POLICE APPSEC: Protecting Cases, Citizens, and Ourselves

COVER SLIDE

W: NEbraskaCERT Cyber Security Forum
W: 2021-05-19 @ 11.30-13.00 CDT
W: Google Meet - https://www.nebraskacert.org/CSF
“In Cyberspace Your Mic is Always Muted”

-- Anthony Kava | Tactical Computer Geek | https://forensic.coffee --
POLICE APPSEC:
Protecting Cases, Citizens, and Ourselves

W: NEbraskaCERT Cyber Security Forum
W: 2021-05-19 @ 11.30-13.00 CDT
W: Google Meet - https://www.nebraskacert.org/CSF
“In Cyberspace Your Mic is Always Muted”

**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM  38911 BASIC BYTES FREE
READY.
POLICE APPSEC: Protecting Cases, Citizens, and Ourselves

W: NEbraskaCERT Cyber Security Forum
W: 2021-05-19 @ 11.30-13.00 CDT
W: Google Meet - https://www.nebraskacert.org/CSF

“In Cyberspace Your Mic is Always Muted”

-=| Anthony Kava | Tactical Computer Geek | https://forensic.coffee |=-.
POLICE APPSEC:
Protecting Cases, Citizens, and Ourselves

W: NEbraskaCERT Cyber Security Forum
W: 2021-05-19 @ 11.30-13.00 CDT
W: Google Meet - https://www.nebraskacert.org/CSF
“In Cyberspace Your Mic is Always Muted”
I LOVE THIS. I FEEL SO SOCIAL.
Rules of (Audience) Engagement

- Opinions expressed are poorly-formed and mine.
- Statements are not official positions of PCSO.
- I can’t hear you so I will assume all jokes land.
- There may be some bad words; blame Google Meet.
Agenda

? : Where the hell is Iowa? Intro

I : US Police Cyber Threats and Woes

II : AppSec and Software Vulnerabilities

III : #BlueLeaks: Breach, Leak, and Pain

IV : Conclusion / Apologies
COMING SOON:

2228-03-22
(a Saturday)
Pottawattamie County
a.k.a. Pott County
Sworn Personnel
(not to scale)
1.1MM Employees
18K L.E. Agencies
12K Local Agencies
75 Federal Agencies
### SPARKS POLICE DEPARTMENT INCIDENT REPORT

**CASE:** 13-9953

**ADDRESS/LOCATION:**
- Occurred from (or at) 2275 18th St.
- When Reported: 10/21/13, Tues 07/16

**CASE SUMMARY:**
- Case Cross Reference 1
- Case Cross Reference 2

**HOW ORIGINALY RECEIVED:**
- Desk Officer
- Mail Officer

**DATE:**
- 10/21/13
- Tues 07/16

**PERSON REPORTING (Signature):**
- Lt. Hawkins

**APPROVING SUPERVISOR:**
- Lt. Hawkins

**SPARKS CASE NO.:** 13-9953

**PERSONNEL:**
- Lt. Hawkins

**BUSINESS NAME:**
- Sparks Middle School

**ADDRESS:**
- Landsherry

---

**Jury Trial:**
- Yes, Explain in Supplement

**INVOVLED:**
- Name (Last, First, Middle)
“We’re the good guys, Marty.”
DIGITAL FORENSICS
CYBERSECURITY
CYBER CRIME
BIT O’ I.T.
Cockrell Hill police lose years worth of evidence in ransom hacking

The Cockrell Hill Police Department lost video evidence and a cache of digital documents after hackers invaded the department’s computer system last month.
The malware, which most likely originated from either Russia or Ukraine, gained access to the department's computer servers after someone clicked on a cloned email made to look like it was sent from a department email address, Barlag said. Messages generated by the computer virus demanded $4,000 worth of internet currency known as Bitcoin as ransom for the return of the files, he said.
Ransomware Strikes
Baltimore's 911 Dispatch System

Fortunately, Baltimore's IT office managed to isolate the threat and quickly restore the city's dispatch system.
Baltimore ransomware attack will cost the city over $18 million

