Digital Extortion: A Forward-looking View

David Sancho
Trend Micro Forward-Looking Threat Research (FTR) Team

A **TrendLabs**SM Research Brief

for Raimund Genes (1963-2017)

Contents

4
What Is Digital Extortion?

7
Online Blackmail

11
Other Forms of Targeted Attacks

12
Ransomware: Its Future as the Tool of Choice

15
Bridging the Gap Between Digital and Physical Assets

17
Trend Micro Advice Against Digital Extortion

19
Conclusion

"Good morning… We hope you've been enjoying the 100+ Gbps DDoS. To make it stop, please pay 30 bitcoins to the following wallet..."

"Did you notice how all the hotels in your chain are lately getting very many negative reviews? If you want this problem to go away, follow the instructions below."

The scenarios above may seem implausible at first. But the unfortunate reality is that many companies have already fallen victim to this particular kind of cybercrime — and many more will follow suit in the future.

Digital extortion has become a fact of life with ransomware and the like. This threat will continue to grow rampant because it is cheap and easy to commit, and many times the victims pay. In fact, it has evolved into the most successful criminal business model in the current threat landscape.

Digital extortion started with denial-of-service extortion attacks back in the early 2000s, but these attacks have evolved quite a lot over the years. While ransomware may have become the go-to modus operandi, online extortionists have a wide field open to them. In this paper, we take a deep dive into the current landscape before moving on to hypothesize how future digital extortion attacks will look like.

What Is Digital Extortion?

When we refer to the term digital extortion, one question always comes up: What is the difference between extortion and blackmail? According to its legal definition, extortion is the coercion of an individual by threatening with violence or the destruction of property. In the case of digital extortion, this translates to threatening to destroy data unless an individual or business pays.

On the other hand, blackmail is legally defined as a criminal activity involving coercion through the threat of revealing information about an individual or their family members. This usually relates to embarrassing, incriminating, or damaging information. This translates to threatening to release sensitive files unless an individual or business pays. Similar to extortion, there is still something that belongs to the victim that is under threat, but instead of tangible property, it is reputation at stake.

Although the two are very similar, the definitions confirm that many digital crimes we normally think of as blackmail are, in fact, extortion — like ransomware. Likewise, some crimes categorized as extortion are actually not. Sextortion comes to mind, wherein an individual is forced to perform acts of a sexual nature under the threat of having compromising material regarding them exposed online. Any attempt by a criminal to coerce a victim into doing something – paying money or performing a favor — falls within the realm of digital extortion. It is of interest to us in the context of this paper.

Physical vs. Digital World

In the digital realm, extortion-related crimes don't have exact counterparts in the physical world. This is a key differentiation that makes things difficult for lawyers to be able to bring these cases to court. For example, in the case of a ransomware infection, though the encryption of digital assets ensures that the victim does not have access to them anymore until a ransom is paid, the same cannot be said if those same digital assets were to be stolen or copied without the owner's authorization. Since the criminal cannot guarantee that the digital information being used for blackmail can be completely returned, this kind of crime cannot ever be as effective as it might be in the physical realm.

In the same vein, crimes such as racketeering (the threat of property loss with a subsequent request for a protection fee) cannot ever work the same in the digital world as they do in real life. The closest thing to it would be a cybercriminal launching a distributed denial of service (DDoS) attack against the victim's network/hosted site and threatening the victim to keep it offline until a certain fee is paid. The missing element would be the protection fee. In the digital world, the criminal cannot guarantee that other cybercriminals will refrain from attacking the victim, thereby losing the protection element of the original crime business model. Network DDoS is a kind of online extortion crime that can never reach the level of racketeering, though it is certainly similar.

How does the future look for these attackers? There is a variety of digital assets prone to being targeted for extortion. These include not only mere data (documents, pictures, databases) but also company secrets (formulas, recipes, supply chain information) and even access to hardware (computers/servers, industrial robots, other company-specific machinery).

A more insidious way of extorting money could be to hack company resources and then coercing the victim to pay in exchange for revealing and resolving the problem. This hacked resource could be anything, from backdoor access to the victim's network to other subtler things like solving manufacturing flaws in the production process. There are multiple real-world examples of this scenario, for example, the attacks against Laboratoire de Biologie Medicale, Banque Cantonale de Genève, Easypay, and Rogers Cable company.

