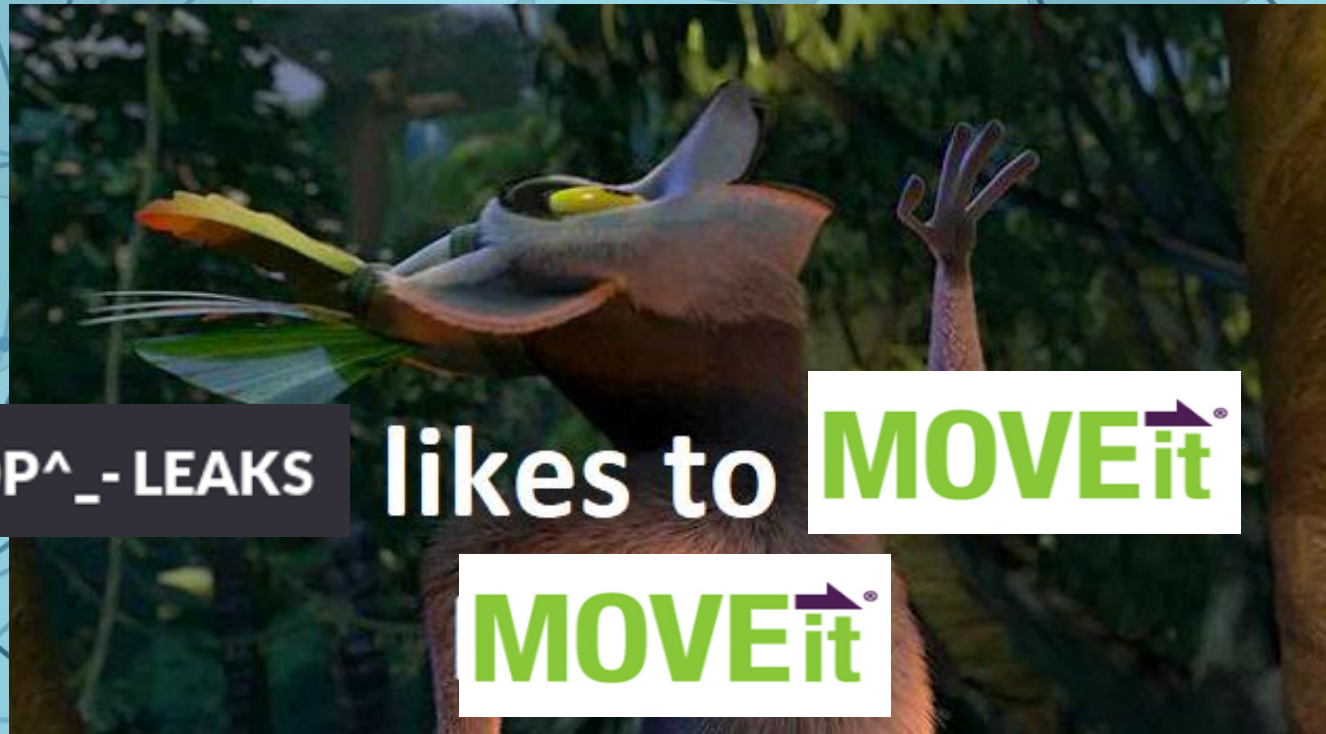



# CLOP LIKES TO MOVEIT MOVEIT



# C:\User\wthomas

Cyber Threat Intelligence Researcher (4 years)

Equinix – the world's digital infrastructure company 

Equinix Threat Analysis Center (ETAC)

Co-author of the SANS FOR589 Cybercrime Intelligence course

Co-founder of the Curated Intelligence trust group

- <https://blog.bushidotoken.net/>
- <https://twitter.com/BushidoToken>
- <https://github.com/BushidoUK>
- <https://www.sans.org/profiles/will-thomas/>
- <https://www.linkedin.com/in/william-t/>



# WHO, WHAT, WHERE, WHEN, WHY, HOW

Who?

The CL0P gang

What?

Hacked hundreds of  
file transfer servers

Where?

Globally

When?

Around 27 May (Bank  
Holiday weekend)

Why?

Money  
(Cryptocurrency)

How?

Zero-days and data  
exfiltration



# WHO ARE THESE GUYS AGAIN?

- The operators of CL0P are a **financially motivated**, Russian- and Ukrainian-speaking **cybercrime group**.
- They are tracked, with **varying degrees of connections**, under multiple threat actor monikers by CTI vendors.

## This includes:

TA505 (Proofpoint)

Lace Tempest (Microsoft)

Graceful Spider (CrowdStrike)

FIN11 (Mandiant)

GOLD TAHOE (Secureworks)

- The ransomware has been used recently by other threat actors, such as **FIN7**, in targeted intrusions according to both [Microsoft](#) and [Secureworks](#).



