Written Testimony of Kemba Walden

United States House Subcommittee on National Security, Illicit Finance, and International Financial Institutions of the Committee on Financial Services
Hearing on "Held for Ransom: How Ransomware Endangers Our Financial System"
April 16, 2024

Chairman Luetkemeyer, Ranking Member Beatty, and Members of the Subcommittee, my name is Kemba Walden, and I am the President of Paladin Global Institute (Paladin), a think tank committed to ensuring that secure critical infrastructure and the safety of people online remain core to sustainable technological innovation. I am also the co-chair of the Disruption working group of the Institute for Security and Technology (IST) Ransomware Task Force, which brings together experts across industries to combat the threat of ransomware.[1] Prior to Paladin, I served as the acting National Cyber Director and Principal Deputy National Cyber Director in the newly formed Office of the National Cyber Director in the Executive Office of the President. I was an Assistant General Counsel in Microsoft's Digital Crimes Unit (DCU), where I led the Ransomware Analysis and Disruption Program. I also spent a decade in government service at the U.S. Department of Homeland Security (DHS). At DHS, I held several attorney roles, specifically as the lead attorney for the DHS representative to the Committee on Foreign Investment in the United States (CFIUS) and then as a cybersecurity attorney for the Cybersecurity and Infrastructure Security Agency (CISA), and its predecessor. I want to thank you for the opportunity to discuss ransomware attacks and illustrate why improved governance, better resilience, and meaningful information-sharing and public-private partnerships are critical to combatting ransomware.

Since my prior testimony and the standup of the Ransomware Task Force (RTF) in 2021, we have seen new trends in the tactics of a ransomware attack which highlight the critical importance of not only improved techniques for disruption but also resilience and deterrence. While the security community and critical infrastructure companies have made progress, there is still more to do. The FBI reports that in 2023,[2] it received 2,825 complaints with adjusted losses of more than $59.6 million which is an increase over 2022[3] when the FBI reported that it received 2,385 complaints with adjusted losses of $34.3 million. I continue to believe the best strategy to decrease ransomware attacks is through targeted disruption campaigns along with improved preparedness and resilience. I will close by highlighting several key opportunities for more effective disruption of this cybercrime, opportunities to raise the collective security of public sector and private sector organizations, and the importance of partnerships.

Ransomware attacks pose an increased danger to all Americans as critical infrastructure owners and operators, small and medium businesses, and state and local governments continue to be targeted by criminal enterprises and nation-state proxies, operated by distinct criminal organizations. A sustainable and successful effort against this threat will thus require a whole-of-government strategy executed in close partnership with the private sector.

A. Paladin Global Institute's approach to cybercrime

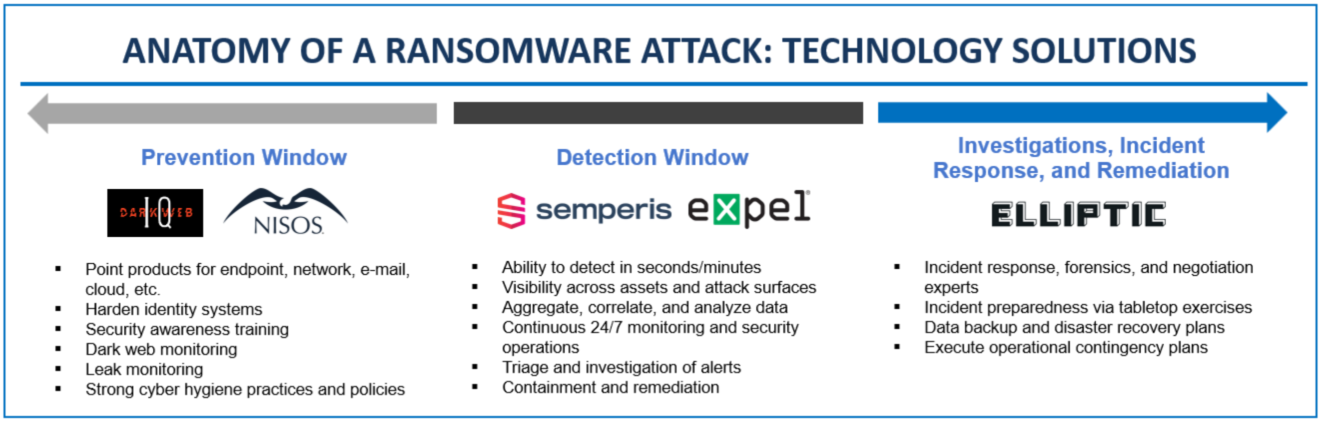
In this testimony, I will leverage the expertise gained through the work of Paladin Global Institute, its insight into various markets, and my own experience through the RTF and previous roles, to provide an overview of the ransomware landscape and provide recommendations that I believe this subcommittee may find relevant as it continues to consider responses to the ransomware threat. Paladin Global Institute leverages its global reach and

[1] In 2021, the Task Force published a framework of actionable solutions aimed to mitigate ransomware as a malicious cyber activity and criminal enterprise: Institute for Security and Technology (IST) » RTF Report: Combatting Ransomware

[2] See 2023 FBI Internet Crime Report. 2023_IC3Report.pdf

[3] See 2022 FBI Internet Crime Report. 2022_IC3Report.pdf

deep bench of cutting-edge thought leaders and policy experts to protect global critical infrastructure. Paladin encourages both (1) operational opportunities to disrupt cybercrime and (2) policy solutions for sustainable cybersecurity and cyber safety improvements. For ransomware, the objective is to give public and private sector entities the upper hand over ransomware criminals at each stage of a potential ransomware attack. For example, Paladin encourages entities to leverage technology to **prevent** ransomware from entering their networks in the first place or to **detect** threats and then **respond** and **recover** immediately upon attack.



ANATOMY OF A RANSOMWARE ATTACK: TECHNOLOGY SOLUTIONS

Prevention Window

- Point products for endpoint, network, e-mail, cloud, etc.
- Harden identity systems
- Security awareness training
- Dark web monitoring
- Leak monitoring
- Strong cyber hygiene practices and policies

Detection Window

- Ability to detect in seconds/minutes
- Visibility across assets and attack surfaces
- Aggregate, correlate, and analyze data
- Continuous 24/7 monitoring and security operations
- Triage and investigation of alerts
- Containment and remediation

Investigations, Incident Response, and Remediation

- Incident response, forensics, and negotiation experts
- Incident preparedness via tabletop exercises
- Data backup and disaster recovery plans
- Execute operational contingency plans

Paladin also encourages technology companies to work closely with law enforcement and agencies such as the Office of Foreign Assets Control (OFAC) to protect information and information systems from the scourge of ransomware. For example, the FBI and DOJ have set up a program with at least one technology company where law enforcement leverages the company's intelligence on threat actor operations to disrupt imminent attacks against U.S. organizations, gather evidence to build cases against the criminals, prosecute, and extradite them. This approach has resulted in the disruption of over 750 potential ransomware attacks in the last two years, one of which included an otherwise imminent attack against one of the nation's largest hospital systems. It is also leading to the unmasking, prosecution, and extradition of dangerous criminals.

