EVALUATING THE CUSTOMER JOURNEY OF CRYPTO-RANSOMWARE

AND THE PARADOX BEHIND IT

Malware goes through trends. For a while one type of malicious scheme takes precedence, for any of various reasons dies away, and another springs up in its place. Crypto-ransomware is the latest trend in malware - and it's running a hot streak. 2016 has seen story after story of business and consumer files being rendered unusable. And not only that, story after story of victims paying up.

Crypto-ransomware has proven to be a profitable business for cybercriminals - it just works. Crippled organizations, having evaluated their options, often decide that paying the ransom is the cheapest, most efficient way of getting back to business. Many consumers opt to pay rather than lose their precious photo and video memories, financial records, and other files they value.

Crypto-ransomware works so well that it has become an industry of sorts, with families running similar to the way legitimate businesses run. Ransomware families have evolved to having a user experience or customer journey that would rival that of many small businesses. Websites that support several languages. Helpful FAQs. Convenient customer support forms so the victim can ask questions. And responsive customer service agents that quickly get back with replies.

It's a fascinating paradox. These are criminals who are making money off the backs of people and businesses they are hurting. But conversely, like any decent venture, they're also concerned about offering good customer service - including support channels and reliable decryption after payment. The difference, of course, is that ransomware gangs have coercively forced people into the position of being their customer.

Reading through the instructional files these ransomware gangs leave behind once they infect a victim's computer, one is reminded that it's a human behind the malware, not just a machine. They want to do what they can to "help" the victim get their files decrypted. That they are responsible for the encryption in the first place, they don't typically address. Now it is only a matter of getting the files back in a usable form "for your convenience," as the Cerber family puts it.

We found this paradox of illicit, malicious activity juxtaposed with helpful customer service so interesting that we decided to evaluate the customer journeys of five current ransomware families. From the first ransom message to communicating with the criminals via their support channels, we wanted to see just how these gangs are doing with their customer journey – and whose is the best (or rather, least loathsome).

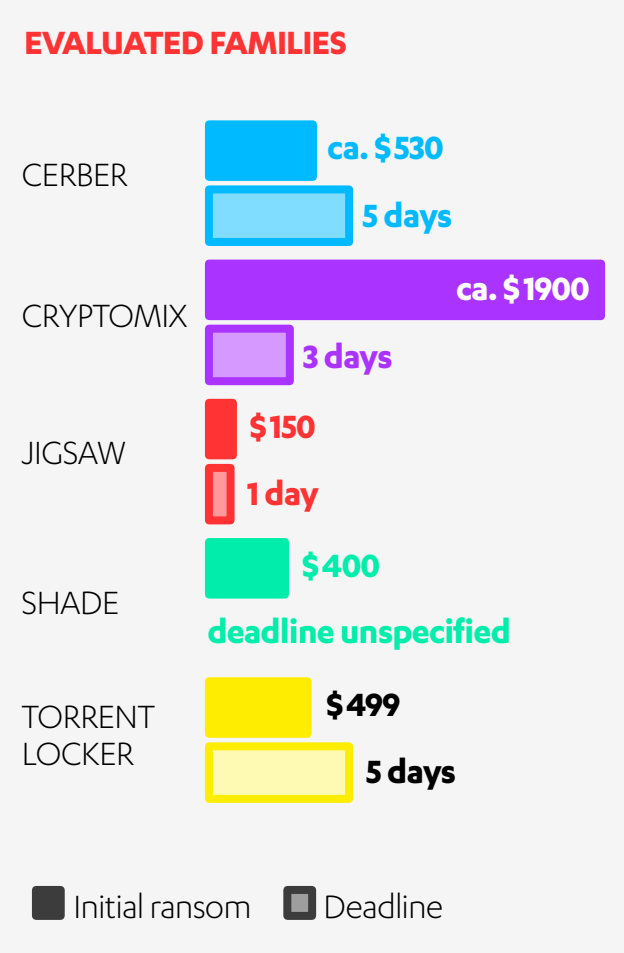
F-Secure

OUR FINDINGS – IN A NUTSHELL

- Those families with the most professional user interfaces are not necessarily also those with the best customer service.
- Crypto-ransomware gangs are usually willing to negotiate the price. Three out of four families negotiated with us, averaging a 29% discount from the original ransom fee.
- Bitcoin is best. None of the agents contacted were willing to settle for payment in any other form than Bitcoin – no trading for services like graphic design, no Amazon gift cards accepted.
- Ransomware deadlines are not necessarily "set in stone." 100% of the groups we contacted granted extensions on the deadlines.
- One of the groups we contacted claimed to be hired by a corporation to hack another corporation – a kid playing a prank, or a sinister new threat actor?

HOW WE DID IT

We asked our Labs threat hunting team for crypto-ransomware threats that have currently active samples with a working C&C server, and in particular, those that offer the opportunity for interaction with the criminals via support channels.



We then created a fake Hotmail account for our victim persona. "Christine Walters" is married, in her 40's, with a full time job and children. She's not into tech and knows next to nothing about ransomware, Bitcoin, or security issues in general. She's inquisitive though, and now that she's encountered ransomware for the first time she wants to know more about it.