Potential Targeted Assets

One big difference between offline and online extortion is the kind of assets that can be targeted. In the digital realm, there are many more possibilities, some of which can have devastating consequences for companies and corporations. What can be used for digital extortion? They can be any of the following:

- Company Secrets — Extortion (ransom in exchange for decrypting data)
- Company Process — Extortion (payment in exchange for fixing hacked process)
- Company Customer Data — Blackmail (promise to not divulge)
- Company Device — Extortion (ransom in exchange for giving back access to device)
- Compromised Data — Blackmail (promise to not divulge)
- Online Sites — Extortion (promise to stop attacking site)
- Reputation — Extortion (promise to stop campaign)

Of course, documents, images, and other digital assets are already well-known targets, but there are newer kinds of data assets that can be attacked.

For example, there have already been attempts to target online users who want to keep their profile private. By threatening to reveal their victims' names publicly, extortionists have started targeting a very abstract online asset: **the user's right to privacy**.

With the increasing popularity and rapid development of Bitcoin, more assets that could be used for extortion attacks in the future will be **blockchain technologies**. These are usually based off a "wallet" or a private key that generates a public key via a unique function. Only those with access to the private key can perform transactions on the peer-to-peer (P2P) network. In a future where such a system is used to represent any complex transaction, targeting these abstract data assets might have a negative impact for the individual or company and they might feel compelled to pay such an extortion.

Another viable target for extortionists would be **supply chains and manufacturing processes**. Extortionists can threaten to disrupt processes or sabotage production after compromising the enterprise network. The processed food or pharmaceutical industries would be especially affected by such attacks. The manufacturing industry has already been heavily hit by ransomware.

Online Blackmail

On paper, online blackmail is not an effective criminal strategy. Any company with a minimum of logical reasoning would realize that giving in to the threats of a criminal that has a copy of their confidential information is not likely to fix the problem. In fact, the extortionists will be more likely to keep asking for more and more money. In this case, the situation may turn into a digital version of racketeering, where the bad guy continues to demand money after the initial payment, in exchange for keeping the stolen information out of the public eye.

Despite this, however, there are two possible reasons that may enable blackmail attacks to be successful:

1. **Extortion fee under pain threshold.** Given data breach laws and regulations (such as the upcoming General Data Protection Regulation) and the very significant impact hacks can have on a company's reputation, the recurring cost of the extortionist's fees may fall within the corporate victim's loss tolerance for brand protection. In that case, some corporate victims may decide to simply pay. In addition, it has been shown that if a company does not pay and allows data to be released, there is a good chance that the company itself will suffer a significant backlash in the media.

   One recent example is when Bell Canada — a major telco in North America — refused to submit to the hacker's demands for payment after an extortion attempt. Media reports about the incident were universally negative. Instead of having sympathy for the company, which was also a victim along with all the individuals that had their information released, the media portrayed Bell Canada as having "ignored" the request and being too greedy to pay the hackers in order to protect their customers. These kinds of attacks are "no-win" situations.

2. **Younger people being extorted for non-monetary reasons.** We have observed this phenomenon in sextortion cases. When some people who fit this profile are blackmailed with their nude or compromising pictures, they are much more likely to give in. This is especially likely to happen when there is no money being asked for, only favors, usually of a sexual nature. The situation usually becomes a spiral of blackmail wherein the victim exposes their privacy with new revealing pictures that are then used by the blackmailer to further threaten the victim. The only logical outcome is for the victim to realize that there is no end to the cycle and assume that the revealing info is already out of their control.

When extortion attacks involving some form of blackmail have been used against corporations, they have usually failed since a board of executives will normally use the logic outlined in the Bell case. The challenge for the would-be extortionist is to convince the victim that paying up is worth considering. The two reasons above, when employed, are often successful: lower the price to fall under the corporate victim's acceptable cost and target immature populations.

Even if the company trusts the attacker to keep their word and they do keep it, there is no guarantee that the deal will not come back to cause more problems. Uber's case is an example of this. In 2016, hackers stole the personal data of 57 million users and drivers of the ridesharing company, and the company subsequently covered it up by paying $100,000 to the hackers-turned-extortionists. A year later, a new management team decided to divulge the incident to the public, and the disclosure was met with generally negative comments.

What other options will extortionists use in the future? We anticipate another possibility for blackmailers: utilizing time-sensitive topics with a clear deadline. The existence of a hard deadline makes the threat more likely to succeed because it eliminates the question of whether the extortionist can be trusted or not.

