OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN BRIEF

29 JUNE 2020 IA-44932-20

CYBER

(U) Criminal Hackers Target US Law Enforcement Data

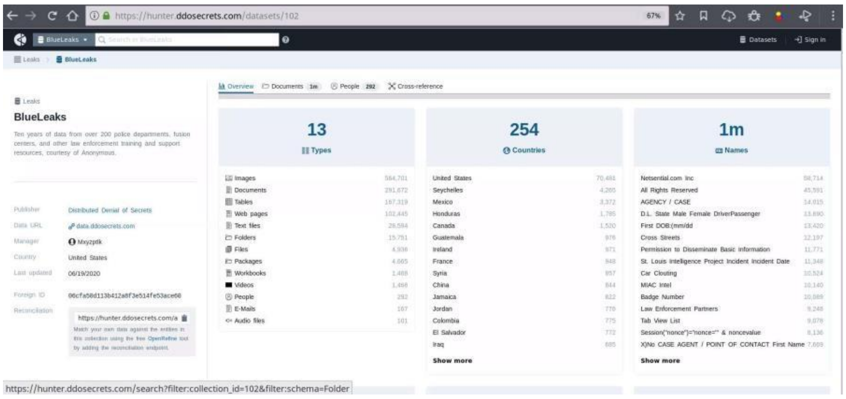
(U//FOUO) ***A criminal hacker group Distributed Denial of Secrets (DDS) on 19 June 2020 conducted a hack-and-leak operation targeting federal, state, and local law enforcement databases, probably in support of or in response to nationwide protests stemming from the death of George Floyd***. DDS leaked ten years of data from 200 police departments, fusion centers, and other law enforcement training and support resources around the globe, according to initial media and DHS reporting. DDS previously conducted hack-and-leak activity against the Russian Government.

- *(U//FOUO)* DDS claimed via Twitter (hashtag BlueLeaks) that it leaked 269 gigabytes of law enforcement documents, images, and videos, including over 400 phone numbers, 117,000 e-mails, nearly a million names, an undetermined number of user names and passwords, and unclassified intelligence reports on a website, according to CISA. A local cyber center confirmed the website hosts a large amount of sensitive fusion center, law enforcement, and state and local government data.

- *(U//FOUO)* DDS likely acquired at least some data by compromising a private company hosting the data of at least 22 fusion centers, according to the Multi-State Information and Analysis Center. Websites of the Missouri Information Analysis Center and the Missouri Intelligence and Analysis, both of which use the same company to host their data, also were compromised, according to CISA. Missouri has shut down the public-facing and administrative networks related to the websites.

- *(U//FOUO)* DDS in January 2019 targeted Russian officials in a hack-and-leak campaign, according to Russian media reporting. The leaks reportedly included 190 gigabytes of data over 10 years of correspondence between senior Russian public officials, politicians, journalists, oligarchs, religious figures, and Ukrainians, according to the same source. Russian media speculated the incident was a response to Russia's hack-and-leak activities targeting the Democratic Party to influence the outcome of the 2016 US presidential election.

(U) Prepared by the Cyber Mission Center
For questions, contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov.



https://hunter.ddosecrets.com/datasets/102

Leaks

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	Mxyzptlk
Country	United States
Last updated	06/19/2020
Foreign ID	06cfa58d113b412a8f3e514fe53ace68
Reconciliation	https://hunter.ddosecrets.com/a Match your own data against the entities in this collection using the free OpenRefine tool by adding the reconciliation endpoint.

13 Types

Images	564,701
Documents	291,672
Tables	167,319
Web pages	102,445
Text files	26,594
Folders	15,751
Files	4,936
Packages	4,665
Workbooks	1,488
Videos	1,456
People	292
E-Mails	167
Audio files	101

254 Countries

United States	70,481
Seychelles	4,265
Mexico	3,372
Honduras	1,795
Canada	1,520
Guatemala	978
Ireland	971
France	948
Syria	857
China	844
Jamaica	822
Jordan	778
Colombia	775
El Salvador	772
Iraq	695

Show more

1m Names

Netsential.com Inc	58,714
All Rights Reserved	45,591
AGENCY / CASE	14,015
D.L. State Male Female DriverPassenger	13,890
First DOB:(mm/dd	13,420
Cross Streets	12,197
Permission to Disseminate Basic Information	11,771
St. Louis Intelligence Project Incident Incident Date	11,348
Car Clouting	10,524
MIAC Intel	10,140
Badge Number	10,089
Law Enforcement Partners	9,248
Tab View List	9,076
Session("nonce")="nonce=" & noncevalue	8,136
X)No CASE AGENT / POINT OF CONTACT First Name	7,609

Show more

https://hunter.ddosecrets.com/search?filter:collection_id=102&filter:schema=Folder

(U//FOUO) Screenshot of website hosting breached date

Source, Reference, and Dissemination Information

Reporting Suspicious Activity	*(U)* **To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* **To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Operations officers are forward deployed to every U.S. state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Warning Notices & Handling Caveats	*(U)* Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS. *(U)* US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.
Customer Feedback	*(U)* Please see feedback form at the end of this document.

CLASSIFICATION:

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: **and function:**

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- □ Drive planning and preparedness efforts, training, and/or emergency response operations
- □ Observe, identify, and/or disrupt threats
- □ Share with partners
- □ Allocate resources (e.g. equipment and personnel)
- □ Reprioritize organizational focus
- □ Author or adjust policies and guidelines
- □ Initiate a law enforcement investigation
- □ Intiate your own regional-specific analysis
- □ Intiate your own topic-specific analysis
- □ Develop long-term homeland security strategies
- □ Do not plan to use
- □ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:

Organization:

Contact Number:

Position:

State:

Email:

Submit Feedback

Privacy Act Statement

CLASSIFICATION:

Product Serial Number:

REV: 01 August 2017