In addition to providing solutions to enterprises and communities for defeating ransomware and partnering with law enforcement to disrupt cybercriminals involved in ransomware attacks, we provide substantial support to the Ransomware Task Force. I personally co-chaired the Task Force's Disruption working group. There are a host of policy choices to make ransomware less profitable and more difficult to deploy by disrupting infrastructure and payment systems that enable ransomware attacks.

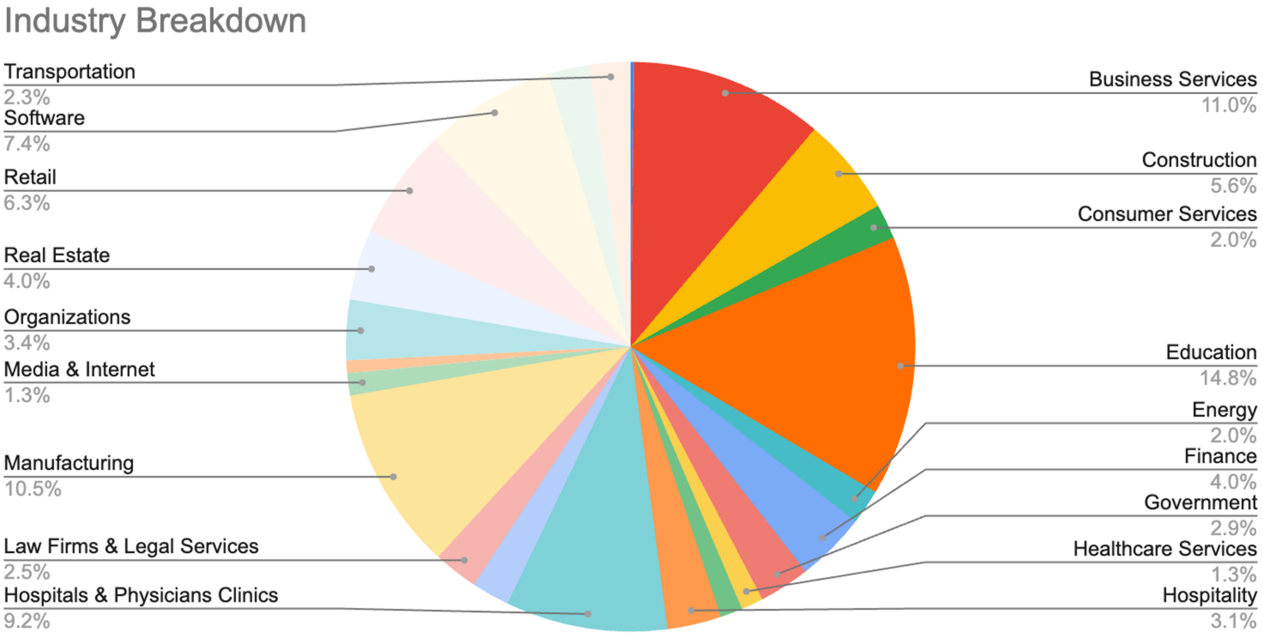
Through Paladin's observations of ransomware deployment and attacks, our active collaboration with the Ransomware Task Force, and my thought leadership in the global discussion on policy and operational opportunities to counter ransomware, I will next address opportunities for more effective disruption of this cybercrime, opportunities to raise the collective security of public sector and private sector organizations, and the importance of partnerships.

B. What is a ransomware attack?

Ransomware is a specific kind of malicious software or "malware" used by cybercriminals to render data or systems inaccessible for the purposes of extortion—i.e., ransom. In a standard ransomware attack the cybercriminal achieves unauthorized access to a victim's network, obtains legitimate credentials of existing employees, executes lateral movement across a network, installs malware to establish persistence in that network and exfiltrate sensitive data, and finally deploys the ransomware. Once the criminal executes the installed ransomware – the final step in the series of crimes described -- the victim's files are locked on that network, making them inaccessible to the victim until a ransom is paid. Usually, the ransom demand is for payment in the form of cryptocurrency – such as Bitcoin. The theft of data compels the victim to engage in negotiations and raises the potential reputational, financial, and legal costs of not paying the ransom as the attackers will not only leave the victim's data locked, but also leak sensitive information that could include confidential business data or personally identifiable information.

Ransomware criminal syndicates will effectively profit from two or more of the phases of a ransomware attack: (1) system encryption/lockout; and (2) data extortion. The locking out aspect of an attack can be decoupled from the data extortion aspect such that victims can experience one without the other or both. For example, in the case of the 2021 ransomware attack on Medibank, an Australian health insurance company, the attackers did not successfully encrypt the files; rather the ransomware group published the stolen records.[4]

Recent, high-profile incidents such as those involving hospital systems illustrate the extent of the threat and the significant, multimillion dollar consequences of ransomware. However, based on data obtained by Paladin, ransomware is not limited to high-profile incidents. It is ubiquitous and pervasive, impacting wide swathes of our economy, from the biggest to the smallest players. Our data shows that the education sector represents one of the most targeted sectors, along with the business services,[5] healthcare, and manufacturing industries.



Ransomware engagements by industry

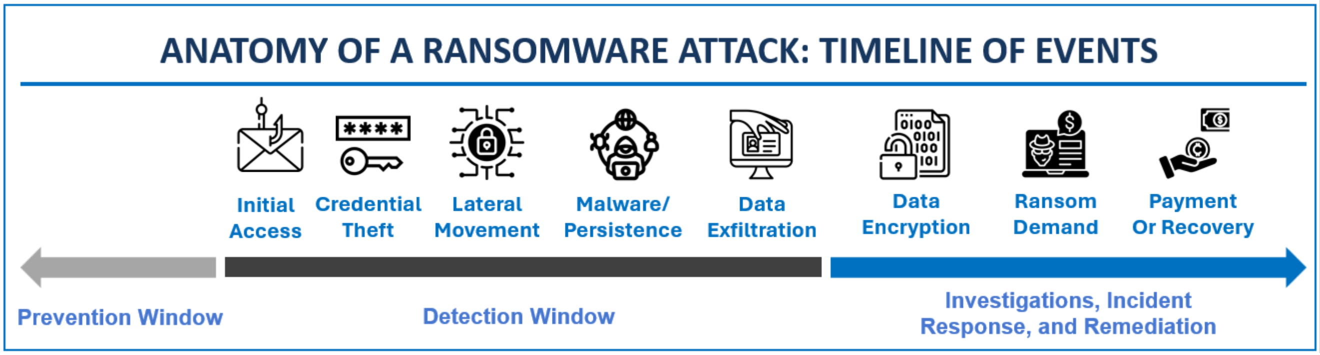
C. How does a ransomware attack work?

