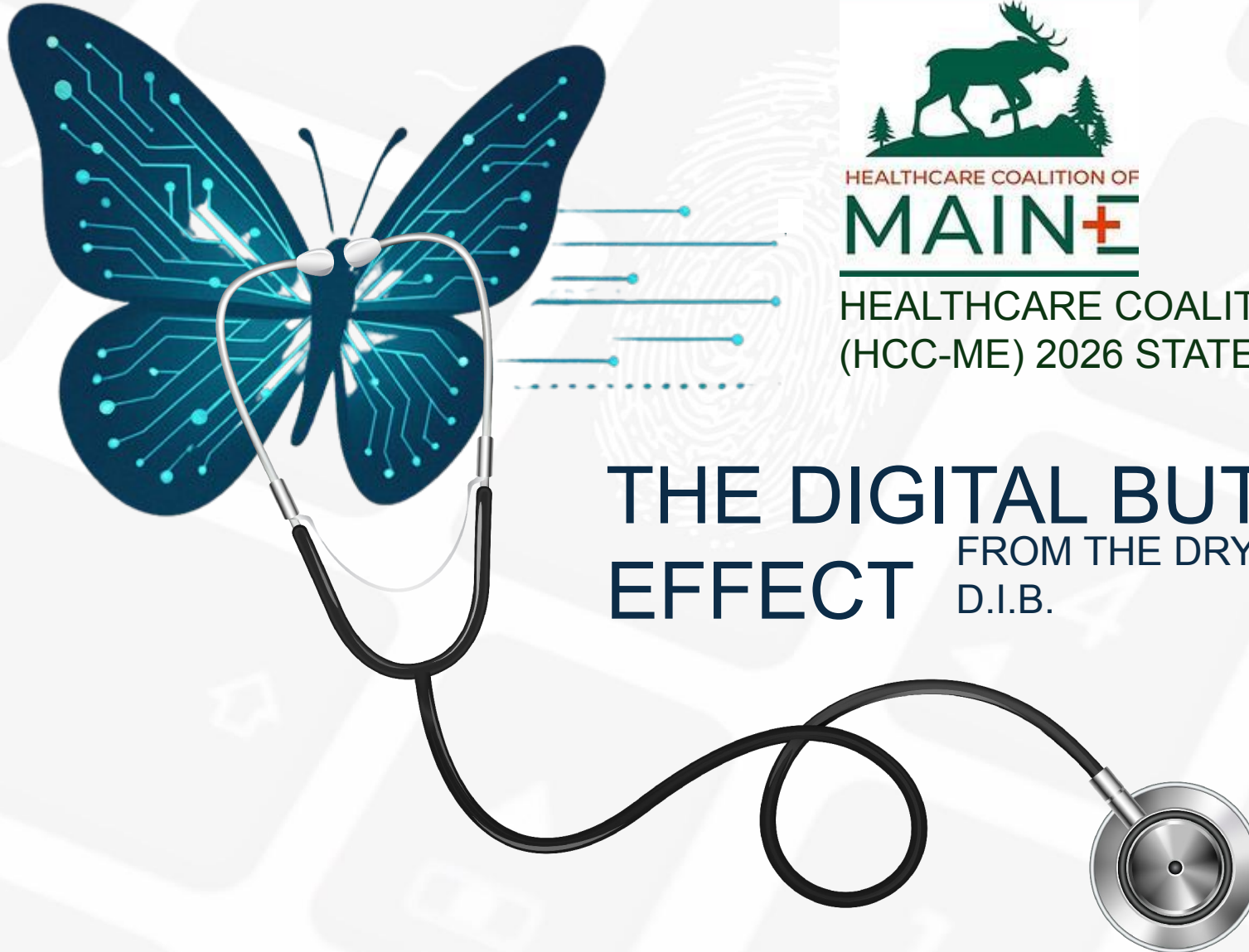




HEALTHCARE COALITION OF MAINE
(HCC-ME) 2026 STATEWIDE CONFERENCE

THE DIGITAL BUTTERFLY EFFECT

FROM THE DRY CLEANER TO THE
D.I.B.

