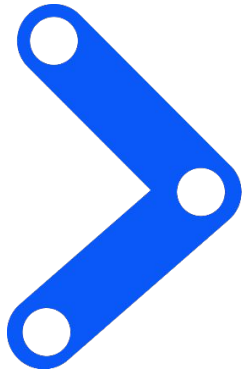


I Like to MOVEit, MOVEit



MoveIt

\$whoami

David @riskymanag3ment

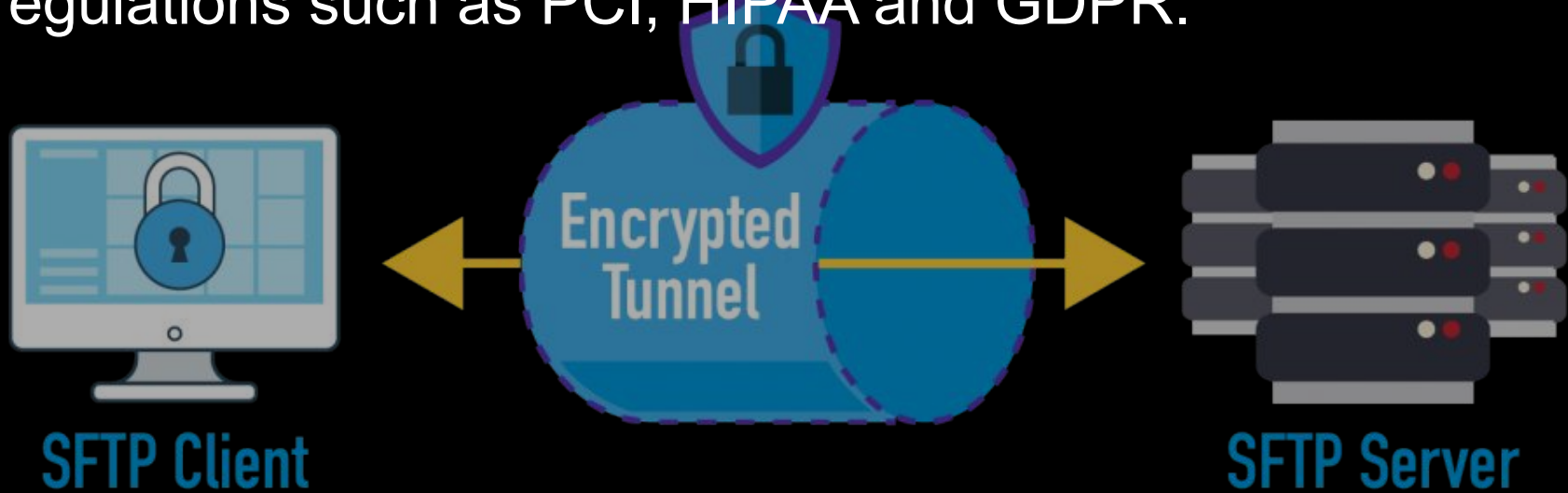
- Information Security for a Financial Institution for the last 5 years
- Nonprofit world for 15 years
- Sec+, SSCP, CCSP, PenTest+, CySA+


* Opinions expressed are solely my own and do not express the views or opinions of my employer.



- 
- A photograph of a dirt path in a forest, with many tree roots exposed on the ground. The path leads into the distance, flanked by dense green foliage and tall trees. The lighting is soft, suggesting a shaded forest environment.
1. Introduction to MOVEit
 2. Introduction to cl0p
 3. How did I get here?
 - a. The Process
 - b. Data Analysis
 4. Lessons Learned

MOVEit provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR.





Cl0p

Ransomware gang started in 2019

Specialized in File Transfer Applications

February 2019 - Maastricht University

December 2020 - Accellion FTA (File Transfer Appliance)

November 2021 - Solarwinds Serv-U MFT (Managed File Transfer)

January 2023 - GoAnywhere MFT

May 2023 - MOVEit



How Did I Get Here?

