The Darknet Index: U.S. Government Edition

RANKING U.S.GOVERMENT AGENCIES USING DARKNET INTELLIGENCE

Introduction

One measure of cybersecurity risk involves assessing how much data is available on the darknet about a company or organization that can be misused by hackers or criminals. A greater availability of data implies a higher risk profile, as more attack vectors are available for use against the organization.

DarkOwl recently reranked the companies of the Fortune 500 based on their darknet footprints[1]. We then ranked the largest commercial entities in Germany[2].

In this report, we address how prominent U.S. government agencies, departments, and the U.S. military fare on the darknet as compared to commercial enterprises. We examine 59 large divisions of the U.S. Government to see whether they have a markedly different darknet footprint than the Fortune 500. Unfortunately, the results reveal that the U.S. Government has the largest collective darknet footprint of all of our darknet indices.

By comparing how much compromised data was available on these numerous private networks, forums and channels, and running this information through our proprietary algorithm, we reached some key takeaways about the differences and similarities between the U.S. Government and large U.S. commercial entities.

Intelligence gained from monitoring the darknets (Tor and other interconnected sources including IRC, I2P, ZeroNet, other hacker forums), as well as FTP servers, select paste sites, high-risk surface internet sites and more, constitutes what DarkOwl calls DARKINT™, or darknet intelligence. These locations attract threat actors seeking to safely sell, purchase or expose stolen data.

TABLE OF CONTENTS

1. https://www.darkowl.com/darknet-index-fortune-500
2. https://www.darkowl.com/darknet-index-germany

KEY TAKEAWAYS FROM OUR ANALYSIS

- **The U.S. Government scored worse than expected as compared to the largest U.S. firms globally.** All of the top ten (10) ranked U.S. government departments would have also ranked in the top 10 in our Fortune 500 index. Overall, the U.S. Government averaged 1.6 points higher than the average Fortune 500 company, which equates to almost a 5x footprint comparison on an aggregate basis.

- **The U.S. Navy leads the U.S. Government Index.** With an Index score of 16.6, the U.S. Navy with its estimated 300,000+ sailors beat out the U.S. Army with its 500,000+ soldiers. Had either group been part of the Fortune 500, they would have been ranked third behind only Amazon and Google. In comparison, Walmart, at 2.2 million people employed, had a much smaller darknet footprint and scored far lower with a score of 9.7.

- **Military and defense groups overall are the largest target, closely followed by Cabinet agencies.** A target's attractiveness stems from the desirability of its protected information. Whether personal or proprietary, it would appear that the groups more closely linked to defense have data that cyber criminals find attractive. Six (6) of the top ten (10) rankings were related to the military. No direct law enforcement, independent, commerce or government branch were in the top echelon, with the exception of the Department of Justice which arguably spans all three (3) categories.

- **Hacked valuable data = increased risk.** The highest scoring government agencies all had credentials and/or intellectual property exposed on the darknet which can be monetized by others. This is identical to commercial enterprises, with the exception that the U.S. Government just seems to have a greater amount of darknet exposure.

- **Vigilance pays off, as shown by the industry's overall standing.** Investing in cybersecurity has tangible index score benefits. While there were exceptions, agencies that take information security seriously should have smaller darknet footprints and, thus, lower Index ratings.

Methodology

One of the biggest hurdles to widespread awareness of darknet activity is the lack of any reliable indices. Unlike the surface web, on which many organizations continuously capture and record internet activity in a historical archive, the darknet is designed to be difficult to trace. The use of special browsers is often required. There is no comprehensive search engine for the darknet, and darknet sites are often put up and taken down within a matter of minutes to maintain anonymity.

As a result, the darknet has become a safe harbor for those looking to remain private online, whether their intentions are good or bad. A high volume of criminal activity has migrated to the darknet.

DarkOwl's proprietary DarkOwl Vision platform contains an expansive database of darknet content which can be accessed via a search interface, API, data feeds and more. Leveraging this, we assessed the U.S. goverment agencies group, ultimately assigning each an overall darknet footprint score. Combined with our proprietary hackishness algorithm — which rates darknet postings based on their potential for criminal use — our calculations yield notable results every time we take a snapshot and perform a static index analysis.