Graceful Spider  
Russian Federation





Національна поліція України

@NPU\_GOV\_UA

Кіберполіція викрила хакерське угруповання у розповсюдженні вірусу-шифрувальника та нанесенні іноземним компаніям пів мільярда доларів збитків

Деталі: [bit.ly/2SCdIOY](https://bit.ly/2SCdIOY)

Translated from Ukrainian by Google

The cyber police exposed a hacker group in the distribution of an encryption virus and causing half a billion dollars in losses to foreign companies

Details: [bit.ly/2SCdIOY](https://bit.ly/2SCdIOY)



9:32 AM · Jun 16, 2021



Arrest of  
CL0P's  
Money  
Laundering  
Network in  
June 2021



 Cellebrite

# HAVE THEY DONE THIS BEFORE? YES

CLOP^\_-LEAKS

This  
includes:

Accellion FTA  
servers (December 2020)

SolarWinds Serv-U FTP  
servers (November 2021)

GoAnywhere MFT  
servers (February 2023)

PaperCut MF/NG  
servers (April 2023)

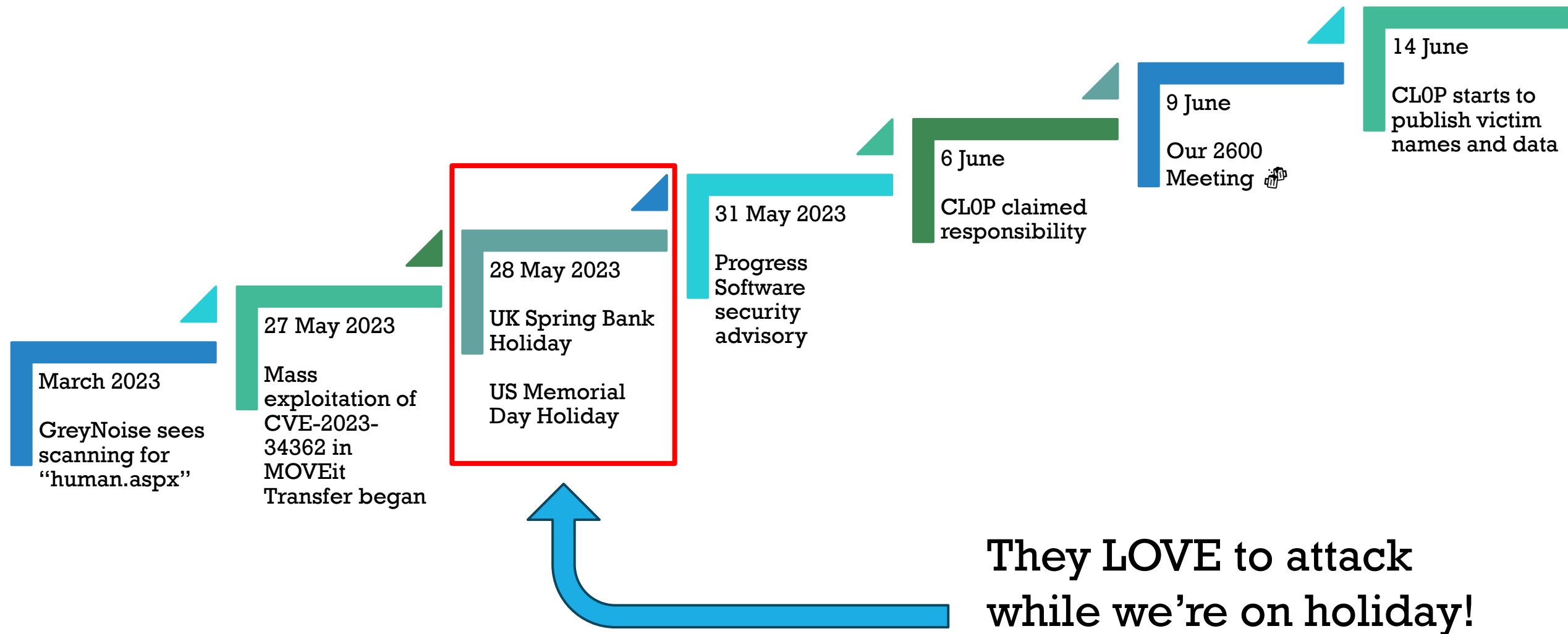
Accellion<sup>®</sup>

 **Serv-U<sup>®</sup>**  
part of the SolarWinds family

 **GO  
ANYWHERE<sup>®</sup>**

PaperCut<sup>™</sup>

# CLOP'S MOVEIT CAMPAIGN TIMELINE



# CLOP'S MOVEIT CAMPAIGN TIMELINE EXTENDED (THANKS TO KROLL)

July 2021

Earliest signs of exploitation commands in IIS logs from MOVEit

April 2022

Additional exploitation of a low number of MOVEit servers

Mid-May 2023

Additional exploit testing before mass campaign against MOVEit servers



# Scanning for MOVEit globally

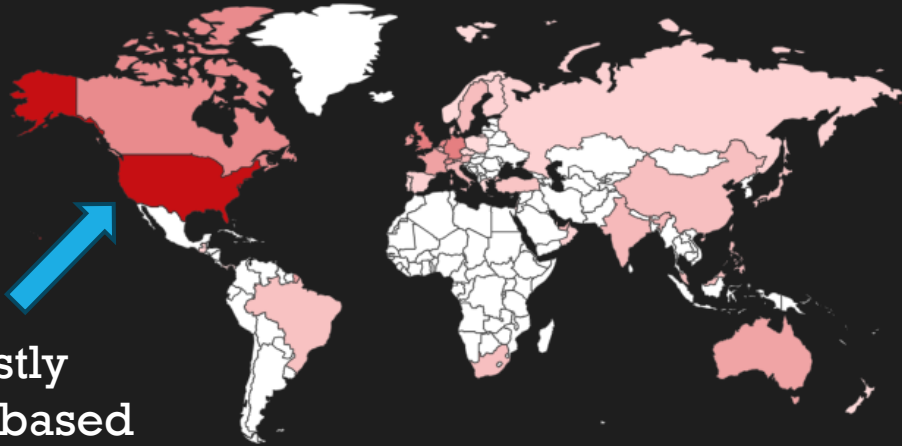
## Shodan Report

http.favicon.hash:989289239

**MOVEit**

Total: 2,549

// GENERAL



### Countries

United States	1,867
United Kingdom	126
Germany	115
Canada	76
Netherlands	75

### Ports

443	1,732
80	808
8443	4
9443	2
444	1

MORE...

### Organization

Microsoft Corporation	637
Amazon Technologies Inc.	67
Amazon Data Services NoVa	28
CenturyLink Communications, LLC	20
AT&T Services, Inc.	18

MORE...

