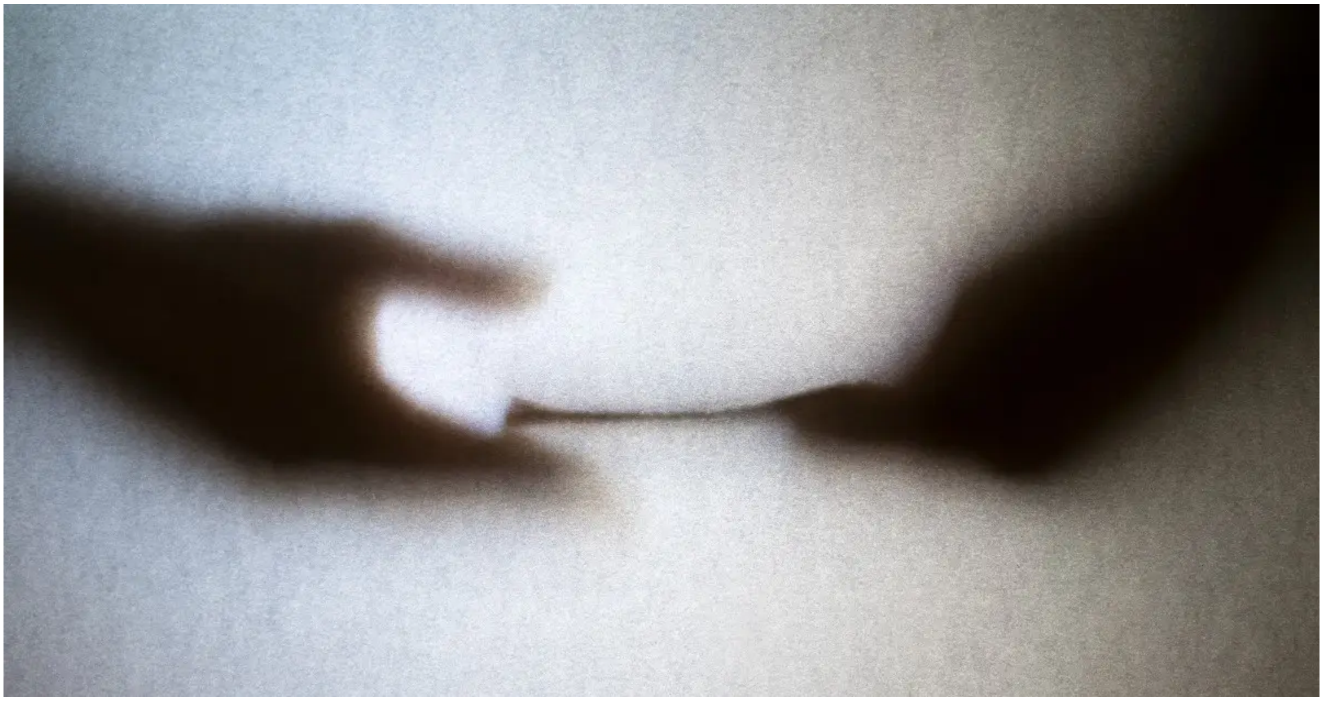
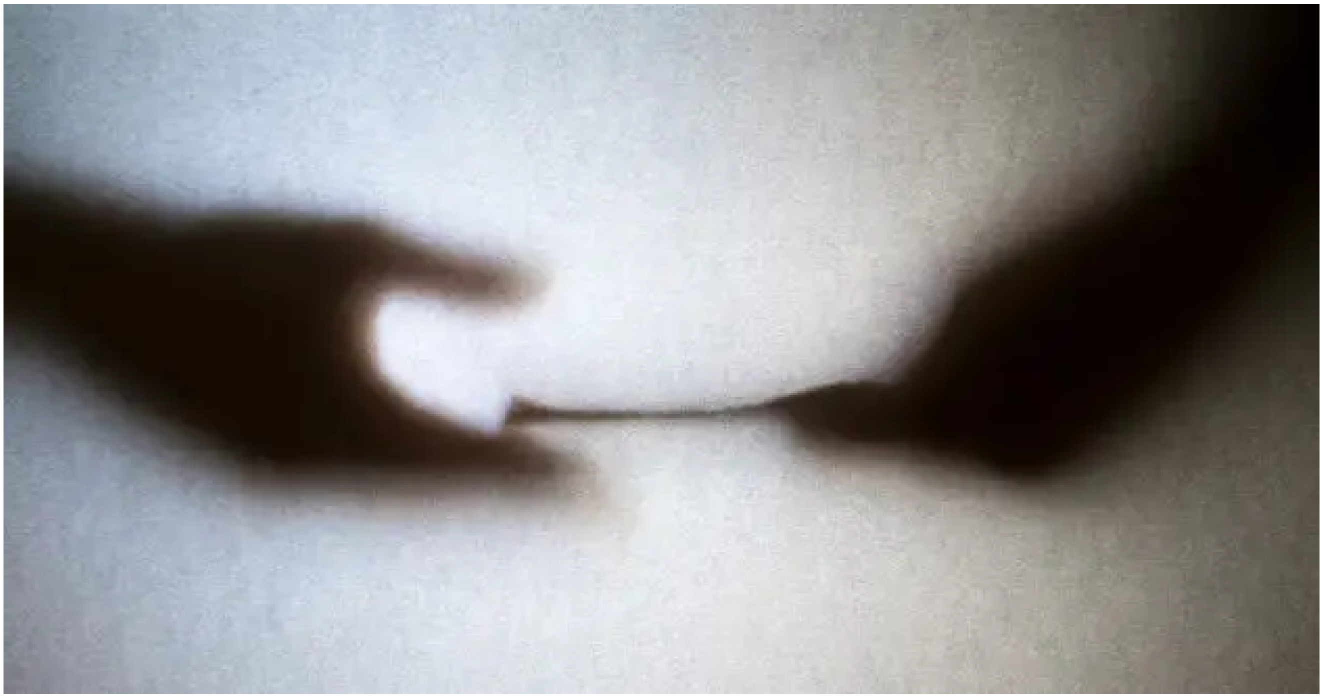
This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered

securityintelligence.com/posts/egregor-ransomware-negotiations-uncovered/



Home&nbsp/ Incident Response

This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered



Incident Response July 21, 2021

By Chris Caridi co-authored by Allison Wikoff 8 min read
Ransomware attacks are topping the charts as the most common attack type to target organizations with a constant drumbeat of attacks impacting industries across the board. In fact, IBM Security X-Force has seen a more than 10% increase in ransomware incident response requests compared to this time last year.

Ransomware is well on its way toward becoming a global billion-dollar enterprise – one that victims are funding. Attackers are operating like a well-oiled business industry, yielding high profits in a year that most businesses struggled. Why? The new ransomware business model is relentless, extortive and paying off.

IBM Security X-Force Threat Intelligence analysts, together with Cylera, an IoT and medical device security intelligence company that works with IBM Security to deliver IoMT solutions, have obtained and analyzed hours of chat correspondence and negotiations that occurred in December 2020 between the notorious Egregor ransomware actors, responsible for upwards of $80 million dollars in losses globally. The chat correspondence had negotiations with approximately 40 victim organizations they chatted with. The activity uncovered in these chat transcripts provides valuable insight into how some ransomware actors operate – from how they conduct ransom payment negotiations, to the strategies and operational structure they used.

Although law enforcement took action against Egregor operations in February 2021, this discovery provides the following insightful takeaways:

- **Defining the Ransom Demand** – Initial ransom amounts ranged from $100,000 to $35 million. The average initial ransom demanded was $5 million. During one negotiation, the threat actors indicated that their initial ransom demand is 5-10% of the potential estimated loss associated with a data leak.
- **Ransom Negotiations** – Several factors played a role in determining the final negotiated ransom amount or data leak outcome, including the operators' perception of the victim's ability and willingness to pay as well as the victim's negotiation strategies such as attempting to buy time and delay the payment.
- **Operational Structure** – The chats reveal a highly sophisticated organized crime group was behind Egregor operations. Numerous roles or teams were mentioned including the financial department, data manager, attackers/IT specialists, PR manager, publications manager and decryption tool master-maker.
- **Compassion with a Catch** – X-Force researchers maintain the operators of ransomware like Egregor are nefarious actors. However, the chat logs revealed a few glimpses of what could be perceived as empathy or practical consideration. During one negotiation, Egregor offered to provide the decryption key, in exchange for the organization publicly announcing that the group does not intentionally target hospitals or charities. In a chat with another victim, the threat actors discuss the hardships of COVID-19, even wishing the victim happy holidays.

What is ‘Egregor’?

The Egregor ransomware was first reported publicly in mid-2020, making it a relatively new entry into the criminal economy. Egregor operators work through an affiliate model, meaning a small group of actors run and maintain the Egregor code base and other actors purchase access to Egregor and use the malware on systems they infect. This model is best known as Ransomware as A Service (RaaS).

Many security analysts speculated that Egregor was the follow-up to the Maze ransomware, pointing to significant technical overlap between the two ransomware families after Maze’s threat actors declared retirement in November 2020. Egregor gained significant recognition in 2021 as affiliates shifted from Maze to using this new ransomware family and leaked stolen information from impacted organizations, extorting them in efforts to collect a ransom.

The impact of Egregor ransomware has been felt worldwide with an estimated $80 million dollars in profit through their operations against at least 150 organizations. Regarding victims, the highest number of reported cases was in the United States with infections clustered primarily within the manufacturing and retail industries. Some of the larger targets have included Barnes and Noble, Randstad, French logistics firm Gefco and video game companies Ubisoft and Crytek.

In February 2021, a joint French and Ukrainian law enforcement operation disrupted Egregor’s infrastructure and arrested multiple Egregor associates. As of the time of this publication, X-Force researchers are not aware of active Egregor intrusions.

What’s in a Ransom?

After reviewing elaborate chat logs between Egregor actors and representatives from victimized organizations, we obtained interesting insights about how the ransom amount was fixed and the overall negotiation process. In a common flow of events, upon initial contact with victims, X-Force and Cylera analysts observed Egregor ransomware actors making an initial demand for a ransom payment that depended on the victim and their perceived ability to pay.

Analysis of approximately 50 ransom negotiations in Egregor chat logs from December 2020 shows that ransom demands varied wildly.