While comparing one static sample's results to another's is not statistically rigorous, if the time frames involved are sufficiently short the conclusions should hold up. Over time, DarkOwl Vision's data continuously improves with its machine-learning protocols so if there is a bias, it is toward higher scores over time.

To compile this U.S. Goverment Darknet Index, we ran each U.S. agency through the DarkOwl Vision database. We focused on specific darknets for matches on each company's website and email domains, and then further adjusted the results based on computations of "hackishness"— our algorithmic rating system which scores based on the likelihood the data could be used for nefarious intent and/or has been recorded within a recent timeframe. Recent results, from within the last 90 days, were given the most weight, as recent breaches or data leaks containing an organization's proprietary information often make the company a target.

ALGORITHM

To compile this U.S. Government Darknet Index, we considered calculations beyond the algorithm used in our other indices because of the volume of non-commercial information involved. Ultimately, we opted to employ the same algorithm used in both our Fortune 500 Index and our German Index in order to make the results from each of our published indices comparable.

Our hackishness algorithm is the most critical input to these rankings as it eliminates uninteresting content hits. For simplicity, our algorithm weighted results from Tor Hidden Services and transitory sites most heavily. All results found in our database were given some weight as per the formula below:

$$H_{90}(\ln RDS + \ln RTS) = H_{ATR}(\ln ATR)$$

H_{90} = Hackishness of last 90 days results
H_{ATR} = Hackishness of all time breach results
RDS = # results from Darknet Sites
RTS = # results from Transitory Paste Sites
ATR = # results from all time breach results

KEY METHODOLOGICAL POINTS

- The U.S. Government Index was constructed with more recent data than the Fortune 500 or German indices, but there is no reason to impute any bias from that timing mismatch (measured in months).
- The Index is simple and objective. It is not biased toward agency nicknames, press mentions, agency size, senior officials' names or other subjective measures.
- The Index scale is logarithmic, meaning every point in the index reflects almost triple the profile of a single point less, assuming hackishness scores to be comparable (which often they are not).
- The Index ranking reflects the attractiveness of the target. It is not a "risk of breach." It is more closely aligned to the attractiveness of the target to a hacker while taking into account the effectiveness of their cyber defenses.
- The size of a single breach is less of a factor than the frequency of breaches over the data collection period.

Darknet Index of U.S. Goverment Agencies: The Top 10

The results of our analysis are presented below for the top ten government agencies in our U.S. Government Darknet Index. The full ranking of the 59 agencies by their darknet footprint can be found on page nine (9). We categorize all companies using the following metrics:

- **DARKINT™ Rank** - The rank of each agency based on their darknet footprint score.
- **Agency Name** - The company's name.
- **Darknet Index Score** - The darknet footprint score on which the rankings are based.
- **Sector** - The market segment of the U.S. goverment agency.

DARKINT™ Rank	Agency Name	Darknet Index Score	Sector
1	United States Navy	16.59	Defense
2	United States Army	16.02	Defense
3	Department of Defense (aggregate)	15.12	Defense
4	Department of Justice (aggregate)	15.09	Cabinet
5	Deparment of Homeland Security	14.93	Defense
6	United States Marine Corps	14.47	Defense
7	National Aeronautics and Space Administration	13.60	Independent
8	Internal Revenue Service	13.31	Independent
9	Department of Veterans Affairs	13.09	Cabinet
10	Department of State	12.66	Cabinet

OBSERVATIONS ABOUT THE TOP 10

- Unlike the U.S. Darknet Index, whose top ten (10) was dominated by six (6) technology firms, the U.S. Government Index is dominated by defense-related departments. In fact, the total number of high-ranking defense agencies would amount to six (6), if we were to count the Department of Veteran's Affairs as a Military defense-related group.
- Overall, scores of the U.S. Government Top 10 are consistent with their private company counterparts (out of a sample size of 500 from the U.S. Fortune 500 Darknet Index). While that ranking had, overall, higher scores at the top despite the smaller number of observations, the U.S. Government's top ten (10) had a high average darknet score of 12.6, while the average score of the Fortune 500 was smaller.
- What matters most is an agency's ranking as compared to others in their sector. When compared to their government counterparts, NASA, the IRS, and the DOJ are outliers, though the intellectual property held by NASA and the IRS lend intuitive sense to their rankings.