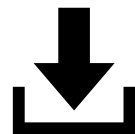
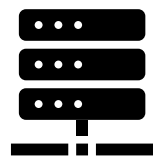
### Vulnerabilities

No information available.

**DIVD**

  
**SHADOWSERVER**

# HOW DID THEY MOVEit MOVEit



Targeted **Windows servers** running **MOVEit Transfer**



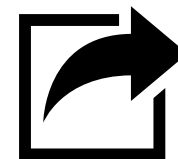
**CVE-2023-34362** can allow an unauthorized attacker to **inject SQL commands**



The system's **svchost.exe** process launches **w3wp.exe**, a **Microsoft IIS** worker process, and writes files to a new working directory in **Temp**



They **uploaded a file** via the **moveitsvc** service account to the server's **\MOVEitTransfer\wwwroot\ directory**



The **w3wp.exe** process launches **csc.exe** to compile the C# code into the payload, which is saved as **human2.aspx**



Exfiltrate the **contents of files** hosted by MOVEit Transfer plus **Azure Storage Blob** contents, including **credentials**



The headlines came rolling in:

## BA, BBC and Boots hit by cyber security breach with contact and bank details exposed

Hackers exploited a vulnerability in MOVEit Transfer software last week to access a range of information which is now casting a cloud over a growing number of UK firms and their staff.



James Sillars  
Business reporter @SkyNewsBiz

Jonathan Greig

June 6th, 2023

News

Industry

## University of Rochester, Nova Scotia first known MOVEit victims in North America



The government of Nova Scotia and the University of Rochester are the first organizations in North America to confirm data theft as a result of the exploitation of a new vulnerability affecting popular file transfer tool MOVEit.

On Sunday, the government of Nova Scotia, a small province in eastern Canada, **warned** that the personal information of some residents was accessed "as part of a global security issue with a file transfer service called MOVEit."