Average initial ransom demand	$5,024,000
Average ransom payment	$387,700
Highest initial ransom demand	$35,000,000

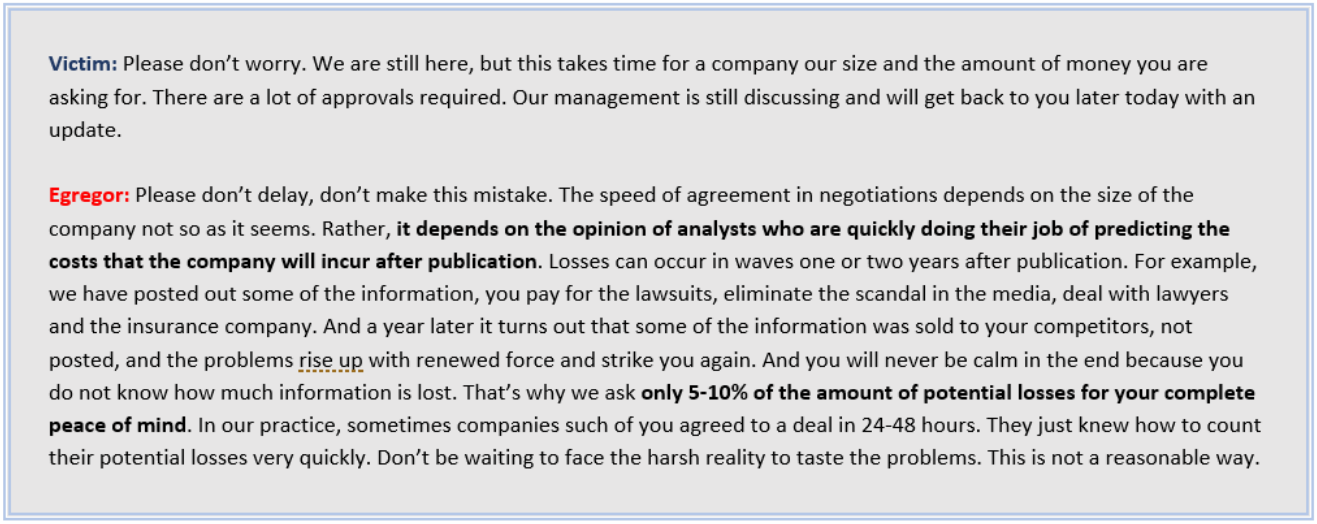
Lowest initial ransom demand	$100,000
Sum of all ransom demands	$226,080,000

Figure 1: Egregor ransom demands and average ransom payment, in U.S. dollars, December 2020 (Source: IBM X-Force/Cylera)

How each ransom amount was determined was likely a judgment call based on a combination of publicly available information about the victim along with what the operators perceived the victim could afford to pay.

Ultimately, researchers observed that the threat actors appeared to strike a balance between a victim's ability and willingness to pay while considering multiple additional factors. In one negotiation, Egregor actors gave the victim organization an initial ransom demand of $1.7 million. Through some negotiating by the victim, explaining they were a small company, Egregor operators decreased the ransom to $1 million.

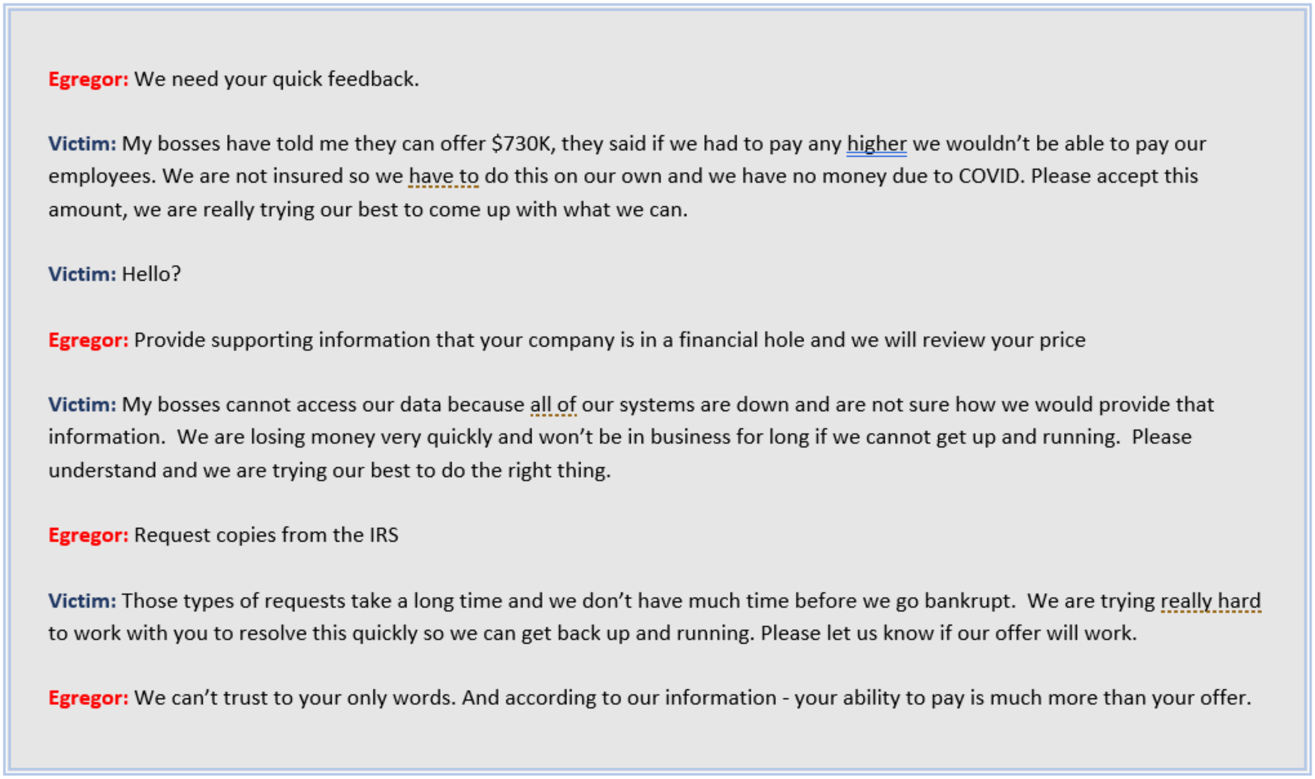
In another example, Egregor operators alluded to using an analyst associated with Egregor operations to estimate a victim's total loss if they were to forego paying the ransom and instead suffer a data leak. The attacker's comments indicate that the initial ransom demand is 5-10% of that estimated loss.