A clear example of such a situation would be an election. Before election day, a targeted politician running for office would be very concerned about sensitive or embarrassing information being leaked as it could potentially change voter perception. A deadline for the ransom before or on election day would more likely compel the politician to pay, rather than a deadline set after the election, when the information would be less damaging.

Another useful distinction we can make is between mass attacks versus targeted attacks. In a targeted extortion, the attacker can have privileged information on the victim and is more likely to spend more resources on finding specific embarrassing data. Likely targets can be prominent public figures or people in a power position (politicians, company executives, etc.).

As for extortions, the kinds of attacks prominent and powerful individuals are exposed to are certainly different from those in massive automated attacks. Some of the possible future attacks outlined below may seem outlandish or too far-fetched when used against the general public — but they make much more sense when the target is very specific.

Future Prospects of Online Blackmail

A forward-looking possibility for these threats: blackmail in social media.

The use of social media as an attack vector is becoming relatively common. The way of attempting extortion through social media could happen by way of spreading fake information about the victim, then asking the victim to pay up to stop the ongoing smear campaign against them. These fake information campaigns could be negative or just pure noise.

Different entities might react differently to such attacks. For example, a targeted individual might find it more annoying when different social media outlets are used to spread false news and information about his public persona than a company would. Public personalities have a reputation to maintain, and a criminal trying to taint it might strike where it hurts most.

Such an application of a classic smear campaign would work even more effectively in the digital world than in real life. Digital data lasts longer than real-world news: a successful smear campaign in 2016 may still be showing high in search ratings in 2017 or later. News can also spread faster online, with social media able to transmit news – fake or otherwise – with the click of a button. That is decidedly a factor in these attacks.

More examples on the use of social media for extortion purposes are detailed in Fake News and Cyber Propaganda: The Use and Abuse of Social Media.

A corporation might be more prone to cave in to the threat of their publicity campaigns being drowned out by noise. In the past, we have seen **hashtag pollution** campaigns against political opponents with a clear agenda of drowning the voice of an opponent in a sea of noise. Something similar can be done systematically against corporations that use social media to spread word of their products or to build expectation for upcoming products, movies, etc. The threat of weakening social media for product promotion can be a powerful enabler for online extortion against certain kinds of companies, like movie studios, streaming services, and other businesses that make heavy use of social media to promote their products.

For these companies, a negative campaign could even be more damaging. Hijacking their online promo or publicity campaign as outlined above can have an impact. Also, spreading false reviews or other damaging product info — real or not — could be detrimental to their marketing efforts and eventually to their bottom lines and can have the potential to enable successful extortion attacks. For instance, hotels, restaurants and other service-oriented businesses are very sensitive to ratings on specialized review sites.

The same thing goes for any product that is being sold on popular crowdsourced review sites such as Amazon. A smear campaign can be very damaging to the companies that provide such services or sell those products.

Regarding possible future targeted attacks, the development of new video and audio technologies can have a big impact for online extortionists. The University of Washington has published academic work on spoofing video footage once there is enough audio available. The software the researchers wrote can generate realistic video and audio of the target person based on arbitrary scripts. The use of these technologies to spread false declarations or news in the context of smear campaigns for extortion has an immense potential for criminals.

With the increase in fake news campaigns, people are becoming more aware of the need to fact-check online sources. But in general, users are far from being adept at it. Most of the time, any shocking rumor spreads easily through social media communities and this is especially true if there is an audiovisual element to it.

Other Forms of Targeted Attacks

Apart from online blackmail attacks, there are other methods cybercriminals can use for digital extortion to target specific digital assets.