Kurtis
Minder

KURTIS
MINDER



FEMA

TEDx

XFIL

protectiv

DeleteMe



CYBER LEADER
NEGOTIATOR
AUTHOR
ADVOCATE
EDUCATOR
CITIZEN

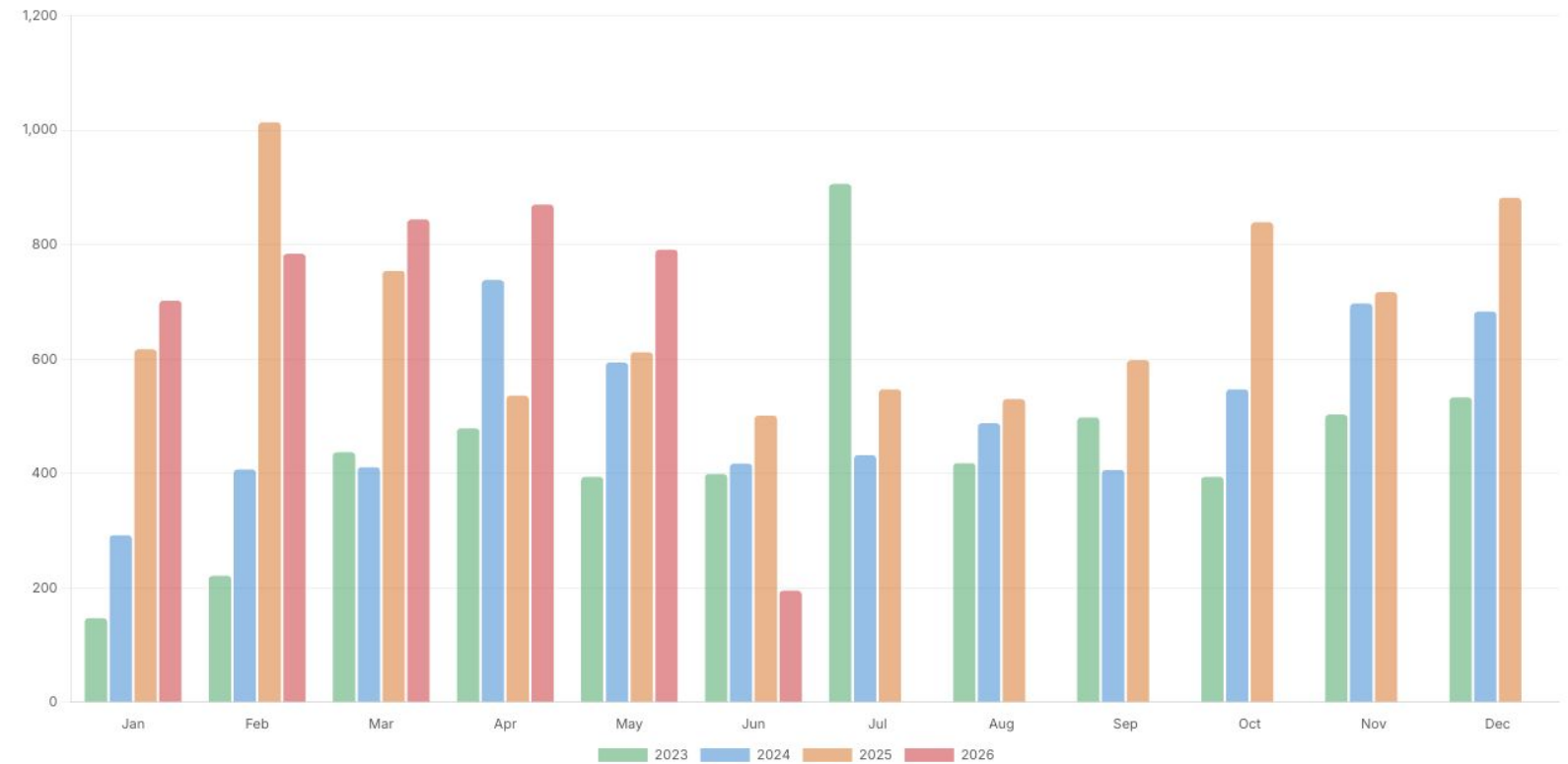


I HAVE A WEIRD JOB

I DON'T NEED TO SHOW YOU STATS



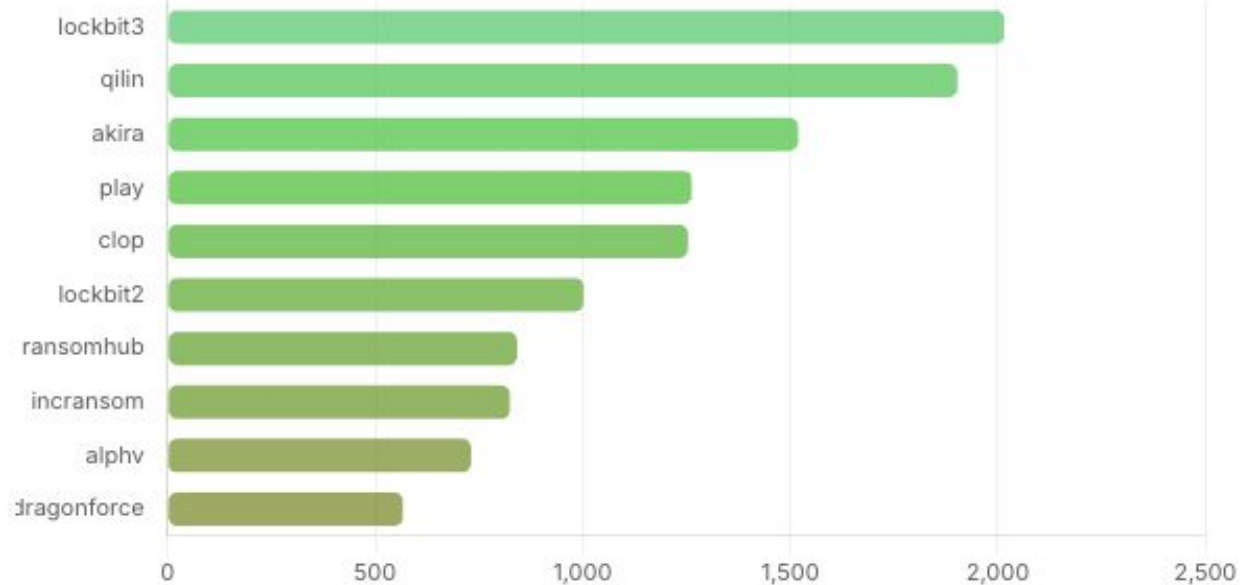
VICTIMS PER MONTH (2023-2026)