CLOP^_- LEAKS

[HOME](#) [HOW TO DOWNLOAD?](#) [ARCHIVE](#) ∨ [SHELL.COM](#) [ARCHIVE2](#) ∨

[ARCHIVE4](#) ∨ [ARCHIVE5](#) ∨ [ARCHIVE3](#) ∨ [1STSOURCE.COM](#) [DATASITE.COM](#)

[PUTNAM.COM](#) [OEKK.CH](#) [UHCSR.COM](#) [LANDAL.COM](#) [HEIDELBERG.COM](#)

[BANKERS-BANK.COM](#) [LEGGETT.COM](#) [UGA.EDU](#) [CUANSWERS.COM](#)

[NAVAXX.LU](#) [DELAWARELIFE.COM](#) [316FIDUCIARIES.COM](#) [ENZO.COM](#)

[CARESERVICESLLC.COM](#) [GENERICON.AT](#) [BRAULT.US](#) [APLUSFCU.ORG](#)

[BARHARBOR.BANK](#) [POWERFI.ORG](#) [EASTWESTBANK.COM](#) [MARTI.COM](#)

[PRAGROUP.NO](#) [COLUMBIABANK.COM](#) ([UMPQUABANK.COM](#)) [UMSYSTEM.EDU](#)

[ICSYSTEM.COM](#) [ARBURG.COM](#) [BOSTONGLOBE.COM](#)

[CNCBINTERNATIONAL.COM](#) [STIWA.COM](#) [CEGEDIM.COM](#) [AON.COM](#)

[NUANCE.COM](#) [PALIG.COM](#) ([PANAMERICAN](#)) [GESA.COM](#) [SCU.EDU](#)

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE..

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.

STEP 2 - EMAIL OUR TEAM UNLOCK@SUP-BOX.COM OR UNLOCK@SUPPORT-MULT.COM

STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE

STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU

STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE

STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING

STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED

STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION

STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

WE GOT A LOT OF EMAILS ABOUT GOVERNMENT DATA, WE DON'T HAVE ANY GOVERNMENT DATA AND ANYTHING DIRECTLY RESIDING ON EXPOSED AND BAD PROTECTED NOT ENCRYPTED FILE TRANSFER WE STILL DO THE POLITE THING AND DELETE ALL. ALL MEDIA SPEAKING ABOUT THIS ARE DO WHAT ALWAYS THEY DO. PROVIDE LITTLE TRUTH IN A BIG LIE. WE ALSO WANT TO REMIND ALL COMPANY THAT IF YOU PUT DATA ON INTERNET WHERE DATA IS NOT PROTECT DO NOT BLAME US FOR PENETRATION TESTING SERVICE. WE ARE ONLY FINANCIAL MOTIVATED AND DO NOT CARE ANYTHING ABOUT POLITICS.

UPDATES

WERUM.COM PAGE PUBLISHED

SE.COM PAGE PUBLISHED

SIEMENS-ENERGY.COM PAGE PUBLISHED

UCLA.EDU PAGE PUBLISHED

ABBVIE.COM PAGE PUBLISHED

Updates between
5:00am-7:00AM PDT
(3:00-5:00 PM MSK)

cl0p
ransomware
steals data
from MOVEit



cl0p
says they
release names
on June 15



cl0p
still releasing
new
names on June 23



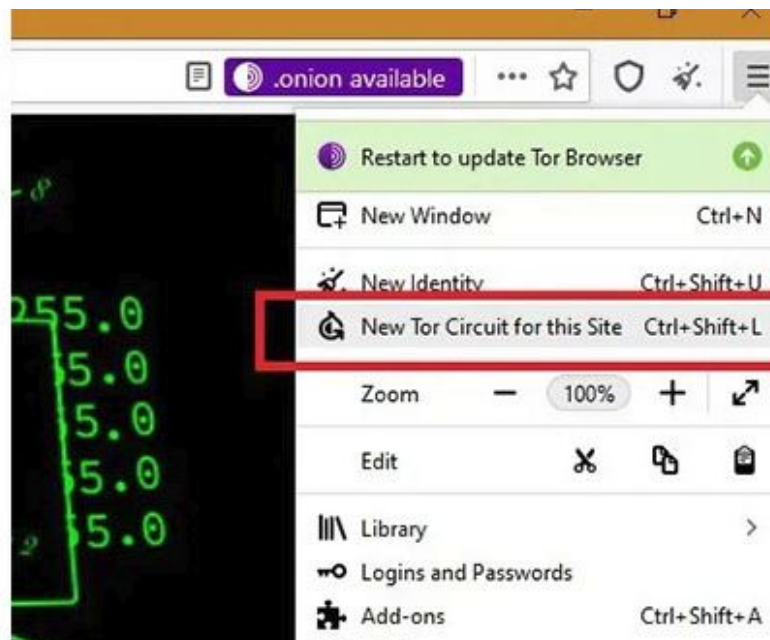
Many questions come to the email about why it is not downloading or is downloading so slowly.