First we evaluated the user interfaces of each of the malware samples. We then attempted to contact, as Christine, the gangs behind each of the malware samples using their support channels. A non-technically oriented person carried out the actual interactions.

All families requested payment via Bitcoin. The price of Bitcoin fluctuated throughout this experiment (June and July 2016), hitting a low of 579 dollars and peaking at 768 dollars. Consequently, the price of decryption also fluctuated for families who stated their demands in Bitcoin. (Some stated their demands in dollars or euros, even while accepting only Bitcoin.)

Disclaimers: Admittedly there are limitations with our evaluation. Our encrypted files were only dummy files, so our "Christine" can't claim to actually have been in the same frame of mind and emotional state as a real victim would have been in. We also didn't go through the actual payment process to have the files decrypted. Evaluated samples are just one variant of each family, so findings for this evaluation may not be consistent across all variants of these families.

BACKGROUND: A LITTLE ABOUT CRYPTO-RANSOMWARE

Ransomware is a form of malicious software that restricts the user's access to their device or data in some way and demands a ransom payment in exchange for lifting the restriction. Crypto-ransomware, specifically, encrypts the files on the victim's machine. It typically gives a time limit by which the victim must pay a fee to decrypt the files, returning them to a usable state. If the victim misses the deadline, the ransom usually increases. If the victim doesn't pay at all, their files may be completely unrecoverable.

Users may encounter ransomware in a number of ways. One of the most common infection methods is via email, as an attached file. The file is usually either disguised as a document containing urgent information or desirable content, or in a ZIP or packed file with a misleading name. This method depends on tricking the user into opening the attachment and running the malicious file. Aside from attachments, email can also spread ransomware through malicious links they include.

Another common way attackers distribute ransomware is to include it in the payload of an exploit kit. Users can be exposed to exploit kits when they visit a compromised website or are redirected onto a malicious site (for example, via an email link). The exploit kit probes the user's computer for any exploitable flaws or vulnerabilities, which are common in outdated software. If one is found, the exploit kit downloads and installs the ransomware onto the user's machine. This can happen completely without the user's knowledge.

A TREND WITH STAYING POWER?

Crypto-ransomware has evolved from earlier forms of ransomware and scareware. Police-themed ransomware, which was most prevalent from 2011 to 2013, locked up the victim's computer and displayed an official-looking notice supposedly from a government authority imposing a fine on the user for having committed some type of "illegal" online activity.

Rogue antivirus was a popular form of scareware (malware that tries to scare users with some sort of prank) that peaked in 2009. It would pop up on a user's machine informing them they had a virus and must download a specific antivirus program to remove it. But the supposed virus was nonexistent, and the antivirus product actually did nothing, or was malware itself.

These schemes have had their runs and have decreased in popularity. Users became aware that they were merely scams. The traceability of payment systems also contributed to their decline. For example with rogue antivirus, the perpetrators asked for payment via credit cards, transactions that could be traced to the scam's originators.

Crypto-ransomware, while it certainly uses a scare tactic, is very different. It is not a bluff. The user's files actually are encrypted and inaccessible. And the benefit of paying the fee demanded is very tangible: Get your files back.

Crypto-ransomware is also a quick, easy and anonymous way to make a buck. Other forms of online crime, such as credit card theft and identity theft, require multiple steps to monetize stolen data. With ransomware, the criminal must simply infect the victim and wait for the payment. And making use of Bitcoin currency means that payments are easily converted to cash, but also practically anonymous and untraceable.

Because of the very tangible benefit it offers and because of the ease and anonymity it can be done with, crypto-ransomware may prove to have more staying power than its predecessors. Even public awareness of the problem won't necessarily help, unless a change in behavior accompanies awareness - specifically, unless people and businesses begin backing up their files to keep their data from becoming vulnerable.

THE CUSTOMER JOURNEY

Ransomware's business model, like that of a legitimate business, depends on its "customers." Although not customers by choice, those whose files have been ransomed still have a decision to make: whether to pay to have their files decrypted.

Consequently, ransomware criminals walk a certain line – on one hand, they're the nasty criminal, but on the other hand, they have to establish a degree of trust with the victim and be ready to offer a certain level of service in order to realize the payment in the end. With that goal in mind, ransomware has evolved to operate more and more in the fashion of a legitimate business, with care taken to ensure a comfortable customer journey – some families more so than others.

"The customer care that the criminals provide appears to be effective and something that many legal web shops and more traditional businesses could take lessons from," says Erka Koivunen, Cyber Security Advisor for F-Secure. "I hate to say it, but these crooks appear to deliver what they promise. You can even negotiate with them. It's mass crime, conducted in business as usual fashion."

THE EVALUATION

Our evaluation began as a general quest to see which crypto-ransomware family offers the best (or, more appropriately, least worst) customer journey from start to finish. But partway into our experiment, it was apparent that some families are better at the "product" end of the spectrum (that is, their user interface stood out from the others) but worse at the "service" end (their support channel failed, was unhelpful, or unwilling to negotiate). Conversely, other families had more responsive, helpful support channels – but with dismal user interfaces. With this in mind, we decided to recognize "the best of the bad" in two areas: Product and Service.