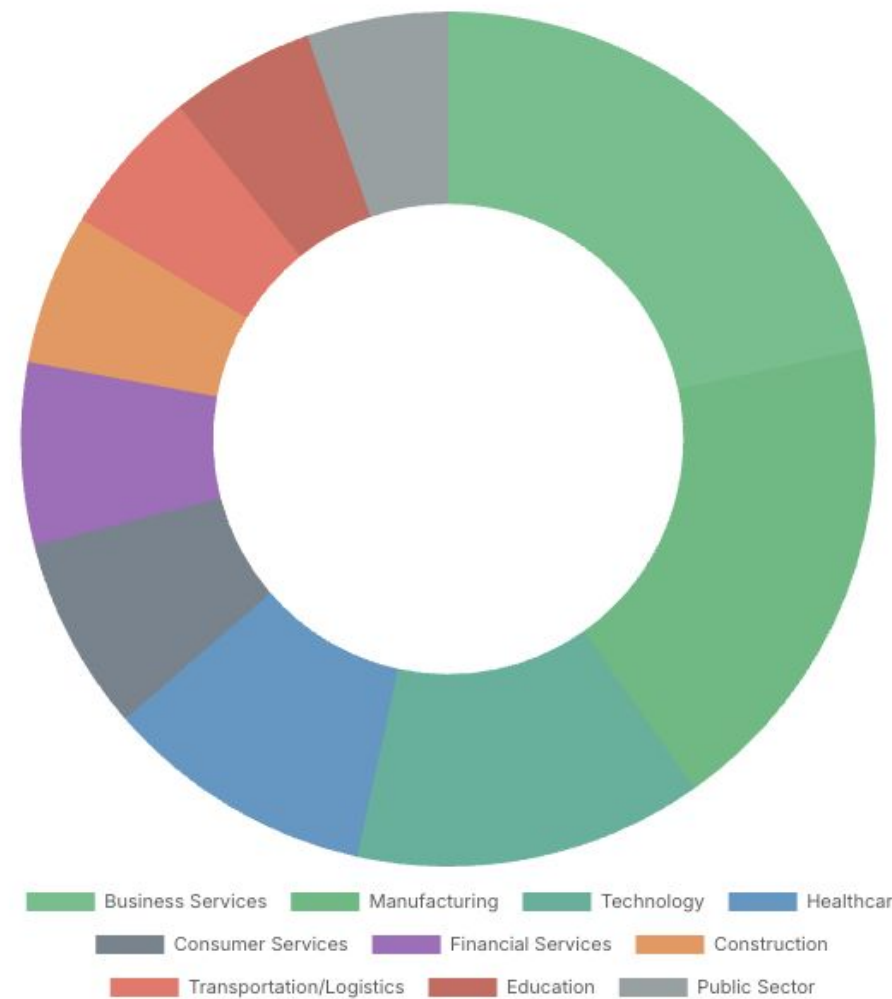
**Ransomware.live*

STATS CONTINUED

TOP 10 GROUPS ALL TIME



TOP 10 SECTORS ALL TIME



**Ransomware.live*

HEALTHCARE: THE #1 TARGET

275M

patient records breached in 2024
up 60% over the year before

≈82%

of the U.S. population
had health data exposed, stolen, or leaked

~2 / day

major healthcare breaches
725 reported in 2024 — 81% from hacking

THE BUTTERFLY EFFECT — HEALTHCARE EDITION

One clearinghouse goes down. The whole country stalls.

The 2024 Change Healthcare ransomware attack exposed **190 million people** — and froze insurance claims and pharmacy payments for hospitals and clinics nationwide. **\$22M ransom paid. \$3.1B in damage.**

Sources: HHS OCR / HIPAA Journal 2024 breach report; UnitedHealth / Change Healthcare disclosures

IT'S ALREADY HAPPENING HERE

Two Maine health systems. One year.

MARCH–JUNE 2025 · DATA BREACH

Central Maine Healthcare

145,000

patient records exposed

Names and Social Security numbers stolen — in a system that serves about 400,000 people across central and western Maine.

MAY 2025 · RANSOMWARE

Covenant Health

3 hospitals

knocked offline across ME & NH

Phones and internet down, lab orders reduced to paper, and extended ER waits across St. Mary's (Lewiston), St. Joseph (Bangor), and their New Hampshire sister hospital.

Sources: Maine AG / HIPAA Journal; The Record (Recorded Future); Covenant Health incident notices, 2025



TODAY'S CYBER INCIDENTS
ARE NOT LIKE FIVE YEARS
AGO



RANSOM NOTE FROM RECENT CASE

-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from your system/network.
Our group cooperates with the mass media.

If you refuse to communicate with us and we do not come to an agreement, your data will be reviewed and published on our blog and on the media page (<https://wikileaks2.site/>)

Blog links:

<http://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad.onion>

<http://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd.onion>

Data includes: |

- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning

- 1) If you modify files - our decrypt software won't able to recover data
- 2) If you use third party software - you can damage/modify files (see item 1)
- 3) You need cipher key / our decrypt software to restore you files.
- 4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.

-- Recovery

- 1) Download tor browser: <https://www.torproject.org/download/>
- 2) Go to domain
- 3) Enter credentials

Please note that communication with us is only possible via the website in the Tor browser, which is specified in this note.

All other means of communication are not real and may be created by third parties, if such were not provided in this note or on the website specified in this note.

