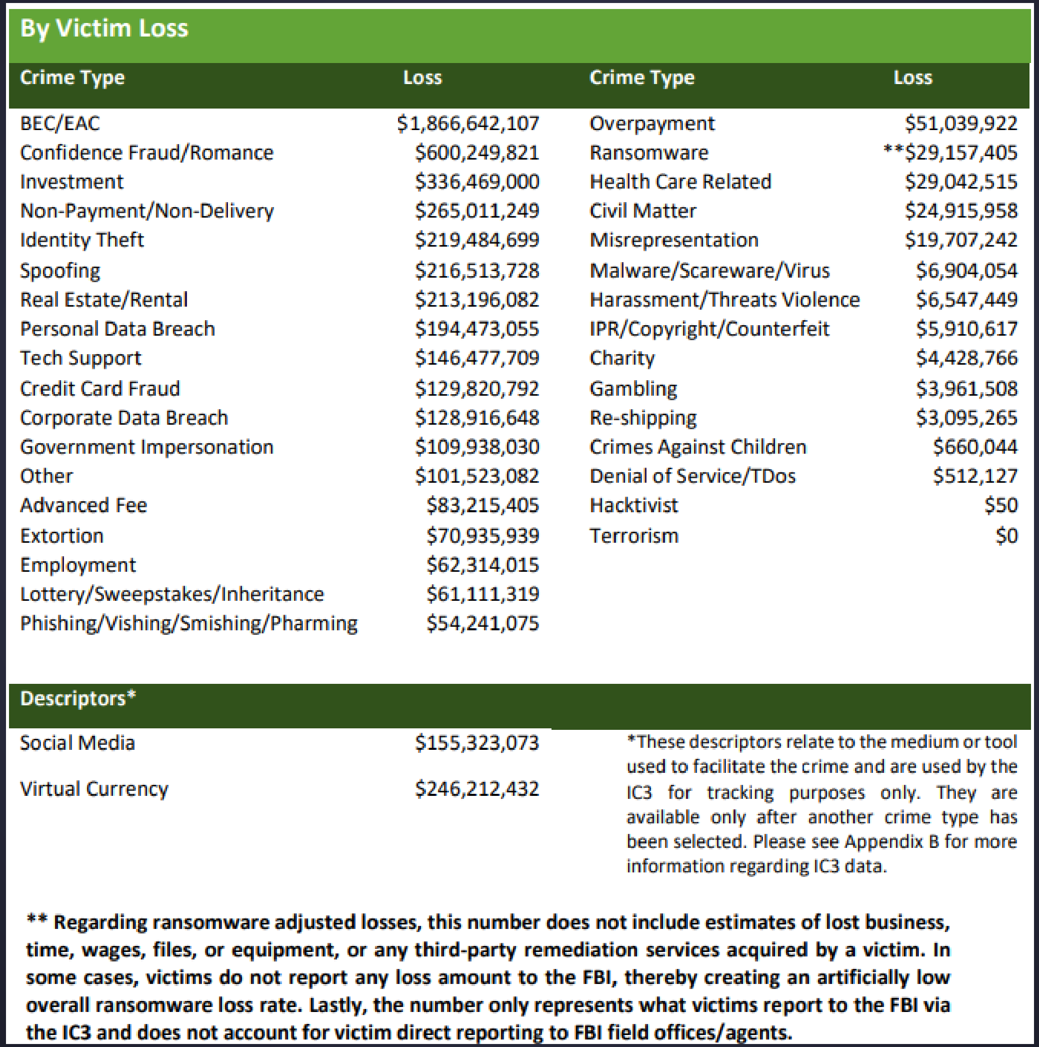
FBI
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
Graphic by
MTC Stephen Harris, USN Ret.

2020 Cyber Crime Losses



By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Descriptors*

Social Media	$155,323,073
Virtual Currency	$246,212,432

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

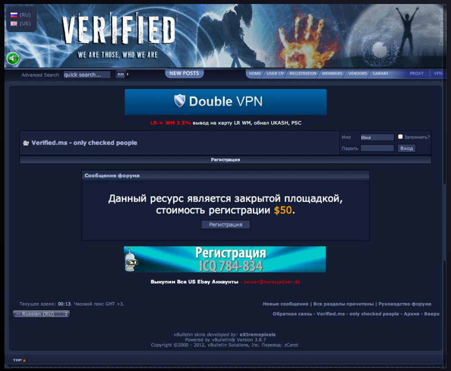
**** Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.**

Underground Economy

- <u>Communication</u>
  - Criminal Forums
  - Jabber
  - IRC
  - Signal, Whatsapp, etc.

- <u>Criminal Forums</u>
  - Multiple languages
  - Carding/Varied
  - Vetted
  - Multiple levels of administration

- <u>Services</u>
  - Money Laundering/Exchange
  - Bulletproof Hosting
  - VPN
  - Coding
    - Malware
    - Exploit Kits
  - Installs
  - Botnets as a service
  - DDoS
  - “Anti-Virus” check
  - Spam/Phishing/Spear Phishing
  - Hacking



LR-> WM 3.5% вывод на карту LR WM, обнал UKASH, PSC

Verified.ms - only checked people

Сообщение форума

Данный ресурс является закрытой площадкой, стоимость регистрации $50.

Выкупим Все US Ebay Аккаунты - power@swissjabber.de

Текущее время: 00:13. Часовой пояс GMT +3.