CL0P confirmed directly to journalists who contacted them

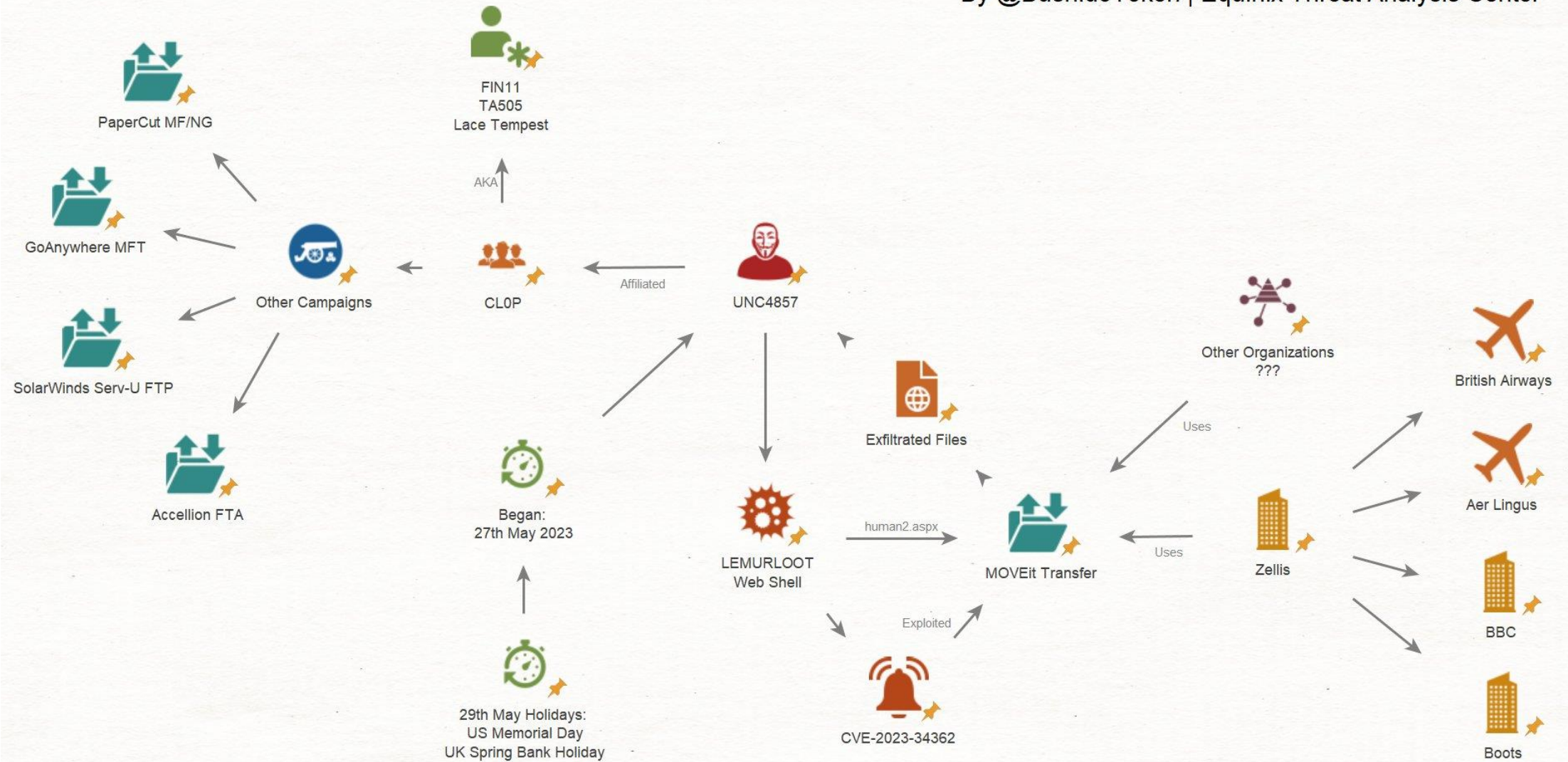
Hi Raphael

Yes, it was our attack, you can see the knee of the victims in us on the blog if someone refuses to pay.

I want to tell you right away that the military,GOV,children's hospitals, police end etc like that we not to attack. and their data erased

cl0p team





CL0P LEAKATHON

**IT BEGINS**

A-CL0P-APLYSE



**CL0P^\_ - LEAKS**

You have been placed in a queue, awaiting forwarding to the platform.

Please do not refresh the page, you will be automatically redirected.



## CLOP^\_- LEAKS

“...penetration testing service after the fact”

“Progress MOVEIT”

“Your data is safe”

“Email our Team”

“Chat URL over Tor”

### *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@RSV-BOX.COM](mailto:UNLOCK@RSV-BOX.COM) OR [UNLOCK@SUPPORT-MULT.COM](mailto:UNLOCK@SUPPORT-MULT.COM)**

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



“hundreds of companies”

“14 June 2023”

“10% proof data”

“3 days to discuss price”

“After 7 days they will leak the data”

“Warranty”

“Government, City, or Police... do not worry”

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

*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.*

# Then came the LEAKS

## 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](#) [SYNLAB.FR](#)

[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](#)

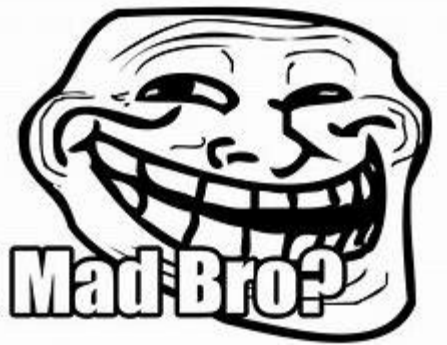
[COLUMBIABANK.COM \(UMPQUABANK.COM\)](#) [UMSYSTEM.EDU](#) [ICSYSTEM.COM](#) [ARBURG.COM](#)

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

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

[CREELIGHTING.COM](#) [NORTONLIFELOCK.COM](#) [STOCKMANBANK.COM](#) [BAESMAN.COM](#) [EMSSHI.COM](#)

[CBESERVICES.COM](#) [ZURICH.COM.BR](#)



1. Only CL0P has the MOVEit zero-day
2. If no ransom is paid, the data is leaked or sold
3. Names are to be published first, followed by data
4. They apparently deleted the data the stole from governments

**Plus**

5. They “do not care for experts”
6. They “have no reason to lie”
7. The media is “creating propaganda”
8. They “want money” and are “reasonable”



CLOP^\_-LEAKS

## Further Clarified

- 1.They “don’t have any government data”
- 2.It was their “penetration testing service”
- 3.They are “only financial motivated”
- 4.They “do not care anything about politics”

*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.*

# CLOP REMOVES UK AND IRISH GOV VICTIMS

- Both listed on 18 July
- UK government's communications regulator Ofcom
- Irish Commission for Communications Regulation (or ComReg)
- Both removed on 20 July
- Seems CL0P is upholding their promise to delete Gov data?