-- Credentials

Extension: zjbQx30SdT

Domain: 56tsorca7[REDACTED]mb5ao4rcfjzfid.onion

login: [REDACTED]

password: [REDACTED]

RANSOMWARE VICTIM SITE

You have 3 days, 02:37:31

* If you do not pay on time, the price will be doubled

* Time ends on

Monero address:

Current price

1578.282 XMR

≈ 200,000 USD

After time ends

3156.564 XMR

≈ 400,000 USD

* XMR will be recalculated in 2 hours with an actual rate.

INSTRUCTIONS

CHAT SUPPORT New

ABOUT US

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

To decrypt your files you need to buy our special software - General-Decryptor.

* If you need guarantees, use trial decryption below.

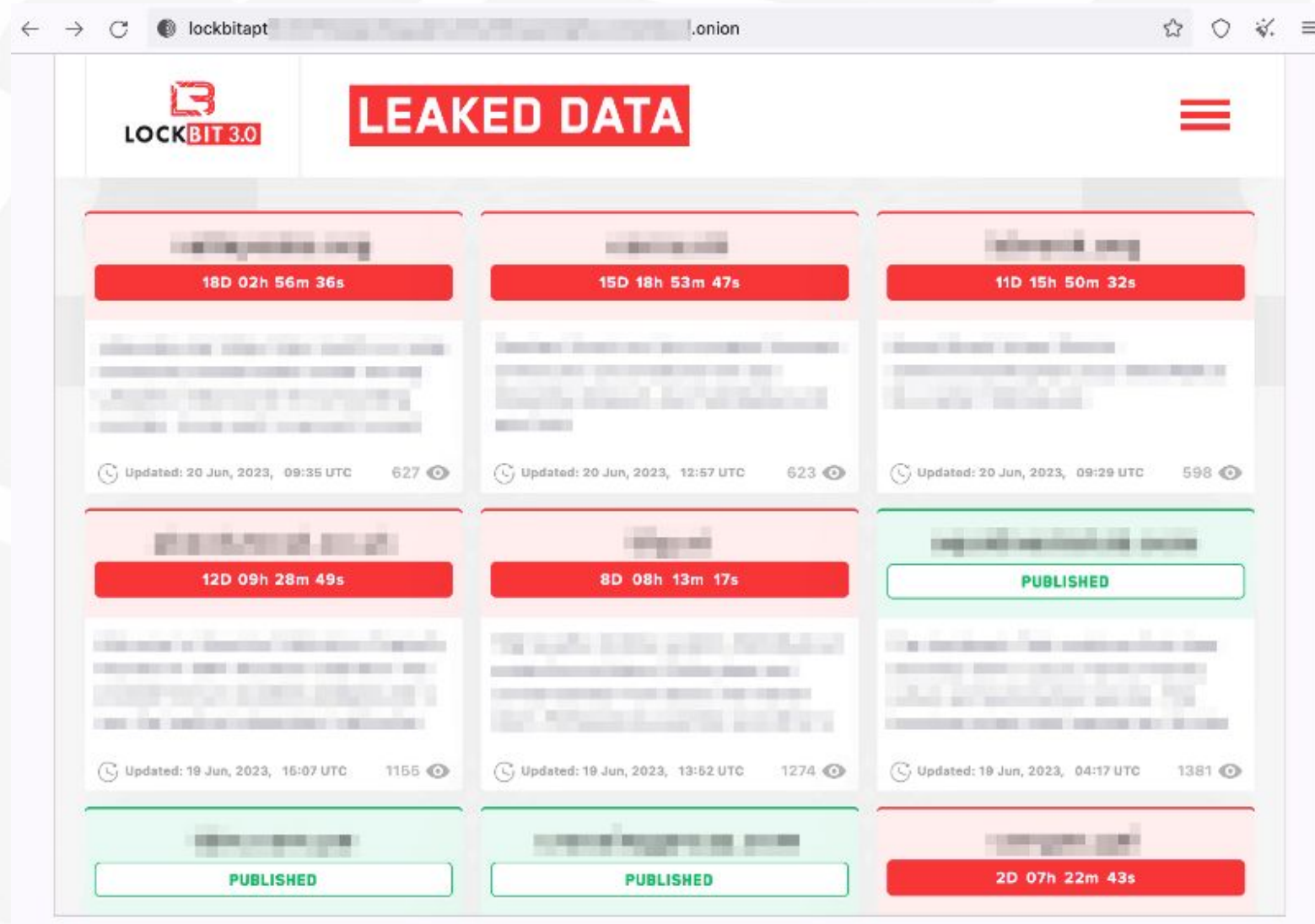
How to buy General-Decryptor?

Buy XMR with Bank

- Kraken
- AnyCoin (EUR)
- BestChange

Buy XMR locally with cash
or online

RANSOMWARE SHAME SITE



RANSOMWARE PLATFORM

PROCESSES TO KILL ?

sql;oracle;ocssd;dbnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;tbirdconfig;mydesktopqos;ocomm;dbeng50;sqbcoreservice;excel;infopath;msaccess;msspub;one

SERVICES TO KILL ?

vss;sql;svc\$;memtas;mepocs;msexchange;sophos;veeam;backup;GxVss;GxBlr;GxFWD;GxCVD;GxCIMgr

ACCOUNTS FOR IMPERSONATIONS ?

Administrator:123QWEqwe!@#!@#

DELETE GPO DELAY ?