Below is an instruction on how to download and unpack files.

To download the archives from our site, you must use the tor browser, which implies the use of the tor network.

The tor network rotates the input and output nodes, which affects the download speed,

so if you fail to download or downloads too slowly, try to make a "New Tor circuit for this Site" in the tor browser as shown in the screenshot below




```
--2023-07-27 13:21:14-- (try:16) http://amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmchnchuayd.onion/1/tdecu/11.z03
Connecting to amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmchnchuayd.onion (amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmchnchuayd.onion)|127.42.42.0|:80... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 734003200 (700M), 118495510 (113M) remaining [application/octet-stream]
Saving to: '11.z03'
```

```
11.z03          91%[+++++++>          ] 638.04M  4.60KB/s   eta 3h 8m  
```

```
, 50120000 (477M) remaining [application/octet-stream]
```

```
50%[+++++++          ] 355.52M  --.-KB/s   eta 47d 3h  
```

```
$ while true; do torsocks wget -c
http://amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7
sf5festvqxmchnchuayd.onion/3/$company/1.zip;
sleep 30; done
```

Tactic Change

*Now we post many company name and proof we have their secrets and data. Some company do not speed to us and decide to stay quiet. We are very reasonable operators and when right situation we offer deep discount to block you data from being sold and publish. Advice you to contact us and begin discussion on how to block publicate of data. On 15 August we start publishing of every company on list that do not contact. You data is going to publishing on clearweb and Tor and for large company we also create clearweb URL to help google index you data. Also all data go on torrent and speed of download is very quick. **YOU NOT HIDING MORE.***

Tactic Change 2.0

STEP 1

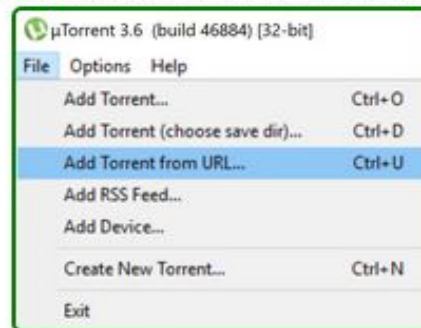
Download and install free **uTorrent** client
(if you don't already have it)

<https://www.utorrent.com/downloads/>

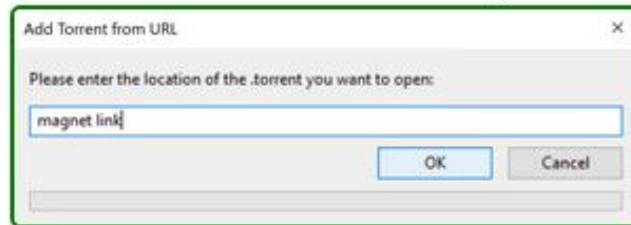
Or any other **torrent** client that you prefer

STEP 2

Run **uTorrent** and select File > Add Torrent from URL



Paste magnet URL to the Add Torrent from URL dialog box and click **OK** button



Mistakes were Made

cncbinternational.com



FULL FILES

magnet:?xt=urn:btih:1d18f14e65e34e6bfb5894eff43c3705be7a909c&
dn=cncbinternational