- **Threats against users' right to privacy** — We can expect more of these attacks in the future. A viable scenario would be, after a porn site data breach, to use open-source intelligence to get detailed information on some of the site users, then approach the users and threaten to reveal their membership publicly. We have seen this scenario in the Ashley-Maddison breach back in 2015.
- **Attacks against blockchain technologies** — Private keys used for wallets for networks like Bitcoin and Ethereum can be targeted and used in extortion. After infecting the victim's computer, an attacker can look for wallets or private keys in order to disable or steal the value of the currency in it. Worse than that, if instead of a currency, the blockchain network represents some other intangible asset, the attacker can alter it with unspecified consequences. Imagine things like Namecoin, a blockchain network for registering domain names, or even Ethereum being used to sign smart contracts. In a future where such a system is used to represent any complex transaction, targeting these abstract data assets might have a negative impact for the individual or company and they might feel compelled to pay extortionists.
- **Supply chain disruption** — Assuming the attackers already have access to the victim's network, they might insert logic bombs or Trojans into specific network locations. The company will have to pay ransom before the attackers reveal where the bugs are so they can be disabled. A more insidious possibility would be for an attacker to keep backdoor access to the company and use it to mount local attacks, then extort the company in exchange for revealing the location of the backdoor.
- **Manufacturing process alteration** — One manufacturing process inside the company might be modified ever so slightly so that the final products are flawed but not obviously so. The criminal would then ask for money to reveal where the manufacturing machinery was modified to introduce the defects or even which exact batches were affected by the defect. The processed food or pharmaceutical industries would be especially affected by such a ploy. The manufacturing industry has already been heavily hit by ransomware.

Ransomware: Its Future as the Tool of Choice

We all know what ransomware is, how it works, and what it does. The fact that ransomware is the number one threat to businesses nowadays is sure to make criminals come up with novel ways to refine and improve their strategies.

One particular issue we can see digital extortionists evolve in their habits is their choice of targets. So far, most of the ransomware we have seen are mass-produced and sent to as many potential victims as possible. When these cybercriminals manage to hit big businesses with their widespread attacks, they can expect high returns for their efforts. It's not unreasonable to assume that at some point ransomware attackers are going to start pointing their digital weapons specifically at industries and companies that yield the most return. Those industries are healthcare (hospitals, etc.) and manufacturing (factories and product makers).

The healthcare industry, for one, needs highly confidential data or personally identifiable information (PII) from patients in day-to-day operations. Any computer that has access to this information has the potential of acting as a tool for the criminals to encrypt or steal data. The consequences of their patient information being stolen, frozen, or compromised can be dire — not only from an operations perspective (i.e., being unable to prescribe the right medicine or treatment to the right patient) but also from a PR perspective, where their more famous patients may face blackmail for their state of health.

Hospitals cannot continue to run their business without their patient history data, so extortion is often successful in this environment. On top of this, healthcare installations are smaller budget-tight companies and traditionally have not focused on security, so their defenses may be weaker than other potential targets like banks or big corporations.

In the case of manufacturing companies, extortion through ransomware is a definite risk because downtime of any sort in a factory translates to heavy monetary losses. A reasonable ransom to continue production is likely to be paid without much hesitation. Also, the machines and robots used in manufacturing assembly lines are very diverse, difficult to update, and often unprotected.

In a similar way, critical infrastructure might also be targeted for the same reasons. They run older machines that cannot be updated often — or at all — and most likely have no security solutions installed. Obviously, downtime is unacceptable, so a potential ransom situation would be paid with a higher probability than in any other industry.

As for the delivery of ransomware, the most common ransomware infection vector is through email phishing and/or webpage drive-by download. In these schemes, the victim is directed through some social engineering technique to a bad website that exploits a browser vulnerability and infects the computer or to download fake anti-malware software. This is not the only method, though.

There are already proactive infections where the attackers hack their way into a server, then manually install ransomware on it. In 2017, we witnessed the mass infection that WannaCry brought upon countless networks worldwide by using a network vulnerability. This last strategy of adding worm-like capabilities to ransomware proved to be very effective, perhaps surprisingly so. **We expect ransomware criminals to add "new" features to their creations by reusing the old book of traditional malware techniques**. It would not be unreasonable to think that they might use PE infectors or any other more aggressive delivery technique in order to increase the speed of the infections and spread the impact far and wide.

We can expect even more innovations from ransomware authors. This kind of malware is quickly becoming their "cash cow" and improving the way it works is not only possible but likely or even expected. A quick way to enhance the speed of encryption, for instance, could be to fine-tune the file types to search for and encrypt based on the industry that the company being infected is part of. This might be more relevant for more targeted attacks. For example, if the criminals want to maximize damage and increase the speed of encryption, when targeting a media company, they would choose to look for image and video files. On the other hand, in a scenario where the malware affects a pharmaceutical company, they would rather search for documents and spreadsheets.

Another way for cybercriminals to enhance these malicious programs could be to **devise systems to minimize the criminal's interaction with the victim**. This would mean automatically storing the encryption key online and setting up sites that verify whether the payment has been received before releasing the key or the decryption tool with the built-in key. Of course, the idea needs to be refined to minimize the probability of the victim getting the key/tool for free. If this were to be successfully implemented, it could mean that the criminals might be able to do mass infections without having to provide manual support to each victim, which is probably the bottleneck of the whole ransomware operation.