1

SELF-SPREAD ? ☒

SPREAD METHOD ? ☒

DELETE EVENTLOGS ? ☒

ENCRYPT FILENAME ? ☒

LANGUAGE CHECK ? ☒

NETWORK SHARES ENCRYPTION ? ☒

RUNNING ONE ? ☒

DESKTOP WALLPAPER ? ☒

SHUT DOWN THE SYSTEM ? ☐

KILL DEFENDER ? ☒

SKIP HIDDEN FOLDERS ? ☐

PSEXEC ? ☒

GPO ? ☒

ENCRYPTION MODE ? ☒

IMPERSONATION ? ☒

KILL SERVICES ? ☒

LOCAL DISKS ? ☒

KILL PROCESSES ? ☒

PRINT A NOTE ? ☒

SET ICON ? ☒

SELF-DELETE ? ☐

WIPE FREE SPACE ? ☐

GPO PS UPDATE ? ☒

AUTO ? ☒

FAST ? ☒

SAME ENCRYPTION KEY ? ☐

MAXIMUM DECRYPTOR PROTECTION ? ☐

GET LOCKBIT BLACK ↻

Hackers Rack Up Credit Card Charges After Data Breach at Dry Cleaners

HOW DO WE GO FROM THIS?

I sell a secret document of the US Department of Defense – information about the NC2 system

hot · 15 minutes ago · documents government usa

[\$600] USDoD / USMC / USAF / US Army Defense Contractor - \$2billion Revenue

by miya - Wednesday April 9, 2025 at 06:46 AM

[CLASSIFIED] NATIONAL SECURITY DOCUMENT LEAK

by HumanError - Thursday February 6, 2025 at 08:35 AM

HumanError

02-06-2025, 08:35 AM

Hello B

TOP SECRET & HIGHLY CONFIDENTIAL UFO/NSA/FBI/CIA/ARMY DATA FOR SALE
100GB OF TOP SECRET GOV DATA

TopSecretDocuments · Wednesday at 9:55 PM

TO THIS?

database
by EnergyWeaponUser - Thursday April 3, 2025 at 06:13 PM

EnergyWeaponUser
Supreme God King
GOD
Posts: 86
Threads: 13
Joined: Feb 2024
Reputation: 1,883

Hello BreachForums Community
Today, I have uploaded the [REDACTED] for you to download. Thanks for reading and enjoy!

Breached by @IntelBroker & @EnergyWeaponUser
In 2nd April 2025 [REDACTED] suffered a data breach that exposed the information.

Data ranges from 2023 to 2024
Compromised User data
login_id, EMAIL, PASSWORD, LASTIP, CREATED, UPDATED, DELETED, WHERE FROM, DATA ALSO INCLUDE PHONE NUMBER, GENDER & MORE
SAMPLE!

```
{1, "a[REDACTED].com", "1999-759e9ee89ec5e95d56ace2e89b4cc08d715337294e29667d;c8b77f8a1981652a3a36e827ae355dc608e15a1f2c73229", "127.0.0.1", "2023-11-01 15:39:22", "2025-04-02 09:46:54", "N", "none", "N", "N"},  
(2, "skyw[REDACTED].concert.com", "1999-4f6bf2c89f5b27e64a0f272bce9b8e8cf201c802fe9b935-91fac79b3b7472a440b7a7243b32789c819259688993cb", "127.0.0.1", "2023-11-02 08:56:08", "2025-01-07 21:15:40", "N", "none", "N", "N"},  
(3, "th[REDACTED].il.net", "1999-c87a8bf3a2e34f257b35a7b98815cae62e6a76bd48233c-4dbf99c9cc93568a707bd9e496437acd56f7962982a5a618", "112.168.241.242", "2023-11-02 15:39:38", "2023-11-02 15:49:21", "N", "none", "N", "N"), (4, "drv811-[REDACTED] 1999-aea950feda3d1f231aa46740a8d884f317556fc26321e1f;fdsee34c4a276dc6695774ab3e68f97e31879c13dc43c0b", "230.124.223.3", "2023-11-02 16:06:13", "2023-11-26 23:48:40", "N", "none", "N", "N"),  
(5, "v[REDACTED]@gmail.com", "1999-025f4bdbc0b89464bca1f40c11c6574a37f8a6282068ab-c7688e53c4645dbf6d755198b54b4495298e11f99195d48", "17.11.126.182", "2023-11-02 17:02:36", "2024-11-05 00:26:25", "N", "none", "N", "N"),  
(6, "[REDACTED] 116203@gmail.com", "1999-75e9d49d9e30121ea7a751f79a70f559c5c2f249c1f3e88:a18a5f796a90bc46e6dc4ee5e9a2adb7e4ace4f5ee377ba0", "79.32.126.58", "2023-11-02 17:03:43", "2024-12-03 09:35:28", "N", "none", "N", "N"),  
(22454, "stop[REDACTED]1.co.id", "1999-08402bc9eb74a24cef9f56ea9599045913ac57dc130d473ed;fa2fff710f452b9e0b6ed34e242b5a7900b3a1fe470e17c9f", NULL, "2023-09-01 00:00:51", "2023-12-30 12:22:33", "N", "none", "N", "N"),  
(22455, "sea[REDACTED]b.co.id", "1999-0965d428ea6c159ef12385da74b72c4546dc181a92bcf84-4a1c769a57dae5728b58728c308a4488a4b1ec858daa6d", NULL, "2023-09-01
```

IT HAPPENS LIKE THIS...