bostonglobe.com

The Boston Globe

FULL FILES

magnet:?xt=urn:btih:b798b713e798876e346dca8d427488d1fced2e73&
dn=bostonglobe

arburg.com

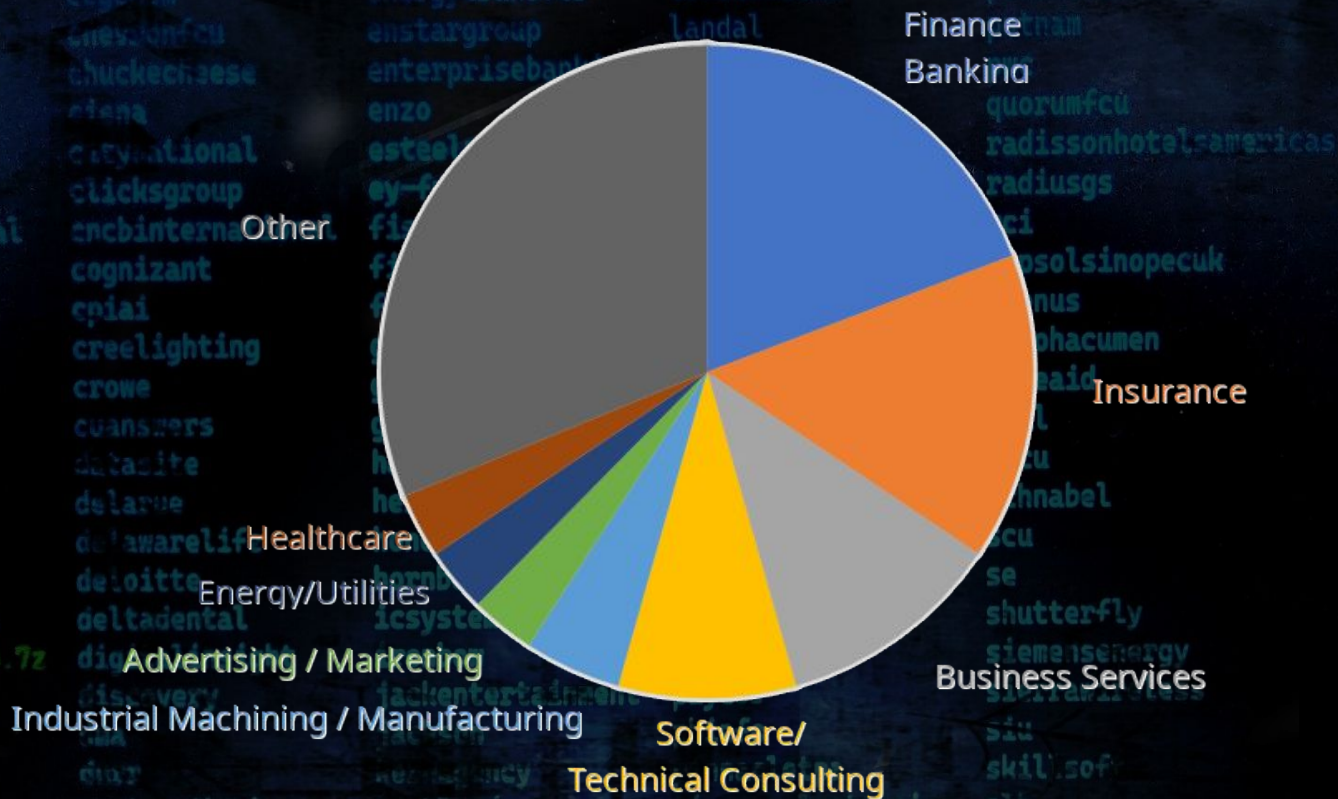


FULL FILES

magnet:?xt=urn:btih:b798b713e798876e346dca8d427488d1fced2e73&
dn=bostonglobe

DUE TO TECHNICAL REASONS, THE UNLOCK@RSV-BOX.COM EMAIL WAS REPLACED BY UNLOCK@SUP-BOX.COM, ALL WHO WROTE, PLEASE RE-WRITE TO UNLOCK@SUP-BOX.COM.

