The Darknet Index: Electric Utilities Edition

RANKING THE EDISON ELECTRIC INSTITUTE U.S. INVESTOR-OWNED (EEI-U.S.) ELECTRIC COMPANIES USING DARKNET INTELLIGENCE

Introduction

After the recently announced Equifax breach, the credit monitoring business will no longer operate in the same obscurity for either the public or the government. As the credit monitoring agencies face the imminent prospect of government regulation, we thought of examining one of those few industries that already work under regulatory scrutiny. Public electric utilities are regulated for just this reason — electricity is simply too important, and this importance is recognized as a potential threat to national security.

In fact, one of the first acknowledged U.S. electric utility network intrusions coincidentally took place around the same time as Equifax lost their data. On July 6, 2017, The New York Times reported "administrative and business networks" were compromised at Wolf Creek Nuclear Operating Corporation. We thought it might be helpful to rank industry participants on this less dramatic but potentially more catastrophic threat - the well-documented but far more mundane vulnerability of the U.S. electrical grid.

DarkOwl regularly assesses cybersecurity risk by objectively scoring how much company-related data is available on the darknet, and then measuring both the quality of that data to a potential attacker as well as its freshness. The greater availability of this data, and the shorter the length of time it has been on the darknet implies a higher risk profile, as more attack vectors are available to potentially use against the organization.

TABLE OF CONTENTS

Having recently re-ranked the Fortune 500[1] as well as the U.S. Government's divisions[2], DarkOwl has now ranked the Edison Electric Institute's U.S. Investor-Owned Electric Companies based on their darknet footprints. How does the electric utility industry stack up against other commercial enterprises?

Intelligence gained from monitoring the darknets (TOR, IRC, I2P, Zeronet, other hacker forums), as well as FTP servers, over 100 paste sites, high-risk surface internet, and other transitory sites constitutes what DarkOwl calls DARKINT™, short for darknet intelligence. These internet locations attract threat actors seeking to safely sell, purchase or expose stolen data.

We examined all 70 of the Edison Electric Institute's U.S. Investor-Owned Electric Companies' (EEI-U.S.) profiles on the darknet to see how their darknet footprint compares to the other indices we have released. Overall this group performed extremely consistently with other commercial enterprises we've examined (with a few notable exceptions) and far better than the government agencies who regulate them.

By comparing how much compromised EEI-U.S. data was available on numerous private internet 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. Utility industry and other U.S. industries.

"Cyber threats to the electricity system are increasing in sophistication, magnitude, and frequency"

– U.S. Department of Energy in Transforming the Nation's Electricity System (January, 2017)

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

KEY TAKEAWAYS FROM OUR ANALYSIS

- **As a whole, the EEI-U.S. group scored almost identically to the Fortune 500.** The average Darknet Index score of the EEI-U.S. group was 6.65, with a standard deviation of 2.60 while the average Fortune 500 firm clocked in at 6.72 on our Fortune 500 Darknet Index with a standard deviation of 2.56. While all of the Fortune 500 firms had a presence on the darknet, only one small utility managed to avoid any darknet presence. These results are consistent with the Fortune 500's Energy Sector (6.32), though it is worth noting that the average electric utility firm examined is much smaller than the energy firms in the Fortune 500.
- **Pacific Gas & Electric (PG&E) leads the EEI-U.S. Index, but Entergy and Consolidated Edison (Con Ed) were not far behind.** With a score of 11.5, PG&E scored higher than Hewlett-Packard and would have ranked 19 on the Fortune 500 Darknet Index. Entergy and Con Ed scored a nearly identical 11.4, and so both would have been in the top 25 had they been part of our Fortune 500 Darknet Index.
- **All Edison Utility Industry companies have a manageable darknet footprint.** Over the last 90 days, we found less than 50 observations for any given electric utility firm. Unlike another regulated industries, such as banking, staying up-to-date on the most recent darknet postings requires relatively less investment.
- **Large Electric Utilities are the largest darknet targets.** All of the top 10 footprints were held by companies with a market capitalization of over $10 billion. The attractiveness of larger enterprises to threat actors intent on disrupting service is obvious, as penetrating their systems can wreak the most havoc.
- **Hacked valuable data = increased risk.** The lack of commercial value for utility customer information is unique to utilities, and might have resulted in lower darknet scores. All criminals may not value electric utility information but certain cyber threat actors, and perhaps also foreign nation-state actors, do. The dominant presence of these groups on the darknet likely accounts for the surprising amount sensitive utility industry information that can be found there.
- **Vigilance pays off, as shown by the industry's notables.** Investing in cybersecurity has tangible Darknet Index score benefits. While there were exceptions, companies who take cybersecurity seriously (and can convince their utility commission that their security spending is prudent), will have smaller darknet footprints and, thus, lower Electric Utility Index scores. For example, Sempra Energy has a similar market capitalization to PG&E but scored only 7.7, meaning that their darknet footprint was about 1% of their California-based peer's. In addition, our results did not find recent darknet exposure on Sempra over the past 90 days.