AND LIKE THIS...

Minnesota City Government Network
by MIYAK000 - Friday March 7, 2025 at 04:34 AM

8 hours ago

Details:
Minnesota City Government Network

Privilege:
Firewall Root Access

Revenue:
Not Public

Price:
\$400

Price is NOT negotiable. SERIOUS BUYERS ONLY
Session:058332638e9d646a610306997816f9f4b482e427176ed105aabbbe99868f56e918
Contact me on session for more details.

PM FOR CONTACT INFO
HELLCAT

Initial Access Broker
GOD
S V
Posts: 352
Threads: 225
Joined: Aug 2024
Reputation: 1,771
View All

IT ISN'T ABOUT THE ONE DATA BREACH



“...Oh I am not that important...”

IT'S ABOUT ALL OF THEM

All Time Totals

Total Sources

102,560

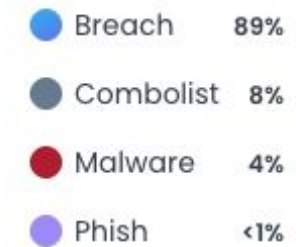
Total Records

77,463,747,862

Records Timeline



Source Types



**Spycloud*

IT'S REALLY NOT THAT COMPLICATED

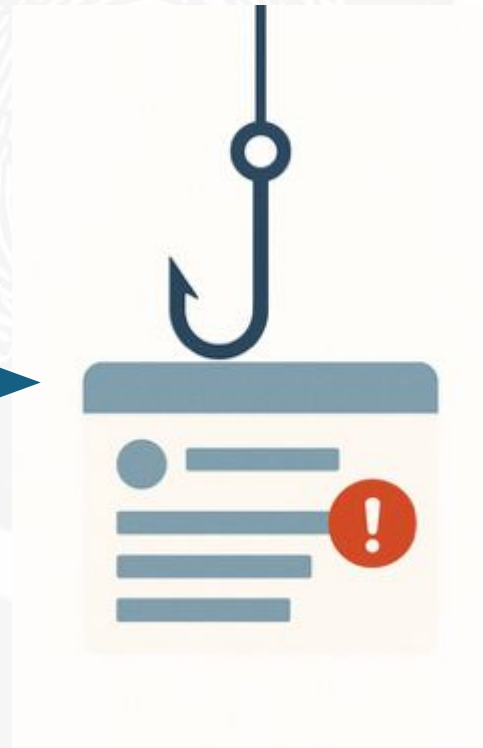


COMMON SCENARIO

**THREAT ACTOR
MONITORS DRY
CLEANER'S INBOX**



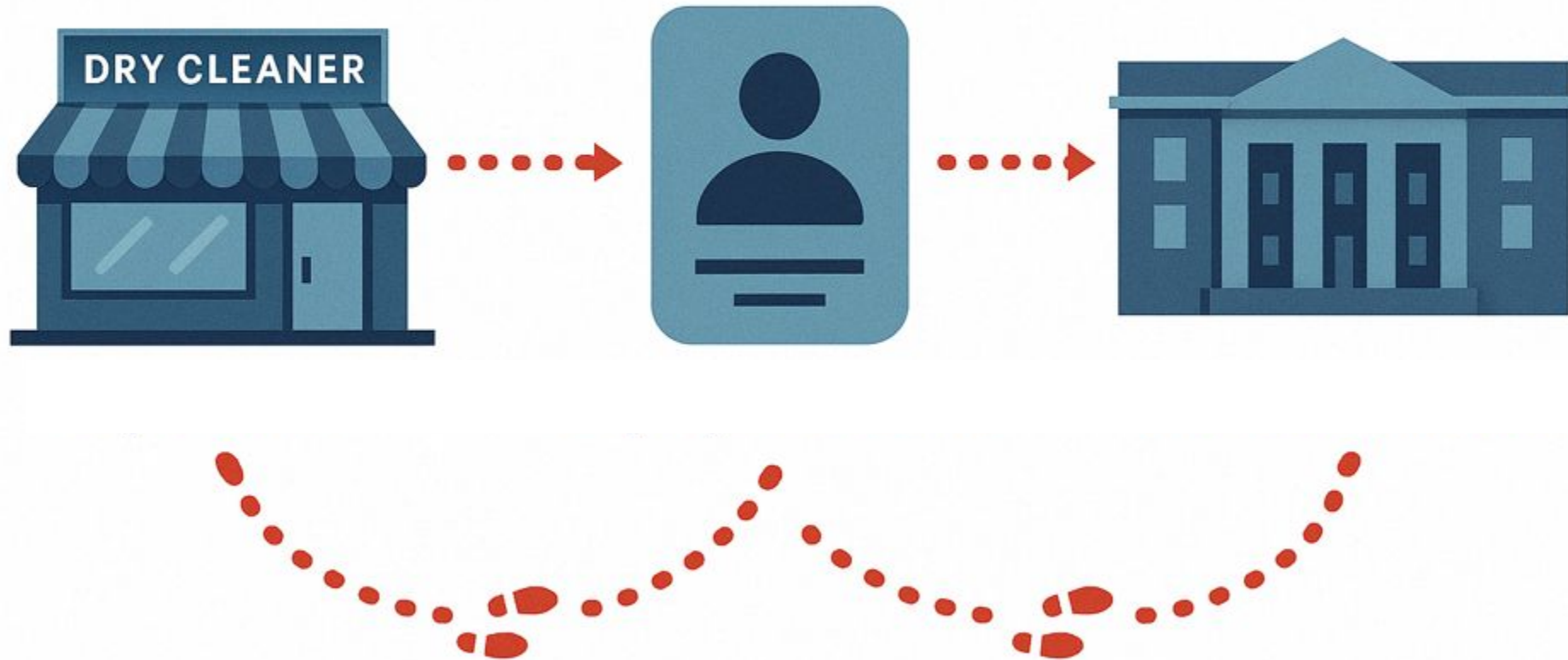
**SENDS CONVINCING
PHISHING EMAIL TO DIB
CONTRACTOR**