Victim: Please don't worry. We are still here, but this takes time for a company our size and the amount of money you are asking for. There are a lot of approvals required. Our management is still discussing and will get back to you later today with an update.

Egregor: Please don't delay, don't make this mistake. The speed of agreement in negotiations depends on the size of the company not so as it seems. Rather, **it depends on the opinion of analysts who are quickly doing their job of predicting the costs that the company will incur after publication**. Losses can occur in waves one or two years after publication. For example, we have posted out some of the information, you pay for the lawsuits, eliminate the scandal in the media, deal with lawyers and the insurance company. And a year later it turns out that some of the information was sold to your competitors, not posted, and the problems rise up with renewed force and strike you again. And you will never be calm in the end because you do not know how much information is lost. That's why we ask **only 5-10% of the amount of potential losses for your complete peace of mind**. In our practice, sometimes companies such of you agreed to a deal in 24-48 hours. They just knew how to count their potential losses very quickly. Don't be waiting to face the harsh reality to taste the problems. This is not a reasonable way.

In another example, a victim pleads with the attackers for a lower ransom price due to the inability to pay as a result of COVID-19 pandemic-related hardships. The Egregor actors demanded proof from the victim that they were experiencing financial hardships, even going as far as requesting information from the IRS.



Egregor: We need your quick feedback.

Victim: My bosses have told me they can offer $730K, they said if we had to pay any higher we wouldn't be able to pay our employees. We are not insured so we have to do this on our own and we have no money due to COVID. Please accept this amount, we are really trying our best to come up with what we can.

Victim: Hello?

Egregor: Provide supporting information that your company is in a financial hole and we will review your price

Victim: My bosses cannot access our data because all of our systems are down and are not sure how we would provide that information. We are losing money very quickly and won't be in business for long if we cannot get up and running. Please understand and we are trying our best to do the right thing.

Egregor: Request copies from the IRS

Victim: Those types of requests take a long time and we don't have much time before we go bankrupt. We are trying really hard to work with you to resolve this quickly so we can get back up and running. Please let us know if our offer will work.