Security

## Ofcom says it won't pay ransom, as new MOVEit hack victims come forward

Carly Page @carlypage\_ / 2:45 PM GMT+1 • July 20, 2023

[Comment](#)



**Headquarters:**

Shell Centre 2 York Rd, London, Greater London, SE1 7NA, United Kingdom

**Phone:**

+44 2079341234

**Website:**

www.shell.com

**Revenue:**

\$381.3B

**Industry:**

Gas Stations, Convenience & Liquor Stores, Retail

**Warning:**

The company doesn't care about its customers, it ignored their security!!!

**FILES PART1 - sftp-sgm.shell.com**

DOWNLOAD1

DOWNLOAD2

DOWNLOAD3

DOWNLOAD4

DOWNLOAD5

DOWNLOAD6

DOWNLOAD7

DOWNLOAD8

DOWNLOAD9

DOWNLOAD10

DOWNLOAD11

DOWNLOAD12

DOWNLOAD13

DOWNLOAD14

DOWNLOAD15

DOWNLOAD16

DOWNLOAD17

DOWNLOAD18

DOWNLOAD19

DOWNLOAD20

DOWNLOAD21

DOWNLOAD22

DOWNLOAD23

**Headquarters:**

1 Embankment PL, London, Greater London, WC2N 6RH, United Kingdom

**Phone:**

+44 2075835000

**Website:**

www.pwc.com

**Revenue:**

\$50.3B

**Industry:**

Accounting & Accounting Services, Business Services

**Warning:**

The company doesn't care about its customers, it ignored their security!!!

**Description:**

121gb + archives

SONY.COM EY.COM PWC.COM GUSCANADA.CA





# CLOP COPYING BLACKCAT?

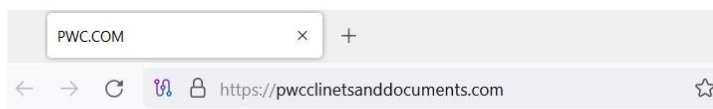
- On 19 July 2023, CL0P created a dedicated domain to publish the data they claim they stole from the PwC MOVEit server



ALL FILES ARE POSTED HERE

FILES [HTTPS://PWCCLINETSANDDOCUMENTS.COM](https://pwcclinetsanddocuments.com)

© CL0P^\_- LEAKS 2020 - 2023  
All rights reserved :)



FILES PART1

<https://pwcclinetsanddocuments.com/pwc/1.zip>  
<https://pwcclinetsanddocuments.com/pwc/1.z01>  
<https://pwcclinetsanddocuments.com/pwc/1.z02>  
<https://pwcclinetsanddocuments.com/pwc/1.z03>  
<https://pwcclinetsanddocuments.com/pwc/1.z04>  
<https://pwcclinetsanddocuments.com/pwc/1.z05>  
<https://pwcclinetsanddocuments.com/pwc/1.z06>  
<https://pwcclinetsanddocuments.com/pwc/1.z07>  
<https://pwcclinetsanddocuments.com/pwc/1.z08>  
<https://pwcclinetsanddocuments.com/pwc/1.z09>  
<https://pwcclinetsanddocuments.com/pwc/1.z10>  
<https://pwcclinetsanddocuments.com/pwc/1.z11>  
<https://pwcclinetsanddocuments.com/pwc/1.z12>  
<https://pwcclinetsanddocuments.com/pwc/1.z13>  
<https://pwcclinetsanddocuments.com/pwc/1.z14>  
<https://pwcclinetsanddocuments.com/pwc/1.z15>  
<https://pwcclinetsanddocuments.com/pwc/1.z16>  
<https://pwcclinetsanddocuments.com/pwc/1.z17>  
<https://pwcclinetsanddocuments.com/pwc/1.z18>  
<https://pwcclinetsanddocuments.com/pwc/1.z19>  
<https://pwcclinetsanddocuments.com/pwc/1.z20>  
<https://pwcclinetsanddocuments.com/pwc/1.z21>  
<https://pwcclinetsanddocuments.com/pwc/1.z22>  
<https://pwcclinetsanddocuments.com/pwc/1.z23>  
<https://pwcclinetsanddocuments.com/pwc/1.z24>  
<https://pwcclinetsanddocuments.com/pwc/1.z25>  
<https://pwcclinetsanddocuments.com/pwc/1.z26>