Finally, a feature that we can expect to be added to ransomware is dynamic pricing. There is a dichotomy that exists between infecting a domestic user versus a corporate computer in terms of how high the price of the ransom should be. If the ransom is set too low, corporations would readily pay, but cybercriminals would stand to lose more potential profit, especially if the asset being held hostage is critical to the company's operations. On the other hand, if the ransom price is set too high, companies might be able to pay, but then the domestic users affected might not be able to afford it, and thus forgo payment.

A dynamic pricing system installed in ransomware, where the price is set up based on the nature of the business affected, would address this. Such a system could, for example, detect the number of IPs on the local network where the ransomware is currently located. It could detect the existence of an Active Directory, or the presence of multiple printers in a network (typical in a business/office setup).

In addition, there are a number of developments recently that can help criminals determine the price ranges that companies would be able to pay to obtain their data back. First, the upcoming General Data Protection Regulation (GDPR) has set up fines for companies who fail to disclose that the company has been penetrated and lost data to criminals. The maximum fine is 4 percent of global annual turnover for the preceding financial year (or 20 million euros, whichever is greater). Ransomware authors can use this as a price ceiling for ransom. Anything higher than this would not make sense to pay from the company's perspective.

Second, insurance firms are already selling cyber insurance for data breaches. Primes for these contracts — if properly found or estimated — are the bottom of the range for companies. Anything less than those primes and the company would rather pay the insurance instead of the criminal.

Another strategy that criminals might start to use in this developing field is data pollution as a means to undermine the value of data backups. This means creating an encrypted copy of the original data, then proceeding to alter the data subtly over the course of days, if not weeks. Finally, when the original data backups are likely to have been replaced by newer and progressively worse backups, the malware can delete the data and show the ransom notice. This strategy can be difficult to implement but, if done properly, can be devastating to any business – even those that pride themselves in keeping rigorous backup copies of every single document.

Bridging the Gap Between Digital and Physical Assets

Digital extortion may target cyber assets, but its impact and methods can cross over to the physical. Given the degree of interconnectivity that modern hardware is being designed with, it is possible that, in the future, most of this new technology can be used for extortion. From activity trackers to smart cars, the Internet of Things (IoT) encompasses a variety of internet-enabled devices. There are, however, two dangers that users risk in the context of digital extortion: losing the data that these devices accumulate and retain and losing access to the device itself.

Which of these two scenarios is more likely to be abused by criminals? Certainly, an attacker would not bother stealing data from a fitness tracker — It's hard to threaten someone about their exercise history. But file repositories, such as Network-Attached Storage devices, are dangerously similar to servers full of files, because they actually are. Data being captured in file repositories and other devices, such as microphones or online cameras, can be stolen and subsequently used to blackmail the owner or plan further crimes.

The second scenario is also plausible: barring access to the device in exchange for a ransom fee. There is a caveat to this, though: If hijacking the device took place in normal circumstances, the victim can just bring it to tech support and have it fixed. On the other hand, if the device is far away and by its very nature is mobile, the situation is much more delicate.

An example of this would be a smart car being hijacked and rendered inoperable by an attacker, causing the car and passenger to be stranded a hundred miles away from home. In this scenario, the car owner would definitely consider paying the ransom to regain access to the car. The same scheme could work on smartphone-accessible bike padlocks.

Any device that holds interesting data could be subject to ransom attacks. Also, any device that is portable (and not necessarily a mobile phone) that can't be easily carried to be fixed could be attacked with a denial of access. The above-mentioned are only two possibilities. With the increasing number and variety of internet-connected machinery being designed each year — and current lack of built-in security and industry standards — this category will be an expanding one in the coming years.

Cybercriminals attacking devices for ransom may seem too far-fetched, but consider that security researchers have already created a Proof-of-Concept ransomware that infects smart thermostats. Similarly, there have been cases of ransomware infections in hotel room locking systems.

Another way cybercriminals could bridge the gap between the digital space and the physical world: requesting physical favors as payments instead of mere monetary payment. As we have alluded to previously, a generic blackmail attack is likely to fail. However, a person with enough access to a building can be blackmailed to provide temporary untraceable access in exchange for his or her naked pictures not being made public. That's a feasible attack that certainly crosses the digital-real world gap.