City residents are still facing issues.
Muscatine cyber attack targets government financial server

POSTED 8:44 AM, OCTOBER 19, 2018, BY WQAD DIGITAL TEAM, UPDATED AT 08:50AM, OCTOBER 19, 2018

2018-10 City of Muscatine, IA
MUSCATINE, Iowa – A MUSCOM server and the City of Muscatine Shieldware, Springbrook (financial) server, and other city servers were the victims of a ransomware attack at approximately 1 a.m. Wednesday, Oct. 10. City of Muscatine IT staff along with other IT personnel have been working to isolate the ransomware and restore servers since that time.
Cybersecurity a top priority for West Des Moines
West Des Moines reports cyber attack on city operations

posted by Jason Taylor - Dec 13, 2019
In a statement, the city said, "It’s important for the public to know that the City has work-arounds and contingency plans in place to handle network and server disruptions. Public safety services (Police, Fire, Emergency Medical Services and Westcom 911 dispatch) are operating and stand ready to provide assistance as usual to anyone who needs them."
Firewall
DMZ
Clients
LAN
(nougat not pictured)
The Local.gov AppSec Experience
How many **VULNS** could you find if you spent quality time with local.gov s/w?
LOCAL.GOV SOFTWARE
TL;DR: same stuff, different industry
(SPOILER ALERT)
Why is this stuff IMPORTANT?
INCOME TAX

PAY 10%
OR
$200
**COMMODORE 64 BASIC V2**

64K RAM SYSTEM 38911 BASIC BYTES FREE

READY.

OOPS, YOUR FILES HAVE BEEN ENCRYPTED

WHAT HAPPENED TO MY COMPUTER?
CAN I RECOVER MY FILES?
HOW DO I PAY?

BITCOIN ACCEPTED HERE

WAITING FOR BLOCKCHAIN...
Every vendor: We assume customer has a “SECURE ENVIRONMENT”
COMMON FEATURES

- Crypto is Ø-BAD
- Hard-coded Creds
- Client-side Enforcement
Client-side vulns are NOT CONSIDERED IMPORTANT
If an attacker is on a client, it’s the CUSTOMER’S FAULT.
lies, damned lies, and 'we take security seriously'
Local.gov often can’t look under the hood
Small Local.gov and LE orgs are LUCKY IF THEY EVEN HAVE I.T.
We need people who CAN AND WILL (LOOK UNDER THE [BONNET])
Cases in point: THREE (3) VENDORS
Names redacted to protect SPEAKER.

All vulns REPORTED 1-5+ years ago, and either ADDRESSED -or- products RETIRED.
The findings that follow started with the Q, "How bad could it be?"
These things were found using "SPARE TIME", either in IT job or DF job.
A Tale of Three Vendors
Vendor A
FINANCES, HR, PAYROLL, INVENTORY, REAL ESTATE, LAW ENFORCEMENT MGMT.
SQL creds baked-into CLIENT INSTALL

Oh, yeah, p/w is l33tsP3aK username

*cough* Also has SA !?!?!?

Bonus: Same at EVERY SITE
- API traffic is in **PLAIN TEXT**
- Auth tokens **NEVER EXPIRE** (weeks+)
- Access controls **NOT ENFORCED** in API
BUT WAIT, THERE'S MORE!
What about that payroll website?
That time API TRAFFIC was in the clear...
... with all your PII and whatnot for WEEKS
Also XSS, but XSS is “NOT A SECURITY ISSUE”
Hosted Payroll Website

Local DB Server

Local App Server

Usually HTTPS
Please...

- Tell customers about HTTP period ->
- Let us suppress SSN (okay, but not DOB/etc.)
- Stop using same SA p/w at all sites (okay...)
- Support p/w complexity + lock-outs! (okay)
- Put someone in charge and audit (...)