"Overall, the U.S. Government averaged 1.6 points higher than the average Fortune 500 company, meaning that the federal government has a higher degree of darknet exposure than top U.S. corporations."

U.S. GOVERMENT INDEX PROFILE ANALYSIS BY SECTOR

Sector	# Entries	Average Index Rank	Average DARKINT™ Index Score
Defense	10	19	11.09
Cabinet	16	19	10.87
Law Enforcement	6	39	5.87
Independent	24	38	6.26
Branch	3	38	6.67

We included an Index Profile Sector analysis to denote an agency's relative DARKINT™ footprint rank against comparable agencies. Overall, we found these sector results make intuitive sense.

The agency sectors fall into two (2) clear footprint categories – those with higher than average results (for example, the Defense and Cabinet sectors) and those with lower average results (such as Law Enforcement, Independents, and Branches). So far in our studies, the U.S. Government has two (2) of the three (3) largest footprint scores that DarkOwl has yet recorded. Only the German technology sector, with a score of 11.3 was higher than U.S. Defense (with a score of 11.1), or the U.S. Cabinet (at 10.9). The U.S. Technology Sector, with an average score of 9.0, seems relatively mild by comparison, especially given the logarithmic scale.

The average U.S. agency DARKINT™ score was 8.3, as compared to an average DARKINT™ score of 6.7 for the U.S. Fortune 500 Index, while the average German company's DARKINT™ score was 5.4. These are not encouraging results when one considers the amount of money expended on cybersecurity by the U.S. Government, its globally acknowledged importance in any future warfare, the growing insistence on collecting sensitive personal citizen information, and its track record of breaches.

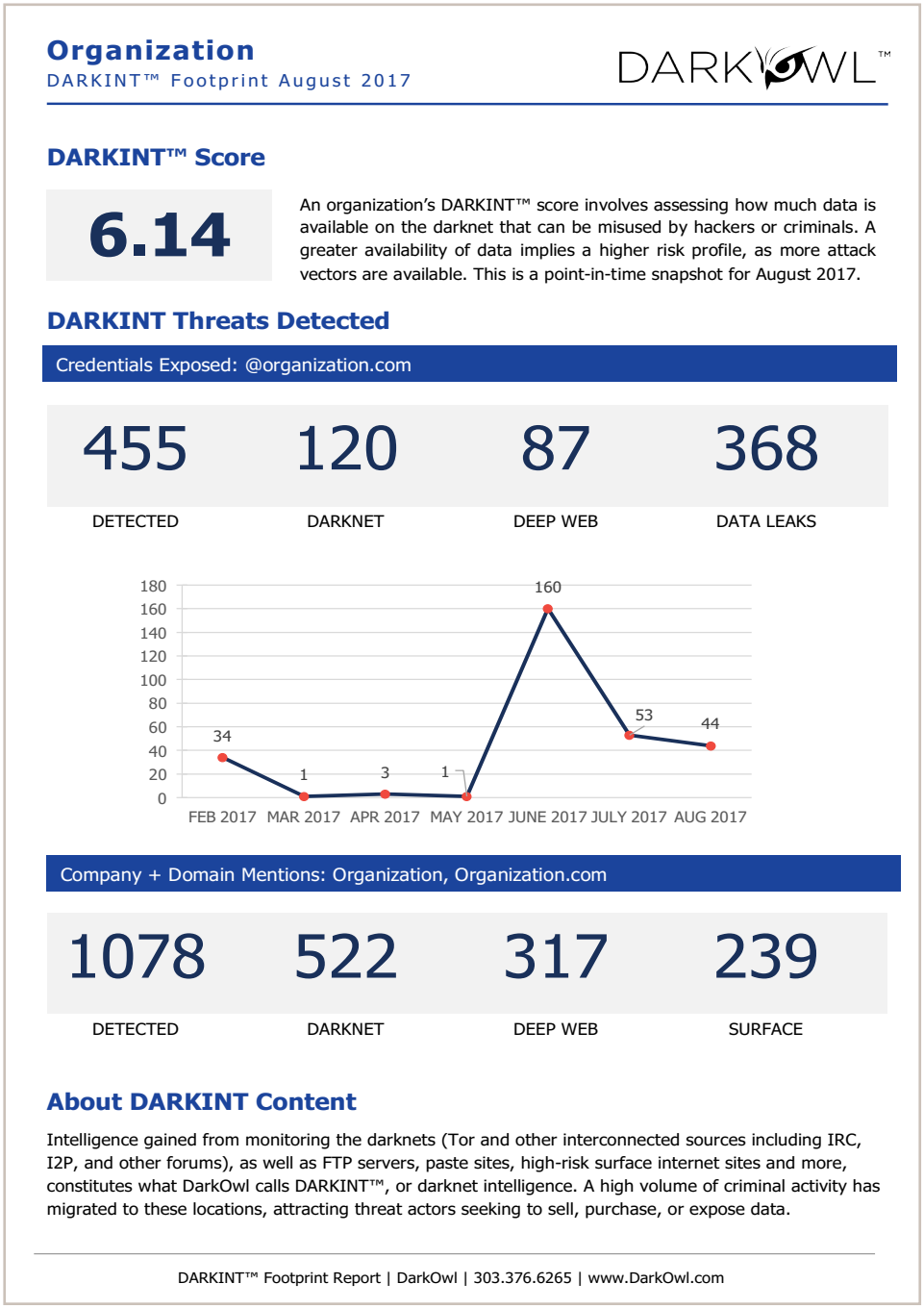
Though we cannot rule out possibilities that commercial companies spend more on information security tools and practices and better train their employees regarding information security or other factors, we suspect that the old adage about government competency sadly holds true. The frequency of government announced breaches is clearly not an anomaly. Their larger darknet footprints than even the largest and most sensitive commercial sectors suggest such troubling news will likely continue.