**EMAIL HAS MALWARE
INSTALLING BACKDOOR
OR KEYLOGGER**



PRETTY MUCH A WALK IN THE PARK



AND HERE WE ARE

I sell a secret document of the US Department of Defense – information about the NC2 system

hot · 15 minutes ago · documents government usa

[\$600] USDoD / USMC / USAF / US Army Defense Contractor - \$2billion Revenue

by miya - Wednesday April 9, 2025 at 06:46 AM

Cloud

Top Secret Documents Leaked Of Nsa,Fbi.,Cia,Ufo,Army

[CLASSIFIED] NATIONAL SECURITY DOCUMENT L

by HumanError - Thursday February 6, 2025 at 08:35 AM

TOP SECRET & HIGHLY CONFIDENTIAL UFO/NSA/FBI/CIA/ARMY DATA
100GB OF TOP SECRET GOV DATA

TopSecretDocuments ·

LeaksChan



Central_Bank_of_Russia (1).torrent

1.0 MB

Central Bank of Russia



Documents_from_the_U.S._Espionage_Den (1).torrent

20.4 KB

Iranian students seized an entire archive of CIA and State Department documents, which represented one of the most extensive losses of secret data in the history of any modern intelligence service. Even though many of these documents were shredded into tiny strips before the Embassy and CIA

DLA Classified Logistics Operations Dashboard

Logged in as: Col. Doe (SCI Clearance) Logout

CLASSIFIED - TOP SECRET ACCESS ONLY | Last Login: 2025-03-15 08:45 UTC | Session ID: DLA-SEC-2025

Total Active Shipments: 12

Critical Alerts: 3

Secure Routes: 9/10

Last Update: 2025-03-15

Search Shipments & Operations...

View Details

Issue Alert

Secure Transmission

SHIPMENT ID	DESCRIPTION	DESTINATION	STATUS	RISK LEVEL	EST. ARRIVAL
SH-2025-L-001	12x AN/PRC-117G Radios (Encrypted VHF/UHF)	Naval Air Base, Norfolk, VA	At Risk	High (Logistics Delay)	2025-03-18
SH-2025-L-002	6x Falcon III Radios (AN/PRC-117G)	Naval Air Station, Norfolk, VA	Delayed	Medium (Supply Chain)	2025-03-20
SH-2025-L-003	4x TRC-9210 Satellite Radios	Naval Air Station, Base, Turkey	Secure - En Route	Low	2025-03-17
SH-2025-L-004	8x XTS-5000 Digital Radios	Fort Campbell, KY	On Hold	Medium	2025-03-14
SH-2025-L-005	2x Schwarz SDR (Software-Defined Radio)	Naval Air Base, Qatar	In Transit	High (Cybersecurity)	2025-03-19



AND THEN A DECISION HAS TO BE MADE



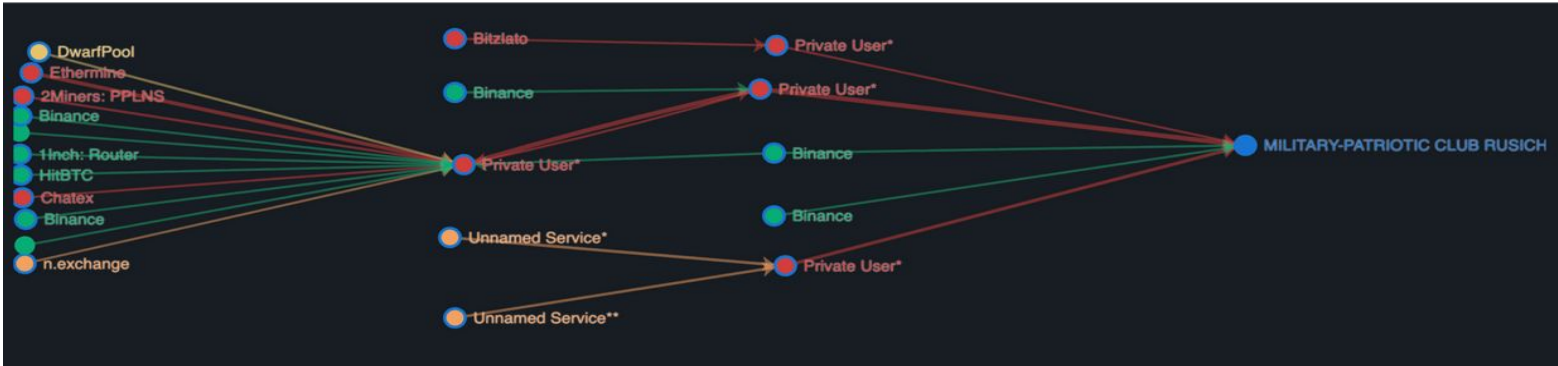
SHOULD I PAY?