Victims by Industry



Downloading Data



Download
Data

Document
Size

Extract Zip
Files

Count File
Extensions

Extract Sub
Archives

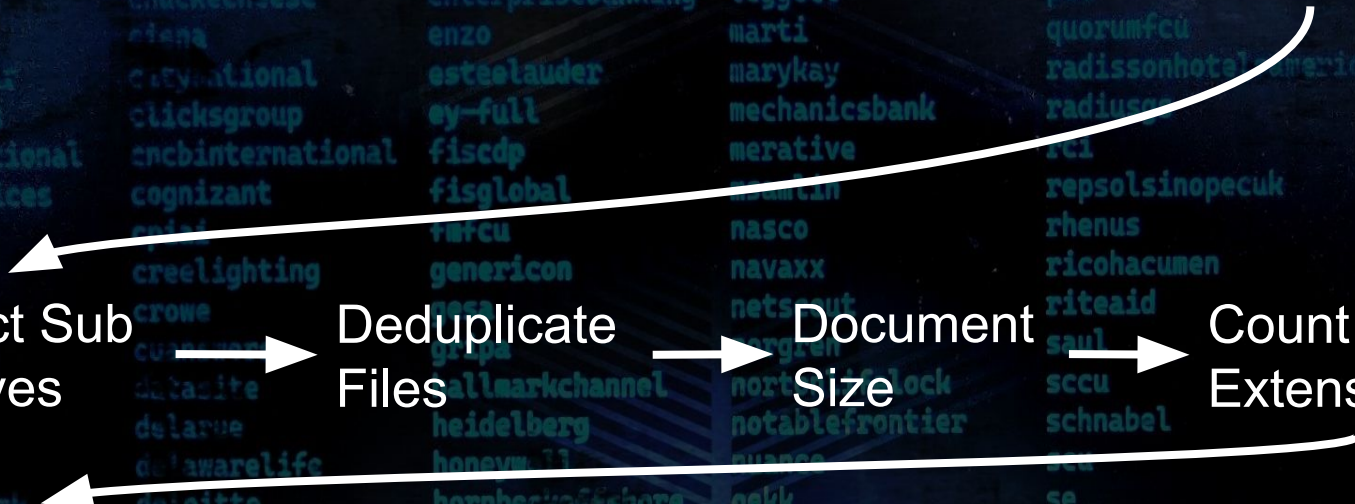
Deduplicate
Files

Document
Size

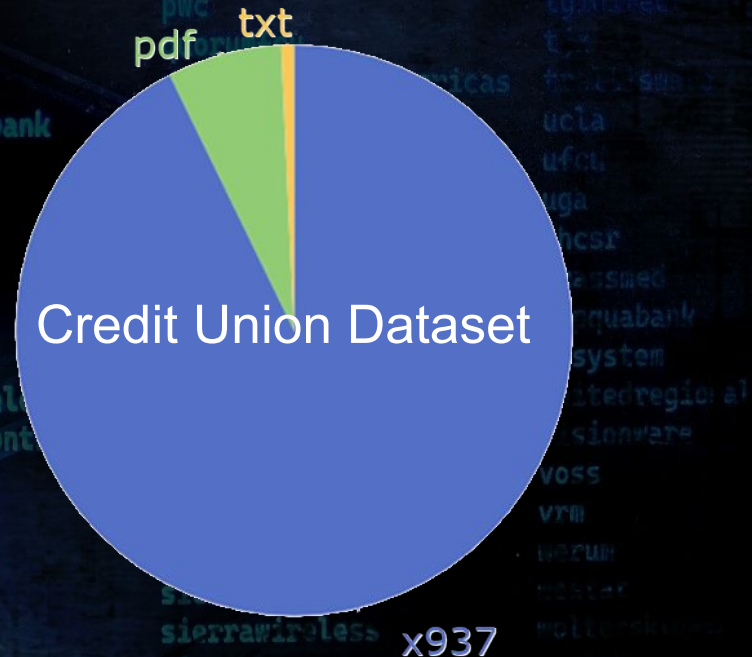
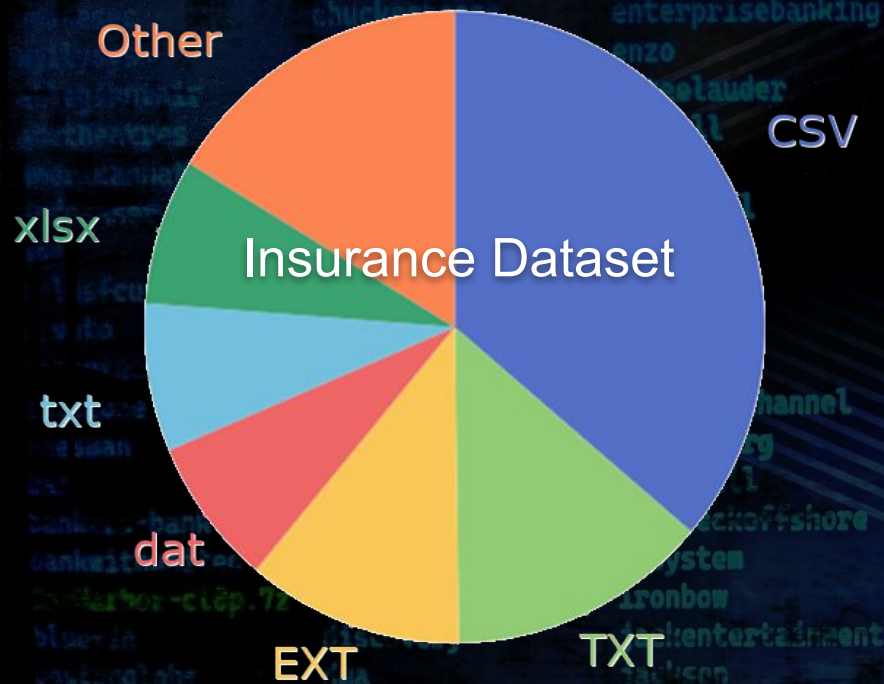
Count File
Extensions