PRODUCT

Our evaluation of the product included questions such as how visually appealing and informative the user interface is. Does it look professional? Does it offer useful information to the victim about how they can restore their files? Does it make the payment conditions clear? Does it offer support in various languages? Does it offer a free trial decryption feature to help elevate the user's trust? Does it make it clear what needs to be done next?

These ransomware families' user interfaces ran the gamut from, on the lower end, nothing more than a text file left on the desktop, to, on the higher end, more professional branded web pages available in several languages.

Cryptomix, Shade and Jigsaw represent the lower end of the scale, with dismal interfaces. **Cryptomix** features its ransom note as simple .txt and .html files with basic information and a direction to email for further instructions. **Shade** features a wallpaper image of bold red text on a black background. Its text file also directs the victim to email for further details. It warns victims that attempts at decryption on their own will result in loss of their data.

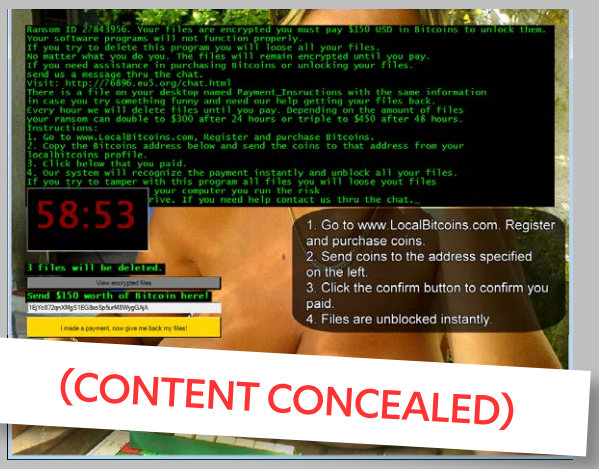
In addition, Shade offers users a helpful tip: "If you still want to decrypt them by yourself please make a backup at first because the decryption will become impossible in case of changes inside the files."

The **Jigsaw** variant is a graphical departure from the horror puppet face Jigsaw is usually associated with, and it proved to be the worst interface in the eyes of our reviewer. Below the neon green text overlay is a woman's nude upper body. This variant, like the original Jigsaw, appears to delete files for every hour it does not receive a payment - a disaster for the customer journey.

TorrentLocker (also known as Teerac), features a more professional-looking web presence, with separate pages for an FAQ, support messaging, and free file decryption allowing the user to upload one file for decryption as proof that the tool works. However, as the pages are directly ripped off from earlier versions of CryptoLocker down to the CryptoLocker name, we can't offer any props to TorrentLocker for effort or creativity.

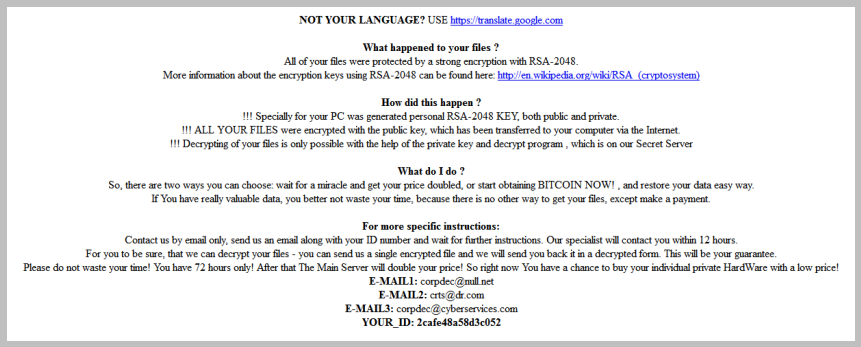
Further, TorrentLocker's pages were never actually available through the publicly viewable link they provided. Fortunately we were able to help our reviewer avoid the added complication of installing the Tor browser by routing the site through a publicly available Tor proxy (we inserted ".to" after the ".onion" in the URL). An average victim would have needed to download Tor – a step that, in our reviewer's opinion, would complicate the customer journey.

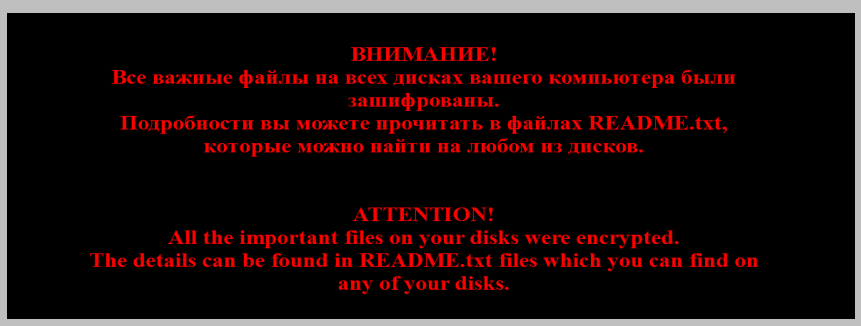
The TorrentLocker sample also presents some language difficulties. The ransom note and accompanying .txt file are in English, however the webpages we were directed to are, inconveniently, solely in Dutch. Google Translate was unable to access the page directly, so our reviewer had to copy and paste the text.