Believe it or not, this has a **HAPPY ENDING**
2014-03  Denial
2015-07  Anger
2015-08  Taunting (Bargaining?)
2016-07  Depression (Ours)
2016-08  Acceptance (Theirs)
2016-12  API Audit Underway!
2017-04  Vendor Promotes Employee!
Vendor B

911 DISPATCH, LE MGMT.,
JAIL MGMT., MOBILE CAD/COMMS
● 90% “serverless” b/c DIRECT SQL
● EVERY user has a SQL account w/ DBO
● One piece has users table, uses PLAINTEXT
Web records tool meant for INTERNET USE

- Creds stored **PLAINTEXT** (later XOR tho)
- Trivial **SQLi AUTH BYPASS**
- XSS, again, “XSS is not a VULN”
- Bonus: Ampersands (&) break the product
SELECT phoneNumber FROM employees WHERE lastName = 'Kava';
712-555-1212

UPDATE dept SET name = 'Sheriff’s Office' WHERE id = 42;
*** SYNTAX ERROR NEAR: s Office’ ***

UPDATE dept SET name = ''; DELETE FROM dept; --

*** Deleted all rows from table “dept” ***
Mobile CAD Software

- Don’t need VPN b/c “WE DO CRYPTO”
- Rolled their own CRYPTO, 64-bit blocks...
- Questionable PADDING (next slide)
- Default keys, same crypto w/ PASSWORDS
DIY-Crypto / Usage

- Password MAX 12 CHAR
- Part >8 chars is PLAINTEXT (0x20 if short)
- Asked for help for I.T. PASSWORD RESETS...
Password Reset Capability

- Set from app on SERVER CONSOLE
- Vendor updated p/w expiry feature
- 1st 90-day cycle: 3x shifts of lock-outs
Password Reset Capability

- Asked for **RECIPE, CODE, or a TOOL**
- Vendor: Will dev tool, 6 months, PM, $10K?
- Our hack? **TWELVE (12) LINES OF PYTHON...**
dll=windll.product
key=b'SECURITY'
length=12
if(operation[:3].lower()==='enc' and input):
    dll.encfunc(input,key,length)           # encrypt
    print('0x' + hexlify(input).decode('utf-8'))
if(operation[:3].lower()==='dec' and input):
    input=input.decode('utf-8')             # decode to string
    if input[:2]=='0x': input=input[2:]
    input=unhexlify(input)                  # drop leading 0x
    dll.decfunc(input,key,length)           # decrypt
    print(input.decode('utf-8'))
Q: How are creds stored? A: “We’re not...”
Ah, yes, UNSALTED MD5 HASHES
Well, at least it can do ACTIVE DIRECTORY...
● Who even knows what $ means in LDAP?
● AD works, but stores MD5 vals ANYWAY
● Correction: strtolower(md5($pass))
- TLS/SSL certs not validated
- **BLIND HYPERLINKS** in messaging
- AD auth only done **ONCE**, no time limit
- TLS/SSL certs not validated
- BLIND HYPERLINKS in messaging
- AD auth only done ONCE, no time limit
Updater doesn’t need ADMIN RIGHTS, cool

B/C ‘Everyone’ on %ProgramFiles%\Client

Uses librsync, only checks SIZE + MTIME
- Client DIRECT SQL FOR AUTH
- Powerful SQL user, ROT13 for safety
- Oh yeah, client handles AUDIT TRAIL too
s/\WHERE\ password = :password/\WHERE 1 = 1/g
Look, ma, no local admin needed

0. Hex editor + SQL
1. Size + mtime
2. Auth/Aud BYPASS
3. ???
4. DEMO (1' 05'')
- All things reported, little interest at first
- Demo video sent to vendor, commanders
- Soon thereafter: Most stuff is fixed
DON'T PANIC
C: Who is your (C)ISO? Who is in charge?
R: We can’t tell you...
C: AUDIT your software! Shouldn’t be on the customer to do it.
R: Someday...maybe

The End?
NICHE software used by local.govs needs AppSec TLC like everything else.
Feds are treating BlueLeaks organization as ‘a criminal hacker group,’ documents show

The group says it’s not involved in hacking

By Ali Winston | Aug 13, 2020, 9:53am EDT

HACK OF 251 LAW ENFORCEMENT WEBSITES EXPOSES PERSONAL DATA OF 700,000 COPS

The BlueLeaks archive contains over 16 million rows of data, including emails, descriptions of alleged crimes, and detailed personal information.