Identify File
Extensions

Identify Business
Interconnections



Overview of Files

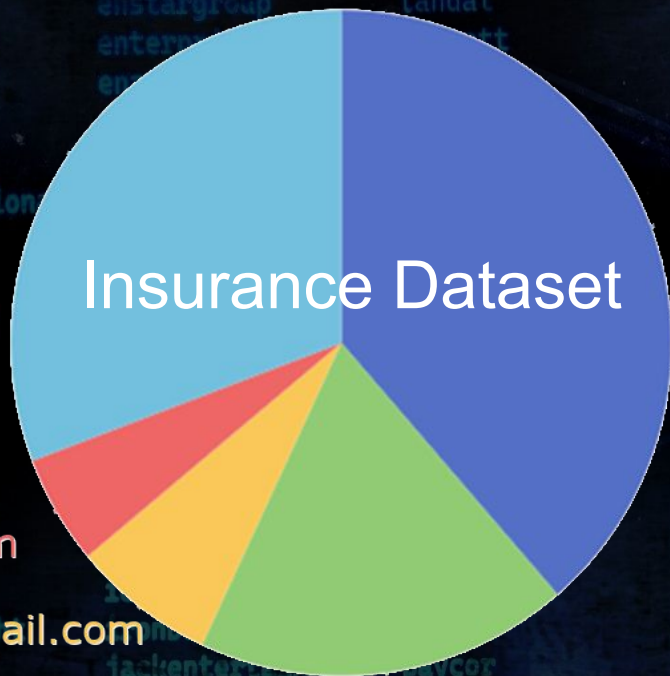


Overview of Files

Insurance Billing Records
Credit Card Information
Wire Records
Audit Information
Property Records
2 EDR Installations
Employee Records
Payroll Information
Corp Accounting Records
Legal Records
MOVEit Installation + License

Powerpoint Presentations
Outlook PST
Training Videos
Certificates
Medical Billing
Marketing Material
Incident Response SOPs
Loan Applications
Policies
Health Records

Email Addresses



gmail.com

Other

aol.com

hotmail.com

yahoo.com

Lessons Learned

- Ransomware Groups make mistakes
- Vendor Management
- Encrypt archives with OOB key
- Don't leave stale data on transfer servers
- Cl0p took most weekends off, except Memorial Day Weekend

Sources and Thanks

https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf
<https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/>

Corey Ham
Dominic Alvieri
Brett Callow

Contact Me

Twitter:

@riskymanag3ment

Mastodon:

@riskymanag3ment@infosec.exchange

Email:

riskymanag3ment@proton.me
github.com/riskymanag3ment/