The image below depicts the basic steps that typically take place before a cybercriminal installs malicious ransomware on a victim's network. First, cybercriminals will gain access to the victim's network through phishing, a stolen password, or through an unpatched software vulnerability. Then, the cybercriminals will seek to obtain legitimate credentials enabling them to move around in a victim's network virtually undetected. The cybercriminal will then use commercially available software to move laterally in a network to obtain higher level privileges, such as those held by the victim's IT Administrator, to access the entire network. Cybercriminals will then conduct reconnaissance within the victim's network, looking for critical systems and

[4] See TechCrunch, Medibank breach: Hackers start leaking health data after ransomware attack | TechCrunch

[5] Professional Services, excluding law firms.

sensitive data, in some cases stealing this data, to facilitate an effective ransom demand. Finally, the cybercriminals will leverage this information to install ransomware on the network that will lock the victim's files until the ransom is paid.



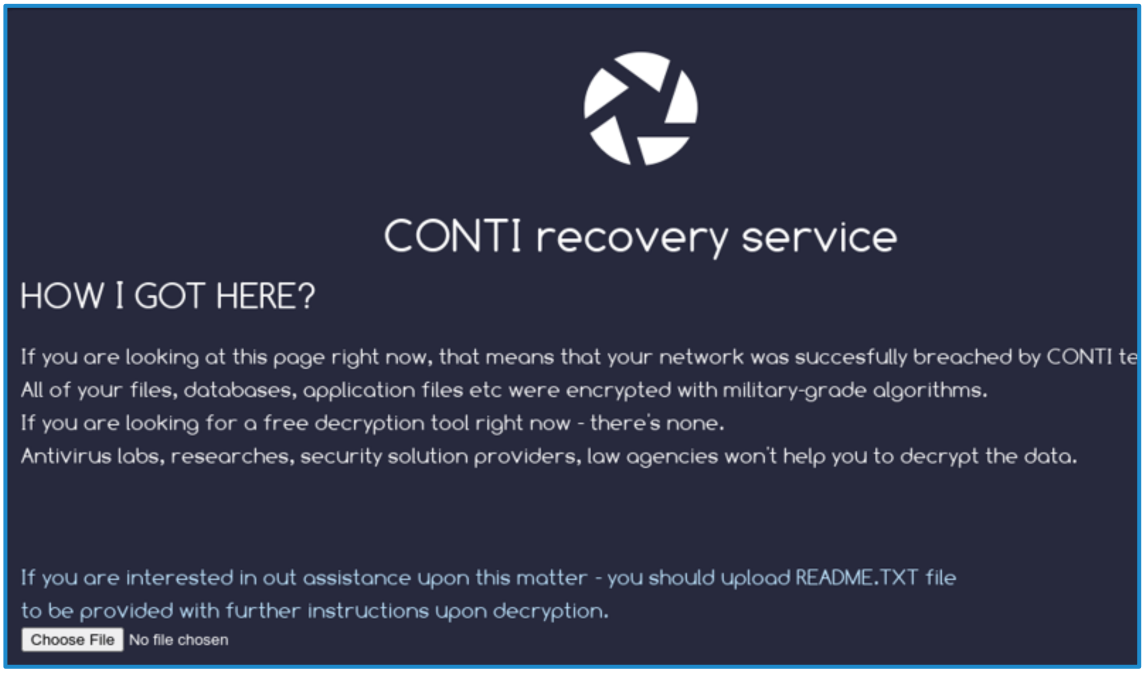
Though the basic anatomy of a ransomware attack has remained static for the last several years, the ransomware actors have refined their tactics to preemptively defeat a victim's backups, which is a common cyber security defensive measure, prior to deploying and executing the ransomware malware in the rest of the organization. Once they obtain legitimate credentials and the ability to escalate privileges to move laterally across the network, actors will take additional steps to increase their chances that an entity will pay a ransom by delaying an enterprise's ability to recover and increasing the costs of a victim's downtime. To accomplish such a delay and increase downtime costs, ransomware actors will seek and encrypt an entity's backup and recovery solutions and defeat an enterprise's identity systems and solutions – a key prerequisite for recovery.

D. How do cybercriminals ransom targets?

Ransomware has evolved into a highly lucrative business model, with an accompanying advanced intelligence collection aspect. Criminal actors collect and perform research and analyze their intelligence to identify an optimal dollar amount for their ransom demand. Once criminal actors break into a network, they may access and study their target's financial documents and insurance policies to better inform their eventual ransom demand and negotiating position. They may even research the penalties associated with that organization's local breach laws. The actors will then extort money from their victims, not only in exchange for unlocking their systems, but to also prevent public disclosure of the victim's stolen data. Leveraging the significant intelligence they can gather on victim companies, the criminal actor will then launch their attack, identifying what they regard as an "appropriate" ransom amount.

Once the criminal actor installs the ransomware and uses it to lock the victim's system, the victim will have access only to a ransom note. The ransom note provides instructions to the victim on how to communicate with the criminal actor. In the example below, the criminal used the ransomware strain known as CONTI which many experts believe has reorganized into Black Basta, a variant in wide-spread use today.[6] The criminal directs the victim to a ReadMe.TXT file – often the only file available to the victim.

[6] According to CISA, "speculation persists that Black Basta may be an offshoot of the Russian-speaking RaaS [Ransomware as a Service] threat group, Conti, or has some members of the formerly proficient group." 202303151200_Black Basta Threat Profile_TLPCLEAR (cisa.gov)



CONTI recovery service

HOW I GOT HERE?

If you are looking at this page right now, that means that your network was succesfully breached by CONTI te