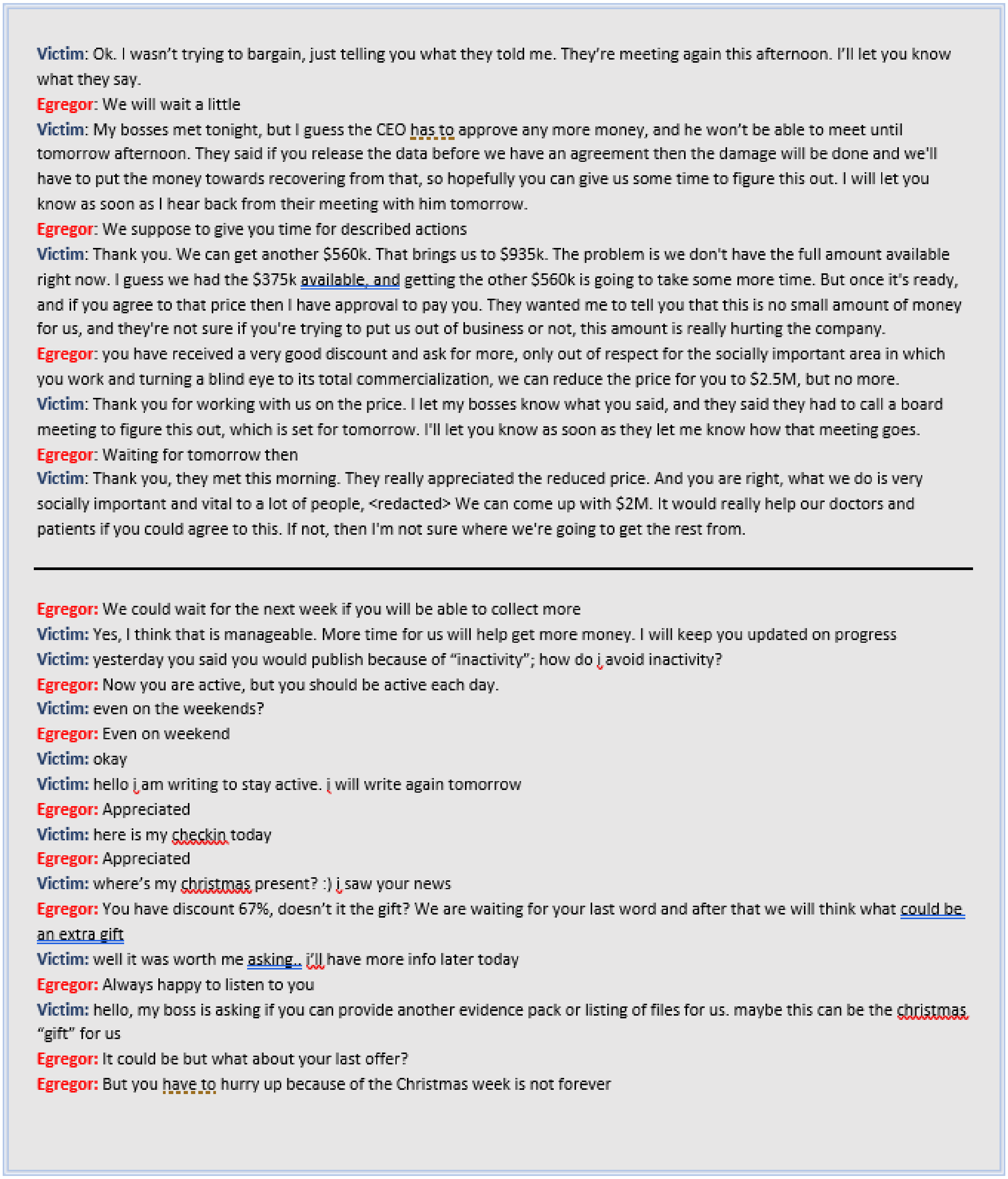
Egregor: We can't trust to your only words. And according to our information - your ability to pay is much more than your offer.

Buying Time: A Victim's Strategy

Deciding whether to pay and negotiating with the attackers is a hotly contested endeavor in the security community. Both paying a ransom or deciding not to pay carry consequences. We encourage organizations to review X-Force's Definitive Guide to Ransomware, which lists the main topics companies should consider when the question arises as to whether they should pay a ransom.

Our review of the Egregor chat logs provides some insight into what mitigation or ransom reduction techniques could be effective if one is ever faced with a ransomware incident:

- **Using company size to discount the ransom:** In some cases, victims explained the size of their business with Egregor actors, which resulted in lower ransom demands.
- **Getting money and cryptocurrency takes time:** In other instances, analysts observed victims explaining the process for acquiring money to pay the ransom, which extended the time before the actors leaked information about the compromised organization.