Новые сообщения | Все разделы прочитаны | Руководство форума

Обратная связь - Verified.ms - only checked people - Архив - Вверх

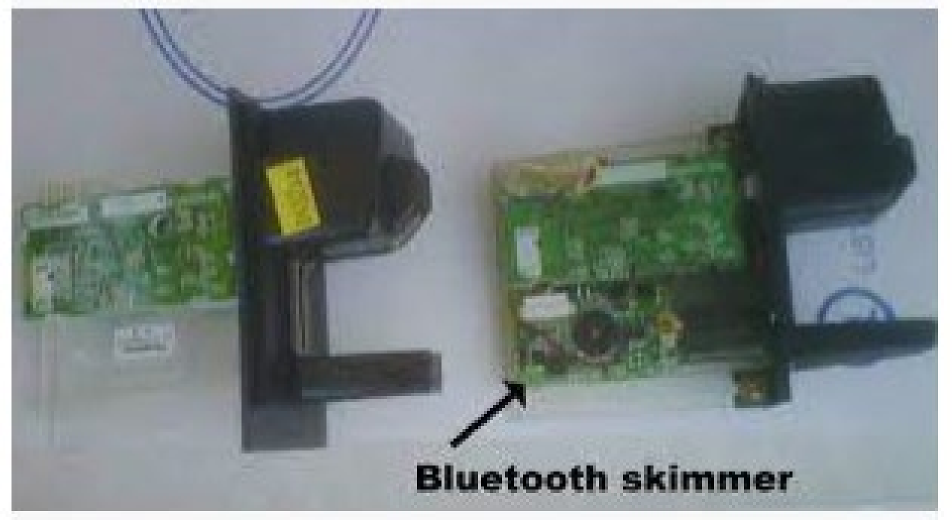
vBulletin skins developed by: eXtremepixels
Powered by vBulletin® Version 3.8.7
Copyright ©2000 - 2012, vBulletin Solutions, Inc. Перевод: zCarot

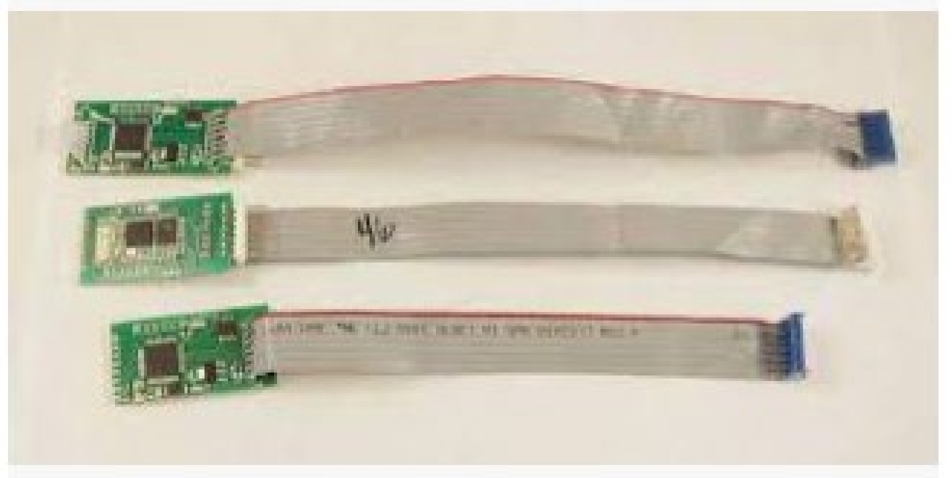
Fuel Pump Skimming

- Very inexpensive (< $1,000 per skimmer)
- Very profitable ($20,000 a week per skimmer)
- Undetectable to the victim
- Common across the entire United States and Europe
- Two basic categories
  - Local crews
  - Travel crews
- Used for several types of fraud
  - Goods purchased by the obtaining criminals
  - Sold to other criminals
  - Used for fuel theft
- Often laundered using Gift Cards

Skimmer Tools

Bluetooth Skimmers





Skimming Convictions

Yusbel Parrado

28 Months

Leonardo Prado

57 Months

Miguel Fornaris

45 Months

Andres Alvarez

39 Months

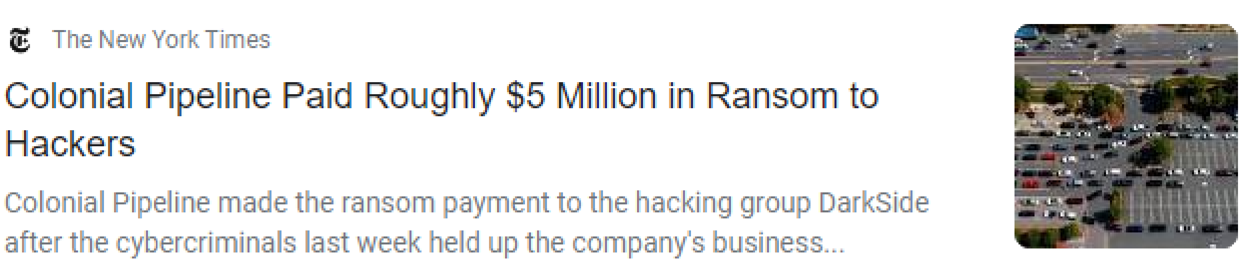
Misael Campos

60 Months

Pabel Vazquez

42 Months

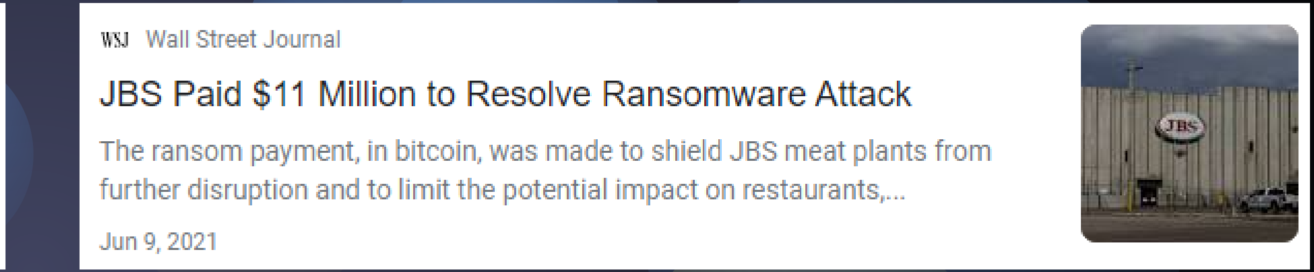
Ransomware



The New York Times

Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

Colonial Pipeline made the ransom payment to the hacking group DarkSide after the cybercriminals last week held up the company's business...