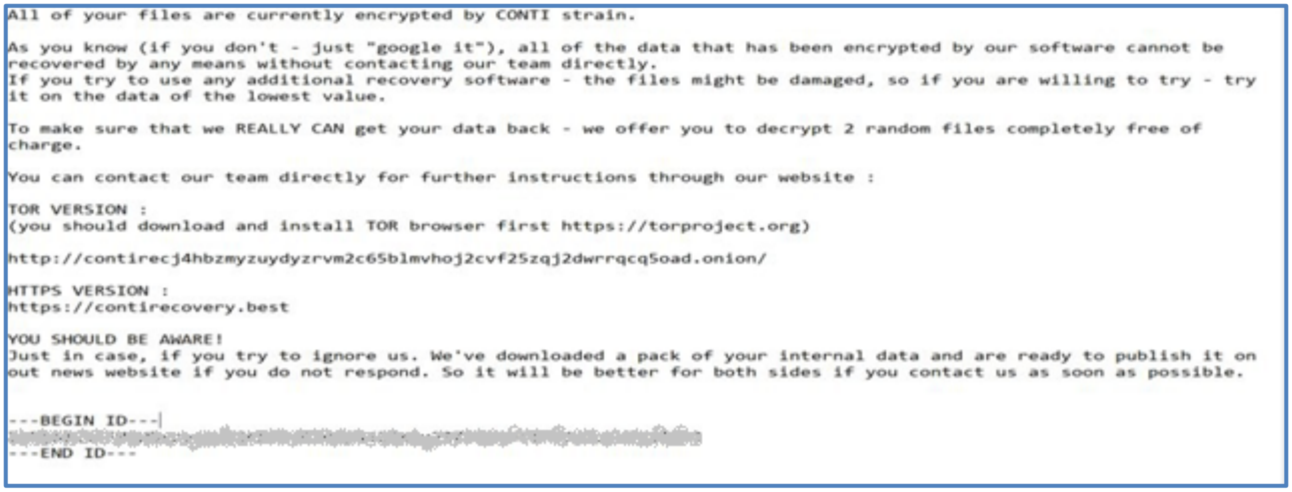
All of your files, databases, application files etc were encrypted with military-grade algorithms.

If you are looking for a free decryption tool right now - there's none.

Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.

If you are interested in out assistance upon this matter - you should upload README.TXT file
to be provided with further instructions upon decryption.

The ReadMe.TXT file then instructs the victim to access the dark web using the Tor browser, a special means for accessing the dark web. The file also assigns a unique "hash" to the victim, a key that allows the criminal to identify the specific victim.[7] At this point, the victim can open communications with the criminal to negotiate the ransom or pay it.

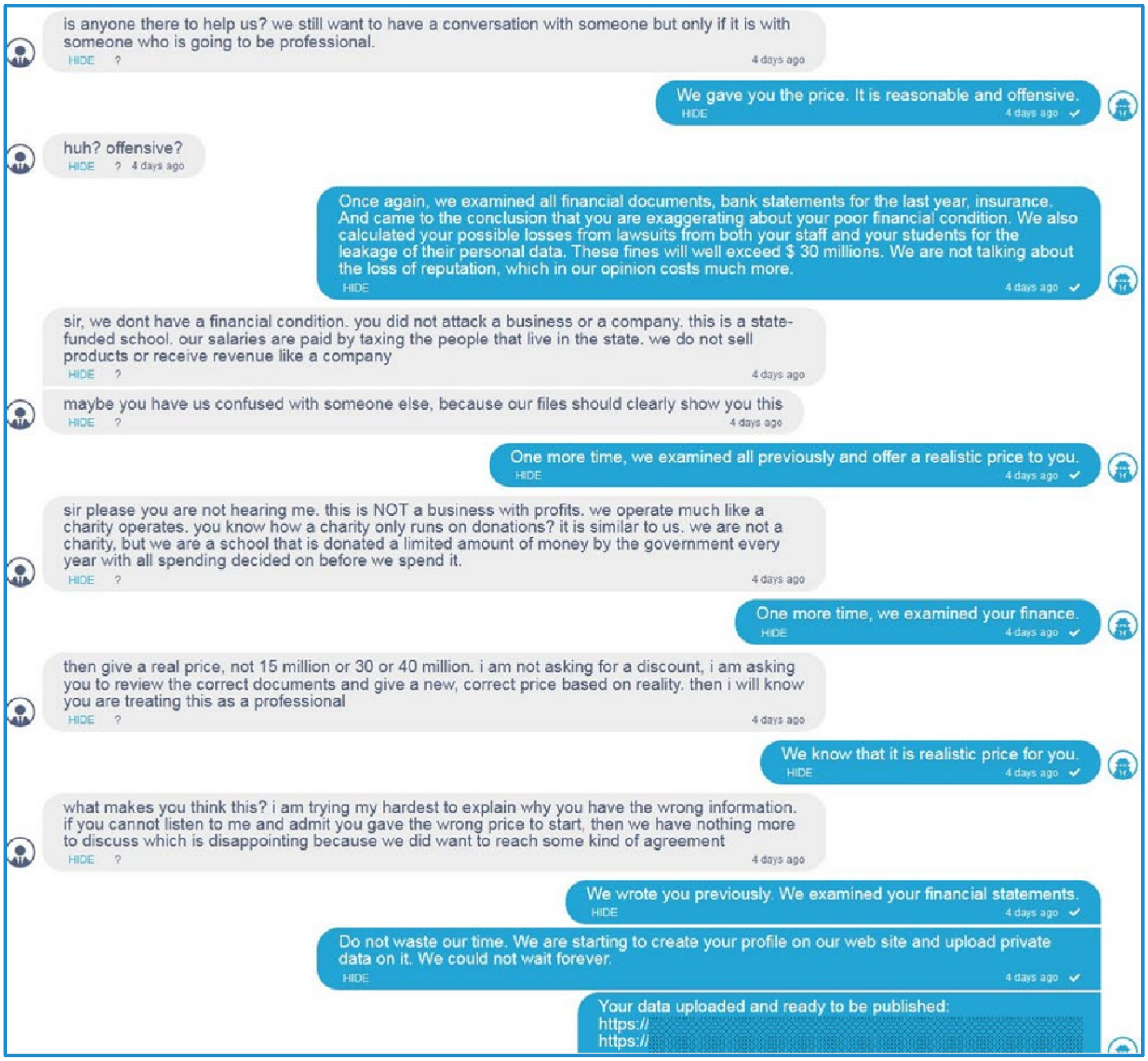


```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be
recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try
it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of
charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on
out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
[redacted]
---END ID---
```

The negotiation process and back-and-forth communications are often surreal and disturbing in the nonchalance with which some criminal actors offer to "help" companies recover from the very attack they have orchestrated. The example below depicts a negotiation chat with a public school district in which the criminals attempt to extort cash in exchange for a key to unlock the ransomware deployed on its network. The interaction demonstrates the research performed by the criminal in advance of the negotiation, as the criminal actor explained that they had "examined all financial documents, bank statements for the last year, insurance. And came to the conclusion that you are exaggerating about poor financial condition. We also calculated your possible losses from lawsuits from both your staff and your students for the leakage of their personal data. These fines will exceed $30 million. We are not talking about the loss of reputation, which in our opinion costs

[7] The hash at the bottom of this sample note is intentionally blurred.

more."[8] In a recent case, one ransomware actor known as ALPHV reportedly filed a complaint with the Securities and Exchange Commission (SEC) reporting a victim company for not disclosing a "material" cyber incident consistent with the SEC's reporting guidelines.[9]



is anyone there to help us? we still want to have a conversation with someone but only if it is with someone who is going to be professional.

We gave you the price. It is reasonable and offensive.

huh? offensive?