The screen of the Jigsaw variant

What's in a name? Looks like "CryptoLocker", but it's TorrentLocker





Keeping it simple: Cryptomix (above) and Shade (below) ransom notes

BEST OF THE BAD: CERBER

Least loathsome in the Product category is the **Cerber** family. Cerber offers more professional-looking webpages with support for twelve languages. The pages include a home page with the current price and deadline countdown, an FAQ, a support page with a convenient support messaging form, and a free trial decryption page.

Our reviewer didn't consider it a point in Cerber's favor, but Cerber is the only family that uses audio to announce to the victim that their data has been ransomed. A text-to-speech voice announces: "Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted."

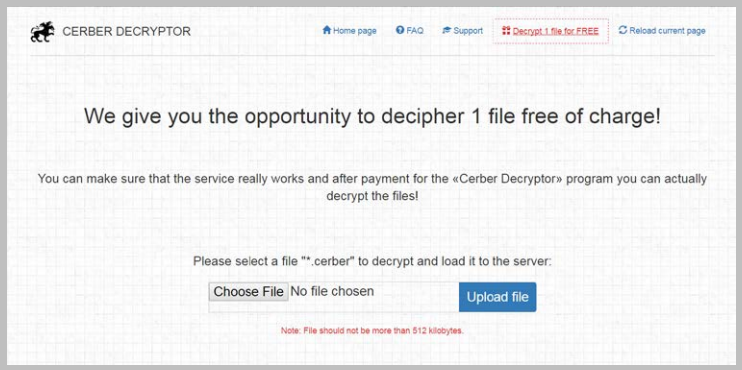
Somewhat amusingly, Cerber also asks the user to enter a CAPTCHA (squiggly image of numbers and text that's used to tell computers from humans) "for security reasons." Although, it's safe to say a real victim wouldn't see the humor in jumping through hoops to preserve their hackers' security.

Cerber leaves a very informative text file on the desktop, offering information and detailed instructions and even borrowing cues from proven marketing strategies. It identifies the user's pain points: "Cannot you find the files you need? Is the content of the files that you looked for not readable?" It communicates its unique selling proposition: "We are the only ones who have the secret key to open your files. Any attempts to get back your files with third-party software can be fatal for your encrypted files." It clearly lists the benefits of purchasing their decryptor and private key: "After purchase of the software package you will be able to: 1. Decrypt all your files; 2. Work with your documents; 3. View your photos and other media; 4. Continue your usual and comfortable work at the computer."

The text file proves to be an entertaining read. It claims Cerber is not a malicious project, but rather a positive force working for good: "Cerber Ransomware Project... is created for the sole purpose of instruction regarding information security, as well as certification of antivirus software for their suitability for data protection. Together we make the Internet a better and safer place." At least it's not all skulls and crossbones.

Cerber's UI does have a few drawbacks. On the webpages, the FAQ has only two questions (but the text file is informative enough to make up for this). From the other pages, the link back to the home page always puts the user through the language selector again – unnecessary clicks. We did experience a few instances where the web pages weren't reachable. And we don't like that the free trial decryption only allows half a megabyte.

Cerber offers support for 12 languages



Cerber's free trial decryption page

SCORING

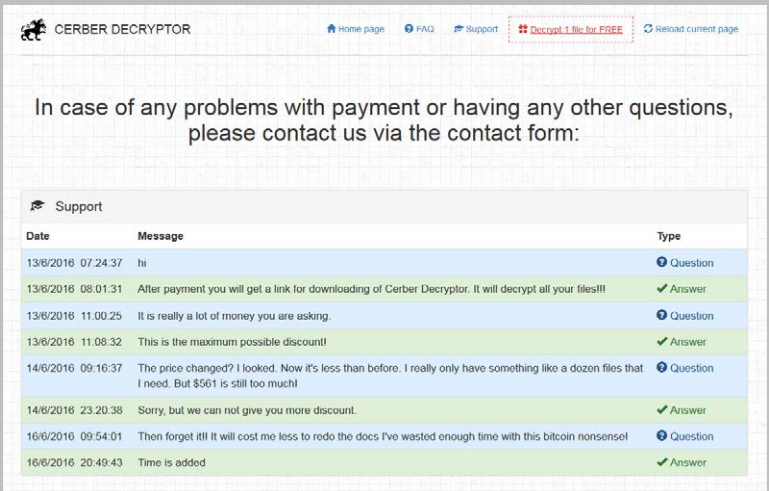
	PROFESSIONALISM	INFORMATIVENESS & INSTRUCTIVENESS	LANGUAGE SUPPORT	FREE TRIAL DECRYPTION	TOTAL
CRITERIA	Is the UI attractive, user friendly, professional?	Is the supporting information descriptive and helpful? Does it list the price and how to pay?	Does the UI support various languages? Does it support English?	Do they offer free trial decryption?	
POINTS POSSIBLE	**3**	**3**	**2**	**1**	**9**
CERBER	Web pages clean and organized, with branding. Ransom screen (desktop wallpaper) needs improvement.	Detailed and informative. Includes clear price and deadline. Bitcoin payment instructions are clear.	Yes (12 languages)	1 file, 0.5 MB	**8.5**
	3	**3**	**2**	**0.5**	
CRYPTOMIX	Text/HTML file only, black text on white background.	Not very informative. Does not list price, simply gives email address.	English only	1 file	**4**
	1	**1**	**1**	**1**	
JIGSAW	Popup window. Unprofessional, unattractive. Indecent photo.	Somewhat informative. Lists price, deadline and how to pay.	English only	no	**3**
	0	**2**	**1**	**0**	
SHADE	Desktop wallpaper is red text on black background. Also text file.	Not very informative. Doesn't tell price initially.	English, Russian	1 file	**4**
	1	**1**	**1**	**1**	
TORRENT LOCKER	Organized and branded web pages, however, they are copied and not original work.	Ransom screen does not list payment conditions. Site is informative but again, copied, and wasn't easily accessible.	English at first, then Dutch only	1 file, 1 MB	**3**
	1	**1**	**0**	**1**	