Conclusions

We live in an era where cybersecurity often dominates the news. Yahoo, Sony and Target are only three of the many companies subjected in recent years to costly cyber attacks, as was the Office of Personnel Management and FBI. No company or organization is immune from these types of attacks, and billions of dollars are spent annually in an attempt to protect the valuable data they hold. Measuring cybersecurity risk therefore becomes important for any company seeking to implement a comprehensive cybersecurity strategy and justify a return on the increasing investments made.

This U.S. Government Index represents only a sliver of our darknet database which includes information on tens of thousands of additional organizations and individuals. We acknowledge the limitations of our analysis and that a more accurate snapshot must include more specific company data than we have utilized for this Index. We regularly provide such customized reports to our clients, as can be seen in the sample report (pictured).

Only by monitoring a firm's customized DARKINT™ footprint over regular time intervals can the efficacy of an organizations cybersecurity efforts be reasonably evaluated. In an age where data leaks are inevitable, malware attacks make global news daily and corporate brands can be greatly diminished at a pace never before seen, it is critical to look at the darknet as a key part of any complete cybersecurity program.



Organization
DARKINT™ Footprint August 2017

DARKOWL™

DARKINT™ Score

6.14

An organization's DARKINT™ score involves assessing how much data is available on the darknet that can be misused by hackers or criminals. A greater availability of data implies a higher risk profile, as more attack vectors are available. This is a point-in-time snapshot for August 2017.

DARKINT Threats Detected

Credentials Exposed: @organization.com

455	120	87	368
DETECTED	DARKNET	DEEP WEB	DATA LEAKS

Company + Domain Mentions: Organization, Organization.com

1078	522	317	239
DETECTED	DARKNET	DEEP WEB	SURFACE

About DARKINT Content

Intelligence gained from monitoring the darknets (Tor and other interconnected sources including IRC, I2P, and other forums), as well as FTP servers, paste sites, high-risk surface internet sites and more, constitutes what DarkOwl calls DARKINT™, or darknet intelligence. A high volume of criminal activity has migrated to these locations, attracting threat actors seeking to sell, purchase, or expose data.