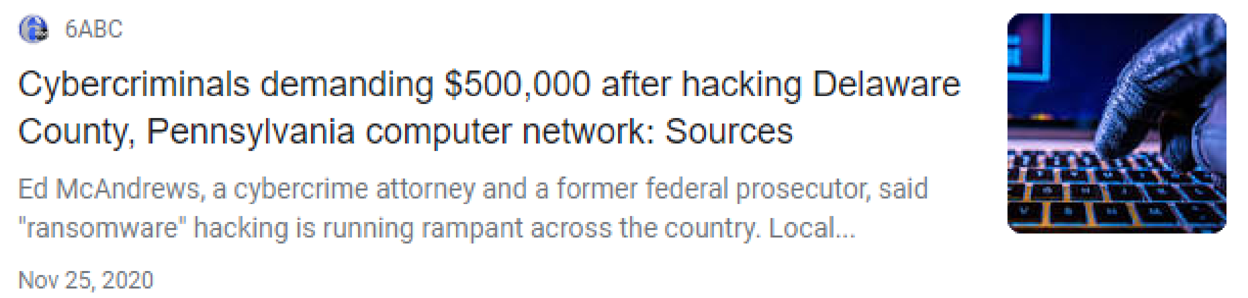


WSJ Wall Street Journal

JBS Paid $11 Million to Resolve Ransomware Attack

The ransom payment, in bitcoin, was made to shield JBS meat plants from further disruption and to limit the potential impact on restaurants,...

Jun 9, 2021

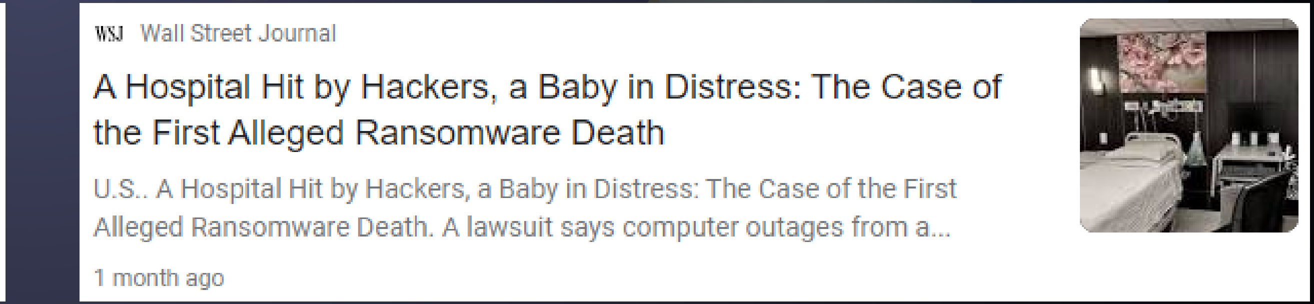


6ABC

Cybercriminals demanding $500,000 after hacking Delaware County, Pennsylvania computer network: Sources

Ed McAndrews, a cybercrime attorney and a former federal prosecutor, said "ransomware" hacking is running rampant across the country. Local...

Nov 25, 2020

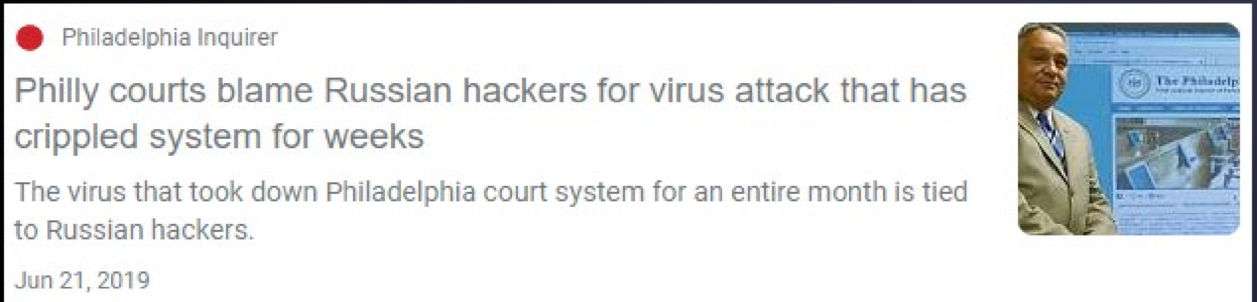


WSJ Wall Street Journal

A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death

U.S.. A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death. A lawsuit says computer outages from a...

1 month ago

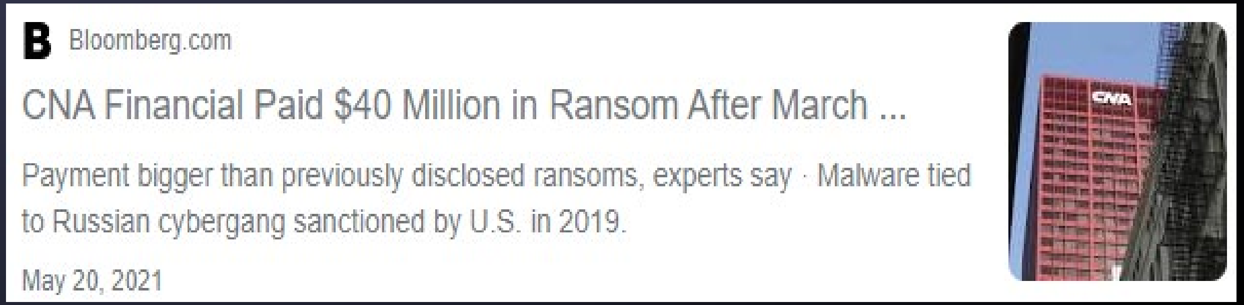


Philadelphia Inquirer

Philly courts blame Russian hackers for virus attack that has crippled system for weeks

The virus that took down Philadelphia court system for an entire month is tied to Russian hackers.

Jun 21, 2019



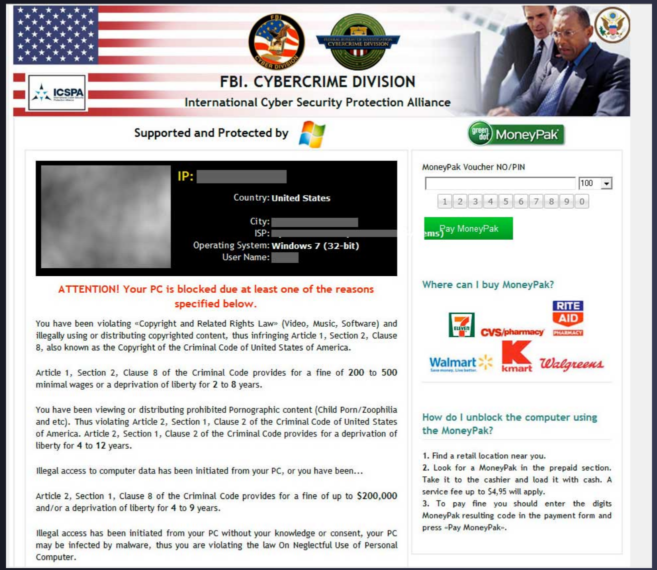
Bloomberg.com

CNA Financial Paid $40 Million in Ransom After March ...