Micah Lee
July 15 2020, 3:00 p.m.
I HAVE NO IDEA WHAT THAT MEANS
Websites that Generate Returns
Keeping you one step ahead of your competition

Netsential has the Experience - Our software is currently being used by Fortune 500 companies, financial institutions, small and medium sized businesses, associations, online publications, government agencies and schools throughout the United States.

Netsential Sites are Easy to Maintain - If you can cut and paste - you can maintain and update your website with Netsential's browser-based software.

Netsential Sites are Affordable & Effective - Websites are no longer labor-intensive and costly to maintain. Netsential provides flexible, customizable modules so you don't have to program everything from scratch.

Flexible, Customizable and Low Cost - Netsential builds sites with as much or as customer involvement that is desired. We train your staff to make updates - you are in control of your website. Netsential can host and manage the applications from its facilities and coordinate ongoing support, maintenance and upgrades. Netsential can customize or build modules to fit a specific market driven need.

Click here to tell us "What you Need"
The Houston Division is pleased to honor Mr. Stephen Gartrell, of Netsential, for his work designing and hosting websites that educate the public about crime and terrorism. Through his work, Mr. Gartrell has encouraged the public to work with law enforcement in an effort to reduce crime in the community.
ALL MODERN DIGITAL INFRASTRUCTURE

A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003
SQL Injection in a Nutshell

SELECT phoneNumber FROM employees WHERE lastName = 'Kava';

712-555-1212

UPDATE dept SET name = 'Sheriff’s Office' WHERE id = 42;

*** SYNTAX ERROR NEAR: s Office ***

DELETE FROM dept;

---

Department: Sheriff's Office

UPDATE dept SET name = ''; DELETE FROM dept; --' WHERE id = 42;

*** Deleted all rows from table “dept” ***
Distributed Denial of Secrets

Transparency is Not A Crime
"Distributed Denial of Secrets is a 501(c)(3) non-profit devoted to enabling the free transmission of data in the public interest. We aim to avoid political, corporate or personal leanings, to act as a beacon of available information."
RELEASE: #BlueLeaks (269 GB)

Ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources. Among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more.

hunter.ddosecrets.com/datasets/102
BlueLeaks

Ten years of data from over 200 police departments, fusion centers, and other law enforcement training and support resources, courtesy of Anonymous.

Publisher: Distributed Denial of Secrets
Data URL: data.ddosecrets.com
Manager: Myzoptik
Country: United States
Last updated: 06/19/2020

**Overview**

- **13** Types
  - Images: 564,701
  - Documents: 291,672
  - Tables: 167,319
  - Web pages: 102,445
  - Text files: 28,594
  - Folders: 15,751
  - Files: 4,936
  - Packages: 4,665
  - Workbooks: 1,468
  - Videos: 1,468

- **254** Countries
  - United States: 70,481
  - Seychelles: 4,265
  - Mexico: 3,372
  - Honduras: 1,785
  - Canada: 1,520
  - Guatemala: 976
  - Ireland: 971
  - France: 948
  - Syria: 857
  - China: 844

- **1m** Names
  - Netsential.com Inc: 58,714
  - All Rights Reserved: 45,591
  - AGENCY / CASE: 14,015
  - D.L. State Male Female Driv...: 13,600
  - First DOB(mm/dd): 13,420
  - Cross Streets: 12,197
  - Permission to Disseminate ...: 11,771
  - St. Louis Intelligence Project...: 11,348
  - Car Clouting: 10,524
  - MIAC Intel: 10,140
The FBI is watching all tweets regarding the protests, and sending them to your local police. #BlueLeaks

SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Potential Activity Alert
LOS ANGELES DIVISION

Approved for Release: 29 May 2020
SIR Number: SIR-0034076587

(U/FOUO) Civil Unrest in Response to Death of George Floyd Threatens Law Enforcement Supporters’ Safety, as of May 2020

SOURCE: (U) A documentary source.