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 and preferred access 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 and other threat actor 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 SaaS platform, API, data feeds, and curated services. Leveraging this database, we assessed each EEI-U.S. utility, ultimately assigning every one with a footprint on the darknet an overall score. Combined with our proprietary hackishness algorithm — which uses machine learning to rate the content of 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.

To compile our Electric Utility Darknet Index, we ran each EEI-U.S. member through the DarkOwl Vision database. We focused on specific matches on each company's website and email domains, and then further adjusted the results based on computations of hackishness. We also weighted data based on how recently the data was found in the darknets: 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 are most useful in targeting organizations.

ALGORITHM

For the purpose of compiling this Electric Utility Darknet Index, we used the exact same algorithm as we did for our other indices.

Our hackishness algorithm (embedded within our ranking algorithm) is the most critical input to these rankings as it eliminates uninteresting content hits. For simplicity, our algorithm weighted results from Darknet Hidden Services (such as Tor) 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 Electric Utility Darknet Index was constructed with more recent data than our earlier Indices. In addition, we have refined our "hackishness" calculations so that they more accurately reflect the data.
- The Index is simple and objective. It is not biased toward company nicknames, press mentions, company 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, particularly across different time frames).
- 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 EEI-U.S. Companies: The Top 10

The results of our analysis are presented below for the top 10 entities in our EEI-U.S. Darknet Index. The full ranking of the 70 entrants by their darknet footprint can be found in the EEI-U.S. Darknet Index section on Page 9. Each is ranked with the following associated data:

- **DARKINT™ Rank** - The rank of each agency based on their darknet footprint score.
- **Company** - The company's name.
- **Darknet Index Score** - The darknet footprint score on which the rankings are based.

DARKINT™ Rank	Company	Darknet Index Score
1	PG&E Corporation	11.55
2	Entergy Corporation	11.42
3	Consolidated Edison	11.41
4	Duke Energy	10.93
5	NextEra Energy	10.84
6	American Electric Power	10.74
7	Ameren Corporation	10.46
8	AVANGRID	10.16
9	Xcel Energy	10.02
10	FirstEnergy	9.64

Conclusions

We live in an era where cybersecurity often dominates the news. No company or organization is immune from breaches, and billions of dollars are spent annually in an attempt to protect the valuable data they hold. Measuring cybersecurity risk therefore becomes particularly important for utilities seeking to implement a comprehensive cybersecurity strategy in order to justify ever increasing investments made to their utility rate commissions. Manually looking for such information is too time consuming for every utility to find such sporadic results, and investing in sophisticated security systems may be overkill. Data monitoring for recently scraped darknet results can enable more effective deployment of resources given the regulatory mandate to control costs.

The integrity of a utility's critical information infrastructure is no less critical than that of its power plants or transmission lines. They simply need to work reliably, continuously, and safely in order to complete their public service mission. When key customer or infrastructure information is found on the darknet, the Electric Utility Industry is in the unique position to potentially capitalize the costs of mitigation, forensics, and issue resolution. Since this industry frequently brings in outside experts for major project repairs, potential cybersecurity threats to the grid should be monitored, mitigated and repaired with similar specialized outsourced resources.

This Electric Utility Darknet Index represents 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 much 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 on Page 8.