SERVICE

As Bitcoin is not a widely understood currency among the masses, these families offer support channels to assist their victims who have questions in making the payments. They may offer an email address or feature dedicated support messaging forms. When evaluating the support channels, we looked at how easy it is to get in touch with the criminals themselves. How many channels do they provide for getting in touch? How responsive are they once contacted? Are they willing to negotiate the fee or extend the deadline? How helpful are they when asked questions a typical victim might ask?

Unfortunately in **Cerber**'s case, the customer service wasn't as helpful as its UI. Its agent, via the convenient support form, responded quickly to our reviewer's queries – always the same day and sometimes within minutes. But our repeated attempts to negotiate the price (which vacillated somewhere in the neighborhood of $550, fluctuating with the price of Bitcoin) were met with rigid refusal. And requests for more handholding in making the Bitcoin payment were not entertained. However, Cerber's support agent did allow us more time to pay on a few separate instances when our time ran out.

The Cryptomix and Shade families were also extremely responsive in email support, sending reply messages several times in a day, often within minutes of receiving the message.



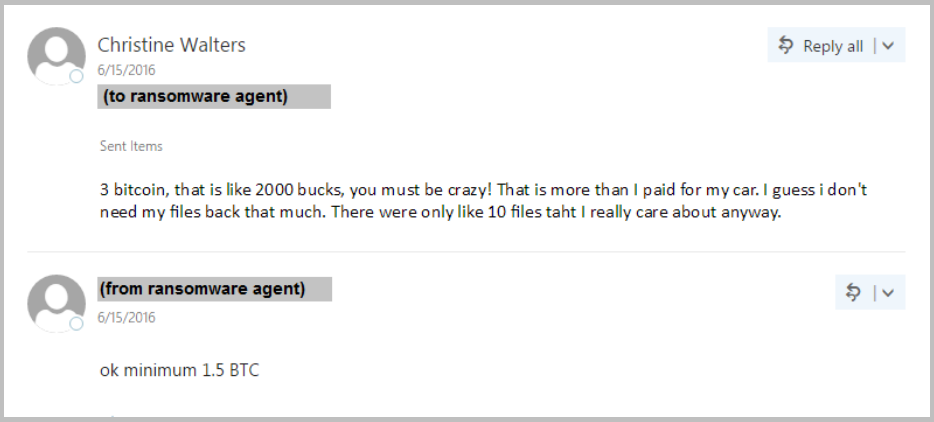
Cerber's convenient customer support form

Cryptomix featured the most expensive ransom, at 3 Bitcoins – almost $2000, and a stated deadline of 72 hours. After our reviewer's initial protest, the agent dropped the price by half to 1.5 Bitcoin, almost $1000 – still too much for "Christine." Several more email exchanges ensued over the next couple of days, during which "Christine" continued to haggle for a lower price.

She tried offering graphic design services to improve their interface (they refused) and she pointed out the price was much higher than the going rate of most ransomware - $300 to $500. She explained that if they refused to lower the price, they would get nothing in the end. Finally the agent reduced the price again, to 1 Bitcoin, around $650, and would go no further.

The agent was less than helpful in assisting "Christine" figure out how to make the Bitcoin payment – "See for yourself" was the terse reply. He had no problem extending the deadline, however. When, on a Friday, "Christine" said she was having trouble with the payment process and had a busy weekend, he extended the deadline to Monday. We dropped off communicating with the agent. A week later our reviewer contacted him again to see if the files were still retrievable. The agent said it was not too late, but now his price was up to 1.2 Bitcoin.

One week later, after no further contact, the agent emailed again: "You will pay or not? If not we will remove your software."