(U) On 27 May 2020, an identified Twitter account dedicated to anarchist ideology and activity in the Los Angeles area.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bolos BOLO</td>
<td>443</td>
</tr>
<tr>
<td>U) Outlook (U//FDUO</td>
<td>442</td>
</tr>
<tr>
<td><a href="mailto:info@counterdrugtraining.com">info@counterdrugtraining.com</a> counterdrug...</td>
<td>441</td>
</tr>
<tr>
<td>Clothing / Shoes Value of Goods Taken</td>
<td>440</td>
</tr>
<tr>
<td>Cybersecurity and Infrastructure Security ...</td>
<td>440</td>
</tr>
<tr>
<td>US Customs</td>
<td>440</td>
</tr>
<tr>
<td>Wall Street Journal</td>
<td>439</td>
</tr>
<tr>
<td>ADDITIONAL FACTORS K-9</td>
<td>438</td>
</tr>
<tr>
<td>George Floyd</td>
<td>438</td>
</tr>
<tr>
<td>Justice Department</td>
<td>438</td>
</tr>
<tr>
<td>Perpetrator Information Center</td>
<td>437</td>
</tr>
<tr>
<td>Larry Mack</td>
<td>436</td>
</tr>
<tr>
<td>Leticia False Compartment</td>
<td>436</td>
</tr>
<tr>
<td>Royal Canadian Mounted Police</td>
<td>436</td>
</tr>
<tr>
<td>John McCoy</td>
<td>435</td>
</tr>
<tr>
<td>Suspicious Ac</td>
<td>434</td>
</tr>
<tr>
<td>Updated Informa</td>
<td>433</td>
</tr>
<tr>
<td>Prophet Muhammad</td>
<td>431</td>
</tr>
<tr>
<td>Column 1</td>
<td>Column 2</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Intel Bulletins
- Shared Files, Emails, Reports
- User Registrations
- Training Registrations
- Survey Responses
Orange County License Plate Reader Program

The purpose of this training bulletin is to provide Orange County law enforcement officers with a brief tutorial on the new license plate reader initiative, which was purchased under the US Department of Homeland Security’s Anaheim/Santa Urban Area Security Initiative (UASI) grant program. The Automated License Plate Reader (ALPR) technology provided by Vigilant Video has deployed to all Orange County law enforcement agencies in the Operational Area. To access the ALPR program, law enforcement personnel must contact their agency representative for training and log-in information. In addition, users of the ALPR system will be required to follow agency polices involving the system, which may vary amongst agencies.

OVERVIEW

The standard configuration of the ALPR system on a patrol vehicle is a set of two forward facing cameras and two rear facing cameras mounted on the vehicle. Mounted cameras can capture two types of images, standard color images during daylight and infrared (IR) images using IR light to reflect an image of the license plate. In both instances, only the license plate image is captured. However, older style license plates (California Blue and Black) may not successfully be captured by ALPR since the older versions are non-reflective.
(U//FOUO) iPhone App May Expose Officer Phones

(U//LES) In late January, a local law enforcement officer working at a large event received a message on his iPhone apparently from an attendee standing nearby. The message was likely delivered using the AirDrop application and may have been an attempt to compromise the officer’s phone with a malicious file. Law enforcement officers are encouraged to keep AirDrop turned off, especially when working at large events.

- (U) AirDrop is a file transfer application found on Apple devices that uses Bluetooth to establish a secure connection between two Apple devices in order to share an image, video, or other file.
- (U//FOUO) When AirDrop is enabled, users can select other Apple devices with AirDrop enabled within a 30 foot radius and send files. If the device name includes the officer’s name or agency, the app displays this information to anyone also using AirDrop.
- (U) Malicious actors can technically infect a device by sending a malicious link or image via AirDrop. A user must accept and then click on the message to enable the malicious activity.