PROFILE CONNECT MONITOR SUPPORT

Whois Lookup

## Whois Record for PwCcliNetsA...cuments.com

### Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	cn
Registrar	CNOBIN INFORMATION TECHNOLOGY LIMITED IANA ID: 3254 URL: <a href="http://www.ordertld.com">http://www.ordertld.com</a> Whois Server: <a href="http://whois.ordertld.com">whois.ordertld.com</a> <a href="mailto:abuse@ordertld.com">abuse@ordertld.com</a> (p) +852.81926949
Registrar Status	clientDeleteProhibited, clientTransferProhibited
Dates	2 days old Created on 2023-07-17 Expires on 2024-07-17 Updated on 2023-07-17
Name Servers	NS3.CNMSN.COM (has 1,446 domains) NS4.CNMSN.COM (has 1,446 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY (f) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY
IP Address	5.188.44.40 is hosted on a dedicated server
IP Location	- Sankt-peterburg - Sankt-peterburg - Petersburg Internet Network Ltd.
ASN	AS34665 PINDC-AS Petersburg Internet Network Ltd., RU (registered Nov 01, 2019)

Due to the fact that the Tor network is abandoning the second version and all domains will be abolished in September or October, we are moving to a new address:

<http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/>

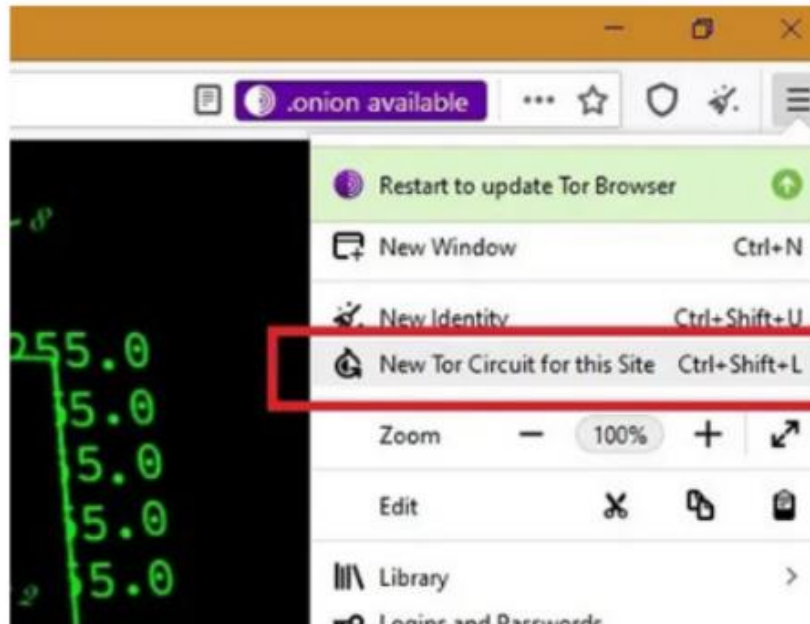
Many questions come to the email about why it is not downloading or is downloading so slowly.

**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

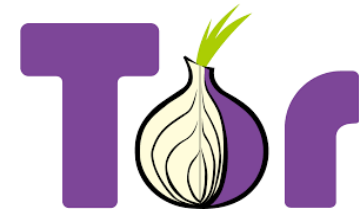


## Getting to CL0P's Tor Data Leak Site

- Guidance of how to use it is even shared by CL0P

# MONITORING A TOR DATA LEAK SITE

- Navigate to the Tor Onion Service with a “Burner Laptop” or Virtual Machine with a VPN or RDP in a Cloud VPS
  - Hit F5 (refresh) and wait for more victims
- Or scrape the Tor site with Privoxy
  - Find URLs, grab HTML, locate target data, save as JSON or CSV
- Checking for Keyword Mentions
  - Downloading data and checking for organization or client exposure