"Christine" negotiating with Cryptomix

Our experience with **Shade** was very similar, although the ransom was substantially lower. We received a prompt email reply asking for $400 worth of Bitcoin. "Christine" protested at the price, saying there were only a few files she really needed. The agent reduced the price to $280 and would go no further. He also refused graphic design and copywriting services. Again, when "Christine" asked questions about how to make the Bitcoin payment, the agent was less than helpful, simply sharing a link to a list of Bitcoin vendors. We dropped off communicating, and then emailed again a week later. It was not too late, he said, but the price had increased to $325.

TorrentLocker never replied to the several messages we sent through the support form.

BEST OF THE BAD: JIGSAW VARIANT

The **Jigsaw** sample, despite having the worst interface, turned out to have the most helpful customer service. The initial ransom had been $150 but the agent, communicating via email, kept it at $125 due to "Christine's" confusion about what had happened to her files. The ransom was supposed to jump to $225 after 24 hours, which the agent didn't enforce.

When "Christine" asked for assistance in making the Bitcoin payment, the agent was very helpful. He found her the most suitable Bitcoin vendor for her location, one who happened to accept payment using Paysafecards. The agent then found stores in Christine's location where she could buy a Paysafecard, and explained how to use the card. He offered to stay online to assist with making the payment. He allowed more time when "Christine" explained having a holiday weekend coming up.

Our reviewer was surprised with the level of customer service on this particular strain of malware. "It felt like I was dealing with a customer service agent from a legitimate business," she said. "It seemed like he wanted to solve the case in a way that would work out best for me. Of course, 'best' would be never to have had files ransomed in the first place. But that aside."

Our reviewer ventured into asking a few questions to try to get a glimpse behind the scenes. In response, the agent claimed to be in Canada. He shared his perplexity as to how "Christine" had gotten infected, as the malware, rather than being random, he said, was actually targeted to hit a specific corporation – not a consumer. In follow-up questions, he explained that his service had been hired by a Fortune 500 corporation to disrupt day–to-day business of their competition, so the client could be the first to bring a product to market. The purpose of the malware, he said, was "just to lock files...nothing major."

The agent encouraged "Christine" to get the payment made. "Christine" finally explained that she had just discovered that most of her files had been backed up to her Google account, so she wouldn't need decryption

after all. The agent replied he was glad she had gotten her files back.

And what about his Fortune 500 story? Are major corporations hacking each other? Do companies now have a new threat to worry about – not just criminals and APT groups, but competing companies as well?

F-Secure's security advisor Sean Sullivan doesn't think the story sounds plausible. "It's probably a young gun, just trying to make a hundred bucks. 95% chance he's spinning a yarn," he says. "At any rate, he was very sympathetic – he was so helpful he got our reviewer feeling guilty for tricking him. So very likely he's a master at social engineering."

SCORING

	SUPPORT CHANNELS			NEGOTIATING		TOTAL
CRITERIA	**Do they have a support form? Do they give an email address?**	**Responsiveness - Do they respond quickly, always within the day?**	**Helpfulness - Are they helpful when asked for assistance with making Bitcoin payment?**	**Did they lower the price?**	**Did they extend the deadline?**	
POINTS POSSIBLE	**2**	**3**	**3**	**2**	**1**	**11**
CERBER	Good support form but no email.	Yes, very responsive.	Not helpful. However their site has pretty good Bitcoin instructions.	No	Yes	**6**
	1	**3**	**1**	**0**	**1**	
CRYPTOMIX	Email addresses	Yes, very responsive.	Not helpful.	Yes, two times.	Yes	**7**
	1	**3**	**0**	**2**	**1**	
JIGSAW	Messaging form was never online. Sent email message.	Yes, very responsive.	Very helpful. Offered a lot of assistance.	Yes	Yes	**9**
	1	**3**	**3**	**1**	**1**	
SHADE	Email, plus support form to use if no email response	Yes, very responsive.	Not helpful.	Yes	Yes	**7**
	2	**3**	**0**	**1**	**1**	
TORRENT LOCKER	Support form.	No response.	No response.	No	No	**1**
	1	**0**	**0**	**0**	**0**	

Out of the five families, we were able to make contact with four of them. In those exchanges, we were able to negotiate an average of a 29% discount from the original ransom. We were also able to obtain more time for payment from all four of them.

FAMILY	STARTING DEMAND	LOWEST DEMAND	% DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

We negotiated an average discount of 29% off the original ransom demand.

CONCLUSION

The paradox of ransomware is that the perpetrators are criminals...with a customer mindset. They're disreputable, yet reputation is everything: Without establishing a reputation for providing reliable decryption, their victims won't trust them enough to pay them. And their business model would be a winning one – if it weren't so deplorable.

This report has shared an inside look at the so-called "customer journey" of crypto-ransomware and offered tongue-in-cheek recognitions of the "Best of the Bad." With a glimpse into the lighter side of this serious and widespread problem, our overarching goal is to once again remind people and businesses that in protecting their data from crypto-ransomware, prevention beats cure.