(U//FOUO) The NCRIC has no additional reporting of similar events. Open source reporting does not show any discussion of the tactic being advocated to compromise iPhones. AirDrop has been used to send prank messages.
● Full Names
● Email Addresses
● Postal Addresses
● Phone Numbers
● Identity Numbers (SOC, OLN)
● IP Addresses
● Passwords
NATIONAL SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL INVESTIGATIVE DIVISION
SACRAMENTO DIVISION

(U) Approved for Release:

(SIIR-00321815682)

(U/FOUO) Unidentified Darknet User(s) Sent Personally Identifiable Information of Federal Law Enforcement Officers to Darknet Website Admins

(U) Source: An anonymous tip reported to a monitored FBI e-mail account.

(U/LES) The purpose of this National Situational Information Report is to advise law enforcement personnel and public safety officials about threats to life by unidentified Darknet user(s) using the name DEEPSTATE.

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U/LES) in this document is the property of the Federal Bureau of Investigation and may be distributed within the federal government (and its contractors), US Intelligence, law enforcement, public safety, or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network without first obtaining FBI approval.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the SACRAMENTO DIVISION and CRIMINAL INVESTIGATIVE DIVISION.

UNCLASSIFIED/LAW ENFORCEMENT SENSITIVE

(U/LES) The FBI assesses Darknet Market (DNM) actors likely convert illicitly obtained Bitcoin into anonymity-enhanced cryptocurrency (AEC) Monero using the MorphoToken cryptocurrency exchange, impeding law enforcement’s ability to trace the destination of the proceeds. This assessment is made with high confidence, based on FBI investigations, blockchain analysis, use of proprietary software, information from MorphoToken, and information obtained from Darknet sites and forums that cater to DNM actors. The FBI assumes the DNM actors’ intent of converting cryptocurrencies is not to diversify their cryptocurrency portfolio if this assumption is incorrect, it could mean DNM actors are not using AECs for operational security purposes and the FBI’s confidence in the assessment would decrease. The FBI bases this assessment on reporting of DNM actors converting Bitcoin to Monero, the availability of information on the inability to trace Monero, and the means of acquiring it without providing any information.

(U/FOUO) As of January 2020, DNM actors associated with Apolon DNM sent at least 11 Bitcoin (worth approximately $580,000) to MorphoToken to convert to Monero between December 2019 and January 2020, according to a proprietary software tool that analyzes financial transactions of the Bitcoin blockchain and use of MorphoToken’s automated programming interface (API).

(U/FOUO) As of October 2019, FBI analysts reviewed transaction fees from Bitcoin transactions conducted on Cyphra DNM between May and September 2019 were sent to addresses associated with MorphoToken, based on an FBI investigation and blockchain analysis. All Bitcoin transactions able to be queried using MorphoToken’s API were converted to Monero.

(U/LES) As of November 2019, the FBI identified four DNM sessions that sent Bitcoin drug site proceeds to MorphoToken, based on FBI investigations, open source blockchain tracking, and use of a proprietary software tool that analyzes financial transactions of the Bitcoin blockchain.

(U) As of January 2020, sites and forums that cater to DNM actors provided guidance to obtain and use Monero. Many user posts on the topic discussed the use of

* See Appendix A: Expressions of Likelihood
* (U/FOUO) Analyst Note: AECs, unlike Bitcoins, do not publish fully public records of all transactions. This prevents law enforcement from exploiting these records to follow the flow of value through blockchain analysis, a key tool in de-anonymizing DNM actors.
* MorphoToken is a fee-based cryptocurrency exchange service. Customers select which cryptocurrency to send and receive from MorphoToken. MorphoToken operates without user accounts and does not collect user information.
* See Appendix B: Confidence in Assessments and Judgments Based on a Body of Information.
We have received official confirmation that #DDoSSecrets' primary public download server was seized by German authorities (Department of Public Prosecution Zwickau file number AZ 210 AR 396/20).

We are working to obtain additional information, but presume it is re #BlueLeaks.
If your seeding the #BlueLeaks data dump I’d highly suggest putting a copy on a ps3 or ps4 as it won’t be confiscated when a raid happens.

4:20 PM · Jul 10, 2020 · Twitter for iPhone
BLUELEAKS

Situational awareness bulletins, training materials and fusion center reports for more than 200 law enforcement agencies. Dated August 1996 to June 2020.