Payment bigger than previously disclosed ransoms, experts say · Malware tied to Russian cybergang sanctioned by U.S. in 2019.

May 20, 2021

Ransomware



FBI. CYBERCRIME DIVISION

International Cyber Security Protection Alliance

Supported and Protected by

IP: [redacted]

Country: United States

City: [redacted]

ISP: [redacted]

Operating System: Windows 7 (32-bit)

User Name: [redacted]

ATTENTION! Your PC is blocked due at least one of the reasons specified below.

You have been violating «Copyright and Related Rights Law» (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 1, Section 2, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article 1, Section 2, Clause 8 of the Criminal Code provides for a fine of 200 to 500 minimal wages or a deprivation of liberty for 2 to 8 years.

You have been viewing or distributing prohibited Pornographic content (Child Porn/Zoophilia and etc). Thus violating Article 2, Section 1, Clause 2 of the Criminal Code of United States of America. Article 2, Section 1, Clause 2 of the Criminal Code provides for a deprivation of liberty for 4 to 12 years.

Illegal access to computer data has been initiated from your PC, or you have been...

Article 2, Section 1, Clause 8 of the Criminal Code provides for a fine of up to $200,000 and/or a deprivation of liberty for 4 to 9 years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer.

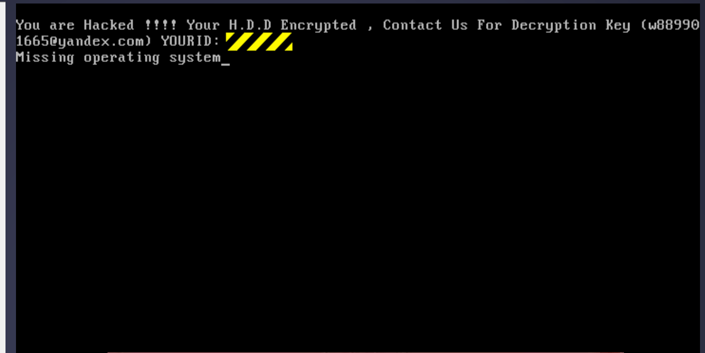
MoneyPak Voucher NO/PIN

100

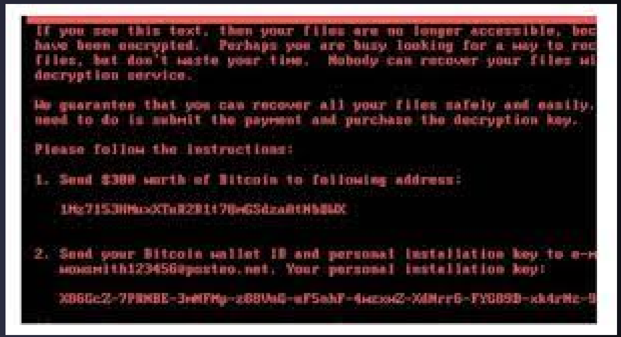
Where can I buy MoneyPak?

How do I unblock the computer using the MoneyPak?

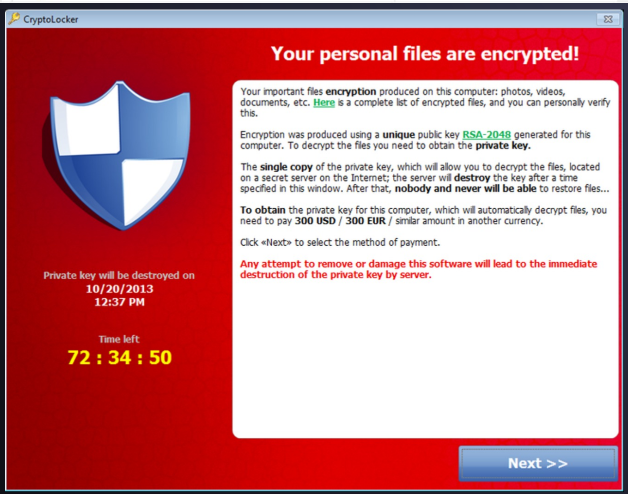
1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee up to $4,95 will apply.
3. To pay fine you should enter the digits MoneyPak resulting code in the payment form and press «Pay MoneyPak».



```
You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (w88990
1665@yandex.com) YOURID: [redacted]
Missing operating system_
```



```
If you see this text, then your files are no longer accessible, bec
have been encrypted.  Perhaps you are busy looking for a way to rec
files, but don't waste your time.  Nobody can recover your files wi
decryption service.

We guarantee that you can recover all your files safely and easily.
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-m
   wowsmith123456@posteo.net. Your personal installation key:

   X06Gc2-7PRKBE-3wMFMp-z88VaG-aFSahF-4wcxw2-XdMrrG-FYG89D-xk4rMc-
```



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

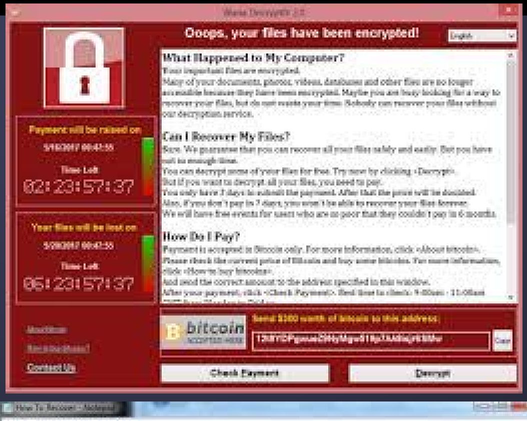
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

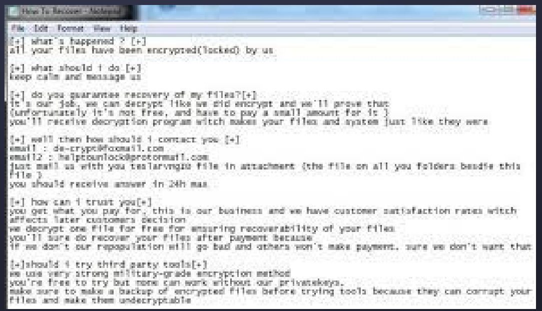
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

