My Drift

Title: Ransomware
Written by: Jerry D. Petersen
Date: 31 Aug 2021
Article Number: 368-2021-17

I think most of us have heard about the recent ransomware attacks on the Colonial Pipeline, Microsoft, banks, hospitals, JBS Foods, and Acer. We will look at these attacks in more details later in this article. Yes, ransomware is bad, and it could happen to you and me. So, let's learn a few things about it.

What is Ransomware?

Ransomware is a type of malicious software cybercriminals use to block you from accessing your own data. The digital extortionists encrypt the files on your system and add extensions to the attacked data and hold it "hostage" until the demanded ransom is paid. During the initial infection, the ransomware may attempt to spread throughout your network to shared drives, servers, attached computers and other accessible systems. Modern ransomware has been seen building in periods of dormancy. During this time, the cybercriminals extort company data, and the malware has the potential to be backed up along with legitimate data, invalidating the use of backups for recovery. If the ransom demands are not met within the timeframe – the system or encrypted data remains unavailable, data may be deleted by the software and the decryption key obliterated. Extortion is increasingly common and in the event an organization refuses to pay the ransom, stolen data may be sold on the dark web. In short, ransomware is a nightmare for unprepared IT administrators.

How Ransomware Works

Ransomware enters your network in a variety of ways, the most popular is a download via a spam email attachment. The download then launches the ransomware program that attacks your system. Other forms of entry include social engineering, downloads of malicious software from the web that can be direct from a site or by clicking on fake ads that unleash the ransomware. The malware can also be spread through chat messages or even removable USB drives.

Typically, the software gets introduced to your network by an executable file that may have been in a zip folder, embedded within Microsoft Office document's macros, or disguised as a fax or other viable attachment. The download file then encrypts your data, adds an extension to your files and makes them inaccessible. More sophisticated versions of the software are propagating themselves and can work without any human action. Known as "drive-by" attacks, this form of ransomware infects your system through vulnerabilities in various browser plugins.

What are the Different Types of Ransomware?

Ransomware variants takes many forms, below are some of the most common types:

1. Crypto ransomware or encryptors are one of the most well-known and damaging variants. This type encrypts the files and data within a system, making the content inaccessible without a decryption key.

2. Lockers completely lock you out of your system, so your files and applications are inaccessible. A lock screen displays the ransom demand, possibly with a countdown clock to increase urgency and drive victims to act.

3. Scareware is fake software that claims to have detected a virus or other issue on your computer and directs you to pay to resolve the problem. Some types of scareware lock the computer, while others simply flood the screen with pop-up alerts without actually damaging files.

4. Leakware threatens to distribute sensitive personal or company information online, and many people panic and pay the ransom to prevent private data from falling into the wrong hands or entering the public domain. One variation is police-themed ransomware, which claims to be law enforcement and warns that illegal online activity has been detected, but jail time can be avoided by paying a fine.

5. RaaS (Ransomware as a Service) refers to malware hosted anonymously by a "professional" hacker that handles all aspects of the attack, from distributing ransomware to collecting payments and restoring access, in return for a cut of the loot.

Ransomware Examples

Below are just a few examples of some infamous ransomware "Names" detected over the last few years:

WannaCry Ransomware

This ransomware first appeared in May 2017 and has left the major mark in the history of cyberattacks. WannaCry has brought down more than 200,000 systems across 150 countries, causing financial losses of more than $4 billion. This, for sure, makes it one of the most notorious examples of ransomware attacks in history. Some countries like the USA, the United Kingdom, and Australia insisted that North Korea was behind the attack.

How WannaCry Spreads

The first step is standard for ransomware infection: a user opens a phishing email and downloads malicious attachment through which malware infects the computer. But this type of ransomware doesn't stop there. It can spread across

