of ethics.

8. Targeting:

The author explicitly mentions certain entities such as companies using the MOVEit software, suggesting a targeted approach to their operations. Moreover, they exclude government, city, or police services, which indicates a certain code of conduct or boundary setting within their activities.

- Specific Software Users: The author directly mentions companies that use the "MoveIT product," indicating that their activities focus on exploiting vulnerabilities in this specific software. This suggests their targets would be organisations that rely on MoveIT for secure data transfer.
- Non-Governmental Organisations: The author explicitly states that they have no interest in exposing information related to governments, cities, or police services. This could imply a focus on private corporations or other non-governmental entities. There could be some fear in targeting victims that have a robust cyber defence capability, or this could simply be a tactic to throw off such potential governmental targets off the scent.
- Selective Exposure: They threaten to publish the names of non-responsive companies on "this page", indicating a tactic of public exposure to pressure their targets. The actual publication of data seems reserved for those who do not agree to their terms, suggesting a sort of calculated and selective targeting strategy.
- Selective Targeting of Larger Organisations: The mention of a negotiation process and the focus on a fairly specialised piece of software might suggest a preference for targeting larger organisations. These entities would likely have more to lose in a data breach and might be more willing and able to pay a ransom.
- English-speaking Companies: The message is written in English, suggesting that their targets are likely in English-speaking regions or global corporations where English is commonly used.
- Companies with Sensitive Data: As with most cybercriminals, the group likely targets organisations that handle sensitive data. The damage potential of a data breach (e.g., reputation damage, potential legal consequences, loss of customer trust, etc.) puts pressure on the victims to comply with the ransom demands.

9. Proof of Authenticity:

They mention providing a proof-of-concept ("OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE"). This implies they understand the need to prove the authenticity of their threats, likely based on experience from previous operations or to increase the veracity of their claims.

Proof of authenticity in this context refers to evidence that can convince the recipients of the message that the sender is indeed in possession of their data and has the means and intent to leak it, should their conditions not be met. Here are some elements in the text related to proof of authenticity:

- Mention of Specific Software: The author mentions the MoveIT product specifically, which could signal to a company using that software that they've been targeted by a group aware of their software usage.
- Offer to Provide Proof: The author writes, "our team will provide 10% proof of data we have and price to delete". This suggests they're ready to show a sample of the stolen data as proof of their claims, a common tactic in ransomware attacks.
- Random File Verification: In step 4, they offer the opportunity to ask for 2-3 random files as proof. This implies they're willing to show even more evidence if required.
- Timeline of Consequences: The author outlines a timeline and sequence of consequences that will follow if their instructions aren't adhered to, further asserting their authenticity and intention.
- Previous Reputation: The writer references a reputation for reliability, stating "we have not even one time not do as we promise". Though without external validation, this claim might be hard to accept at face value, it still serves as an attempt to project authenticity.
- Confidentiality Assurance: The assurance given that they don't wish to expose government, city, or police service data adds an element of selectivity to their operations, making their threats to other entities seem more credible.

10. Structured Organisation:

The use of a structured process with steps for response and escalation indicates an organised operation. This could imply a larger, more coordinated group, as opposed to a single individual acting alone.

- Division of Labour: The author refers to "our team" multiple times, suggesting that there's more than one person involved in these operations. There's likely a division of labour among the group members, with different individuals or teams responsible for different tasks (such as exploiting software vulnerabilities, communicating with victims, handling the ransom negotiation and payment, etc.).

- Defined Process: The message outlines a clear, step-by-step process for communication, negotiation, and actions to be taken if the demands are not met. This structured approach suggests an organised operation with predefined procedures.
- Communication Channels: The group seems to have defined channels for communication, with specific email addresses provided for contact and a "dedicated chat URL over TOR" mentioned for further discussions. This implies a level of technical sophistication and coordination.
- Long-Term Planning: The mention of specific future dates and actions if their conditions aren't met suggests long-term planning, another sign of a structured organisation.
- Specialisation: The focus on exploiting a specific software product and dealing with its users indicates a level of specialisation within the group. They likely have individuals who are experts in certain areas or tasks.
- Self-Presentation: The group presents itself as a professional organisation offering a "service". While this is a skewed portrayal given their criminal activities, it does imply an attempt at projecting an image of organisation and professionalism.