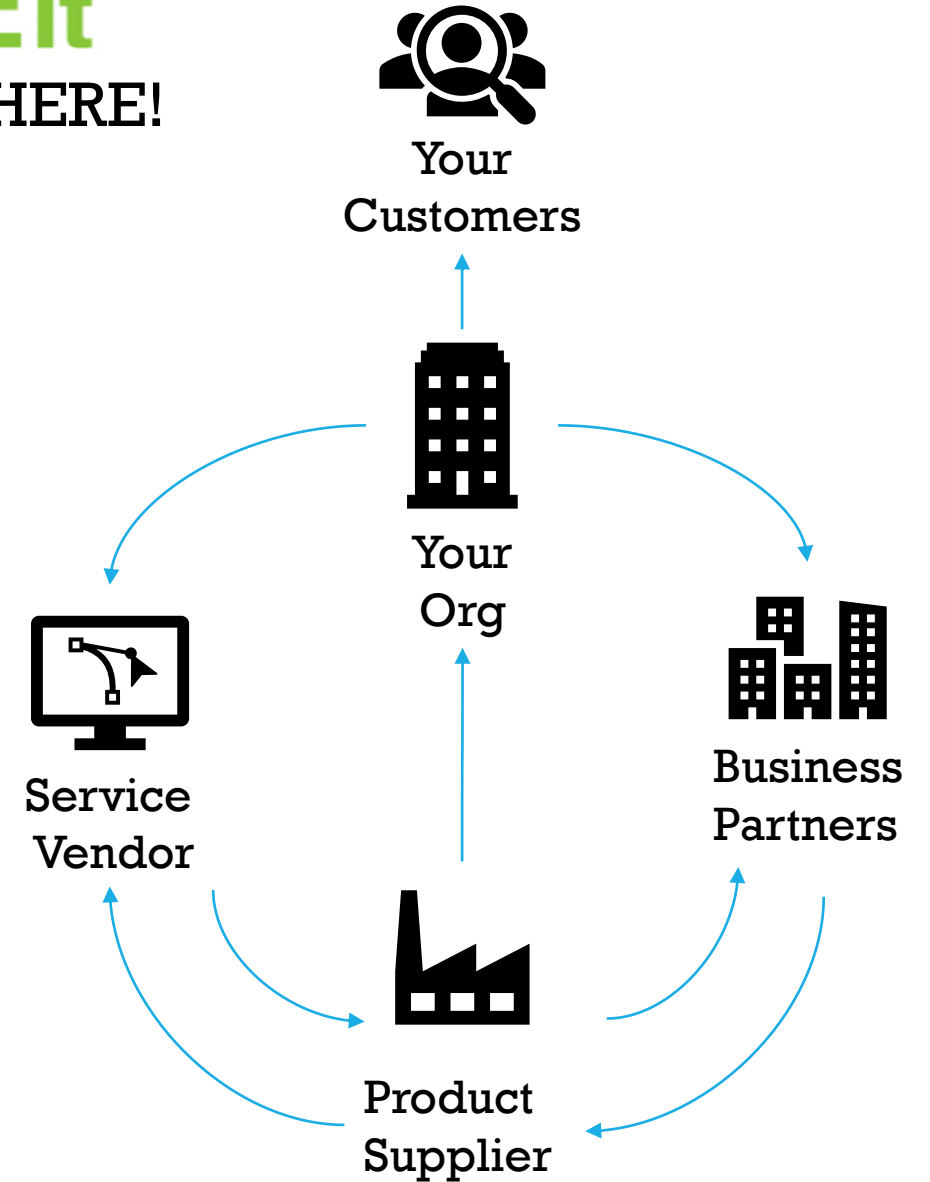
# 3<sup>RD</sup>, 4<sup>TH</sup>, AND 5<sup>TH</sup> PARTY BREACHES?

Is your organization impacted?

**Think:**

- Vendors, Suppliers, Partners
- Vendors of Suppliers
- Vendors of Partners
- Partners of Suppliers
- Vendors of Vendors
- Vendors of... And on it goes

It seems  
**MOVEit**  
is EVERYWHERE!





Let's Review

# TIMELINE OF CLOP CAMPAIGNS

CL0P variant of  
CryptoMix  
appears

February 2019

First victim is  
listed on  
CL0P^\_-Leaks

April 2020

CL0P money  
launderers arrested

June 2021

South Staffordshire  
Water hit by CL0P

August 2022

GoAnywhere MFT  
data extortion

January 2023

2019

2020

2021

2022

2023

MOVEit  
data extortion

May 2023

December 2020

Accellion FTA  
data extortion

Mid-2019

TA505 begins  
delivering CL0P  
ransomware

November 2021

SolarWinds Serv-U  
data extortion

December 2022

CL0P Linux variant  
appears

April 2023

PaperCut MF/NG  
data extortion

# OLD GEN RANSOMWARE

## THE 7 STEPS



1

2

3

4

5

6

7



Initial  
Access



Establish  
Foothold



Internal  
Recon



Lateral  
Movement



Privilege  
Escalation



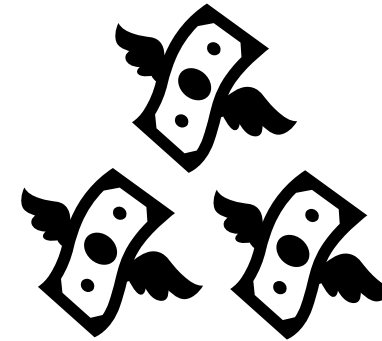
Data  
Exfiltration



Data  
Encrypted

# NEXT GEN RANSOMWARE

## THE 3 STEPS



1

2

3

4

5

6

7



Initial  
Access



Establish  
Foothold



Internal  
Recon



Internal  
Movement



Privilege  
Escalation



Data  
Exfiltration



Data  
Encrypted

# WHO'S NEXT?



Will

@BushidoToken

Which MFT could #CLOP target next?

This list should get you started:

Globalscape EFT

Pro2col Coviant Diplomat MFT

Axway MFT

Cleo MFT

Oracle MFT

Citrix ShareFile MFT

Adobe Send & Track MFT

LeapFile

IBM MFT

Accellion Kiteworks

Check for updates & ensure you've got logs ⚠️

4:53 PM · Jun 27, 2023 · 14.9K Views

View Tweet analytics

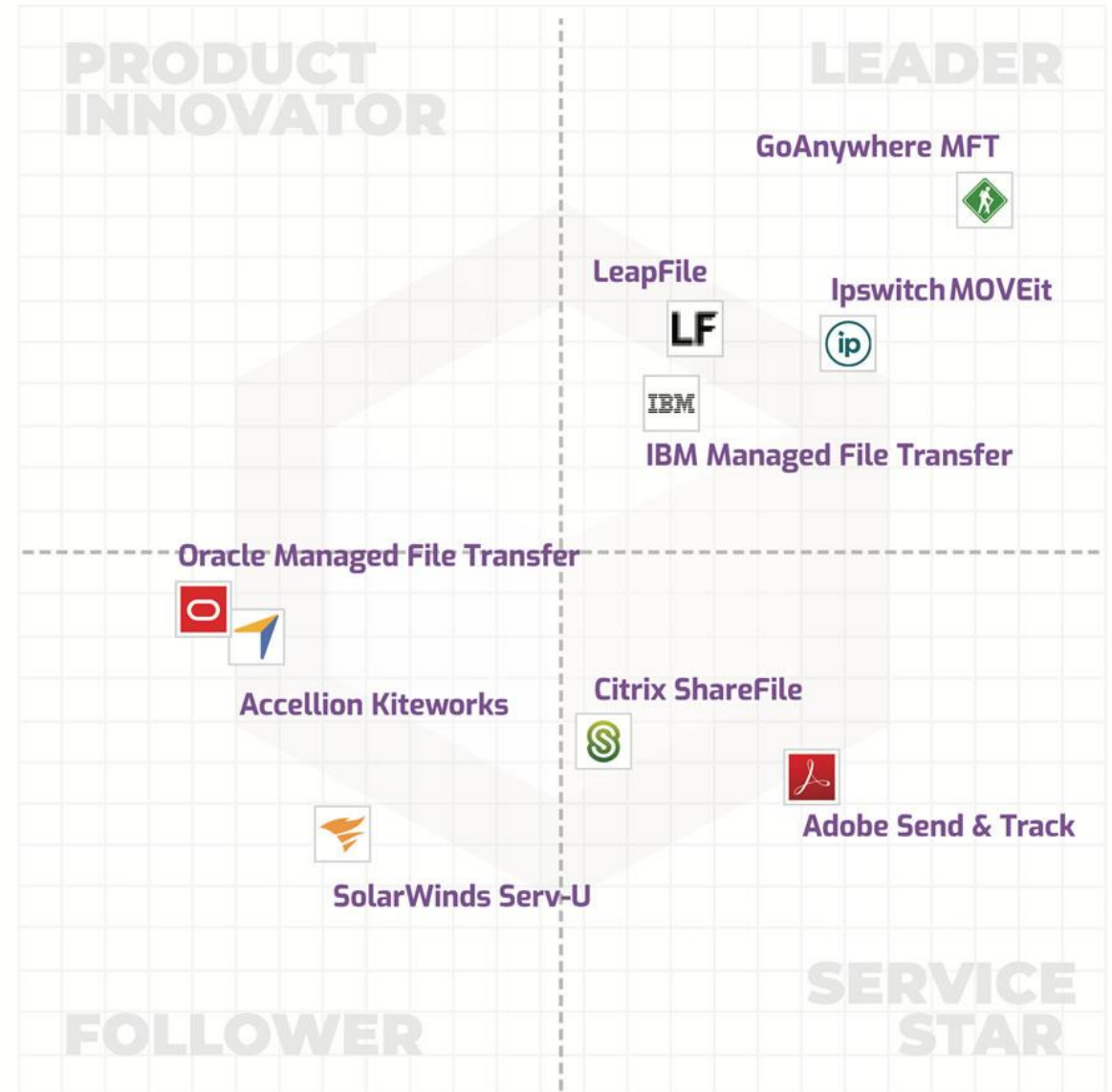
12 Retweets 1 Quote 68 Likes 11 Bookmarks

9.4

PRODUCT FEATURES AND SATISFACTION

7.4

Y  
X



6.4

VENDOR EXPERIENCE AND CAPABILITIES

10





# MOVEit-Transfer

PublicEdit PinsWatch 14Fork 4Starred 54main1 branch0 tagsGo to fileAdd file<> CodeBushidoUK Update README.mde344b3d 7 hours ago122 commitsImagesAdd files via upload7 hours agoREADME.mdUpdate README.md7 hours agoREADME.md

## MOVEit Transfer Hacking Campaign Tracking

- A repository for tracking events related to the MOVEit Transfer Hacking Campaign
- Events mapped to the Diamond Model, plus resources and information

### Event Summary Diagram

### About



A repository for tracking events related to the MOVEit Transfer Cl0p Campaign

[www.curatedintel.org/2023/06/cl0p-likes...](https://www.curatedintel.org/2023/06/cl0p-likes...)

ransomwarecticybercrimecl0pReadmeActivity54 stars14 watching4 forksReport repository

### Releases

No releases published

[Create a new release](#)

### Packages

No packages published

[Publish your first package](#)

### Contributors 5

BushidoUK BushidoToken

C:\User\wthomas

# Thanks for Listening!

- <https://blog.bushidotoken.net/>
- <https://twitter.com/BushidoToken>
- <https://github.com/BushidoUK>
- <https://www.sans.org/profiles/will-thomas/>
- <https://www.linkedin.com/in/william-t/>