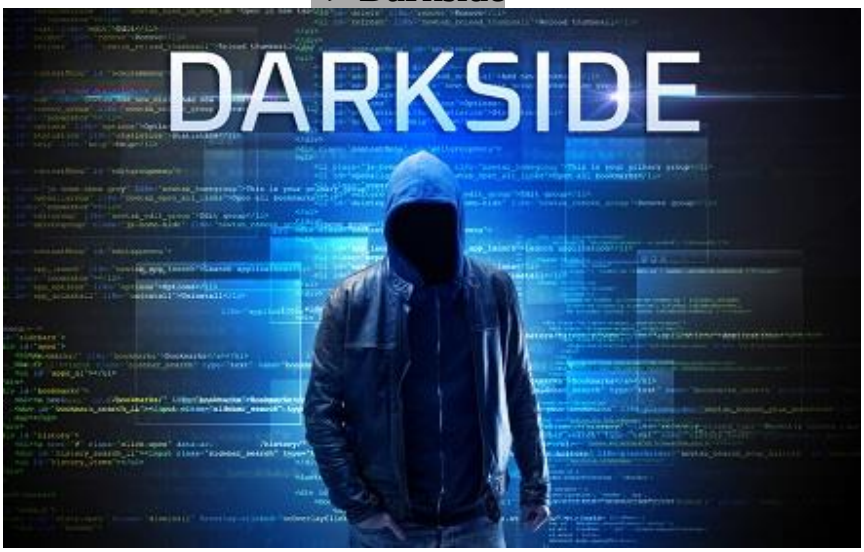
other connected computers by using a vulnerability in the Windows systems called Eternal Blue. More precisely – through the Server Message Block (SMB) protocol.

It doesn't infect all connected computers though – only those that have the same Eternal Blue vulnerability. Older versions of Windows still have that vulnerability. It has been fixed in Windows 10 and later providing you updated your Windows OS when updates or patches were first available. However, if you use a new Windows OS, you can be at risk as well if you don't update your OS on time. This is what happened with thousands of users who fell victim to WannaCry: they didn't download new patches in time. As a result – they got infected through the network without even clicking on anything.

How WannaCry Works

This ransomware tries to access a hard-coded URL, and, in case it can't, it starts to encrypt files in different formats. Once the files are encrypted, the user sees a ransom notification (like the one above) that demands $300 in Bitcoin.

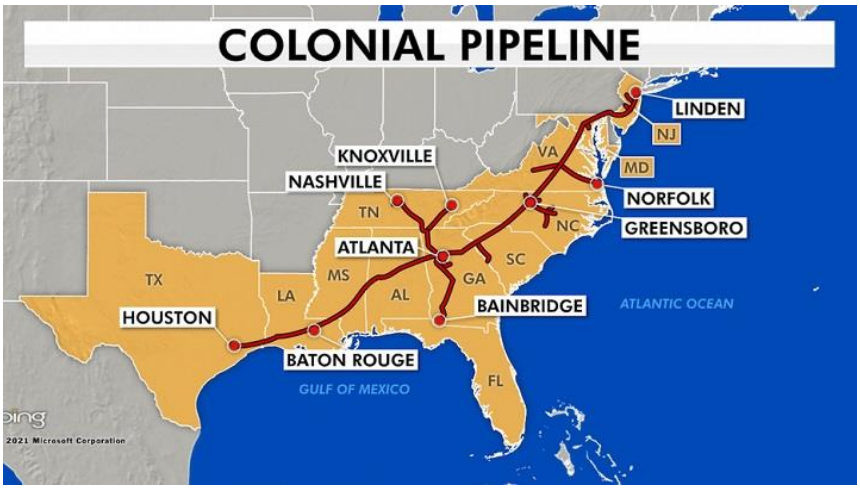
Darkside



Colonial Pipeline Ransomware Attack

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. In response, Colonial Pipeline Company halted all of the pipeline's operations to contain the attack. With the assistance of the FBI, Colonial Pipeline paid the requested ransom (75 bitcoin

or $4.4 million) within several hours after the attack. The hackers then sent Colonial Pipeline a software application with the decryption key necessary to restore their network.



This was the largest cyberattack on an oil infrastructure target in the history of the United States. The FBI and various media sources identified the criminal hacking group DarkSide as the responsible party. DarkSide is believed to be based in Russia. The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack.

On June 7, the Department of Justice announced that it had recovered 63.7 of the bitcoins (approximately $2.3 million) from the ransom payment.

REvil

REvil (Ransomware Evil; also known as Sodinokibi) is a Russia-based private ransomware-as-a-service (RaaS) operation. After an attack, REvil would threaten to publish the information on their page "Happy Blog" unless the ransom was received.