11. Appeal to Fear:

The writing uses explicit threats and deadlines to create a sense of urgency and fear. It's a common tactic in psychological manipulation and indicates an understanding of human psychology and persuasion techniques, albeit a basic one.

Appeal to fear is a type of persuasive strategy where fear is used to sway the audience into taking a desired action or accepting a particular viewpoint. In this passage, the author uses multiple tactics to instil fear in the reader:

- Threat of Exposure: The author threatens to release company data and specifically mentions the intent to publicly expose the company's name. The possibility of a public data breach can significantly damage a company's reputation and trustworthiness, making this a potent source of fear.
- Penetration Testing: By positioning themselves as a top organisation that offers "penetration testing service after the fact", the author introduces the fear of a security breach that has already occurred, playing on the recipient's fear of the unknown or uncontrolled situation.
- Deadline Pressure: The author establishes firm deadlines for response and action. The sense of urgency adds to the fear and pressure, making the recipient more likely to act exigently, possibly without thorough consideration or seeking proper advice.
- Inevitability of Consequences: The author outlines a series of steps that will be taken if their instructions are not followed, culminating in the public release of the victim's data. This inevitability of consequences, unless the victim complies, is designed to enhance the fear factor.

- Display of Power and Control: By dictating the terms, the author establishes a power dynamic where they are in control, and the victim is helpless. This imbalance can create fear and uncertainty, leading the victim to comply to regain some sense of control.
- Exclusivity of Threat: Claiming that they are "the only one who performs such attacks" although this assertion might not be wholly true, it serves to amplify the fear by suggesting that the recipients are up against an unprecedented threat that they are likely unprepared to handle.

12. Economic Motive:

The overall purpose of this message appears to be economic gain, as inferred from the discussion about price and the threat of publication of sensitive data if payment is not made. This could provide insights into the group's primary motivations.

- Ransom-Based Revenue: The primary economic motive is clear: the group offers a service to delete the stolen data for a price. This is a common model used by ransomware groups, who extort money by demanding payment in exchange for not releasing sensitive data.
- Threat of Exposure: The threat to publish the victim's data if the ransom isn't paid is also tied to economic motives. This added pressure can incentivise or pressure the victim to pay the ransom in order to avoid the potential financial and reputational harm that could come from having their data exposed.
- Selection of Targets: The fact that the group seems to be focusing on companies using a specific software product suggests they are targeting entities that are likely to have the means to pay. The larger and more financially stable a company is, the more likely they are to pay a ransom to prevent damage.
- Exclusion of Certain Entities: The group specifically states they have no interest in exposing information related to government, city, or police services. While the motive behind this isn't directly clear, it could be economic in nature. Entities like these might have more resources to trace the group or less likely to pay ransoms due to policies against such actions.

13. Professionalism:

Despite the language inaccuracies, there's a certain degree of “professionalism” displayed in the way the author lays out the process in detail, uses specific terminology, and promises certain standards (like providing proof of data, deleting data after payment, and even making video proofs). This may reflect an experienced group with a developed modus operandi.

- Establishing Authority: The use of terms such as "our team" and "we" is an attempt to present the group as a coordinated, organized entity with a division of labour and a hierarchy, which are characteristics typically associated with legitimate professional organizations.
- Formal Language and Structure: The passage is laid out in a step-by-step manner, much like a formal letter or an official announcement, which adds to the sense of professionalism. The group lays out a detailed process for victims to follow, indicating planning and organisation.
- Offering 'Services': They position themselves as a 'penetration testing service' organization, which is a legitimate profession in the cybersecurity industry. This could be a tactic to make their actions seem more professional and less criminal in nature.
- Reputation and Reliability: The author insists on their reliability, stating that they have always done as they promise. This is an attempt to portray a sense of professional reliability and trustworthiness.
- Disclaimers: They specify who they are willing to interact with (companies) and who they are not (media, researchers, government, city, or police service). This selective engagement imitates the professional boundaries that a business might set.

Whilst these elements could mimic certain aspects of “professionalism”, it's important to remember that this is a ransomware threat and inherently a criminal activity, exploiting fear and vulnerability for financial gain. The seeming professionalism is likely a manipulation tactic intended to legitimise their demands and make victims more likely to pay.