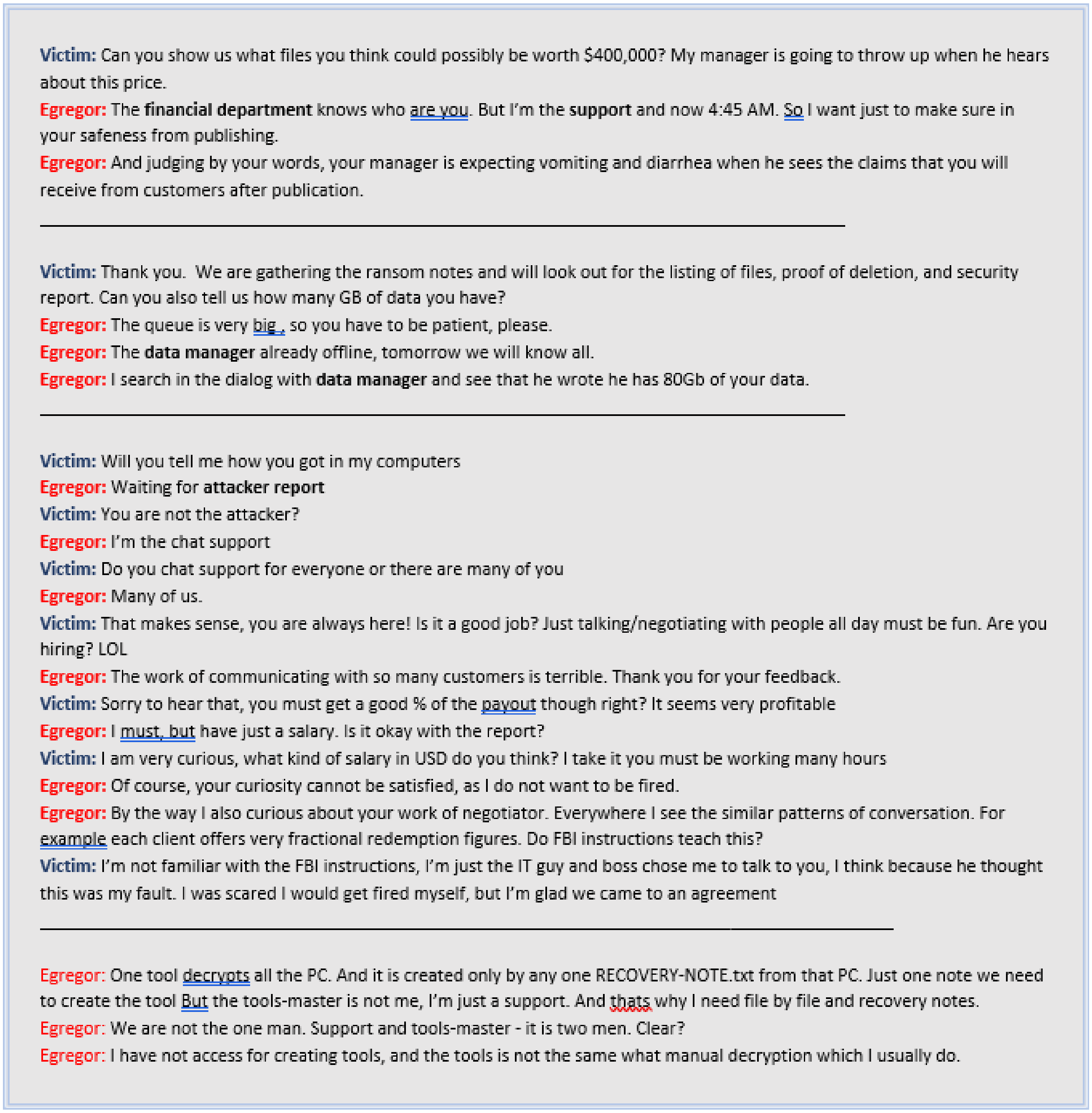
Victim: Ok. I wasn't trying to bargain, just telling you what they told me. They're meeting again this afternoon. I'll let you know what they say.
Egregor: We will wait a little
Victim: My bosses met tonight, but I guess the CEO has to approve any more money, and he won't be able to meet until tomorrow afternoon. They said if you release the data before we have an agreement then the damage will be done and we'll have to put the money towards recovering from that, so hopefully you can give us some time to figure this out. I will let you know as soon as I hear back from their meeting with him tomorrow.
Egregor: We suppose to give you time for described actions
Victim: Thank you. We can get another $560k. That brings us to $935k. The problem is we don't have the full amount available right now. I guess we had the $375k available, and getting the other $560k is going to take some more time. But once it's ready, and if you agree to that price then I have approval to pay you. They wanted me to tell you that this is no small amount of money for us, and they're not sure if you're trying to put us out of business or not, this amount is really hurting the company.
Egregor: you have received a very good discount and ask for more, only out of respect for the socially important area in which you work and turning a blind eye to its total commercialization, we can reduce the price for you to $2.5M, but no more.
Victim: Thank you for working with us on the price. I let my bosses know what you said, and they said they had to call a board meeting to figure this out, which is set for tomorrow. I'll let you know as soon as they let me know how that meeting goes.
Egregor: Waiting for tomorrow then
Victim: Thank you, they met this morning. They really appreciated the reduced price. And you are right, what we do is very socially important and vital to a lot of people, <redacted> We can come up with $2M. It would really help our doctors and patients if you could agree to this. If not, then I'm not sure where we're going to get the rest from.

Egregor: We could wait for the next week if you will be able to collect more
Victim: Yes, I think that is manageable. More time for us will help get more money. I will keep you updated on progress
Victim: yesterday you said you would publish because of "inactivity"; how do i avoid inactivity?
Egregor: Now you are active, but you should be active each day.
Victim: even on the weekends?
Egregor: Even on weekend
Victim: okay
Victim: hello i am writing to stay active. i will write again tomorrow
Egregor: Appreciated
Victim: here is my checkin today
Egregor: Appreciated
Victim: where's my christmas present? :) i saw your news
Egregor: You have discount 67%, doesn't it the gift? We are waiting for your last word and after that we will think what could be an extra gift
Victim: well it was worth me asking.. i'll have more info later today
Egregor: Always happy to listen to you
Victim: hello, my boss is asking if you can provide another evidence pack or listing of files for us. maybe this can be the christmas "gift" for us
Egregor: It could be but what about your last offer?
Egregor: But you have to hurry up because of the Christmas week is not forever

Well-Organized Cybercrime

While parsing through multiple conversations, X-Force and Cylera analysts noticed a variety of roles the threat actors alluded to during the negotiation process.

Egregor negotiators referred to themselves as “members of the support team” who only get a fixed salary and fear being fired. During discussions, they referred to other teams, including the financial department, data manager, attackers/IT specialists, PR manager, publications manager, and decryption tool master-maker.



Victim: Can you show us what files you think could possibly be worth $400,000? My manager is going to throw up when he hears about this price.
Egregor: The **financial department** knows who are you. But I'm the **support** and now 4:45 AM. So I want just to make sure in your safeness from publishing.
Egregor: And judging by your words, your manager is expecting vomiting and diarrhea when he sees the claims that you will receive from customers after publication.