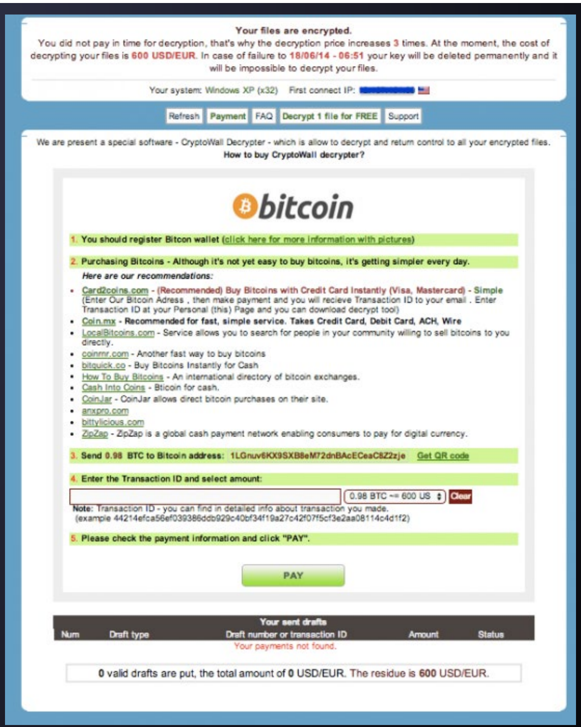
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



How To Recover - Notepad

```
[+] what's happened ? [+]
all your files have been encrypted(locked) by us

[+] what should i do [+]
keep calm and message us

[+] do you guarantee recovery of my files?[+]
it's our job, we can decrypt like we did encrypt and we'll prove that
(unfortunately it's not free, and have to pay a small amount for it )
you'll receive decryption program witch makes your files and system just like they were

[+] well then how should i contact you [+]
email : de-crypt@foxmail.com
email2 : helptounlock@protonmail.com
just mail us with you teslarvng10 file in attachment (the file on all you folders besdie this
file )
you should receive answer in 24h max

[+] how can i trust you[+]
you get what you pay for, this is our business and we have customer satisfaction rates witch
affects later customers decision
we decrypt one file for free for ensuring recoverability of your files
you'll sure do recover your files after payment because
if we don't our repopulation will go bad and others won't make payment. sure we don't want that

[+]should i try third party tools[+]
we use very strong military-grade encryption method
you're free to try but none can work without our privatekeys.
make sure to make a backup of encrypted files before trying tools because they can corrupt your
files and make them undecryptable
```



Your files are encrypted.

You did not pay in time for decryption, that's why the decryption price increases 3 times. At the moment, the cost of decrypting your files is 600 USD/EUR. In case of failure to 18/06/14 - 06:51 your key will be deleted permanently and it will be impossible to decrypt your files.

Your system: Windows XP (x32) First connect IP: [redacted]

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. **You should register Bitcon wallet (click here for more information with pictures)**
2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

   Here are our recommendations:

   - Card2coins.com - (Recommended) Buy Bitcoins with Credit Card Instantly (Visa, Mastercard) - Simple (Enter Our Bitcoin Adress , then make payment and you will recieve Transaction ID to your email . Enter Transaction ID at your Personal (this) Page and you can download decrypt tool)
   - Coin.mx - **Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire**
   - LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
   - coinmr.com - Another fast way to buy bitcoins
   - bitquick.co - Buy Bitcoins Instantly for Cash
   - How To Buy Bitcoins - An international directory of bitcoin exchanges.
   - Cash Into Coins - Bticoin for cash.
   - CoinJar - CoinJar allows direct bitcoin purchases on their site.
   - anxpro.com
   - bittylicious.com
   - ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. **Send 0.98 BTC to Bitcoin address:** 1LGnuv6KX9SXB8eM72dnBAcECeaC8Z2zje Get QR code
4. **Enter the Transaction ID and select amount:**

   0.98 BTC ~= 600 US

   Note: Transaction ID - you can find in detailed info about transaction you made. (example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. **Please check the payment information and click "PAY".**

Your sent drafts

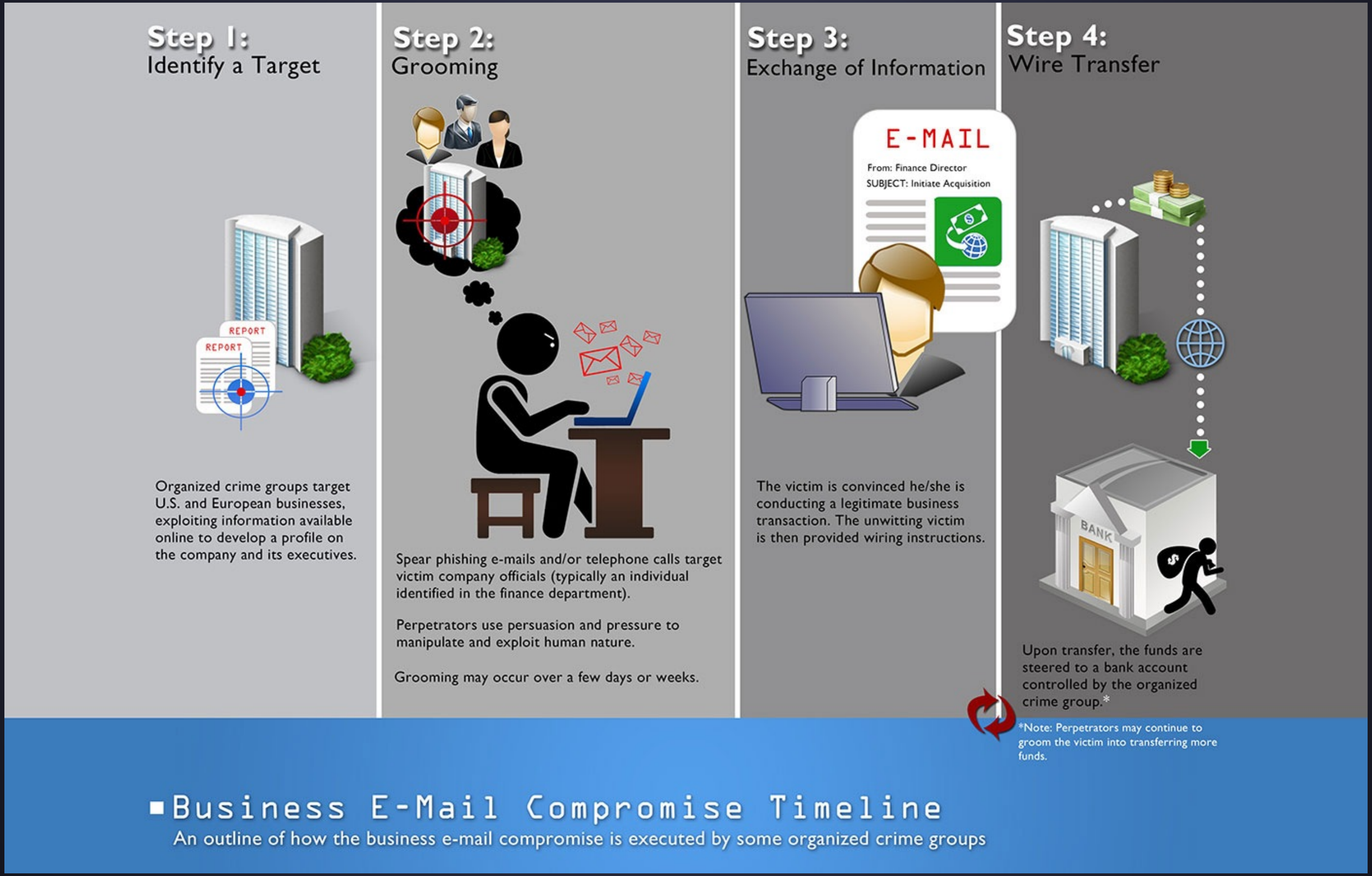
Num	Draft type	Draft number or transaction ID	Amount	Status
		Your payments not found.		