14. Emotional Manipulation:

The writer attempts to downplay the severity of their actions with phrases such as "relax because your data is safe" and "friendly CLOP," which contrasts with the inherent threat in the message. This could be an attempt to manipulate the emotions of the reader, creating a false sense of security or trying to establish an incongruous rapport.

Emotional manipulation is a form of psychological influence to exploit or control others through deceptive or abusive tactics. In the given passage, there are several ways in which the author attempts to emotionally manipulate their targets:

- Fear and Anxiety: The primary emotion that this message tries to evoke is fear. The threat of releasing sensitive data is intended to scare the recipient into compliance. The strict deadlines and the detailed process of data release are likely designed to heighten this sense of fear and urgency.
- False Reassurance: The message paradoxically provides reassurances amidst the threats. For instance, it claims, "relax because your data is safe". This is a form of manipulation, intending to confuse the recipient and make them believe that cooperation with the authors may lead to a safe resolution.

- Intimidation: The author uses an intimidating tone throughout the message, asserting control over the situation and showcasing their power. They dictate the terms and conditions, emphasising their position of dominance.
- Pressure and Stress: The author establishes a series of steps with associated deadlines. This tactic can induce stress and pressure, causing recipients to potentially rush their decisions or actions.
- Doubt and Guilt: The author employs tactics to sow doubt and guilt. For instance, they mention that if a company doesn't respond until a certain date, its name will be published, potentially inciting guilt over the perceived public embarrassment or harm to reputation.
- Relief: By saying they have erased all data of government, city, or police services, the author attempts to provide relief to such organisations, creating a contrast to the threat imposed on companies, thereby amplifying the impact on the victim.

15. Cultural References:

The phrase "measle dollars" is unusual and could possibly be a mistranslation or misinterpretation of a phrase from the writer's native language, indicating a specific cultural background.

- Use of Language: As previously mentioned, the writer uses English in a non-standard way. This may suggest that English is not their first language, potentially pointing to a non-Anglophone culture. However, this is speculative and should be taken with caution as it could also be a deliberate attempt to throw off investigators.
- Use of TOR Network: The writer's use of the TOR network for communication points to a culture of privacy, anonymity, and counter-surveillance that is common within certain technically capable, hacker, or cybercriminal communities.
- Ransomware Culture: The writer's approach aligns with common practices in the ransomware community (e.g., the detailed step-by-step process, the offer of proof, the use of deadlines). This could be seen as an indirect reference to the subculture of cybercrime and ransomware groups.

TTP Analysis:

TTP analysis based on perceived behaviours gathered from the note. This is purely based on the extortion note and not associated within any pre-existing determination or actual behaviour exhibited and attributed to the threat actor in the past or current operations.

1. Tactic: Initial Access, Technique: Phishing (T1566): While the text itself doesn't mention the method of initial compromise, phishing is a common method used by threat actors to gain initial access, and it could be the case here given their intended audience - companies using MOVEit software.

2. Tactic: Execution, Technique: User Execution (T1204): The group could have exploited user interaction (like clicking a link or opening a file) to execute their malicious payload.

3. Tactic: Persistence, Technique: Server Software Component (T1501): The threat actor seems to target MOVEit, a managed file transfer software. They may have achieved persistence by modifying or adding a component to this server software.

4. Tactic: Defense Evasion, Technique: Obfuscated Files or Information (T1027) and Deobfuscate/Decode Files or Information (T1140): The authors hint at using TOR for communication, suggesting they might use encryption or obfuscation techniques to evade detection.

5. Tactic: Discovery, Technique: System Network Configuration Discovery (T1016): The authors mention that they have already downloaded a lot of data, implying they might have conducted an internal reconnaissance to understand the network configuration of their target.

6. Tactic: Collection, Technique: Data from Information Repositories (T1213): The message suggests that the threat actor collects and exfiltrates data from targeted organisations as part of their operation.

7. Tactic: Impact, Technique: Data Encrypted for Impact (T1486): The threat actor appears to hold the victim's data and offers to delete it upon payment, hinting at possible encryption or other data manipulation.

Credits:
Cover Art: https://www.pexels.com/@anniroenkae/
Cl0p Ransom Note: Dominic Alvieri - @AlvieriD