Once again, we examined all financial documents, bank statements for the last year, insurance. And came to the conclusion that you are exaggerating about your poor financial condition. We also calculated your possible losses from lawsuits from both your staff and your students for the leakage of their personal data. These fines will well exceed $ 30 millions. We are not talking about the loss of reputation, which in our opinion costs much more.

sir, we dont have a financial condition. you did not attack a business or a company. this is a state-funded school. our salaries are paid by taxing the people that live in the state. we do not sell products or receive revenue like a company

maybe you have us confused with someone else, because our files should clearly show you this

One more time, we examined all previously and offer a realistic price to you.

sir please you are not hearing me. this is NOT a business with profits. we operate much like a charity operates. you know how a charity only runs on donations? it is similar to us. we are not a charity, but we are a school that is donated a limited amount of money by the government every year with all spending decided on before we spend it.

One more time, we examined your finance.

then give a real price, not 15 million or 30 or 40 million. i am not asking for a discount, i am asking you to review the correct documents and give a new, correct price based on reality. then i will know you are treating this as a professional

We know that it is realistic price for you.

what makes you think this? i am trying my hardest to explain why you have the wrong information. if you cannot listen to me and admit you gave the wrong price to start, then we have nothing more to discuss which is disappointing because we did want to reach some kind of agreement

We wrote you previously. We examined your financial statements.

Do not waste our time. We are starting to create your profile on our web site and upload private data on it. We could not wait forever.

Your data uploaded and ready to be published:
https://[redacted]
https://

E. What barriers to entry exist to executing a ransomware attack?

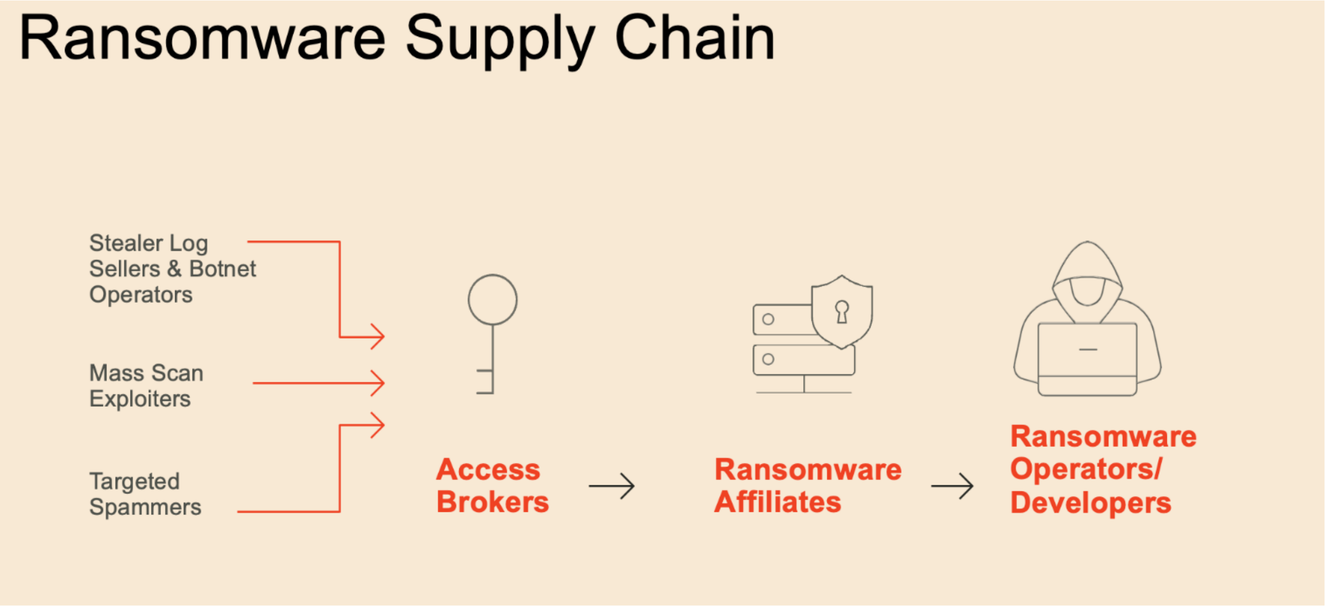
Since the Colonial Pipeline attack in 2021, the private sector, working closely with the public sector, raised the costs of committing this crime, but the barrier to entry still remains too low. A cybercriminal does not need specialized computer coding skills to profit from ransomware. The only cybercriminal in the entire ransomware lifecycle who requires specialized code development skills is the originator who develops the malicious software in the first place. There are hundreds, if not thousands of different ransomware variants, such as Black Basta, Royal, ALPHV, and LOCKBIT. Attacks are often misleadingly named after the malicious software installed on a victim's network, though the cybercriminals involved in the attack may not have any link to that ransomware's creator. A single cybercriminal may use any number of ransomware variants in conjunction with

[8] See also Parents were at the end of their chain — then ransomware hit (nbcnews.com)
[9] See Ransomware group reports victim it breached to SEC regulators (arstechnica.com)

other tools to attack victim networks.

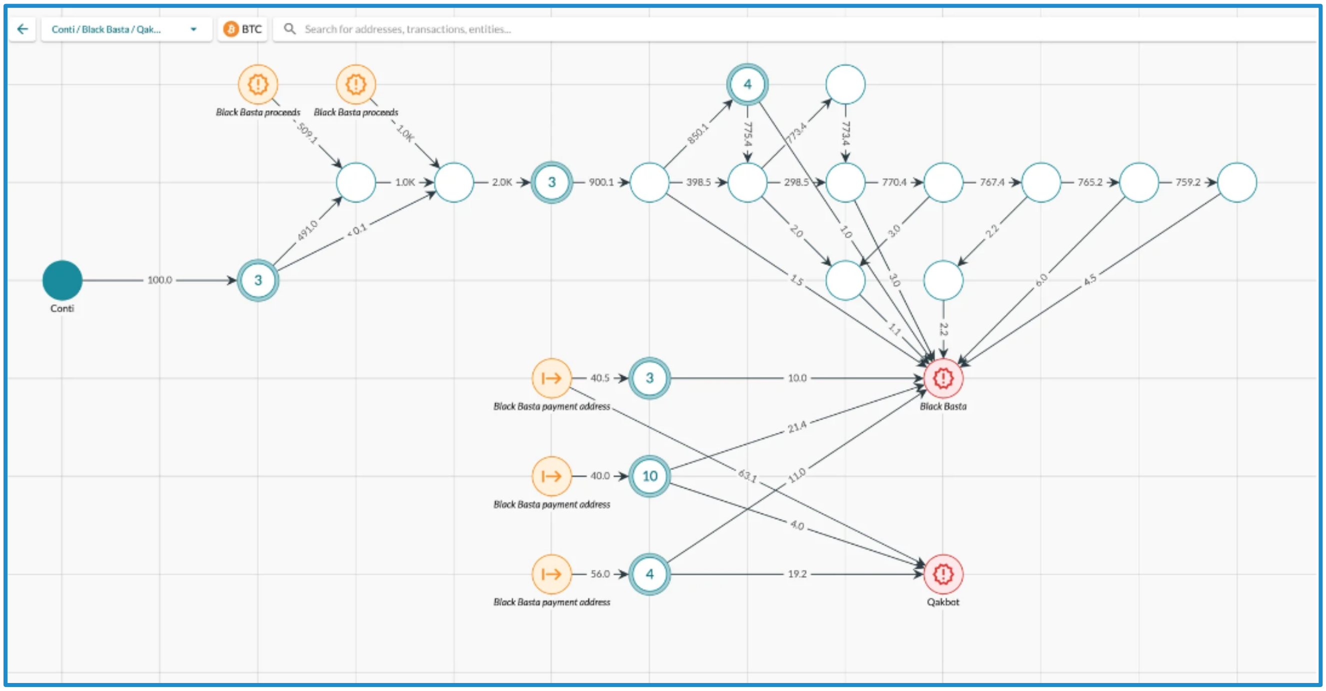
Many ransomware groups operate a "Ransomware as a Service" business model that is driven by human intelligence and research. This has further decreased the barriers to entry for any cybercriminal. Ransomware as a Service is a "modular" business model where individuals with limited technical skills can leverage the malware developed by others to conduct their own attacks.