Victim: Thank you. We are gathering the ransom notes and will look out for the listing of files, proof of deletion, and security report. Can you also tell us how many GB of data you have?
Egregor: The queue is very big , so you have to be patient, please.
Egregor: The **data manager** already offline, tomorrow we will know all.
Egregor: I search in the dialog with **data manager** and see that he wrote he has 80Gb of your data.

Victim: Will you tell me how you got in my computers
Egregor: Waiting for **attacker report**
Victim: You are not the attacker?
Egregor: I'm the chat support
Victim: Do you chat support for everyone or there are many of you
Egregor: Many of us.
Victim: That makes sense, you are always here! Is it a good job? Just talking/negotiating with people all day must be fun. Are you hiring? LOL
Egregor: The work of communicating with so many customers is terrible. Thank you for your feedback.
Victim: Sorry to hear that, you must get a good % of the payout though right? It seems very profitable
Egregor: I must, but have just a salary. Is it okay with the report?
Victim: I am very curious, what kind of salary in USD do you think? I take it you must be working many hours
Egregor: Of course, your curiosity cannot be satisfied, as I do not want to be fired.
Egregor: By the way I also curious about your work of negotiator. Everywhere I see the similar patterns of conversation. For example each client offers very fractional redemption figures. Do FBI instructions teach this?
Victim: I'm not familiar with the FBI instructions, I'm just the IT guy and boss chose me to talk to you, I think because he thought this was my fault. I was scared I would get fired myself, but I'm glad we came to an agreement

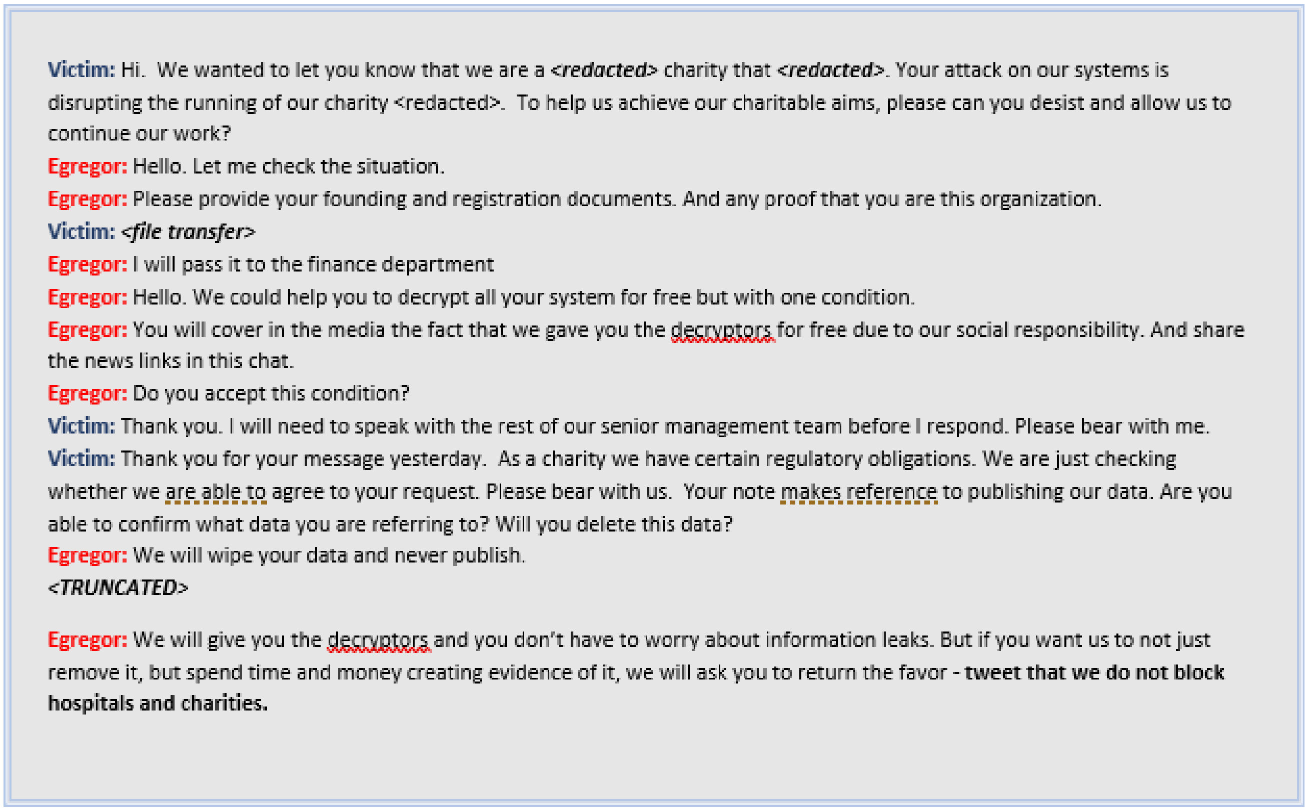
---

Egregor: One tool decrypts all the PC. And it is created only by any one RECOVERY-NOTE.txt from that PC. Just one note we need to create the tool But the tools-master is not me, I'm just a support. And thats why I need file by file and recovery notes.
Egregor: We are not the one man. Support and tools-master - it is two men. Clear?
Egregor: I have not access for creating tools, and the tools is not the same what manual decryption which I usually do.

Operators with a Heart?