### DATASET DETAILS

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>Hack</td>
</tr>
<tr>
<td>SOURCE</td>
<td>Anonymous</td>
</tr>
<tr>
<td>FILE SIZE</td>
<td>269 GB</td>
</tr>
</tbody>
</table>

### DOWNLOADS (How to Download)

- **MAGNET**: [Link](#)
- **TORRENT**
- **IPFS**: Qmd:VIA
Maine Information Analysis Center

** ATTENTION: NOTICE OF DATABASE BREACH **

Consistent with Title 10, Chapter 210-B of the Maine Revised Statutes, this notice is being posted to notify the general public information that a database utilized by the Maine Information & Analysis Center (“MIAC”) was unlawfully accessed in June 2020. If you have reason to think you have been affected by this breach, please contact LT Michael P. Johnston, Director of the MIAC, at
“June 24, Maine Department of Public Safety commissioner Michael Saushuck faced questions about the activities of their fusion center at a legislative hearing...

The Maine fusion center was found to be sending their reports about political activists to ... large corporations and lobbyists.”
BILL WOULD GUT MAINE SPY AGENCY

DHS “Fusion Center” under fire for spreading far-right conspiracies, pushing racially and politically biased intel

by Nathan Bernard | Mar 8, 2021
<table>
<thead>
<tr>
<th>BlueLeaks Directory</th>
<th>Website</th>
<th>Description</th>
<th>City</th>
<th>State</th>
<th>Size (MiB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>211stbay</td>
<td>211stbay.org</td>
<td>San Francisco Bay Area Robbery Investigators</td>
<td>San Francisco</td>
<td>CA</td>
<td>2,806.77</td>
</tr>
<tr>
<td>acpriea</td>
<td>acpriea.org</td>
<td>Amarillo College Panhandle Regional Law Enforcement Academy</td>
<td>TX</td>
<td></td>
<td>215.76</td>
</tr>
<tr>
<td>acticaz</td>
<td>new.acticaz.org</td>
<td>Arizona Counter Terrorism Information Center</td>
<td>AZ</td>
<td></td>
<td>64.41</td>
</tr>
<tr>
<td>akorca</td>
<td>akorca.org</td>
<td>Alaska Organized Retail Crime Alliance (AKORCA)</td>
<td>AK</td>
<td></td>
<td>747.25</td>
</tr>
<tr>
<td>alabamafusioncenter</td>
<td>alabamafusioncenter.org</td>
<td>Alabama Fusion Center</td>
<td>Montgomery</td>
<td>AL</td>
<td>571.45</td>
</tr>
<tr>
<td>alabamalecc</td>
<td>alabamalecc.org</td>
<td>Alabama LECC</td>
<td>Orange Beach</td>
<td>AL</td>
<td>24.86</td>
</tr>
<tr>
<td>alertmidsouth</td>
<td>alertmidsouth.org</td>
<td>Alert Mid-South Organized Retail Crime Alliance</td>
<td></td>
<td></td>
<td>747.22</td>
</tr>
<tr>
<td>aoorca</td>
<td>aoorca.org</td>
<td>Arkansas Organized Retail Crime Association</td>
<td>AR</td>
<td></td>
<td>121.70</td>
</tr>
<tr>
<td>aricetxas</td>
<td>new.aricetxas.org</td>
<td>Austin Regional Intelligence Center (ARIC)</td>
<td>Austin</td>
<td>TX</td>
<td>9,530.98</td>
</tr>
<tr>
<td>atlantahida</td>
<td><a href="http://www.achida.org">www.achida.org</a></td>
<td>Atlanta Carolinas HIDTA</td>
<td></td>
<td></td>
<td>1,387.81</td>
</tr>
<tr>
<td>attackwa</td>
<td>attackwa.org</td>
<td>ATTACK WA</td>
<td>GA</td>
<td></td>