With this in mind, we can also see how attackers with political agendas may spy on influential leaders and hold information for ransom in exchange for political advantages or perhaps other smaller favors. This can even be taken further to the cyber-war arena and theorize how nation-states could play the same game. This situation is possible, but it is also likely that even if it happens, it would not make it to mass media and public attention.

A curious case of extortionists that demand something else different from money happened recently. In that ransomware attack, the attackers asked for nude pictures of the victim, possibly with the intention of continuing the extortion with an attempt to blackmail the victim. In that case, the attack was largely unsuccessful, but it's an example of extortion demanding a non-monetary price. However, it is unlikely that future ransomware will go that way.

Trend Micro Advice Against Digital Extortion

Despite the doom-and-gloom scenarios described above clearly being dire enough, there is always a way to be secure against them. Where cybercriminals are concerned — even when ransomware is involved — all is not lost. The following defense strategies can mitigate the risk of digital extortion schemes.

Corporations should have potential extortion scenarios figured out by the time they are affected. Normally, the decision of whether or not to pay an extortionist is clear: Since the extortionist cannot be trusted, paying the fee will never make the problem go away. The only logical solution is to refuse to pay. Discuss the scenario with your board of directors or decision-makers and let them conclude with this decision on their own before the situation ever comes up. This way, you will all be prepared if and when the time comes. Oftentimes, running such an exercise with decision-makers ahead of time will yield better results than waiting for the attack to happen and making decisions in panic mode.

The above applies to sextortion blackmail as well. When an individual is being extorted with compromising photographs or media, attempting to satisfy the extortionist's demands will only exacerbate the issue. The victim needs to be convinced that once the pictures are out of his or her control, there is nothing that can be done. Sending more pictures to the extortionist is only throwing more fuel to the fire. A solution here is to go to the authorities to report the incident and hopefully trigger an investigation that would lead to the arrest and indictment of the culprit.

Conversely, when the victim gives less value to the material the extortionist already has, the data also loses value in the attacker's eyes and will be less likely to use it. This was illustrated recently when Australian singer Sia was extorted with her naked pictures. Her response was quite unusual: she published the pictures.

In the case of smear campaigns and denial-of-service (DOS) attacks against businesses, the outcome should be similar: the attack or abuse will not stop even if the extortion fee is paid. One possible move in these cases is to go to the press and explain the situation. Even though it is not certain that the problem will be solved, the products will receive some free air time and the company will be seen in a positive light for its honesty. If publicizing the attack is not an option or too much of a risk, at least inform the administrators of the sites where the smear campaign is being run (e.g., TripAdvisor, Yelp, Amazon, Facebook).

In incident response plans, any new or novel assets should be taken into account. Assets such as blockchain technology accounts, wallets, and the like should be reflected in the plan, as well as what to do when those are compromised or attacked. The same is true for any business process that is susceptible to being attacked. Any system involved should be accounted for and a viable strategy to deal with extortion attacks should be devised ahead of time.

Similarly, ransom attacks need to be foreseen and prevented. The usual way of doing this is having current backups, but this may not be completely effective in the case of data pollution attacks. For those, an offline backup system would not be enough. On the other hand, these kinds of long-term attacks are more prone to being detected by regular antivirus/anti-malware solutions and online monitoring techniques. This means that the risk is much lower than that of plain old vanilla ransomware attacks.

Conclusion

Digital extortion is not a new idea, and since the advent of ransomware, it has been growing in the cybercriminal's portfolio.

Blackmail still exists as a semi-viable strategy against certain populations, although it is not usually effective against businesses. Ransomware is a growing threat and criminals are innovating their infection vectors and delivery systems — and they are likely to come up with creative new ways of attacking.

Blackmail has a tendency to be a personal targeted threat. Ransomware, on the other hand, tends to be mass-delivered to any target, though companies are the juicier targets. There are novel ways in which these tendencies can be modified, both in their delivery methods and in the ways they can affect users. These possibilities are wide open to criminals and they will not hesitate to explore them further to increase digital extortion's effectiveness — and, therefore, their bottom lines.

Users and enterprises can protect themselves from blackmail and extortion attempts by securing the digital assets and data that extortionists could leverage. Adopting security best practices as well as planning for incident response can help mitigate the impact of these cybercrimes, even if they evolve and expand.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com