REvil has emerged as the world's most notorious ransomware operators. In just the past month (June 2021), it extracted an $11 million payment from the U.S. subsidiary of the world's largest meatpacking company based in Brazil, demanded $5 million from a Brazilian medical diagnostics company, and launched a large-scale attack on dozens, perhaps hundreds, of companies that use IT management software from Kaseya VSA.

Kaseya VSA (Virtual System Active Directory) is a cloud-based IT management and remote monitoring solution for businesses of all sizes across various industries. It provides a central console for managing IT operations including handling complaints, ticketing, auditing, monitoring performance and reporting.

REvil started operating in 2018 when they were working with a group known as GandCrab. At the time, they were mostly focused on distributing ransomware through malicious advertisements and malware tools that hackers use to infect victims through drive-by downloads when they visit a malicious website.

That group morphed into REvil, grew, and earned a reputation for exfiltrating massive data sets and demanding multimillion dollar ransoms. It is now among an elite group of cyber extortion gangs that are responsible for the surge in debilitating attacks that have made ransomware among the most pressing security threats to businesses and nations around the globe.

Encryption is the process of translating plain text data into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plain text data.

REvil is one of the most prominent providers of ransomware as a service (RaaS). This criminal group provides adaptable encryptors and decryptors, infrastructure and services for negotiation communications, and a leak site for publishing stolen data when victims don't pay the ransom demand. For these services, REvil takes a percentage of the negotiated ransom price as their fee. Affiliates of REvil often use two approaches to persuade victims into paying up: They encrypt data so that organizations cannot access information, use critical computer systems, or restore from backups, and they also steal data and threaten to post it on a leak site (a tactic known as double extortion).

The gang behind REvil operations often stage and exfiltrate data followed by encryption of the environment as part of their double extortion scheme. If the victim organization does not pay, REvil threatens to publish the exfiltrated information. REvil focuses on attacking large organizations, which has enabled them to obtain increasingly large ransoms. REvil and its affiliates pulled in an average payment of about $2.25 million during the first six months of 2021. The size of specific ransoms depends on the size of the organization and type of data stolen. Further, when victims fail to meet deadlines for making payments via bitcoin, the attackers often double the demand. Eventually, they post stolen data on the leak site if the victim doesn't pay up.

Finally, some good news

President Biden and Russian President Putin - June 16, 2021, Meeting

After that meeting and a July 9th phone call between Joe Biden and Vladimir Putin, Biden told the press, "I made it very clear to him that the United States expects when a ransomware operation is coming from his soil even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is." Biden later added that the United States would take the group's servers down if Putin did not.

As of July 13th, The REvil Ransomware Hackers have gone offline. The group's dark web site, dubbed the "Happy Blog," has been shut down and REvil has not attacked anybody since then. Maybe Biden's meeting and phone call did some good after all!

Regardless, there are still thousands of ransomware hackers out there attacking companies all around the world. Here are a few of them:

- **Locky**
- **Bad Rabbit**
- **Bit Paymer**
- **Cerber**
- **Cryptolocker**
- **Dharma**
- **Doppel Paymer**
- **GandCrab**
- **Maze**
- **MeduzaLocker**
- **NetWalker**
- **NotPetya**
- **Petya**
- **Ryuk**
- **SamSam**

A Few Other Famous Attacks

Responsible for one-third of the 203 million U.S. ransomware attacks in 2020, the Ryuk Ransomware Gang is the most prolific in the world and has targeted at least 235 US hospitals.

With ties to Russian government security services and named after its signature software, Ryuk has hit general hospitals and inpatient psychiatric facilities in addition to dozens of other healthcare facilities in the US since 2018.

Ryuk Ransomware collected at least $100 million in paid ransom last year. Some of the criminal group's most recent healthcare targets include King of Prussia, Pa.-based Universal Health Services, which lost $67 million from Ryuk's malware attack last September, and DCH Health System in late 2019.