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, especially for an industry with regulators who often assess risk, rate base, and public service using their rear-view mirror. Best to engage experts in DARKINT, particularly if they can demonstrate cost-effective security solutions.

SAMPLE DARKINT FOOTPRINT REPORT

Organization

DARKINT™ Footprint August 2017

DARKINT™ Score

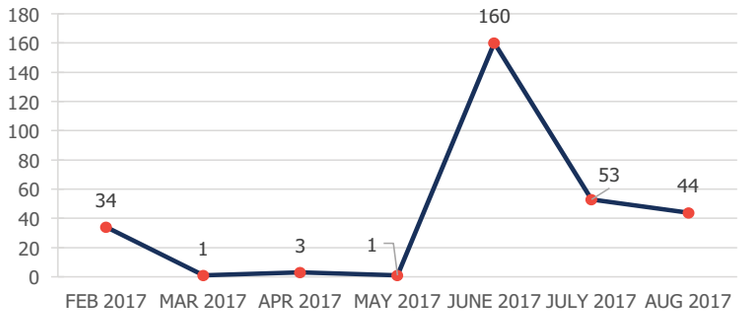
6.14

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.

THE DARKNET INDEX RANKING OF ELECTRIC UTILITY COMPANIES

DARKINT™ Rank	Company	Darknet Index Score
1	PG&E Corporation	11.55
2	Entergy Corporation	11.42
3	Consolidated Edison	11.41
4	Duke Energy	10.93
5	NextEra Energy	10.84
6	American Electric Power	10.74
7	Ameren Corporation	10.46
8	AVANGRID	10.16
9	Xcel Energy	10.02
10	FirstEnergy	9.64
11	CenterPoint Energy	9.52
12	AES Corporation	8.92
13	Exelon Corporation	8.89
14	Alliant Energy Corporation	8.85
15	Southern Company	8.69
16	Puget Holdings	8.67
17	Dominion Energy	8.58
18	SCANA Corporation	8.53
19	Berkshire Hathaway Energy	8.50
20	ALLETE	8.44
21	Tennessee Valley Authority	8.24
22	Pinnacle West Capital Corporation	8.20
23	OGE Energy Corporation	8.00

DARKINT™ Rank	Company	Darknet Index Score
24	PPL Corporation	7.95
25	National Grid	7.76
26	Sempra Energy	7.72
27	Great Plains Energy	7.57
28	Energy Future Holdings Corporation	7.47
29	Public Service Enterprise Group	7.38
30	WEC Energy Group	7.29
31	Edison International	7.16
32	Portland General Electric	7.03
33	Emera	6.93
34	UGI Corporation	6.77
35	Westar Energy	6.69
36	UNS Energy Corporation	6.54
37	Avista Corporation	6.46
38	Vectren Corporation	6.43
39	IDACORP	6.42
40	MDU Resources Group	6.30
41	Otter Tail Corporation	6.23
42	NiSource	6.22
43	CMS Energy	6.09
44	Los Angeles Department of Water and Power	5.91
45	DTE Energy	5.89

DARKINT™ Rank	Company	Darknet Index Score
46	PNM Resources	5.73
47	Austin Energy	5.40
48	Chesapeake Utilities Corporation	5.17
49	Ambit Energy	4.89
50	Central Hudson Energy Group	4.82
51	Black Hills Corporation	4.73
52	NorthWestern Energy	4.54
53	El Paso Electric	4.47
54	Liberty Utilities	4.46
55	MGE Energy	4.28
56	Unitil Corporation	4.25
57	Gaz Metro (Quebec)	4.22
58	ITC Holdings Corp	4.10
59	Cleco Corporate Holdings	4.03
60	Hawaiian Electric Industries	3.99
61	OneGas	3.94
62	Eversource Energy	3.91
63	Central Vermont Public Service Corp	3.71
64	LS Power	3.49
65	Northern New England Power Corporation	3.30
66	United Power Collective	3.11
67	Duquesne Light Company	3.07
68	InfraREIT	1.46
69	Mt. Carmel Public Utility Company	1.21
70	Tacoma Public Utilities	0.00

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.