DARKINT™ Footprint Report | DarkOwl | 303.376.6265 | www.DarkOwl.com

THE DARKNET INDEX RANKING OF U.S. GOVERMENT AGENCIES

DARKINT™ Rank	Agency Name	Darknet Index Score	Sector
1	United States Navy	16.59	Defense
2	Unites States Army	16.02	Defense
3	Department of Defense	15.12	Defense
4	Department of Justice	15.09	Cabinet
5	Department of Homeland Security	14.93	Defense
6	United States Marine Corps	14.47	Defense
7	National Aeronautics and Space Administration	13.60	Independent
8	Internal Revenue Service	13.31	Independent
9	Department of Veterans Affairs	13.09	Cabinet
10	Department of State	12.66	Cabinet
11	Federal Bureau of Investigation	12.51	Law Enforcement
12	Department of Transportation	12.37	Cabinet
13	Department of Health and Human Services	12.23	Cabinet
14	Social Security Administration	11.95	Cabinet
15	Department of the Interior	11.77	Cabinet
16	Department of Commerce	11.61	Cabinet
17	United States Air Force	11.51	Defense
18	United States Environmental Protection Agency	11.32	Cabinet
19	National Institute of Health	11.14	Cabinet
20	United States Army Corp of Engineers	10.74	Independent
21	Department of Labor	10.57	Cabinet
22	Department of Education	9.97	Cabinet
23	General Services Administration	9.73	Independent
24	Defense Information Systems Agency	9.42	Defense

DARKINT™ Rank	Agency Name	Darknet Index Score	Sector
25	Federal Communications Commission	9.36	Independent
26	Department of Energy	9.05	Cabinet
27	Office of Personnel Management	8.98	Independent
28	United States Department of Agriculture	8.71	Cabinet
29	United States Secret Service	8.07	Law Enforcement
30	Federal Deposit Insurance Corporation	8.03	Independent
31	Nuclear Regulatory Commission	7.89	Independent
32	Security and Exchange Commission	7.71	Independent
33	Federal Trade Commission	7.70	Independent
34	National Security Agency	7.57	Defense
35	Small Business Administration	7.54	Cabinet
36	Government Accountability Office	7.53	Independent
37	Judicial Branch	7.11	Branch
38	Executive Branch (White House)	6.67	Branch
39	Legislative Branch	6.23	Branch
40	National Science Foundation	6.16	Independent
41	Federal Energy Regulatory Commission	5.92	Independent
42	Federal Emergency Management Agency	5.59	Independent
43	Food & Drug Administration	5.19	Law Enforcement
44	Office of National Security Intelligence	5.17	Defense
45	Peace Corps	5.16	Independent
46	Equal Employment Opportunity Commission	5.03	Independent
47	Department of the Treasury	4.90	Cabinet
48	Central Intelligence Agency	4.82	Law Enforcement
49	United States International Trade Commission	4.30	Law Enforcement

DARKINT™ Rank	Agency Name	Darknet Index Score	Sector
50	Consumer Product Safety Commission	4.20	Independent
51	Commodity Futures Trading Commission	4.14	Independent
52	Federal Election Commission	4.01	Independent
53	Selective Services System	3.10	Independent
54	Office of Government Ethics	2.03	Independent
55	Drug Enforcement Administration	0.34	Law Enforcement
56	Consumer Financial Protection Bureau	0.30	Independent
57	United States Cyber Command	0.11	Defense
58	Federal Reserve System	0.04	Independent
59	Office of Management & Budget	0.00	Independent

About DarkOwl

DarkOwl is based in Denver, Colorado providing darknet threat intelligence data and services to allow companies and organizations to understand and mitigate their digital risks. DarkOwl's data platform allows companies to see in real-time the theft, breach or other compromise of their proprietary data on the darknet, allowing them to both mitigate damage prior to the information being misused and to highlight gaps in their cybersecurity perimeter.

This database is believed to be the largest database of darknet content available to commercial users. DarkOwl complements this with a full range of cybersecurity consulting services, including security assessments, penetration testing, application and code review, incident response, and digital forensics.