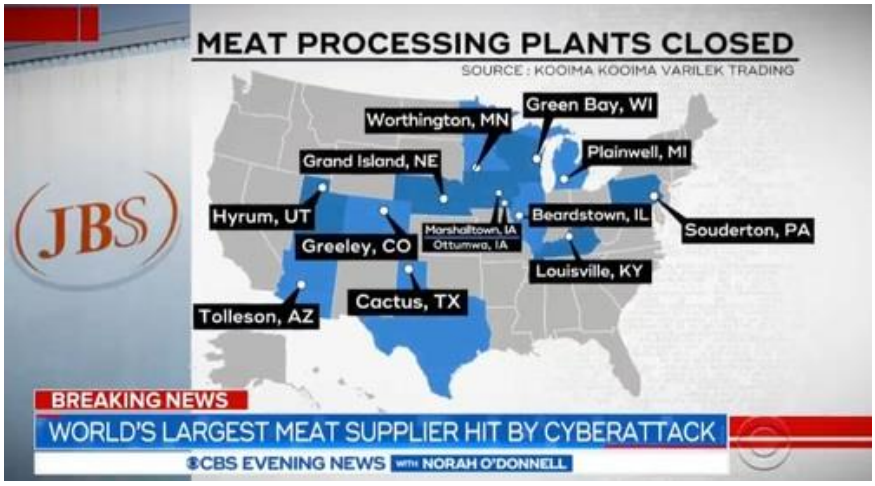
While some ransomware gangs avoid hospitals over fear of disrupting operations that could lead to patient deaths, Ryuk doesn't care! Ryuk uses disposable webmail accounts to negotiate with victims and speaks with a single, consistent voice, terse and to the point, and offering no hint of a personality.

Ryuk also uses victim's financial documents during some negotiations. If the hospital says they can't afford to pay the ransom, the hackers respond back with financial documents in their email and say, "Yes you can."

Ryuk counts on its attacks to wreak havoc. A security analyst who monitors the Eastern European underground said he saw a Ryuk organizer discussing plans online to attack 400 hospitals in the U.S. and saying, "expect panic."

JBS Foods

JBS Foods, the world's largest meat supplier and a recent ransomware victim, revealed on June 9, 2021, that it paid $11 million to hackers. The FBI announced the following day that the attack came from a hacker organization known as REvil which is believed to be based in Russia.



ACER

In May 2021, the computer manufacturer Acer was attacked by the REvil hacker group, the same group responsible for an attack on London foreign exchange firm Travelex. The $50 million ransom stood out as the largest known to date. REvil hackers exploited a vulnerability in a Microsoft Exchange server

to get access to Acer's files and leaked images of sensitive financial documents and spreadsheets.

Banks Hit in Global $70M Ransomware Attack
US banks are among hundreds of companies affected by a global ransomware attack involving financial organizations around the world being extorted for a record ransom of $70 million.

How can Banks/Credit Unions Protect their Data from Ransomware Attacks?

According to the Ohio Bankers League, several banks were targeted in the attack orchestrated by the notorious REvil cyber-criminal network on July 5, 2021.

Ransomware Statistics

1. There were more than 304 million ransomware attacks worldwide last year (2020). A company, organization, or computer user is attacked every 12 seconds. About 146 million of these attacks took place in the United States.

2. 73% of all ransomware attacks were successful in encrypting data.

3. 55% of attacks hit businesses with 100 or fewer employees. 75% of attacks struck organizations with less than $50M in annual revenue.

4. According to Microsoft, nearly 97% of all ransomware infections take less than 4 hours to successfully infiltrate their target. The fastest can take over systems in less than 45 minutes.

5. Downtime due to ransomware increased by 200% over the past year.

6. Downtime costs related to ransomware attacks are 2300% greater than the average ransom request.

7. 27% of businesses that fell victim to ransomware made payments to hackers.

8. The average ransom demand grew to more than $178,000 in 2020. However, average ransom demand for a small to medium sized business is only $5,900. For an individual, it is usually a smaller amount like $300.

9. More than 95 new ransomware families (virus types) have been discovered in the last 2 years.

10. The global cost associated with ransomware recovery will exceed $20 billion in 2021.

How to defend against Ransomware

Whether you need to know how to defend against REvil, Ryuk, or any of the other thousands of daily attacks, the first component of the solution is to educate co-workers about clicking suspicious links and downloading questionable file attachments. Training and testing help, and there are even solutions to help provide visual cues and feedback to further empower front line employees. This won't prevent all attacks, but it will help. It is also critical to ensure that your servers are being patched regularly, as many security gaps that ransomware hackers take advantage of are often protected in the latest Microsoft patches. Failing to stay up to date can cause major issues down the line. No matter what, you have to prepare for the reality that you may be attacked. It's critical you not only have backups but secure, tested backups and a well-documented disaster recovery plan – detailing the steps to remediate an attack. On the data protection side of things, keep these 5 things in mind:

1. **Protect**

Use backups! Follow the 3-2-1-1 rule. Maintain three copies of your data on 2 different types of media with 1 version stored off-site and one copy that is immutable (unable to be modified). Immutable media may be rotational media such as a disk or tape which is disconnected from the network and taken off-site to a secured secondary location. Some vendors offer immutable storage via a cloud service. If you do get hit by ransomware, having secure offsite copies will help you have an easier recovery. When considering offsite options, keep in mind recovery times are longer from offline backups, and offline backups can be more difficult to test. Faster recovery times can be achieved by replication to a hot target such as a secondary appliance or cloud service where backups are stored in a state that is readily available for recovery.

2. **Secure**

Ransomware predominantly targets Windows OS. Recent findings show more than 83% of malware is designed to penetrate Windows systems. As backup systems can require many role-based instances for centralized management, data movement, reporting, search, and analytics, securing all those machines can be complex. Consider locking them down to do only what they are required, and nothing more. Newer solutions based on integrated backup appliances typically remove that complexity and come hardened out of the factory. Security can be far simpler in those newer architectures.

3. **Test**

Regularly test the viability of your backup and disaster recovery strategy. Many factors can impede successful recovery, including attempting to restore from backups of machines that are already infected. Automated recovery testing is becoming a trend in the data management and data protection industry. These features must be used more as security threats become more impactful to IT.

4. **Detect**

Early ransomware detection means faster recovery. More backup vendors are starting to use predictive analytics and machine learning to recognize possible attacks and alert administrators of abnormal fluctuations of data as backups are ingested. Analyzing data based on several heuristic characteristics provides insight into threats traditional security tools don't catch and can be particularly helpful in identifying catching slower burning infections.

5. **Instant Recovery**

If you've effectively backed up your data and tested its recoverability, you will be ready to roll back your network to a safe restore point and avoid downtime, data failure and revenue loss.

Ransomware attacks are ferocious. It's not a matter of if, but when…be prepared with the above line of defenses.

What can your company do when it has suffered a Ransomware attack?

Victims of ransomware attacks have three options after an infection: they can either pay the ransom, try to remove the encryption, or rebuild/restart the device.

Without paying for the key, it is very difficult to decrypt files after an attack. A verified, tested, and secure backup eliminates the need to succumb to ransomware demands.

My Plan on what to do in the event of a ransomware or other malware virus attack that keeps me from using my computer.

I have never been the victim of a ransomware attack, but I have had many viruses and a couple that made my computer unusable. Remember that the effectiveness of most antivirus security software like McAfee detects and stops up to 98% of malicious software from entering your computer. Here is what do when my computer doesn't work right, and I suspect a virus:

1. **Restart my computer. If that don't work…**
2. **Turn it off and back on again. If that don't work…**
3. **Call McAfee tech support - my antivirus security provider. In most cases, the person I talk to (in India) is able to fix the problem by taking control of my PC and cleaning up all the bad stuff. However, twice it was so bad that McAfee techs could not fix it. In this case…**
4. **I unplug and unhook the cables from my PC and carry it outside and throw it in the trash.**
5. **Then I jump into my truck and drive down to Best Buy and buy a new computer. This is also what I would do if I was a victim of ransomware. No way in hell would I pay a ransom to a gang of hackers from Russia or China or North Korea.**

NOTE: Here is the part of my plan computer users need to pay attention to.

6. **I keep a backup of all my important files and data in at least two places – most of it is in three places.**

- **I backup all my important documents and data (pictures, articles, tax returns, my will, etc.) to a thumb drive. I alternate 4 thumb drives.**
- **I use Microsoft One Drive which is my automatic personal Cloud Storage. Most of my data is there if I need it.**
- **I also have my own website with GoDaddy where some of my data is stored out there somewhere on their server.**

7. **So, I hook up my new computer and call McAfee to get my antivirus security software downloaded and active. Then I download the Microsoft Office products and make sure my cloud storage is working. Then I plug in my most recent thumb drive and copy my important documents and data to my new computer.**
8. **I'm back in business!**

Do you have a Cyber Security Plan?