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 600 USD/EUR.

Business Email Compromise

- In 2020, the IC3 received 19,369 Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints with adjusted losses over $1.8 billion.
- Has evolved to include compromise of personal emails, compromise of vendor emails, spoofed lawyer email accounts, requests for W-2 information, the targeting of the real estate sector, and fraudulent requests for large amount of gift cards.
- In new variations, the victim is initially being scammed in non-BEC/EAC situations to include Extortion, Tech Support, Romance Scams, etc., that involved a victim providing a form of ID to a bad actor. That identifying information was then used to establish a bank account to receive stolen BEC/EAC funds and then transferred to a cryptocurrency account.

Business Email Compromise



Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

- Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

Financial Fraud Kill Chain

- Minimum $50,000
- International Transfer
- <72 Hours Since Wire Transfer Initiated
- FBI, USSS, FINCEN, NCFTA, FS-ISAC

Financial Fraud Kill Chain

- Minimum $50,000
- Summary of the Incident:
- Victim Name:
- Victim Location (City, State):
- Originating Bank Name:
- Originating Bank Account Number:
- Beneficiary Name:
- Beneficiary Bank:
- Beneficiary Account Number:
- Beneficiary Bank Location (if available):
- Intermediary Bank Name (if available):
- SWIFT Number:
- Date:
- Amount of Transaction:
- Additional Information (if available) - including “FFC”- For Further Credit; “FAV” – In Favor

SolarWinds Orion

- Actors surreptitiously tampered with updates released by SolarWinds for its Orion platform, a suite of network management tools. A platform used to monitor, analyze and mange Information Technology.
- Affected versions: 2019.4 through 2020.2.1 HF1
- Actors were exploiting SolarWinds Orion products containing SUNBURST malware to gain access to network traffic management systems.
- Seen on victim networks achieving full privileged access through trusted legitimate credentials, accounts, and applications. These credentials are often leveraged from victim-dedicated IP addresses.
- Once found, its up to the Cyber Security Professionals and System Administrators to determine if the actors used that vulnerability to pivot to a higher form of access.

SolarWinds Orion

- more than 425 of the U.S. Fortune 500
- all ten of the top ten US telecommunications companies
- all five branches of the U.S. military
- all five of the top five U.S. accounting firms
- the Pentagon
- the State Department
- the National Security Agency
- the Department of Justice
- The White House

Microsoft Exchange Email Server Hack

- This exploit remains ongoing, although significant mitigation measures are now in place
- Another malicious event attributed to Chinese state-sponsored actors
- Illustrates the speed and scale to which damage can spread
- Highlights the importance of timely application of software patches