Developers or managers will use hacker forums to recruit affiliate hackers. Affiliates often pay another type of threat actor known as an "initial access broker" to gain access to victim networks. This specialization of labor among criminals with different skillsets has been a primary driver of the increase in ransomware frequency in recent years. The emergence of this supply chain, which began to take hold in 2019, enables a small group of ransomware operators to attack victims on a much larger scale.



To facilitate the business aspect of the relationship, developers create and run ransomware and payment sites with affiliates who hack businesses and lock their devices. Developers typically get 20-30% of any ensuing ransom, with affiliates receiving 70-80%. This is effectively a crime syndicate where each member is paid for a particular expertise. Affiliates can work with one or more ransomware groups at any given time.

Sometimes, particularly after notable events, ransomware groups may rebrand. According to blockchain analytics company Elliptic, in the example below, on-chain links were identified to support the suggestion of a connection between Conti and Black Basta ransomware groups. Examining the blockchain data also revealed that a portion of some victims' ransoms were sent to Qakbot malware wallets.



A screenshot from Elliptic blog post available at [Black Basta ransomware victims have paid over $100 million (elliptic.co)]

F. Opportunities for Disruption

Disruption of criminal activity does not eliminate the problem, but it raises the cost of committing the crime. Arrests and prosecution in cybercrime can be difficult, disrupting the infrastructure that is used by cybercriminals in ransomware attacks is therefore a key part of deterrence. In the case of ransomware, there are opportunities for both the public and private sector to focus on making the crime more difficult to commit (infrastructure and supply chain disruption) and opportunities to focus on making the crime less profitable (payment disruption). The theory is that by shifting this balance, criminal actors will abandon this crime.

1. **Disrupt the ability for the criminal syndicate and affiliates from doing business with each other.**

Engaging in public-private partnerships to infiltrate the ransomware supply chain and intercept attacks to impose costs on criminals makes it more difficult for them to target critical infrastructure and financial institutions. Successfully targeting the supply chain itself would limit the ability of ransomware affiliates and operators to outsource parts of the attack lifecycle and reduce the number of victims they could successfully attack. These engagements can also surface technical indicators on threat actors across the supply chain, leading to more opportunities for offensive operations. Law enforcement has been able to leverage intelligence from a technology company's threat actor engagements to access ransomware affiliate command and control servers, access decryption keys that are then offered to victims experiencing attacks, and identify infrastructure used by the access brokers supplying affiliates with victims.

2. **Disrupt the infrastructure by targeting the criminal actor's ability to communicate with the victim or publicly disclose stolen data.**

There is not a "one-size-fits-all" infrastructure disruption that will eliminate ransomware; rather, disruption will make it more difficult for the criminal actor to accomplish their goals, thereby raising the cost of committing this crime. Generally, infrastructure disruption focuses on removing the infrastructure such as websites, servers, or email accounts that enable the criminal actor to negotiate the ransom with the victim and publicly disclose the victim's sensitive data. Ransomware attacks often use the same infrastructure for multiple campaigns.

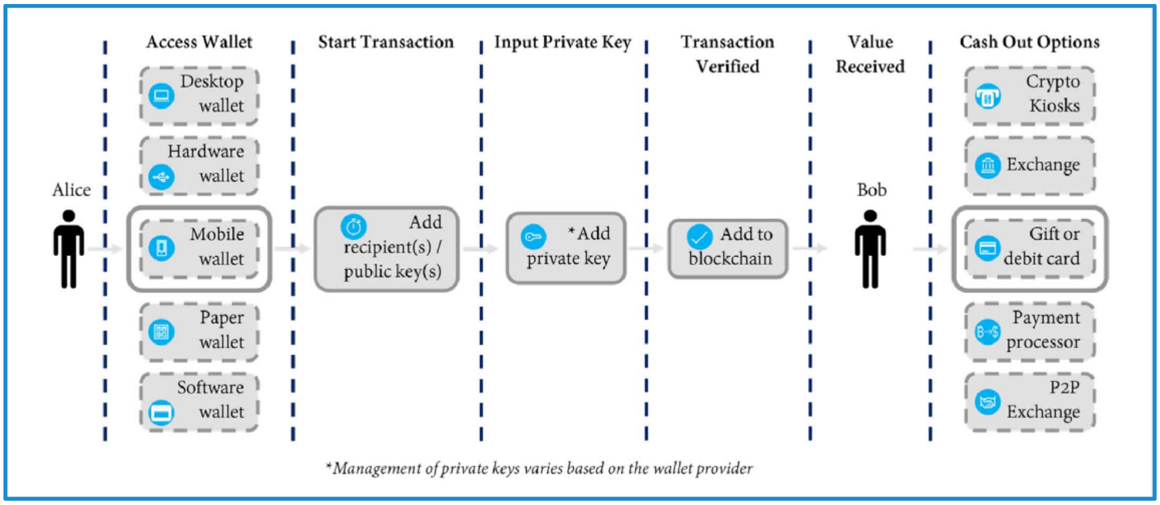
Cybercriminals decide how to conduct their attack based on what security tools were present, whether the network had good cyber hygiene, and which data the cybercriminals wanted to exfiltrate from the network.