<td>264.68</td>
</tr>
<tr>
<td>azhida</td>
<td><a href="http://www.azhida.org">www.azhida.org</a></td>
<td>Welcome to Arizona HIDTA</td>
<td>Chandler</td>
<td>AZ</td>
<td>5,644.75</td>
</tr>
<tr>
<td>azorca</td>
<td>azorca.org</td>
<td>Arizona Organized Retail Crime Association (AZORCA)</td>
<td></td>
<td></td>
<td>1,658.24</td>
</tr>
<tr>
<td>bostonbric</td>
<td>survey.bostonbric.org</td>
<td>Boston Regional Intelligence Center</td>
<td>MA</td>
<td></td>
<td>1,003.72</td>
</tr>
<tr>
<td>burlingamepolice</td>
<td>coplink.burlingamepolice.info</td>
<td>Burlingame PD</td>
<td>Burlingame</td>
<td>CA</td>
<td>1,180.36</td>
</tr>
<tr>
<td>cal-orca</td>
<td>cal-orca.org</td>
<td>California Organized Retail Crimes Association</td>
<td>CA</td>
<td></td>
<td>1,962.58</td>
</tr>
<tr>
<td>calera</td>
<td>caloes.org</td>
<td>California Governor's Office of Emergency Services - Training and Exercise</td>
<td>Mather</td>
<td>CA</td>
<td>488.18</td>
</tr>
<tr>
<td>calstas</td>
<td></td>
<td>Milwaukee High Intensity Drug Trafficking Area (HIDTA)</td>
<td></td>
<td></td>
<td>2,679.36</td>
</tr>
<tr>
<td>cbaghidta</td>
<td>sdhidta.org</td>
<td>San Diego - Imperial HIDTA</td>
<td>San Diego</td>
<td>CA</td>
<td>266.14</td>
</tr>
<tr>
<td>ccroc</td>
<td>ccroc.us</td>
<td>Cook County Regional Organized Crime Task Force (CCROC)</td>
<td>IL</td>
<td></td>
<td>377.35</td>
</tr>
<tr>
<td>chicagoheat</td>
<td>chicagopeat.org</td>
<td>Chicago Heat</td>
<td>Chicago</td>
<td>IL</td>
<td>820.11</td>
</tr>
<tr>
<td>chicagolandfsg</td>
<td>chicagolandfsg.org</td>
<td>Chicagoland Financial Security Group</td>
<td>IL</td>
<td></td>
<td>118.19</td>
</tr>
<tr>
<td>ciscco</td>
<td>new.reportstreetracing.com</td>
<td>Report Colorado Street Racing</td>
<td>CO</td>
<td></td>
<td>2,919.32</td>
</tr>
<tr>
<td>cnsoa3</td>
<td>cnoregionaltraining.com</td>
<td>California Narcotic Officers Association</td>
<td>Santa Clarita</td>
<td>CA</td>
<td>814.66</td>
</tr>
<tr>
<td>cnoatfrc</td>
<td>site.cnoatfrc.org</td>
<td>California Narcotic Officers Association</td>
<td>Los Angeles</td>
<td>CA</td>
<td>162.71</td>
</tr>
<tr>
<td>cnyorca</td>
<td>new.nyorca.org</td>
<td>New York Organized Retail Crime Alliance (NYORCA)</td>
<td>NY</td>
<td></td>
<td>336.67</td>
</tr>
<tr>
<td>coorca</td>
<td>COORCA.org</td>
<td>Colorad Organized Retail Crime Alliance (COORCA)</td>
<td>CO</td>
<td></td>
<td>3,202.97</td>
</tr>
<tr>
<td>corca</td>
<td>corca.org</td>
<td>Carolinas Organized Retail Crime Alliance</td>
<td>Johnston</td>
<td>IA</td>
<td>1,242.39</td>
</tr>
<tr>
<td>counterfdrtraining</td>
<td>counterfdtraining.org</td>
<td>Midwest Counterspan Training Center</td>
<td></td>
<td></td>
<td>5,118.84</td>
</tr>
</tbody>
</table>
35,275 / 247,354 (14.3%)  
Password Hashes Cracked  
(cheaply in three days)
FOR OFFICIAL USE ONLY
This document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT (FOIA)
CONCLUSION

THE END IS NIGH
I'm doing my part!
https://forensic.coffee
akava[at]sheriff[dit]pottcounty-ia.gov