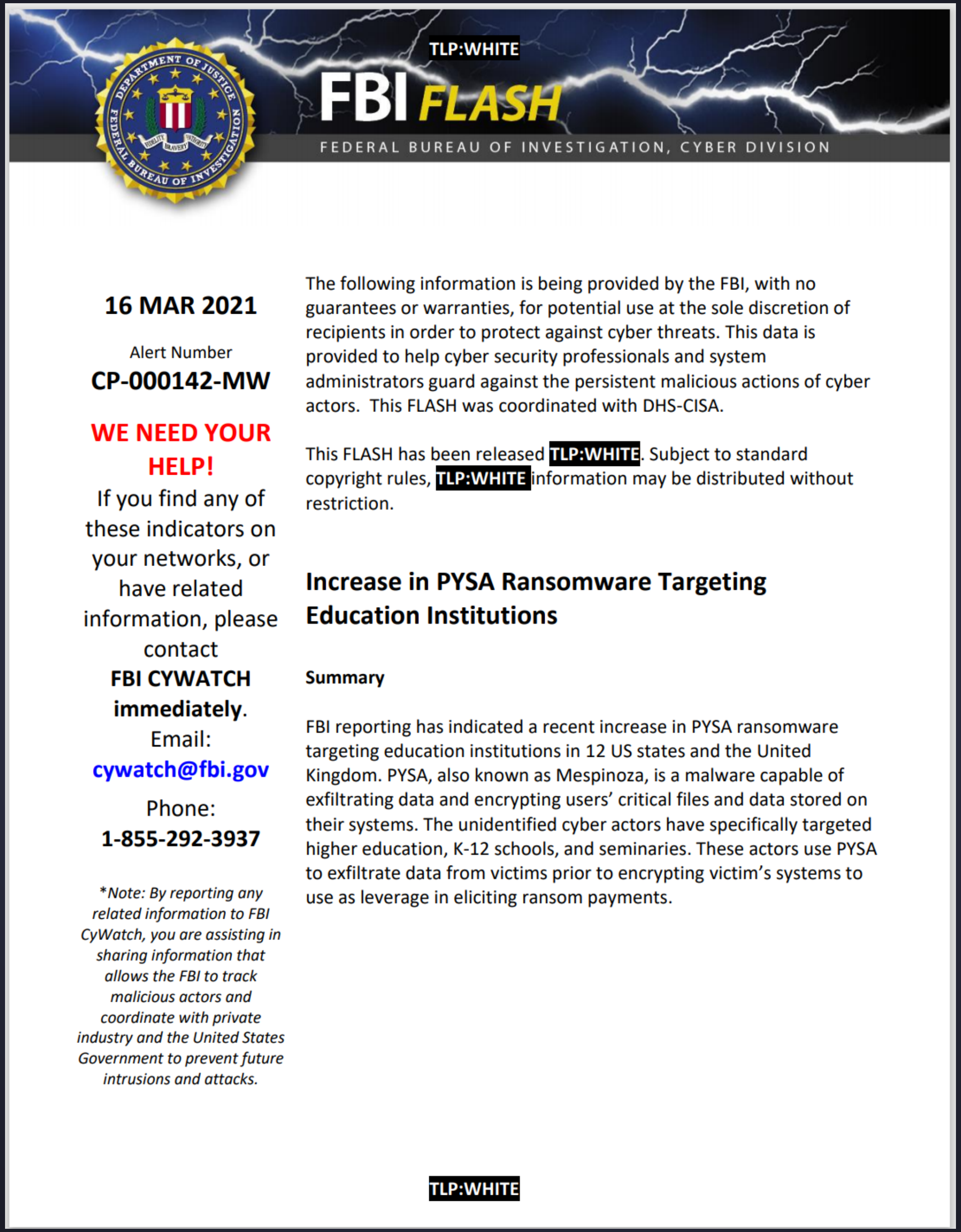
(all of the following information derived from open sources)

MS Exchange Hack: Overview

- Scope assessment of impact grew rapidly – by mid-March 2021 it was assessed that hundreds of thousands of organizations/servers were impacted worldwide
- Microsoft assessed that cloud-based Exchange email systems were not impacted
- Chinese state-sponsored APT hacking group “Hafnium” is attributed as the actor
- This attack is unique in the size, scope and un-targeted nature
- Victims are primarily small-to-medium-sized businesses

MS Exchange Hack: Contrast to Solar Winds

- MS Exchange hack is much larger in scope – damage assessment is ongoing
- This hack is less discrete and therefore easier to detect, but more widely distributed



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

16 MAR 2021

Alert Number

CP-000142-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact

FBI CYWATCH immediately.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

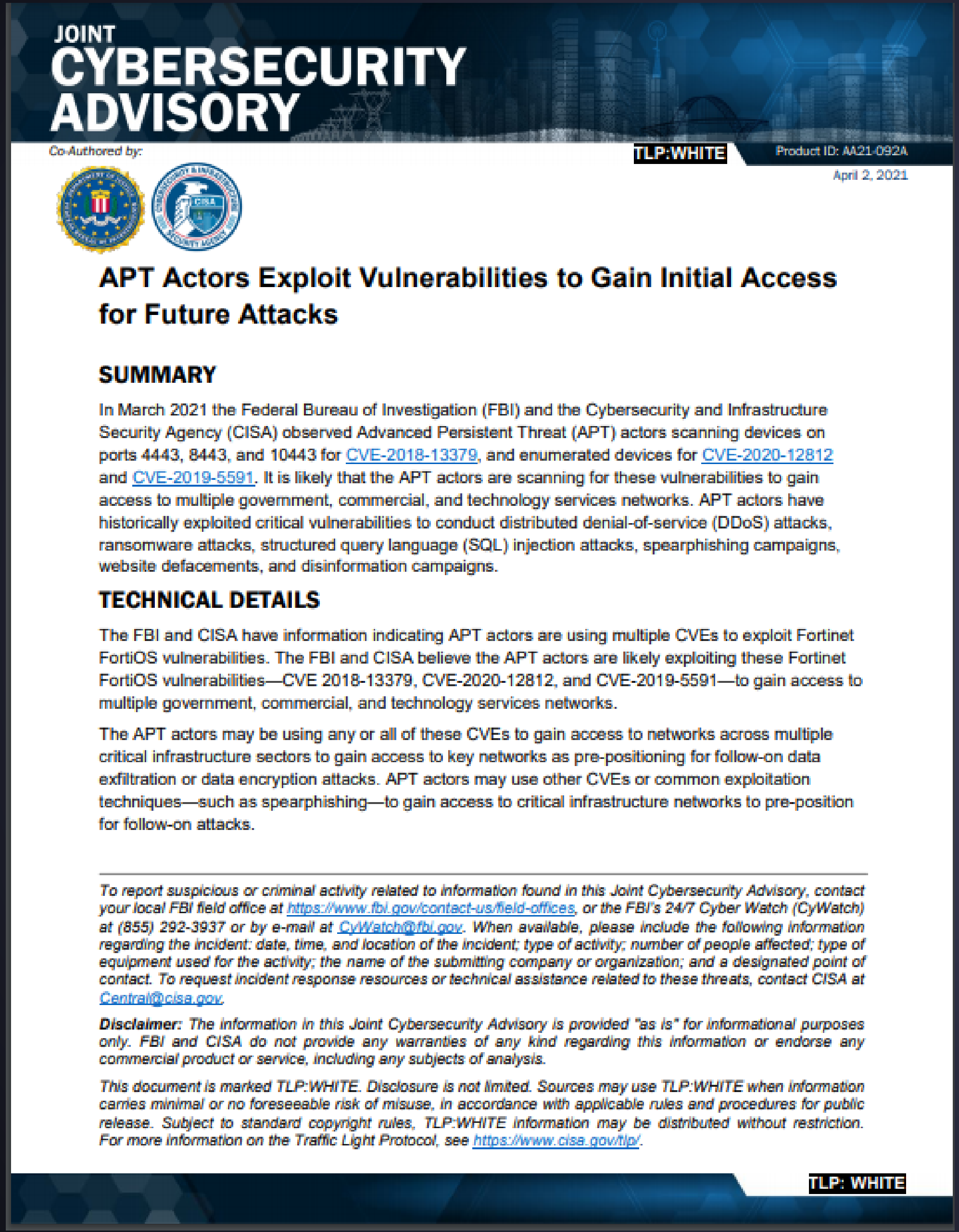
This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Increase in PYSA Ransomware Targeting Education Institutions

Summary

FBI reporting has indicated a recent increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom. PYSA, also known as Mespinoza, is a malware capable of exfiltrating data and encrypting users' critical files and data stored on their systems. The unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors use PYSA to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments.