Although the new Ransomware as a Service business model relies on a variety of tools and ultimate choice of ransomware, all of them need to operate in a similar manner to effectively extract payment from victims. The infrastructure used is rather consistent. For example, every ransomware scheme needs a location to publicize the stolen data and an opportunity to establish communication with their victims to negotiate the terms of the ransom. This provides a disruption opportunity.

3. **Disrupt the payment distribution system by targeting intermediaries that support the vulnerable elements of the system.**

Disrupting the payment distribution system that supports this crime makes ransomware attacks less profitable. Improving our technical means and legal process for disrupting the infrastructure that supports payments earned through ransom will significantly impact the profitability (and thereby prevalence) of this crime. Because the payment distribution system and the intermediaries that support the money flow range across international borders, disrupting the payment distribution system will require a global strategy.

The infographic below demonstrates the flow of payment and opportunities for disruption: a victim (Alice) will obtain a wallet that is able to send cryptocurrency. There are several types of wallets – wallets that are held by a service provider on behalf of the owner (otherwise known as a "custodial" wallet) or wallets that are in the sole custody of the owner and are not accessible by any other party (otherwise known as a "non-custodial" wallet). Victims and criminals may use either custodial or non-custodial wallets. There are a series of actions that are taken to send cryptocurrency in a pseudonymous manner ultimately resulting in its receipt by the criminal (Bob). B ob then has a variety of choices to convert his cryptocurrency payment into traditional fiat currency, like U.S. dollars. Those options include going through a crypto kiosk (which is akin to an automated teller machine), using a crypto exchange, using a peer-to-peer exchange, or using an over-the-counter trading desk. Other options include purchasing gift cards, gambling, or going through some other payment processor. It is these on-ramps (exchanging fiat currencies for cryptocurrency) and the off-ramps (exchanging cryptocurrency into fiat currency) where the criminal actor is most vulnerable and the opportunity for disruption is greatest.



Infographic taken from U.S. Department of Justice Report of the Attorney General's Cyber Digital Task Force

Regardless of where ransomware is deployed, typically the threat actors will demand payment via cryptocurrency. Though the underlying blockchain technology facilitates transparent cryptocurrency flows, the owners of wallets remain pseudonymous. To achieve this pseudonymity, first a threat actor must create a wallet either by, for example, using software or creating an account with a wallet provider and second, the threat actor will seek to cash out its crypto currency through some sort of platform. At its core, the criminal actor needs to append the blockchain with a transaction and ultimately find a way to cash out. Most stakeholders in this cryptocurrency system do not want their platforms used for nefarious purposes. Those that are compliant with U.S. laws are interested in partnering with the security community to make it more difficult for criminal actors to use their platforms. However, some wallet service providers and crypto currency exchanges can exist in jurisdictions that are either unwilling or unable to effectively police these service providers. These intermediaries facilitate the flow of ill-gotten earnings from ransomware. The private sector through civil litigation, and the government through criminal seizure, regulatory enforcement, and international collaboration can take coordinated action to disrupt these weak points in the payment process.

For example, in traditional anti-money laundering (AML) operations – whether the ill-gotten earnings are in fiat or cryptocurrency – the idea is to make it more and more difficult to exit successfully laundered funds. In cryptocurrency, that takes the form of screening payments for smaller and smaller exposure to ransomware attacks. Once the proceeds derived from those attacks are labeled, whether they have gone through bridges, across multiple assets, or passed through many wallets, identification remains possible. To dissuade ransomware attackers, firms serving as fiat offramps for crypto must push the thresholds lower and lower, holistically detecting exposure to ransomware attackers and making obfuscation more and more difficult. This results in increasingly convoluted and obviously obfuscated transaction patterns, explicitly designed to evade analytics programs. In turn, this makes the activity increasingly more detectable, as there may be no legitimate business purpose for such complicated transactional patterns.

I applaud the U.S. Department of Justice's focus on victims and executing successful operations to not only identify and indict threat actors but to also obtain decryption keys and seize wallets and cryptocurrency from these threat actors.

G. Improving resilience and raising awareness for potential victims.

Although disruption is important, improving organizational awareness and resilience is equally important. Potential victims, governments, organizations, and businesses of all sizes are at varying levels of preparedness maturity. Ensuring that all potential victims increase their security and resilience is key.

Cybercriminals who install ransomware use tried and true methods for access. Often, applying basic cybersecurity hygiene can prevent a cybercriminal's ability to ransom a system. Several technology companies recommend at least four basic steps that can be effective for both large and small organizations to **prevent**, **detect,** and **respond** to a ransomware attack: (1) inventory your assets, (2) prioritize patching,[10] (3) deploy endpoint detection/recovery and multifactor authentication tools, and (4) ensure appropriate configuration of systems and software.

On patching, consider the ransomware attack on Change Healthcare.[11]The attackers got to Change Healthcare through the ConnectWise software flaw (CVE-2024-1709) which, according to CISA's Known Exploited Vulnerabilities (KEV) Catalog, contains an authentication bypass vulnerability that allows an attacker with network access to the management interface to create a new, administrator-level account on affected devices. ConnectWise is a remote access technology generally used by small and medium sized businesses. Exploitation of remote desktop protocols is a common entry point for ransomware actors. CISA posted this vulnerability to the KEV Catalog on February 22, 2024, which is the same day that UnitedHealth filed its Form 8-K disclosing the cyber incident. NIST gave this vulnerability a high severity score of 10.00.

[10] CISA's known exploit vulnerability (KEV) catalog is a great source for critical patches. In November 2021, CISA exercised its authority to issue a binding operational directive (BOD 22-01) to require federal civilian executive branch agencies to remediate any such vulnerabilities included in the KEV catalog.

[11] See Exclusive: Cyberattack on Change Healthcare was an exploit of the ConnectWise flaw | SC Media (scmagazine.com)

On multifactor authentication, consider the ransomware attack on EDGAR, the Securities and Exchange Commission's Electronic Data Gathering, Analysis, and Retrieval system.[12] Cybercriminals were able to access the network through an IT Administrator's password that was compromised in an earlier breach.[13] A study[14] done at Microsoft estimates that more than 99% of all cyberattacks would have been prevented if multi-factor authentication were deployed. Multi-factor authentication is important to raising friction for entry but will take time to complete as part of a larger security journey. Other steps can be taken to identify and close off vulnerable entry points. Limiting the scope of damage forces the attackers to work harder to gain access to multiple business critical systems by establishing least privileged access and adopting Zero Trust Principles. These steps make it harder for an attacker who gets into a network to travel across the network to find valuable data to lock up. There are many resources that describe how to do this effectively, and simple tools, like those from the Cyber Risk Institute[15] or the Center for Internet Security,[16]can help even small and medium sized businesses do this work. Finally, encouraging potential victims to prepare for the worst-case scenario is designed to minimize the monetary incentives for ransomware attackers by making it harder to access and disrupt systems and easier for victims to recover from an attack without paying the ransom.