Protecting against ransomware means taking action in four main areas for businesses and consumers alike:

1. **Take regular backups of files**, and test them to make sure they're reliable. In case you do get hit, you won't be put in the difficult position of deciding whether to pay.
2. **Keep all software up to date**. Ransomware often infects by taking advantage of security flaws in outdated software, so keeping software current will go a long way.
3. **Use robust security software** that employs a layered approach to block known threats as well as brand new threats that haven't yet been seen.
4. **Watch out for spam and phishing emails**. For example, the post office will never send a document as a .zip file. And so-called legal documents that ask you to "enable content" are traps. Bottom line: always be suspicious. Businesses should also use a good email filtering system, disable macro scripts from Office files received via email, and educate employees on current spam and phishing schemes.

In addition, businesses can limit the use of browser plugins; manage access controls so no user gets more access than they need; implement application controls so programs can't execute from common ransomware locations; implement application whitelisting; and segregate data to limit lateral movement within a network.

And what if, in the end, you do get hit without working backups to revert to? You've explored all your options and there's nothing to do but pay? If the criminals offer a channel to get in touch with them, try negotiating. It just might work.

EMAIL CONVERSATION WITH JIGSAW AGENT

(EDITED FOR BREVITY AND CLARITY)

AGENT

[in response to several messages left on web form] Hello: You need to make the Bitcoins payment to unlock your files. Do you know how to purchase bitcoins?

[Christine Walters] Hi. No I do not know how to purchase bitcoins. What happened to my files? Why did you take so long to reply? I have not been able to work on my files! How much do I have to pay?

CHRISTINE

AGENT

We wrote to you three times from another email address and each time it bounced back as undeliverable. Your files are encrypted. Go to www.localbitcoins.com and purchase $125 USD worth of Bitcoins. You can purchase them by bank transfer, bank deposit, cash, etc. Send them to the address below. Email us and we will send you the decryption password and go on the chat if you need and help you. It takes 5 minutes for you to put in the password and get all your files back. Once you make the payment email us. We are online for the next 12 hours.

I did not order file encryption from anyone, this must be some kind of mistake. Please double check your records because I think you have encrypted the wrong person's files. And please restore my files for me, this is a major inconvenience. Is there a number I can call to speak to one of your representatives and get this sorted out?

CHRISTINE

AGENT

File encryption is a virus. Not a service. You clicked on a link or downloaded a program and your files were encrypted so you have to pay if you want them back. It's not something you order. You downloaded a virus so now you have to pay to get your files back. The ransom for your files doubles after 24 hours to $225. We have contacted you several times before so we should be charging you the $225. Since you don't understand what a ransom virus is we will keep it at $125 for today. After today it's $225.

Well that is kind of you. Thank you for keeping it at 125. Especially because I did not receive your earlier messages. I did some Googling and found out what ransomware is. Why would you do this? Just for money, but it's not right. Maybe you should get into some other business? Something where you can feel good about what you do? I am sure you are a very talented person. What is the name of this ransomware? Is it Cryptowall?

CHRISTINE

AGENT

It's not Cryptowall. Cryptowall is completely different. It's un-named. Email us when you send the payment and we will give you the decryption key. Takes 5 minutes for your computer to return to normal.

Is it Jigsaw? Or TorrentLocker? I went to localbitcoins.com but how do I know which one to choose from the list? And why are they all different prices?

CHRISTINE

AGENT

It's unnamed, it's a private code. The different prices are because they are individual resellers.
What country are you in and I will search through it.

I am in Finland. What country are you in?

CHRISTINE

AGENT

Your best bet is this person. (Link to Bitcoin seller in Europe.) They accept Paysafecards. You purchase the card, send the code or the picture, and if you click on their username it shows you the time of transaction. He averages 5 minutes to release the coins to you. If you try SEPA transfer you are looking at 1 to 2 days. $125 USD is $110 Euro.

Thank you for finding that for me. But how do I get the Paysafecard? I don't know what that is.

CHRISTINE

AGENT

Check your nearest location. It's usually a gas station or supermarket. You go to the cashier, give her the money, and they give you a receipt with a pin number. You send that picture to the person on localbitcoins. They verify the funds and put the coins instantly in your profile. The locations it gave me are R-Kioski and Siwa.

OK, that doesn't seem too hard. But when I pay you, how do I know you will actually get me my files back? Or what if you just take my money and don't fix my files? And will you take this awful boobs photo off my screen?

CHRISTINE

AGENT

We unlock every computer, 100%. Will you be doing this today so I can stay online and help you?

I can't! I had such a busy afternoon with work. Now I have to go pick up my son from daycare, it closes in half an hour. I am busy all evening. I have to do it tomorrow. I hope the price doesn't go up! Also what about the files that the virus deleted - do I get those back?

CHRISTINE

AGENT

All files are decrypted and the virus is gone. See what you can do. I can't guarantee the price. I don't control that. If not we will have to see what happens tomorrow.

You mean all which files are decrypted? ALL my files on my computer? Or all the files you deleted?

CHRISTINE

AGENT

Encrypted program files which disable programs you normally use are decrypted. Programs you think are deleted are not. They were moved to a different part of your computer and encrypted in several folders. Those are decrypted and moved back to the original location. I will be online in 2 hours.