AND THERE IS THIS



Are the bad guys buying
G-Wagons or Kalashnikovs?

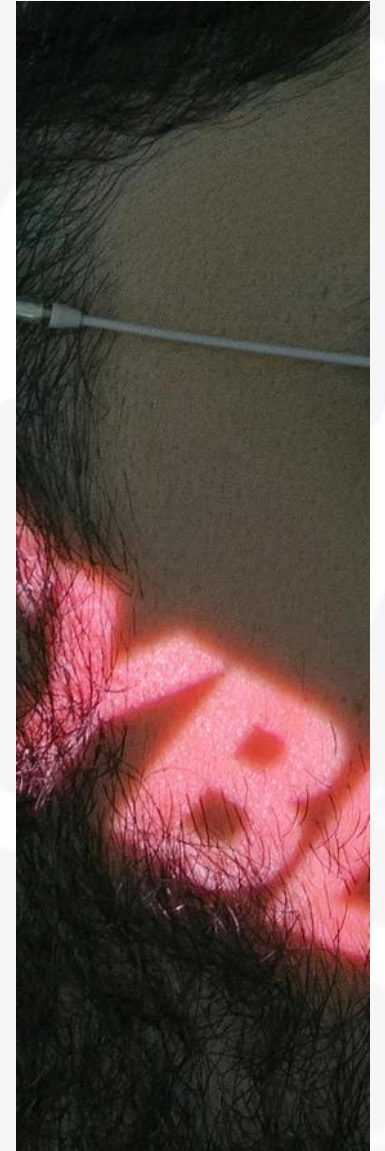
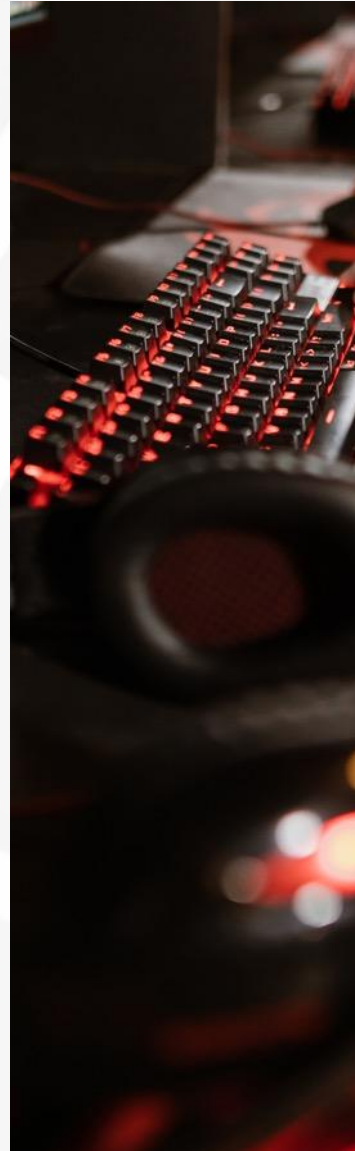




**special thanks to Paul Marrinan and Nominis*

HOW DO WE STOP THIS?

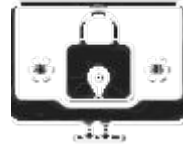
- Better Cyber Hygiene and Culture
- Incident Response Planning and TTX
- Policy shift
- Shift Accountability



DO THESE THINGS AND PROTECT YOURSELF



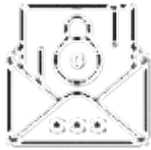
Password Policy



Use a
Password
Manager



Multi-Factor
Authentication



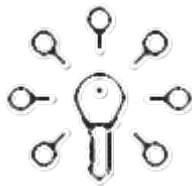
Email &
Credential Policy



Patch



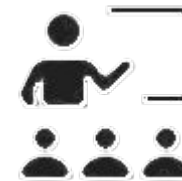
Backups



Secure Remote Access



Digital Risk
Protection Services



Security Awareness
Training

A close-up, slightly angled view of a computer keyboard. The keys are light gray with white characters. A fingerprint is overlaid on the central keys, specifically over the 'Enter' and 'Shift' keys. The text "IT ISN'T ONLY ABOUT DEFENSE. IT IS ABOUT RESILIENCE." is centered over the keyboard.

IT ISN'T ONLY ABOUT DEFENSE. IT IS ABOUT RESILIENCE.

GEN AI IS HERE

THREATS EMERGED

EARLY Synthetic content

Data synthesis

EVOLVED QUICKLY

Vuln discovery

Auto exploit dev

AUTOMATED CAMPAIGNS

Phishing

Scam

Exploitation



GEN AI cont.

WAR OF THE ROBOTS

GOOD CYBER HYGEINE IS A CIVIC DUTY

- Everyone is a target
- Everyone is important
- Together we can shift the tide
- Be a good citizen!



THANK YOU – READ MY BOOK?

- CYBER **ESPIONAGE**
- RANSOMWARE **RESPONSE**
- CYBER INTEL **PROCESS**
- OPSEC **BEST PRACTICES**
- CYBERWAR **EXPLAINED**
- CYBER DEFENSE **EXPLAINED**

You may reach me @
kurtisminder.com
[linkedin.com/in/kurtisminder](https://www.linkedin.com/in/kurtisminder)
@kurtisminder on X
kurtis@kurtisminder.com