Despite the intention of stealing millions of dollars from victims, the attackers have backed off from their demands in some circumstances if they believed they could receive positive press for doing so.

In one instance, X-Force and Cylera analysts observed negotiations between Egregor and a charity. After a long conversation between the victim organization and Egregor operators, Egregor offered to provide the decryption key, asking that the organization publicly announce that the group does not intentionally target hospitals or charities.



Victim: Hi. We wanted to let you know that we are a *<redacted>* charity that *<redacted>*. Your attack on our systems is disrupting the running of our charity <redacted>. To help us achieve our charitable aims, please can you desist and allow us to continue our work?
Egregor: Hello. Let me check the situation.
Egregor: Please provide your founding and registration documents. And any proof that you are this organization.
Victim: *<file transfer>*
Egregor: I will pass it to the finance department
Egregor: Hello. We could help you to decrypt all your system for free but with one condition.
Egregor: You will cover in the media the fact that we gave you the decryptors for free due to our social responsibility. And share the news links in this chat.
Egregor: Do you accept this condition?
Victim: Thank you. I will need to speak with the rest of our senior management team before I respond. Please bear with me.
Victim: Thank you for your message yesterday. As a charity we have certain regulatory obligations. We are just checking whether we are able to agree to your request. Please bear with us. Your note makes reference to publishing our data. Are you able to confirm what data you are referring to? Will you delete this data?
Egregor: We will wipe your data and never publish.
<TRUNCATED>

Egregor: We will give you the decryptors and you don't have to worry about information leaks. But if you want us to not just remove it, but spend time and money creating evidence of it, we will ask you to return the favor - **tweet that we do not block hospitals and charities.**

In another ransom negotiation, the victim, a small U.S. dental practice, and Egregor support are discussing the hardships of 2020, specifically COVID-19.

Key Takeaways

Despite the holiday wishes and reduced ransom in some instances, the December 2020 chat logs obtained by X-Force and Cylera demonstrate that many Egregor attacks were a successful, ruthless criminal operation. Although the threat actors have ceased from using the Egregor ransomware family specifically, and only since the law enforcement activity in February 2021, X-Force analysts believe that a new infrastructure can be mounted and the same code can be used again in its original form or as modified code. Moreover, with these attacks yielding extremely high profits for those residing in less prosperous parts of the world, new ransomware families and gangs will continue to emerge and may take Egregor's place in the near future.

Ransomware attacks continue to be the top threat to organizations globally as this threat grows and expands its reach year over year. Yet, even in the face of sophisticated threats, there are actions companies can take that can help mitigate risks and minimize damage:

- **Establish and drill an incident response team.** Whether in-house or as a retained service, the formation of an incident response team and drilling the most relevant attack scenarios to your organization can make a big difference in attack outcomes and costs.
- **Establish and maintain offline backups.** Ensure you have files safely stored from attacker accessibility with read-only access. Also consider the use of offsite/cold storage solutions. The availability of backup files is a significant differentiator for organizations that can help recover from a ransomware attack.
- **Implement a strategy to prevent unauthorized data theft,** especially as it applies to uploading large amounts of data to legitimate cloud storage platforms that attackers can abuse. Consider blocking outbound traffic to unapproved cloud hosting services.
- **Employ user and entity behavior analytics to identify potential security incidents.** When triggered, assume a breach has taken place. Audit, monitor and quickly act on suspected abuse related to privileged accounts and groups.
- **Deploy multifactor authentication** on all remote access points into an enterprise network — with particular care given to secure or disable remote desktop protocol (RDP) access. Multiple ransomware attacks have been known to exploit weak RDP access to gain initial entry into a targeted network.
- **Use penetration testing to identify weak points** in enterprise networks and vulnerabilities that should be prioritized for patching. In particular, we recommend implementing mitigations for CVE-2019-19781, which multiple threat actors have used to gain initial entry into enterprises in 2020 and 2021 — including for ransomware attacks.
- **Consider prioritizing the immediate remediation,** as applicable, of the following frequently exploited software vulnerabilities:
    - CVE-2019-2725
    - CVE-2020-2021
    - CVE-2020-5902
    - CVE-2018-8453

VPN-related CVEs

- CVE-2019-11510
- CVE-2019-11539
- CVE-2018-13379
- CVE-2019-18935
- CVE-2021-22893

RDP

-
    - Restrict port access on TCP port 3389
    - Apply multifactor authentication to remote access logins
    - Remediate RDP vulnerabilities such as Windows RDP CVE-2019-0708 (BlueKeep)
    - CVE-2020-3427
    - CVE-2020-0610
    - CVE-2020-0609
- **Segment networks** according to the data they host.
- **Encrypt** the data most likely to be stolen in an attack.
- **Consider adopting a Zero Trust approach and framework** to better control what users can access and potentially halt an attack in its tracks.

If you are experiencing cybersecurity issues or an incident, contact X-Force to help: U.S. Hotline: 1-888-241-9812 | Global Hotline: +(001) 312-212-8034. Learn more about X-Force's threat intelligence and incident response services.

Chris Caridi
Strategic Cyber Threat Analyst, IBM X-Force IRIS

Chris Caridi is a cyber threat intelligence analyst with IBM X-Force Incident Response and Intelligence Services (IRIS). Chris brings 9 years of experience w...