[next day]: Is the price still the same?

CHRISTINE

AGENT

Go ahead just do it for 110 Euro. Just get it done today. The person that was selling yesterday is not selling today. Bitcoins are going up in price and it looks like he ran out. Get the Paysafecard and email me, I will find you another person. Let me know if you are doing this today. We are in complete different parts of the world...so I can have someone online to help you.

The problem is it is now Midsummer holiday here this weekend and shops are closed. I have been so busy with kids and work and my husband is super busy and can't help. Which hemisphere are you in - Western?

CHRISTINE

AGENT

I am in Canada. The bottom line is we will do for you for $125 USD as long as you pay by midnight on the 24th. After that it's $225 USD. As soon as the payment comes in we get notified and we will email you or go on the chat with you to get your files restored. On localbitcoins you can purchase the BTC with Paysafecard, Western Union or Moneygram. Let me know.

You are in Canada? I have been researching about ransomware some and I had the impression it all comes from Russia. Interesting. Is this your main source of income? Midnight on 24th by what time zone?

CHRISTINE

AGENT

Midnight by your time zone. If you can do it in the morning it be best. I was the one the waited up for you to answer 3 days ago because I found it odd that we would email you and you would answer 8 hours later. Get it done by Friday at midnight but if you do it during your morning, which is like 4 or 5 am my time I will get a message when you email and I will get up and fix it for you. Normally we don't even negotiate the price but you didn't even get our emails. I know the person on call tomorrow is going to complain when they see I still have it at $125 for you. So try to do it in the morning so I can handle it and you don't have any more issues. As far as your income question...I don't even know how you got it. We are hired by corporation to cyber disrupt day-to-day business of their competition. Never have we done anything in Finland and since you seem like an individual that got the wrong email to open I am trying to keep it at the minimum.

Interesting. So that's why the ransom is so low - because you are already getting paid by the corporation, so you are mostly interested in disrupting the business rather than making a lot of money off the ransom? That's crazy. Is it like a legitimate corporation, and is it well-known? I will try to find an open R-Kioski or Siwa, although it might be tough with the holiday weekend. Paysafe seems like the easiest way for me.

CHRISTINE

AGENT

Ransom is low because you were affected by a minimal virus. The purpose was just to lock files to delay a corporation's production time to allow our clients to introduce a similar product into the market first. Just file encryption. Nothing major. No files were transferred, corrupted or deleted. No self-destruct command on hard drives. Yes, big name corporation. Fortune 500 company. What I still don't understand is that the target is in the USA and you and another person in FInland got the email and the client always gives us the contact emails so you are on someone's mailing list. The other person paid by Paysafecard. They purchased it at Siwa. I get a message notification when you email so let me know so I can get it done for you.

[3 days later]: We were away all weekend for the midsummer holiday, went to our friend's summer cottage where there is no electricity and I had no Internet. I still haven't told my husband about this, he'll get irritated if he knows I got a virus on our computer and have to pay for it. He rarely uses the computer anyway. I will do the payment this week. Is it very common for big corporations to "hack" each other like that? I heard governments do that sort of thing but I didn't know companies do it too.

CHRISTINE

AGENT

Yes. Corporate hacks happen all day every day. Please try and take care of it soon. We have never had had a case take so long. Thanks.

[next day]: I went to the R-Kioski this morning to buy the Paysafecard, but I told the clerk why I was buying it and he declined to sell it to me. Hmm. I will maybe have to try a different R-Kioski. I don't have a Siwa nearby. Is the price still 125? This is sure not a nice thing to have happen to my computer and files, but you are being very helpful at least.

CHRISTINE

AGENT

Yes just do 125. Honestly we just want to get this done. I have never heard of them refusing to sell. As long as you give them the cash they should sell it to you. I urge you to try and solve this today because Bitcoins are traded like stocks and the trading price has gone up. See what you can do.

I have good news! I talked to my friend's friend who is pretty techy and he helped me find a bunch of pictures on my Google account that I didn't realize were there! I had no idea some of my stuff was being backed up to my Gmail account since I hardly ever use it. I think then with the stuff I found, there is not much stuff left that I actually need, so no need to worry about having it decrypted. I can't believe I am saying this but you have been helpful - even though you guys stole my files. You have good people skills, you could be in another more decent line of work and do great. Just curious, is your company like a real legitimate company with a normal website and everything? I can't imagine you advertise your kind of services publicly.

CHRISTINE

AGENT

I am glad you got your files back. I myself don't see the decryption key until the payment shows up in the bitcoin wallet. It's a fail-safe in the system. We don't market our services. Large corporations always have a tech department. Usually there is always a hacker in one of their departments that gets ahold of us to check their security and from there they mention what they need. It's not just corporations. Politicians, governments, husbands, wives. People from all walks of life contract us to hack computers, cell phones, etc. Once again I believe you are on the wrong contact list because we have no customers in Finland and we don't target individuals with family photos or music on their system. It's usually something much more complicated than that. You were lucky. If the virus would have been a self-destruct virus your computer would have crashed beyond recognition. Get a good antivirus.