What is cybersecurity? ***Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks by hackers.***

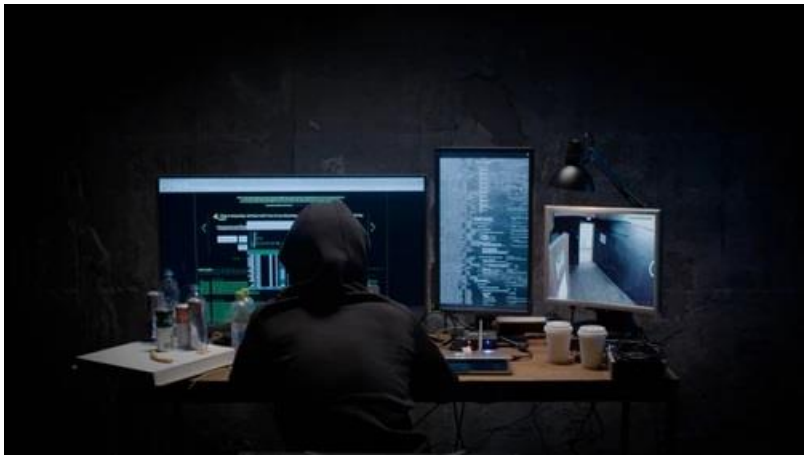
Some Burning Questions

What makes Russian hackers so good?

Since the 2016, hacking has become synonymous with one country: Russia.

But cybercrimes emanating from Russia and Russian-speaking countries have been around for years, fueling attacks like a 2014 data breach of more than 500 million Yahoo! accounts and a scheme that stole 160 million credit cards from American corporations.

"If someone wants to hack you, they're gonna be able to," a former expert NSA hacker stated. And if a Russian wants to hack you, they've certainly got the tools available to do it." The Department of Homeland Security confirmed that 75 percent of all ransomware attacks were created in Russia.



Russian Hacker

The apparent lack of ethical consideration in the buildup of Russian information technology and cybersecurity is rooted in decades of technical education under Stalin, who launched polytechnic schools to train engineers for his military-industrial complex. Russia's cyber capabilities can now be used for just about everything, ranging from digital bank robberies to tampering with critical infrastructure.

Spurred by the trillions of dollars online and a generation raised on the web, hacking from Russia and around the world is flourishing.

Do cybercriminals (hackers) ever get caught?
Yes, but not very often. Due to the sophisticated tactics that hackers use to cover their tracks, it's extremely difficult to catch them and bring them to justice. Only 5% of cybercriminals are apprehended for their crimes which demonstrates just how challenging it is for law enforcement agencies to arrest and prosecute these offenders.

Good Hackers are Rarely Caught

Hackers will often use secure software such as a proxy server to hide their identity and funnel their communications through lots of different countries in order to evade detection. Other technologies like Tor Browser and encryption enable them to add multiple layers to mask their identity. The combination of these tools allows them to commit their crimes undetected and in countries where they know they can't be prosecuted.

Tracking hackers down is laborious and often takes a lot of time, collaboration, and investigative research. Specialist cybercrime units need to be assembled to retrieve and analyze any potential evidence. Encrypted files will need to be decrypted, deleted files recovered and passwords cracked, etc.

What are the penalties for hacking?
The law punishes hacking under the computer crime statutes. These crimes carry penalties ranging from a class B misdemeanor (punishable by up to six months in prison, a fine of up to $1,000, or both) to a class B felony (punishable by up to 20 years in prison, a fine of up to $15,000, or both).

How much do good ransomware hackers make a year?
Nobody knows for sure, but it is probably more than a million dollars a year.

What is Cyberwarfare?
Cyberwarfare is the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes. As a major developed economy, the United States is highly dependent on the Internet and therefore greatly exposed to cyber attacks. At the same time, the United States has substantial capabilities in both defense and power projection thanks to comparatively advanced technology and a large military budget. Cyber warfare presents a growing threat to physical systems and infrastructures that are linked to the internet. Malicious hacking from domestic or foreign enemies remains a constant threat to the United States. In response to these growing threats, the United States has developed significant cyber capabilities.

The United States government and our military needs to figure out a better way to stop these ransomware hackers!

Bigdrifter44@gmail.com

Bigdrifter.com