TLP:WHITE



JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-092A

April 2, 2021

APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks

SUMMARY

In March 2021 the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) observed Advanced Persistent Threat (APT) actors scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591. It is likely that the APT actors are scanning for these vulnerabilities to gain access to multiple government, commercial, and technology services networks. APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns.

TECHNICAL DETAILS

The FBI and CISA have information indicating APT actors are using multiple CVEs to exploit Fortinet FortiOS vulnerabilities. The FBI and CISA believe the APT actors are likely exploiting these Fortinet FortiOS vulnerabilities—CVE 2018-13379, CVE-2020-12812, and CVE-2019-5591—to gain access to multiple government, commercial, and technology services networks.

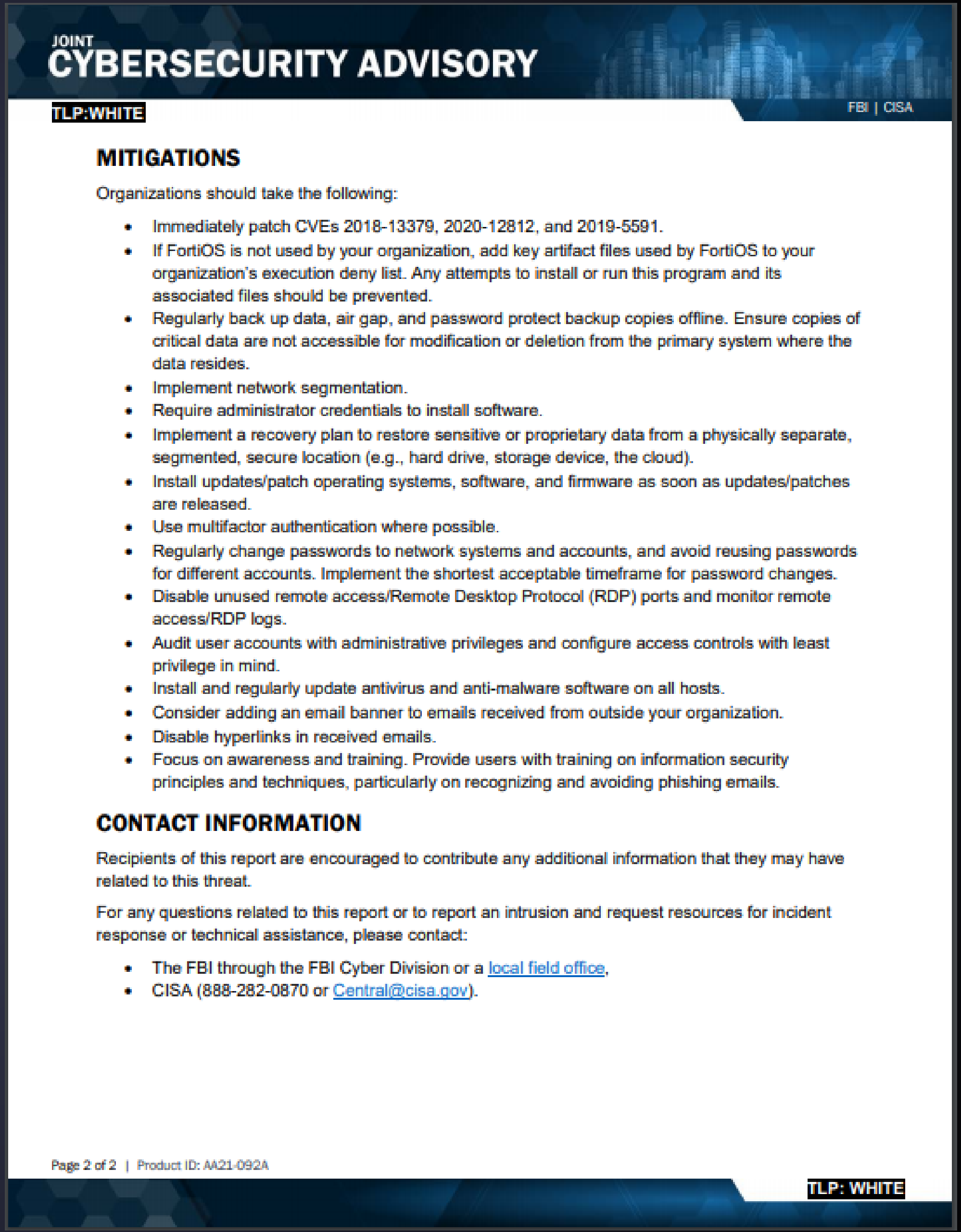
The APT actors may be using any or all of these CVEs to gain access to networks across multiple critical infrastructure sectors to gain access to key networks as pre-positioning for follow-on data exfiltration or data encryption attacks. APT actors may use other CVEs or common exploitation techniques—such as spearphishing—to gain access to critical infrastructure networks to pre-position for follow-on attacks.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at https://www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

***Disclaimer:** The information in this Joint Cybersecurity Advisory is provided "as is" for informational purposes only. FBI and CISA do not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis.*

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/.

TLP: WHITE



JOINT
CYBERSECURITY ADVISORY

TLP:WHITE

FBI | CISA

MITIGATIONS

Organizations should take the following:

- Immediately patch CVEs 2018-13379, 2020-12812, and 2019-5591.
- If FortiOS is not used by your organization, add key artifact files used by FortiOS to your organization's execution deny list. Any attempts to install or run this program and its associated files should be prevented.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the primary system where the data resides.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to restore sensitive or proprietary data from a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts. Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Focus on awareness and training. Provide users with training on information security principles and techniques, particularly on recognizing and avoiding phishing emails.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division or a local field office,
- CISA (888-282-0870 or Central@cisa.gov).

Page 2 of 2 | Product ID: AA21-092A

TLP: WHITE