If a persistent actor defeats a company's cyber defenses, a company should be prepared to minimize downtime and improve opportunities for **recovery**. A ransomware actor is betting on a company making the choice to pay a ransom to offset the costly prospect of downtime. Enterprises could also benefit from improving their governance and recovery system by taking several proactive steps:

- Map your critical assets and define the priorities in which your systems should be recovered. During a ransomware incident, you will want to focus on recovering the most critical applications and the infrastructure on which they are dependent first.
- Develop an offsite/offline backup of the information system and the information that flows through it.
- Develop and test a resilience and incident response plan to withstand the market forces that contribute to decisions to pay the ransom. This is a dynamic process. Entities must continuously update and test these plans to be effective.
- Ensure appropriate configuration of identity systems. As the vast majority of attacks now include a breach of an identity system, bad actors try to take advantage of misconfigurations in identity systems such as Active Directory, Entra ID, Okta, and others. Once an identity system is fully compromised the attacker effectively has all the required permissions to own the enterprise.
- In many of the recent attacks prior to the encryption of the enterprise production systems, the bad actor encrypted the backup and recovery system. Make sure to review who has access to your backup and recovery solution, reduce access to the required personnel only, and monitor in real time for any changes.
- Make sure that the management team is confident in the recovery procedure, including how much down time the company will need to work through so they can be confident when they decide.

Paladin recommends that the government enable federal and non-federal entities to develop governance and preparedness models that counteract a ransomware actor's tactics to delay recovery in hope to improve the chances that an entity will ultimately pay the ransom. Although NIST has done an excellent job of addressing many aspects of these attacks, organizations still struggle with where to start (especially smaller organizations with limited staff and experience). Any government guidance should clearly state top security priorities, and why they are important. For example, a simple three-step approach could be effective: (1) prepare for the worst, (2) limit the scope of damage. and (3) make it harder to get in.

[12] Column: He spent 24 years building his business. A ransomware attack blew it to smithereens (yahoo.com)
[13] Hiltzik: The threat of ransomware - Los Angeles Times (latimes.com)
[14] Microsoft Report
[15] See Cyber Risk Institute – Don't risk risk.
[16] See CIS Center for Internet Security (cisecurity.org)

The Stop Ransomware website hosted by DHS/CISA remains a fantastic resource for explaining ransomware, providing a step-by-step guide to responding to a ransomware attack, and providing best practices for preparedness. However, awareness should not stop there. The government should also engage in public outreach efforts to help companies prepare for the worst and take steps to improve resilience.

H. The importance of public–private partnerships

Just as committing ransomware attacks requires collective effort, countering ransomware attacks needs the same focus and global coordination. As these attacks have evolved to more enterprise-like operations involving multiple players, countering these efforts requires a multi-stakeholder approach. Each of us has an important role to play, with the foundation of our efforts being reliable information and operational collaboration. The private sector and the U.S. government have engaged in and experimented with technical and legal models, globally, to disrupt and dismantle cybercrime infrastructure. Efforts to date illustrate that a collaborative multi-stakeholder approach – sharing actionable information and leveraging the combined capabilities of the private sector and the government – yields the best opportunity to disrupt cybercrime quickly and at scale.

Our direct experience with technology companies engaging in public-private partnerships has shown how potent collaboration can be. At least one technology company that helped facilitate many hundreds of FBI victim notifications has had an impact far wider than just the victims saved. In one engagement, an attack was intercepted against an IT Provider that has over 600 large financial institution customers. The threat actor was planning to sell access to a ransomware affiliate who would then attempt to encrypt many dozens of the IT Provider's customer networks. The potential ripple effect could have created a catastrophic impact, not just on the victim's business, but many of its customers. The ability to scale up public-private partnerships like this can have disruptive effects on the criminal supply chain, making it harder for ransomware affiliates to find and attack victims.

The take down of Emotet, a botnet known to support the distribution of the Ryuk ransomware, involved law enforcement around the world as well as private sector security researchers. Individual computers infected with malicious software are called bots. These bots are controlled by the cybercriminal to create a botnet –that can be used to engage in further criminal activity. These botnets can range from a few hundred to tens of millions of compromised systems. In taking down the Emotet botnet, law enforcement seized assets and arrested the cyber criminals in Ukraine while researchers working with law enforcement took down Emotet's command and control infrastructure used to operate the botnet and cleaned the individual computers in the botnet. The effort involved a worldwide coalition of law enforcement agencies across the U.S., Canada, the UK, the Netherlands, Germany, France, Lithuania, and Ukraine to disrupt and take over Emotet's infrastructure which was located in more than 90 countries[17] — while simultaneously arresting at least two of the cybercriminals. [18]

As the U.S. government has recognized, for example, with the creation of the interagency ransomware taskforce and the FBI's cyber strategy, unilateral action, whether public or private, is not a sustainable solution against nation-state sponsored or financially motivated, sophisticated, organized cybercrime. To combat ransomware, we recommend:

- Clearly measuring the impact of ransomware on specific sectors and the broader U.S. economy: Cybercriminals currently take advantage of the internet and the limitations of sovereignty to carry out crime against victims located anywhere in the world, while the internet and technological tools enable cybercriminals to operate with almost absolute anonymity.

[17] Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware' | WIRED

[18] For a more recent example, this podcast describes an incident where a school system received a warning from the government about a breach that was about to turn into ransomware of their system and then engaged two private sector entities, Semparis and CrowdStrike to successfully fight it off.

- Focusing on what can be done to address the problem: In addition to focusing on disruption to raise the costs of the crime of a ransomware attack, entities must also focus on preparedness and recovery to improve the likelihood that a victim will find it more cost effective to be well prepared to withstand minimal downtime.
- Increasing focus on critical areas: To increase the scope and scale of disruptions, public-private collaboration, threat tracking and prioritization, and victim remediation needs to be improved.

A collaborative, multi-stakeholder approach to countering cybercrime, including ransomware must be nimble and function at scale. We have seen a shift in the U.S. government and foreign governments to actions to disrupt cybercriminal infrastructure. Traditional enforcement mechanisms are a critical piece of global cybersecurity and U.S. national security; however, we must continue to focus on the more immediate "takedown" or disruption of infrastructure, which more strategically aligns with the needs and priorities of many victims and is a significant public interest. This focus on preparedness, resilience, and disruption should be a primary strategy to combat ransomware.

I. Conclusion

I am pleased to see that the U.S. Government, the security community, state and local governments, and the international community are coming together for a coordinated response to ransomware. There is much work that needs to be done but I am optimistic that we collectively have the leadership and ability to accomplish our goals. The Ransomware Task Force published a set of thoughtful and measured policy and operational recommendations, including several that may require legislative action. Approximately half have been implemented to date and I encourage all stakeholders involved to act where they can to reduce the incidence of ransomware attacks.